The Theory of Quantum Information

John Watrous
Institute for Quantum Computing
University of Waterloo

To be published by Cambridge University Press.

Please note that this is a draft, pre-publication copy only. The final, published version of this book will be available for purchase through Cambridge University Press and other standard distribution channels. This draft copy is made available for personal use only and must not be sold or redistributed.

Contents

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