Quantum Computer Science

An Introduction

In the 1990s it was realized that quantum physics has some spectacular applications in computer science. This book is a concise introduction to quantum computation, developing the basic elements of this new branch of computational theory without assuming any background in physics. It begins with a novel introduction to the quantum theory from a computer-science perspective. It illustrates the quantum-computational approach with several elementary examples of quantum speed-up, before moving to the major applications: Shor's factoring algorithm, Grover's search algorithm, and quantum error correction.

The book is intended primarily for computer scientists who know nothing about quantum theory but would like to learn the elements of quantum computation either out of curiosity about this new paradigm, or as a basis for further work in the subject. It will also be of interest to physicists who want to learn the theory of quantum computation, and to physicists and philosophers of science interested in quantum foundational issues. It evolved during six years of teaching the subject to undergraduates and graduate students in computer science, mathematics, engineering, and physics, at Cornell University.

N. DAVID MERMIN is Horace White Professor of Physics Emeritus at Cornell University. He has received the Lilienfeld Prize of the American Physical Society and the Klopsteg award of the American Association of Physics Teachers. He is a member of the U.S. National Academy of Sciences and the American Academy of Arts and Sciences. Professor Mermin has written on quantum foundational issues for several decades, and is known for the clarity and wit of his scientific writings. Among his other books are *Solid State Physics* (with N. W. Ashcroft, Thomson Learning 1976), *Boojums all the Way Through* (Cambridge University Press 1990), and *It's about Time: Understanding Einstein's Relativity* (Princeton University Press 2005).

> "This is one of the finest books in the rapidly growing field of quantum information. Almost every page contains a unique insight or a novel interpretation. David Mermin has once again demonstrated his legendary pedagogical skills to produce a classic."

> > Lov Grover, Bell Labs

"Mermin's book will be a standard for instruction and reference for years to come. He has carefully selected, from the mountain of knowledge accumulated in the last 20 years of research in quantum information theory, a manageable, coherent subset that constitutes a complete undergraduate course. While selective, it is in no sense "watered down"; Mermin moves unflinchingly through difficult arguments in the Shor algorithm, and in quantum error correction theory, providing invaluable diagrams, clear arguments, and, when necessary, extensive appendices to get the students successfully through to the end. The book is suffused with Mermin's unique knowledge of the history of modern physics, and has some of the most captivating writing to be found in a college textbook."

David DiVincenzo, IBM T. J. Watson Research Center

"Mermin's book is a gentle introduction to quantum computation especially aimed at an audience of computer scientists and mathematicians. It covers the basics of the field, explaining the material clearly and containing lots of examples. Mermin has always been an entertaining and comprehensible writer, and continues to be in this book. I expect it to become the definitive introduction to this material for non-physicists." *Peter Shor, Massachusetts Institute of Technology*

"Textbook writers usually strive for a streamlined exposition, smoothing out the infelicities of thought and notation that plague any field's early development. Fortunately, David Mermin is too passionate and acute an observer of the cultural side of science to fall into this blandness. Instead of omitting infelicities, he explains and condemns them, at the same time using his experience of having taught the course many times to nip nascent misunderstandings in the bud. He celebrates the field's mongrel origin in a shotgun wedding between classical computer scientists, who thought they knew the laws of information, and quantum physicists, who thought information was not their job. Differences remain: we hear, for example, why physicists love the Dirac notation and mathematicians hate it. Worked-out examples and exercises familiarize students with the necessary algebraic manipulations, while Mermin's lucid prose and gentle humor cajole them toward a sound intuition for what it all means, not an easy task for a subject superficially so counterintuitive."

Charles Bennett, IBM T. J. Watson Research Center

Quantum Computer Science An Introduction

N. David Mermin

Cornell University



In memory of my brother, Joel Mermin

You would have enjoyed it.

CAMBRIDGE UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning and research at the highest international levels of excellence.

www.cambridge.org Information on this title: www.cambridge.org/9780521876582

© N. D. Mermin 2007

This publication is in copyright. Subject to statutory exception and to the provisions of relevant collective licensing agreements, no reproduction of any part may take place without the written permission of Cambridge University Press.

First published 2007 4th printing 2015

Printed in the United States of America by Sheridan Books, Inc.

A catalog record for this publication is available from the British Library

ISBN 978-0-521-87658-2 Hardback

Cambridge University Press has no responsibility for the persistence or accuracy of URLs for external or third-party internet websites referred to in this publication, and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

CAMBRIDGE

Contents

Prefe	<i>page</i> xi			
A no	XV			
1 C	1			
1.1	What is a quantum computer?	1		
1.2	Cbits and their states	3		
1.3	Reversible operations on Cbits	8		
1.4	Manipulating operations on Cbits	11		
1.5	Qbits and their states	17		
1.6	Reversible operations on Qbits	19		
1.7	Circuit diagrams	21		
1.8	Measurement gates and the Born rule	23		
1.9	The generalized Born rule	28		
1.10	Measurement gates and state preparation	30		
1.11	Constructing arbitrary 1- and 2-Qbit states	32		
1.12	Summary: Qbits versus Cbits	34		
2 G	36			
2.1	The general computational process	36		
2.2	Deutsch's problem	41		
2.3	Why additional Qbits needn't mess things up	46		
2.4	The Bernstein–Vazirani problem	50		
2.5	Simon's problem	54		
2.6	Constructing Toffoli gates	58		
3 Breaking RSA encryption 63				
3.1	Period finding, factoring, and cryptography	63		
3.2	Number-theoretic preliminaries	64		
3.3	RSA encryption	66		
3.4	Quantum period finding: preliminary remarks	68		
3.5	The quantum Fourier transform	71		
3.6	Eliminating the 2-Obit gates	76		
3.7	Finding the period	79		

