3. *Branching Programs and Binary Decision Diagrams* by Wegener.

4. *When Least is Best: How Mathematicians Discovered many clever ways to make things as small (or as large) as possible* by Nahin.

5. *Stories about Maxima and Minima* by Tikhomirov.

6. *Decision and Elections: Explaining the Unexpected* by Saari.

7. *Creative Mathematics* by Wall

8. *Is Mathematics Inevitable? A Miscellany* Edited by Underwodd Dudley.

9. *Comprehensive Mathematics for Computer Scientists 1: Sets and numbers, graphs and algebra, logic and machines, linear geometry* by Mazzola, Milmeister, and Weissmann.

10. *Difference Equations: From Rabbits to Chaos* by Cull, Flahive, and Robson.

11. *Mathematical Tools for Data Mining* by Simovici and Djeraba.

12. *A Concise introduction to Data Compression* by Salomon.

13. *Practical Text Mining with Perl* by Roger Biliosly.

14. *The space and motion of communication agents* by Milner.

Review of[2]
Quantum Computation and Quantum Communication:
Theory and Experiments
Author of book: Mladen Pavicic
239 pages, Springer, $88.00
Author or Review: George Hacken

1 Introduction

Though post-relay and post-vacuum-tube digital computers are 'quantum' in the sense that Quantum Mechanics underlies solid-state (in particular, semiconductor) physics, Quantum Computing could, with my apologies to quantum field theorists, fairly be characterized as Computing's 'second quantization.' Pavicic's book achieves its own characteristic balance between the complementary attributes, depth and breadth, such that algorithmists and computation theorists will be reading both within and very much around their subject as that subject is conventionally construed. (James D. Watson advises in his recent book[3] that we should indeed "read around" our subject.) The book's preface states that "the theory of the field leads the experiments in a particular way .... As a consequence, both mathematics and physics are equally essential for any approach in [sic] the field and therefore for this book as well."

[2] ©2009 George Hacken

[3] *Avoid Boring People*, Random House, 2007

Quantum Computation and Quantum Communication is subtitled *Theory and Experiments*; it comprises three chapters: Chapter 1, *Bits and Qubits*, is an explication of computation-theory as built up from, and related to, states that are quantum-mechanical ('coherent') superpositions of 0s and 1s, these latter being construed as quantum-mechanical Hilbert-space basis states (qubits) $|0>$ and $|1>$ that are subject to Cartesian-product juxtaposition for the case of higher dimensions. Chapter 2, *Experiments*, is a substantial enumeration of evidence for, and possibilities of, realizable quantum computers. Chapter 3, *Perspectives*, is a synthesis and elaboration of the first two chapters, ending in a section titled *Quantum Turing Machines vs. Quantum Algebra.*

As this review is at least *intended* specifically to serve the SIGACT community, I'll give my answer here to a thought-experimental question that I posed to myself after having read the book: "Quick! Is this a physics book or is it a computation-theory book?" My 'gut' answer, i.e., the eigenstate that the question ('measurement') forced me into was $|\text{Physics}>$. This is, of course, an incomplete characterization of the book, as the book gives ample evidence, via counterpoint and interleaving, of its author's and his colleagues' erudite mathematico-theoretical work in Computation Theory, which a good part of the book also reflects in a 'survey' sort of way with what I deem as pockets of mathematical depth sprinkled throughout and appearing especially at the end of the book.

I recall nodding in recognition when Donald Knuth wrote (somewhere and some time ago) that when he works in pure mathematics it has an entirely different 'feel' from that of computing, i.e., algorithmics *per se.* (For what it's worth, I have always found computing science to be impossible to distinguish from mathematics, but that's *my* problem.) Well, the pervasive physics parts of Pavicic's book, with their beam-splitters, polarizers, radiation by stimulated emission ..., gave me the ultimate physics-feel, i.e., *déjà vu*: Physics courses, even highly theoretical ones, generally come to grips with the non-Platonic reality of their subject, the infant String (a/k/a M) Theory to the contrary notwithstanding. Physics is inductive and, at large, does not *depend* on proof, but on evidence. This observation goes equally well for the theoretical-physics parts of Pavicic's book, in which P.A.M. Dirac's austere (but standard) bra-ket notation is used as a 'given.' The great Dirac is in fact quoted (elsewhere) as having said, "I am not interested in proofs, I am only interested in how Nature works," in response to accusations of a promiscuous lack of mathematical rigor. (The rigor was subsequently supplied by Laurent Schwartz, James Lighthill, et al; Dirac's physics remained invariant. Molière was also involved, as Dirac used group theory and Clifford algebra "without previous knowledge of [them]," to quote Dirac's response to an audience-member's challenge, "but you *are* using group theory!")

