

Principles of Quantum Computation and Information

Volume I: Basic Concepts

Giuliano Benenti and Giulio Casati

Università degli Studi dell'Insubria, Italy
Istituto Nazionale per la Fisica della Materia, Italy

Giuliano Strini

Università di Milano, Italy

 World Scientific

NEW JERSEY • LONDON • SINGAPORE • BEIJING • SHANGHAI • HONG KONG • TAIPEI • CHENNAI

Contents

<i>Preface</i>	vii
<i>Introduction</i>	1
1. Introduction to Classical Computation	9
1.1 The Turing machine	9
1.1.1 Addition on a Turing machine	12
1.1.2 The Church–Turing thesis	13
1.1.3 The universal Turing machine	14
1.1.4 The probabilistic Turing machine	14
1.1.5 * The halting problem	15
1.2 The circuit model of computation	15
1.2.1 Binary arithmetics	17
1.2.2 Elementary logic gates	17
1.2.3 Universal classical computation	22
1.3 Computational complexity	24
1.3.1 Complexity classes	27
1.3.2 * The Chernoff bound	30
1.4 * Computing dynamical systems	30
1.4.1 * Deterministic chaos	31
1.4.2 * Algorithmic complexity	33
1.5 Energy and information	35
1.5.1 Maxwell’s demon	35
1.5.2 Landauer’s principle	37
1.5.3 Extracting work from information	40
1.6 Reversible computation	41

1.6.1	Toffoli and Fredkin gates	43
1.6.2	* The billiard-ball computer	45
1.7	A guide to the bibliography	47
2.	Introduction to Quantum Mechanics	49
2.1	The Stern–Gerlach experiment	50
2.2	Young’s double-slit experiment	53
2.3	Linear vector spaces	57
2.4	The postulates of quantum mechanics	76
2.5	The EPR paradox and Bell’s inequalities	88
2.6	A guide to the bibliography	97
3.	Quantum Computation	99
3.1	The qubit	100
3.1.1	The Bloch sphere	102
3.1.2	Measuring the state of a qubit	103
3.2	The circuit model of quantum computation	105
3.3	Single-qubit gates	108
3.3.1	Rotations of the Bloch sphere	110
3.4	Controlled gates and entanglement generation	112
3.4.1	The Bell basis	118
3.5	Universal quantum gates	118
3.5.1	* Preparation of the initial state	127
3.6	Unitary errors	130
3.7	Function evaluation	132
3.8	The quantum adder	137
3.9	Deutsch’s algorithm	140
3.9.1	The Deutsch–Jozsa problem	141
3.9.2	* An extension of Deutsch’s algorithm	143
3.10	Quantum search	144
3.10.1	Searching one item out of four	145
3.10.2	Searching one item out of N	148
3.10.3	Geometric visualization	149
3.11	The quantum Fourier transform	152
3.12	Quantum phase estimation	155
3.13	* Finding eigenvalues and eigenvectors	158
3.14	Period finding and Shor’s algorithm	161
3.15	Quantum computation of dynamical systems	164

3.15.1	Quantum simulation of the Schrödinger equation . . .	164
3.15.2	* The quantum baker's map	168
3.15.3	* The quantum sawtooth map	170
3.15.4	* Quantum computation of dynamical localization .	174
3.16	First experimental implementations	178
3.16.1	Elementary gates with spin qubits	179
3.16.2	Overview of the first implementations	181
3.17	A guide to the bibliography	185
4.	Quantum Communication	189
4.1	Classical cryptography	189
4.1.1	The Vernam cypher	190
4.1.2	The public-key cryptosystem	191
4.1.3	The RSA protocol	192
4.2	The no-cloning theorem	194
4.2.1	Faster-than-light transmission of information?	197
4.3	Quantum cryptography	198
4.3.1	The BB84 protocol	199
4.3.2	The E91 protocol	202
4.4	Dense coding	205
4.5	Quantum teleportation	208
4.6	An overview of the experimental implementations	213
4.7	A guide to the bibliography	214
Appendix A	Solutions to the exercises	215
<i>Bibliography</i>		241
<i>Index</i>		253