

Quantum computation and information is a rapidly developing interdisciplinary field. It is not easy to understand its fundamental concepts and central results without facing numerous technical details. This book provides the reader with a useful guide. In particular, the initial chapters offer a simple and self-contained introduction; no previous knowledge of quantum mechanics or classical computation is required.



Various important aspects of quantum computation and information are covered in depth, starting from the foundations (the basic concepts of computational complexity, energy, entropy, and information, quantum superposition and entanglement, elementary quantum gates, the main quantum algorithms, quantum teleportation, and

quantum cryptography) up to advanced topics (like entanglement measures, quantum discord, quantum noise, quantum channels, quantum error correction, quantum simulators, and tensor networks).

It can be used as a broad range textbook for a course in quantum information and computation, both for upper-level undergraduate students and for graduate students. It contains a large number of solved exercises, which are an essential complement to the text, as they will help the student to become familiar with the subject. The book may also be useful as general education for readers who want to know the fundamental principles of quantum information and computation.

Benenti  
Casati  
Rossini  
Strini

Principles of Quantum Computation and Information  
A Comprehensive Textbook

Giuliano Benenti Giulio Casati  
Davide Rossini Giuliano Strini



Principles of Quantum Computation  
and Information  
A Comprehensive Textbook

“Thorough introductions to classical computation and irreversibility, and a primer of quantum theory, lead into the heart of this impressive and substantial book. All the topics – quantum algorithms, quantum error correction, adiabatic quantum computing and decoherence are just a few – are explained carefully and in detail. Particularly attractive are the connections between the conceptual structures and mathematical formalisms, and the different experimental protocols for bringing them to practice. A more wide-ranging, comprehensive, and definitive text is hard to imagine.”

— Sir Michael Berry, *University of Bristol, UK*

“This second edition of the textbook is a timely and very comprehensive update in a rapidly developing field, both in theory as well as in the experimental implementation of quantum information processing. The book provides a solid introduction into the field, a deeper insight in the formal description of quantum information as well as a well laid-out overview on several platforms for quantum simulation and quantum computation. All in all, a well-written and commendable textbook, which will prove very valuable both for the novices and the scholars in the fields of quantum computation and information.”

— Rainer Blatt, *Universität Innsbruck and IQOQI Innsbruck, Austria*

“The book by Benenti, Casati, Rossini and Strini is an excellent introduction to the fascinating field of quantum information, of great benefit for scientists entering the field and a very useful reference for people already working in it. The second edition of the book is considerably extended with new chapters, as the one on many-body systems, and necessary updates, most notably on the physical implementations.”

— Rosario Fazio, *The Abdus Salam International Centre for Theoretical Physics, Trieste, Italy*

World Scientific  
www.worldscientific.com  
10909 hc



World Scientific

# 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 . . . . .	11
1.1.2 The Church–Turing thesis . . . . .	13
1.1.3 The universal Turing machine . . . . .	14
1.1.4 The probabilistic Turing machine . . . . .	15
1.1.5 * The halting problem . . . . .	15
1.2 The circuit model of computation . . . . .	16
1.2.1 Binary arithmetics . . . . .	17
1.2.2 Elementary logic gates . . . . .	18
1.2.3 Universal classical computation . . . . .	21
1.3 Computational complexity . . . . .	22
1.3.1 Tractable vs. intractable problems . . . . .	23
1.3.2 Complexity classes . . . . .	30
1.3.3 * The Chernoff bound . . . . .	34
1.4 * Computing dynamical systems . . . . .	34
1.4.1 * Deterministic chaos . . . . .	35
1.4.2 * Algorithmic complexity . . . . .	37
1.5 Energy and information . . . . .	39
1.5.1 Maxwell’s demon . . . . .	39
1.5.2 Landauer’s principle . . . . .	40
1.5.3 Extracting work from information . . . . .	42
1.6 Reversible computation . . . . .	43
1.6.1 Toffoli and Fredkin gates . . . . .	45
1.6.2 * The billiard-ball computer . . . . .	46
1.7 * Energy dissipation in computation . . . . .	48
1.7.1 * Experimental realization of a Maxwell’s demon . . . . .	48

