
Theory of Quantum Information

John Watrous
Institute for Quantum Computing
University of Waterloo



This work is licensed under the Creative Commons Attribution-ShareAlike 3.0 Unported License. Visit <http://creativecommons.org/licenses/by-sa/3.0/> to view a copy of this license.

Contents

1	Mathematical preliminaries	1
1.1	Linear algebra	1
1.1.1	Complex Euclidean spaces	1
1.1.2	Linear operators	8
1.1.3	Operator decompositions and norms	26
1.2	Analysis, convexity, and probability theory	37
1.2.1	Analysis and convexity	37
1.2.2	Probability theory	50
1.2.3	Semidefinite programming	57
1.3	Suggested references	61
2	Basic notions of quantum information	63
2.1	Registers and states	63
2.1.1	Registers and classical state sets	63
2.1.2	Quantum states of registers	66
2.1.3	Reductions and purifications of quantum states	73
2.2	Quantum channels	79
2.2.1	Definitions and basic notions concerning channels	79
2.2.2	Representations and characterizations of channels	84
2.2.3	Examples of channels and other mappings	99
2.2.4	Extremal channels	105
2.3	Measurements	109
2.3.1	Two equivalent definitions of measurements	109
2.3.2	Basic notions concerning measurements	114
2.3.3	Extremal measurements and ensembles	123
2.4	Exercises	130
2.5	Bibliographic remarks	132

3	Similarity and distance among states and channels	135
3.1	Quantum state discrimination	135
3.1.1	Discriminating between pairs of quantum states	136
3.1.2	Discriminating quantum states of an ensemble	144
3.2	The fidelity function	151
3.2.1	Elementary properties of the fidelity function	152
3.2.2	Alternative characterizations of the fidelity function	156
3.2.3	Further properties of the fidelity function	168
3.3	Channel distances and discrimination	178
3.3.1	Channel discrimination	178
3.3.2	The completely bounded trace norm	181
3.3.3	Distances between channels	189
3.3.4	Properties of the completely bounded trace norm	200
3.4	Exercises	213
3.5	Bibliographic remarks	214
4	Unital channels and majorization	219
4.1	Subclasses of unital channels	219
4.1.1	Mixed-unitary channels	220
4.1.2	Weyl-covariant channels	231
4.1.3	Schur channels	239
4.2	General properties of unital channels	243
4.2.1	Extreme points of the set of unital channels	243
4.2.2	Fixed-points, spectra, and norms of unital channels	249
4.3	Majorization	254
4.3.1	Majorization for real vectors	254
4.3.2	Majorization for Hermitian operators	263
4.4	Exercises	268
4.5	Bibliographic remarks	270
5	Quantum entropy and source coding	273
5.1	Classical entropy	273
5.1.1	Definitions of classical entropic functions	273
5.1.2	Properties of classical entropic functions	276
5.2	Quantum entropy	289
5.2.1	Definitions of quantum entropic functions	289
5.2.2	Elementary properties of quantum entropic functions	292

5.2.3	Joint convexity of quantum relative entropy	300
5.3	Source coding	309
5.3.1	Classical source coding	309
5.3.2	Quantum source coding	315
5.3.3	Encoding classical information into quantum states	320
5.4	Exercises	333
5.5	Bibliographic remarks	335
6	Bipartite entanglement	339
6.1	Separability	339
6.1.1	Separable operators and states	340
6.1.2	Separable maps and the LOCC paradigm	355
6.1.3	Separable and LOCC measurements	363
6.2	Manipulation of entanglement	371
6.2.1	Entanglement transformation	371
6.2.2	Distillable entanglement and entanglement cost	378
6.2.3	Bound entanglement and partial transposition	385
6.3	Phenomena associated with entanglement	392
6.3.1	Teleportation and dense coding	392
6.3.2	Non-classical correlations	406
6.4	Exercises	419
6.5	Bibliographic remarks	422
7	Permutation invariance and unitarily invariant measures	427
7.1	Permutation-invariant vectors and operators	427
7.1.1	The subspace of permutation-invariant vectors	428
7.1.2	The algebra of permutation-invariant operators	438
7.2	Unitarily invariant probability measures	447
7.2.1	Uniform spherical measure and Haar measure basics . . .	447
7.2.2	Applications of unitarily invariant measures	460
7.3	Measure concentration and its applications	470
7.3.1	Lévy's lemma and Dvoretzky's theorem	470
7.3.2	Applications of measure concentration	489
7.4	Exercises	503
7.5	Bibliographic remarks	505

