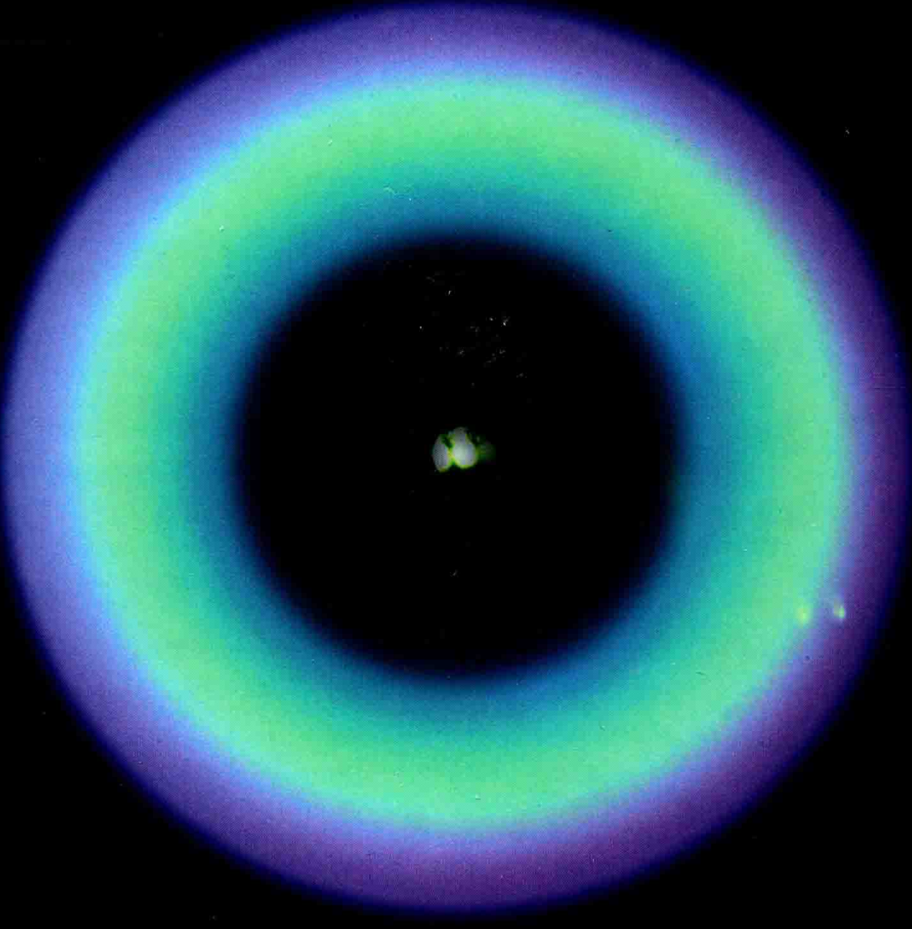
Elements *of* Quantum Computation *and* Quantum Communication



Anirban Pathak

CRC Press
Taylor & Francis Group
A CHAPMAN & HALL BOOK

Elements of Quantum Computation and Quantum Communication

Anirban Pathak

Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
A CHAPMAN & HALL BOOK

Taylor & Francis
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed on acid-free paper
Version Date: 20130404

International Standard Book Number-13: 978-1-4665-1791-2 (Hardback)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Library of Congress Cataloging-in-Publication Data

Pathak, Anirban.
Elements of quantum computation and quantum communication / author, Anirban Pathak.
pages cm
Includes bibliographical references and index.
ISBN 978-1-4665-1791-2 (hardback)
1. Quantum computers. 2. Quantum communication. 3. Quantum theory--Mathematics. I. Title.

QA76.889.P37 2013
004.1--dc23 2013010831

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Elements *of* Quantum Computation *and* Quantum Communication

This book is dedicated to my mother, Mrs. Chandana Pathak, for the elementary and fundamental lessons of life that she taught me.

