from *SIAM News*, Volume 34, Number 5

Shhhh—Quantum Computer At Work

By Barry A. Cipra

Quantum computers are still more science fiction than fact—even the most optimistic of experts predict a decade or more before anyone builds one that actually computes anything. But the theory of quantum computation is making steady progress—and even if the technology never blossoms, the insights it's been bringing into the nature of quantum mechanics may be worth it. In a session on quantum computation at this year's meeting of the American Association for the Advancement of Science, held in San Francisco in February, Dorit Aharonov of the University of California at Berkeley described one such insight: The effects of decoherence that bedevil quantum computation are characterized by a phase transition.

Quantum computation depends on a phenomenon known as entanglement, in which a system of physical objects like ions is simultaneously in several states. Entanglement makes it possible for N quantum bits, or "qubits," to be in 2^N different states at the same time. But entangled states are subject to interactions with the environment, which causes the system to lose its quantum coherence, a process called decoherence. In some cases, it is reasonable to assume that the interactions with the environment are local, and that each qubit suffers independently. Roughly speaking, the effect of such decoherence can be viewed as the environment kicking the quantum state of each qubit around more or less at random.

Quantum computing was one of several mathematical topics on the program at this year's AAAS meeting; see "Poltitcal Calculus" for Barry Cipra's report on the session on the mathematics of apportionment.

The fact that a quantum computer can work at all when it's constantly battered by the environment was one of the great breakthroughs in the field. The "no cloning theorem," which rules out the possibility of correcting errors by simple duplication of qubits, seemed to be the death sentence for quantum computation. But in 1995, Peter Shor of AT&T Labs Research, who had earlier invigorated the field with the discovery of a polynomial-time factoring algorithm for quantum computers, showed that error correction is nonetheless possible (see "Quantum Computation: A New Spin on Complexity Theory," *SIAM News*, October 1998; http://www.siam.org/siamnews/10-98/quantum.pdf). Shor also showed how quantum error correction could, in principle, be parlayed into a method for fault-tolerant quantum computation.

(The distinction between error correction and fault tolerance is subtle. It can be compared to the difference between hydrostatics and hydrodynamics. Roughly speaking, error correction aims to maintain a quantum state as is. Fault-tolerant quantum computation copes with the harder problem of manipulating the state to perform computations, including error corrections, while everything is contantly decohering.)

Numerous researchers have refined these insights, to the point that some experts feel that quantum computation may eventually prove practical. In joint work with Michael Ben-Or of the Hebrew University in Jerusalem, Aharonov showed that quantum computing retains its full power as long as the "noise rate" η—that is, the probability of a faulty event, per particle per time step—is less than some threshold η_0, but is no better than an ordinary classical computer—and an extremely fragile one, at that—if η exceeds some higher threshold η_1. The current best bounds on these thresholds are $10^{-4} \leq \eta_0 \leq \eta_1 \leq 1/2$.

The question is, What's going on in those three orders of magnitude between the known bounds? How high can η_0 be raised, how much can η_1 be lowered? Can they be brought together, or is there some inexorable gulf between them, across which the power of quantum computing gradually erodes, until nothing but classical capabilities is left? (Of course, if it turns out that $P = NP$ or, better, that $P = PSPACE$, the power of quantum computing may be rendered irrelevant. But don't count on it.)

Building on her joint work with Ben-Or, Aharonov has ruled out the gradual erosion option. As η increases from 0, the quantum-to-classical transition occurs abruptly, in much the same way that ice melts at 0° Celsius.

The proof is based on a new notion that Aharonov calls "entanglement length," which, loosely speaking, governs the maximum physical distance between entanglable objects in a noisy system. More precisely, the entanglement length establishes the rate of exponential decay of entanglement between components: If A and B are disjoint sets of particles separated by a distance r, the extent of their entanglement (itself a subtle concept) is proportional to some polynomial in the sizes of the two sets multiplied by $e^{-r/L}$, L being the entanglement length. This is analogous to the notion of correlation length in statistical mechanics.

Using techniques from percolation theory, Aharonov has shown that if there's too much noise, the entanglement length is finite, which limits the size—and computing power—of the quantum computer. But she's proved that if the noise is sufficiently small, the entanglement length is infinite, which means there's no limit (in theory) to the number of qubits the computer can handle.

The switch from finite to infinite entanglement length must occur at some precise value, analogous to the melting point of ice. But the details of the phase transition are still a mystery, Aharonov explains. In particular, strange things could still be happening in the gap between entanglement lengths known to be finite and those known to be infinite. It's conceivable, for example, that the entanglement length fluctuates between finite and infinite values. Nor is there any handle on what the "critical exponents" of the transition might be—or even if such standard concepts apply.

Details aside, the presence of a phase transition, Aharonov believes, may help explain why ordinary macroscopic objects, like people or cats, are never found in the weird conditions—simultaneously dead and alive, for instance—that quantum mechanics commonly creates in the atomic and subatomic world. In effect, there's too much noise in the macroscopic world for large-scale entanglement to survive; it boils off like water tossed on fire.

That extrapolation isn't automatic, though, Aharonov points out. "It is possible that the classical behavior of big quantum systems can be explained by the fact that these systems are simply in their supercritical phase, where entanglement length is finite. One can speculate that in the finite-entanglement-length regime of a quantum system, everything behaves classically when looked at in scales much larger than the entanglement length. To understand whether this is true, a lot of work needs to be done, both theoretically and experimentally."

The theoretical aspect is analogous to the question of whether, say, Boyle's law is derivable from the Boltzmann model of gas dynamics. The experimental aspect would include testing whether the model's assumptions of local noise and interactions are valid. But in principle, at least, it ought to be possible to test for exponential decay of entanglement in large systems and measure the corresponding entanglement lengths, Aharonov says. If it is—and if researchers can quiet a large quantum system enough to make it subcritical—it might be possible to "see" the cutoff between quantum and classical behavior. And who knows—maybe part of the confirmation will come from a computation done by a quantum computer.

Barry A. Cipra is a mathematician and writer based in Northfield, Minnesota.