

Giuliano Benenti Giulio Casati Giuliano Strini

S	A	T	O	R
A	R	E	P	O
T	E	N	E	T
O	P	E	R	A
R	O	T	A	S

# Principles of Quantum Computation and Information

Volume II: Basic Tools and Special Topics

**World Scientific**

# Principles of Quantum Computation and Information

Volume II: Basic Tools and Special Topics

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

*Published by*

World Scientific Publishing Co. Pte. Ltd.

5 Toh Tuck Link, Singapore 596224

*USA office:* 27 Warren Street, Suite 401-402, Hackensack, NJ 07601

*UK office:* 57 Shelton Street, Covent Garden, London WC2H 9HE

**British Library Cataloguing-in-Publication Data**

A catalogue record for this book is available from the British Library.

**PRINCIPLES OF QUANTUM COMPUTATION AND INFORMATION**

**Volume II: Basic Tools and Special Topics**

Copyright © 2007 by World Scientific Publishing Co. Pte. Ltd.

*All rights reserved. This book, or parts thereof, may not be reproduced in any form or by any means, electronic or mechanical, including photocopying, recording or any information storage and retrieval system now known or to be invented, without written permission from the Publisher.*

For photocopying of material in this volume, please pay a copying fee through the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, USA. In this case permission to photocopy is not required from the publisher.

ISBN-13 978-981-256-345-3

ISBN-10 981-256-345-8

ISBN-13 978-981-256-528-0 (pbk)

ISBN-10 981-256-528-0 (pbk)



**Giuliano Benenti.** Born in Voghera (Pavia), Italy, November 7, 1969. He is a researcher in Theoretical Physics at Università dell' Insubria, Como. He received his Ph.D. in physics at Università di Milano, Italy and was a postdoctoral fellow at CEA, Saclay, France. His main research interests are in the fields of classical and quantum chaos, open quantum systems, mesoscopic physics, disordered systems, phase transitions, many-body systems and quantum information theory.



**Giulio Casati.** Born in Brenna (Como), Italy, December 9, 1942. He is a professor of Theoretical Physics at Università dell' Insubria, Como, former professor at Milano University, and distinguished visiting professor at NUS, Singapore. A member of the Accademia Europea, and director of the Center for Nonlinear and Complex Systems, he was awarded the F. Somaini Italian prize for physics in 1991. As editor of several volumes on classical and quantum chaos, he has done pioneering research in nonlinear dynamics, classical and quantum chaos with applications to atomic, solid state, nuclear physics and, more recently, to quantum computers.



**Giuliano Strini.** Born in Roma, Italy, September 9, 1937. He is an associate professor in Experimental Physics and has been teaching a course on Quantum Computation at Università di Milano, for several years. From 1963, he has been involved in the construction and development of the Milan Cyclotron. His publications concern nuclear reactions and spectroscopy, detection of gravitational waves, quantum optics and, more recently, quantum computers. He is a member of the Italian Physical Society, and also the Optical Society of America.

*To Silvia and Arianna*  
g.b.

*To my wife for her love and encouragement*  
g.c.

*To my family and friends*  
g.s.

## *About the Cover*

This acrostic is the famous *sator* formula. It can be translated as:

*'Arepo the sower holds the wheels at work'*

The text may be read in four different ways:

- (i) horizontally, from left to right (downward) and from right to left (upward);
- (ii) vertically, downward (left to right) and upward (right to left).

The resulting phrase is always the same.

It has been suggested that it might be a form of secret message.

This acrostic was unearthed during archeological excavation work at Pompeii, which was buried, as well known, by the eruption of Vesuvius in 79 A.D. The formula can be found throughout the Roman Empire, probably also spread by legionnaires. Moreover, it has been found in Mesopotamia, Egypt, Cappadocia, Britain and Hungary.

The *sator* acrostic may have a mystical significance and might have been used as a means for persecuted Christians to recognize each other (it can be rearranged into the form of a cross, with the opening words of the Lord's prayer, *A Paternoster O*, both vertically and horizontally, intersecting at the letter N, the Latin letters A and O corresponding to the Greek letters alpha and omega, beginning and end of all things).

