

Mark M. Wilde

Quantum Information Theory

CAMBRIDGE

Quantum Information Theory

MARK M. WILDE

McGill University, Montréal



CAMBRIDGE
UNIVERSITY PRESS

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

Cambridge University Press
The Edinburgh Building, Cambridge CB2 8RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9781107034259

© Mark M. Wilde 2013

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 2013

Printed and bound in the United Kingdom by the MPG Books Group

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

Library of Congress Cataloguing in Publication data

Wilde, Mark, 1980–

Quantum information theory / Mark Wilde, McGill University, Montréal.
pages cm.

ISBN 978-1-107-03425-9 (hardback)

1. Quantum computers. 2. Quantum communication. 3. Information theory – Data
processing. 4. Electronic data processing – Technological innovations. I. Title.

QA76.889.W544 2013

003'.54–dc23

2012047378

ISBN 978-1-107-03425-9 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.

Quantum Information Theory

Finally, here is a modern, self-contained text on quantum information theory suitable for graduate-level courses. Developing the subject “from the ground up,” it covers classical results as well as major advances of the past decade.

Beginning with an extensive overview of classical information theory suitable for the non-expert, the author then turns his attention to quantum mechanics for quantum information theory, and the important protocols of teleportation, super-dense coding, and entanglement distribution. He develops all of the tools necessary for understanding important results in quantum information theory, including capacity theorems for classical, entanglement-assisted, private, and quantum communication. The book also covers important recent developments such as superadditivity of private, coherent, and Holevo information, and the superactivation of quantum capacity.

This book will be warmly welcomed by the upcoming generation of quantum information theorists and by the already established community of classical information theorists.

MARK M. WILDE is currently a Lecturer in the School of Computer Science at McGill University, Montréal and will begin in August 2013 as an Assistant Professor with a joint appointment in the Department of Physics and Astronomy and the Center for Computation and Technology at Louisiana State University, Baton Rouge.

How To Use This Book

For Students

Prerequisites for understanding the content in this book are a solid background in probability theory and linear algebra. If you are new to information theory, then there is enough background in this book to get you up to speed (Chapters 2, 10, 12, and 13). Though, classics on information theory such as Cover and Thomas (1991) and MacKay (2003) could be helpful as a reference. If you are new to quantum mechanics, then there should be enough material in this book (Part II) to give you the background necessary for understanding quantum Shannon theory. The book of Nielsen and Chuang (sometimes known as “Mike and Ike”) has become the standard starting point for students in quantum information science and might be helpful as well (Nielsen & Chuang, 2000). Some of the content in that book is available in Nielsen’s dissertation (Nielsen, 1998). If you are familiar with Shannon’s information theory (at the level of Cover and Thomas (1991), for example), then this book should be a helpful entry point into the field of quantum Shannon theory. We build on intuition developed classically to help in establishing schemes for communication over quantum channels. If you are familiar with quantum mechanics, it might still be worthwhile to review Part II because some content there might not be part of a standard course on quantum mechanics.

The aim of this book is to develop “from the ground up” many of the major, exciting, pre- and post-millennium developments in the general area of study known as quantum Shannon theory. As such, we spend a significant amount of time on quantum mechanics for quantum information theory (Part II), we give a careful study of the important unit protocols of teleportation, superdense coding, and entanglement distribution (Part III), and we develop many of the tools necessary for understanding information transmission or compression (Part IV). Parts V and VI are the culmination of this book, where all of the tools developed come into play for understanding many of the important results in quantum Shannon theory.

For Instructors

This book could be useful for self-learning or as a reference, but one of the main goals is for it to be employed as an instructional aid for the classroom. To aid instructors in designing a course to suit their own needs, a preprint version of this book is available from <http://arxiv.org/abs/1106.1445> under a Creative Commons Attribution-NonCommercial-ShareAlike license. This means that you can modify and redistribute the preprint version of this book as you wish, as long as you attribute the author, you do not use it for commercial purposes, and you share a modification or derivative work under the same license (see <http://creativecommons.org/licenses/by-nc-sa/3.0/> for a readable summary of the terms of the license). These requirements can be waived if you obtain permission from the present author. By releasing the preprint version of this book under this license, I expect and encourage instructors to modify it for their own needs. This will allow for the addition of new exercises, new developments in the theory, and the latest open problems. It might also be a helpful starting point for a book on a related topic, such as network quantum Shannon theory.

