

Texts in Computer Science

Editors

David Gries

Fred B. Schneider

For further volumes:

<http://www.springer.com/series/3191>

Colin P. Williams

Explorations in Quantum Computing

Second edition

 Springer

Dr. Colin P. Williams
California Institute of Technology
NASA Jet Propulsion Laboratory
Oak Grove Drive 4800
Pasadena, CA 91109-8099
USA
Colin.P.Williams@jpl.nasa.gov

Series Editors

David Gries
Department of Computer Science
Upson Hall
Cornell University
Ithaca, NY 14853-7501, USA

Fred B. Schneider
Department of Computer Science
Upson Hall
Cornell University
Ithaca, NY 14853-7501, USA

ISSN 1868-0941
ISBN 978-1-84628-886-9
DOI 10.1007/978-1-84628-887-6
Springer London Dordrecht Heidelberg New York

e-ISSN 1868-095X
e-ISBN 978-1-84628-887-6

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Control Number: 2010936191

1st edition: © Springer-Verlag New York, Inc. 1998
2nd edition: © Springer-Verlag London Limited 2011
© Springer-Verlag London Limited 2011

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms of licenses issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside those terms should be sent to the publishers.

The use of registered names, trademarks, etc., in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant laws and regulations and therefore free for general use.

The publisher makes no representation, express or implied, with regard to the accuracy of the information contained in this book and cannot accept any legal responsibility or liability for any errors or omissions that may be made.

Cover design: SPI, Puducherry, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

To my wife and children

Preface

In the decade since the publication of the first edition of “Explorations in Quantum Computing” the field has blossomed into a rich and diverse body of knowledge, and tremendous progress has been made on building functional quantum computer hardware. Yet I find that a discussion of *applications* of quantum computers still remains largely confined to Shor’s algorithm for factoring composite integers and Grover’s algorithm for quantum search. As more and more books have been written on quantum computing this standard presentation has been reinforced, thereby overlooking less well known, but arguably more interesting, applications.

In this edition I have tried to survey the field of quantum computing from a fresh perspective, showing how it can be applied to solve problems in a wide range of technical areas including physics, computer science, mathematics, chemistry, simulation, and finance. For sure, many of the newer quantum algorithms have their roots in Shor’s algorithm or Grover’s algorithm, but I think it is important to appreciate how the daughter algorithms have diverged from their parents. Moreover, there are now several quantum transforms known, such as the quantum wavelet and quantum cosine transforms, which show promising complexity properties and yet await exploitation in practical quantum algorithms. The classical versions of these transforms are of widespread utility in classical computing, especially signal and image processing, and I am optimistic that some fresh attention might stimulate others to find good uses for them.

The second edition is organized around four main parts. Part I addresses the question “What is Quantum Computing?” It provides the mathematical framework and physics concepts needed to understand quantum computing, and introduces the first quantum trick—quantum parallelism—and its use within the Deutsch-Jozsa algorithm. I assume the quantum circuit model but discuss several non-standard 2-qubit gates, such as SWAP ^{α} , iSWAP, and Berkeley B, that lend themselves more easily to implementation than does CNOT. In addition, I describe how to quantify the entangling power of quantum gates, and several techniques for constructing quantum circuits that achieve arbitrary n -qubit unitary, and non-unitary, operators including numerical, algebraic, and re-use methods, as well as specialized tricks for constructing optimal circuits for 2-qubit unitary operators.

Part II addresses the question “What Can you Do With a Quantum Computer?” I begin with Grover’s algorithm for quantum search, and applications thereof to speeding up randomized algorithms and synthesizing arbitrary superpositions. I then review Shor’s algorithm for factoring composite integers and computing discrete logarithms, and show how to apply these to breaking the RSA and elliptic curve public key cryptosystems. This is followed with a look at phase transition phenomena in computation and how to apply the insights gleaned from these studies to characterize the complexity of a nested quantum search I developed with Nicolas Cerf and Lov Grover for solving **NP-Complete** problems. This is followed by chapters on applications of quantum algorithms to quantum simulation, quantum chemistry and mathematics. These three areas have the greatest potential for finding new and important quantum algorithms for solving practical problems.

