Review of:

Colin P. Williams and Scott H. Clearwater, *Explorations in Quantum Computing.*
Springer-Verlag (The Electronic Library of Science), 1998.
xx+307 pages, 78 illustrations, includes CD-rom, ISBN 0 387 94768 X

1 Introduction

This book aims to give a self-contained introduction to the field of quantum computation, "currently one of the hottest topics in computer science, physics, and engineering", as the authors write. It is the first book on the subject. The following description of its contents serves as an overview of the book as well as the field it describes.

Chapter 1. Computer Technology Meets Quantum Reality. Classical computers are built according to classical physics. Over the past 50 years, there has been a steady exponential growth of the power of such computers, which has tremendously influenced our society and economy. This growth has largely been due to the fact that more and more stuff could be squeezed in smaller areas. Such continuous miniaturization, however, will bump into the fundamentally non-classical laws of quantum physics within a few decades. New technology based on quantum mechanics will be needed to keep up the growth of computing power.

Chapter 2. The Capabilities of Computing Machinery. Apart from certain issues in complexity theory, the power of the classical deterministic or probabilistic computer (Turing machine) is fairly well understood: we roughly know what we can and cannot compute.

Chapter 3. Quantum Mechanics and Computers. A rather different model of computation arises if we look at computation according to the laws of quantum rather than classical physics. It turns out that such quantum computers are in some respects remarkably stronger than classical ones. Computers that make use of quantum effects were defined by Paul Benioff and Richard Feynman in the early 1980s, and David Deutsch in 1985 provided the definition of a universal quantum Turing machine.

Chapter 4. Simulating a Simple Quantum Computer. The states of a quantum computer are so-called superpositions of several classical states, allowing the computer to explore many computational paths simultaneously. The computation evolves according to the laws of quantum mechanics. The final answer of the computation is extracted from the computer by means of a measurement, which collapses the superposition to a classical state.

Chapter 5. The Effects of Imperfections. Quantum computers and the states they work on are very vulnerable and sensitive, but imperfections in preparation, evolution or measurement are not impossible to fight.

Chapter 6. Breaking Unbreakable Codes. The greatest success of quantum computing to date is Shor's 1994 algorithm for prime factorization. Whereas factoring is generally believed, though not proved, to be intractable on a classical computer, on a quantum computer we can efficiently find the prime factors of very large numbers. This is particularly interesting because most of current cryptography (notably the RSA algorithm, widely used on for instance the Internet) relies for its security on the assumption that factoring is hard. Accordingly, if a quantum computer can be built, RSA and the things it protects (electronic money!) will fall prey to hackers.

Chapter 7. True Randomness. Other than classical physics, quantum mechanics is a fundamentally non-deterministic and probabilistic theory. Accordingly, a quantum computer can effectively "toss a coin" to generate random bits, something a computer based on classical physics cannot do.

Chapter 8. Quantum Cryptography. As mentioned, quantum computing allows us to break classical cryptographic schemes like RSA, rendering much of current cryptography totally insecure. Fortunately, this danger to our economy can be averted using quantum computing itself: quantum mechanics allows for cryptographic schemes that even a quantum computer cannot crack.

Chapter 9. Quantum Teleportation. Using entangled pairs of qubits (which are correlated despite being far apart) and transmission of classical bits, quantum states can be transmitted faithfully over long distances, something which thus far seemed possible only to the minds of science fiction authors.

Chapter 10. Quantum Error Correction. The biggest problem in actually building a quantum computer is decoherence: because of interaction of a computer with its environment, it is very hard to maintain the coherent superposition of states that a quantum computer needs. However, some solutions for this problem have been developed, notably error-correcting codes which allow a computer to correct errors that arise from decoherence and to work in a fault-tolerant way.

Chapter 11. How to Make a Quantum Computer. Error-correcting codes offer a possible solution to the problem of decoherence, but actually building a real non-trivial quantum computer is a daunting task, which researchers have only just begun to explore. The final chapter discusses some of the proposals and initial experimental work on physical implementations of quantum computers.

