

# Contents

<b>1</b>	<b>Preface</b>	<b>9</b>
<b>2</b>	<b>Introduction</b>	<b>12</b>
2.1	Computing and the Laws of Physics . . . . .	13
2.2	Quantum Information . . . . .	15
2.3	Quantum Computers . . . . .	16
2.4	The Wave and the Corpuscular Nature of Light . . . . .	20
2.5	Deterministic versus Probabilistic Photon Behavior . . . . .	21
2.6	State Description, Superposition, and Uncertainty . . . . .	22
2.7	Measurements in Multiple Bases . . . . .	24
2.8	Measurements of Superposition States . . . . .	27
2.9	An Augmented Probabilistic Model. The Superposition Probability Rule . . . . .	30
2.10	A Photon Coincidence Experiment . . . . .	34
2.11	A Three Beam Splitter Experiment . . . . .	36
2.12	BB84, the Emergence of Quantum Cryptography . . . . .	37
2.13	A Qubit of History . . . . .	41
2.14	Summary and Further Readings . . . . .	45
2.15	Exercises and Problems . . . . .	47
<b>3</b>	<b>Quantum Mechanics, a Mathematical Model of the Physical World</b>	<b>49</b>
3.1	Vector Spaces . . . . .	50
3.2	$n$ -Dimensional Real Euclidean Vector Space . . . . .	51
3.3	Linear Operators and Matrices . . . . .	53
3.4	Hermitian Operators in a Complex $n$ -Dimensional Euclidean Vector Space . . . . .	55
3.5	$n$ -Dimensional Hilbert Spaces. Dirac Notations . . . . .	58
3.6	The Inner Product in an $n$ -Dimensional Hilbert Space . . . . .	61
3.7	Tensor and Outer Products . . . . .	64
3.8	Quantum States . . . . .	65
3.9	Quantum Observables. Quantum Operators . . . . .	67
3.10	Spectral Decomposition of a Quantum Operator . . . . .	72
3.11	The Measurement of Observables . . . . .	74
3.12	More about Measurements. The Density Operator . . . . .	77
3.13	Double-Slit Experiments . . . . .	79
3.14	Stern-Gerlach Type Experiments . . . . .	84
3.15	The Spin as an Intrinsic Property . . . . .	86
3.16	Schrödinger's Wave Equation . . . . .	88
3.17	Heisenberg's Uncertainty Principle . . . . .	90
3.18	A Brief History of Quantum Ideas . . . . .	92
3.19	Summary and Further Readings . . . . .	95
3.20	Exercises and Problems . . . . .	97
<b>4</b>	<b>Qubits and Their Physical Realization</b>	<b>100</b>
4.1	One Qubit, a Very Small Bit . . . . .	100
4.2	The Bloch Sphere Representation of One Qubit . . . . .	103
4.3	Rotation Operations on the Bloch Sphere . . . . .	106
4.4	The Measurement of a Single Qubit . . . . .	109

4.5	Pure and Impure States of a Qubit . . . . .	111
4.6	A Pair of Qubits. Entanglement. . . . .	113
4.7	The Fragility of Quantum Information. Schrödinger’s Cat . . . . .	115
4.8	Qubits: from Hilbert Spaces to Physical Implementation . . . . .	116
4.9	Qubits as Spin One-Half Particles . . . . .	118
4.10	The Measurement of the Spin . . . . .	121
4.11	The Qubit as a Polarized Photon . . . . .	125
4.12	Entanglement . . . . .	129
4.13	The Exchange of Information Using Entangled Particles . . . . .	130
4.14	Summary and Further Readings . . . . .	132
4.15	Exercises and Problems . . . . .	135
<b>5</b>	<b>Quantum Gates and Quantum Circuits</b>	<b>136</b>
5.1	Classical Logic Gates and Circuits . . . . .	137
5.2	One-Qubit Gates . . . . .	140
5.3	The Hadamard Gate, Beam Splitters and Interferometers . . . . .	142
5.4	Two-Qubit Gates. The CNOT Gate . . . . .	144
5.5	Can We Build Quantum Copy Machines? . . . . .	147
5.6	Three-Qubit Gates. The Fredkin Gate . . . . .	149
5.7	The Toffoli Gate . . . . .	154
5.8	Quantum Circuits . . . . .	156
5.9	The No Cloning Theorem . . . . .	156
5.10	Qubit Swapping and Full Adder Circuits . . . . .	158
5.11	More about Unitary Operations and Rotation Matrices . . . . .	161
5.12	Single-Qubit Controlled Operations . . . . .	164
5.13	Multiple Qubit Controlled Operations . . . . .	171
5.14	Universal Quantum Gates . . . . .	174
5.15	A Quantum Circuit for the Walsh-Hadamard Transform . . . . .	178
5.16	The State Transformation Performed by Quantum Circuits . . . . .	179
5.17	Mathematical Models of a Quantum Computer . . . . .	183
5.18	Errors, Uniformity Conditions, and Time Complexity . . . . .	187
5.19	Summary and Further Readings . . . . .	188
5.20	Exercises and Problems . . . . .	190
<b>6</b>	<b>Quantum Algorithms</b>	<b>192</b>
6.1	From Classical to Quantum Turing Machines . . . . .	193
6.2	Computational Complexity and Entanglement . . . . .	195
6.3	Classes of Quantum Algorithms . . . . .	198
6.4	Quantum Parallelism . . . . .	199
6.5	Deutsch’s Problem . . . . .	202
6.6	Quantum Fourier Transform . . . . .	206
6.7	Tensor Product Factorization . . . . .	208
6.8	A Circuit for Quantum Fourier Transform . . . . .	209
6.9	A Case Study: A Three-Qubit QFT . . . . .	212
6.10	Shor’s Factoring Algorithm and Order Finding . . . . .	218
6.11	A Quantum Circuit for Computing $f(x)$ Modulo $2^m$ . . . . .	224
6.12	Simon’s Algorithm for Phase Estimation . . . . .	226
6.13	The Fourier Transform on an Abelian Group . . . . .	229

