Quantum Information and Computation, Vol. 1, No. 3 (2003) 95–96

BOOK REVIEW

on

An Introduction to Quantum Computing Algorithms

by Arthur O. Pittenger
Birkhäuser, December 1999
Hardcover $44.95 (138 pages) ISBN: 0817641270

and

Quantum Computing

by Mika Hirvensalo
Springer, May 2001
Hardcover $44.95 (190 pages) ISBN: 3540667830

and

Classical and Quantum Computation

by A. Yu. Kitaev, A. Shen, and M. N. Vyalyi
American Mathematical Society, July 2002
Hardcover $59.00 (272 pages) ISBN: 082182161X (softcover should be considerably cheaper)

A quick survey on `amazon.com` shows that the number of books on quantum computing ($\gg 20$) is more than 10 times as high as the number of quantum algorithms that we have today (2: Shor's and Grover's). Many people in the field, including this reviewer, feel that Nielsen and Chuang's *Quantum Computation and Quantum Information* is probably the best and most comprehensive of these. Nevertheless, there is room for some other books with different perspectives. Here we review and compare three books that focus mainly on the algorithmic side of the field, and hence can afford to be significantly shorter than Nielsen and Chuang's 675-page volume.

1. Pittenger

Arthur Pittenger's *An Introduction to Quantum Computing Algorithms* reflects its author's own experience in learning the mathematics and theoretical physics required for the subject, as he writes in the acknowledgments. It is generally written in a pleasant and informal style, with much motivation in between the mathematics. Of the three books reviewed here it is probably the most readable.

It consists of three parts of about 40 pages each. The first part (Chapters 1 and 2) covers the computational model: states and operations, some quantum mechanical background, and the circuit model of quantum gates, generalizing classical reversible circuits. The chapter does not go into the issue of approximating arbitrary circuits by a finite set of basis gates. The second part (Chapter 3) reflects the title of the book. It explains the main quantum algorithms: Deutsch-Jozsa, Simon, Grover, Shor, and the generalization of the latter to the Abelian hidden subgroup problem. The chapter is self-contained, except for some of the number theory needed for the classical post-processing and analysis of Shor's algorithm. The final part (Chapter 4) discusses quantum error-correction in detail. It covers the 9-qubit, 7-qubit, and 5-qubit codes, as well as the general framework of stabilizer codes and Calderbank-Shor-Steane (CSS) codes. Fault-tolerant implementation of gates is not dealt with. Still, in just 120 pages this book manages to explain much of the core of quantum computing, and to explain it well.

2. Hirvensalo

Mika Hirvensalo's *Quantum Computing* is more recent but covers quite similar ground. It too is much shorter than Nielsen-Chuang and has a clear computer science focus; one wonders whether Hirvensalo was aware of the earlier Pittenger book, which he does not reference. His style of writing is more formal and mathematical than Pittenger's.

The six chapters of his book explain the circuit model (like Pittenger, without a discussion of universal gate sets), Shor's algorithm, the hidden subgroup problem, Grover's algorithm, and the polynomial method for query complexity lower bounds. As a bonus, the last 80 pages of the book consist of two very extensive appendices. The first covers the mathematical foundations of quantum mechanics. This includes quite a few advanced topics that are not used in the main text, such as an entropic version of the uncertainty relations, Gleason's theorem that every well-behaved assignment of probabilities comes from a density matrix, and a characterization of completely positive maps on density matrices. The second appendix explains some mathematical background: group theory, the discrete Fourier transform, linear algebra, number theory including the continued fraction expansion used in Shor's classical post-processing, and some information theory.

3. Kitaev, Shen, and Vyalyi

The very recent *Classical and Quantum Computation* by Kitaev, Shen, and Vyalyi (KSV) grew out of a course on classical and quantum computing given by Kitaev and Shen in Moscow in 1999. It is a translated and expanded version of an earlier Russian book, which is still available for free at `http://www.mccme.ru/free-books` for those who can read Russian.[*] From a researcher's perspective it is by far the most interesting of the three books, and I will correspondingly be more detailed in discussing it.

The book has three parts: classical computing, quantum computing, and solutions to exercises. The classical part is quite excellent. In a clear and intuitive style of writing it describes the essentials of the theory of classical algorithms and complexity. This covers Turing machines, circuits, reversible computing, NP-completeness, randomized algorithms, and the polynomial hierarchy. This 30-page exposition also includes some more advanced results like $BPP \subseteq P/poly$ and $BPP \subseteq \Sigma_2$.

The quantum part of the book (Chapters 6 to 15) devotes about half of its 120 pages to a

[*] The translation no doubt caused the occasional absence of the definite article in the English text.

thorough exposition of the quantum circuit model, including representing or approximating arbitrary unitaries by means of elementary gates, quantum computation with mixed states, and a detailed account of measurement. After all the details of the circuit model are in place, the book continues in Chapter 13 to describe the phase estimation technique (originally due to Kitaev) and the way it can be used to solve the Abelian hidden subgroup problem, including factoring and discrete logarithms. Chapter 14 deals with a quantum version of the complexity class NP and a complete promise problem for this class. Finally, Chapter 15 describes quantum error-correcting codes and ends with a brief description of Kitaev's work on toric codes and anyons, where error correction would be a natural property of the underlying physical system itself.