8	Quantum channel capacities	507
8.1	Classical information over quantum channels	507
8.1.1	Classical capacities of quantum channels	508
8.1.2	The Holevo–Schumacher–Westmoreland theorem	521
8.1.3	The entanglement-assisted classical capacity theorem . . .	539
8.2	Quantum information over quantum channels	559
8.2.1	Definitions of quantum capacity and related notions . . .	559
8.2.2	The quantum capacity theorem	568
8.3	Non-additivity and super-activation	587
8.3.1	Non-additivity of the Holevo capacity	588
8.3.2	Super-activation of quantum channel capacity	594
8.4	Exercises	606
8.5	Bibliographic remarks	608

Preface

This is a draft of a book that began as a set of course notes for a graduate course on the theory of quantum information that I have taught several times at the University of Waterloo.

The book 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 on the subject. The focus of the book is on the mathematical aspects of quantum information, with an emphasis on proofs. No attention is paid to motives for studying the theory of quantum information, as it is assumed that the reader has already been motivated—and is perhaps interested in proving new theorems on quantum information of his or her own. It should also be said that this is not a physics book: the Schrödinger equation will not be found herein, and the difficult technological challenge of building quantum information processing devices is blissfully ignored.

The selection of topics covered in this book is not intended to be fully representative of the diverse subject of quantum information science. There is, for example, no discussion of quantum cryptography, quantum error correcting codes and fault-tolerance, quantum algorithms and complexity theory, or topological quantum computing, which are among the topics within the theoretical branches of quantum information science having fundamental importance. Nevertheless, one is likely to encounter some of the core mathematical notions discussed in this book when studying these and other topics.

As the students who have taken my course on the theory of quantum information will attest, I sometimes choose to deviate from the standard conventions of quantum information and computation, particularly with respect to notation and terminology. I have exhibited this behavior once again when writing this book. For example, I have avoided the use of the

commonly used Dirac notation, and in some cases I have changed the names and symbols associated with concepts as I have seen fit. I hope that readers who have previously grown familiar with the notation and conventions of quantum information that I have chosen not to follow will excuse me for this, and hope that they will find value in this book nevertheless.

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 much more difficult. In some cases, these exercises have been derived from research papers that clearly reveal their solutions, and I have not attempted to disguise this fact or hide their source. 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.

I thank Debbie Leung, Ashwin Nayak, Marco Piani, and Patrick Hayden for helpful discussions on some of the topics covered in this book, and I thank Sascha Agne for assisting me with German translations. I also thank the following people for comments, corrections, and suggestions on my course notes and previous versions of this book:

Alessandro Cosentino,	Leung Ming Lam,	Alexey Rastegin,
Mohammad Derakhshani,	Alexandre Laplante,	John Rinehart,
Olivia Di Matteo,	Anthony Leverrier,	Ansis Rosmanis,
Edward Effros,	Ben Lovitz,	Vincent Russo,
Chris Ferrie,	Abel Molina,	Fred Shultz,
Mirmojtaba Gharibi,	Adam Meikle,	Yuan Su,
Gus Gutoski,	Maris Ozols,	Le Phuc Thinh,
Guiyang Han,	Dan Puzzuoli,	Chunhao Wang,
Anirudh Krishna,	Hammam Qassim,	Nengkun Yu.

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

Finally, I thank Christiane Lemieux for encouraging my efforts to write this book on too many occasions to count.

John Watrous
john.watrous@uwaterloo.ca
Waterloo, September 2016