I used an earlier version of this book in a one-semester course on quantum Shannon theory at McGill University during Winter semester 2011 (in many parts of the USA, this semester is typically called “Spring semester”). We almost went through the entire book, but it might also be possible to spread the content over two semesters instead. Here is the order in which we proceeded:

1. Introduction in Part I.
2. Quantum mechanics in Part II.
3. Unit protocols in Part III.
4. Chapter 9 on distance measures, Chapter 10 on classical information and entropy, and Chapter 11 on quantum information and entropy.
5. The first part of Chapter 13 on classical typicality and Shannon compression.
6. The first part of Chapter 14 on quantum typicality.
7. Chapter 17 on Schumacher compression.
8. Back to Chapters 13 and 14 for the method of types.
9. Chapter 18 on entanglement concentration.
10. Chapter 19 on classical communication.
11. Chapter 20 on entanglement-assisted classical communication.
12. The final explosion of results in Chapter 21 (one of which is a route to proving the achievability part of the quantum capacity theorem).

The above order is just a particular order that suited the needs for the class at McGill, but other orders are of course possible. One could sacrifice the last part of Part III on the unit resource capacity region if there is no desire to cover the quantum dynamic capacity theorem. One could also focus on going from classical communication to private classical communication to quantum communication in order to develop some more intuition behind the quantum capacity theorem.

Other Sources

There are many other sources to obtain a background in quantum Shannon theory. The standard reference has become the book of Nielsen and Chuang (2000), but it does not feature any of the post-millennium results in quantum Shannon theory. Other books that cover some aspects of quantum Shannon theory are Hayashi (2006) and Holevo (2002a). Patrick Hayden has had a significant hand as a collaborative guide for many PhD and Masters' theses in quantum Shannon theory, during his time as a postdoctoral fellow at the California Institute of Technology and as a professor at McGill University. These include the theses of Yard (2005), Abeyesinghe (2006), Savov (2008, 2012), Dupuis (2010), and Dutil (2011). All of these theses are excellent references. Naturally, Hayden also had a strong influence over the present author during the development of this book.

Acknowledgments

I began working on this book in the summer of 2008 in Los Angeles, with much time to spare in the final months of dissertation writing. I had a strong determination to review quantum Shannon theory, a beautiful area of quantum information science that Igor Devetak had taught me three years earlier at USC in fall 2005. I was carefully studying a manuscript entitled “Principles of Quantum Information Theory,” a text that Igor had initiated in collaboration with Patrick Hayden and Andreas Winter. I read this manuscript many times, and many parts of it I understood well, though other parts I did not.

After a few weeks of reading and rereading, I decided “if I can write it out myself from scratch, perhaps I would then understand it!”, and thus began the writing of the chapters on the packing lemma, the covering lemma, and quantum typicality. I knew that Igor’s (now former) students Min-Hsiu Hsieh and Zhicheng Luo knew the topic well because they had already written several quality research papers with him, so I requested if they could meet with me weekly for an hour to review the fundamentals. They kindly agreed and helped me quite a bit in understanding the packing and covering techniques.

Not much later, after graduating, I began collaborating with Min-Hsiu on a research project that Igor had suggested to the both of us: “find the triple trade-off capacity formulas of a quantum channel.” This was perhaps the best starting point for me to learn quantum Shannon theory because proving this theorem required an understanding of most everything that had already been accomplished in the area. After a month of effort, I continued to work with Min-Hsiu on this project while joining Andreas Winter’s Singapore group for a two-month visit. As I learned more, I added more to the notes, and they continued to grow.

