

Contents

Preface xi

1 Introduction 1

I QUANTUM BUILDING BLOCKS 7

2 Single-Qubit Quantum Systems 9

- 2.1 The Quantum Mechanics of Photon Polarization 9
 - 2.1.1 A Simple Experiment 10
 - 2.1.2 A Quantum Explanation 11
- 2.2 Single Quantum Bits 13
- 2.3 Single-Qubit Measurement 16
- 2.4 A Quantum Key Distribution Protocol 18
- 2.5 The State Space of a Single-Qubit System 21
 - 2.5.1 Relative Phases versus Global Phases 21
 - 2.5.2 Geometric Views of the State Space of a Single Qubit 23
 - 2.5.3 Comments on General Quantum State Spaces 25
- 2.6 References 25
- 2.7 Exercises 26

3 Multiple-Qubit Systems 31

- 3.1 Quantum State Spaces 32
 - 3.1.1 Direct Sums of Vector Spaces 32
 - 3.1.2 Tensor Products of Vector Spaces 33
 - 3.1.3 The State Space of an n -Qubit System 34
- 3.2 Entangled States 38
- 3.3 Basics of Multi-Qubit Measurement 41
- 3.4 Quantum Key Distribution Using Entangled States 43
- 3.5 References 44
- 3.6 Exercises 44

4 Measurement of Multiple-Qubit States 47

- 4.1 Dirac's Bra/Ket Notation for Linear Transformations 47
- 4.2 Projection Operators for Measurement 49

- 6.5 References 120
- 6.6 Exercises 121

II QUANTUM ALGORITHMS 123

7 Introduction to Quantum Algorithms 125

- 7.1 Computing with Superpositions 126
 - 7.1.1 The Walsh-Hadamard Transformation 126
 - 7.1.2 Quantum Parallelism 128
- 7.2 Notions of Complexity 130
 - 7.2.1 Query Complexity 131
 - 7.2.2 Communication Complexity 132
- 7.3 A Simple Quantum Algorithm 132
 - 7.3.1 Deutsch's Problem 133
- 7.4 Quantum Subroutines 134
 - 7.4.1 The Importance of Unentangling Temporary Qubits in Quantum Subroutines 134
 - 7.4.2 Phase Change for a Subset of Basis Vectors 135
 - 7.4.3 State-Dependent Phase Shifts 138
 - 7.4.4 State-Dependent Single-Qubit Amplitude Shifts 139
- 7.5 A Few Simple Quantum Algorithms 140
 - 7.5.1 Deutsch-Jozsa Problem 140
 - 7.5.2 Bernstein-Vazirani Problem 141
 - 7.5.3 Simon's Problem 144
 - 7.5.4 Distributed Computation 145
- 7.6 Comments on Quantum Parallelism 146
- 7.7 Machine Models and Complexity Classes 148
 - 7.7.1 Complexity Classes 149
 - 7.7.2 Complexity: Known Results 150
- 7.8 Quantum Fourier Transformations 153
 - 7.8.1 The Classical Fourier Transform 153
 - 7.8.2 The Quantum Fourier Transform 155
 - 7.8.3 A Quantum Circuit for Fast Fourier Transform 156
- 7.9 References 158
- 7.10 Exercises 159

8 Shor's Algorithm 163

- 8.1 Classical Reduction to Period-Finding 164
- 8.2 Shor's Factoring Algorithm 164
 - 8.2.1 The Quantum Core 165
 - 8.2.2 Classical Extraction of the Period from the Measured Value 166
- 8.3 Example Illustrating Shor's Algorithm 167
- 8.4 The Efficiency of Shor's Algorithm 169
- 8.5 Omitting the Internal Measurement 170
- 8.6 Generalizations 171
 - 8.6.1 The Discrete Logarithm Problem 172
 - 8.6.2 Hidden Subgroup Problems 172

