Quantum Information and Computation, Vol. 3, No. 5 (2003) 465–467

BOOK REVIEW

on

A Shortcut Through Time
George Johnson
Alfred A. Knopf, New York, 2003
Hardcover $24.00 (204 pages) ISBN: 0-375-41193-3

and

The Quest for the Quantum Computer
Julian Brown
Simon & Schuster, New York, 2001
Paperback $16.00 (396 pages) ISBN: 0-684-87004-5

These highly readable volumes by two distinguished science writers offer quite different approaches to the problem of how to explain the quantum computation revolution to nonspecialists. Julian Brown's *The Quest for the Quantum Computer* (originally published in England in 2000 as *Minds, Machines, and the Multiverse*) operates at the level of *Scientific American* back in its finest days. George Johnson's *A Shortcut Through Time* is considerably less sophisticated, being at about the level of the *New York Times* Sunday magazine.

Brown sets out to explain quantum computation to a reader willing to do a little thinking. He is quite thorough in his coverage, devoting his long second chapter to an important piece of prehistory: the classical theory of reversible computation. I learned a lot from his survey of the very early days, and many younger practitioners of the subject might too. He also tells of the early steps toward quantum computation by Richard Feynman and Paul Benioff.

When Brown gets to the modern era he provides his readers with non-technical but accurate and detailed descriptions of Peter Shor's factoring algorithm, Lov Grover's search algorithm, and even quantum error correction. In the course of leading up to Shor, he explains classical public key cryptography, both RSA and Diffie-Hellman. Readers will also learn about quantum money, the ups and downs of quantum bit commitment, teleportation, and, of course quantum cryptography. In addition to all this Brown critically surveys half a dozen candidates for the actual physical hardware. He does all of this with a minimum of technical analysis, relegating most formal details to a series of short, readable, elementary, yet accurate Appendices.

I have only a few criticisms. The book would have been better without its last chapter. Like the finale to a fireworks show, it launches a great barrage of spectacular items, but many of them have only a tenous link to what has gone before. We are given, among other things, DNA computation, nanotechnology, the problem of consciousness, Roger Penrose's

new mind, and decoherent histories. What Brown has to say about all these new topics is, like the rest of his book, as clear and sensible as they allow him to be, though some of them defy any attempts at clarity and sensibility. This final chapter reads more like the prospectus for a new book than as a summing up of what had been a singlemindedly clear and comprehensive survey of a well-defined subject.

Occasionally Brown slips, though surprisingly infrequently, considering the difficulty of the task he has set himself. The square root of NOT is not a 45 degree (polarization) or a 90 degree (spin) rotation. More importantly, the square root speed-up in Grover's search algorithm is not a reduction in the number of entries in a database that the program has to examine. And whatever "horribly" may mean, it is surely not the case that Shor's algorithm will work even if the phase changes in the quantum Fourier transform are "horribly inaccurate".

While Brown should not be blamed for propagating some of the misleading statements prominent practitioners of the subject have produced, I would guess that the following specimen of hype is his alone: "If you imagine the difference between an abacus and the world's fastest supercomputer, you would still not have the barest inkling of how much more powerful a quantum computer could be compared with the computers we have today."

The fact that these are the worst blemishes I noticed is a measure of the considerable achievement of this book. The writing is beautiful. The excitement of the field is well conveyed. A remarkably high percentage of what is said is clear and accurate. Your nonscientist friends who are not phobic about elementary mathematics will enjoy this book. So, I suspect, will you.

George Johnson, on the other hand, offers his readers quantum computation lite. He acknowledges having made repeated use of Brown's "comprehensive overview" in preparing his own book, which does indeed read like a popularization of a popularization. While Johnson did his own independent research into the field and thanks an impressive list of luminaries for having "read parts, and in some cases, all of the manuscript", too much of what he has to say is either off the point or incorrect.

Off the point are early chapters on Johnson's childhood experiences with a disappointing "Geniac" kit, and on the efforts of MIT students to build a computer out of children's Tinkertoy sets. I suppose they are intended to make vivid the fact that computers are physical systems. Although these stories are entertainng, they play a negligible role in setting the stage for what comes next, and they struck me as an unnecessarily elaborate roadblock on the way to the main story.

A more serious problem is that major mistakes lie all about:

- Quantum mechanics does not teach us that "a single particle can be in two places at the same time".
- To learn the square root of every number from 1 to 1,000 you cannot just "load them all onto a row of 10 atoms, perform a single calculation and you instantly have all 1,000 answers."
- It is not the case that when Shor's algorithm has done it's job "the solutions — the factors of the number being analyzed — will all be in superposition." It is wrong to say that "his algorithm created a quantum waveform representing every possible factor and then collapsed it to produce the answer." Nor will a quantum code-breaking machine "try out all the possible factors simultaneously, in superposition, then collapse to reveal the answer."
- Positive and negative amplitudes coming together and cancelling each other out is not

"precisely what is happening when a superposition. . .collapses to reveal a single outcome."

• Grover's algorithm does not mean that "Instead of having to look through half the items of a database. . .a quantum device need only comb through the square root of the number of items." (This might reflect one of the rare lapses of Brown, noted above.)

Johnson's book, in short, while engaging and entertaining, will be a constant source of irritation to anybody who understands the subject, and will cheerfully fill the interested amateur with much misinformation about both quantum mechanics and its application to computation. Your friends will have to work harder reading Brown than they would with Johnson, but Brown also has the general reader very much in mind, he writes just as well as Johnson, he tells a more complete and better constructed story, and almost everything he says is correct.

N. David Mermin (ndm4@cornell.edu)
Laboratory of Atomic and Solid State Physics
Cornell University, Ithaca, NY 14853-2501, USA