

# Contents

<b>1. Introduction</b> .....	1
1.1 A Brief History of Quantum Computation .....	1
1.2 Classical Physics .....	2
1.3 Probabilistic Systems .....	4
1.4 Quantum Mechanics .....	7
<b>2. Devices for Computation</b> .....	13
2.1 Classical Computational Models .....	13
2.1.1 Turing Machines .....	13
2.1.2 Probabilistic Turing Machines .....	16
2.1.3 Multitape Turing Machines .....	20
2.2 Quantum Information .....	21
2.2.1 Quantum Bits .....	22
2.2.2 Quantum Registers .....	24
2.2.3 More on Quantum Information .....	27
2.2.4 Quantum Turing Machines .....	30
2.3 Circuits .....	34
2.3.1 Boolean Circuits .....	34
2.3.2 Reversible Circuits .....	36
2.3.3 Quantum Circuits .....	38
<b>3. Fast Factorization</b> .....	41
3.1 Quantum Fourier Transform .....	41
3.1.1 General Framework .....	41
3.1.2 Hadamard-Walsh Transform .....	43
3.1.3 Quantum Fourier Transform in $\mathbb{Z}_n$ .....	44
3.1.4 Complexity Remarks .....	49
3.2 Shor's Algorithm for Factoring Numbers .....	50
3.2.1 From Periods to Factoring .....	50
3.2.2 Orders of the Elements in $\mathbb{Z}_n$ .....	52
3.2.3 Finding the Period .....	54
3.3 The Correctness Probability .....	56
3.3.1 The Easy Case .....	56
3.3.2 The General Case .....	57

3.3.3	The Complexity of Shor's Factorization Algorithm . . . . .	61
3.4	Excercises . . . . .	62
<b>4.</b>	<b>Finding the Hidden Subgroup . . . . .</b>	<b>63</b>
4.1	Generalized Simon's Algorithm . . . . .	64
4.1.1	Preliminaries . . . . .	64
4.1.2	The Algorithms . . . . .	65
4.2	Examples . . . . .	69
4.2.1	Finding the Order . . . . .	69
4.2.2	Discrete Logarithm . . . . .	69
4.2.3	Simon's Original Problem . . . . .	70
4.3	Exercises . . . . .	70
<b>5.</b>	<b>Grover's Search Algorithm . . . . .</b>	<b>73</b>
5.1	Search Problems . . . . .	73
5.1.1	Satisfiability Problem . . . . .	73
5.1.2	Probabilistic Search . . . . .	74
5.1.3	Quantum Search with One Query . . . . .	76
5.2	Grover's Amplification Method . . . . .	79
5.2.1	Quantum Operators for Grover's Search Algorithm . . . . .	79
5.2.2	Amplitude Amplification . . . . .	80
5.2.3	Analysis of Amplification Method . . . . .	84
5.3	Utilizing Grover's Search Method . . . . .	87
5.3.1	Searching with Unknown Number of Solutions . . . . .	87
<b>6.</b>	<b>Complexity Lower Bounds for Quantum Circuits . . . . .</b>	<b>91</b>
6.1	General Idea . . . . .	91
6.2	Polynomial Representations . . . . .	92
6.2.1	Preliminaries . . . . .	92
6.2.2	Bounds for the Representation Degrees . . . . .	96
6.3	Quantum Circuit Lower Bound . . . . .	98
6.3.1	General Lower Bound . . . . .	98
6.3.2	Some Examples . . . . .	101
<b>7.</b>	<b>Appendix A: Quantum Physics . . . . .</b>	<b>103</b>
7.1	A Brief History of Quantum Theory . . . . .	103
7.2	Mathematical Framework for Quantum Theory . . . . .	105
7.2.1	Hilbert Spaces . . . . .	107
7.2.2	Operators . . . . .	108
7.2.3	Spectral Representation of Self-adjoint Operators . . . . .	109
7.2.4	Spectral Representation of Unitary Operators . . . . .	111
7.3	Quantum States as Hilbert Space Vectors . . . . .	115
7.3.1	Quantum Time Evolution . . . . .	116
7.3.2	Observables . . . . .	118
7.3.3	The Uncertainty Principles . . . . .	121

7.4	Quantum States as Operators . . . . .	125
7.4.1	Density Matrices . . . . .	126
7.4.2	Subsystem States . . . . .	130
7.4.3	More on Time Evolution . . . . .	135
7.4.4	Representation Theorems . . . . .	136
7.5	Exercises . . . . .	144
<b>8.</b>	<b>Appendix B: Mathematical Background . . . . .</b>	<b>145</b>
8.1	Group Theory . . . . .	145
8.1.1	Preliminaries . . . . .	145
8.1.2	Subgroups, Cosets . . . . .	146
8.1.3	Factor Groups . . . . .	147
8.1.4	Group $\mathbb{Z}_n^*$ . . . . .	149
8.1.5	Group Morphisms . . . . .	151
8.1.6	Direct Product . . . . .	153
8.2	Fourier Transforms . . . . .	154
8.2.1	Characters of Abelian Groups . . . . .	154
8.2.2	Orthogonality of the Characters . . . . .	156
8.2.3	Discrete Fourier Transform . . . . .	158
8.2.4	The Inverse Fourier Transform . . . . .	160
8.2.5	Fourier Transform and Periodicity . . . . .	161
8.3	Linear Algebra . . . . .	161
8.3.1	Preliminaries . . . . .	161
8.3.2	Inner Product . . . . .	164
8.4	Number Theory . . . . .	167
8.4.1	Euclid's Algorithm . . . . .	167
8.4.2	Continued Fractions . . . . .	168
8.5	Shannon Entropy and Information . . . . .	175
8.5.1	Entropy . . . . .	175
8.5.2	Information . . . . .	179
8.6	Exercises . . . . .	181
	<b>References . . . . .</b>	<b>183</b>
	<b>Index . . . . .</b>	<b>187</b>