2 Strengths

The rise of quantum computation as an important and exciting subfield of physics and computer science began roughly five years ago, Shor's 1994 factoring algorithm being a focal point. By now, the field is still growing extremely fast but also seems to be maturing somewhat, and the need for one or more good books becomes more and more evident. As mentioned already, this is the first book on the subject. Here I will discuss its strengths, in the next section some of its weaknesses.

The book is popularly written and fairly easy to read, avoiding the mathematician's "definition-theorem-proof" style in favor of informal descriptions of techniques and results. The first chapter puts quantum computing in the right economical and social perspective, and the subsequent chapters give a fairly good introduction to the relevant physics. In all, the book gives a nice overview of most of the important issues in quantum computing, particularly valuable for those new to the field. Apart from Grover's algorithm (see below) and very recent developments like quantum communication complexity, the book seems to cover all main topics in quantum computation.

A CD-rom is included which contains simulations of some quantum computations and which allows you to play around a little with the material (though the cryptographic parts are disabled "to insure compliance with U.S. export controls regarding the export of cryptographic software"). Program traces from this CD-rom are often used in the book to illustrate the material.

3 Weaknesses

Apart from some typos and minor inaccuracies (for instance, Gödel's incompleteness theorems are dated 1936 instead of 1931 and the rise of algorithmic information theory is attributed to Chaitin in the 1970s rather than Solomonoff, Kolmogorov, and Chaitin in the 1960s), the main weaknesses of the book concern the computer science aspects of the field. I will mention two.

Firstly, the description of quantum complexity theory, which deals with the quantum analogues of classical complexity classes like P, NP, and BPP, is misleading. Notably, the authors state at least twice (p.40 and 43) that proper inclusion of P in its quantum analogue QP has been proven. This separation, however, is only relative to an oracle and is certainly not "the first definitive complexity separation between classical and quantum computers". Since QP sits in PSPACE, a proof of strict inclusion of P in QP would imply strict inclusion of P in PSPACE, which has been one of the main open problems of classical complexity theory for decades. In fact, proving absolute (non-oracle) separations between classes like P, NP, BPP, PSPACE, QP, or BQP is the main goal of complexity theory, but no such separation between any two of these classes has been established so far. Furthermore, the description of the class NP and its highly important NP-complete members is too imprecise and hence somewhat misleading. For example, the distinction between decision problems and search problems should have been made and the characterization of NP as the class of problems for which candidate answers can be checked efficiently is too informal. It is perhaps telling that the bibliography does not contain any of the many standard textbooks on classical computational complexity theory, such as *Computers and intractability: A guide to the theory of NP-completeness* by Garey & Johnson, or *Computational complexity* by Papadimitriou.

Secondly, the book contains a reasonably good description of Shor's factoring algorithm, but does not explain any other quantum algorithms. Not many such algorithms are known to date, but a book like this should include a detailed description of Lov Grover's 1996 algorithm for efficient database search. This important algorithm is mentioned only twice in passing in the book, and the subsequent results spawned by its discovery are not mentioned at all.

Finally, despite having 1998 as its year of publication, the book only cites papers from 1996 or earlier, and hence is already – perhaps inevitably – somewhat outdated. Some of the more recent technical issues are mentioned but not explained in any detail. In particular, more attention might have been devoted to error-correcting codes and fault-tolerant computation, which is probably the most important development in quantum computing of the last two years.

4 Conclusion

One wonders what the intended audience of this book is. On one hand, the book is neither sufficiently up-to-date nor sufficiently rigorous to serve as a reference work for researchers. On the other hand, the book seems not well suited for a very broad audience either, as at least some familiarity with linear algebra and other mathematics is presupposed. The book does probably suit an intermediate audience of non-expert scientists.

To sum up: Is this a good book? Yes, if you want an informal and fairly readable first introduction to the field of quantum computation; No, if you want a book that provides you with rigorous up-to-date descriptions of the main results of quantum computation. In

particular on the side of computer science there are some errors and omissions. This book does not quite fill the need for a textbook for researchers, which is a pity since this new and very interesting field could definitely use one. Fortunately, rumor has it that several other – probably more research-oriented – books are currently being written by some prominent people in the field.

Ronald de Wolf
CWI and University of Amsterdam