After landing a job in the DC area for January 2009, I realized that I had almost enough material for teaching a course, and so I contacted local universities in the area to see if they would be interested. Can Korman, formerly chair of the Electrical Engineering Department at George Washington University, was excited about the possibility. His enthusiasm was enough to keep me going on the notes, and so I continued to refine and add to them in my spare time in preparing for teaching. Unfortunately (or perhaps fortunately?), the course ended up being canceled. This was disheartening to me, but in the mean time, I had contacted Patrick Hayden to see if he would be interested in having me join his group at

McGill University for postdoctoral studies. Patrick Hayden and David Avis then offered me a postdoctoral fellowship, and I moved to Montréal in October 2009.

After joining, I learned a lot by collaborating and discussing with Patrick and his group members. Patrick offered me the opportunity to teach his graduate class on quantum Shannon theory while he was away on sabbatical, and this encouraged me further to persist with the notes.

I am grateful to everyone mentioned above for encouraging and supporting me during this project, and I am also grateful to everyone who provided feedback during the course of writing up. In this regard, I am especially grateful to Dave Touchette for detailed feedback on all of the chapters in the book. Dave's careful reading and spotting of errors has immensely improved the quality of the book. I am grateful to my father, Gregory E. Wilde, Sr., for feedback on earlier chapters and for advice and love throughout. I thank Ivan Savov for encouraging me, for feedback, and for believing that this is an important scholarly work. I also thank Constance Caramanolis, Raza-Ali Kazmi, John M. Schanck, Bilal Shaw, and Anna Vershynina for valuable feedback. I am grateful to Min-Hsiu Hsieh for the many research topics we have worked on together that have enhanced my knowledge of quantum Shannon theory. I thank Michael Nielsen and Victor Shoup for advice on Creative Commons licensing and Kurt Jacobs for advice on book publishing. I acknowledge funding from the MDEIE (Quebec) PSR-SIIRI international collaboration grant. I am grateful to Sarah Payne and David Tranah of Cambridge University Press for their extensive feedback on the manuscript and their outstanding support throughout the publication process.

I am indebted to my mentors who took me on as a student during my career. Todd Brun was a wonderful PhD supervisor—helpful, friendly, and encouraging of creativity and original pursuit. Igor Devetak taught me quantum Shannon theory in fall 2005 and helped me once per week during his office hours. He also invited me to join Todd's and his group, and more recently, Igor provided much encouragement and “big-picture” feedback during the writing of this book. Bart Kosko shaped me as a scholar during my early years at USC and provided helpful advice regarding the book project. Patrick Hayden has been an immense bedrock of support at McGill. His knowledge of quantum information and many other areas is unsurpassed, and he has been kind, inviting, and helpful during my time at McGill. I am also grateful to Patrick for giving me the opportunity to teach at McGill and for advice throughout the development of this book.

I thank my mother, father, sister, and brother and all of my surrounding family members for being a source of love and support. Finally, I am indebted to my wife Christabelle and her family for warmth and love. I dedicate this book to the memory of my grandparents Joseph and Rose McMahon, and Norbert Jay and Mary Wilde. *Lux aeterna luceat eis, Domine.*

Contents

	<i>How To Use This Book</i>	page xi
	<i>Acknowledgments</i>	xiv
Part I	Introduction	1
1	Concepts in Quantum Shannon Theory	3
	1.1 Overview of the Quantum Theory	7
	1.2 The Emergence of Quantum Shannon Theory	11
2	Classical Shannon Theory	26
	2.1 Data Compression	26
	2.2 Channel Capacity	35
	2.3 Summary	49
Part II	The Quantum Theory	51
3	The Noiseless Quantum Theory	53
	3.1 Overview	54
	3.2 Quantum Bits	55
	3.3 Reversible Evolution	61
	3.4 Measurement	68
	3.5 Composite Quantum Systems	74
	3.6 Summary and Extensions to Qudit States	89
	3.7 History and Further Reading	96
4	The Noisy Quantum Theory	97
	4.1 Noisy Quantum States	98
	4.2 Measurement in the Noisy Quantum Theory	110
	4.3 Composite Noisy Quantum Systems	112
	4.4 Noisy Evolution	120
	4.5 Summary	139
	4.6 History and Further Reading	140
5	The Purified Quantum Theory	141
	5.1 Purification	142
	5.2 Isometric Evolution	143

