from *SIAM News*, Volume 36, Number 8, October 2003

Mathematics, Metaphor, and the State of Quantum Computation

A Shortcut Through Time: The Path to the Quantum Computer. *By George Johnson, Knopf, New York, 2003, 256 pages, $24.00.*

BOOK REVIEW

By Greg Kuperberg

A Shortcut Through Time is a well-written book and a fair effort. It is a good book about quantum computation for readers who do not want to think mathematically. The author, George Johnson, is a science writer for *The New York Times*. In keeping with his profession and his intended audience, he writes in the introduction that he will discuss quantum computation using "metaphor instead of mathematics."

But Johnson also sets an unusually high standard for a popular book about science. He wants to provide a genuine explanation of quantum computation, not just to report on it. Unfortunately, his expository approach prevents him from achieving this goal. Using metaphor instead of mathematics is not like translating between English and French; it is not expressing the same ideas in different words. Certain ideas can be understood only with mathematics, and quantum computation is one of them.

The Rubik's Cube provides one example of the limits of nonmathematical thinking. Solving it is a fairly mathematical skill. When the Cube was popular, 20 years ago, many people with little mathematical training wanted to be able to solve it. Some Cube owners took a literary approach, buying solution books intended for untrained readers: When one didn't work, they bought several more. One friend asked me, "How do you solve Rubik's Cube? I bought a book, but it didn't make any sense." In fact, those books are painful to read. Without some group theory or at least some combinatorial insight, solutions to the Rubik's Cube can't make sense. Talking about the Cube in lay terms goes only so far. Yet with only a little bit of mathematical experience, the Cube is not very hard.

It takes more mathematics to understand quantum mechanics and quantum computation than to solve the Rubik's Cube. The prerequisites are undergraduate material, mainly multilinear algebra, complex numbers, and computer algorithms. Johnson draws the line much lower than that, at about 7th-grade mathematics. In fact he provides good explanations of background concepts like exponential growth, classical logic gates, base 2 arithmetic, and modular arithmetic. These explanations work in part because here Johnson resorts to equations and functions after all: mathematics instead of metaphor.

By contrast, his discussion of the hard part—quantum mechanics and computational complexity—tilts toward metaphor and wonderment. He writes that quantum mechanics is "hard to believe," "impossible but true," "[seemingly] so absurd," and a "jarring truth." Incredulity about quantum mechanics is healthy in moderation. But it is not healthy to remain incredulous, because the quantum rules are logical. It is much better to derive new intuition from these rules than to imagine quantum mechanics as *deus ex equationes*.

The first important concept not properly explained in the book is quantum superposition. Johnson reduces it to the symbol "0 1," which conveys the idea that a qubit (the quantum version of a bit) can lie in a superposition of the bit states 0 and 1. Thus, a quantum computer with n qubits can be in 2^n states simultaneously and therefore perform massively parallel computation. This description has some truth to it, but it is very misleading.

Here is a more accurate description: The quantum rules are analogous to and ultimately a generalization of classical probability theory. You can think of the state of a randomized bit as a superposition of the states 0 and 1. Such a state can be written formally as

$$p\,[0] + (1 - p)\,[1],$$

where p is the probability that the bit is 0. Randomized computation (also called Monte Carlo computation) is also in a sense parallel computation—but only in a weak sense. Randomized algorithms are sometimes moderately faster than deterministic algorithms (for, say, primality testing), but they are much slower than unrestricted parallel algorithms.

Given that quantum mechanics generalizes classical probability theory, it should not be too surprising that quantum Monte Carlo algorithms can be even faster than classical Monte Carlo algorithms. In quantum probability, a (pure) state of a qubit is given by a formal expression:

$$a|0\rangle + b|1\rangle.$$

Here a and b are complex numbers, called amplitudes, with $|a|^2 + |b|^2 = 1$. Amplitudes are closely related to probabilities: The squared norm $|a|^2$ is the probability corresponding to the amplitude a. The state of n qubits is described by 2^n amplitudes, just as the state of a randomized bit is described by 2^n probabilities. Modulo the equivalence $(a, b) \sim (e^{i\theta}a, e^{i\theta}b)$, these states form a sphere in which the basic states $|0\rangle$ and $|1\rangle$ are antipodal. Despite Johnson's "0 1," all of these states are on an equal footing. For example, one person's

$$\frac{3}{5}|0\rangle + \frac{4}{5}|1\rangle$$

and

$$\frac{4}{5}|0\rangle - \frac{3}{5}|1\rangle$$

are another's $|0\rangle$ and $|1\rangle$. One consequence is that, whereas the NOT gate is the only interesting unary operation on a bit, the group of reversible unary operations on a qubit is SO(3), the rotation group of the sphere.

Fortified with this expanded notion of superposition, a quantum computer, using Shor's algorithm, can factor a number in polynomial time (in the number of its digits). It can also perform an arbitrary combinatorial search in a space of size N in time $O(\sqrt{N})$ using Grover's algorithm. But quantum computation is still much slower than unrestricted parallel computation. For example, Grover's algorithm is known to be the fastest possible general quantum guessing algorithm. By contrast, a freely parallel computer could guess all N choices in a constant amount of time (in units of the time needed to check one guess).

With his symbol "0," then, Johnson has oversimplified a qubit. In other cases, he conveys a point inaccurately the first time, but then fixes it with a more accurate description later. For example, he writes on page 72 that the output of Shor's algorithm is a superposition of the factors of the input number n. But as he correctly explains on page 78, Shor's algorithm produces a superposition of other numbers that lead to the factors, not the factors themselves. Some of the errors in the last chapter remain uncorrected. He uses the adjective "NP-complete" as a noun, and defines it essentially as freely parallel, polynomial-time computation. In fact, the NP complexity class is another restricted form of parallelism, although it does include many hard problems. Algorithms that run in polynomial time with unrestricted parallelism constitute the much larger class PSPACE.

For the reader who does not want the math, these are minor details. At a nonmathematical level, the book is very good. In particular, it properly summarizes the current state of quantum computation. My own microsummary is as follows: Some quantum algorithms are known to be faster than what is classically possible, but quantum complexity theory is still very mysterious. Useful quantum computers are possible, in principle. If built, they would alter the field of cryptography; but so far, only toy quantum computers have been built. Among other necessary ideas, large quantum computers would require quantum error correction.

The book has a bibliography with many references to technical papers, although most of the intended readers are unlikely to enjoy them. Moreover, the bibliography has one cardinal omission: Most workers in quantum computation get research papers from the quant-ph section of a digital library called the arXiv, which is both free and more current than journals.

I discovered from other reviews that my impression of *A Shortcut Through Time* is far from universal. Many of its fans are not lay readers, but rather scientists and mathematicians. Mathematically prepared readers should take note of the remark at the very end of the bibliography: "The bible of the field is Michael A. Nielsen and Isaac L. Chuang's monumental *Quantum Computation and Quantum Information*." It certainly is. Chapter 1 of Nielsen and Chuang is a nontechnical introduction that covers most of the material presented in *A Shortcut Through Time* in fewer pages and with more authority. Best of all, the reader can then proceed to the other chapters.

Greg Kuperberg is a professor in the Department of Mathematics at the University of California, Davis.