Apart from its conciseness and rigor, one of the main strengths of this book is the attention it gives to Kitaev's contributions to quantum computing. These include a detailed analysis of efficient approximation of arbitrary circuits using only gates from a specific finite basis, the Abelian hidden subgroup problem, quantum NP-completeness, and toric codes. These topics are explained in much detail and with many subtleties and insights that are often glossed over in other presentations—and for things like quantum NP-completeness there *is* no other presentation. A good understanding of the quantum part of this book (including the exercises and their solutions) will provide the researcher with invaluable insights and tools for new research.

At the same time, this bias towards Kitaev's quantum work may also be viewed as a weakness of this book. Even if one restricts attention to computer science aspects of quantum computing, various things are missing. The work of a number of key researchers is completely ignored, including that of Andris Ambainis, Harry Buhrman, Daniel Gottesman, Peter Høyer, Richard Jozsa, Michele Mosca, and Umesh Vazirani. Between them, these people have contributed a large fraction of the main results on quantum algorithms and complexity, yet none of their papers is even cited. The Deutsch-Jozsa algorithm is absent; there is nothing about the applications of Grover's algorithm in counting, collision-finding etc. The result that Grover's algorithm is optimal for quantum search is only mentioned in passing and the paper that first proved this (Bennett, Bernstein, Brassard, and Vazirani "Strengths and weaknesses of quantum computing") is not cited. There is nothing else on lower bounds, virtually nothing about quantum communication or communication complexity, no quantum cryptography, etc. The book's cover suggests using it as a textbook for a graduate course on quantum computing, but I fear that such a course would give a somewhat biased view of the field.

A second problem with using this book for a course is the disparity between its classical and quantum parts. These are apparently written predominantly by different authors. The classical part is generally very well and intuitively written, and does not presuppose much. On the other hand, the quantum part is a much less smooth read. It is significantly more demanding and not quite self-contained. For instance, the proof that the standard basis of elementary gates can efficiently approximate circuits over other bases (Section 8.3) assumes some knowledge of Lie groups and Lie algebras, and the last sections about error-correcting codes assume some acquaintance with homology of manifolds. Again, this may be problematic when using KSV as a textbook for a course, since most students will not be very familiar with this material. As another example, the use of quantum phase estimation in quantum algorithms is originally due to Kitaev, but the exposition of his method in the subsequent paper "Quantum algorithms revisited" by Cleve, Ekert, Macchiavello, and

Mosca is much more clear than the exposition given here.

The above points notwithstanding, a lot can be learned from this book; much more than from the other two, but it requires a greater effort by the reader. This is fine when that reader is a researcher—and that is probably where the book will be used the most: as a valuable resource for people who want to look up or learn the intricacies of things like the circuit model, quantum NP-completeness, etc.

4. Comparison and conclusion

The overlap between these three books is quite large. All three are explicitly oriented towards computer science, devoting most of their pages to the quantum circuit model and the main quantum algorithms. The contents of the Pittenger and Hirvensalo books in particular are very close. The main differences are that Pittenger has a chapter on error-correction and his style of writing is somewhat more informal and intuitive, while Hirvensalo has a chapter on lower bounds and some more mathematical background (such as continued fractions).

The KSV book offers more than the other two books. This includes a succinct but very nice introduction to a lot of classical complexity theory, a more in-depth discussion of the quantum circuit model, and topics like quantum NP-completeness and toric codes that are not readily available in any other books. On the downside, I found its quantum part more demanding and harder to read at times than the other two books.

All three books are precise and reasonably succinct introductions to the algorithmic aspects of the field of quantum computation. As such they will be most useful to computer scientists and mathematicians who want to learn about the algorithms without being bothered too much by the physics. The books are suitable for a 1-semester course on quantum algorithms (omitting some of the more advanced sections in the case of KSV). All three books have many exercises, but KSV is the only one that gives the solutions as well. Hirvensalo discusses some lower bounds but Pittenger and KSV do not, and none of the books treat communication-based topics like quantum cryptography, channel capacities, or communication complexity, nor the various applications of Grover's algorithm.

So, which book to choose? If you want a very accessible first introduction to quantum algorithms, I would recommend Pittenger's book. If you prefer more formal mathematics, Hirvensalo also gives a good first introduction to roughly the same topics. If you have sufficient mathematical maturity and/or are prepared to do some work while reading, then go for the KSV book. For everyone with a broader interest in quantum computing (including quantum information theory), I would still recommend Nielsen and Chuang over these books. It contains *much* more material, is very readable, and not significantly more expensive than the three books discussed here.

Finally, to all those currently working on yet another book about quantum computing: what this field needs most is more algorithms, not more books.

Ronald de Wolf (`rdewolf@cwi.nl`)
CWI
Kruislaan 413
1098 SJ Amsterdam
The Netherlands