3.8Calculating the periodic function833.9The unimportance of small phase errors843.10Period finding and factoring864Scarching with a quantum computer884.1The nature of the search884.2The Grover iteration894.3How to construct W944.4Generalization to several special numbers964.5Searching for one out of four items985Quantum error correction995.1The miracle of quantum error correction995.2A simplified example1005.3The physics of error generation1095.4Diagnosing error syndromes1135.5The 5-Qbit error-correcting code1215.6The 7-Qbit error-correcting code1215.7Operations on 7-Qbit codewords1245.8A 7-Qbit encoding circuit1286Protocols that use just a few Qbits1366.1Bell states1366.2Quantum cryptography1376.3Bit commitment1436.4Quantum dense coding1466.5Teleportation1496.6The GHZ puzzle154A vector spaces: basic properties and Dirac notation19A.Vector spaces: basic properties and Dirac notation19Spooky action at a distance17310Spooky action at a distance17511Other aspects of Dec	viii	CON	ITENTS	
3.8 Calculating the periodic function 83 3.9 The unimportance of small phase errors 84 3.10 Period finding and factoring 86 4 Searching with a quantum computer 88 4.1 The nature of the search 88 4.2 The Grover iteration 89 4.3 How to construct W 94 4.4 Generalization to several special numbers 96 4.5 Searching for one out of four items 98 5 Quantum error correction 99 5.1 The miracle of quantum error correction 99 5.2 A simplified example 100 5.3 The physics of error generation 109 5.4 Diagnosing error syndromes 117 5.6 The 7-Qbit error-correcting code 121 5.7 The factoring circuit 127 5.9 A 5-Qbit encoding circuit 128 6 Protocols that use just a few Qbits 136 6.1 Bell states 136 6.2 Quantum dense coding 146 6.3 <t< th=""><th></th><th></th><th></th><th></th></t<>				
3.9 The unimportance of small phase errors 84 3.10 Period finding and factoring 86 4 Searching with a quantum computer 88 4.1 The anure of the search 88 4.2 The Grover iteration 89 4.3 How to construct W 94 4.4 Generalization to several special numbers 96 4.5 Searching for one out of four items 98 5 Quantum error correction 99 5.1 The miracle of quantum error correction 99 5.2 A simplified example 100 5.3 The physics of error generation 109 5.4 Diagnosing error syndromes 113 5.5 The 5-Qbit error-correcting code 121 5.6 The 7-Qbit encoding circuit 127 5.9 A 5-Qbit encoding circuit 128 6 Protocols that use just a few Qbits 136 6.1 Bell states 136 6.2 Quantum dense coding 146 6.3 Teleportation 149 6.4 Cantum erypt		3.8	Calculating the periodic function	83
3.10Period finding and factoring864Searching with a quantum computer884.1The nature of the search884.2The Grover iteration894.3How to construct W944.4Generalization to several special numbers964.5Searching for one out of four items985Quantum error correction995.1The miracle of quantum error correction995.2A simplified example1005.3The physics of error generation1095.4Diagnosing error syndromes1135.5The 5-Qbit error-correcting code1175.6The 7-Qbit encoding circuit1275.9A 5-Qbit encoding circuit1286Protocols that use just a few Qbits1366.1Bell states1366.2Quantum cryptography1376.3Bit commitment1436.4Quantum dense coding1466.5Teleportation1496.6The GHZ puzzle1547.8Nector spaces: basic properties and Dirac notation1598Structure of the general 1-Qbit unitary transformation168C.Structure of the general 1-Qbit state173D.Spooky action at a distance173D.Spooky action at a distance175F.Consistency of the general 1-Qbit unitary transformation168G.The orbability of success in Simon's problem183<		3.9	The unimportance of small phase errors	84
4Searching with a quantum computer884.1The auture of the search884.2The Grover iteration894.3How to construct W944.4Generalization to several special numbers964.5Searching for one out of four items985Quantum error correction995.1The miracle of quantum error correction995.2A simplified example1005.3The physics of error generation1095.4Diagnosing error syndromes1135.5The 5-Qbit error-correcting code1215.7Operations on 7-Qbit codewords1245.8A 7-Qbit encoding circuit1286Protocols that use just a few Qbits1366.1Bell states1366.2Quantum dense coding1436.4Quantum dense coding1496.5Teleportation1496.6The GHZ puzzle154A vector spaces: basic properties and Dirac notation7.9S. Structure of the general 1-Qbit unitary transformation7.9S. Structure of the general 1-Qbit state1757.0S. Spooky action at a distance1757.1S. Spooky action at a distance1758.3Che raspects of Deutsch's problem1839.4Other aspects of Dustsch's problem1839.5Other aspects of Dustsch's problem1839.6The probability of success in Simon's problem183<		3.10	Period finding and factoring	86
4.1The nature of the search884.2The Grover iteration894.3How to construct W944.4Generalization to several special numbers964.5Searching for one out of four items985Quantum error correction995.1The miracle of quantum error correction995.2A simplified example1005.3The physics of error generation1095.4Diagnosing error syndromes1135.5The 5-Qbit error-correcting code1215.7Operations on 7-Qbit codewords1245.8A 7-Qbit encoding circuit1286Protocols that use just a few Qbits1366.1Bell states1366.2Quantum cryptography1376.3Bit commitment1436.4Quantum dense coding1466.5Teleportation1496.6The GHZ puzzle154AppendicesAVector spaces: basic properties and Dirac notationBStructure of the general 1-Qbit unitary transformation168C. Structure of the general 1-Qbit state173D. Spooky action at a distance175E. Consistency of the generalized Born rule181F. Other aspects of Deutsch's problem183G. The probability of success in Simon's problem183J. Some simple number theory193J. Some simple number theory193J. Some simple number theory		4 Se	earching with a quantum computer	88