The second edition also includes a greatly expanded discussion of quantum information theory. In particular, in Part III “What Can you Do with Quantum Information”, I look at the notion of pure versus mixed states, density operators, entanglement, how to quantify it, the partial transpose (for signalling the presence of entanglement), the partial trace (for characterizing part of a larger quantum system), and Schmidt decompositions. I have gone beyond the standard presentations on quantum teleportation and superdense coding, to include less well known but potentially useful protocols such as quantum data compression, universal quantum cloning and universal negation—all with complete quantum circuit descriptions. I again emphasize applications of these protocols. In particular, I describe how quantum teleportation has inspired an entirely new, and very promising, model of quantum computation, and how approximate clones and approximate negated states can be used to determine the exact expectation values of observables of ideal clones and ideal negated states. I then describe the most mature of the quantum technologies—quantum cryptography—and discuss the challenges in integrating quantum cryptography with the commercial secure communications infrastructure. I survey the three main quantum key distribution protocols—Bennett and Brassard’s BB84, Bennett’s B92, and Ekert’s E91 protocols, and how they have been implemented in fiber and free-space systems, and look at the prospects for extending the range of quantum cryptography using quantum repeaters and Earth-to-Space channels.

Finally, the book concludes with Part IV “Towards Practical Quantum Computers” by examining some of the practical issues in designing scalable quantum computers. However, I have elected to focus not on hardware per se, for which many excellent texts already exist, but more on reliability and architectural issues. In particular, I describe several techniques for quantum error correction including error reduction by symmetrization, quantum error correcting codes, the optimal 5-qubit code, stabilizer codes, bounds on quantum codes, fault-tolerance and concatenated quantum codes. I end the book by discussing the amazing array of alternative models of quantum computing beyond the quantum circuit model, showing how they are inter-related, and how certain schemes lend themselves naturally to implementation in particular types of quantum computer hardware.

The new edition also includes numerous end-of-chapter exercises. Many of these were field tested on students I taught at Stanford University while teaching my “Introduction to Quantum Computing and Quantum Information Theory” course for

several years. In so doing, I learned first hand which concepts students found most difficult. Moreover, in teaching these classes and elsewhere I have learned that quantum physics appeals to many people who might not otherwise have much interest in science. For example, Playboy Playmate Carmen Elektra has been quoted as saying “*I’m really into quantum physics. Some of my friends are into it, some of them aren’t, so I’m trying to get them excited about discovering all these interesting things about thoughts and the power of thoughts. It gives me chills thinking about it. It’s fun.*” [169]. Although some of my colleagues have mocked her for saying this, I say bravo Carmen! Quantum physics is indeed an amazing branch of science, which challenges our most foundational assumptions about the nature of reality. It’s a wonderful thing when a scientific field can so electrify someone that they are compelled to seek a deeper understanding. Certainly, experience in teaching to a very diverse student body has encouraged me to explain things as simply as possible in a self-contained volume. And I hope the reader benefits from my more inclusive style. I can certainly say that Carmen Elektra’s interest in matters quantum has at least given me a more arresting answer to the question “Who did you have in mind when you wrote your book?” than is typical of most scholarly texts!

Finally, I would like to thank the people who have helped me make this second edition a reality. First my family for putting up with the countless evenings and weekends I was away from them. And to Wayne Wheeler and Simon Rees of Springer-Verlag for their encouragement, and eternal patience, in seeing the manuscript through to completion. They deserve a very big thank you! In addition, I am indebted to the physicists and computer scientists who have developed the field of quantum computing to what it is today. Many of these people are known to me personally, but some only via their research papers. I hope I have done justice to their research contributions in writing about them. Known personally to me or not, they have all greatly enriched my life via their discoveries and insights.

Colin P. Williams

Contents

Part I What is Quantum Computing?

1	Introduction	3
1.1	Trends in Computer Miniaturization	4
1.2	Implicit Assumptions in the Theory of Computation	7
1.3	Quantization: From Bits to Qubits	8
1.3.1	Ket Vector Representation of a Qubit	9
1.3.2	Superposition States of a Single Qubit	9
1.3.3	Bloch Sphere Picture of a Qubit	11
1.3.4	Reading the Bit Value of a Qubit	15
1.4	Multi-qubit Quantum Memory Registers	17
1.4.1	The Computational Basis	17
1.4.2	Direct Product for Forming Multi-qubit States	19
1.4.3	Interference Effects	20
1.4.4	Entanglement	21
1.5	Evolving a Quantum Memory Register: Schrödinger's Equation	23
1.5.1	Schrödinger's Equation	24
1.5.2	Hamiltonians	24
1.5.3	Solution as a Unitary Evolution of the Initial State	25
1.5.4	Computational Interpretation	26
1.6	Extracting Answers from Quantum Computers	26
1.6.1	Observables in Quantum Mechanics	26
1.6.2	Observing in the Computational Basis	29
1.6.3	Alternative Bases	30
1.6.4	Change of Basis	32
1.6.5	Observing in an Arbitrary Basis	34
1.7	Quantum Parallelism and the Deutsch-Jozsa Algorithm	35
1.7.1	The Problem: Is $f(x)$ Constant or Balanced?	36
1.7.2	Embedding $f(x)$ in a Quantum Black-Box Function	37
1.7.3	Moving Function Values Between Kets and Phase Factors	38
1.7.4	Interference Reveals the Decision	39
1.7.5	Generalized Deutsch-Jozsa Problem	40

