Quantum Information and Computation, Vol. 2, No. 2 (2002) 177–178

BOOK REVIEW

on

Introduction to Quantum Computation and Information

edited by Hoi-Kwong Lo, Sandu Popescu, and Tim Spiller

World Scientific, 1998 (Paperback edition in 2001)

Paperback $38.00 (364 pages) ISBN: 981024410X

Introduction to Quantum Computation and Information, first published in 1998, was one of the first of what has since become a slew of textbooks on quantum computation. It has aged well, and remains one of the better introductory books on quantum information. It is a collection of articles written by experts covering most of the basics of the field. While the articles are individually of high quality, the book as a whole suffers from a lack of coordination between them. Most of the authors are physicists rather than computer scientists, and consequently the writing style and choice of subjects will appeal more to those readers with a background in physics. While it has a difficult time competing with Nielsen and Chuang's textbook (reviewed in QIC Vol.1, No.2, September 2001) or John Preskill's on-line lecture notes (http://www.theory.caltech.edu/people/preskill/ph229/#lecture), *Introduction to Quantum Computation and Information* can still provide newcomers with an excellent grounding in the field.

The history of the study of quantum information can be divided into three eras. In the earliest, "Pre-Shor", era (before 1994), quantum computation was an obscure field, of interest only to a few people. The years 0-3 Post-Shor (1994-1997) were marked by explosive growth in the community and rapid scientific progress, including the discovery of Shor's and Grover's algorithms, the invention of quantum error correction and fault-tolerant quantum computation, and breakthroughs in quantum cryptography and the experimental realization of quantum computers. By 1998, the study of quantum information had entered the third era. Since then, the field has continued to grow rapidly, but progress has been more incremental than fundamental.

Introduction to Quantum Computation and Information was written at a propitious time, just late enough to report the breakthroughs of the early Post-Shor years. The choice of topics is by and large good, which accounts for the book's longevity in a field which has nearly tripled in size since it was written (in 1997, the quant-ph e-print archive had 689 submissions; in 2001, there were 1911). The book begins with a brief introduction to quantum mechanics, and continues with chapters on entanglement, quantum information theory, theoretical and experimental quantum cryptography, quantum algorithms, error correction and fault-tolerance, and experimental implementations. These still cover the main subjects one would choose today to get a good overall grounding in the field; only the experimental quantum computation chapters substantially show their age, due to subsequent progress in both experiments and proposed implementations. While the other chapters necessarily omit various tricks and techniques, some quite useful, that have been discovered in the past few years, they still contain most of the vital background a new researcher would need. Particularly noteworthy are Adriano Barenco's careful discussion of Shor's algorithm, and John Preskill's description of topological fault-tolerance, which remains the best introduction to that subject.

The coverage of the Pre-Shor era is, by contrast, remarkably scanty. While quantum data compression has excellent coverage (first a brief description in the chapter on entanglement, followed by a much more detailed one in Richard Josza's chapter on quantum information theory), Holevo's theorem on the classical capacity of quantum channels barely rates a mention. Quantum Turing machines are not mentioned at all; perhaps this is not a critical omission, however, since they are rarely used nowadays. More serious is the lack of any systematic discussion of universal sets of quantum gates (which also falls into the earliest part of the Post-Shor era). Instead, each author invokes whichever universal set is needed for the problem at hand. Consequently, this important information is scattered throughout the book and not emphasized anywhere; it is quite possible a novice reader could finish the book without absorbing even a single universal set. No doubt this is a subject that fell through the cracks when topics were parcelled out to the chapter authors.

A lack of coordination shows in other ways as well. For instance, quantum teleportation is invoked in the chapter on entanglement (by Sandu Popescu and Daniel Rohrlich), but is not described in detail until the following chapter. A number of basic tools — density matrices, the no-cloning theorem, the Schmidt decomposition — are described multiple times, sometimes in great detail. Preskill's chapter on fault-tolerance recapitulates many of the basics of quantum error correction described in the previous chapter by Andrew Steane. The chapters also vary considerably in detail and many are poorly proofread. Luckily, the genesis of this book as a collection of separate chapters shows itself more often as redundancy than omissions.

While it lacks the heft of the Nielsen and Chuang textbook, *Introduction to Quantum Computation and Information* still manages to fulfill the promise of its title. Its relatively brief length means there are many topics that only get a short treatment or none at all: for instance, channel capacity only rates a brief mention, and upper bounds on quantum algorithms even less. This is inevitable with a field as diverse as quantum information, so should certainly not be considered a criticism. Despite its age, this book remains an excellent way to learn the basics of quantum information.

Daniel Gottesman (gottesma@eecs.berkeley.edu)
Computer Science Division
University of California, Berkeley, CA 94720, USA