BOOKS

August 11, 2003
Volume 81, Number 32
CENEAR 81 32 pp. 36-37
ISSN 0009-2347

QUANTUM COMPUTERS MADE LUCID

A SHORTCUT THROUGH TIME: The Path to the Quantum Computer, *by George Johnson, Knopf, 2003, 224 pages, $24 (ISBN: 0-375-41193-3)*

REVIEWED BY DANIEL LIDAR

The quest to get something out of nothing dates back at least to the alchemists. In "A Shortcut Through Time: The Path to the Quantum Computer," his remarkably lucid new book about quantum computers, George Johnson describes what may be the ultimate free lunch, spawned by our harnessing of the laws of nature at the quantum level. Potentially bigger than the transition from the abacus to integrated semiconductor circuits, quantum computers may one day revolutionize computation.

The key to their success, as aptly put by Johnson, is that "performing a quantum computation is a matter of jumping on the wagon and going along for the ride." The wagon is the mysterious and wonderful world of quantum mechanics, at a level of sophistication no higher than as taught in an advanced undergraduate course. The ride is a rather wild one, through the rugged and vast expanses of abstract Hilbert space, traversing superpositions and quantum entanglement.

But Johnson, a science writer for the *New York Times* and author of several other successful popular-science books, has a remarkable ability to tame the abstract using metaphors and pictures, such as his gem of an explanation of modular arithmetic using five-houred clocks. His presentation is suitable for and aimed at the nonspecialist. It is the most readable account of quantum computing I have encountered so far in this category.

Quantum computers are by now rather famous for their (theoretically demonstrated) ability to crack cryptographic codes and efficiently search large databases. They have even trickled into some science fiction and spy books. Less well known, but no less important, is that they also excel at simulating quantum systems.

Words such as "efficiently" and "excel" have a precise quantitative meaning: In the case of code cracking and simulations of quantum mechanics, the speedup offered by quantum computers is believed to be exponential in the size of the problem. (Equally efficient classical algorithms may still be found, but this seems exceedingly unlikely.) In the case of database search, the speedup is provably quadratic and cannot be improved upon.

The implications are mind-boggling. Consider code-cracking: An eavesdropper in possession of a quantum computer could conceivably gain access to society's best-kept secrets in a matter of a few hours or days. And the efficient simulation of quantum mechanical systems could conceivably be exploited for the ab initio design of drugs or high-temperature superconductors. As Johnson puts it, "Quantum computing would be to ordinary computing what nuclear energy is to fire."

The book's title, "A Shortcut Through Time," suggests that quantum computers perform their computational feats via a trick. From the perspective of "classical" computers, this is indeed the case. A classical computer can be defined as a device that does not use the laws of quantum mechanics to represent information. This includes what we currently call desktops, laptops, supercomputers, optical computers, and even DNA computing.

What does it mean to represent information quantum mechanically? At the most basic level, it means that the unit of information is no longer the classical "0 *or* 1" bit, but rather the "0 *and* 1" quantum bit (qubit). "And" refers here to the superposition principle of quantum mechanics, whereby an object can be at once in two (or more) mutually exclusive states. Johnson introduces the suggestive symbol "⦶"--1 in 0--for this purpose. Zero and one are just convenient labels for states of light or matter--for example, a spin-up or -down state of a nucleus or electron, horizontal or vertical polarization of a photon, or left or right chiral states of a molecule.

"What if, in a kind of mathematical jujitsu, quantum mechanics could be pitted against quantum mechanics, fighting fire with fire?"

Once one accepts the notion that information also can enter into a superposition state, the dramatic implications follow when one ponders the states of many qubits. Two qubits can represent the numbers 00, 01, 10, and 11 (in binary notation) in superposition, and N qubits can represent all 2^N integers from 0 to 2^N-1. The shortcut through time refers to the parallel processing of all these exponentially many numbers at once, made possible by virtue of their existence in superposition. This feat has no classical analog: A classical computer is doomed to process numbers serially. (Of course, a classical parallel computer is just a bunch of serial machines working in parallel.)

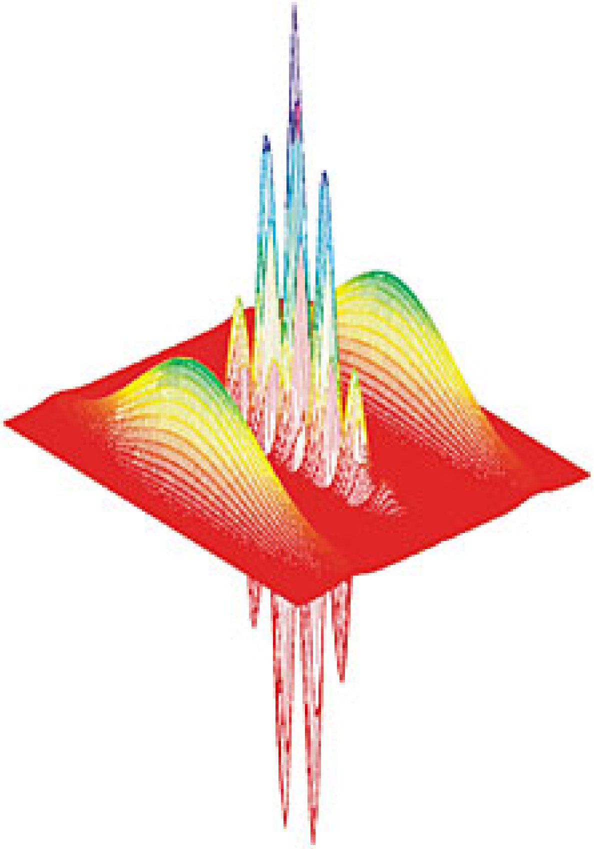
To be fair, the situation is in fact more complicated, and concepts such as quantum entanglement and measurements play a crucial role. Johnson admirably explains these subtleties in layman's terms, closely obeying Stephen Hawking's famous law of popular-science writing, that each equation halves the number of readers. (I counted three, such as y = 2x, and these were all illustrated by graphs.) Johnson takes the reader on a tour of the state of the art of the field all the way from the beginning (Richard Feynman's first observation that quantum computers can solve the problem of simulating quantum mechanics), to mid-2002, necessarily focusing on only a few aspects he deems central. The account often reads storylike and is peppered with occasional anecdotes.