4.2 The Grover iteration 89 4.3 How to construct W 94 4.4 Generalization to several special numbers 96 4.5 Searching for one out of four items 98 5 Quantum error correction 99 5.1 The miracle of quantum error correction 99 5.2 A simplified example 100 5.3 The physics of error generation 109 5.4 Diagnosing error syndromes 113 5.5 The 5-Qbit error-correcting code 121 5.6 The 7-Qbit error-correcting code 121 5.7 Operations on 7-Qbit codewords 124 5.8 A 7-Qbit encoding circuit 127 5.9 A 5-Qbit encoding circuit 128 6 Protocols that use just a few Qbits 136 6.1 Bell states 136 6.2 Quantum dense coding 146 6.5 Teleportation 149 6.6 The GHZ puzzle 154 A. Vector spaces: basic properties and Dirac notation 159 A. Vector spaces: basic prop		4.1	The nature of the search	88
4.3How to construct W 944.4Generalization to several special numbers964.5Searching for one out of four items985Quantum error correction995.1The miracle of quantum error correction995.2A simplified example1005.3The physics of error generation1095.4Diagnosing error syndromes1135.5The 5-Qbit error-correcting code1215.6The 7-Qbit error-correcting code1215.7Operations on 7-Qbit codewords1245.8A 7-Qbit encoding circuit1286Protocols that use just a few Qbits1366.1Bell states1366.2Quantum cryptography1376.3Bit commitment1436.4Quantum dense coding1466.5Teleportation1496.6The GHZ puzzle154Appendices9A. Vector spaces: basic properties and Dirac notation9B. Structure of the general 1-Qbit unitary transformation168C. Structure of the general 1-Qbit state173D. Spooky action at a distance175E. Consistency of the generalized Born rule181F. Other aspects of Deutsch's problem183G. The probability of success in Simon's problem187H. One way to make a cNOT gate189I. A little elementary group theory193J. Some simple number theory193J. Some s		4.2	The Grover iteration	89
4.4Generalization to several special numbers964.5Searching for one out of four items985Quantum error correction995.1The miracle of quantum error correction995.2A simplified example1005.3The physics of error generation1095.4Diagnosing error syndromes1135.5The 5-Qbit error-correcting code1215.6The 7-Qbit error-correcting code1215.7Operations on 7-Qbit codewords1245.8A 7-Qbit encoding circuit1286Protocols that use just a few Qbits1366.1Bell states1366.2Quantum cryptography1376.3Bit commitment1436.4Quantum dense coding1466.5Teleportation1496.6The GHZ puzzle154Appendices8Structure of the general 1-Qbit unitary transformation9B.Structure of the general 1-Qbit state75F.Consistency of the general 1-Qbit state75F.Consistency of the general 2000 mrule8G.Three orbit state9Sopoky action at a distance9Sopoky action at a cNOT gate18F.9Other aspects of Deutsch's problem1879A. Success in simon's problem1879A.9I.9J.9Some si		4.3	How to construct W	94
4.5 Searching for one out of four items 98 5 Quantum error correction 99 5.1 The miracle of quantum error correction 99 5.2 A simplified example 100 5.3 The physics of error generation 109 5.4 Diagnosing error syndromes 113 5.5 The 5-Qbit error-correcting code 121 5.6 The 7-Qbit error-correcting code 121 5.7 Operations on 7-Qbit codewords 124 5.8 A 7-Qbit encoding circuit 127 5.9 A 5-Qbit encoding circuit 128 6 Protocols that use just a few Qbits 136 6.1 Bell states 136 6.2 Quantum cryptography 137 6.3 Bit commitment 143 6.4 Quantum dense coding 146 6.5 Teleportation 149 6.6 The GHZ puzzle 154 Appendices 75 F. Consistency of the general 1-Qbit unitary transformation 168 C. Structure of the general 1-Qbit state <td></td> <td>4.4</td> <td>Generalization to several special numbers</td> <td>96</td>		4.4	Generalization to several special numbers	96
5Quantum error correction995.1The miracle of quantum error correction995.2A simplified example1005.3The physics of error generation1095.4Diagnosing error syndromes1135.5The 5-Qbit error-correcting code1175.6The 7-Qbit error-correcting code1215.7Operations on 7-Qbit codewords1245.8A 7-Qbit encoding circuit1275.9A 5-Qbit encoding circuit1286Protocols that use just a few Qbits1366.1Bell states1366.2Quantum cryptography1376.3Bit commitment1436.4Quantum dense coding1466.5Teleportation1496.6The GHZ puzzle154A vector spaces: basic properties and Dirac notation159B. Structure of the general 1-Qbit unitary transformation168C. Structure of the general 1-Qbit state173D. Spooky action at a distance175E. Consistency of the generalized Born rule181F. Other aspects of Deutsch's problem183G. The probability of success in Simon's problem183J. Some simple number theory193J. Some simple number theory<		4.5	Searching for one out of four items	98
5.1The miracle of quantum error correction995.2A simplified example1005.3The physics of error generation1095.4Diagnosing error syndromes1135.5The 5-Qbit error-correcting code1175.6The 7-Qbit error-correcting code1215.7Operations on 7-Qbit codewords1245.8A 7-Qbit encoding circuit1275.9A 5-Qbit encoding circuit1286Protocols that use just a few Qbits1366.1Bell states1366.2Quantum cryptography1376.3Bit commitment1436.4Quantum dense coding1466.5Teleportation1496.6The GHZ puzzle154AppendicesAVector spaces: basic properties and Dirac notation9Structure of the general 1-Qbit unitary transformation168C.Structure of the general 1-Qbit state173D.Spooky action at a distance175E.Consistency of the generalized Born rule181F.Other aspects of Deutsch's problem183G.The erobability of success in Simon's problem187H.One way to make a cNOT gate189I.A little elementary group theory193J.Some simple number theory195K.Period finding and continued fractions197L.Better estimates of success in period finding201<		5 Q	uantum error correction	99
