AIAA JOURNAL
Vol. 36, No. 11, November 1998

Book Review

Explorations in Quantum Computing

Colin P. Williams and Scott H. Clearwater, Springer–Verlag, New York, 1998, 307 pp., $49.95

The first figure in this book shows the number of atoms required to store one bit of information. Starting at about 10^{20} around 1950, the number fairly consistently halves every 18 months, and it stood in the mid-1980s at about 10^{10}. Extrapolation suggests that by the year 2020 (I am amazed by the number of events predicted to come about in the year 2020; when that time comes will we all have 20-20 hindsight?) we will need only one atom per bit! If this, or anything like it, comes to pass, computers will be afflicted with quantum uncertainty. One trembles at the prospect of coding or debugging under such circumstances; it makes the current agonies of parallelism seem positively serene. Error detection and majority votes would become necessary elements of reliable computing. The authors deal mostly with a different question, though. Is there anything about quantum computing, other than simply size and speed, that might actually prove advantageous?

It seems that there could be. A true quantum computer, all of whose states are merely probable, can be thought of as working simultaneously not just on one problem but on many versions of the same problem (quantum parallelism). The snag is that by observing the results we cause a collapse of the wave function and usually see the answer to only one of the problems. There is, however, an alternative: that we might instead have access to something that was true of all of the problems. Recently a quantum algorithm was devised that would make it possible to factor large integers in polynomial time, essentially by considering in parallel a whole set of candidate factors. This has dramatic implications for cryptography. That and the less surprising ability to generate truly random numbers to eliminate bias in Monte Carlo computations are the successes with potential practical application that encourage the research. The authors suggest that the first impact of quantum computing might be the development of "quantum circuits" within conventional computers. These would handle very specialized tasks, maybe in a quite transparent manner.

It would be difficult to describe this book as required professional reading even for the most computer-struck researcher, but it is well worth noting it as an early sign of something that could in the future, just possibly, have major effects on the way we think and do research. The notion of quantum parallelism is oddly evocative for me of recent suggestions made by Pierre Perrier of Dassault Aviation that computational fluid dynamics is essentially inefficient if its output is merely the prediction of a single flow. He notes that the information produced is relevant to a great number of associated questions such as the stability and controllability of that flow and the favorable or unfavorable effects of a design perturbation. Hence he considers that all of these things should be computed simultaneously.

This book bears one of the newer imprints, TELOS, The Electronic Library of Science, of the usually staid Springer–Verlag company. The book is not staid. It is written in a lively style reminiscent of a good *Scientific American* article but is backed up with many technical references. The authors supply a good deal of popular material on the history of computing and quantum mechanics and allude to, without engaging in, the current debate on the nature of consciousness. The physicist/philosopher Roger Penrose has suggested that the distinctive nature of human, as opposed to mechanical, intelligence might lie in its having an unpredictable quantum component, and it might even be that quantum parallelism is the secret of our human ability to synthesize patterns. People with a taste for this branch of speculation could consider adding this book to their library. It comes with a CD-ROM that lets you emulate certain aspects of a quantum computer using Mathematica notebooks.

Philip Roe
University of Michigan