

THE THEORY OF QUANTUM INFORMATION

This largely self-contained book on the theory of quantum information focuses on precise mathematical formulations and proofs of fundamental facts that form the foundation of the subject. It is intended for graduate students and researchers in mathematics, computer science, and theoretical physics seeking to develop a thorough understanding of key results, proof techniques, and methodologies that are relevant to a wide range of research topics within the theory of quantum information and computation.

The book is accessible to readers with an understanding of basic mathematics, including linear algebra, mathematical analysis, and probability theory. An introductory chapter summarizes these necessary mathematical prerequisites, and starting from this foundation the book includes clear and complete proofs of all results it presents. Each subsequent chapter includes challenging exercises intended to help readers develop their own skills for discovering proofs concerning the theory of quantum information.

JOHN WATROUS is a Professor in the School of Computer Science and a Faculty Member of the Institute for Quantum Computing at the University of Waterloo, Canada. He is also an Affiliate Member of the Perimeter Institute for Theoretical Physics and a Senior Fellow of the Canadian Institute for Advanced Research. Quantum information and computation has been his primary research focus for over 20 years.

Cambridge University Press
978-1-107-18056-7 – The Theory of Quantum Information
John Watrous
Frontmatter
[More Information](#)

THE THEORY OF QUANTUM INFORMATION

JOHN WATROUS
University of Waterloo, Canada



CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom
One Liberty Plaza, 20th Floor, New York, NY 10006, USA
477 Williamstown Road, Port Melbourne, VIC 3207, Australia
314–321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre, New Delhi – 110025, India
79 Anson Road, #06–04/06, Singapore 079906

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning, and research at the highest international levels of excellence.

www.cambridge.org

Information on this title: www.cambridge.org/9781107180567

DOI: 10.1017/9781316848142

© John Watrous 2018

This publication is in copyright. Subject to statutory exception and to the provisions of relevant collective licensing agreements, no reproduction of any part may take place without the written permission of Cambridge University Press.

First published 2018

Printed in the United Kingdom by Clays, St Ives plc

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

ISBN 978-1-107-18056-7 Hardback

Cambridge University Press has no responsibility for the persistence or accuracy of URLs for external or third-party internet websites referred to in this publication and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

Contents

	<i>Preface</i>	<i>page vii</i>
1	Mathematical Preliminaries	1
	1.1 Linear Algebra	1
	1.2 Analysis, Convexity, and Probability Theory	35
	1.3 Suggested References	57
2	Basic Notions of Quantum Information	58
	2.1 Registers and States	58
	2.2 Quantum Channels	72
	2.3 Measurements	100
	2.4 Exercises	120
	2.5 Bibliographic Remarks	122
3	Similarity and Distance Among States and Channels	124
	3.1 Quantum State Discrimination	124
	3.2 The Fidelity Function	139
	3.3 Channel Distances and Discrimination	164
	3.4 Exercises	197
	3.5 Bibliographic Remarks	198
4	Unital Channels and Majorization	201
	4.1 Subclasses of Unital Channels	201
	4.2 General Properties of Unital Channels	222
	4.3 Majorization	233
	4.4 Exercises	246
	4.5 Bibliographic Remarks	247
5	Quantum Entropy and Source Coding	250
	5.1 Classical Entropy	250
	5.2 Quantum Entropy	265

vi	<i>Contents</i>	
	5.3 Source Coding	283
	5.4 Exercises	306
	5.5 Bibliographic Remarks	308
6	Bipartite Entanglement	310
	6.1 Separability	310
	6.2 Manipulation of Entanglement	339
	6.3 Phenomena Associated With Entanglement	358
	6.4 Exercises	384
	6.5 Bibliographic Remarks	386
7	Permutation Invariance and Unitarily Invariant Measures	390
	7.1 Permutation-Invariant Vectors and Operators	390
	7.2 Unitarily Invariant Probability Measures	408
	7.3 Measure Concentration and Its Applications	429
	7.4 Exercises	460
	7.5 Bibliographic Remarks	462
8	Quantum Channel Capacities	464
	8.1 Classical Information Over Quantum Channels	464
	8.2 Quantum Information Over Quantum Channels	512
	8.3 Non-Additivity and Super-Activation	538
	8.4 Exercises	556
	8.5 Bibliographic Remarks	558
	<i>References</i>	561
	<i>Index of Symbols</i>	573
	<i>Index</i>	584

Preface

This is a book on the mathematical theory of quantum information, focusing on a formal presentation of definitions, theorems, and proofs. It is primarily intended for graduate students and researchers having some familiarity with quantum information and computation, such as would be covered in an introductory-level undergraduate or graduate course, or in one of several books on the subject that now exist.

Quantum information science has seen an explosive development in recent years, particularly within the past two decades. A comprehensive treatment of the subject, even if restricted to its theoretical aspects, would certainly require a series of books rather than just one. Consistent with this fact, the selection of topics covered herein is not intended to be fully representative of the subject. Quantum error correction and fault tolerance, quantum algorithms and complexity theory, quantum cryptography, and topological quantum computation are among the many interesting and fundamental topics found within the theoretical branches of quantum information science that are not covered in this book. Nevertheless, one is likely to encounter some of the core mathematical notions discussed in this book when studying these topics.

More broadly speaking, while the theory of quantum information is of course motivated both by quantum mechanics and by the potential utility of implementing quantum computing devices, these topics fall well outside of the scope of this book. The Schrödinger equation will not be found within these pages, and the difficult technological challenge of building quantum information processing devices is blissfully ignored. Indeed, no attention is paid in general to motives for studying the theory of quantum information; it is assumed that the reader has already been motivated to study this theory, and is perhaps interested in proving new theorems on quantum information of his or her own.

Some readers will find that this book deviates in some respects from the standard conventions of quantum information and computation, particularly with respect to notation and terminology. For example, the commonly used Dirac notation is not used in this book, and names and symbols associated with certain concepts differ from many other works. These differences are, however, fairly cosmetic, and those who have previously grown familiar with the notation and conventions of quantum information that are not followed in this book should not find it overly difficult to translate between the text and their own preferred notation and terminology.

Each chapter aside from the first includes a collection of exercises, some of which can reasonably be viewed as straightforward, and some of which are considerably more difficult. While the exercises may potentially be useful to course instructors, their true purpose is to be useful to students of the subject; there is no substitute for the learning experience to be found in wrestling with (and ideally solving) a difficult problem. In some cases the exercises represent the results of published research papers, and in those cases there has naturally been no attempt to disguise this fact or hide their sources, which may clearly reveal their solutions.

I thank Debbie Leung, Ashwin Nayak, Marco Piani, and Patrick Hayden for helpful discussions on some of the topics covered in this book. Over a number of years, this book has developed from a set of lecture notes, through a couple of drafts, to the present version, and during that time many people have brought mistakes to my attention and made other valuable suggestions, and I thank all of them. While the list of such people has grown quite long, and will not be included in this preface, I would be remiss if I did not gratefully acknowledge the efforts of Yuan Su and Maris Ozols, who provided extensive and detailed comments, corrections, and suggestions. Thanks are also due to Sascha Agne for assisting me with German translations.

The Institute for Quantum Computing and the School of Computer Science at the University of Waterloo have provided me both with the opportunity to write this book and with an environment in which it was possible, for which I am grateful. I also gratefully acknowledge financial support for my research program provided by the Natural Sciences and Engineering Research Council of Canada and the Canadian Institute for Advanced Research.

Finally, I thank Christiane, Anne, Liam, and Ethan, for reasons that have nothing to do with quantum information.