Preface

This introductory textbook is written primarily for undergraduate students of physics, mathematics, computer science and other related disciplines. It is also expected to be valuable to teachers as well as to researchers working in other domains, who are interested in obtaining an understanding of quantum computation and quantum communication. I used to offer a course on quantum information theory from 2002-2006. Later I offered a few short courses in different summer schools and workshops. This book is prepared mainly from those lectures. There are many excellent textbooks on quantum information theory. However, most of those books are either too technical for beginners or they are not complete. This was one of my reasons for writing this book. But more importantly, every teacher has his/her own way to present the subject and teachers are usually biased on that. I belong to that class of biased teachers and this book is an initiative to present the subject in my way. Another fact that played a very important role in the present initiative is that there are engineering students who hardly know anything about quantum mechanics and there are physics students who do not know what a Turing machine is. But students from both groups are equally interested in quantum computing and often they join the same course. Keeping both kinds of students in mind, this book aims to give a brief idea of quantum computation and quantum communication in a self-contained manner. It does not demand any prior knowledge of quantum mechanics or computer science. It is written in a lucid manner, and a large number of problems with detailed solutions are provided in each chapter (especially in Chapter 3). In addition, a set of thought-provoking cartoons is included to make the subject more attractive. This is an introductory textbook so it will not be so thick that readers get afraid of the volume of the book and leave it before they begin. The field of quantum information and quantum computation is rapidly growing. I have tried to give a flavor of the new developments and open questions in the field, but I could not accommodate all the flavors of this interdisciplinary subject. Specifically, I could not do justice to experimental techniques. I'll consider the book successful if the readers find it easily understandable, interesting and encouraging enough to read more advanced texts and journal papers.

I understand that many students and researchers do not have access to all the journals. Keeping them in the mind, I have tried to mention all such sources where one can get access to interesting articles and courses for free. Especially in the bibliography I have provided several references from arxiv.org, and in the "further reading" sections of each chapter I have mentioned sources where seminal papers related to the field covered can be read for free. I hope readers with restricted library access will find these sources useful.

I have tried my best to avoid typos and errors. Still there may be a few present in the book. I request readers to communicate any errors, typos and suggestions by kindly sending an email to anirban.pathak@gmail.com.

This book has been written over a considerable amount of time and most of the book originates from my lecture notes. I have tried to properly cite all sources that are used here but there is a possibility that some are unintentionally omitted. I am extremely sorry for any such occurrence.

In the process of writing this book, I received help, support and encouragement from many individuals and institutes at various stages and in various forms. I would like to thank all of them. To begin with I must mention that the first few words of this book were written in 2003. It took much longer than expected. In this long period, I have lost many people who were very close to me and would have liked to see this book. I have lost my grandmother, my father, my aunts, a few of my teachers and friends who would have been very happy to see this book in existence but who passed away before it was completed. I thank them for their interest and encouragement in all my academic activities including this book-writing project. I am thankful to Dr. Anindita Banerjee and Ms. Chitra Shukla who have helped me considerably by creating the figures, correcting the typos and giving their feedback. The front cover of this book shows the image of the processed output of spontaneous parametric down conversion (SPDC) process. In the center of the image we can see the pump beam. The experiment was carried out by my colleagues at the Joint Laboratory of Optics, Olomouc. I am specially thankful to my colleagues Dr. Martin Hamar and Mr. Radek Machulka for producing this image. My old friend Mr. Anshuman Das has drawn the cartoons included in this book. His kind help has made the text more attractive. Prof. Avijit Pathak and Dr. Subhashish Banerjee have carefully read part of the manuscript and have provided their valuable feedback. I am thankful to them. Prof. Ajoy Ghatak's interest in the book was a constant encouragement. It was he who advised me to include as many examples as possible. As I see the final manuscript, it appears that his suggestion has really made it a textbook that can be used for classroom teaching. I am thankful to him for his valuable advice. The manuscript took its final form during my one-year stay at Palacky University, Czech Republic. This visit provided me ample time and the perfect ambiance to complete the manuscript. Prof. J. Peřina, Prof. V. Peřinová, Dr. O. Haderka, Dr. J. Peřina Jr. and Prof. M. Hrabovský, whose collaboration and help made this visit possible, deserve special words of thanks. Without their kind support it would have been impossible to complete the book. My special friend, Dr. R. Srikanth, who was always awake late at night to share my concerns about the book, has helped me in many ways. My long late-night conversations with him have many direct and indirect contributions to this book. No word of thanks is enough for his help. I would also like to thank all my collaborators and students together with whom I have learned the subject discussed in this book. As I mentioned, to finish this book, I took a one-year leave from JIIT, India and visited Palacky University. During this period my wife Dr. Papia Chowdhury and my son Master Pustak Pathak were very cooperative. Their selfless encouragement and support made it possible. During most of the time while I was working on this manuscript, my research activities on quantum computing and quantum communication were supported by the Department of Science and Technology, India through project numbers SR/S2/LOP-0012/2010 and SR/FTP/PS-13/2004. My activities were also supported by the Operational Program Education for Competitiveness - European Social Fund project CZ.1.07/2.3.00/20.0017 and Operational Program Research and Development for Innovations - European Regional Development Fund project CZ.1.05/2.1.00/03.0058 of the Ministry of Education, Youth and Sports of the Czech Republic. Support obtained from these projects was the backbone of my book-writing project. I thank these agencies for their support. I am thankful to the administration of JIIT, Noida for granting me the sabbatical to complete the book. I am also thankful to IMSc, Chennai for offering me the associateship. I especially mentioned this because Ms. Aastha Sharma of CRC Press approached me with their proposal to write a textbook during my stay in IMSc. I had a half-written manuscript that had been gathering dust for a long time. This coincidence revived the project.