4.3	Hermitian Operator Formalism for Measurement	53
4.3.1	The Measurement Postulate	55
4.4	EPR Paradox and Bell's Theorem	60
4.4.1	Setup for Bell's Theorem	62
4.4.2	What Quantum Mechanics Predicts	62
4.4.3	Special Case of Bell's Theorem: What Any Local Hidden Variable Theory Predicts	63
4.4.4	Bell's Inequality	64
4.5	References	65
4.6	Exercises	66
5	Quantum State Transformations	71
5.1	Unitary Transformations	72
5.1.1	Impossible Transformations: The No-Cloning Principle	73
5.2	Some Simple Quantum Gates	74
5.2.1	The Pauli Transformations	75
5.2.2	The Hadamard Transformation	76
5.2.3	Multiple-Qubit Transformations from Single-Qubit Transformations	76
5.2.4	The Controlled-NOT and Other Singly Controlled Gates	77
5.3	Applications of Simple Gates	80
5.3.1	Dense Coding	81
5.3.2	Quantum Teleportation	82
5.4	Realizing Unitary Transformations as Quantum Circuits	84
5.4.1	Decomposition of Single-Qubit Transformations	84
5.4.2	Singly-Controlled Single-Qubit Transformations	86
5.4.3	Multiply-Controlled Single-Qubit Transformations	87
5.4.4	General Unitary Transformations	89
5.5	A Universally Approximating Set of Gates	91
5.6	The Standard Circuit Model	93
5.7	References	93
5.8	Exercises	94
6	Quantum Versions of Classical Computations	99
6.1	From Reversible Classical Computations to Quantum Computations	99
6.1.1	Reversible and Quantum Versions of Simple Classical Gates	101
6.2	Reversible Implementations of Classical Circuits	103
6.2.1	A Naive Reversible Implementation	103
6.2.2	A General Construction	106
6.3	A Language for Quantum Implementations	110
6.3.1	The Basics	111
6.3.2	Functions	112
6.4	Some Example Programs for Arithmetic Operations	115
6.4.1	Efficient Implementation of AND	115
6.4.2	Efficient Implementation of Multiply-Controlled Single-Qubit Transformations	116
6.4.3	In-Place Addition	117
6.4.4	Modular Addition	117
6.4.5	Modular Multiplication	118
6.4.6	Modular Exponentiation	119

8.7	References	175
8.8	Exercises	176
9	Grover's Algorithm and Generalizations	177
9.1	Grover's Algorithm	178
9.1.1	Outline	178
9.1.2	Setup	178
9.1.3	The Iteration Step	180
9.1.4	How Many Iterations?	181
9.2	Amplitude Amplification	183
9.2.1	The Geometry of Amplitude Amplification	185
9.3	Optimality of Grover's Algorithm	188
9.3.1	Reduction to Three Inequalities	189
9.3.2	Proofs of the Three Inequalities	191
9.4	Derandomization of Grover's Algorithm and Amplitude Amplification	193
9.4.1	Approach 1: Modifying Each Step	194
9.4.2	Approach 2: Modifying Only the Last Step	194
9.5	Unknown Number of Solutions	196
9.5.1	Varying the Number of Iterations	197
9.5.2	Quantum Counting	198
9.6	Practical Implications of Grover's Algorithm and Amplitude Amplification	199
9.7	References	200
9.8	Exercises	201
III	ENTANGLED SUBSYSTEMS AND ROBUST QUANTUM COMPUTATION	203
10	Quantum Subsystems and Properties of Entangled States	205
10.1	Quantum Subsystems and Mixed States	206
10.1.1	Density Operators	207
10.1.2	Properties of Density Operators	213
10.1.3	The Geometry of Single-Qubit Mixed States	215
10.1.4	Von Neumann Entropy	216
10.2	Classifying Entangled States	218
10.2.1	Bipartite Quantum Systems	218
10.2.2	Classifying Bipartite Pure States up to LOCC Equivalence	222
10.2.3	Quantifying Entanglement in Bipartite Mixed States	224
10.2.4	Multipartite Entanglement	225
10.3	Density Operator Formalism for Measurement	229
10.3.1	Measurement of Density Operators	230
10.4	Transformations of Quantum Subsystems and Decoherence	232
10.4.1	Superoperators	233
10.4.2	Operator Sum Decomposition	234
10.4.3	A Relation Between Quantum State Transformations and Measurements	238
10.4.4	Decoherence	239
10.5	References	240
10.6	Exercises	240

