

Contents

Preface	x
Acknowledgements	xi
1 INTRODUCTION AND BACKGROUND	1
1.1 Overview	1
1.2 Computers and the Strong Church–Turing Thesis	2
1.3 The Circuit Model of Computation	6
1.4 A Linear Algebra Formulation of the Circuit Model	8
1.5 Reversible Computation	12
1.6 A Preview of Quantum Physics	15
1.7 Quantum Physics and Computation	19
2 LINEAR ALGEBRA AND THE DIRAC NOTATION	21
2.1 The Dirac Notation and Hilbert Spaces	21
2.2 Dual Vectors	23
2.3 Operators	27
2.4 The Spectral Theorem	30
2.5 Functions of Operators	32
2.6 Tensor Products	33
2.7 The Schmidt Decomposition Theorem	35
2.8 Some Comments on the Dirac Notation	37
3 QUBITS AND THE FRAMEWORK OF QUANTUM MECHANICS	38
3.1 The State of a Quantum System	38
3.2 Time-Evolution of a Closed System	43
3.3 Composite Systems	45
3.4 Measurement	48

3.5	Mixed States and General Quantum Operations	53	7.3	Finding-Orders	130
3.5.1	Mixed States	53	7.3.1	The Order-Finding Problem	130
3.5.2	Partial Trace	56	7.3.2	Some Mathematical Preliminaries	131
3.5.3	General Quantum Operations	59	7.3.3	The Eigenvalue Estimation Approach to Order Finding	134
4	A QUANTUM MODEL OF COMPUTATION	61	7.3.4	Shor's Approach to Order Finding	139
4.1	The Quantum Circuit Model	61	7.4	Finding Discrete Logarithms	142
4.2	Quantum Gates	63	7.5	Hidden Subgroups	146
4.2.1	1-Qubit Gates	63	7.5.1	More on Quantum Fourier Transforms	147
4.2.2	Controlled- U Gates	66	7.5.2	Algorithm for the Finite Abelian Hidden Subgroup Problem	149
4.3	Universal Sets of Quantum Gates	68	7.6	Related Algorithms and Techniques	151
4.4	Efficiency of Approximating Unitary Transformations	71	8	ALGORITHMS BASED ON AMPLITUDE AMPLIFICATION	152
4.5	Implementing Measurements with Quantum Circuits	73	8.1	Grover's Quantum Search Algorithm	152
5	SUPERDENSE CODING AND QUANTUM TELEPORTATION	78	8.2	Amplitude Amplification	163
5.1	Superdense Coding	79	8.3	Quantum Amplitude Estimation and Quantum Counting	170
5.2	Quantum Teleportation	80	8.4	Searching Without Knowing the Success Probability	175
5.3	An Application of Quantum Teleportation	82	8.5	Related Algorithms and Techniques	178
6	INTRODUCTORY QUANTUM ALGORITHMS	86	9	QUANTUM COMPUTATIONAL COMPLEXITY THEORY AND LOWER BOUNDS	179
6.1	Probabilistic Versus Quantum Algorithms	86	9.1	Computational Complexity	180
6.2	Phase Kick-Back	91	9.1.1	Language Recognition Problems and Complexity Classes	181
6.3	The Deutsch Algorithm	94	9.2	The Black-Box Model	185
6.4	The Deutsch-Jozsa Algorithm	99	9.2.1	State Distinguishability	187
6.5	Simon's Algorithm	103	9.3	Lower Bounds for Searching in the Black-Box Model: Hybrid Method	188
7	ALGORITHMS WITH SUPERPOLYNOMIAL SPEED-UP	110	9.4	General Black-Box Lower Bounds	191
7.1	Quantum Phase Estimation and the Quantum Fourier Transform	110	9.5	Polynomial Method	193
7.1.1	Error Analysis for Estimating Arbitrary Phases	117	9.5.1	Applications to Lower Bounds	194
7.1.2	Periodic States	120	9.5.2	Examples of Polynomial Method Lower Bounds	196
7.1.3	GCD, LCM, the Extended Euclidean Algorithm	124			
7.2	Eigenvalue Estimation	125			

9.6	Block Sensitivity	197	A.6	Black-Boxes for Group Computations	250
9.6.1	Examples of Block Sensitivity Lower Bounds	197	A.7	Computing Schmidt Decompositions	253
9.7	Adversary Methods	198	A.8	General Measurements	255
9.7.1	Examples of Adversary Lower Bounds	200	A.9	Optimal Distinguishing of Two States	258
9.7.2	Generalizations	203	A.9.1	A Simple Procedure	258
10	QUANTUM ERROR CORRECTION	204	A.9.2	Optimality of This Simple Procedure	258
10.1	Classical Error Correction	204	Bibliography		260
10.1.1	The Error Model	205	Index		270
10.1.2	Encoding	206			
10.1.3	Error Recovery	207			
10.2	The Classical Three-Bit Code	207			
10.3	Fault Tolerance	211			
10.4	Quantum Error Correction	212			
10.4.1	Error Models for Quantum Computing	213			
10.4.2	Encoding	216			
10.4.3	Error Recovery	217			
10.5	Three- and Nine-Qubit Quantum Codes	223			
10.5.1	The Three-Qubit Code for Bit-Flip Errors	223			
10.5.2	The Three-Qubit Code for Phase-Flip Errors	225			
10.5.3	Quantum Error Correction Without Decoding	226			
10.5.4	The Nine-Qubit Shor Code	230			
10.6	Fault-Tolerant Quantum Computation	234			
10.6.1	Concatenation of Codes and the Threshold Theorem	237			
APPENDIX A		241			
A.1	Tools for Analysing Probabilistic Algorithms	241			
A.2	Solving the Discrete Logarithm Problem When the Order of a Is Composite	243			
A.3	How Many Random Samples Are Needed to Generate a Group?	245			
A.4	Finding r Given $\frac{k}{r}$ for Random k	247			
A.5	Adversary Method Lemma	248			