# Preface

## *Purpose of the book*

This book is addressed to undergraduate and graduate students in physics, mathematics and computer science. It is written at a level comprehensible to readers with the background of a student near the end of an undergraduate course in one of the above three disciplines. Note that no prior knowledge of either quantum mechanics or classical computation is required to follow this book. Indeed, the first two chapters are a simple introduction to classical computation and quantum mechanics. Our aim is that these chapters should provide the necessary background for an understanding of the subsequent chapters.

The book is divided into two volumes. In volume I, after providing the necessary background material in classical computation and quantum mechanics, we develop the basic principles and discuss the main results of quantum computation and information. Volume I would thus be suitable for a one-semester introductory course in quantum information and computation, for both undergraduate and graduate students. It is also our intention that volume I be useful as a general education for other readers who wish to learn the basic principles of quantum computation and information and who have the basic background in physics and mathematics acquired in undergraduate courses in physics, mathematics or computer science.

Volume II deals with various important aspects, both theoretical and experimental, of quantum computation and information. The areas include quantum data compression, accessible information, entanglement concentration, limits to quantum computation due to decoherence, quantum error correction, and the first experimental implementations of quantum information protocols. This volume also includes a selection of special topics:

chaos and the quantum-to-classical transition, quantum trajectories, quantum computation and quantum chaos, and the Zeno effect. For an understanding of this volume, a knowledge of the material discussed in the first volume is necessary.

### *General approach*

Quantum computation and information is a new and rapidly developing field. It is therefore not easy to grasp the fundamental concepts and central results without having to face many technical details. Our purpose in this book is to provide the reader interested in the field with a useful and not overly heavy guide. Mathematical rigour is therefore not our primary concern. Instead, we have tried to present a simple and systematic treatment, such that the reader might understand the material presented without the need for consulting other texts. Moreover, we have not tried to cover all aspects of the field, preferring to concentrate on the fundamental concepts. Nevertheless, the two volumes should prove useful as a reference guide to researchers just starting out in the field.

To gain complete familiarity with the subject, it is important to practice problem solving. The book contains a large number of exercises (with solutions), which are an essential complement to the main text. In order to develop a solid understanding of the arguments dealt with here, it is indispensable that the student try to solve a large part of them.

### *Note to the reader*

Some of the material presented is not necessary for understanding the rest of the book and may be omitted on a first reading. We have adopted two methods of highlighting such parts:

- 1) The sections or subsections with an asterisk before the title contain more advanced or complementary material. Such parts may be omitted without risk of encountering problems in reading the rest of the book.
- 2) Comments, notes or examples are printed in a small typeface.

### *Acknowledgments*

We are indebted to several colleagues for criticism and suggestions. In particular, we wish to thank Alberto Bertoni, Gabriel Carlo, David Cory, Jürgen Eschner, Paolo Facchi, Rosario Fazio, Giuseppe Florio, Bertrand Georgeot, Luigi Lugiato, Paolo Mataloni, Sandro Morasca, Simone Montangero, Massimo Palma, Saverio Pascazio, Christian Roos, Davide Rossini, Nicoletta Sabadini, Marcos Saraceno, Fabio Sciarrino, Stefano Serra Capiz-



zано, Lorenza Viola and Robert Walters, who read preliminary versions of the book. We are also grateful to Federico Canobbio and Sisi Chen. Special thanks is due to Philip Ratcliffe, for useful remarks and suggestions, which substantially improved our book. Obviously no responsibility should be attributed to any of the above regarding possible flaws that might remain, for which the authors alone are to blame.