xii	<i>Principles of Quantum Computation and Information. II</i>	
	1.7.2 * Experimental verification of Landauer's principle . . . . .	49
	1.7.3 * Energy dissipation in real classical computer . . . . .	50
	1.7.4 * Experimental realization of reversible computers . . . . .	51
	1.7.5 * Neuromorphic computing . . . . .	53
1.8	A guide to the bibliography . . . . .	54
2.	Introduction to quantum mechanics . . . . .	55
2.1	The Stern–Gerlach experiment . . . . .	56
2.2	Young's double-slit experiment . . . . .	59
2.3	The postulates of quantum mechanics . . . . .	63
	2.3.1 Dynamical evolution . . . . .	63
	2.3.2 Outcomes of a measurement . . . . .	64
	2.3.3 The post-measurement state . . . . .	67
	2.3.4 Heisenberg's uncertainty principle . . . . .	69
2.4	The EPR paradox . . . . .	72
2.5	Bell's inequalities . . . . .	77
2.6	The density matrix . . . . .	81
	2.6.1 Composite systems . . . . .	86
2.7	The Schmidt decomposition . . . . .	89
2.8	Purification . . . . .	91
2.9	Generalized measurements . . . . .	93
	2.9.1 POVM measurements . . . . .	94
2.10	A guide to the bibliography . . . . .	96
3.	Quantum computation . . . . .	97
3.1	The qubit . . . . .	98
	3.1.1 Pure qubit states: The Bloch sphere . . . . .	99
	3.1.2 Mixed qubit states: The Bloch ball . . . . .	100
3.2	Measuring the state of a qubit . . . . .	103
	3.2.1 Pure qubit states . . . . .	103
	3.2.2 Mixed qubit states . . . . .	104
3.3	The circuit model of quantum computation . . . . .	105
3.4	Single-qubit gates . . . . .	108
	3.4.1 Rotations of the Bloch sphere . . . . .	109
3.5	Controlled gates and entanglement generation . . . . .	111
	3.5.1 The Bell basis . . . . .	115
3.6	Hamiltonian model for one- and two-qubit gates . . . . .	116
3.7	Universal quantum gates . . . . .	117
	3.7.1 * Preparation of the initial state . . . . .	124
3.8	Unitary errors . . . . .	127
3.9	Function evaluation . . . . .	128
3.10	* The quantum adder . . . . .	132

## Contents

xiii

3.11	Adiabatic theorem . . . . .	134
3.11.1	Adiabatic condition . . . . .	136
3.11.2	Berry phase . . . . .	137
3.12	* Non Abelian geometric phase . . . . .	141
3.13	Adiabatic quantum computation . . . . .	145
3.14	* Maximum speed of quantum gates . . . . .	150
3.14.1	* Speed limit of an autonomous time evolution . . . . .	150
3.14.2	* Speed limit of single-qubit gates . . . . .	151
3.15	* Holonomic quantum computation . . . . .	152
3.16	A guide to the bibliography . . . . .	155
4.	Quantum algorithms . . . . .	157
4.1	Deutsch's algorithm . . . . .	157
4.1.1	The Deutsch–Jozsa problem . . . . .	158
4.1.2	* An extension of Deutsch's algorithm . . . . .	159
4.2	Quantum search . . . . .	161
4.2.1	Searching one item out of four . . . . .	161
4.2.2	Searching one item out of $N$ . . . . .	163
4.2.3	Geometric visualization . . . . .	164
4.2.4	Searching by adiabatic quantum evolution . . . . .	166
4.3	The quantum Fourier transform . . . . .	168
4.4	Quantum phase estimation . . . . .	171
4.5	* Finding eigenvalues and eigenvectors . . . . .	173
4.6	Period finding and Shor's algorithm . . . . .	175
4.7	Quantum computation of dynamical systems . . . . .	179
4.7.1	Quantum simulation of the Schrödinger equation . . . . .	179
4.7.2	* The quantum baker's map . . . . .	183
4.7.3	* The quantum sawtooth map . . . . .	185
4.7.4	Information extraction for dynamical quantum systems . . . . .	188
4.8	Universal quantum simulation . . . . .	190
4.9	A guide to the bibliography . . . . .	192
5.	Quantum communication . . . . .	195
5.1	Classical cryptography . . . . .	195
5.1.1	The Vernam cypher . . . . .	196
5.1.2	The public-key cryptosystem . . . . .	197
5.1.3	The RSA protocol . . . . .	198
5.2	The no-cloning theorem . . . . .	199
5.2.1	Faster-than-light transmission of information? . . . . .	201
5.2.2	* The no-signalling condition . . . . .	203
5.2.3	* Universal quantum cloning . . . . .	204
5.2.4	* The universal-NOT gate . . . . .	206

