Quantum Inf Process (2014) 13:587–590
DOI 10.1007/s11128-013-0690-x

BOOK REVIEW

# Mark M. Wilde: Quantum information theory

**Joseph M. Renes**

Received: 5 November 2013 / Accepted: 12 November 2013 / Published online: 26 November 2013


A decade ago, it was not uncommon for researchers in quantum information theory to be fairly well-acquainted with essentially all the results in the field. Today, this is scarcely possible, as the field has grown tremendously and led to several specialized subfields. One of these is "quantum Shannon theory," the study of the fundamental limits to communication and storage when using quantum-mechanical information carriers, named after the pioneer of (classical) information theory, Claude Shannon. Although quantum Shannon theory is the oldest part of quantum information theory—the earliest investigations were concerned with the effects of the quantum nature of light on reliable communication [1]—the last ten years have produced an enormous number of fundamental results, not the least of which is an expression for the capacity of noisy quantum channels to reliably transmit quantum information.

As is often the case for highly technical results, the journal literature appears as a nearly impenetrable thicket of mathematical prose to those not already well-acquainted with the field. The situation of having many exciting, but inaccessible results cries out for an introductory and pedagogical overview. Enter *Quantum Information Theory* by Mark M. Wilde, recently published by Cambridge University Press. This book has two target audiences and goals: It not only aims to make the results of quantum Shannon theory more comprehensible to quantum information theorists, but also to demonstrate to classical information theorists the natural continuation of topics and methods from the classical to the quantum setting. Other currently available options available to the reader interested in quantum Shannon theory, such as Nielsen & Chuang's classic *Quantum Information & Computation* or the excellent lecture notes of Preskill, are too outdated to cover the recent results. On the other hand, while Hayashi's *Quantum Information Theory: An Introduction* covers much if not essentially all of the recent

J. M. Renes (✉)
Institute for Theoretical Physics, ETH Zurich, Wolfgang-Pauli-Strasse 27, 8093 Zurich, Switzerland
e-mail: renes@phys.ethz.ch

literature (as well as develops new results!), I would venture that it is less of an introduction than the title suggests.

Wilde's *Quantum Information Theory* consists of six parts. Bearing in mind his dual audience, the first technical part of the book (part two) is devoted to an overview of the formalism of quantum mechanics. Part three investigates three basic information processing protocols of quantum theory which have no classical analog: entanglement distribution, superdense coding, and quantum teleportation. Moreover, the description of these protocols is made simple by the use of *resource inequalities*, which greatly simplifies the discussion of more complicated protocols discussed later on. For instance, the protocol of *superdense coding*, in which two classical bits of information are transmitted by using one pair of entangled quantum states and one use of a quantum communication channel, can be represented compactly as

$$[q \to q] + [qq] \geq 2[c \to c]. \tag{1}$$

The presentation is at a level suitable for readers with no knowledge of quantum mechanics and will be immediately familiar to quantum information theorists in all parts of the field.

Part four introduces the information-theoretic tools which will be needed to understand the results of quantum Shannon theory: definitions and properties of *entropy*, *typicality* both classical and quantum, as well as the *packing* and *covering* lemmas. Packing and covering refer to two primitive tasks useful in information processing, namely squeezing as many signals as possible into an allotted space such that they are nevertheless distinguishable (packing) and mimicking the average of a large number of signals by a subset of as few of them as possible (covering). Apart from the quantum-mechanical language, this part should be immediately familiar to classical information theorists. They should also be pleased to find that quantum, like classical, Shannon theory can be constructed on the foundation of the packing and covering lemmas (see [2] for a contemporary treatment in the classical case).

With the necessary background suitably established, eight chapters of parts five and six carefully guide the reader through quantum Shannon theory, discussing and proving the central results. Part five is quick, covering noiseless quantum Shannon theory, namely compression of quantum sources (a.k.a. Schumacher compression) and concentration of partial entanglement in pure states to maximally entangled form. Noisy quantum Shannon theory is where the action is at, however. The ultimate aim of part six is a precise statement and proof of the quantum channel capacity (chapter 23), and the various trade-offs in resources used to achieve this aim (chapter 24). Wilde builds up to this, starting from more classical protocols, by following the route pioneered by Devetak. In this approach, one thinks of quantum information, or specifically quantum entanglement, as akin to shared, *secret* classical randomness. Then, as Devetak showed in the original fully rigorous treatment of the achievability of the quantum capacity, classical protocols for transmitting classical information privately can be directly transformed into quantum protocols for transmitting quantum information [3].

