Review of the book

"Classical and Quantum Information Theory"
by Emmanuel Desurvire
Cambridge Univ. Press, 2009

ISBN: 978-0-521-88171-5

M. Frederic Ezerman
Centre for Quantum Technologies, National University of Singapore

August 2013

1 Summary of the review

This is a review of Desurvire's introductory text designed for telecom scientists entitled *Classical and Quantum Information Theory*. The author's stated target audience covers telecom engineers, investors and entrepreneurs, decision makers from private sectors or from government agencies. His rationale is that those with deep professional and administrative interest in the telecom industry often are not exposed to the the quantum sides of information theory and its potentials to revolutionize the field in the (hopefully not too far) future.

The book tries to convince telecom practitioners that quantum information theory (QIT) is a field with real engineering worth and perspectives to shape the future, and not just some kind of cool, academic plaything. Classical Information Theory (CIT) and QIT share many background concepts. In a sense the two great theories, namely Information Theory and Quantum Mechanics have somehow reach each other, in most unexpected and elegant ways. It is in linking and explaining this merging of these two great streams Desurvire's book takes its place.

By now there are many textbooks available treating and or combining classical and quantum information theory. Most are directed towards specialists or would be specialists so the treatment one often finds is highly technical and can be intimidating to many not having sufficient background mathematics, computer science, quantum mechanics, optics, and information theory. This is where this book can serve as a useful come hither kind in one's first few encounters with QIT.

This is an introductory book that tries to appeal to as broad an audience base as possible. The trade-off is that the treatment covers only the very basic materials in each topic. Those with interest in a specific topic or a small set of related topics will quickly find that their thirst is left unquenched and that the coverage in most part are lacking in depth.

2 Summary of the book

The book's coverage is extensive. The contents are divided into roughly two parts. The first two chapters of the book provide a refresher course on probability. Chapters 3 to 14 form the treatment of classical information theory. Chapters 15 to 24 cover quantum information theory. Chapter 25 caps the book with a treatment of cryptography from both classical and quantum perspectives. Technical proofs are often relegated to the appendices. There are altogether 25 appendices in the book. Chapter 21 has the most number of appendices with 4 of them, followed by Chapter 4 with 3.

What the book deliberately omits are two key issues: the effects of quantum decoherence and the physical implementations of quantum circuits. The reason the author puts forward is that the experimental domain is still at its infancy.

In the first part of the book, the author expounds on fundamental topics in classical information theory such as entropy, Shannon capacity theorems, data compressions, error-correcting codes, and channel capacity theorems. Notable is the inclusion of Kolmogorov complexity and Turing machines in this part.

Chapter 15 marks the transition into the second part of the book. Reversible computation is the chosen topic to kick start the tour. Then come the now standard list of topics: quantum bits and gates, quantum measurement, quantum algorithms, and quantum Fourier transform. Along the way, the topics of superdense coding and teleportation, the algorithms of Deutsch-Jozsa, Grover, and Shor are discussed in considerable details to show what common concepts they share with their classical counterparts and what uniquely quantum about them that has no classical analogue. The topics of entropy, data compression, channel capacity, and error correction in the quantum set up take one chapter each, consecutively.

Arguing that it is most beneficial to consider cryptography within the combined framework of classical and quantum, in the last chapter the author discusses how to secure information against unauthorized access and tampering both when the ingredients are bits and qubits.

3 What is the book like?

This is a gentle text, friendly to people who are interested in but are not yet sure if they have the necessary background to dip their toes into the very interdisciplinary field of QIT. The exposition is clear, with plenty of illustrative examples and ample historical background. In this sense the book is very useful to orient a newcomer to the landscape.

The book comes supplied with the necessary math and physics background so it assumes very little background on the part of the readers. The pacing is more or less even. More technical parts come with warning of its level of difficulty and supplemented with appendices.

In general, the text is engaging and friendly. It encourages the readers to think concretely. There is a wealth of original and practical examples that can delight even seasoned practitioners and experts. There are plenty of commendable innovations in its descriptive approach. If a topic can be found in this book then it can be safely assumed that it is well explained. My favorite is Chapter 20 on Shor's Algorithm that comes with detailed explanation, nice examples and illustrations. I have not encountered any better exposition from other sources thus far.

4 Would you recommend this book?

The most delightful feature of the book in my opinion is how the illustrations and examples provided really fit into the author's discussions of the topics. Having read several introductory textbooks on either and both classical and quantum information, I find this book the most successful in integrating illustrations and examples.

I would recommend the book to the following audience:

① Beginning students looking for a broad view of possible areas of concentration and their interconnections.

② Telecom practitioners with experiences and knowledge in aspects of classical information theory with interests in knowing what the corresponding concepts are in the quantum world and what possible benefits they can gain from exploiting the unique features of quantum mechanics useful for possible future telecom applications.

③ Future or present policy makers seeking more clarity on the significance of and possible contribution of quantum information theory.

④ Entrepreneurs with interests in telecom looking for sound background knowledge to make informed investment decisions in the emerging areas of quantum technologies.

Experts looking for ready reference in technical aspects of quantum information theory and advanced graduate students making their ways into the frontiers of hot research topics, however, may find the treatment lacking in both depth and width.

5 Some Suggestions

What I feel had not been mentioned adequately is how explorations in QIT help shed light on open problems in CIT and provide better proofs and or explanations on known classical results. There are two examples that can be mentioned. The first is that QIT in many instances supplies quantum proofs for classical results. Some of these proofs are for new results while most are for known results. The second example is how the studies of quantum error-correcting codes renew interest in the studies of additive codes and in refining the bounds on the distances of the dual of well-known classical codes.

To be included in the errata list: Chp. 24 Section 3, in the title and in the first paragraph (see p. 509), should be *Steane* not *Steine*. Please correct it in the table of content as well.

The reviewer is a research fellow at CQT at NUS, working mostly in the area of coding theory and cryptology, both classical and quantum.