Quantum Information and Computation, Vol. 5, No. 2 (2005) 178–180

BOOK REVIEW

on

Principles of Quantum Computation and Information
Volume 1: Basic Concepts

by Giuliano Benenti, Giulio Casati, and Guiliano Strini
World Scientific, 2004
Paperback $34.00 (256 pages) ISBN: 981-238-858-3

The goal of the new textbook *Principles of Quantum Computation and Information. Volume 1: Basic Concepts* is, according to the blurb on the book's back cover, to provide "a useful and not-too-heavy guide" to quantum computation and information and to provide a "simple and self-contained introduction [requiring] no previous knowledge of quantum mechanics or classical computation." The intended audience of this book consists of students in a "one-semester introductory course in quantum information and computation, both for upper-level undergraduate students and for graduate students." This review will serve as a guide to the contents of this volume, and in particular what role the book can serve in the quantum information science community.

Volume 1 consists of four chapters, introduction to classical computation, introduction to quantum mechanics, quantum computation, and quantum communication. Volume 2 (which I am not reviewing here and which has not yet been released) includes chapters on quantum information theory, decoherence, quantum error-correction and first experimental implementations.

Chapter 1 - Introduction to Classical Computation (pp. 9-47)– This chapter begins by introducing Turing machines, and discusses various aspects of Turing machines (the Church-Turing thesis, universal Turing machines, probabilistic Turing machines, and the halting problem.) These subjects are discussed in a clear and introductory manner. To give one an idea of the depth here, the construction of a universal Turing machines is not shown, for example, but a basic Turing machine which adds in unary is explicitly given. After introducing the Turing machine, the authors discuss the circuit model, introducing some basic elementary gates, discussing universal gate sets, and then move on to computational complexity. Again, to bracket the depth in the book, we note that the notion of a circuit family (uniform or otherwise) is not discussed here, but the basic complexity classes are covered (**P**, **NP**, **PSPACE**, **BPP**, **BQP**.) Here, unfortunately, the authors introduce a use of the big-O notation to mean both an upper and lower asymptotic bound which is not standard in computer science. In two optional chapters, the authors discuss deterministic chaos and Kolmogorov complexity, which are nice additions to the basic introduction, before moving on to the final sections which discuss Maxwell's demon, the cost of information erasure, and reversible computation.

Chapter 2 - Introduction to Quantum Mechanics (pp. 49-97)–This chapter begins with a basic description of the Stern-Gerlach and Young two-slit experiments. After these motivating examples, the authors give a concise introductions to linear algebra: going from vector spaces, to diagonalizing Hermitian matrices, to tensor products in twenty-nine pages. While there are eight exercises in this section and the section is "self-contained and no previous knowledge of linear algebra is required," for someone who has never seen linear algebra before, this section may be a bit rough. More exercises would have been helpful here. For comparison, in *Quantum Computation and Quantum Information* by Michael A. Nielsen and Isaac L. Chuang, a similar introduction provides fifty exercises (although to be fair, the eight exercises in this book are also presented with solutions.) After the rush through linear algebra, the authors present quantum theory from the perspective of three basic axioms. These basics are enough to introduce quantum states, unitary evolution, and projective measurements. Density matrices, generalized measurements, and POVMs are not covered here, but are listed as being covered in Volume 2. There are five exercises in this section. The chapter concludes with a discussion of the EPR experiment and Bell inequalities (via the CHSH inequality.)

Chapter 3 - Quantum computation (pp. 99-187)–This chapter begins by introducing the qubit, especially as represented on the Bloch sphere, and single qubit rotations. Universal quantum gates are introduced including the standard two level proof as well as a not so standard proof based on the CS decomposition (C and S stand for cosine and sine.) The linear error rate of composing unitary gates is addressed, but the level of detail on the subject of universality is not so deep as to delve into the Solovay-Kitaev theorem. Classical reversible circuits are then introduced (function evaluation and an adder) as a prelude to the Deutsch and Deutsch-Jozsa algorithm. Grover's algorithm is introduced via the one-in-four search and then is discussed in the now standard geometric picture of rotating the initial state to the target state. The chapter then moves on to the quantum Fourier transform and its application to phase estimation, eigenvalue estimation, and period finding. It is not explained why order finding breaks the RSA cryptosystem. Quantum simulation of quantum dynamical systems is then discussed with optional material on the quantum baker's map, quantum sawtooth map, and dynamical localization. Finally, a survey of the earliest experimental implementations of quantum computers is given. This consists of a short discussion of Rabi flopping and a two qubit Ising interaction followed by a list of eight physical implementations with short one paragraph descriptions of these implementations.

Chapter 4 - Quantum communication (pp. 189-214)–The final chapter begins by discussing some basic cryptography including one-time pads and public key cryptography including RSA. Moving back to the quantum world, the authors then discuss the no-cloning theorem and give a description of the two quantum cryptography protocols BB84 and E91. The security of either of these protocols is not proved. The authors conclude by discussing dense coding, teleportation and give a brief page to experimental implementations of quantum communication protocols.

The book contains forty nine examples with solutions. In the order of the chapters these problems are divided as three, seventeen, twenty-two, and seven. The problems are uniformly well stated and the level of the problems is fair for someone who is new to the field of quantum computation and information.

Returning now to the purpose of the book, how well does this book succeed in being a "simple and self-contained introduction" and what role can it serve in the quantum information science community? The strength of the book is in its clear and straightforward presentation. As an introduction to the field of quantum computation it works quite well and covers many, but not all, of the basics. The authors should be commended for writing such a readable book.

On the other hand, the level of detail in the book is not high enough to merit using this book for anything other than an introductory course. At times, the book will be troublesome even for the introductory student, who may be frustrated by assertions without proof (as for, example, in not explaining how factoring is achieved by order finding, or in not giving the details of why quantum cryptography is secure.) I have difficulty imagining using this text for a graduate level class, as is claimed on the back cover. The book is too cursory for a graduate student whose intellectual sophistication can handle something much more challenging.

So, I believe that if you are looking for a textbook to teach an introductory course in quantum information science course, then this a good textbook to consider. But if you are aiming for an audience who wants more than an introduction, or are a researcher who wants a good reference book, then this book is probably not for you.

Dave Bacon (dabacon@santafe.edu)
Santa Fe Institute, Santa Fe, NM 87501