Quantum Computing: On the Horizon?

Quantum Computing

Edited by *Samuel L. Braunstein*

WILEY-VCH, Weinheim, 2000. xiii + 292 pp., hardcover DM 248.00.—ISBN 3-527-40284-5

"Where do we want to go tomorrow?" is the subtitle of the book "Quantum Computing" edited by Samuel L. Braunstein. This permutation of the slogan of a well-known software company implies some promise for the future where quantum computers might solve certain problems in polynomial time, which seem unsolvable by classical computers. As an example let us consider a 400 digit integer number n which should be factored into the product $n = p \times q$ of two prime numbers p and q. This is an "unsolvable" problem with state of the art computers, because it would take about 10^{10} years (about the age of the universe) with current high performance computers. Cryptographic key distribution based on prime factor analysis of such a number is, therefore, absolutely safe. However, it was shown by Shor that a quantum computer could perform this operation in about three years, thus shattering current cryptographic schemes.

This book is not a textbook. Nor is it an introduction to quantum computing. It is written by experts for physicists, computer scientists, and everybody who is interested in the subject. The book consists of a collection of articles on quantum information and computation, where each of the articles has an introductory section, but focuses on specific aspects of quantum computing. The whole collection is wrapped up by a detailed and readable review on quantum computing by Samuel Braunstein.

This section contains book reviews written by invitation from the editor. Suggestions for books to be reviewed and for book reviewers are welcome. Publishers should send brochures or (better) books to the Editorial Office, ChemPhysChem, Postfach 101161, 69469 Weinheim, Federal Republic of Germany. The editor reserves the right of selecting which books will be reviewed. Univited books not chosen for review will not be returned.

Quantum computers don't exist yet, although some basic algorithms have already been demonstrated by experiments. In this sense, we must wait for "tomorrow" for the quantum computers to come. However, the concepts of quantum computing were developed quite intensively in the 1980s and 90s, starting with proposals by Benioff, Feynman, and Deutsch. Since then it was a playground for scientist interested in the basics of quantum mechanics and quantum information processing. Only recently the subject attracted considerable attention when Shor introduced his factoring algorithm for prime numbers. Although the editor claims in the introduction "the subjects discussed in this book include both experimental and theoretical aspects on...quantum computers" the vast majority of the articles is conerned with theoretical aspects.

Just the two contributions on ion traps with the titles "The Los Alamos Trapped Ion Quantum Computer Experiment" by R. J. Hughes et al. and "Experimental Primer on the Trapped Ion Quantum Computer" by D. H. Wineland et al. from Boulder (USA) refer to experimental realizations. Both articles discuss the experimental prerequisites for addressing the electronic states of ions in an ion trap by laser light following a proposal by Cirac and Zoller. Selected ground and excited states act as quantum bits (qubits) and the qubit bus represented by the vibronic interaction of the ions achieves the necessary entanglement of different ion states. Interesting experimental aspects are detailed in both articles. Unfortunately, no quantum algorithm is demonstrated experimentally in these two articles. We obviously must wait for tomorrow. The third article on ion traps with the title "Measurement and State Preparation via Ion Trap Quantum Computing" by S. Schneider et al. is a short theoretical digression about "a measurement scheme for the determination of the vibrational quantum number of the lowest normal mode of N ions confined to a trap". The authors investigate the readout of the electronic states in form of a binary string, which represent an integer. Their theory includes partitions of binary strings, much like in binary search routines.

Not only ionic quantum states can be used as qubits but, among others, also photons. The article by K. M. Gheri et al. on "Photon-Wavepackets as Flying Quantum Bits" discusses the interaction of single (or few) one-photon wave packets with a quantum system like an atom or ion. They demonstrate how quantum logical operations on photon wave packets can be performed by nonlinear optical elements, which operate on single photons. Their theoretical treatment covers the description of the one- and two-photon wave packet in terms of the appropriate master equations for the density matrix. Wave function simulations as well as the tailoring of wave packets are discussed. A. A. Khan and M. S. Zubairy treat a simple scheme for a two-bit quantum logic gate based on center-of-mass momentum states interacting with a resonant cavity field in the Bragg regime.