What role is there for chemistry in quantum computing research? Interestingly, the first demonstration of rudimentary quantum algorithms was performed using a method familiar to every chemist: liquid-state nuclear magnetic resonance spectroscopy. In fact, to date, NMR is still the front-runner in terms of the number of qubits that have been harnessed for the purpose of running quantum computing algorithms, setting the current world record at seven.

Unfortunately, this number is not likely to grow beyond 10 or so, for noise quickly overwhelms the NMR signal as the size of the molecule increases. Indeed, the qubits in NMR are the nuclear spins of (often specially synthesized) molecules. The striking success of NMR-based quantum computing can be attributed to decades of chemistry research into synthesis and NMR spectroscopy.

Similarly, chemical expertise comes in handy, for example, in constructing quantum computers based on semiconductor nanocrystals, fullerenes, carbon nanotubes, and a variety of other macromolecular designer architectures. Such architectures hold the promise for large-scale quantum computers, though at present the leading candidates seem to be other solid-state architectures, in particular those offering the prospect of integration with the existing semiconductor technology infrastructure, such as silicon-based proposals.

Another area of chemistry research that is poised to make some remarkable contributions is coherent and optimal quantum control. After all, one can view quantum computing as the desire to navigate from point A (an input) to point B (a final answer) in Hilbert space, a goal shared by the quantum control community, where A and B instead typically represent chemical reagents and products.



SYSTEMATIC Physicist Eugene Wigner's representation of the quantum superposition state (the two lumps) showing interference fringes in the center. Image also corresponds to a qubit in a superposition state of "0 and 1."
COURTESY OF IBM ALMADEN RESEARCH CENTER

Yet another area where expertise developed in the theoretical chemistry community is likely to become an invaluable resource for quantum computer design is numerical simulation methods for quantum systems. For example, surprisingly little numerical work has gone into materials-related questions in quantum computer design. This is an indication that the field is still very young, grappling at the moment with fundamental questions such as "how to make a single solid-state qubit work well," "what makes quantum computers so powerful," and "how to protect quantum computers against external disturbances."

The latter is in fact generally perceived as the biggest obstacle to the full-scale realization of the quantum computing dream: It turns out that quantum superposition states are exquisitely sensitive to external disturbances such as inevitably arise from the coupling of a quantum computer to its environment. Even a single stray photon can cause irreversible damage. The resulting effect, known as decoherence, leads to the rapid transformation of the quantum "and" of mutually exclusive states to the familiar classical "or." In the process, all the quantum computational advantage is lost.

But a decohered quantum computer is worse than just a regular classical computer that processes its information in serial fashion. Because decoherence attacks at random, the result is an uncontrolled, stochastic computer that will output a string of gibberish. Early critics of quantum computing ideas pointed out that, in the presence of decoherence, quantum computers were doomed to fail, because decoherence acts essentially like the second law of thermodynamics.

Remarkably, this criticism turned out to be too harsh. "Quantum error correction and avoidance" methods were developed that allow the precious quantum information to survive even in the presence of decoherence, through a process somewhat analogous to cooling. Johnson devotes only a relatively short section to this fascinating subject. I find this somewhat unfortunate, because it is the absolute key to the future success of quantum computing efforts and one of the most surprising theoretical discoveries in many years. Nevertheless, the short treatment of this admittedly difficult subject is another marvel of popular-science exposition.

One of the final chapters is judiciously devoted to quantum cryptography, the one aspect of quantum information science that has already seen commercial applications. This subject is, in a way, the mirror image of quantum computing, for it allows one to restore the security undermined by quantum computers' ability to crack classical cryptographic codes.

To cite from Johnson's prose: "What if, in a kind of mathematical jujitsu, quantum mechanics could be pitted against quantum mechanics, fighting fire with fire?" This turns out to be possible: As powerful as quantum computers are, the uncertainty principle prohibits an eavesdropper from going undetected while acquiring complete information about a signal that is transmitted between two communicating parties. This forms the basis of a new type of unconditional communication security that follows straight from the laws of quantum mechanics.

Johnson's account of the emerging quantum computing revolution is an easy and most commendable read. My only real quibble is with the rather steep price of the book, $24 for fewer than 200 smallish pages, but hopefully the soft-cover edition will fix that (classical) bug.

DANIEL LIDAR *is an assistant professor of theoretical chemical physics at the University of Toronto. His research focuses on aspects of quantum computers, including decoherence problems, and the study of quantum dots as potential quantum computers.*

Top