5.2A simplified example1005.3The physics of error generation1095.4Diagnosing error syndromes1135.5The 5-Qbit error-correcting code1215.6The 7-Qbit error-correcting code1215.7Operations on 7-Qbit codewords1245.8A 7-Qbit encoding circuit1275.9A 5-Qbit encoding circuit1286Protocols that use just a few Qbits1366.1Bell states1366.2Quantum cryptography1376.3Bit commitment1436.4Quantum dense coding1466.5Teleportation1496.6The GHZ puzzle154Appendices159A. Vector spaces: basic properties and Dirac notation159B. Structure of the general 1-Qbit unitary transformation168C. Structure of the general 1-Qbit state173D. Spooky action at a distance175E. Consistency of the generalized Born rule181F. Other aspects of Deutsch's problem183G. The probability of success in Simon's problem187H. One way to make a cNOT gate189I. A little elementary group theory193J. Some simple number theory193J. Some simple number theory195K. Period finding and continued fractions197L. Better estimates of success in period finding201		5.1	The miracle of quantum error correction	99
5.3The physics of error generation1095.4Diagnosing error syndromes1135.5The 5-Qbit error-correcting code1175.6The 7-Qbit error-correcting code1215.7Operations on 7-Qbit codewords1245.8A 7-Qbit encoding circuit1275.9A 5-Qbit encoding circuit1286Protocols that use just a few Qbits1366.1Bell states1366.2Quantum cryptography1376.3Bit commitment1436.4Quantum dense coding1466.5Teleportation1496.6The GHZ puzzle154Appendices159A. Vector spaces: basic properties and Dirac notation159B. Structure of the general 1-Qbit unitary transformation168C. Structure of the general 1-Qbit state173D. Spooky action at a distance175E. Consistency of the generalized Born rule181F. Other aspects of Deutsch's problem183G. The probability of success in Simon's problem187H. One way to make a cNOT gate189I. A little elementary group theory193J. Some simple number theory193J. Some simple number theory195K. Period finding and continued fractions197L. Better estimates of success in period finding201		5.2	A simplified example	100
5.4Diagnosing error syndromes1135.5The 5-Qbit error-correcting code1175.6The 7-Qbit error-correcting code1215.7Operations on 7-Qbit codewords1245.8A 7-Qbit encoding circuit1275.9A 5-Qbit encoding circuit1286Protocols that use just a few Qbits1366.1Bell states1366.2Quantum cryptography1376.3Bit commitment1436.4Quantum dense coding1466.5Teleportation1496.6The GHZ puzzle154Appendices159A.A.Vector spaces: basic properties and Dirac notation159B.Structure of the general 1-Qbit unitary transformation168C.Structure of the general 1-Qbit state173D.Spooky action at a distance175E.Consistency of the generalized Born rule181F.Other aspects of Deutsch's problem183G.The probability of success in Simon's problem184H.One way to make a cNOT gate185K.Period finding and continued fractions197L.Better estimates of success in period finding201L.Better estimates of success in period finding		5.3	The physics of error generation	109
5.5The 5-Qbit error-correcting code1175.6The 7-Qbit error-correcting code1215.7Operations on 7-Qbit codewords1245.8A 7-Qbit encoding circuit1275.9A 5-Qbit encoding circuit1286Protocols that use just a few Qbits1366.1Bell states1366.2Quantum cryptography1376.3Bit commitment1436.4Quantum dense coding1466.5Teleportation1496.6The GHZ puzzle154AppendicesAVector spaces: basic properties and Dirac notationBStructure of the general 1-Qbit state173D.Spooky action at a distance175E.Consistency of the generalized Born rule181F.Other aspects of Deutsch's problem183G.The probability of success in Simon's problem187H.One way to make a cNOT gate189I.A little elementary group theory193J.Some simple number theory195K.Period finding and continued fractions197L.Better estimates of success in period finding201		5.4	Diagnosing error syndromes	113
5.6The 7-Qbit error-correcting code1215.7Operations on 7-Qbit codewords1245.8A 7-Qbit encoding circuit1275.9A 5-Qbit encoding circuit1286Protocols that use just a few Qbits1366.1Bell states1366.2Quantum cryptography1376.3Bit commitment1436.4Quantum dense coding1466.5Teleportation1496.6The GHZ puzzle154AppendicesA.Vector spaces: basic properties and Dirac notation159B.Structure of the general 1-Qbit unitary transformation168C.Structure of the general 1-Qbit state75E.Consistency of the generalized Born rule181F.Other aspects of Deutsch's problem183G.The probability of success in Simon's problem187H.One way to make a cNOT gate188I.A little elementary group theory193J.Some simple number theory193L.Better estimates of success in period finding201L.Better estimates of success in period finding		5.5	The 5-Qbit error-correcting code	117
