

# 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.

## *Series Editors*

Professor William T. Rhodes  
Department of Computer and Electrical Engineering and Computer Science  
Imaging Science and Technology Center  
Florida Atlantic University  
777 Glades Road SE, Room 456  
Boca Raton, FL 33431  
USA  
[wrhodes@fau.edu](mailto:wrhodes@fau.edu)

Professor H. Eugene Stanley  
Center for Polymer Studies Department of Physics  
Boston University  
590 Commonwealth Avenue, Room 204B  
Boston, MA 02215  
USA  
[hes@bu.edu](mailto:hes@bu.edu)

Professor Richard Needs  
Cavendish Laboratory  
JJ Thomson Avenue  
Cambridge CB3 0HE  
UK  
[rn11@cam.ac.uk](mailto:rn11@cam.ac.uk)

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

© Springer Science+Business Media New York 2013

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer is part of Springer Science+Business Media ([www.springer.com](http://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  
New York, NY, USA

János A. Bergou  
Mark Hillery



# Contents

<b>1</b>	<b>Introduction</b> .....	1
1.1	The Qubit .....	1
1.2	Quantum Gates .....	3
1.3	Quantum Circuits .....	4
1.4	The Deutsch Algorithm .....	5
1.5	Problems .....	7
	References .....	8
<b>2</b>	<b>The Density Matrix</b> .....	9
2.1	Ensembles and Subsystems .....	9
2.2	Properties .....	11
2.3	Pure States and Mixed States of a Qubit .....	12
2.4	Pure State Decompositions and the Ensemble Interpretation .....	14
2.5	A Mathematical Aside: The Schmidt Decomposition of a Bipartite State .....	17
2.6	Purification, Reduced Density Matrices, and the Subsystem Interpretation .....	19
2.7	Problems .....	19
	References .....	21
<b>3</b>	<b>Entanglement</b> .....	23
3.1	Definition of Entanglement .....	23
3.2	Bell Inequalities .....	24
3.3	Representative Applications of Entanglement: Dense Coding and Teleportation .....	27
	3.3.1 Dense Coding .....	27
	3.3.2 Teleportation .....	27
3.4	Conditions of Separability .....	28
3.5	Entanglement Distillation and Formation .....	33
	3.5.1 Local Operations and Classical Communication [LOCC] .....	33
	3.5.2 Entanglement Distillation: Procrustean Method .....	34
	3.5.3 Entanglement Formation .....	34

3.6	Entanglement Measures .....	35
3.6.1	The von Neumann Entropy as an Entanglement Measure for Pure Bipartite States: A First Set of Properties..	35
3.6.2	A Useful Auxiliary Quantity: Relative Entropy and Klein's Inequality .....	36
3.6.3	The von Neumann Entropy: A Second Set of Properties .....	37
3.6.4	The Effect of Local Measurements on Entanglement .....	39
3.6.5	Towards the Entanglement of Mixed States .....	40
3.6.6	The Effect of Throwing Away Part of the System Locally on Entanglement .....	40
3.6.7	Bound Entanglement .....	41
3.7	Concurrence .....	42
3.8	Problems .....	44
	References .....	47
<b>4</b>	<b>Generalized Quantum Dynamics</b> .....	<b>49</b>
4.1	Quantum Maps or Superoperators .....	49
4.1.1	Quantum Maps and Their Kraus Representation .....	49
4.1.2	Properties of Quantum Maps .....	50
4.1.3	Properties of the Kraus Operators .....	53
4.2	An Example: The Depolarizing Channel .....	54
4.3	Impossible Maps .....	55
4.3.1	The Cloning Map and the No-Cloning Theorem .....	55
4.3.2	Faster than Light Communication .....	56
4.4	Problems .....	56
	References .....	58
<b>5</b>	<b>Quantum Measurement Theory</b> .....	<b>59</b>
5.1	Outline .....	59
5.2	Standard Quantum Measurements .....	59
5.3	Positive Operator Valued Measures .....	63
5.4	Neumark's Theorem and the Implementation of a POVM Via Generalized Measurements .....	66
5.5	Examples: Strategies for State Discrimination .....	70
5.5.1	Unambiguous Discrimination of Two Pure States .....	71
5.5.2	Minimum-Error Discrimination of Two Quantum States .....	75
5.6	Problems .....	79
	References .....	81
<b>6</b>	<b>Quantum Cryptography</b> .....	<b>83</b>
6.1	Outline .....	83
6.2	The One-Time Pad .....	84
6.3	The B92 Quantum Key Distribution Protocol .....	85
6.4	The BB 84 Protocol .....	86
6.5	The E91 Protocol .....	88
6.6	Quantum Secret Sharing .....	89

- 6.7 Problems ..... 90
- References ..... 91
- 7 Quantum Algorithms** ..... 93
  - 7.1 The Deutsch–Jozsa Algorithm ..... 93
  - 7.2 The Bernstein–Vazirani Algorithm ..... 95
  - 7.3 Quantum Search: The Grover Algorithm ..... 96
  - 7.4 Period Finding: Simon’s Algorithm ..... 101
  - 7.5 Quantum Fourier Transform and Phase Estimation ..... 102
  - 7.6 Quantum Walks ..... 105
  - 7.7 Problems ..... 115
  - References ..... 115
- 8 Quantum Machines** ..... 117
  - 8.1 Introduction ..... 117
  - 8.2 Cloners and U-NOT Gates ..... 117
  - 8.3 Programmable Machines: A General Result ..... 120
  - 8.4 Probabilistic Processors ..... 123
  - 8.5 A Programmable State Discriminator ..... 125
  - 8.6 Problems ..... 129
  - References ..... 130
- 9 Decoherence and Quantum Error Correction** ..... 133
  - 9.1 General Theory of Quantum Error-Correcting Codes ..... 133
  - 9.2 An Example: CSS Codes ..... 141
  - 9.3 Decoherence-Free Subspaces ..... 146
  - 9.4 Problems ..... 148
  - References ..... 148
- Index** ..... 149