1.8	Summary	44
1.9	Exercises	45
2	Quantum Gates	51
2.1	Classical Logic Gates	52
2.1.1	Boolean Functions and Combinational Logic	52
2.1.2	Irreversible Gates: AND and OR	53
2.1.3	Universal Gates: NAND and NOR	55
2.1.4	Reversible Gates: NOT, SWAP, and CNOT	57
2.1.5	Universal Reversible Gates: FREDKIN and TOFFOLI	60
2.1.6	Reversible Gates Expressed as Permutation Matrices	61
2.1.7	Will Future Classical Computers Be Reversible?	63
2.1.8	Cost of Simulating Irreversible Computations Reversibly	64
2.1.9	Ancillae in Reversible Computing	66
2.2	Universal Reversible Basis	67
2.2.1	Can All Boolean Circuits Be Simulated Reversibly?	68
2.3	Quantum Logic Gates	69
2.3.1	From Quantum Dynamics to Quantum Gates	70
2.3.2	Properties of Quantum Gates Arising from Unitarity	71
2.4	1-Qubit Gates	71
2.4.1	Special 1-Qubit Gates	71
2.4.2	Rotations About the x -, y -, and z -Axes	76
2.4.3	Arbitrary 1-Qubit Gates: The Pauli Decomposition	81
2.4.4	Decomposition of R_x Gate	83
2.5	Controlled Quantum Gates	83
2.5.1	Meaning of a “Controlled” Gate in the Quantum Context	85
2.5.2	Semi-Classical Controlled Gates	86
2.5.3	Multiply-Controlled Gates	87
2.5.4	Circuit for Controlled- U	87
2.5.5	Flipping the Control and Target Qubits	90
2.5.6	Control-on- $ 0\rangle$ Quantum Gates	90
2.5.7	Circuit for Controlled-Controlled- U	91
2.6	Universal Quantum Gates	92
2.7	Special 2-Qubit Gates	94
2.7.1	CSIGN, $SWAP^\alpha$, iSWAP, Berkeley B	95
2.7.2	Interrelationships Between Types of 2-Qubit Gates	97
2.8	Entangling Power of Quantum Gates	100
2.8.1	“Tangle” as a Measure of the Entanglement Within a State	101
2.8.2	“Entangling Power” as the Mean Tangle Generated by a Gate	103
2.8.3	CNOT from any Maximally Entangling Gate	106
2.8.4	The Magic Basis and Its Effect on Entangling Power	106
2.9	Arbitrary 2-Qubit Gates: The Krauss-Cirac Decomposition	107
2.9.1	Entangling Power of an Arbitrary 2-Qubit Gate	109