5.7Operations on 7-Qbit codewords1245.8A 7-Qbit encoding circuit1275.9A 5-Qbit encoding circuit1286Protocols that use just a few Qbits1366.1Bell states1366.2Quantum cryptography1376.3Bit commitment1436.4Quantum dense coding1466.5Teleportation1496.6The GHZ puzzle154Appendices159A.A.Vector spaces: basic properties and Dirac notation159B.Structure of the general 1-Qbit unitary transformation168C.Structure of the general 1-Qbit state173D.Spooky action at a distance175E.Consistency of the generalized Born rule181F.Other aspects of Deutsch's problem183G.The probability of success in Simon's problem187H.One way to make a cNOT gate189I.A little elementary group theory193J.Some simple number theory195K.Period finding and continued fractions197L.Better estimates of success in period finding201		5.6	The 7-Qbit error-correcting code	121
5.8A 7-Qbit encoding circuit1275.9A 5-Qbit encoding circuit1286Protocols that use just a few Qbits1366.1Bell states1366.2Quantum cryptography1376.3Bit commitment1436.4Quantum dense coding1466.5Teleportation1496.6The GHZ puzzle154AppendicesAppendices159A.Vector spaces: basic properties and Dirac notation159B.Structure of the general 1-Qbit unitary transformation168C.Structure of the general 1-Qbit state173D.Spooky action at a distance175E.Consistency of the generalized Born rule181F.Other aspects of Deutsch's problem187H.One way to make a cNOT gate189I.A little elementary group theory193J.Some simple number theory193L.Better estimates of success in period finding201		5.7	Operations on 7-Qbit codewords	124
5.9A 5-Qbit encoding circuit1286Protocols that use just a few Qbits1366.1Bell states1366.2Quantum cryptography1376.3Bit commitment1436.4Quantum dense coding1466.5Teleportation1496.6The GHZ puzzle154AppendicesA.Vector spaces: basic properties and Dirac notationB.Structure of the general 1-Qbit unitary transformation168C.Structure of the general 1-Qbit state173D.Spooky action at a distance175E.Consistency of the generalized Born rule181F.Other aspects of Deutsch's problem183G.The probability of success in Simon's problem187H.One way to make a cNOT gate189I.A little elementary group theory193J.Some simple number theory195K.Period finding and continued fractions197L.Better estimates of success in period finding201		5.8	A 7-Qbit encoding circuit	127
6 Protocols that use just a few Qbits1366.1Bell states1366.2Quantum cryptography1376.3Bit commitment1436.4Quantum dense coding1466.5Teleportation1496.6The GHZ puzzle154 Appendices 159A.Vector spaces: basic properties and Dirac notation159B.Structure of the general 1-Qbit unitary transformation168C.Structure of the general 1-Qbit state173D.Spooky action at a distance175E.Consistency of the generalized Born rule181F.Other aspects of Deutsch's problem183G.The probability of success in Simon's problem187H.One way to make a cNOT gate189I.A little elementary group theory193J.Some simple number theory195K.Period finding and continued fractions197L.Better estimates of success in period finding201		5.9	A 5-Qbit encoding circuit	128
6.1Bell states1366.2Quantum cryptography1376.3Bit commitment1436.4Quantum dense coding1466.5Teleportation1496.6The GHZ puzzle154Appendices159A.Vector spaces: basic properties and Dirac notation159B.Structure of the general 1-Qbit unitary transformation168C.Structure of the general 1-Qbit state173D.Spooky action at a distance175E.Consistency of the generalized Born rule181F.Other aspects of Deutsch's problem183G.The probability of success in Simon's problem187H.One way to make a cNOT gate189I.A little elementary group theory193J.Some simple number theory195K.Period finding and continued fractions197L.Better estimates of success in period finding201		6 P1	rotocols that use just a few Qbits	136
6.2Quantum cryptography1376.3Bit commitment1436.4Quantum dense coding1466.5Teleportation1496.6The GHZ puzzle154AppendicesA.Vector spaces: basic properties and Dirac notationB.Structure of the general 1-Qbit unitary transformation168C.Structure of the general 1-Qbit state173D.Spooky action at a distance175E.Consistency of the generalized Born rule181F.Other aspects of Deutsch's problem183G.The probability of success in Simon's problem187H.One way to make a cNOT gate189I.A little elementary group theory193J.Some simple number theory195K.Period finding and continued fractions197L.Better estimates of success in period finding201		6.1	Bell states	136
6.3Bit commitment1436.4Quantum dense coding1466.5Teleportation1496.6The GHZ puzzle154Appendices159A.Vector spaces: basic properties and Dirac notation159B.Structure of the general 1-Qbit unitary transformation168C.Structure of the general 1-Qbit state173D.Spooky action at a distance175E.Consistency of the generalized Born rule181F.Other aspects of Deutsch's problem183G.The probability of success in Simon's problem187H.One way to make a cNOT gate189I.A little elementary group theory193J.Some simple number theory195K.Period finding and continued fractions197L.Better estimates of success in period finding201		6.2	Quantum cryptography	137
6.4Quantum dense coding1466.5Teleportation1496.6The GHZ puzzle154Appendices159A.Vector spaces: basic properties and Dirac notation159B.Structure of the general 1-Qbit unitary transformation168C.Structure of the general 1-Qbit state173D.Spooky action at a distance175E.Consistency of the generalized Born rule181F.Other aspects of Deutsch's problem183G.The probability of success in Simon's problem187H.One way to make a cNOT gate189I.A little elementary group theory193J.Some simple number theory195K.Period finding and continued fractions197L.Better estimates of success in period finding201		6.3	Bit commitment	143