I am indebted to many more people for their indirect support to this book. I especially acknowledge the support and help of Mrs. Chandana Pathak, Mr. S. R. Chaudhuri, Ms. Dipti Ray, Mr. Kunal Jha, Mr. Sanjit Pathak, Mrs. Anindita Pathak, Dr. Gautam Sarkar, Dr. Y. Medury, Prof. K. C. Mathur, Prof. D. K. Rai, Prof. S. K. Kak, Prof. Swapan Mandal, Prof. P. K. Panigrahi, Prof. M. R. B. Wahiddin, Prof. Barry Sanders, Prof. Marco Genovese, Prof. J. Banerjee, Prof. Adam Miranowicz, Dr. Chiranjib Sur, Dr. Amit Verma, Dr. Biswajit Sen, Dr. B. P. Chamola, Dr. Somshubhro Bandyopadhyay, Mr. Aayush Bhandari, and Mr. Rishabh Jain.

Lastly many thanks to Ms. Aastha Sharma, Ms. Amy Rodriguez and their colleagues at CRC Press for their initiative to publish this book.

Olomouc, Czech Republic Anirban Pathak
December 15, 2012

Author

Anirban Pathak is a theoretical physicist. He is a professor at Jaypee Institute of Information Technology (JIIT), Noida, India and a visiting scientist at Palacky University, Czech Republic. He received his Ph.D. from Visva Bharati, Santiniketan, India. Subsequently, he was a post-doctoral fellow at Freie University, Berlin. He joined JIIT in 2002. At present he is actively involved in teaching and research related to several aspects of quantum optics and quantum information. His group's recent research activities are focused on foundational aspects of quantum mechanics, secure quantum communication, quantum circuits and nonclassical states. His group has active research collaborations with several research groups in India, Czech Republic, Poland, Malaysia, Germany and Argentina.

Contents

Chapter 1

Introduction and overview

Once upon a time there was a curious man. He knew nothing about the subject called "Information Technology." One day he visited a library and suddenly saw a book entitled "*Information Technology: The Art of Managing Information*." First, he thought: "This title is not for me. Let me ignore it and look at the next title." But then the curious man started thinking: "What is it? What is information technology? What is information? Why do I need to know how to manage it?" Since a curious man lives in all of us, it would be tempting to follow the sequence of his thoughts and try to answer these questions. Let us start with a simple question: What is information technology? This question is very important as far as this book or any other text related to information theory is concerned. The simplest answer to this question is already provided in the title of that book as: Information technology is the art of managing information. As soon as we accept this particular definition, the other two questions that appeared in his mind become extremely relevant. In this chapter, we will try to answer those two questions and develop a quantitative perception of classical and quantum information. Once a basic perception is built in the first part of this chapter, we will describe a short history of quantum computation and quantum communication at the end of this chapter.

