

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 I: Basic Concepts

World Scientific

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

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.

First published 2004

Reprinted 2005, 2008

PRINCIPLES OF QUANTUM COMPUTATION AND INFORMATION

Volume I: Basic Concepts

Copyright © 2004 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.

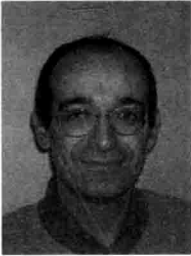
ISBN-13 978-981-238-830-8

ISBN-10 981-238-830-3

ISBN-13 978-981-238-858-2 (pbk)

ISBN-10 981-238-858-3 (pbk)

Printed in Singapore by B & JO Enterprise



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
g.b.

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

To my family and friends
g.s.

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 to the end of an undergraduate course in one of the above three disciplines. Note that no prior knowledge either of quantum mechanics or of 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 would like 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. This volume necessarily contains parts that are more technical or specialized. For its understanding, 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 this field with a useful and not overly heavy guide. Therefore, mathematical rigour is 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 fully familiarize oneself with the subject, it is important to practice solving problems. 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, Rosario Fazio, Bertrand Georgeot, Luigi Lugiato, Sandro Morasca, Simone Montangero, Massimo Palma, Saverio Pascazio, Nicoletta Sabadini, Marcos Saraceno, Stefano Serra Capizzano 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.

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).

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

Contents of Volume II

5.	Quantum Information Theory	1
5.1	The density matrix	2
5.1.1	Density matrix for a qubit: The Bloch sphere	7
5.1.2	Composite systems	10
5.1.3	* Quantum copying machine	14
5.2	Schmidt decomposition	16
5.3	Purification	18
5.4	The Kraus representation	20
5.5	Measurement of the density matrix for a qubit	26
5.6	Generalized measurements	28
5.6.1	POVM measurements	29
5.7	Shannon entropy	32
5.8	Classical data compression	33
5.8.1	Shannon's noiseless coding theorem	33
5.8.2	Examples of data compression	36
5.9	Von Neumann entropy	37
5.9.1	Example 1: Source of orthogonal pure states	38
5.9.2	Example 2: Source of non orthogonal pure states	39
5.10	Quantum data compression	42
5.10.1	Schumacher's quantum noiseless coding theorem	42
5.10.2	Compression of a n -qubit message	43
5.10.3	Example 1: Two-qubit messages	45
5.10.4	* Example 2: Three-qubit messages	46
5.11	Accessible information	49
5.11.1	The Holevo bound	51
5.11.2	Example 1: Two non-orthogonal pure states	52

5.11.3	* Example 2: Three non orthogonal pure states . . .	56
5.12	Entanglement concentration	59
6.	Decoherence	63
6.1	Decoherence models for a single qubit	64
6.1.1	Quantum black box	65
6.1.2	Measuring a quantum operation acting on a qubit . .	67
6.1.3	Quantum circuits simulating noise channels	68
6.1.4	Bit flip channel	71
6.1.5	Phase flip channel	71
6.1.6	Bit-phase flip channel	74
6.1.7	Depolarizing channel	74
6.1.8	Amplitude damping	75
6.1.9	Phase damping	77
6.1.10	Deentanglement	79
6.2	The master equation	82
6.2.1	* Derivation of the master equation	83
6.2.2	* Master equation and quantum operations	87
6.2.3	Master equation for a single qubit	90
6.3	Quantum to classical transition	93
6.3.1	The Schrödinger's cat	93
6.3.2	Decoherence and destruction of cat states	95
6.3.3	* Chaos and quantum to classical transition	102
6.4	* Decoherence and quantum measurements	102
6.5	Decoherence and quantum computation	106
6.5.1	* Quantum trajectories	106
6.6	* Quantum computation and quantum chaos	106
7.	Quantum Error-Correction	107
7.1	The three-qubit bit flip code	109
7.2	The three-qubit phase flip code	113
7.3	The nine-qubit Shor code	114
7.4	General properties of quantum error-correction	119
7.4.1	The quantum Hamming bound	121
7.5	* The five-qubit code	121
7.6	* Classical linear codes	124
7.6.1	* The Hamming codes	126
7.7	* CSS codes	129

7.8	Decoherence-free subspaces	132
7.8.1	* Conditions for decoherence-free dynamics	133
7.8.2	* The spin-boson model	136
7.9	* The Zeno effect	137
7.10	Fault-tolerant quantum computation	137
7.10.1	Avoiding error propagation	138
7.10.2	Fault-tolerant quantum gates	140
7.10.3	Noise threshold for quantum computation	140
8.	First Experimental Implementations	145
8.1	Quantum optics implementations	147
8.1.1	Teleportation	147
8.1.2	Quantum key distribution	147
8.2	NMR quantum information processing	147
8.2.1	Physical apparatus	147
8.2.2	Quantum ensemble computation	147
8.2.3	Liquid state NMR	147
8.2.4	Demonstration of quantum algorithms	147
8.3	Cavity quantum electrodynamics	147
8.3.1	Manipulating atoms and photons in a cavity	147
8.3.2	Rabi oscillations	147
8.3.3	Entanglement generation	147
8.3.4	The quantum phase gate	147
8.3.5	Schrödinger cat states and decoherence	147
8.4	The ion-trap quantum computer	147
8.4.1	Experimental setup	147
8.4.2	Building logic quantum gates	147
8.4.3	Entanglement generation	147
8.4.4	Realization of the Cirac-Zoller CNOT gate	147
8.4.5	Quantum teleportation of atomic qubits	147
8.5	Josephson-junction qubits	147
8.5.1	Charge and flux qubits	147
8.5.2	Controlled manipulation of a single qubit	147
8.5.3	Conditional gate operation	147
8.6	Other solid-state proposals	147
8.6.1	Spin in semiconductors	147
8.6.2	Quantum dots	147
8.7	Problems and prospects	147

Introduction

Quantum mechanics has had an enormous technological and societal impact. To appreciate this point, it is sufficient to consider the invention of the transistor, perhaps the most remarkable among the countless other applications of quantum mechanics. On the other hand, it is also easy to see the enormous impact of computers on everyday life. The importance of computers is such that it is appropriate to say that we are now living in the *information age*. This information revolution became possible thanks to the invention of the transistor, that is, thanks to the synergy between computer science and quantum physics.