6.5Teleportation1496.6The GHZ puzzle154Appendices159A.Vector spaces: basic properties and Dirac notation159B.Structure of the general 1-Qbit unitary transformation168C.Structure of the general 1-Qbit state173D.Spooky action at a distance175E.Consistency of the generalized Born rule181F.Other aspects of Deutsch's problem183G.The probability of success in Simon's problem187H.One way to make a cNOT gate189I.A little elementary group theory193J.Some simple number theory195K.Period finding and continued fractions197L.Better estimates of success in period finding201		6.4	Quantum dense coding	146
6.6The GHZ puzzle154Appendices159A.Vector spaces: basic properties and Dirac notation159B.Structure of the general 1-Qbit unitary transformation168C.Structure of the general 1-Qbit state173D.Spooky action at a distance175E.Consistency of the generalized Born rule181F.Other aspects of Deutsch's problem183G.The probability of success in Simon's problem187H.One way to make a cNOT gate189I.A little elementary group theory193J.Some simple number theory195K.Period finding and continued fractions197L.Better estimates of success in period finding201		6.5	Teleportation	149
Appendices159A.Vector spaces: basic properties and Dirac notation159B.Structure of the general 1-Qbit unitary transformation168C.Structure of the general 1-Qbit state173D.Spooky action at a distance175E.Consistency of the generalized Born rule181F.Other aspects of Deutsch's problem183G.The probability of success in Simon's problem187H.One way to make a cNOT gate189I.A little elementary group theory193J.Some simple number theory195K.Period finding and continued fractions197L.Better estimates of success in period finding201		6.6	The GHZ puzzle	154
A.Vector spaces: basic properties and Dirac notation159B.Structure of the general 1-Qbit unitary transformation168C.Structure of the general 1-Qbit state173D.Spooky action at a distance175E.Consistency of the generalized Born rule181F.Other aspects of Deutsch's problem183G.The probability of success in Simon's problem187H.One way to make a cNOT gate189I.A little elementary group theory193J.Some simple number theory195K.Period finding and continued fractions197L.Better estimates of success in period finding201		Арр	Appendices	
B.Structure of the general 1-Qbit unitary transformation168C.Structure of the general 1-Qbit state173D.Spooky action at a distance175E.Consistency of the generalized Born rule181F.Other aspects of Deutsch's problem183G.The probability of success in Simon's problem187H.One way to make a cNOT gate189I.A little elementary group theory193J.Some simple number theory195K.Period finding and continued fractions197L.Better estimates of success in period finding201		А.	Vector spaces: basic properties and Dirac notation	159
C.Structure of the general 1-Qbit state173D.Spooky action at a distance175E.Consistency of the generalized Born rule181F.Other aspects of Deutsch's problem183G.The probability of success in Simon's problem187H.One way to make a cNOT gate189I.A little elementary group theory193J.Some simple number theory195K.Period finding and continued fractions197L.Better estimates of success in period finding201		B.	Structure of the general 1-Qbit unitary transformation	168
D.Spooky action at a distance175E.Consistency of the generalized Born rule181F.Other aspects of Deutsch's problem183G.The probability of success in Simon's problem187H.One way to make a cNOT gate189I.A little elementary group theory193J.Some simple number theory195K.Period finding and continued fractions197L.Better estimates of success in period finding201		C.	Structure of the general 1-Qbit state	173
E.Consistency of the generalized Born rule181F.Other aspects of Deutsch's problem183G.The probability of success in Simon's problem187H.One way to make a cNOT gate189I.A little elementary group theory193J.Some simple number theory195K.Period finding and continued fractions197L.Better estimates of success in period finding201		D.	Spooky action at a distance	175
F.Other aspects of Deutsch's problem183G.The probability of success in Simon's problem187H.One way to make a cNOT gate189I.A little elementary group theory193J.Some simple number theory195K.Period finding and continued fractions197L.Better estimates of success in period finding201		E.	Consistency of the generalized Born rule	181
G.The probability of success in Simon's problem187H.One way to make a cNOT gate189I.A little elementary group theory193J.Some simple number theory195K.Period finding and continued fractions197L.Better estimates of success in period finding201		F.	Other aspects of Deutsch's problem	183
H.One way to make a cNOT gate189I.A little elementary group theory193J.Some simple number theory195K.Period finding and continued fractions197L.Better estimates of success in period finding201		G.	The probability of success in Simon's problem	187
I.A little elementary group theory193J.Some simple number theory195K.Period finding and continued fractions197L.Better estimates of success in period finding201		H.	One way to make a cNOT gate	189
J.Some simple number theory195K.Period finding and continued fractions197L.Better estimates of success in period finding201		I.	A little elementary group theory	193
K.Period finding and continued fractions197L.Better estimates of success in period finding201		I.	Some simple number theory	195
L. Better estimates of success in period finding 201		K.	Period finding and continued fractions	197
1 U		L.	Better estimates of success in period finding	201