# Contents – Volume I

<i>Preface</i>	ix
<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  $N$  . . . . . 147
    - 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 . . . . .	204
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

# Contents – Volume II

<i>Preface</i>	vii
5. Quantum Information Theory	257
5.1 The density matrix . . . . .	258
5.1.1 The density matrix for a qubit . . . . .	264
5.1.2 Composite systems . . . . .	267
5.1.3 * The quantum copying machine . . . . .	271
5.2 The Schmidt decomposition . . . . .	273
5.3 Purification . . . . .	276
5.4 The Kraus representation . . . . .	278
5.5 Measurement of the density matrix for a qubit . . . . .	284
5.6 Generalized measurements . . . . .	286
5.6.1 * Weak measurements . . . . .	288
5.6.2 POVM measurements . . . . .	290
5.7 The Shannon entropy . . . . .	293
5.8 Classical data compression . . . . .	294
5.8.1 Shannon’s noiseless coding theorem . . . . .	294
5.8.2 Examples of data compression . . . . .	296
5.9 The von Neumann entropy . . . . .	297
5.9.1 Example 1: source of orthogonal pure states . . . . .	299
5.9.2 Example 2: source of non-orthogonal pure states . . . . .	300
5.10 Quantum data compression . . . . .	303
5.10.1 Schumacher’s quantum noiseless coding theorem . . . . .	303
5.10.2 Compression of an $n$ -qubit message . . . . .	304
5.10.3 Example 1: two-qubit messages . . . . .	306
5.10.4 Example 2: three-qubit messages . . . . .	308

5.11	Accessible information . . . . .	311
5.11.1	The Holevo bound . . . . .	313
5.11.2	Example 1: two non-orthogonal pure states . . . . .	313
5.11.3	* Example 2: three non-orthogonal pure states . . . . .	317
5.12	Entanglement concentration and von Neumann entropy . . . . .	319
5.13	The Peres separability criterion . . . . .	323
5.14	* Entropies in physics . . . . .	325
5.14.1	* Thermodynamic entropy . . . . .	325
5.14.2	* Statistical entropy . . . . .	328
5.14.3	* Dynamical Kolmogorov–Sinai entropy . . . . .	330
5.15	A guide to the bibliography . . . . .	333
6.	Decoherence . . . . .	335
6.1	Decoherence models for a single qubit . . . . .	336
6.1.1	The quantum black box . . . . .	337
6.1.2	Measuring a quantum operation acting on a qubit . . . . .	339
6.1.3	Quantum circuits simulating noise channels . . . . .	340
6.1.4	The bit-flip channel . . . . .	343
6.1.5	The phase-flip channel . . . . .	344
6.1.6	The bit-phase-flip channel . . . . .	345
6.1.7	The depolarizing channel . . . . .	346
6.1.8	Amplitude damping . . . . .	347
6.1.9	Phase damping . . . . .	349
6.1.10	De-entanglement . . . . .	351
6.2	The master equation . . . . .	354
6.2.1	* Derivation of the master equation . . . . .	355
6.2.2	* The master equation and quantum operations . . . . .	359
6.2.3	The master equation for a single qubit . . . . .	362
6.3	Quantum to classical transition . . . . .	365
6.3.1	Schrödinger’s cat . . . . .	365
6.3.2	Decoherence and destruction of cat states . . . . .	367
6.4	* Decoherence and quantum measurements . . . . .	375
6.5	* Quantum chaos . . . . .	378
6.5.1	* Dynamical chaos in classical mechanics . . . . .	379
6.5.2	* Quantum chaos and the correspondence principle . . . . .	382
6.5.3	* Time scales of quantum chaos . . . . .	385
6.5.4	* Quantum chaos and Anderson localization . . . . .	392
6.5.5	* The hydrogen atom in a microwave field . . . . .	395
6.5.6	* Quantum chaos and universal spectral fluctuations . . . . .	400

