Review of the book

"Quantum Computation and Quantum Information"

by Michael A. Nielsen, Isaac L. Chang

Cambridge University Press, 2010

ISBN: 978-1-107-00217-3

Maria Cristina Onete
CASED (TU Darmstadt) & INRIA/IRISA Rennes

1 What the book is about

This book provides a thorough introduction to quantum information theory and quantum computation in general, especially covering the theoretical and computational, rather than experimental, aspects of these fields. The particular strengths of the volume are: the completeness of both basic and more advanced aspects of quantum computation and theory (including simple topics such as qubits and qubit gates, but also the more advanced quantum Fourier transform and several quantum search algorithms), the well-chosen and broad spectrum of application fields (from more classical optical experiments to Shor's algorithm, NMR, and ion traps), and the thorough assessment of quantum information theory, in particular with respect to noise, error correction, and cryptographic algorithms. Another important quality of this book is that it provides new information to almost any reader, whether their background is computer science, mathematics, or physics (i.e. the three "typical" sub-backgrounds that meet in the study of quantum information theory).

The book is divided into three parts: Fundamental Concepts, Quantum Computation, and Quantum Information Theory. This division is also shown in detail in the Preface, and is succinctly described below:

- **Part I:** Fundamental Concepts:
  - Chapter 1: introductory concepts such as qubits, qubit computations, qubit gates, Bell states, quantum algorthms (quantum parallelism, Deutsch's algorithm, the Deutsch-Josza algorithm), some quantum information experiments (Stern-Gerlach), and basic quantum information problems and prospects. This chapter will provide the basic notational and conceptual background for a reader unfamiliar with quantum computation.

- Chapter 2: some basic quantum-mechanical concepts, such as linear and Hermitian operators, tensor products (such concepts might be familiar for a reader with a background in mathematics, but could provide a necessary formal background for other readers), the postulates of quantum mechanics, quantum states and measurement (concepts a physicist might be familiar with already, but which may provide novelty for other readers), superdense coding, the reduced density operator, Schmidt decompositions, and EPR pairs.
- Chapter 3: some introduction to computer-scientific concepts, such as Turing machines, circuits, and complexity classes, including an introduction to decision problems in P and NP, and concepts such as energy and computational costs. The ideas presented in this chapter will be useful when analyzing applications such as Shor's algorithm, which solves the factoring problem. Such concepts are particularly useful to readers who do not have the corresponding backgrounds in computer science.

- **Part II:** Quantum Computation:

  - Chapter 4: which builds on the concepts of chapters 1 and 2, introducing more in depth quantum algorithms, qubit operations, qubit gates, quantum circuits, and finally, notions of quantum simulation.
  - Chapter 5: which introduces the quantum Fourier transform, with applications in order-finding and factoring, and other, more general applications, such as: period-finding, discrete logarithms, and the hidden-subgroup problem.
  - Chapter 6: describing quantum search algorithms, in particular showing the advantage of the quantum versus the classical approach with respect to computational speed in the NP complexity class. The final subsections of the chapter could be particularly interested for readers familiar with complexity theory, as they explore the optimality of quantum search algorithms and the limits of black-box use of the algorithm.
  - Chapter 7: which is a more practical chapter, describing the physical realization of quantum computers. This chapter is interesting for any reader who is sufficiently familiar with theoretical concepts of quantum mechanics and quantum information theory, but who wishes to understand the problems in the practical construction of quantum systems, and in particular, more practical manifestations and visualization of quantum systems. The chapter describes harmonic oscillator quantum computer and the optical photon quantum computer, then describes topics such as: optical cavity quantum electrodynamics, ion traps, and NMR.

- **Part III:** Quantum Information:

  - Chapter 8: elaborating on the topic of noise, quantum noise (with examples in the context of quantum operations, applications such as quantum process tomography), and some limitations of the quantum operations model.
  - Chapter 9: describing in detail how to measure the distance between quantum states, with respect to trace distance and fidelity.
  - Chapter 10: which shows aspects of quantum error-correction, from the theory of quantum error correction (Section 3), to constructions of quantum codes (Sections 4 and 5), and fault-tolerant quantum computations (Section 6).
  - Chapter 11: describing concepts of entropy (with basic properties, conditional entropy, and mutual information), Shannon and Von Neumann entropy, and the mode advanced idea of strong subadditivity. This chapter is best understood by those who already have some knowledge of probability theory and quantum physics.
  - Chapter 12: which concludes the book by describing concepts of quantum information theory, such as distinguishing quantum states (the Holevo bound), data compression (Shannon's noiseless channel coding theorem, Schumacher's quantum noiseless channel coding theorem), classical and quantum information transmission over noisy (quantum and classical) channels, the advantage of entanglement, and aspects of quantum cryptography, including quantum key distribution.

2 What is the book like (style)?

This book is not overly dense, but moves at a quite fast pace. It is not a self-standing book, in the sense that a basic background in selected areas of mathematics, computer science, and physics is somewhat necessary in order to fully grasp more advanced topics. It is for instance not quite clear for some time, for the unversed reader, that quantum computation and quantum information theory is a model meant to describe the phenomena observed in e.g. the Stern-Gerlach experiment. The chapters are logically written and thorough, but it is often easy to lose track of the big picture. At such time, the chapter introductions, summaries, and the initial introductory chapter are invaluable. The book also contains numerous exercises, which are not always difficult, but always provide insight into the theory presented thus far.

Though quite a comprehensive guide to quantum information and computation, this book is written in an accessible style, with numerous explanations and exercises. Four appendices also provide some much-needed background in e.g. number and probability theory. The information could be divided into: theoretical representation (e.g. the computation model, qubits, qubit gates, and circuits), practical and experimental representations (e.g. the Stern-Gerlach experiment,

Chapter 7), and applications (culminating with quantum cryptographic concepts). Another natural division is: mathematical information, complexity theory, and quantum physics.

One of the book's best qualities is the remarkably logical and systematic style in which the authors present quantum information and computation systems. This is both a thorough and detailed book, and one which is very interesting and easy to read. It is remarkable that even a reader with a good understanding of selected topics of quantum information and computation may still find this book useful.

3 Would you recommend this book?

I would heartily recommend this book to anyone who is interested in quantum information and quantum computation. However, whereas the book serves as a good reminder to readers who have basic knowledge of e.g. linear algebra, complexity theory, or quantum physics, I think it is difficult for a reader fully unfamiliar with such topics to both understand the basics and move on to advanced topics in this book within a reasonable time. Thus, it is my recommendation that readers interested in this book should first build a basic understanding of the topics in the Appendices and at least a half of the topics presented in the first three chapters.

The reviewer has completed a Ph.D. at the Center for Advanced Security Research Darmstadt (CASED) and is currently a researcher at IRISA/INRIA in Rennes.