		CONTENTS	ix
M.	Factoring and period finding	203	
N. O.	A circuit-diagrammatic treatment of the 7-Qbit code	207 210	
Р.	On bit commitment	216	
Index		218	

Preface

It was almost three quarters of a century after the discovery of quantum mechanics, and half a century after the birth of information theory and the arrival of large-scale digital computation, that people finally realized that quantum physics profoundly alters the character of information processing and digital computation. For physicists this development offers an exquisitely different way of using and thinking about the quantum theory. For computer scientists it presents a surprising demonstration that the abstract structure of computation cannot be divorced from the physics governing the instrument that performs the computation. Quantum mechanics provides new computational paradigms that had not been imagined prior to the 1980s and whose power was not fully appreciated until the mid 1990s.

In writing this introduction to quantum computer science I have kept in mind readers from several disciplines. Primarily I am addressing computer scientists, electrical engineers, or mathematicians who may know little or nothing about quantum physics (or any other kind of physics) but who wish to acquire enough facility in the subject to be able to follow the new developments in quantum computation, judge for themselves how revolutionary they may be, and perhaps choose to participate in the further development of quantum computer science. Not the least of the surprising things about quantum computation is that remarkably little background in quantum mechanics has to be acquired to understand and work with its applications to information processing. Familiarity with a few fundamental facts about finite-dimensional vector spaces over the complex numbers (summarized and reviewed in Appendix A) is the only real prerequisite.

One of the secondary readerships I have in mind consists of physicists who, like myself – I am a theorist who has worked in statistical physics, solid-state physics, low-temperature physics, and mathematical physics – know very little about computer science, but would like to learn about this extraordinary new application of their discipline. I stress, however, that my subject is quantum computer science, not quantum computer design. This is a book about quantum computational software – not hardware. The difficult question of how one might actually build a quantum computer is beyond its scope.

xii

PREFACE

Another secondary readership is made up of those philosophers and physicists who - again like myself - are puzzled by so-called foundational issues: what the strange quantum formalism implies about the nature of the world that it so accurately describes. By applying quantum mechanics in an entirely new way - and especially by applying it to the processing of knowledge - quantum computation gives a new perspective on interpretational questions. While I rarely address such matters explicitly, for purely pedagogical reasons my presentation is suffused with a perspective on the quantum theory that is very close to the venerable but recently much reviled Copenhagen interpretation. Those with a taste for such things may be startled to see how well quantum computation resonates with the Copenhagen point of view. Indeed, it had been my plan to call this book Copenhagen Computation until the excellent people at Cambridge University Press and my computer-scientist friends persuaded me that virtually no members of my primary readership would then have had any idea what it was about.

Several years ago I mentioned to a very distinguished theoretical physicist that I spent the first four lectures of a course in quantum computation giving an introduction to quantum mechanics for mathematically literate people who knew nothing about quantum mechanics, and quite possibly little if anything about physics. His immediate response was that any application of quantum mechanics that can be taught after only a four-hour introduction to the subject cannot have serious intellectual content. After all, he remarked, it takes any physicist many years to develop a feeling for quantum mechanics.

It's a good point. Nevertheless computer scientists and mathematicians with no background in physics have been able quickly to learn enough quantum mechanics to understand and make major contributions to the theory of quantum computation. There are two main reasons for this.