2.9.2	Circuit for an Arbitrary Real 2-Qubit Gate	110
2.9.3	Circuit for an Arbitrary Complex 2-Qubit Gate	111
2.9.4	Circuit for an Arbitrary 2-Qubit Gate Using $SWAP^{\rho\alpha}$	111
2.10	Summary	112
2.11	Exercises	113
3	Quantum Circuits	123
3.1	Quantum Circuit Diagrams	123
3.2	Computing the Unitary Matrix for a Given Quantum Circuit	124
3.2.1	Composing Quantum Gates in Series: The Dot Product	126
3.2.2	Composing Quantum Gates in Parallel: The Direct Product	127
3.2.3	Composing Quantum Gates Conditionally: The Direct Sum	128
3.2.4	Measures of Quantum Circuit Complexity	130
3.3	Quantum Permutations	131
3.3.1	Qubit Reversal Permutation: P_{2^n}	131
3.3.2	Qubit Cyclic Left Shift Permutation: Π_{2^n}	135
3.3.3	Amplitude Downshift Permutation: Q_{2^n}	137
3.3.4	Quantum Permutations for Classical Microprocessor Design?	139
3.4	Quantum Fourier Transform: QFT	140
3.4.1	Continuous Signals as Sums of Sines and Cosines	141
3.4.2	Discrete Signals as Samples of Continuous Signals	142
3.4.3	Discrete Signals as Superpositions	144
3.4.4	QFT of a Computational Basis State	145
3.4.5	QFT of a Superposition	147
3.4.6	QFT Matrix	148
3.4.7	QFT Circuit	150
3.5	Quantum Wavelet Transform: QWT	151
3.5.1	Continuous Versus Discrete Wavelet Transforms	152
3.5.2	Determining the Values of the Wavelet Filter Coefficients	154
3.5.3	Factorization of Daubechies $D_{2^n}^{(4)}$ Wavelet Kernel	157
3.5.4	Quantum Circuit for $D_{2^n}^{(4)}$ Wavelet Kernel	158
3.5.5	Quantum Circuit for the Wavelet Packet Algorithm	158
3.5.6	Quantum Circuit Wavelet Pyramidal Algorithm	160
3.6	Quantum Cosine Transform: QCT	162
3.6.1	Signals as Sums of Cosines Only	163
3.6.2	Discrete Cosine Transform DCT-II and Its Relation to DFT	163
3.6.3	QCT_N^{II} Transformation	165
3.6.4	QCT_N^{II} Matrix	165
3.6.5	QCT_N^{II} Circuit	166
3.7	Circuits for a Arbitrary Unitary Matrices	172
3.7.1	Uses of Quantum Circuit Decompositions	173

3.7.2	Choice of Which Gate Set to Use	173
3.7.3	Circuit Complexity to Implement Arbitrary Unitary Matrices	173
3.7.4	Algebraic Method	174
3.7.5	Simplification via Rewrite Rules	178
3.7.6	Numerical Method	180
3.7.7	Re-use Method	184
3.8	Probabilistic Non-unitary Quantum Circuits	190
3.8.1	Hamiltonian Built from Non-unitary Operator	191
3.8.2	Unitary Embedding of the Non-unitary Operator	191
3.8.3	Non-unitarily Transformed Density Matrix	191
3.8.4	Success Probability	193
3.8.5	Fidelity when Successful	193
3.9	Summary	194
3.10	Exercises	195
4	Quantum Universality, Computability, & Complexity	201
4.1	Models of Computation	202
4.1.1	The Inspiration Behind Turing’s Model of Computation: The <i>Entscheidungsproblem</i>	202
4.1.2	Deterministic Turing Machines	204
4.1.3	Probabilistic Turing Machines	205
4.1.4	The Alternative Gödel, Church, and Post Models	207
4.1.5	Equivalence of the Models of Computation	208
4.2	Universality	208
4.2.1	The Strong Church-Turing Thesis	208
4.2.2	Quantum Challenge to the Strong Church-Turing Thesis	209
4.2.3	Quantum Turing Machines	210
4.3	Computability	213
4.3.1	Does Quantum Computability Offer Anything New?	214
4.3.2	Decidability: Resolution of the <i>Entscheidungsproblem</i>	215
4.3.3	Proof Versus Truth: Gödel’s Incompleteness Theorem	217
4.3.4	Proving Versus Providing Proof	218
4.4	Complexity	221
4.4.1	Polynomial Versus Exponential Growth	223
4.4.2	Big $\mathcal{O}$, Θ and Ω Notation	225
4.4.3	Classical Complexity Zoo	225
4.4.4	Quantum Complexity Zoo	229
4.5	What Are Possible “Killer-Aps” for Quantum Computers?	233
4.6	Summary	234
4.7	Exercises	235
Part II What Can You Do with a Quantum Computer?		
5	Performing Search with a Quantum Computer	241
5.1	The Unstructured Search Problem	242