6.5.7	* The chaos border for the quantum computer hardware	412
6.5.8	* The quantum Loschmidt echo . . . . .	416
6.5.9	* Dynamical stability of quantum motion . . . . .	423
6.5.10	* Dynamical chaos and dephasing: the double-slit experiment . . . . .	425
6.5.11	* Entanglement and chaos . . . . .	430
6.6	Decoherence and quantum computation . . . . .	434
6.6.1	* Decoherence and quantum trajectories . . . . .	439
6.7	* Quantum computation and quantum chaos . . . . .	449
6.7.1	* Quantum versus classical errors . . . . .	451
6.7.2	* Static imperfections versus noisy gates . . . . .	452
6.8	A guide to the bibliography . . . . .	457
7.	Quantum Error Correction	459
7.1	The three-qubit bit-flip code . . . . .	461
7.2	The three-qubit phase-flip code . . . . .	465
7.3	The nine-qubit Shor code . . . . .	466
7.4	General properties of quantum error correction . . . . .	471
7.4.1	The quantum Hamming bound . . . . .	473
7.5	* The five-qubit code . . . . .	474
7.6	* Classical linear codes . . . . .	476
7.6.1	* The Hamming codes . . . . .	478
7.7	* CSS codes . . . . .	481
7.8	Decoherence-free subspaces . . . . .	484
7.8.1	* Conditions for decoherence-free dynamics . . . . .	486
7.8.2	* The spin-boson model . . . . .	488
7.9	* The Zeno effect . . . . .	490
7.10	Fault-tolerant quantum computation . . . . .	494
7.10.1	Avoidance of error propagation . . . . .	495
7.10.2	Fault-tolerant quantum gates . . . . .	497
7.10.3	The noise threshold for quantum computation . . . . .	497
7.11	* Quantum cryptography over noisy channels . . . . .	500
7.12	* Quantum channels with memory . . . . .	506
7.13	A guide to the bibliography . . . . .	510
8.	First Experimental Implementations	513
8.1	NMR quantum computation . . . . .	514
8.1.1	The system Hamiltonian . . . . .	515

8.1.2	The physical apparatus . . . . .	518
8.1.3	Quantum ensemble computation . . . . .	519
8.1.4	Refocusing . . . . .	522
8.1.5	Demonstration of quantum algorithms . . . . .	523
8.2	Cavity quantum electrodynamics . . . . .	528
8.2.1	Rabi oscillations . . . . .	535
8.2.2	Entanglement generation . . . . .	538
8.2.3	The quantum phase gate . . . . .	542
8.3	The ion-trap quantum computer . . . . .	544
8.3.1	The Paul trap . . . . .	544
8.3.2	Laser pulses . . . . .	547
8.3.3	Realization of the Cirac-Zoller CNOT gate . . . . .	554
8.3.4	Entanglement generation . . . . .	556
8.4	Solid state qubits . . . . .	561
8.4.1	Spins in semiconductors . . . . .	561
8.4.2	Quantum dots . . . . .	562
8.4.3	Superconducting qubit circuits . . . . .	566
8.5	Quantum communication with photons . . . . .	573
8.5.1	Linear optics . . . . .	573
8.5.2	Experimental quantum teleportation . . . . .	578
8.5.3	Experimental quantum-key distribution . . . . .	587
8.6	Problems and prospects . . . . .	591
8.7	A guide to the bibliography . . . . .	592
Appendix B Solutions to the exercises		595
<i>Bibliography</i>		657
<i>Index</i>		675



## Chapter 5

# Quantum Information Theory

Classical information theory deals with the transmission of messages (say, binary strings) over communication channels. Its fundamental questions are: How much can a message be compressed and still be transmitted reliably? Can we protect this message against errors that will appear in noisy communication channels? In this chapter, we discuss the above questions in the light of quantum mechanics, which opens up new possibilities for information theory. Before doing so, we need to introduce a few useful tools. The density-matrix formalism is the natural framework in which to treat open and composite quantum systems. We also introduce the concept of generalized measurement and discuss a simple example in which it proves to be useful.

Following this, we review the main results of classical information theory. It turns out that it is possible to compress a message into a shorter string of letters, the compression factor being the Shannon entropy. This is the content of Shannon's celebrated noiseless coding theorem. We discuss the natural extension of this result to quantum mechanics. To this end one may consider a message whose letters are quantum states, transmitted through a quantum communication channel. Such quantum states may be treated as though they were (quantum) information and one might thus ask to what extent this quantum message can be compressed. Schumacher's quantum noiseless coding theorem states that the optimal compression factor is given by the von Neumann entropy. Therefore, the von Neumann entropy is the appropriate measure of quantum information, just as the Shannon entropy is for classical information. If Alice codes a classical message by means of quantum states, it is natural to ask how much information Bob can gain on the message by performing (generalized) measurements on the quantum states received. This is not an easy question since the