Pavicic states that the book "is not conceived as a textbook, ... but more as a guide." There is no homework, nor are there exercises, and "most of the required details are elaborated within the main body of the book." Pavicic intends for the reader to profit from a "polynomial complexity," once-through use of his book. The book is certainly not 'how-to,' but serves as an eye-opener, albeit a dizzying one for student and practitioner of 'classical' computing alike, to a genuinely new computing paradigm. The "classical" Turing machine is given enough detail, including formal definition of its deterministic species, to form the basis for at least a superficial notion of the quantum Turing machine's (currently tentative) role in the theory of quantum computation.

The beginning of the book gets right down to the business of computability by summarizing Turing-computability in terms of that abstract machine, and alluding to Church's conjecture that effective computability is what the theories of Turing, Church, Herbrand, Gödel, Kleene, Hilbert and Bernays, Post, and Markov have in common, i.e., are equivalent to. (Church's conjecture, a/k/a thesis is, of course, about the theory, not the theorists.) The important notion in addition to "calculability" (Pavicic's term) is decidability, and Pavicic achieves good cognitive and pedagogical flow to Boolean algebra by pointing out that "few proofs [of decidability and calculability] turned out to be possible for simple theories at the beginning of the twentieth century ...." In proffering the notion of axiom-based proofs, i.e., the theorem-proving or term-rewriting method over the brute-force truth-table-enumeration approach, the author makes the (I suppose) minor error that at least 30 billion truth-values need to be checked in verifying the correct functioning of a 16-bit adder that comprises over 30 boolean variables; the correct answer is more like one billion, as $2^{30} \approx 10^9$. I hasten to add that the prinicple remains illustrated, and that errors are the exception, not the rule, in this book. Pavicic is very clear throughout when he makes a scientific point, however nuanced computation theory *cum* quantum mechanics may be.

There is, in fact, a great deal of educational enrichment of *classical* computation-theory to be had here. Many of us know, for example, that the connectives *and, or, not* can be expressed via the *single* Sheffer stroke, $|$, which is the *nAnd* connective. The author quotes McCune et al's 2002 result to the effect that the *single* axiom $A|((B|A)|A))|(B|(C|A) \equiv B$ is equivalent to the five (depending on how one counts) axioms of Boolean algebra as based on *and, or, not*: closure; commutativity; identities 0 and 1; distributivity; and complements and inverses. (I don't intend to double-check *that*, as I suspect more than the back of an envelope, let alone skill, to be necessary.)

This axiomatic, abstract subsection is followed, in a fashion that is typical throughout the book, by an almost down-and-dirty physics section wherein bits realized by transistors are analyzed for energy dissipation, which is a major limiting factor in achieving speed of computation in physical machines. One major amelioration was industry's elimination of transistor-gate resistive losses via the synthesis of complementary metal-oxide semiconductor (CMOS) gates that are resistor-free (but capacitance-intensive). Pavicic goes on to mention more recent, post-CMOS, innovations it logic-gate technology, and thus segues into what I call an architectural, not technological, problem: irreversible gates. For example, in the Boolean equation $C = A \wedge B$, the 'culprit' in the 'output' C's being 0 (i.e., false) cannot be recovered when an ordinary, i.e., irreversible *and* gate processes inputs A, B. The section on the classical reversible versions of the Boolean operators[4] *not, and, or* prepares the reader for the quantum versions of reversible operations. This abstract, mathematical section is followed by its physics counterpoint, which here involves Gibbsian vector analysis, classical electromagnetic theory, and nonrelativistic quantum mechanics. Though I do not presume that SIGACT members at large have any less of a physics background than I do, I must state that this (and other) physics-intensive expositions are simply incomprehensible without such prior acquaintance; this can lead to a loss of patience on the reader's part, as the physics is anything but self-contained. For example (page 28) the notions of quantum-mechanical pure state versus that of a mixture (which latter is, in my words, doubly statisical), will be lost on the reader whose first exposure to quantum mechanics is this book. The same goes for the motivation behind

[4] I was lucky in this regard to have read Brian Hayes's, *Reverse Engineering*, American Scientist, March-April 2006

the introduction of hermitian and unitary operators (on quantum state-vectors). Of course, the beam-splitter as $\sqrt{NOT}$ gate will be a revelation to any interested party. Pavicic states the two main quantum-mechanical algorithms for classical applications to be factoring of integers (Shor) and search (Grove). A single ten-(decimal)-digit number needs only *one* q-gate, versus the several needed in current digital computing.