5.3	Quantum cryptography . . . . .	207
5.3.1	The BB84 protocol . . . . .	207
5.3.2	The E91 protocol . . . . .	210
5.4	Dense coding . . . . .	212
5.5	Quantum teleportation . . . . .	215
5.5.1	* Conclusive teleportation . . . . .	219
5.6	Quantum mechanics with continuous variables . . . . .	220
5.6.1	* General framework for Gaussian states . . . . .	233
5.7	Quantum cryptography with continuous variables . . . . .	237
5.8	A guide to the bibliography . . . . .	240
6.	Entanglement and non-classical correlations . . . . .	241
6.1	Definition of entanglement . . . . .	241
6.1.1	Basic properties . . . . .	242
6.2	Bipartite separability criteria . . . . .	243
6.2.1	The Peres separability criterion . . . . .	244
6.2.2	Positive maps . . . . .	245
6.2.3	Entanglement witnesses . . . . .	246
6.2.4	Positive maps and witnesses . . . . .	248
6.3	The Shannon entropy . . . . .	248
6.3.1	Mutual information . . . . .	250
6.4	The von Neumann entropy . . . . .	252
6.4.1	Example 1: source of orthogonal pure states . . . . .	255
6.4.2	Example 2: source of non-orthogonal pure states . . . . .	255
6.5	Entanglement concentration . . . . .	256
6.5.1	* Entanglement of a random state . . . . .	260
6.6	Requirements for bipartite entanglement measures . . . . .	263
6.7	Other entanglement measures . . . . .	264
6.7.1	* Concurrence . . . . .	264
6.7.2	* Negativity . . . . .	265
6.8	* Multipartite entanglement . . . . .	266
6.8.1	* Monogamy of entanglement and tangle measures . . . . .	268
6.9	Quantum discord . . . . .	269
6.9.1	Definition . . . . .	270
6.9.2	Basic properties . . . . .	273
6.9.3	Examples . . . . .	274
6.9.4	* Other measures of quantum correlations . . . . .	275
6.10	* Quantum discord in continuous systems . . . . .	277
6.10.1	* Entropy of a Gaussian state . . . . .	277
6.10.2	* Discord of a Gaussian state . . . . .	278
6.11	* Entropies in physics . . . . .	279
6.11.1	* Thermodynamic entropy . . . . .	280