5.1.1	Meaning of the Oracle	243
5.2	Classical Solution: Generate-and-Test	244
5.3	Quantum Solution: Grover's Algorithm	245
5.4	How Does Grover's Algorithm Work?	247
5.4.1	How Much Amplitude Amplification Is Needed to Ensure Success?	248
5.4.2	An Exact Analysis of Amplitude Amplification	249
5.4.3	The Oracle in Amplitude Amplification	250
5.5	Quantum Search with Multiple Solutions	251
5.5.1	Amplitude Amplification in the Case of Multiple Solutions	252
5.6	Can Grover's Algorithm Be Beaten?	254
5.7	Some Applications of Quantum Search	255
5.7.1	Speeding Up Randomized Algorithms	255
5.7.2	Synthesizing Arbitrary Superpositions	256
5.8	Quantum Searching of Real Databases	260
5.9	Summary	261
5.10	Exercises	262
6	Code Breaking with a Quantum Computer	263
6.1	Code-Making and Code-Breaking	264
6.1.1	Code-Breaking: The Enigma Code and Alan Turing	265
6.2	Public Key Cryptosystems	267
6.2.1	The RSA Public-Key Cryptosystem	267
6.2.2	Example of the RSA Cryptosystem	271
6.3	Shor's Factoring Algorithm for Breaking RSA Quantumly	272
6.3.1	The Continued Fraction Trick at the End of Shor's Algorithm	276
6.3.2	Example Trace of Shor's Algorithm	280
6.4	Breaking Elliptic Curve Cryptosystems with a Quantum Computer	285
6.5	Breaking DES with a Quantum Computer	287
6.6	Summary	289
6.7	Exercises	290
7	Solving NP-Complete Problems with a Quantum Computer	293
7.1	Importance and Ubiquity of NP-Complete Problems	295
7.1.1	Worst Case Complexity of Solving NP-Complete Problems	296
7.2	Physics-Inspired View of Computational Complexity	297
7.2.1	Phase Transition Phenomena in Physics	297
7.2.2	Phase Transition Phenomena in Mathematics	299
7.2.3	Computational Phase Transitions	299
7.2.4	Where Are the <i>Really</i> Hard Problems?	302
7.3	Quantum Algorithms for NP-Complete Problems	302

7.3.1	Quantum Solution Using Grover's Algorithm	303
7.3.2	Structured Search Spaces: Trees and Lattices	304
7.4	Quantum Solution Using Nested Grover's Algorithm	308
7.4.1	The Core Quantum Algorithm	308
7.4.2	Analysis of Quantum Structured Search	309
7.4.3	Quantum Circuit for Quantum Structured Search	312
7.4.4	Quantum Average-Case Complexity	312
7.5	Summary	316
7.6	Exercises	316
8	Quantum Simulation with a Quantum Computer	319
8.1	Classical Computer Simulations of Quantum Physics	320
8.1.1	Exact Simulation and the Problem of Memory	321
8.1.2	Exact Simulation and the Problem of Entanglement	321
8.1.3	Approximate Simulation and the Problem of Fidelity	322
8.2	Quantum Computer Simulations of Quantum Physics	325
8.2.1	Feynman Conceives of a Universal Quantum Simulator	326
8.2.2	Quantum Systems with Local Interactions	326
8.2.3	Lloyd-Zalka-Wiesner Quantum Simulation Algorithm	327
8.3	Extracting Results from Quantum Simulations Efficiently	328
8.3.1	Single Ancilla-Assisted Readout	328
8.3.2	Multi-Ancilla-Assisted Readout	330
8.3.3	Tomography Versus Spectroscopy	332
8.3.4	Evaluating Correlation Functions	333
8.4	Fermionic Simulations on Quantum Computers	334
8.4.1	Indistinguishability and Implications for Particle Statistics	334
8.4.2	Symmetric Versus Anti-Symmetric State Vectors	335
8.4.3	Bosons and Fermions	336
8.4.4	Bose-Einstein Statistics	337
8.4.5	Pauli Exclusion Principle and Fermi-Dirac Statistics	337
8.4.6	Fermionic Simulations via the Jordan-Wigner Transformation	339
8.4.7	Fermionic Simulations via Transformation to Non-interacting Hamiltonians	341
8.5	Summary	344
8.6	Exercises	345
9	Quantum Chemistry with a Quantum Computer	349
9.1	Classical Computing Approach to Quantum Chemistry	349
9.1.1	Classical Eigenvalue Estimation via the Lanczos Algorithm	351
9.2	Quantum Eigenvalue Estimation via Phase Estimation	352
9.2.1	The "Phase" State	352
9.2.2	Binary Fraction Representation of the Phase Factor	353
9.3	Quantum Phase Estimation	354