First of all, a quantum computer – or, more accurately, the abstract quantum computer that one hopes someday to be able to embody in actual hardware – is an extremely simple example of a physical system. It is discrete, not continuous. It is made up out of a finite number of units, each of which is the simplest possible kind of quantum-mechanical system, a so-called two-state system, whose behavior, as we shall see, is highly constrained and easily specified. Much of the analytical complexity of learning quantum mechanics is connected with mastering the description of continuous (infinite-state) systems. By restricting attention to collections of two-state systems (or even d-state systems for finite d) one can avoid much suffering. Of course one also loses much wisdom, but hardly any of it – at least at this stage of the art – is relevant to the basic theory of quantum computation.

Second, and just as important, the most difficult part of learning quantum mechanics is to get a good feeling for how the formalism

CAMBRIDGE

Cambridge University Press 978-0-521-87658-2 - Quantum Computer Science: An Introduction N. David Mermin Frontmatter More information

PREFACE

can be applied to actual phenomena. This almost invariably involves formulating oversimplified abstract models of real physical systems, to which the quantum formalism can then be applied. The best physicists have an extraordinary intuition for what features of the phenomena are essential and must be represented in a model, and what features are inessential and can be ignored. It takes years to develop such intuition. Some never do. The theory of quantum computation, however, is entirely concerned with an abstract model – the easy part of the problem.

To understand how to *build* a quantum computer, or even to study what physical systems are promising candidates for realizing such a device, you must indeed have many years of experience in quantum mechanics and its applications under your belt. But if you only want to know what such a device is capable in principle of doing once you have it, then there is no reason to get involved in the really difficult physics of the subject. Exactly the same thing holds for ordinary classical computers. One can be a masterful practitioner of computer science without having the foggiest notion of what a transistor is, not to mention how it works.

So while you should be warned that the subset of quantum mechanics you will acquire from this book is extremely focused and quite limited in its scope, you can also rest assured that it is neither oversimplified nor incomplete, when applied to the special task for which it is intended.

I might note that a third impediment to developing a good intuition for quantum physics is that in some ways the behavior implied by quantum mechanics is highly counterintuitive, if not downright weird. Glimpses of such strange behavior sometimes show up at the level of quantum computation. Indeed, for me one of the major appeals of quantum computation is that it affords a new conceptual arena for trying to come to a better understanding of quantum weirdness. When opportunities arise I will call attention to some of this strange behavior, rather than (as I easily could) letting it pass by unremarked upon and unnoticed.

The book evolved as notes for a course of 28 one-hour lectures on quantum computation that I gave six times between 2000 and 2006 to a diverse group of Cornell University undergraduates, graduate students, and faculty, in computer science, electrical engineering, mathematics, physics, and applied physics. With so broad an audience, little common knowledge could be assumed. My lecture notes, as well as my own understanding of the subject, repeatedly benefited from comments and questions in and after class, coming from a number of different perspectives. What made sense to one of my constituencies was often puzzling, absurd, or irritatingly simple-minded to others. This final form of my notes bears little resemblance to my earliest versions, having been improved by insightful remarks, suggestions, and complaints about everything from notation to number theory.

xiii

xiv

PREFACE

In addition to the 200 or so students who passed through P481-P681-CS483, I owe thanks to many others. Albert J. Sievers, then Director of Cornell's Laboratory of Atomic and Solid State Physics, started me thinking hard about quantum computation by asking me to put together a two-week set of introductory lectures for members of our laboratory, in the Fall of 1999. So many people showed up from all over the university that I decided it might be worth expanding this survey into a full course. I'm grateful to two Physics Department chairs, Peter Lepage and Saul Teukolsky, for letting me continue teaching that course for six straight years, and to the Computer Science Department chair, Charlie van Loan, for support, encouragement, and a steady stream of wonderful students. John Preskill, though he may not know it, taught me much of the subject from his superb online Caltech lecture notes. Charles Bennett first told me about quantum information processing, back when the term might not even have been coined, and he has always been available as a source of wisdom and clarification. Gilles Brassard has on many occasions supplied me with help from the computer-science side. Chris Fuchs has been an indispensable quantum-foundational critic and consultant. Bob Constable made me, initially against my will, a certified Cornell Information Scientist and introduced me to many members of that excellent community. But most of all, I owe thanks to David DiVincenzo, who collaborated with me on the 1999 two-week LASSP Autumn School and has acted repeatedly over the following years as a sanity check on my ideas, an indispensable source of references and historical information, a patient teacher, and an encouraging friend.

A note on references

Quantum Computer Science is a pedagogical introduction to the basic structure and procedures of the subject – a quantum-computational primer. It is not a historical survey of the development of the field. Many of these procedures are named after the people who first put them forth, but although I use their names, I do not cite the original papers unless they add something to my own exposition. This is because, not surprisingly, work done since the earliest papers has led to clearer expositions of those ideas. I learned the subject myself almost exclusively from secondary, tertiary, or even higher-order sources, and then reformulated it repeatedly in the course of teaching it for six years.

On the few occasions when I do cite a paper it is either because it completes an exposition that I have only sketched, or because the work has not yet become identified in the field with the name(s) of the author(s) and I wanted to make clear that it was not original with me.

Readers interested in hunting down earlier work in the field can begin (and in most cases conclude) their search at the quantum-physics subdivision of the Cornell (formerly Los Alamos) E-print Archive, http://arxiv.org/archive/quant-ph, where most of the important papers in the field have been and are still being posted.