*Contents*

xv

6.11.2	* Statistical entropy . . . . .	282
6.11.3	* Dynamical Kolmogorov–Sinai entropy . . . . .	284
6.12	A guide to the bibliography . . . . .	285
7.	Decoherence . . . . .	287
7.1	The Kraus representation . . . . .	287
7.2	Decoherence models for a single qubit . . . . .	293
7.2.1	The quantum black box . . . . .	294
7.2.2	Measuring a quantum operation acting on a qubit . . . . .	295
7.2.3	Quantum circuits simulating noise channels . . . . .	296
7.2.4	The bit-flip channel . . . . .	298
7.2.5	The phase-flip channel . . . . .	299
7.2.6	The bit-phase-flip channel . . . . .	300
7.2.7	The depolarizing channel . . . . .	301
7.2.8	Amplitude damping . . . . .	302
7.2.9	Phase damping . . . . .	303
7.2.10	De-entanglement . . . . .	305
7.3	* The Bloch-Fano representation . . . . .	307
7.3.1	* Bloch-Fano representation of a state . . . . .	307
7.3.2	* Bloch-Fano representation of a quantum operation . . . . .	308
7.4	The master equation . . . . .	310
7.4.1	* Derivation of the master equation . . . . .	311
7.4.2	The master equation and quantum operations . . . . .	319
7.4.3	The master equation for a single qubit . . . . .	322
7.5	* Non-Markovian quantum dynamics . . . . .	324
7.6	Quantum to classical transition . . . . .	329
7.6.1	Schrödinger’s cat . . . . .	329
7.6.2	Decoherence and destruction of cat states . . . . .	330
7.7	Decoherence and quantum measurements . . . . .	335
7.7.1	* Weak measurements . . . . .	337
7.7.2	* Decoherence and quantum trajectories . . . . .	340
7.8	A guide to the bibliography . . . . .	344
8.	Quantum information theory . . . . .	345
8.1	Classical data compression . . . . .	346
8.1.1	Shannon’s noiseless coding theorem . . . . .	346
8.1.2	Examples of data compression . . . . .	348
8.1.3	Capacity of classical channels . . . . .	349
8.2	Quantum data compression . . . . .	351
8.2.1	Schumacher’s quantum noiseless coding theorem . . . . .	351
8.2.2	Compression of an $n$ -qubit message . . . . .	352
8.2.3	Example 1: two-qubit messages . . . . .	354

8.2.4	Example 2: three-qubit messages . . . . .	355
8.3	Accessible information . . . . .	357
8.3.1	The Holevo bound . . . . .	358
8.3.2	Example 1: two non-orthogonal pure states . . . . .	359
8.3.3	* Example 2: three non-orthogonal pure states . . . . .	362
8.4	Capacities of quantum channels . . . . .	363
8.4.1	Classical capacity . . . . .	364
8.4.2	Quantum capacity . . . . .	365
8.5	* Quantum memory channels . . . . .	371
8.6	A guide to the bibliography . . . . .	378
9.	Quantum error correction . . . . .	379
9.1	The three-qubit bit-flip code . . . . .	381
9.2	The three-qubit phase-flip code . . . . .	384
9.3	The nine-qubit Shor code . . . . .	385
9.4	General properties of quantum error correction . . . . .	389
9.4.1	The quantum Hamming bound . . . . .	391
9.5	Stabilizer coding . . . . .	392
9.5.1	The nine-qubit Shor code revisited . . . . .	392
9.5.2	* General formalism for stabilizer codes . . . . .	394
9.5.3	* Logical operators for stabilizer codes . . . . .	395
9.6	* The five-qubit code . . . . .	396
9.7	Decoherence-free subspaces . . . . .	399
9.7.1	* Conditions for decoherence-free dynamics . . . . .	401
9.7.2	* The spin-boson model . . . . .	402
9.8	* Dynamical decoupling . . . . .	404
9.8.1	* Explicit form of control Hamiltonian . . . . .	406
9.9	* The Zeno effect . . . . .	407
9.10	Fault-tolerant quantum computation . . . . .	411
9.10.1	Avoidance of error propagation . . . . .	411
9.10.2	Fault-tolerant quantum gates . . . . .	413
9.10.3	The noise threshold for quantum computation . . . . .	414
9.11	A guide to the bibliography . . . . .	415
10.	Principles of experimental implementations of quantum protocols . . . . .	417
10.1	Cavity quantum electrodynamics . . . . .	418
10.1.1	Interaction of a two-level atom with a classical field . . . . .	420
10.1.2	The Jaynes–Cummings model . . . . .	421
10.1.3	Rabi oscillations . . . . .	422
10.1.4	Entanglement generation . . . . .	423
10.2	The ion-trap quantum computer . . . . .	424
10.2.1	The Paul trap . . . . .	425