6.14	Periodicity and the Quantum Fourier Transform . . . . .	233
6.15	The Discrete Logarithms Evaluation Problem . . . . .	235
6.16	The Hidden Subgroup Problem . . . . .	237
6.17	Quantum Search Algorithms . . . . .	240
6.18	Historical Notes . . . . .	247
6.19	Summary and Further Readings . . . . .	248
6.20	Exercises and Problems . . . . .	252
<b>7</b>	<b>The “Entanglement” of Computing and Communication with Quantum Me-</b>	
	<b>chanics. Reversible Computations</b>	<b>254</b>
7.1	Communication, Entropy, and Quantum Information . . . . .	255
7.2	Information Encoding . . . . .	258
7.3	Quantum Teleportation with Maximally Entangled Particles . . . . .	259
7.4	Anti-Correlation and Teleportation . . . . .	267
7.5	Dense Coding . . . . .	269
7.6	Quantum Key Distribution . . . . .	274
7.7	EPR Pairs and Bell States . . . . .	277
7.8	Uncertainty and Locality . . . . .	279
7.9	Possible Explanations of the EPR Experiment . . . . .	282
7.10	The Bell Inequality. Local Realism . . . . .	283
7.11	Reversibility and Entropy . . . . .	285
7.12	Thermodynamics and Thermodynamic Entropy . . . . .	286
7.13	The Maxwell Demon . . . . .	288
7.14	Energy Consumption. Landauer Principle . . . . .	289
7.15	Low Power Computing. Adiabatic Switching . . . . .	292
7.16	Bennett Information Driven Engine . . . . .	292
7.17	Logically Reversible Turing Machines and Physical Reversibility . . . . .	293
7.18	Historical Notes . . . . .	295
7.19	Summary and Further Readings . . . . .	297
7.20	Exercises and Problems . . . . .	299
<b>8</b>	<b>Appendix I: Algebraic Structures</b>	<b>300</b>
8.1	Rings, Commutative Rings, Integral Domains, Fields . . . . .	300
8.2	Complex Numbers . . . . .	302
8.3	Abstract Groups and Isomorphisms . . . . .	304
8.4	Matrix Representation . . . . .	306
8.5	Groups of Transformations . . . . .	306
8.6	Symmetry in a Plane . . . . .	307
8.7	Finite Fields . . . . .	308
<b>9</b>	<b>Appendix II: Modular Arithmetic</b>	<b>311</b>
9.1	Elementary Number Theory Concepts . . . . .	311
9.2	Euclid’s Algorithm for Integers . . . . .	314
9.3	The Chinese Remainder Theorem and its Applications . . . . .	315
9.4	Computer Arithmetic for Large Integers . . . . .	316

<b>10 Appendix III: Welsh-Hadamard Transform</b>	<b>319</b>
10.1 Hadamard Matrices . . . . .	319
10.2 The Fast Hadamard Transform . . . . .	322
<b>11 Appendix IV: Fourier Transform and Fourier Series</b>	<b>326</b>
<b>12 Glossary</b>	<b>337</b>