5.3	Coherent Quantum Instrument	154
5.4	Coherent Measurement	155
5.5	History and Further Reading	156
Part III	Unit Quantum Protocols	157
6	Three Unit Quantum Protocols	159
6.1	Non-local Unit Resources	160
6.2	Protocols	162
6.3	Optimality of the Three Unit Protocols	171
6.4	Extensions for Quantum Shannon Theory	173
6.5	Three Unit Qudit Protocols	174
6.6	History and Further Reading	180
7	Coherent Protocols	181
7.1	Definition of Coherent Communication	182
7.2	Implementations of a Coherent Bit Channel	184
7.3	Coherent Dense Coding	185
7.4	Coherent Teleportation	187
7.5	The Coherent Communication Identity	189
7.6	History and Further Reading	190
8	The Unit Resource Capacity Region	191
8.1	The Unit Resource Achievable Region	191
8.2	The Direct Coding Theorem	195
8.3	The Converse Theorem	196
8.4	History and Further Reading	200
Part IV	Tools of Quantum Shannon Theory	201
9	Distance Measures	203
9.1	Trace Distance	204
9.2	Fidelity	212
9.3	Relationships between Trace Distance and Fidelity	219
9.4	Gentle Measurement	223
9.5	Fidelity of a Noisy Quantum Channel	226
9.6	The Hilbert–Schmidt Distance Measure	230
9.7	History and Further Reading	231
10	Classical Information and Entropy	232
10.1	Entropy of a Random Variable	233
10.2	Conditional Entropy	237
10.3	Joint Entropy	239
10.4	Mutual Information	239
10.5	Relative Entropy	240

10.6	Conditional Mutual Information	241
10.7	Information Inequalities	243
10.8	Classical Information and Entropy of Quantum Systems	249
10.9	History and Further Reading	251
11	Quantum Information and Entropy	252
11.1	Quantum Entropy	253
11.2	Joint Quantum Entropy	258
11.3	Potential yet Unsatisfactory Definitions of Conditional Quantum Entropy	261
11.4	Conditional Quantum Entropy	263
11.5	Coherent Information	265
11.6	Quantum Mutual Information	267
11.7	Conditional Quantum Mutual Information	270
11.8	Quantum Relative Entropy	272
11.9	Quantum Information Inequalities	275
11.10	History and Further Reading	290
12	The Information of Quantum Channels	292
12.1	Mutual Information of a Classical Channel	293
12.2	Private Information of a Wiretap Channel	299
12.3	Holevo Information of a Quantum Channel	303
12.4	Mutual Information of a Quantum Channel	309
12.5	Coherent Information of a Quantum Channel	314
12.6	Private Information of a Quantum Channel	319
12.7	Summary	325
12.8	History and Further Reading	326
13	Classical Typicality	327
13.1	An Example of Typicality	328
13.2	Weak Typicality	329
13.3	Properties of the Typical Set	331
13.4	Application of Typical Sequences: Shannon Compression	333
13.5	Weak Joint Typicality	335
13.6	Weak Conditional Typicality	338
13.7	Strong Typicality	341
13.8	Strong Joint Typicality	350
13.9	Strong Conditional Typicality	352
13.10	Application: Shannon's Channel Capacity Theorem	358
13.11	Concluding Remarks	362
13.12	History and Further Reading	363
14	Quantum Typicality	364
14.1	The Typical Subspace	365
14.2	Conditional Quantum Typicality	375

