

# Contents

<b>Preface</b>	x
<b>Acknowledgements</b>	xi
<b>1 INTRODUCTION AND BACKGROUND</b>	<b>1</b>
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
<b>2 LINEAR ALGEBRA AND THE DIRAC NOTATION</b>	<b>21</b>
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
<b>3 QUBITS AND THE FRAMEWORK OF QUANTUM MECHANICS</b>	<b>38</b>
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
3.5.1	Mixed States	53
3.5.2	Partial Trace	56
3.5.3	General Quantum Operations	59
<b>4</b>	<b>A QUANTUM MODEL OF COMPUTATION</b>	61
4.1	The Quantum Circuit Model	61
4.2	Quantum Gates	63
4.2.1	1-Qubit Gates	63
4.2.2	Controlled- $U$ Gates	66
4.3	Universal Sets of Quantum Gates	68
4.4	Efficiency of Approximating Unitary Transformations	71
4.5	Implementing Measurements with Quantum Circuits	73
<b>5</b>	<b>SUPERDENSE CODING AND QUANTUM TELEPORTATION</b>	78
5.1	Superdense Coding	79
5.2	Quantum Teleportation	80
5.3	An Application of Quantum Teleportation	82
<b>6</b>	<b>INTRODUCTORY QUANTUM ALGORITHMS</b>	86
6.1	Probabilistic Versus Quantum Algorithms	86
6.2	Phase Kick-Back	91
6.3	The Deutsch Algorithm	94
6.4	The Deutsch–Jozsa Algorithm	99
6.5	Simon’s Algorithm	103
<b>7</b>	<b>ALGORITHMS WITH SUPERPOLYNOMIAL SPEED-UP</b>	110
7.1	Quantum Phase Estimation and the Quantum Fourier Transform	110
7.1.1	Error Analysis for Estimating Arbitrary Phases	117
7.1.2	Periodic States	120
7.1.3	GCD, LCM, the Extended Euclidean Algorithm	124
7.2	Eigenvalue Estimation	125

7.3	Finding-Orders	130
7.3.1	The Order-Finding Problem	130
7.3.2	Some Mathematical Preliminaries	131
7.3.3	The Eigenvalue Estimation Approach to Order Finding	134
7.3.4	Shor's Approach to Order Finding	139
7.4	Finding Discrete Logarithms	142
7.5	Hidden Subgroups	146
7.5.1	More on Quantum Fourier Transforms	147
7.5.2	Algorithm for the Finite Abelian Hidden Subgroup Problem	149
7.6	Related Algorithms and Techniques	151
<b>8</b>	<b>ALGORITHMS BASED ON AMPLITUDE AMPLIFICATION</b>	152
8.1	Grover's Quantum Search Algorithm	152
8.2	Amplitude Amplification	163
8.3	Quantum Amplitude Estimation and Quantum Counting	170
8.4	Searching Without Knowing the Success Probability	175
8.5	Related Algorithms and Techniques	178
<b>9</b>	<b>QUANTUM COMPUTATIONAL COMPLEXITY THEORY AND LOWER BOUNDS</b>	179
9.1	Computational Complexity	180
9.1.1	Language Recognition Problems and Complexity Classes	181
9.2	The Black-Box Model	185
9.2.1	State Distinguishability	187
9.3	Lower Bounds for Searching in the Black-Box Model: Hybrid Method	188
9.4	General Black-Box Lower Bounds	191
9.5	Polynomial Method	193
9.5.1	Applications to Lower Bounds	194
9.5.2	Examples of Polynomial Method Lower Bounds	196

9.6	Block Sensitivity	197
9.6.1	Examples of Block Sensitivity Lower Bounds	197
9.7	Adversary Methods	198
9.7.1	Examples of Adversary Lower Bounds	200
9.7.2	Generalizations	203
<b>10</b>	<b>QUANTUM ERROR CORRECTION</b>	<b>204</b>
10.1	Classical Error Correction	204
10.1.1	The Error Model	205
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
	<b>APPENDIX A</b>	<b>241</b>
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

A.6	Black-Boxes for Group Computations	250
A.7	Computing Schmidt Decompositions	253
A.8	General Measurements	255
A.9	Optimal Distinguishing of Two States	258
A.9.1	A Simple Procedure	258
A.9.2	Optimality of This Simple Procedure	258
	<b>Bibliography</b>	260
	<b>Index</b>	270