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

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

Giuliano Strini

Universitá 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

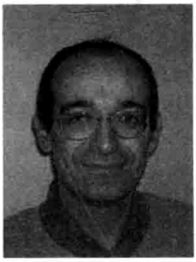
British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

First published 2004
Reprinted 2005, 2008

PRINCIPLES OF QUANTUM COMPUTATION AND INFORMATION
Volume I: Basic Concepts

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 Universita 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 Academia 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 Universita 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

Contents of Volume II

6. Decoherence 63

7. Quantum Error-Correction 107

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.