11	Quantum Error Correction	245
11.1	Three Simple Examples of Quantum Error Correcting Codes	246
11.1.1	A Quantum Code That Corrects Single Bit-Flip Errors	246
11.1.2	A Code for Single-Qubit Phase-Flip Errors	251
11.1.3	A Code for All Single-Qubit Errors	252
11.2	Framework for Quantum Error Correcting Codes	253
11.2.1	Classical Error Correcting Codes	254
11.2.2	Quantum Error Correcting Codes	257
11.2.3	Correctable Sets of Errors for Classical Codes	258
11.2.4	Correctable Sets of Errors for Quantum Codes	259
11.2.5	Correcting Errors Using Classical Codes	261
11.2.6	Diagnosing and Correcting Errors Using Quantum Codes	264
11.2.7	Quantum Error Correction across Multiple Blocks	268
11.2.8	Computing on Encoded Quantum States	268
11.2.9	Superpositions and Mixtures of Correctable Errors Are Correctable	269
11.2.10	The Classical Independent Error Model	270
11.2.11	Quantum Independent Error Models	271
11.3	CSS Codes	274
11.3.1	Dual Classical Codes	274
11.3.2	Construction of CSS Codes from Classical Codes Satisfying a Duality Condition	275
11.3.3	The Steane Code	278
11.4	Stabilizer Codes	280
11.4.1	Binary Observables for Quantum Error Correction	280
11.4.2	Pauli Observables for Quantum Error Correction	282
11.4.3	Diagnosing and Correcting Errors	283
11.4.4	Computing on Encoded Stabilizer States	285
11.5	CSS Codes as Stabilizer Codes	289
11.6	References	290
11.7	Exercises	291
12	Fault Tolerance and Robust Quantum Computing	293
12.1	Setting the Stage for Robust Quantum Computation	294
12.2	Fault-Tolerant Computation Using Steane's Code	297
12.2.1	The Problem with Syndrome Computation	297
12.2.2	Fault-Tolerant Syndrome Extraction and Error Correction	298
12.2.3	Fault-Tolerant Gates for Steane's Code	300
12.2.4	Fault-Tolerant Measurement	303
12.2.5	Fault-Tolerant State Preparation of $ \widetilde{\pi/4}\rangle$	304
12.3	Robust Quantum Computation	305
12.3.1	Concatenated Coding	306
12.3.2	A Threshold Theorem	308
12.4	References	310
12.5	Exercises	310
13	Further Topics in Quantum Information Processing	311
13.1	Further Quantum Algorithms	311
13.2	Limitations of Quantum Computing	313

13.3	Further Techniques for Robust Quantum Computation	314
13.4	Alternatives to the Circuit Model of Quantum Computation	316
13.4.1	Measurement-Based Cluster State Quantum Computation	317
13.4.2	Adiabatic Quantum Computation	318
13.4.3	Holonomic Quantum Computation	319
13.4.4	Topological Quantum Computation	320
13.5	Quantum Protocols	320
13.6	Insight into Classical Computation	321
13.7	Building Quantum Computers	322
13.8	Simulating Quantum Systems	325
13.9	Where Does the Power of Quantum Computation Come From?	326
13.10	What if Quantum Mechanics Is Not Quite Correct?	327

APPENDIXES 329

A Some Relations Between Quantum Mechanics and Probability Theory 331

A.1	Tensor Products in Probability Theory	331
A.2	Quantum Mechanics as a Generalization of Probability Theory	337
A.3	References	339
A.4	Exercises	339

B Solving the Abelian Hidden Subgroup Problem 341

B.1	Representations of Finite Abelian Groups	341
B.1.1	Schur's Lemma	344
B.2	Quantum Fourier Transforms for Finite Abelian Groups	345
B.2.1	The Fourier Basis of an Abelian Group	345
B.2.2	The Quantum Fourier Transform Over a Finite Abelian Group	347
B.3	General Solution to the Finite Abelian Hidden Subgroup Problem	348
B.4	Instances of the Abelian Hidden Subgroup Problem	350
B.4.1	Simon's Problem	350
B.4.2	Shor's Algorithm: Finding the Period of a Function	351
B.5	Comments on the Non-Abelian Hidden Subgroup Problem	351
B.6	References	351
B.7	Exercises	352

Bibliography 353

Notation Index 365

Index 369