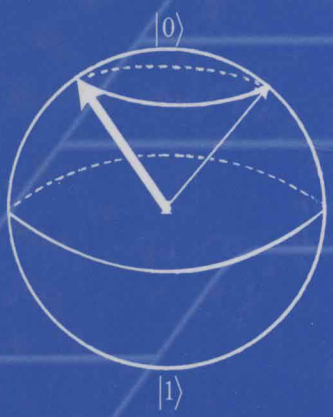
QUANTUM COMPUTING FOR COMPUTER SCIENTISTS



Noson S. Yanofsky
Mirco A. Mannucci

QUANTUM COMPUTING FOR COMPUTER SCIENTISTS

Noson S. Yanofsky
Brooklyn College, City University of New York

and

Mirco A. Mannucci
HoloMathics, LLC

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo, Delhi

Cambridge University Press
32 Avenue of the Americas, New York, NY 10013-2473, USA

www.cambridge.org
Information on this title: www.cambridge.org/9780521879965

First published 2008

Printed in the United States of America

A catalog record for this publication is available from the British Library.

Library of Congress Cataloging in Publication data

Yanofsky, Noson S., 1967–
Quantum computing for computer scientists / Noson S. Yanofsky and
Mirco A. Mannucci.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-521-87996-5 (hardback)
1. Quantum computers. I. Mannucci, Mirco A., 1960– II. Title.

QA76.889.Y35 2008
004.1–dc22 2008020507

ISBN 978-0-521-879965 hardback

Quantum Computing for Computer Scientists

The multidisciplinary field of quantum computing strives to exploit some of the uncanny aspects of quantum mechanics to expand our computational horizons. *Quantum Computing for Computer Scientists* takes readers on a tour of this fascinating area of cutting-edge research. Written in an accessible yet rigorous fashion, this book employs ideas and techniques familiar to every student of computer science. The reader is not expected to have any advanced mathematics or physics background. After presenting the necessary prerequisites, the material is organized to look at different aspects of quantum computing from the specific standpoint of computer science. There are chapters on computer architecture, algorithms, programming languages, theoretical computer science, cryptography, information theory, and hardware. The text has step-by-step examples, more than two hundred exercises with solutions, and programming drills that bring the ideas of quantum computing alive for today's computer science students and researchers.

Noson S. Yanofsky, PhD, is an Associate Professor in the Department of Computer and Information Science at Brooklyn College, City University of New York and at the PhD Program in Computer Science at The Graduate Center of CUNY.

Mirco A. Mannucci, PhD, is the founder and CEO of HoloMathics, LLC, a research and development company with a focus on innovative mathematical modeling. He also serves as Adjunct Professor of Computer Science at George Mason University and the University of Maryland.

Dedicated to
Moishe and Sharon Yanofsky
and
to the memory of
Luigi and Antonietta Mannucci

Wisdom is one thing: to know the thought by which
all things are directed through all things.

ἓν τὸ σοφόν, ἐπίστασθαι γνώμην,
ὅκη κυβερνᾶται πάντα διὰ πάντων.

Heraclitus of Ephesus (535–475 BCE)
as quoted in Diogenes Laertius's
Lives and Opinions of Eminent Philosophers
Book IX, 1.

Preface

Quantum computing is a fascinating new field at the intersection of computer science, mathematics, and physics, which strives to harness some of the uncanny aspects of quantum mechanics to broaden our computational horizons. This book presents some of the most exciting and interesting topics in quantum computing. Along the way, there will be some amazing facts about the universe in which we live and about the very notions of information and computation.

The text you hold in your hands has a distinct flavor from most of the other currently available books on quantum computing. First and foremost, we do not assume that our reader has much of a mathematics or physics background. This book should be readable by anyone who is in or beyond their second year in a computer science program. We have written this book specifically with computer scientists in mind, and tailored it accordingly: we assume a bare minimum of mathematical sophistication, a first course in discrete structures, and a healthy level of curiosity. Because this text was written specifically for computer people, in addition to the many exercises throughout the text, we added many programming drills. These are a hands-on, fun way of learning the material presented and getting a real feel for the subject.