9.4	Eigenvalue Kick-Back for Synthesizing the Phase State	357
9.5	Quantum Eigenvalue Estimation Algorithms	361
9.5.1	Abrams-Lloyd Eigenvalue Estimation Algorithm	361
9.5.2	Kitaev Eigenvalue Estimation Algorithm	361
9.6	Quantum Chemistry Beyond Eigenvalue Estimation	364
9.7	Summary	364
9.8	Exercises	365
10	Mathematics on a Quantum Computer	369
10.1	Quantum Functional Analysis	369
10.1.1	Quantum Mean Estimation	370
10.1.2	Quantum Counting	371
10.2	Quantum Algebraic Number Theory	375
10.2.1	The Cattle Problem of Archimedes and Pell's Equation	375
10.2.2	Why Solving Pell's Equation Is Hard	376
10.2.3	Solution by Finding the "Regulator"	377
10.2.4	The Regulator and Period Finding	378
10.2.5	Quantum Core of Hallgren's Algorithm	378
10.2.6	Hallgren's Quantum Algorithm for Solving Pell's Equation	378
10.2.7	What Is the Significance of Pell's Equation?	381
10.3	Quantum Signal, Image, and Data Processing	382
10.3.1	Classical-to-Quantum Encoding	382
10.3.2	Quantum Image Processing: 2D Quantum Transforms	384
10.3.3	Quantum-to-Classical Readout	385
10.4	Quantum Walks	385
10.4.1	One-Dimensional Quantum Walks	387
10.4.2	Example: Biased Initial Coin State & Hadamard Coin	389
10.4.3	Example: Symmetric Initial Coin State & Hadamard Coin	391
10.4.4	Example: Chiral Initial Coin State & Hadamard Coin	392
10.4.5	Example: Symmetric Initial Coin State & Non-Hadamard Coin	393
10.4.6	Quantum Walks Can Spread Faster than Classical Walks	395
10.5	Summary	397
10.6	Exercises	398

Part III What Can You Do with Quantum Information?

11	Quantum Information	403
11.1	What is Classical Information?	404
11.1.1	Classical Sources: The Shannon Entropy	405
11.1.2	Maximal Compression (Source Coding Theorem)	407
11.1.3	Reliable Transmission (Channel Coding Theorem)	408
11.1.4	Unstated Assumptions Regarding Classical Information	410

11.2	What is Quantum Information?	411
11.2.1	Pure States cf. Mixed States	411
11.2.2	Mixed States from Partial Knowledge: The Density Operator	411
11.2.3	Mixed States from Partial Ignorance: The Partial Trace	417
11.2.4	Mixed States as Parts of Larger Pure States: “Purifications”	419
11.2.5	Quantifying Mixedness	420
11.3	Entanglement	422
11.3.1	Separable States Versus Entangled States	422
11.3.2	Signalling Entanglement via Entanglement Witnesses	423
11.3.3	Signalling Entanglement via the Peres-Horodecki Criterion	425
11.3.4	Quantifying Entanglement	429
11.3.5	Maximally Entangled Pure States	431
11.3.6	Maximally Entangled Mixed States	432
11.3.7	The Schmidt Decomposition of a Pure Entangled State	433
11.3.8	Entanglement Distillation	436
11.3.9	Entanglement Swapping	441
11.3.10	Entanglement in “Warm” Bulk Matter	443
11.4	Compressing Quantum Information	444
11.4.1	Quantum Sources: The von Neumann Entropy	445
11.4.2	Schumacher-Jozsa Quantum Data Compression	445
11.4.3	“Discard-on-Fail” Quantum Data Compression Protocol	447
11.4.4	“Augment-on-Fail” Quantum Data Compression Protocol	449
11.4.5	Quantum Circuit for Schumacher-Jozsa Compressor	450
11.4.6	Is Exponential Compression Possible?	452
11.5	Superdense Coding	453
11.5.1	Bell States	454
11.5.2	Interconversion Between Bell States by Local Actions	455
11.5.3	Superdense Coding Protocol	455
11.6	Cloning Quantum Information	457
11.6.1	Historical Roots and Importance of Quantum Cloning	457
11.6.2	Impossibility of Exact Deterministic Quantum Cloning	458
11.6.3	Universal Approximate Quantum Cloning	460
11.6.4	Circuit for Quantum Cloning	463
11.6.5	Usability of the Quantum Clones	464
11.6.6	Universal Probabilistic Quantum Cloning	468
11.6.7	Broadcasting Quantum Information	470
11.7	Negating Quantum Information	470
11.7.1	Universal Quantum Negation Circuit	471
11.7.2	Expectation Value of an Observable Based on the Negated State	472
11.8	Summary	472
11.9	Exercises	474

