# Preface

Like many such endeavors, this book evolved out of lecture notes for a master level course on quantum information theory that I have given several times at ETH Zürich and at the Technical University of Darmstadt. The main goal of the book, as with the course, is to understand in detail some of the fundamental limitations and possibilities of information processing with quantum-mechanical information carriers. The particular focus is on communication and cryptographic tasks, leaving computational issues for another day.

In outlook and aims, this book is very much inspired by Asher Peres's *Quantum Theory: Concepts and Methods* and John Baez and Javier Muniain's *Gauge Fields, Knots and Gravity*. Peres's "strictly instrumentalist" focus was formative for my own initial understanding of the field, and I follow an operational approach throughout. This helps avoid imbuing the mathematical quantities one can define in quantum theory with any unwarranted physical meaning. The relentless operational approach leads to a slight clash with many other texts in that standard quantities such as distinguishability or fidelity are defined here in variational terms, having to do with optimal measurements or similar, and only later are the corresponding closed forms derived. Continuing in this operational spirit, I felt, justified borrowing a bit from Peres's title. Baez and Muniain is, in my opinion, a real masterpiece of exposition. I have sought (perhaps in vain) to emulate their logical, elegant, and motivated presentation and development of the topics under consideration, though of course the particular topics here are completely different.

I have also borrowed the three-part structure from both. The first covers the formalism of quantum information theory, or really open quantum systems of finite dimension, developing it by explicit analogy with classical probability theory. The second part deals with the tools useful for analyzing information processing tasks, most of which also find application in other parts of the field. Characteristic of Part II is a heavy reliance, if not overreliance, on semidefinite programming to phrase and derive most of the main results. I have attempted to keep the required background for the reader to a modest level—a thorough understanding of linear algebra—and then to derive everything from there. The third part takes up the information processing protocols themselves, with the particular emphasis on so-called "one-shot" statements of structureless resources. These statements are formulated in terms of a quantity involved in the simpler task of binary hypothesis testing. From there, results for the usual setting of i. i. d. resources can be recovered by Stein's lemma relating hypothesis testing to entropy. This is also quite at odds with most texts on information theory, which places entropy front and center, even treating it axiomatically. Again, I follow the strictly operational approach. My aim here has also been to keep the number of different tools developed in Part II and techniques employed in Part III to a minimum. The statements found in the latest literature use a bewildering variety of quantities and methods, and we have to make a cut somewhere. I also thought it useful to make a

https://doi.org/10.1515/9783110570250-201

somewhat different choice of techniques than other texts, if only for variety. Moreover, the relationship between privacy and error correction in the quantum realm, mediated by concrete formulations of the uncertainty principle, is too grand not to explore in more detail.

The material contained in these pages owes much inspiration to the lecture notes by Carl Caves, John Preskill, and Renato Renner, as well as John Watrous's *Theory of Quantum Information* and Mark Wilde's *Quantum Information Theory*. But much more than that it is the result of wrestling with the material contained therein, scrutinizing and rehashing it, adding some bits and subtracting others, and finally molding it to fit my own sense of the landscape of the theory. The two quotes in the epigraph speak beautifully to this point. Readers who really wish to understand the material will have to undertake their own struggle of course, and I hope they (you!) at least gain some inspiration from seeing the particular development here. Working through the exercises will also help.

I have benefited enormously from often lengthy conversations over the past decade with the members of the quantum information theory group at ETH Zürich, and the book would not be what it is were it not for the very stimulating atmosphere of the group and the Institute of Theoretical Physics as a whole. I especially thank Volkher Scholz, Michael Walter, David Sutter, Christophe Piveteau, Ernest Tan, Henrik Wilming, Fred Dupuis, Marco Tomamichel, Mario Berta, and Renato Renner. The material on quantum error correction has benefited greatly from my earlier collaborations with Graeme Smith and especially with Jean-Christian Boileau. The overall presentation has been refined by the very helpful feedback from students and teaching assistants in the quantum information theory course over the years. I am grateful to the assistants Sandra Stupar, Jinzhao Wang, Lisa Hänggli, Philipp Kammerlander, Raban Iten, Alessandro Tarantola, Imre Májer, and Ernest Tan, and students too numerous to list here. To be sure, there is about twice as much material here as for our one semester course, but more than a few rough edges have been polished, and several gaps in the proofs fixed through their feedback, particularly in the earlier material.

Finally, I am immensely grateful to my wonderful wife Andrea. Without her encouragement, love, and support this project could never have been started, let alone finished.

Zürich, May 2022 Joseph M. Renes