Graduate Texts in Physics

For further volumes:
http://www.springer.com/series/8431

Graduate Texts in Physics

Graduate Texts in Physics publishes core learning/teaching material for graduate- and advanced-level undergraduate courses on topics of current and emerging fields within physics, both pure and applied. These textbooks serve students at the MS- or PhD-level and their instructors as comprehensive sources of principles, definitions, derivations, experiments and applications (as relevant) for their mastery and teaching, respectively. International in scope and relevance, the textbooks correspond to course syllabi sufficiently to serve as required reading. Their didactic style, comprehensiveness and coverage of fundamental material also make them suitable as introductions or references for scientists entering, or requiring timely knowledge of, a research field.

János A. Bergou • Mark Hillery

Introduction to the Theory of Quantum Information Processing

Springer

János A. Bergou
Department of Physics and Astronomy
Hunter College
City University of New York
New York, NY, USA

Mark Hillery
Department of Physics and Astronomy
Hunter College
City University of New York
New York, NY, USA

ISSN 1868-4513 ISSN 1868-4521 (electronic)
ISBN 978-1-4614-7091-5 ISBN 978-1-4614-7092-2 (eBook)
DOI 10.1007/978-1-4614-7092-2
Springer New York Heidelberg Dordrecht London

Library of Congress Control Number: 2013934474

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

To Valéria, Attila, Miklós and Katalin
JB

To Carol
MH

Preface

These notes are the result of a one-semester graduate course that was first taught during the Spring 2003 Semester at the CUNY Graduate Center and has been offered several times since. The students in the courses were all physicists, so a familiarity with quantum mechanics at the first-year graduate level was assumed. The hope was that after taking the course, students could explore the original literature in the subject on their own.

The course covers a range of topics in quantum information but, given the limited amount of time, is not by any means exhaustive. We begin with the density matrix and its representations. Next we study entanglement, starting with Bell's inequalities and continuing with tests for entanglement, in particular, the Peres partial transposition test. It is also possible to quantify entanglement, and we show how this can be done for both pure and mixed states, finishing with a discussion of concurrence as a measure of entanglement for states of two qubits. Entanglement is a resource that can be used for quantum communication. Teleportation and dense coding are examples of this. Next, we consider quantum dynamics. In particular, we study generalized quantum dynamics that generalize the standard unitary evolution of quantum states. The Kraus representation of quantum maps is derived and applied to examples, such as the depolarizing channel. There are also certain kinds of maps that are impossible, such as the cloning map, a map that produces a perfect copy of an arbitrary input state.

We then move on to the study of quantum measurements. Just as quantum maps generalize the standard unitary evolution, positive operator valued measures (POVMs) generalize the standard projective measurements. Here we develop an extensive theory of generalized measurements that are described by POVMs. The problem of discriminating between two nonorthogonal quantum states provides a useful illustration of this type of measurement, and the two commonly employed strategies, the minimum-error strategy and the unambiguous state discrimination strategy, are discussed. These POVMs lead to a discussion of quantum cryptography. In particular, the B92 proposal and the original BB84 proposal are studied from this perspective. Many of the fascinating applications of quantum information theory in the area of quantum communication, such as secret sharing, rely on the impossibility of certain maps.

In quantum computation, the other major area of quantum information processing, consequences of the superposition principle are exploited. In the area of quantum algorithms, we focus primarily on the Deutsch–Jozsa algorithm, the Bernstein–Vazirani algorithm, the Grover search algorithm, and period finding. We also explore a technique that has been useful in finding new algorithms, the quantum walk. In a real quantum computation it is necessary to protect against errors, and for this quantum error-detecting codes are necessary. We develop the general theory of such codes and discuss some examples such as the Shor code and CSS codes.

We also have a chapter on quantum machines, devices that perform certain operations on quantum systems. These may be single purpose or programmable, and we discuss the limits on programmable machines. We conclude with an example of a programmable state discriminator, in which the states to be discriminated are provided as a program rather than hardwired into the machine.

This covers a lot of material, but it also leaves out a lot. In a single semester we cannot touch on subjects such as the applications of information theory to quantum information or the physical implementations of quantum information protocols, both of which are important subjects. We also do not treat the Shor algorithm for finding the prime factors of a number, not because it is not important but because it requires some background in number theory. When teaching a one-semester course, time constraints are a very real consideration, and we felt that an adequate presentation of the Shor algorithm and its background would take too much time. Our choice of subjects has been guided by the requirement of providing a firm foundation for further study and by our own interests as we have explored the field.

The chapters are completed with problems and a cursory list of the most relevant literature. The references are not meant to be exhaustive but to serve as a guide to further reading.

We should also mention two standard sources that we found useful in preparing the notes from which this book originated. One is *Quantum Computation and Quantum Information* by Michael Nielsen and Isaac Chuang. The second is the set of lecture notes by John Preskill for Physics 219 at Caltech, which can be found at http://www.theory.caltech.edu/people/preskill/ph229/. These cover some of the topics we discuss in more depth and also treat many topics that we do not. A more recent book, which can also supplement what we present here, is *Quantum Information* by Stephen Barnett.

Over the years, we benefitted from numerous discussions and close collaborations with many colleagues and friends. Among them we want to particularly thank Erika Andersson, Emilio Bagan, Stephen Barnett, Sam Braunstein, Vladimir Bužek, Luiz Davidovich, Berge Englert, Edgar Feldman, Ulrike Herzog, Igor Jex, Miguel Orszag, Daniel Reitzner, Wolfgang Schleich, Aephraim Steinberg, Mario Ziman, and M. Suhail Zubairy.

Finally, we are most grateful for the love and support of our families to whom this book is dedicated.

New York, NY, USA — János A. Bergou
New York, NY, USA — Mark Hillery

Contents