"Models of Quantum Turing Machines" by P. Benioff elaborates on "the other types of quantum computers", which are not represented by logic gates but rather by a finite state head interacting with a qubit lattice. The dynamical evolution of the system is governed by a unitary operator dictating evolution in finite time interval steps, which can also be represented by the Hamiltonian for the model. Benioff as the "father" of quantum Turing machines covers in depth the concepts of designing the step operator, how to generate distinct paths and their relation to qubit transformation, and quantum inteferometry. The article is rather abstract and requires some insight in the underlying concepts.

Even though quantum computers don't exist, researchers worry already about their errors. Isolation of the qubits from the outside world will in reality not be completely possible, thus introducing noise, unwanted bit flips, and phase errors. Unfortunately there is the "no cloning principle" for qubits, which implies that it is impossible to create an exact copy of an arbitray quantum state. In fact, for some time it was believed that quantum computers would never work because of this. Fortunately error correction schemes have been devised which take care of this. The article by A. M. Steane is the first in this book, which addresses the question of "Space, Time, Parallelism, and Noise Requirements for Reliable Quantum Computing". Different coding schemes are discussed which employ "ancilla qubits" which serve as quantum information storage by entangling them with working qubits. If the working qubits suffer an error, the entangled information is retrieved form the ancillas. Steane gives a detailed account on how to set up an "ancilla factory" and devises a number of different schemes in order to combat noise. A somewhat related but still different approach is proposed by T. Beth and M. Grassl by introducing "The Quantum Hamming and Hexacodes". They nicely draw the connection between algebra and physics in the context of quantum error correcting codes. I particularly like their comparison of binary codes and spin $^{1}/_{2}$ quantum systems. After an in-depth treatment of the underlying symmetry groups of so-called GF(4) codes, they discuss in great detail the encoding and decoding of the quantum Hamming code. The Hexacode concludes this article. The authors hope that their encoding scheme might be implemented in ion-trap quantum computers.

Fast database searching is one of the most often occurring tasks in computers. Grover has proposed a scheme by which a quantum computer can find "a needle in a haystack" fast. M. Boyer et al. discuss variants of Grover and other search algorithms in an article "Tight Bounds on Quantum Searching". They treat several schemes in detail and discuss their efficiency. They find that "Grover's algorithm comes within 2.62% of being optimal".

Cheating in communication between two people or two computers is of concern to H. F. Chau and H.-K. Lo in their article "Making an Empty Promise with a Quantum Computer". Suppose Alice and Bob are negotiating certain matters where Alice has to make a decision and stick to it. She does not want to tell Bob the decision she has made but it is sufficient for Bob to be sure that Alice does not change her mind later. How can she get Bob's trust and can she implement a scheme which does not allow her to change her mind at a later time? It was believed that quantum entanglement would provide such a scheme through the uncertainty principle of quantum mechanics. Chau and Lo shatter this believe by demonstrating how Alice can always change her mind later with the help of a quantum computer.

Although cloning of qubits is forbidden, V. Buzek et al. describe how "Flocks of Quantum Clones: Multiple Copying of Qubits" can be created. C. A. Fuchs addresses the question how quantum cryptography works and information disturbance can be detected in his article on "Information Gain versus State Disturbance in Quantum Theory". Two-particle entanglement is a standard procedure in quantum information theory; not so multi-particle entanglement. N. Linden and S. Popescu therefore discuss an important point in their article "On Multi-Particle Entanglement". The last article of the book on "Generalized Coherent States and Phase-Space-Interference in Multi-Mode Systems" by M. J. Gagen deals with a rather complex problem of multi-mode description of quantum states.

As an experimentalist, I regret that not more experimental papers were included. In fact, interesting experimental demonstrations of quantum algorithms were already performed by NMR. Nevertheless the collection of papers presented in this book is at the forefront of quantum information processing. I at least have enjoyed reading the different articles and recommend everyone who wants to learn more about the special theoretical concepts covered in this book to get a copy.

Michael Mehring
Physikalisches Institut
Universität Stuttgart