The calculus-phobic reader will be happy to learn that derivatives and integrals are virtually absent from our text. Quite simply, we avoid differentiation, integration, and all higher mathematics by carefully selecting only those topics that are critical to a basic introduction to quantum computing. Because we are focusing on the fundamentals of quantum computing, we can restrict ourselves to the finite-dimensional mathematics that is required. This turns out to be not much more than manipulating vectors and matrices with complex entries. Surprisingly enough, the lion's share of quantum computing can be done without the intricacies of advanced mathematics.

Nevertheless, we hasten to stress that this is a technical textbook. We are not writing a popular science book, nor do we substitute hand waving for rigor or mathematical precision.

Most other texts in the field present a primer on quantum mechanics in all its glory. Many assume some knowledge of classical mechanics. We do not make these assumptions. We only discuss what is needed for a basic understanding of quantum

computing *as a field of research in its own right,* although we cite sources for learning more about advanced topics.

There are some who consider quantum computing to be solely within the domain of physics. Others think of the subject as purely mathematical. We stress the computer science aspect of quantum computing.

It is not our intention for this book to be the definitive treatment of quantum computing. There are a few topics that we do not even touch, and there are several others that we approach briefly, not exhaustively. As of this writing, the bible of quantum computing is Nielsen and Chuang's magnificent *Quantum Computing and Quantum Information* (2000). Their book contains almost everything known about quantum computing at the time of its publication. We would like to think of our book as a useful first step that can prepare the reader for that text.

FEATURES

This book is almost entirely self-contained. We do not demand that the reader come armed with a large toolbox of skills. Even the subject of complex numbers, which is taught in high school, is given a fairly comprehensive review.

The book contains many solved problems and easy-to-understand descriptions. We do not merely present the theory; rather, we explain it and go through several examples. The book also contains many exercises, which we strongly recommend the serious reader should attempt to solve. There is no substitute for rolling up one's sleeves and doing some work!

We have also incorporated plenty of programming drills throughout our text. These are hands-on exercises that can be carried out on your laptop to gain a better understanding of the concepts presented here (they are also a great way of having fun). We hasten to point out that we are entirely language-agnostic. The student should write the programs in the language that feels most comfortable. We are also paradigm-agnostic. If declarative programming is your favorite method, go for it. If object-oriented programming is your game, use that. The programming drills build on one another. Functions created in one programming drill will be used and modified in later drills. Furthermore, in Appendix C, we show how to make little quantum computing emulators with MATLAB or how to use a ready-made one. (Our choice of MATLAB was dictated by the fact that it makes very easy-to-build, quick-and-dirty prototypes, thanks to its vast amount of built-in mathematical tools.)

This text appears to be the first to handle quantum programming languages in a significant way. Until now, there have been only research papers and a few surveys on the topic. Chapter 7 describes the basics of this expanding field: perhaps some of our readers will be inspired to contribute to quantum programming!

This book also contains several appendices that are important for further study:

- Appendix A takes readers on a tour of major papers in quantum computing. This bibliographical essay was written by Jill Cirasella, Computational Sciences Specialist at the Brooklyn College Library. In addition to having a master's degree in library and information science, Jill has a master's degree in logic, for which she wrote a thesis on classical and quantum graph algorithms. This dual background uniquely qualifies her to suggest and describe further readings.

- Appendix B contains the answers to some of the exercises in the text. Other solutions will also be found on the book's Web page. We strongly urge students to do the exercises on their own and then check their answers against ours.
- Appendix C uses MATLAB, the popular mathematical environment and an established industry standard, to show how to carry out most of the mathematical operations described in this book. MATLAB has scores of routines for manipulating complex matrices: we briefly review the most useful ones and show how the reader can quickly perform a few quantum computing experiments with almost no effort, using the freely available MATLAB quantum emulator Quack.
- Appendix D, also by Jill Cirasella, describes how to use online resources to keep up with developments in quantum computing. Quantum computing is a fast-moving field, and this appendix offers guidelines and tips for finding relevant articles and announcements.
- Appendix E is a list of possible topics for student presentations. We give brief descriptions of different topics that a student might present before a class of his peers. We also provide some hints about where to start looking for materials to present.