14.3	The Method of Types for Quantum Systems	384
14.4	Concluding Remarks	387
14.5	History and Further Reading	387
15	The Packing Lemma	388
15.1	Introductory Example	389
15.2	The Setting of the Packing Lemma	389
15.3	Statement of the Packing Lemma	391
15.4	Proof of the Packing Lemma	393
15.5	Derandomization and Expurgation	398
15.6	History and Further Reading	400
16	The Covering Lemma	401
16.1	Introductory Example	402
16.2	Setting and Statement of the Covering Lemma	404
16.3	Proof of the Covering Lemma	406
16.4	History and Further Reading	413
Part V	Noiseless Quantum Shannon Theory	415
17	Schumacher Compression	417
17.1	The Information-Processing Task	418
17.2	The Quantum Data-Compression Theorem	420
17.3	Quantum Compression Example	424
17.4	Variations on the Schumacher Theme	425
17.5	Concluding Remarks	427
17.6	History and Further Reading	427
18	Entanglement Concentration	429
18.1	An Example of Entanglement Concentration	430
18.2	The Information-Processing Task	433
18.3	The Entanglement Concentration Theorem	433
18.4	Common Randomness Concentration	440
18.5	Schumacher Compression versus Entanglement Concentration	441
18.6	Concluding Remarks	445
18.7	History and Further Reading	445
Part VI	Noisy Quantum Shannon Theory	447
19	Classical Communication	451
19.1	Naive Approach: Product Measurements at the Decoder	453
19.2	The Information-Processing Task	456
19.3	The Classical Capacity Theorem	458
19.4	Examples of Channels	463

19.5	Superadditivity of the Holevo Information	471
19.6	Concluding Remarks	474
19.7	History and Further Reading	475
20	Entanglement-Assisted Classical Communication	477
20.1	The Information-Processing Task	479
20.2	A Preliminary Example	480
20.3	The Entanglement-Assisted Classical Capacity Theorem	484
20.4	The Direct Coding Theorem	484
20.5	The Converse Theorem	493
20.6	Examples of Channels	501
20.7	Concluding Remarks	506
20.8	History and Further Reading	507
21	Coherent Communication with Noisy Resources	508
21.1	Entanglement-Assisted Quantum Communication	509
21.2	Quantum Communication	514
21.3	Noisy Super-Dense Coding	515
21.4	State Transfer	518
21.5	Trade-off Coding	522
21.6	Concluding Remarks	530
21.7	History and Further Reading	531
22	Private Classical Communication	532
22.1	The Information-Processing Task	533
22.2	The Private Classical Capacity Theorem	536
22.3	The Direct Coding Theorem	536
22.4	The Converse Theorem	545
22.5	Discussion of Private Classical Capacity	546
22.6	History and Further Reading	549
23	Quantum Communication	550
23.1	The Information-Processing Task	551
23.2	The No-Cloning Theorem and Quantum Communication	553
23.3	The Quantum Capacity Theorem	554
23.4	The Direct Coding Theorem	555
23.5	Converse Theorem	562
23.6	An Interlude with Quantum Stabilizer Codes	564
23.7	Example Channels	571
23.8	Discussion of Quantum Capacity	574
23.9	Entanglement Distillation	579
23.10	History and Further Reading	582

24	Trading Resources for Communication	585
24.1	The Information-Processing Task	586
24.2	The Quantum Dynamic Capacity Theorem	588
24.3	The Direct Coding Theorem	593
24.4	The Converse Theorem	596
24.5	Examples of Channels	606
24.6	History and Further Reading	616
25	Summary and Outlook	618
25.1	Unit Protocols	619
25.2	Noiseless Quantum Shannon Theory	619
25.3	Noisy Quantum Shannon Theory	620
25.4	Protocols Not Covered in This Book	623
25.5	Network Quantum Shannon Theory	624
25.6	Future Directions	625
Appendix A	Miscellaneous Mathematics	626
Appendix B	Monotonicity of Quantum Relative Entropy	633
	<i>References</i>	639
	<i>Index</i>	653

Part I

Introduction

