

Contents

<i>Preface</i>	<i>page xi</i>
<i>A note on references</i>	<i>xv</i>
1 Cbits and Qbits	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 General features and some simple examples	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-Qbit gates	76
3.7 Finding the period	79

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	113
5.5	The 5-Qbit error-correcting code	117
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	159
A.	Vector spaces: basic properties and Dirac notation	159
B.	Structure of the general 1-Qbit unitary transformation	168
C.	Structure of the general 1-Qbit state	173
D.	Spooky action at a distance	175
E.	Consistency of the generalized Born rule	181
F.	Other aspects of Deutsch's problem	183
G.	The probability of success in Simon's problem	187
H.	One way to make a cNOT gate	189
I.	A little elementary group theory	193
J.	Some simple number theory	195
K.	Period finding and continued fractions	197
L.	Better estimates of success in period finding	201

CONTENTS

ix

M.	Factoring and period finding	203
N.	Shor's 9-Qbit error-correcting code	207
O.	A circuit-diagrammatic treatment of the 7-Qbit code	210
P.	On bit commitment	216
	<i>Index</i>	218