ORGANIZATION

The book begins with two chapters of mathematical preliminaries. Chapter 1 contains the basics of complex numbers, and Chapter 2 deals with complex vector spaces. Although much of Chapter 1 is currently taught in high school, we feel that a review is in order. Much of Chapter 2 will be known by students who have had a course in linear algebra. We deliberately did not relegate these chapters to an appendix at the end of the book because the mathematics is necessary to understand what is really going on. A reader who knows the material can safely skip the first two chapters. She might want to skim over these chapters and then return to them as a reference, using the index and the table of contents to find specific topics.

Chapter 3 is a gentle introduction to some of the ideas that will be encountered throughout the rest of the text. Using simple models and simple matrix multiplication, we demonstrate some of the fundamental concepts of quantum mechanics, which are then formally developed in Chapter 4. From there, Chapter 5 presents some of the basic architecture of quantum computing. Here one will find the notions of a qubit (a quantum generalization of a bit) and the quantum analog of logic gates.

Once Chapter 5 is understood, readers can safely proceed to their choice of Chapters 6 through 11. Each chapter takes its title from a typical course offered in a computer science department. The chapters look at that subfield of quantum computing from the perspective of the given course. These chapters are almost totally independent of one another. We urge the readers to study the particular chapter that corresponds to their favorite course. Learn topics that you like first. From there proceed to other chapters.

Figure 0.1 summarizes the dependencies of the chapters.

One of the hardest topics tackled in this text is that of considering two quantum systems and combining them, or "entangled" quantum systems. This is done mathematically in Section 2.7. It is further motivated in Section 3.4 and formally presented in Section 4.5. The reader might want to look at these sections together.

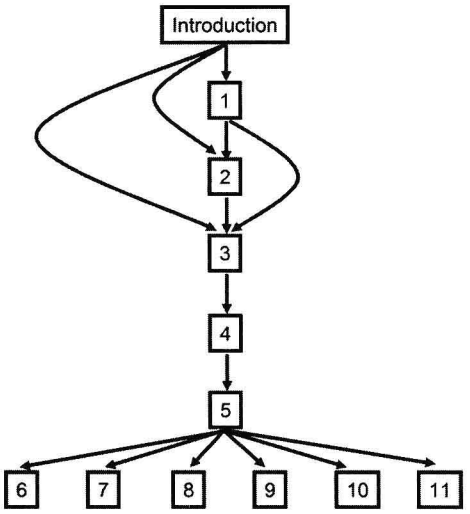


Figure 0.1. Chapter dependencies.

There are many ways this book can be used as a text for a course. We urge instructors to find their own way. May we humbly suggest the following three plans of action:

(1) A class that provides some depth might involve the following: Go through Chapters 1, 2, 3, 4, and 5. Armed with that background, study the entirety of Chapter 6 ("Algorithms") in depth. One can spend at least a third of a semester on that chapter. After wrestling a bit with quantum algorithms, the student will get a good feel for the entire enterprise.

(2) If breadth is preferred, pick and choose one or two sections from each of the advanced chapters. Such a course might look like this: (1), 2, 3, 4.1, 4.4, 5, 6.1, 7.1, 9.1, 10.1, 10.2, and 11. This will permit the student to see the broad outline of quantum computing and then pursue his or her own path.

(3) For a more advanced class (a class in which linear algebra and some mathematical sophistication is assumed), we recommend that students be told to read Chapters 1, 2, and 3 on their own. A nice course can then commence with Chapter 4 and plow through most of the remainder of the book.

If this is being used as a text in a classroom setting, we strongly recommend that the students make presentations. There are selected topics mentioned in Appendix E. There is no substitute for student participation!

Although we have tried to include many topics in this text, inevitably some others had to be left out. Here are a few that we omitted because of space considerations:

- many of the more complicated proofs in Chapter 8,
- results about oracle computation,
- the details of the (quantum) Fourier transforms, and
- the latest hardware implementations.

We give references for further study on these, as well as other subjects, throughout the text.

ANCILLARIES

We are going to maintain a Web page for the text at

www.sci.brooklyn.cuny.edu/~noson/qctext.html/

The Web page will contain

- periodic updates to the book,
- links to interesting books and articles on quantum computing,
- some answers to certain exercises not solved in Appendix B, and
- errata.

The reader is encouraged to send any and all corrections to

noson@sci.brooklyn.cuny.edu

Help us make this textbook better!

