Preface

Quantum information theory studies the general laws of transfer, storage, and processing of information in systems obeying the laws of quantum mechanics. It took shape as a self-consistent area of research in the 1990s, while its origin can be traced back to the 1950–1960s, which was when the basic ideas of reliable data transmission and of Shannon’s information theory were developed. At the first stage, which covers the period 1960–1980, the main issue consisted of the fundamental restrictions on the possibilities of information transfer and processing caused by the quantum mechanical nature of its carrier. Modern technological developments, relying upon the achievements of quantum electronics and quantum optics, suggest that in the foreseeable future such restrictions will become the main obstacle limiting further extrapolation of existing technologies and principles of information processing.

The emergence, in the 1980–1990s, of the ideas of quantum computing, quantum cryptography, and the new communication protocols, on the other hand, allowed discussing not only the restrictions, but also the new possibilities created by the use of specific quantum resources, such as quantum entanglement, quantum complementarity, and quantum parallelism. Quantum information theory provides the clue to understanding these fundamental issues and stimulates the development of experimental physics, with potential importance to new, effective applications. At present, investigations in the area of quantum information science, including information theory, its experimental aspects, and technological developments, are ongoing in advanced research centers throughout the world.

The mathematical toolbox of “classical” information theory contains methods based on probability theory, combinatorics, and modern algebra, including algebraic geometry. For a mathematician sensible to the impact of his research on the natural sciences, information theory can be a source of deep ideas and new, challenging problems, with sound motivation and applications. This equally, if not to a greater extent, applies to quantum information theory, the scope of which turns out to be closely connected to multilinear algebra and noncommutative analysis, convexity, and asymptotic theory of finite-dimensional normed spaces, subtle aspects of positivity and tensor products in operator algebras, and the methods of random matrices. Nowadays, the intimate connections to operator spaces and so-called “quantum functional analysis” have been revealed and explored.

In 2002, the Moscow Independent University published the author’s lecture notes (in Russian), in which an attempt was made at a mathematician’s introduction to problems of quantum information theory. In 2010, a substantially expanded text was published with the title “Quantum systems, channels, information.” The author’s intention was to provide a widely accessible and self-contained introduction to the subject, starting from primary structures and leading up to nontrivial results with rather de-
tailed proofs, as well as to some open problems. The present English text is a further step in that direction, extending and improving the Russian version of 2010.

The exposition is organized in concentric circles, the $N$th round consisting of Parts I to $N$, where each circle is self-contained. The reader can restrict himself to any of these circles, depending on the depth of presentation that he or she demands. In particular, in Part I to Part IV, we consider finite-dimensional systems and channels, whereas the infinite-dimensional case is treated in the final Part V.

Part I starts with a description of the statistical structure of quantum theory. After introducing the necessary mathematical prerequisites in Chapter 1, the central focus in Chapters 2, 3 is on discussing the key features of quantum complementarity and entanglement. The former is reflected by the noncommutativity of the algebra of observables of the system, while the latter is reflected by the tensor product structure of composite quantum systems. Chapter 3 also contains the first applications of the information-theoretic approach to quantum systems.

In information theory, the notions of a channel and its capacity, giving a measure of ultimate information-processing performance of the channel, play a central role. In Chapter 4 of Part II, a review of the basic concepts and necessary results from classical information theory is provided, the quantum analogs of which are the main subject of the following chapters. The concepts of random coding and typicality are introduced and then extended to the quantum case in Chapter 5. That chapter contains direct and self-consistent proofs of the quantum information bound and of the primary coding theorems for the classical-quantum channels, which will later serve as a basis for the more advanced capacity results in Chapter 8.

Part III is devoted to the study of quantum channels and their entropy characteristics. In Chapter 6, we discuss the general concept and structure of a quantum channel, with the help of a variety of examples. From the point of view of operator algebras, these are normalized completely positive maps, the analog of Markov maps in noncommutative probability theory, and they play the role of morphisms in the category of quantum systems. From the point of view of statistical mechanics, a channel gives an overall description of the evolution of an open quantum system interacting with an environment — a physical counterpart of the mathematical dilation theorem. Various entropic quantities essential to the characterization of the information-processing performance, as well as the irreversibility of the channel, are investigated in Chapter 7.

Part IV is devoted to the proofs of advanced coding theorems, which give the main capacities of a quantum channel. Remarkably, in the quantum case, the notion of the channel capacity splits, giving a whole spectrum of information-processing characteristics, depending on the kind of data transmitted (classical or quantum), as well as on the additional communication resources. In Chapter 8, we discuss the classical capacity of a quantum channel, i.e., the capacity for transmitting classical data. We touch upon the tremendous progress made recently in the solution of the related additivity problem and point out the remaining questions. Chapter 9 is devoted to the classical entanglement-assisted capacity and its comparison with unassisted capacity. In
Chapter 10, we consider reliable transmission of quantum information (i.e., quantum states), which turns out to be closely related to the private transmission of classical information. The corresponding coding theorems provide the quantum capacity and the private classical capacity of a quantum channel.

In Part V, we pass from finite-dimensional to separable Hilbert space. Chapter 11 deals with the new obstacles characteristic for infinite-dimensional channels – singular behavior of the entropy (infinite values, discontinuity) and the emergence of the input channel constraints (e.g., finiteness of the signal energy) and of the continuous optimizing state ensembles. Chapter 12 treats the bosonic Gaussian systems and channels on the canonical commutation relations (many experimental demonstrations of quantum information processing were realized in such “continuous-variables” systems, based in particular on the principles of quantum optics). We assume the reader has some minor background in the field and start with a rather extended introduction at the beginning of Chapter 12. Next, we describe and study in detail the Gaussian states and channels. The main mathematical problems here are the structure of the multimode quantum Gaussian channels and the computation of the various entropic quantities characterizing their performance. While the classical entanglement-assisted capacity is, in principle, computable for a general Gaussian channel, the quantum capacity is found only for restricted classes of channels, and the unassisted classical capacity in general presents an open analytical problem, namely, that of verifying the conjecture of “quantum Gaussian optimizers,” which is comparable in complexity to the additivity problem (also open for the class of Gaussian channels) and appears to be closely related to it.

This book does not intend to be an all-embracing text in quantum information theory and its content definitely reflects the author’s personal research interests and preferences. For example, the important topics of entanglement quantification and error correction are mentioned only briefly. An interested reader can find an account of these in other sources, listed in the notes and references to the individual chapters. Quantum information theory is in a stage of fast development and new, important results continue to appear. Yet, we hope the present text will be a useful addition to the existing literature, particularly for mathematically inclined readers eager to penetrate the fascinating world of quantum information.

The basis for these lecture notes was a course taught by the author at the Moscow Institute of Physics and Technology, Moscow State University, and several Western institutions. The author acknowledges stimulating discussions, collaborations, and invaluable support of R. Ahlswede, A. Barchielli, C. H. Bennett, G. M. D’Ariano, C. Fuchs, V. Giovannetti, O. Hirota, R. Jozsa, L. Lanz, O. Melsheimer, H. Neumann, M. B. Ruskai, P. W. Shor, Yu. M. Suhov, K. A. Valiev, R. Werner, A. Winter, and M. Wolf.

I extend special thanks to my colleagues Maxim Shirokov and Andrey Bulinsky for their careful reading of the manuscript and the suggestions for numerous improvements.
This work was supported by the Russian Foundation for Basic Research, Fundamental Research Programs of the Russian Academy of Sciences, and the Cariplo Fellowship organized by the Landau Network – Centro Volta.