1.1 What is information?

To a large extent, our general perception of information is qualitative. For example, often after a lecture we say, "this talk was quite informative" or "there was not much new information in this talk." This type of qualitative perception of information has been in existence from the beginning of human civilization, but a clear definition of information was not present until 1948. To begin with, we may define information as: *Information is something that we do not already know* [1]. Some simple examples may help us to develop a perception about the meaning of this simple notion of information. Suppose you are watching a football (soccer) match with your friends and you have seen that Ronaldo has scored a goal. Immediately after that, one of your friends shouts: "Oh it's a goal!" Here, when you see Ronaldo score, you gain some information, but you don't gain any information from your friend's shout because you already know that. So your friend's shout only provides some data to you, but no information. Thus *information is useful data for a particular analysis or decision task.* It helps us to choose reliably between alternatives. Let us give another example. "Sholay" is a popular Hindi movie. In this movie there are two characters called Veeru and Jai. In the movie Jai often tosses a coin, which has the same symbol on both the sides. Jai knows it, but Veeru does not know. Now whatever the call of Veeru, Jai never gains any information from the outcome of the toss since he already knows the result.

There are many technical definitions of information, but here we have opted for a simple definition which states that information is what we do not already know. However, with just a good definition we cannot compare the amount of information. Suppose I want to compare the capacity of your pendrive with that of mine, then the above definition of information will not help us to do the comparison. However, I can conclude that my pendrive is better than your pendrive if my pendrive can store 50 units of information, but your pendrive can store only 30 units of information. To do so, we need a quantitative measure of information. Claude Shannon introduced such a measure of information in 1948 [2]. The existence of a quantitative measure of information implies that information is a quantity and that leads to a fundamental question: Is information a physical quantity? If yes, then we may be able to construct some new physical laws for information and existing laws of the physical world must be applicable to information, too. Further, since the physical world is quantum mechanical the essential nature of information should be quantum mechanical. Thus before we start talking about quantum information, we need to establish that the information is physical.

1.1.1 Is information physical?

Different views about the nature of information have co-existed for centuries. One of those views is that information is not an abstract entity and it is always tied to a physical representation. This particular view was strongly established by Rolf Landauer in the later part of the last century [3]. Landauer argued that since information is always tied to a physical representation the limitations and possibilities of the real physical world would be applicable to information, too. We can obtain a stronger perception of this particular notion of information if we try to understand how information is really stored, transferred or processed in the real world. For example, consider a situation in which we are in an auditorium and I am delivering a lecture to convince you that information is physical. In this situation, how do you obtain information from me? The words spoken by me are conveyed by air pressure fluctuations which vibrate the membranes of your ears; nerves convert mechanical energy into electrical energy and finally the brain receives an electrical signal and you listen. So a physical process is involved in the communication of information. Similarly, writing on a piece of paper is essentially painting molecules of the paper in a certain meaningful fashion; in a magnetic hard disk we arrange magnetic dipoles in a certain meaningful fashion to store information. In brief, we cannot dissociate information from physical objects and consequently, information is not abstract and laws of physics are applicable to information. This fact that information is physical has a deeper meaning. It intrinsically implies that computer science is part of physics.

Since we need physical means to store, process and communicate information, the physical laws applicable to the physical resources used for the purpose of information processing, storage or communication would be applicable to information, too. A nice example is the following version of Einstein's postulate of the special theory of relativity: We cannot communicate information with velocity greater than that of light in vacuum. We know many things about the essential nature of physical observables. Let us list a few of them as examples and check whether these specific characteristics of physical observables are also observed in information or not.

- **Physical observable can be expressed in various ways without losing its essential nature:** For example, a cricket ball delivered by Kapil Dev and the sound coming out of a drum beaten by one of his excited fans can have the same energy. The same is true for information as it can also be expressed in various ways. For example, the following two statements: "I don't know where Malda is" and "I am completely unaware of the location of Malda" have something in common, although they share only one word in common. Loosely speaking the thing they have in common is their information content [4]. Essentially, the same information can be expressed in various ways, for example, you may substitute numbers for letters in a scheme such as a=1; b=2; c=3 and so on. The fact that information can be expressed in various ways without losing its essential nature is very useful in computation. This is so because it allows automatic manipulation of information. To be precise, it allows us to construct computing machines, which can process information by handling binary digits only [4].

- **Physical quantities can be transformed from one form to another:** For example, electrical energy can be converted to kinetic energy. The same is true for information because information is not sensitive to exactly how it is expressed and it can be easily trans-