The section titled *Technological Candidates for Quantum Computers* is clear about the state of the art: "To date – about ten years after the first experimental implementation of one qubit – most of the numerous proposals for quantum computing prototypes have not been able to implement more than one or two qubits. Thus, one still cannot single out a most promising technological candidate for a future quantum computer." (Recall that, as alluded to above, a qubit $|q>$ is a superposition of basis states $|0>$ and $|1>$: $|q>= a|0> +b|1>, a, b$ complex with $|a|^2 + |b|^2 = 1$.) This is valuable real-world information for all of us, and I dare say that it is all the more credible by virtue of Pavicic's treatment of the physics that underlies quantum computing – however demanding or frustrating the reading of those parts of the book may be. Speaking of physics, I believe that the author is mistaken (in the typographical-error sense, on pages 112 and 117) in attributing *anti*commutation relations to Bose-Einstein (integer-spin) operators and commutation relations to Fermi-Dirac (half-integer spin) operators. Unless I'm missing something, it should be *vice versa*. The section titled *Future Experiments* begins with an enumeration of the DiVincenzo criteria, namely, "five generally accepted requirements for the implementation of quantum computing," plus two "networkability" conditions. The first is scalability, and the last is faithful transmission of qubits between specified locations. *Table 2.1*, page 124, shows how the following technologies currently fare with respect to these criteria: Nuclear Magnetic Resonance; Solid State; Trapped Ion; Cavity Quantum Electrodynamics; Neutral Atoms; Optical; Superconducting; and 'Unique' Qubits. None of them are currently viable for all seven DiVincenzo criteria. Near the end of Chapter 2 is mention of an existing, 18-mile quantum network administered by the Defense Advanced Research Projects Agency (DARPA), which includes quantum cryptography and anti-eavesdropping features.

Pavicic estimates, at the beginning of Chapter 3, *Perspectives*, that the shrinking of computer elements will encounter the quantum barrier by 2025. As quantum computing is "inherently parallel," he expects, by 2012, a 50-qubit computer that can accommodate a quantum superposition of 10^{15} states. The discussion on how 50 qubits evolve together to perform a quantum computation in one step is quite clear as a simple elucidation of the basic nature of quantum computing which, in view of the heterogeneous nature of this book, is a welcome summary. There is also a moderately detailed treatment of quantum communication *per se*, using the standard characters Alice (the transmitter or source), Bob (the receiver), and Eve (the eavesdropper).

The last sixth of the book is the most consistently mathematical and, if I may say so, SIGACT-like. It treats quantum algorithms, quantum algebra, and quantum Turing machines in a way that is closely parallel with their classical counterparts. Here we have our lattices, *C** and *Bear algebras*, and – yes – the Schrödinger equation as discretized for qubits. There is also treatment of a fascinating, purely quantum phenomenon, *counterfactual computation*, which involves non-destructive, interaction-free probing of a quantum state. (I learned this more than four decades ago as "the influence of the possible on the actual" in quantum mechanics; Pavicic tells me it's real!)

Quantum Computation and Quantum Communication is by no means an easy book, and there is no claim that it is. Its eclectic nature alone makes it demanding reading. That it captures its author's single, unified, and expert vision of quantum computing is a great strength. The book will be valuable for researchers, and for neophytes who want to get the 'flavor' of quantum computing, assuming that these latter beginners can keep their self-promises not to succumb to being overwhelmed.

2 Acknowledgement

We would like to thank Joshua Scott for help with the LaTeX.

Review of[5]

Quantum Computing for Computer Scientists
Author of Book: Noson S. Yanofsky and Mirco A. Mannucci
Cambridge University Press, 2008, 368 pages
ISBN-13: 978-0-521-87996-5, Price U$ 70.00

Review by S.C. Coutinho
Departamento de Ciência da Computação
Instituto de Matemática
Universidade Federal do Rio de Janeiro
P.O. Box 68530, 21945-970 Rio de Janeiro, RJ, Brazil.
`collier@impa.br`

1 Introduction

I first heard of quantum computing in 1995, a year after it had come of age. For more than ten years this had been a notion of only theoretical interest; then came Peter Shor's 1994 paper, and all was changed. What he proved was that a quantum computer would be able to factor integers and solve the discrete logarithm problem in *polynomial time*. Since the security of most internet communication depends on the difficulty of solving one of these two problems, his algorithms had a huge potential impact, and soon brought quantum computation into the news.

It was only much later that I learned that the roots of the subject go back to the 1980s, when Richard Feynman began to talk about simulating quantum mechanics with a computer. In a keynote address delivered at the MIT Physics of Computation Conference in 1981 he pointed out that Nature is not classical, and then added that

> if you want to make a simulation of Nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy; [1].

By 1983, Feynman was talking in terms of

> a computing device in which the numbers are represented by a row of atoms with each atom in either of the two states; [2].

[5] ©2009 S.C. Coutinho