Giuliano Benenti Giulio Casati Giuliano Strini

SATOR
AREPO
TENET
OPERA
ROTAS

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

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

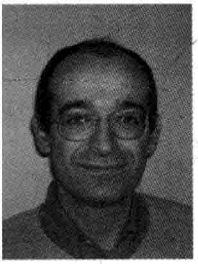
World Scientific Publishing Co. Pte. Ltd.
5 Toh Tuck Link, Singapore 596224
USA office: 27 Warren Street, Suite 401-402, Hackensack, NJ 07601
UK office: 57 Shelton Street, Covent Garden, London WC2H 9HE

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

PRINCIPLES OF QUANTUM COMPUTATION AND INFORMATION
Volume II: Basic Tools and Special Topics

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)

Printed in Singapore by World Scientific Printers (S) Pte Ltd



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 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-

zano, 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

Contents – Volume II

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