12	Quantum Teleportation	483
12.1	Uncertainty Principle and “Impossibility” of Teleportation	483
12.1.1	Heisenberg Uncertainty Principle	484
12.2	Principles of True Teleportation	486
12.2.1	Local Versus Non-local Interactions	486
12.2.2	Non-locality: Einstein’s “Spooky Action at a Distance”	488
12.2.3	Bell’s Inequality	489
12.3	Experimental Tests of Bell’s Inequality	492
12.3.1	Speed of Non-local Influences	494
12.4	Quantum Teleportation Protocol	496
12.4.1	Teleportation Does Not Imply Superluminal Communication	499
12.5	Working Prototypes	500
12.6	Teleporting Larger Objects	501
12.7	Summary	502
12.8	Exercises	503
13	Quantum Cryptography	507
13.1	Need for Stronger Cryptography	508
13.1.1	Satellite Communications Can Be Tapped	508
13.1.2	Fiber-Optic Communications Can Be Tapped	510
13.1.3	Growing Regulatory Pressures for Heightened Security	512
13.1.4	Archived Encrypted Messages Retroactively Vulnerable	512
13.2	An Unbreakable Cryptosystem: The One Time Pad	515
13.2.1	Security of OTP: Loopholes if Used Improperly	518
13.2.2	Practicality of OTP: Problem of Key Distribution	519
13.3	Quantum Key Distribution	520
13.3.1	Concept of QKD	520
13.3.2	Security Foundations of QKD	520
13.3.3	OTP Made Practical by QKD	521
13.3.4	Varieties of QKD	521
13.4	Physics Behind Quantum Key Distribution	522
13.4.1	Photon Polarization	522
13.4.2	Single Photon Sources	523
13.4.3	Entangled Photon Sources	524
13.4.4	Creating Truly Random Bits	525
13.4.5	Encoding Keys in Polarized Photons	526
13.4.6	Measuring Photon Polarization with a Birefringent Crystal	528
13.4.7	Measuring Photon Polarization with a Polarizing Filter	529
13.5	Bennett and Brassard’s BB84 QKD Scheme	529
13.5.1	The BB84 QKD Protocol	531
13.5.2	Example: BB84 QKD in the Absence of Eavesdropping	534
13.5.3	Example: BB84 QKD in the Presence of Eavesdropping	536
13.5.4	Spedalieri’s Orbital Angular Momentum Scheme for BB84	537

13.5.5	Generalization of BB84: Brass' 6-State Protocol	538
13.6	Bennett's 2-State Protocol (B92)	539
13.6.1	The B92 QKD Protocol	539
13.6.2	Threat of "Discard-on-Fail" Unambiguous State Discrimination	540
13.7	Ekert's Entanglement-Based Protocol	541
13.7.1	The E91 Protocol	541
13.8	Error Reconciliation and Privacy Amplification	542
13.8.1	Error Reconciliation	543
13.8.2	Privacy Amplification	544
13.9	Implementations of Quantum Cryptography	545
13.9.1	Fiber-Optic Implementations of Quantum Cryptography .	545
13.9.2	Extending the Range of QKD with Quantum Repeaters .	547
13.9.3	Earth-to-Space Quantum Cryptography	548
13.9.4	Hijacking Satellites	550
13.9.5	Commercial Quantum Cryptography Systems	554
13.10	Barriers to Widespread Adoption of Quantum Cryptography . . .	555
13.10.1	Will People Perceive a Need for Stronger Cryptography?	555
13.10.2	Will People Believe the Foundations of QKD Are Solid?	556
13.10.3	Will People Trust the Warranties of Certification Agencies?	556
13.10.4	Will Wide Area Quantum Cryptography Networks Be Practical?	557
13.10.5	Will Key Generation Rate Be High Enough to Support OTP?	558
13.10.6	Will Security Be the Dominant Concern?	558
13.11	Summary	558
13.12	Exercises	560

Part IV Towards Practical Quantum Computers

14	Quantum Error Correction	567
14.1	How Errors Arise in Quantum Computing	568
14.1.1	Dissipation-Induced Bit Flip Errors	568
14.1.2	Decoherence-Induced Phase Shift Errors	569
14.1.3	Natural Decoherence Times of Physical Systems	570
14.1.4	What Makes Quantum Error Correction so Hard?	571
14.2	Quantum Error Reduction by Symmetrization	573
14.2.1	The Symmetrization Trick	574
14.2.2	Quantum Circuit for Symmetrization	576
14.2.3	Example: Quantum Error Reduction via Symmetrization .	577
14.3	Principles of Quantum Error Correcting Codes (QECCs)	579
14.3.1	Classical Error Correcting Codes	579