*Contents*

xvii

10.2.2	Laser pulses . . . . .	427
10.3	Solid-state qubits . . . . .	433
10.3.1	Spins in semiconductors . . . . .	433
10.3.2	Quantum dots . . . . .	434
10.3.3	Superconducting qubit circuits . . . . .	437
10.4	Quantum communication with photons . . . . .	443
10.4.1	Linear optics . . . . .	444
10.4.2	Non-linear optics and probabilistic gates . . . . .	447
10.4.3	Experimental quantum-key distribution . . . . .	449
10.5	Problems and prospects . . . . .	455
10.6	A guide to the bibliography . . . . .	455
11.	Quantum information in many-body systems . . . . .	457
11.1	Quantum simulators . . . . .	458
11.1.1	Ultracold atoms . . . . .	458
11.1.2	Arrays of coupled QED cavities . . . . .	461
11.2	Emergence of quantum correlations . . . . .	466
11.2.1	The Hubbard model . . . . .	467
11.3	The spin-1/2 quantum Ising chain . . . . .	469
11.3.1	Jordan–Wigner transformation . . . . .	470
11.3.2	Diagonalization of the Ising chain . . . . .	472
11.3.3	Two-spin concurrence . . . . .	478
11.3.4	Entanglement block entropy . . . . .	479
11.3.5	The Ising model revisited: Kitaev chain . . . . .	481
11.4	Area-law scaling of the entanglement . . . . .	484
11.5	Matrix product states . . . . .	487
11.5.1	Examples of MPS wave functions . . . . .	490
11.6	Graphical representation of matrix product states . . . . .	492
11.6.1	Expectation values of observables . . . . .	494
11.6.2	* Scaling of correlation functions with the distance . . . . .	496
11.6.3	Gauge freedom . . . . .	498
11.6.4	Schmidt decomposition of a MPS . . . . .	500
11.7	Ground-state search in the Hilbert space corner . . . . .	503
11.7.1	Density-matrix renormalization group . . . . .	506
11.7.2	* DMRG as a variational optimization over the MPS class . . . . .	510
11.8	Time evolution of matrix product states . . . . .	512
11.8.1	Finite-temperature calculations . . . . .	515
11.8.2	Mixed-state time evolution . . . . .	517
11.9	* General tensor-network structures . . . . .	519
11.9.1	* Projected entangled pair states . . . . .	519
11.9.2	* Hierarchical tensor networks . . . . .	524
11.10	A guide to the bibliography . . . . .	526



<i>Conclusions and Prospects</i>	529
Appendix A Elements of linear algebra	535
A.1 Finite-dimensional vector spaces . . . . .	535
A.1.1 Basic properties of vector spaces . . . . .	535
A.1.2 Inner product and norm of a vector . . . . .	536
A.1.3 Linear independence and the notion of basis . . . . .	538
A.1.4 Linear operators . . . . .	540
A.1.5 Tensor product . . . . .	545
A.1.6 Matrix decompositions . . . . .	547
A.1.7 Symplectic decompositions . . . . .	555
A.2 Infinite-dimensional vector spaces . . . . .	557
A.2.1 Discrete and continuous bases . . . . .	557
A.2.2 The Dirac delta function . . . . .	558
A.2.3 Orthonormality and completeness relations . . . . .	559
A.2.4 Position and momentum representations . . . . .	560
A.2.5 Position and momentum operators . . . . .	563
Appendix B Solutions to the exercises	565
B.1 Chapter 1 . . . . .	565
B.2 Chapter 2 . . . . .	566
B.3 Chapter 3 . . . . .	573
B.4 Chapter 4 . . . . .	584
B.5 Chapter 5 . . . . .	585
B.6 Chapter 6 . . . . .	594
B.7 Chapter 7 . . . . .	600
B.8 Chapter 8 . . . . .	615
B.9 Chapter 9 . . . . .	618
B.10 Chapter 10 . . . . .	625
B.11 Chapter 11 . . . . .	644
B.12 Appendix A . . . . .	648
<i>Bibliography</i>	651
<i>Index</i>	677