The Theory of Quantum Information

John Watrous
Institute for Quantum Computing
University of Waterloo

To be published by Cambridge University Press.

Contents

Preface *page* vii

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 24

1.2 Analysis, convexity, and probability theory 35

1.2.1 Analysis and convexity 35

1.2.2 Probability theory 47

1.2.3 Semidefinite programming 53

1.3 Suggested references 57

2 Basic notions of quantum information 58

2.1 Registers and states 58

2.1.1 Registers and classical state sets 58

2.1.2 Quantum states of registers 61

2.1.3 Reductions and purifications of quantum states 67

2.2 Quantum channels 72

2.2.1 Definitions and basic notions concerning channels 72

2.2.2 Representations and characterizations of channels 77

2.2.3 Examples of channels and other mappings 91

2.2.4 Extremal channels 96

2.3 Measurements 100

2.3.1 Two equivalent definitions of measurements 100

2.3.2 Basic notions concerning measurements 105

2.3.3 Extremal measurements and ensembles 113

2.4 Exercises 120

2.5 Bibliographic remarks 122

3 Similarity and distance among states and channels 124
3.1 Quantum state discrimination 124
3.1.1 Discriminating between pairs of quantum states 125
3.1.2 Discriminating quantum states of an ensemble 132
3.2 The fidelity function 139
3.2.1 Elementary properties of the fidelity function 140
3.2.2 Characterizations of the fidelity function 144
3.2.3 Further properties of the fidelity function 155
3.3 Channel distances and discrimination 164
3.3.1 Channel discrimination 164
3.3.2 The completely bounded trace norm 166
3.3.3 Distances between channels 175
3.3.4 Characterizations of the completely bounded trace norm 185
3.4 Exercises 197
3.5 Bibliographic remarks 198

4 Unital channels and majorization 201
4.1 Subclasses of unital channels 201
4.1.1 Mixed-unitary channels 202
4.1.2 Weyl-covariant channels 212
4.1.3 Schur channels 219
4.2 General properties of unital channels 222
4.2.1 Extreme points of the set of unital channels 222
4.2.2 Fixed-points, spectra, and norms of unital channels 228
4.3 Majorization 233
4.3.1 Majorization for real vectors 233
4.3.2 Majorization for Hermitian operators 241
4.4 Exercises 246
4.5 Bibliographic remarks 247

5 Quantum entropy and source coding 250
5.1 Classical entropy 250
5.1.1 Definitions of classical entropic functions 250
5.1.2 Properties of classical entropic functions 253
5.2 Quantum entropy 265
5.2.1 Definitions of quantum entropic functions 265
5.2.2 Elementary properties of quantum entropic functions 267
5.2.3 Joint convexity of quantum relative entropy 276
5.3 Source coding 283

5.3.1 Classical source coding 284
5.3.2 Quantum source coding 289
5.3.3 Encoding classical information into quantum states 294
5.4 Exercises 306
5.5 Bibliographic remarks 308

6 Bipartite entanglement 310
6.1 Separability 310
6.1.1 Separable operators and states 310
6.1.2 Separable maps and the LOCC paradigm 324
6.1.3 Separable and LOCC measurements 332
6.2 Manipulation of entanglement 339
6.2.1 Entanglement transformation 339
6.2.2 Distillable entanglement and entanglement cost 345
6.2.3 Bound entanglement and partial transposition 352
6.3 Phenomena associated with entanglement 358
6.3.1 Teleportation and dense coding 359
6.3.2 Non-classical correlations 371
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
7.1.1 The subspace of permutation-invariant vectors 391
7.1.2 The algebra of permutation-invariant operators 400
7.2 Unitarily invariant probability measures 408
7.2.1 Uniform spherical measure and Haar measure 408
7.2.2 Applications of unitarily invariant measures 420
7.3 Measure concentration and it applications 429
7.3.1 Lévy's lemma and Dvoretzky's theorem 430
7.3.2 Applications of measure concentration 447
7.4 Exercises 460
7.5 Bibliographic remarks 462

8 Quantum channel capacities 464
8.1 Classical information over quantum channels 464
8.1.1 Classical capacities of quantum channels 465
8.1.2 The Holevo–Schumacher–Westmoreland theorem 476
8.1.3 The entanglement-assisted classical capacity theorem 493
8.2 Quantum information over quantum channels 512

8.2.1 Definitions of quantum capacity and related notions 512
8.2.2 The quantum capacity theorem 521
8.3 Non-additivity and super-activation 538
8.3.1 Non-additivity of the Holevo capacity 539
8.3.2 Super-activation of quantum channel capacity 545
8.4 Exercises 556
8.5 Bibliographic remarks 558

References 561
Index of Symbols 573
Index 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 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 with both 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.

John Watrous
Waterloo, January 2018