14.3.2	Issues Unique to Quantum Error Correcting Codes	580
14.3.3	Modeling Errors in Terms of Error Operators	581
14.3.4	Protecting Quantum Information via Encoding	583
14.3.5	Digitizing and Diagnosing Errors by Measuring Error Syndromes	585
14.3.6	Reversing Errors via Inverse Error Operators	585
14.3.7	Abstract View of Quantum Error Correcting Codes . . .	585
14.4	Optimal Quantum Error Correcting Code	588
14.4.1	Laflamme-Miquel-Paz-Zurek's 5-Qubit Code	588
14.4.2	Error Operators for the 5-Qubit Code	588
14.4.3	Encoding Scheme for the 5-Qubit Code	589
14.4.4	Error Syndromes & Corrective Actions for the 5-Qubit Code	591
14.4.5	Example: Correcting a Bit-Flip	592
14.5	Other Additive Quantum Error Correcting Codes	593
14.5.1	Shor's 9-Qubit Code	593
14.5.2	Steane's 7-Qubit Code	594
14.6	Stabilizer Formalism for Quantum Error Correcting Codes . . .	594
14.6.1	Group Theory for Stabilizer Codes	595
14.6.2	The Stabilizer	595
14.6.3	Example: A Stabilizer for the 5-Qubit Code	596
14.6.4	Using a Stabilizer to Find the Codewords It Stabilizes . .	597
14.6.5	How the Stabilizer is Related to the Error Operators . . .	599
14.6.6	Example: Stabilizers and Error Operators for the 5-Qubit Code	600
14.6.7	Stabilizer-Based Error Correction: The Encoding Step . .	603
14.6.8	Stabilizer-Based Error Correction: Introduction of the Error	603
14.6.9	Stabilizer-Based Error Correction: Error Diagnosis & Recovery	603
14.6.10	Stabilizers for Other Codes	604
14.7	Bounds on Quantum Error Correcting Codes	605
14.7.1	Quantum Hamming Bound	606
14.7.2	Quantum Singleton Bound	606
14.7.3	Quantum Gilbert-Varshamov Bound	607
14.7.4	Predicting Upper and Lower Bounds on Additive Codes .	607
14.7.5	Tightest Proven Upper and Lower Bounds on Additive Codes	611
14.8	Non-additive (Non-stabilizer) Quantum Codes	611
14.9	Fault-Tolerant Quantum Error Correcting Codes	611
14.9.1	Concatenated Codes and the Threshold Theorem	617
14.10	Errors as Allies: Noise-Assisted Quantum Computing	620
14.11	Summary	621
14.12	Exercises	622

15	Alternative Models of Quantum Computation	627
15.1	Design Principles for a Quantum Computer	627
15.2	Distributed Quantum Computer	628
15.3	Quantum Cellular Automata Model	630
15.4	Measurement I: Teleportation-Based Quantum Computer	633
15.5	Measurement II: One-Way Quantum Computer	640
15.6	Topological Quantum Computer	641
15.6.1	Topological Quantum Effects	642
15.6.2	Beyond Fermions and Bosons—Anyons	643
15.6.3	Abelian Versus Non-Abelian Anyons	644
15.6.4	Quantum Gates by Braiding Non-Abelian Anyons	644
15.6.5	Do Non-Abelian Anyons Exist?	649
15.7	Adiabatic Quantum Computing	649
15.8	Encoded Universality Using Only Spin-Spin Exchange Interactions	653
15.8.1	The Exchange Interaction	653
15.8.2	SWAP ^α via the Exchange Interaction	654
15.8.3	Problem: Although SWAP ^α Is Easy 1-Qubits Gates Are Hard	655
15.8.4	Solution: Use an Encoded Basis	655
15.8.5	$U_{\mathcal{L}}^{1,2}$, $U_{\mathcal{L}}^{2,3}$, and $U_{\mathcal{L}}^{1,3}$	656
15.8.6	R_z Gates in Encoded Basis	657
15.8.7	R_x Gates in Encoded Basis	657
15.8.8	R_y Gates in Encoded Basis	658
15.8.9	CNOT in Encoded Basis	658
15.9	Equivalences Between Alternative Models of Quantum Computation	659
15.10	Summary	660
15.11	Exercises	660
	References	663
	Index	689