Review of the book

"Quantum Computer Science" by N. David Mermin Cambridge University Press, 2007

ISBN: 978-0-521-87658-2

G.A. Kohring

1 Summary of the review

Quantum Computer Science is a well written text book covering the theoretical aspects of quantum computer science. The monumental algorithms from Shor and Grover are discussed in detail as are a number of other interesting algorithms including those for error correction and quantum cryptography. As a text book it is aimed at the advanced undergraduate or graduate student, but will also be of interest to professionals looking for a clear, concise introduction to this fascinating subject matter.

2 Summary of the book

The book starts off with a short digression into etymology whereby the author explains his preference for denoting a quantum bit as, *Qbit*, instead of the more common, *qubit*. (In deference to the author, we will use his notation in this article, but a quick look through the literature suggests he is fighting a losing battle.)

In the first chapter, the classical bit, referred to in the book as a *Cbit*, is cast in the Dirac notation borrowed from Quantum Mechanics. For the Cbit, this is certainly overkill, but it helps the reader to transit from a mental reference frame in which a bit is a variable taking on two values to frame in which a bit is associated with a state in a two-dimensional Hilbert space. While a Cbit can only take on one of the two orthonormal basis vectors in this space, the Qbit can assume any linear combination of the states $|0\rangle$ and $|1\rangle$.

The second chapter covers the simplest examples of quantum computing, demonstrating the differences between it and classical computing. In particular, Deutsch's problem, which launched the whole quantum computing movement 25 years ago is discussed in detail. Although of theoretical interest, most of the algorithms discussed in this chapter have no practical applications.

It is the third chapter entitled "*Breaking RSA Encryption*" that will probably be of most interest to IACR members. Here Prof. Mermin describes in great detail Shor's algorithm for factoring numbers along with its application to breaking the standard RSA public key encryption system. Having read this chapter IACR member's can rest much easier. To break RSA using keys containing N *Cbits*, would require a quantum computer with $4N$ *Qbits*, whereas the largest quantum computer to date has only 12 *Qbits*. Whether current designs can be scaled up to thousands of *Qbits* is questionable. (Note: A Quantum computer from the company D-Wave possessing 128 *Qbits* has been in the news of late, but it is not a general purpose Quantum computer and cannot run Shor's algorithm.)

Searching using Grover's algorithm is discussed in the fourth chapter. Again, the author describes this algorithm in great detail. The algorithms of Grover and Shor are the two most important algorithms discovered so far in field of quantum computing, so chapters three and four can be said to comprise the heart of this short book.

The fifth chapter describes quantum error correction. Unlike other applications, quantum error correction is not intended to speed up any classical applications, rather it is needed to ensure the correctness of the output of a quantum computer itself. Quantum computers are inherently noisier than classical computers, so without error correction they would be nearly useless.

Unlike the previous chapters, the final chapter of this book describes algorithms not intended for quantum computers *per se*, but which use quantum effects. Most notable is the discussion of what is called "*Quantum Cryptography*". Basically, this is a quantum mechanical mechanism for exchanging cryptographic key material. Covered in a mere six pages, this may actually turn out to be the algorithm with the highest impact in the short term as it is the most advanced of all quantum algorithms in terms of practical implementations.

Although the book has only 6 chapters, it comes with no less than 16 appendices. In addition to providing some mathematical background, the appendices delve into numerous side issues associated with the algorithms discussed in the main part of the book.

3 What is the book like (style)?

N. David Mermin is a well known physics professor from Cornell University, whose text book on Solid State Physics trained a generation of physicists. Prof. Mermin is also one of those rare University Professors who actually takes his teaching duties seriously. This is clearly evident by the clear, lucid prose used to explain the complex subject matter without a trace of hubris. In part the book is tough slogging given the Dirac notation coupled with graduate level mathematics, but its worth the effort if the reader wants to understand all the fuss surrounding quantum computing at more than just a superficial level.

The reader will not find glossy colored pictures in this highly mathematical treatise, but there are numerous black and white drawings depicting the various quantum circuits discussed in the text. For ease of reading, the book is set in a clear, crisp typeface, including ample white space around the displayed equations. Furthermore, the page margins are wide enough for note taking.

4 Would you recommend this book?

This book is highly recommendable for anyone who wants to learn the theoretical foundations behind quantum computing. Lecturers who want to use the book in their own courses should be aware that they will have to come up with exercises on their own since the book itself offers none.

Unfortunately, the reader will not find any discussion of the practical, though equally difficult question of how to actually build a quantum computer. The author has deliberately desisted from including any discussion of the state of the art in the field of quantum computers, leaving us with a self-contained, though purely theoretical work.

There is one theoretical topic missing from this otherwise excellent book, namely there is no discussion of computational complexity theory. Although the computational complexity of each algorithm is mentioned, there is no cohesive discourse on the subject of where quantum computing sits in terms of the PSPACE hierarchy. While it is understandable that a physicist may not be particularly interested in this topic, it is a major short coming for a book calling itself *Quantum Computer Science.*

The reviewer is an analyst and researcher with Inversik Laboratories in Germany.