ACKNOLWEDGMENTS

Both of us had the great privilege of writing our doctoral theses under the gentle guidance of the recently deceased Alex Heller. Professor Heller wrote the following[1] about his teacher Samuel "Sammy" Eilenberg and Sammy's mathematics:

> As I perceived it, then, Sammy considered that the highest value in mathematics was to be found, not in specious depth nor in the overcoming of overwhelming difficulty, but rather in providing the definitive clarity that would illuminate its underlying order.

This never-ending struggle to bring out the underlying order of mathematical structures was always Professor Heller's everlasting goal, and he did his best to pass it on to his students. We have gained greatly from his clarity of vision and his view of mathematics, but we also saw, embodied in a man, the classical and sober ideal of contemplative life at its very best. We both remain eternally grateful to him.

While at the City University of New York, we also had the privilege of interacting with one of the world's foremost logicians, Professor Rohit Parikh, a man whose seminal contributions to the field are only matched by his enduring commitment to promote younger researchers' work. Besides opening fascinating vistas to us, Professor Parikh encouraged us more than once to follow new directions of thought. His continued professional and personal guidance are greatly appreciated.

We both received our Ph.D.'s from the Department of Mathematics in The Graduate Center of the City University of New York. We thank them for providing us with a warm and friendly environment in which to study and learn real mathematics. The first author also thanks the entire Brooklyn College family and, in particular, the Computer and Information Science Department for being supportive and very helpful in this endeavor.

[1] See page 1349 of Bass et al. (1998).

Several faculty members of Brooklyn College and The Graduate Center were kind enough to read and comment on parts of this book: Michael Anshel, David Arnow, Jill Cirasella, Dayton Clark, Eva Cogan, Jim Cox, Scott Dexter, Edgar Feldman, Fred Gardiner, Murray Gross, Chaya Gurwitz, Keith Harrow, Jun Hu, Yedidyah Langsam, Peter Lesser, Philipp Rothmaler, Chris Steinsvold, Alex Sverdlov, Aaron Tenenbaum, Micha Tomkiewicz, Al Vasquez, Gerald Weiss, and Paula Whitlock. Their comments have made this a better text. Thank you all!

We were fortunate to have had many students of Brooklyn College and The Graduate Center read and comment on earlier drafts: Shira Abraham, Rachel Adler, Ali Assarpour, Aleksander Barkan, Sayeef Bazli, Cheuk Man Chan, Wei Chen, Evgenia Dandurova, Phillip Dreizen, C. S. Fahie, Miriam Gutherc, Rave Harpaz, David Herzog, Alex Hoffnung, Matthew P. Johnson, Joel Kammet, Serdar Kara, Karen Kletter, Janusz Kusyk, Tiziana Ligorio, Matt Meyer, James Ng, Severin Ngnosse, Eric Pacuit, Jason Schanker, Roman Shenderovsky, Aleksandr Shnayderman, Rose B. Sigler, Shai Silver, Justin Stallard, Justin Tojeira, John Ma Sang Tsang, Sadia Zahoor, Mark Zelcer, and Xiaowen Zhang. We are indebted to them.

Many other people looked over parts or all of the text: Scott Aaronson, Stefano Bettelli, Adam Brandenburger, Juan B. Climent, Anita Colvard, Leon Ehrenpreis, Michael Greenebaum, Miriam Klein, Eli Kravits, Raphael Magarik, John Maiorana, Domenico Napoletani, Vaughan Pratt, Suri Raber, Peter Selinger, Evan Siegel, Thomas Tradler, and Jennifer Whitehead. Their criticism and helpful ideas are deeply appreciated.

Thanks to Peter Rohde for creating and making available to everyone his MATLAB q-emulator Quack and also for letting us use it in our appendix. We had a good deal of fun playing with it, and we hope our readers will too.

Besides writing two wonderful appendices, our friendly neighborhood librarian, Jill Cirasella, was always just an e-mail away with helpful advice and support. Thanks, Jill!

A very special thanks goes to our editor at Cambridge University Press, Heather Bergman, for believing in our project right from the start, for guiding us through this book, and for providing endless support in all matters. This book would not exist without her. Thanks, Heather!

We had the good fortune to have a truly stellar editor check much of the text many times. Karen Kletter is a great friend and did a magnificent job. We also appreciate that she refrained from killing us every time we handed her altered drafts that she had previously edited.

But, of course, all errors are our own!