The intermediate stations toward this goal thus treat the tasks of transmitting classical information either publicly or privately over noisy quantum channels, for which the

aforementioned packing and covering lemmas are central. The book is also notable for including the consideration of these tasks under the extra assumption that the sender and receiver have access to additional resources besides a noisy quantum channel, such as noiseless classical or quantum channels or quantum entanglement. Indeed, the case of entanglement-assisted communication (classical or quantum) is simpler than the unassisted case, and analysis of the former serves as a springboard for that of the latter. To keep the treatment of so many protocols from becoming too complicated to follow, the book makes use of the resource framework for describing quantum information protocols. In particular, this formalism is very helpful in avoiding a new, full proof for every new protocol.

The clear, thorough, and above all self-contained presentation will aid quantum information researchers in coming up to speed with the latest results in this area of the field. Meanwhile, the familiar setting and language will help classical information theorists who wish to become more acquainted with the quantum aspects of information processing. If information theory journals are any indication, such readers are also not put off by expressions and equations of seemingly arbitrary complexity; they will feel at home in certain parts of the book (page 491 presents a representative example of the style). Experts will also benefit from the book as a reference. The presentation is well-structured, making it easy to jump to the desired topic and quickly determine on what that topic depends and how it is used going forward.

A book of 655 pages can only cover so much, however, and alternative methods of arriving at the results are not treated. Modesty forbids the reviewer from detailing the complementarity-based approach (see [4] for an overview and [5] for a different method in the same spirit). Particularly absent is the so-called decoupling approach, which has become the standard method in recent years, though the end of chapter 23 sketches the idea (see [6] for an overview). Instead of constructing quantum protocols from private classical protocols, proofs employing decoupling "proceed[s] by showing that the protocol destroys all correlation between the sender and a reference system. Since destruction is a relatively indiscriminate goal, the resulting proof is correspondingly simple" Abeyesinghe et al. [7]. This is not to suggest that the approach taken in the book is outdated or not useful for future research. Indeed, the "Devetak approach" shares some aspects with decoupling, as ensuring secrecy of classical information is after all decoupling of classical information. Moreover, the Devetak approach is surely the simplest entry to quantum Shannon theory for those with a background in classical information theory. Finally, while the great merit of the decoupling approach is its simplicity and ease of establishing in-principle results, eventually the discussion of information processing protocols must turn to the efficiency of their implementation. The more constructive nature of the approach taken in the book is more suitable for attacking such problems.

Despite the author's laudable effort in organizing the material to make it more accessible, I feel that many in the quantum information theory community, perhaps particularly those coming from physics, will still find the presentation too complicated. This is not really a criticism of the book, but rather of the methods common in information theory itself. Each new protocol seems to require its own proof, even when more elaborate protocols are composed of simpler elements. True, almost all proofs make use of the same few tricks, and the resource calculus is good at making it clear

how to recycle results. However, even simpler would be a recycling of the protocols themselves, treating simple protocols as building blocks whose internal details need not be examined when combining them into more complicated schemes.

These criticisms notwithstanding, *Quantum Information Theory* fills an important gap in the existing literature and will, I expect, help propagate the latest and greatest results in quantum Shannon theory to both quantum and classical researchers.

## References

1. Gabor, D.: Communication theory and physics. Philos. Mag. Ser. 7 **41**(322), 1161–1187 (1950)
2. El Gamal, A.A., Kim, Y.-H.: Network Information Theory. Cambridge University Press, Cambridge (2011)
3. Devetak, I.: The private classical capacity and quantum capacity of a quantum channel. IEEE Trans. Inf. Theory (2005). doi:10.1109/TIT.2004.839515
4. Renes, J.M.: The physics of quantum information: complementarity, uncertainty, and entanglement. Habilitation Thesis, TU Darmstadt, December 2011.arXiv:1212.2379 [quant-ph]
5. Hayden, P., Shor, P.W., Winter, A.: Random quantum codes from gaussian ensembles and an uncertainty relation. Open Syst. Inf. Dyn. (2008). doi:10.1142/S1230161208000079
6. Dupuis, F.: The decoupling approach to quantum information theory. PhD Thesis, University of Montreal, April 2010. arXiv:1004.1641 [quant-ph]
7. Abeyesinghe, A., Devetak, I., Hayden, P., Winter, A.: The mother of all protocols: restructuring quantum information's family tree. Proc. R. Soc. A (2009). doi:10.1098/rspa.2009.0202