Today this synergy offers completely new opportunities and promises exciting advances in both fundamental science and technological application. We are referring here to the fact that **quantum mechanics can be used to process and transmit information**.

Miniaturization provides us with an intuitive way of understanding why, in the near future, quantum laws will become important for computation. The electronics industry for computers grows hand-in-hand with the decrease in size of integrated circuits. This miniaturization is necessary to increase computational power, that is, the number of floating-point operations per second (flops) a computer can perform. In the 1950's, electronic computers based on vacuum-tube technology were capable of performing approximately 10^3 floating-point operations per second, while nowadays there exist supercomputers whose power is greater than 10 teraflops (10^{13} flops). As we have already remarked, this enormous growth of computational power has been made possible owing to progress in miniaturization, which may be quantified empirically in Moore's law. This law is the result of a remarkable observation made by Gordon Moore in 1965: the number

of transistors that may be placed on a single integrated-circuit chip doubles approximately every 18 – 24 months. This exponential growth has not yet saturated and Moore’s law is still valid. At the present time the limit is approximately 10^8 transistors per chip and the typical size of circuit components is of the order of 100 nanometres. Extrapolating Moore’s law, one would estimate that around the year 2020 we shall reach the atomic size for storing a single bit of information. At that point, quantum effects will become unavoidably dominant.

It is clear that, besides quantum effects, other factors could bring Moore’s law to an end. In the first place, there are economic considerations. Indeed, the cost of building fabrication facilities to manufacture chips has also increased exponentially with time. Nevertheless, it is important to understand the ultimate limitations set by quantum mechanics. Even though we might overcome economic barriers by means of technological breakthroughs, quantum physics sets fundamental limitations on the size of the circuit components. The first question under debate is whether it would be more convenient to push the silicon-based transistor to its physical limits or instead to develop alternative devices, such as quantum dots, single-electron transistors or molecular switches. A common feature of all these devices is that they are on the nanometre length scale and therefore quantum effects play a crucial role.

So far, we have talked about quantum switches that could substitute silicon-based transistors and possibly be connected together to execute classical algorithms based on Boolean logic. In this perspective, quantum effects are simply unavoidable corrections that must be taken into account owing to the nanometre size of the switches. A quantum computer represents a radically different challenge: the aim is to build a machine *based on quantum logic*, that is, it processes the information and performs logic operations by exploiting the laws of quantum mechanics.

The unit of quantum information is known as a *qubit* (the quantum counterpart of the classical *bit*) and a quantum computer may be viewed as a many-qubit system. Physically, a qubit is a two-level system, like the two spin states of a spin- $\frac{1}{2}$ particle, the vertical and horizontal polarization states of a single photon or the ground and excited states of an atom. A quantum computer is a system of many qubits, whose evolution can be controlled, and a quantum computation is a unitary transformation that acts on the many-qubit state describing the quantum computer.

The power of quantum computers is due to typical quantum phenomena, such as the *superposition* of quantum states and *entanglement*. There is an

inherent quantum parallelism associated with the superposition principle. In simple terms, a quantum computer can process a large number of classical inputs in a single run. On the other hand, this implies a large number of possible outputs. It is the task of quantum algorithms, which are based on quantum logic, to exploit the inherent quantum parallelism of quantum mechanics to highlight the desired output. In short, to be useful, quantum computers require the development of appropriate quantum software, that is, of efficient quantum algorithms.

In the 1980's Feynman suggested that a quantum computer based on quantum logic would be ideal for simulating quantum-mechanical systems and his ideas have spawned an active area of research in physics. It is also remarkable that quantum mechanics can help in the solution of basic problems of computer science. In 1994, Peter Shor proposed a quantum algorithm that efficiently solves the prime-factorization problem: given a composite integer, find its prime factors. This is a central problem in computer science and it is conjectured, though not proven, that for a classical computer it is computationally difficult to find the prime factors. Shor's algorithm efficiently solves the integer factorization problem and therefore it provides an exponential improvement in speed with respect to any known classical algorithm. It is worth mentioning here that there are cryptographic systems, such as RSA, that are used extensively today and that are based on the conjecture that no efficient algorithms exist for solving the prime factorization problem. Hence, Shor's algorithm, if implemented on a large-scale quantum computer, would break the RSA cryptosystem. Lov Grover has shown that quantum mechanics can also be useful for solving the problem of searching for a marked item in an unstructured database. In this case, the gain with respect to classical computation is quadratic.

Another interesting aspect of the quantum computer is that, in principle, it avoids dissipation. Present day classical computers, which are based on irreversible logic operations (gates), are *intrinsically* dissipative. The minimum energy requirements for irreversible computation are set by Landauer's principle: each time a single bit of information is erased, the amount of energy dissipated into the environment is at least $k_B T \ln 2$, where k_B is Boltzmann's constant and T the temperature of the environment surrounding the computer. Each irreversible classical gate must dissipate at least this amount of energy (in practice, present-day computers dissipate more by orders of magnitude). In contrast, quantum evolution is unitary and thus quantum logic gates must be reversible. Therefore, at least in principle, there is no energy dissipation during a quantum computer run.