This book could not have been written without the help of my daughter, Hadassah. She added meaning, purpose, and joy.

N.S.Y.

My dear wife, Rose, and our two wondrous and tireless cats, Ursula and Buster, contributed in no small measure to melting my stress away during the long and painful hours of writing and editing: to them my gratitude and love. (Ursula is a scientist cat and will read this book. Buster will just shred it with his powerful claws.)

M.A.M.

Contents

Introduction

THE FEATURES OF THE QUANTUM WORLD

In order to learn quantum computing, it is first necessary to become familiar with some basic facts about the quantum world. In this introduction, some unique features of quantum mechanics are introduced, as well as the way they influence the tale we are about to tell.[2]

From Real Numbers to Complex Numbers

Quantum mechanics is different from most other branches of science in that it uses complex numbers in a fundamental way. Complex numbers were originally created as a mathematical curiosity: $i = \sqrt{-1}$ was the asserted "imaginary" solution to the polynomial equation $x^2 = -1$. As time went on, an entire mathematical edifice was constructed with these "imaginary" numbers. Complex numbers have kept lonely mathematicians busy for centuries, while physicists successfully ignored these abstract creations. However, things changed with the systematic study of wave mechanics. After the introduction of Fourier analysis, researchers learned that a compact way to represent a wave was by using functions of complex numbers. As it turns out, this was an important step on the road to using complex numbers in quantum theory. Early quantum mechanics was largely based on wave mechanics.

At first glance, we do not seem to experience complex numbers in the "real world." The length of a rod is a real number, not a complex number. The temperature outside today is 73°, not $(32 - 14i)°$. The amount of time a chemical process takes is 32.543 seconds, not $-14.65i$ seconds. One might wonder what possible role complex numbers can have in any discussion of the physical world. It will soon become apparent that they play an important, indeed an essential, role in quantum mechanics. We shall explore complex numbers in Chapters 1 and 2 of the text.

[2] This Introduction is not the proper place for technical details. Some of the concepts are covered in the text and some of them can be found only in quantum mechanics textbooks. See the end of Chapter 4 for some recommendations of easy, yet detailed, introductions to quantum physics.

From Single States to Superpositions of States

In order to survive in this world, human beings, as infants, must learn that every object exists in a unique place and in a well-defined state, even when we are not looking at it. Although this is true for large objects, quantum mechanics tells us that it is false for objects that are very small. A microscopic object can "hazily" be in more than one place at one time. Rather than an object's being in one position or another, we say that it is in a "superposition," i.e., in some sense, it is simultaneously in more than one location at the same time. Not only is spatial position subject to such "haziness" but so are other familiar physical properties, like energy, momentum, and certain properties that are unique to the quantum world, such as "spin."

We do not actually see superposition of states. Every time we look, or more properly, "measure," a superposition of states, it "collapses" to a single well-defined state. Nevertheless, before we measure it, it is in many states at the same time.

One is justified in greeting these claims with skepticism. After all, how can one believe something different from what every infant knows? However, we will describe certain experiments that show that this is exactly what happens.

From Locality to Nonlocality

Central to modern science is the notion that objects are directly affected only by nearby objects or forces. In order to determine why a phenomenon occurs at a certain place, one must examine all the phenomena and forces near[3] that place. This is called "locality," i.e., the laws of physics work in a local way. One of the most remarkable aspects of quantum mechanics is that its laws predict certain effects that work in a nonlocal manner. Two particles can be connected or "entangled" in such a way that an action performed on one of them can have an immediate effect on the other particle light-years away. This "spooky action at a distance," to use Einstein's colorful expression, was one of the most shocking discoveries of quantum mechanics.

From Deterministic Laws to Probabilistic Laws

To which specific state will a superposition of states collapse when it is measured? Whereas in other branches of physics the laws are deterministic,[4] i.e., there is a unique outcome to every experiment, the laws of quantum mechanics state that we can only know the probability of the outcome. This, again, might seem dubious. It was doubted by the leading researchers of the time. Einstein himself was skeptical and coined the colorful expression "God does not play dice with the Universe" to express this. However, because of repeated experimental confirmations, the probabilistic nature of quantum mechanics is no longer in question.

[3] By "near" we mean anything close enough to affect the object. In physics jargon, anything in the past light cone of the object.

[4] Statistical mechanics being one major exception.