Quantum Computing: Dream or Nightmare?

Recent experiments have deepened our insight into the wonderfully counterintuitive quantum theory. But are they really harbingers of quantum computing? We doubt it.

Serge Haroche and Jean-Michel Raimond

The principles of quantum computing were laid out about 15 years ago by computer scientists applying the superposition principle of quantum mechanics to computer operation. Quantum computing has recently become a hot topic in physics, with the recognition that a two-level system can be presented as a quantum bit, or "qubit," and that an interaction between such systems could lead to the building of quantum gates obeying nonclassical logic. (See PHYSICS TODAY, October 1995, page 24 and March 1996, page 21.)

In principle, a network of such gates could process large qubit registers in superposition states, achieving massive parallelism and solving some problems in far fewer steps than a classical machine would require. The discovery, by Peter Shor at Bells Labs, of an efficient number-factoring algorithm for an idealized quantum machine has fueled considerable interest in this field. The factoring problem is so hard to solve on existing computers that it is widely used for secure encryption. By factoring faster, quantum computers would render existing encryption systems obsolete.

At this stage we think that some critical reflection is required in a field boiling with excitement. We feel that the enthusiasm is certainly justified, but not necessarily for the reasons generally adduced. Although the idea of quantum computing involves some fascinating new physics that goes far beyond the rather mundane problem of merely computing faster, we believe that performing large-scale calculations will remain an impossible dream for the foreseeable future.

In the process of studying simple gate operations and the entanglement of a few qubits, physicists will however learn a lot about the elusive boundary between the classical and quantum worlds, and address some of the deepest issues raised more than half a century ago by the founders of quantum mechanics. This research benefits greatly from the concepts introduced by computer scientists, thus providing a striking example of cross-disciplinary fertilization between mathematics and physics. At the same time, we feel the need to raise a caveat against the dangers of unrealistic promises of practical applications in a field in which too many overoptimistic predictions have already been made. One may recall the great hopes once held out for optical and Josephson computers.

The elementary building block of an ideal quantum computer is a gate that has two interacting qubits: a "control" bit and a "target" bit. The control remains unchanged, but its state determines the evolution of the target: If the control is 0, nothing happens to the target; if it is 1, the target undergoes a well-defined transformation.

Quantum mechanics admits additional options. If the control is in some coherent superposition of 0 and 1, the output of the gate is entangled. That is to say, the two qubits are strongly correlated in a nonseparable state, analogous to the particle pairs of the Einstein–Podolsky–Rosen paradox. The superposition of the input qubits and the entanglement of the output states are the basic features that differentiate these gates from classical ones and that open, at least in theory, a much richer realm of computing capabilities.

Recent experiments

A variety of recent experiments with trapped ions or with atoms and photons in tiny cavities have displayed all the ingredients necessary for a quantum gate. Atomic or field states can be schematized as two-level systems. By making them interact, one can achieve the essential qubit operations. That, we think, is the main reason why the notion of quantum computing has recently become so popular.

Thus, experimental setups originally designed to test fundamental aspects of quantum theory have been used recently to demonstrate quantum-logic operations. Although operating a single quantum-logic gate poses no fundamental difficulties, the situation changes drastically when one considers the operation of a large-scale computer that combines many gates. For the computation to proceed, the machine has to evolve into a huge superposition of qubit states resulting from the quantum interference of a large number of classically alternative paths.

Such a dream scenario would require a machine completely isolated from the outside world. But in fact, quantum coherence is exceedingly sensitive to the unavoidable coupling with the environment. This caveat has already been stressed in many studies. A *single* relaxation event affecting an excited qubit state can destroy the coherence required by the computation.

A simple argument will help us understand the magnitude of the decoherence problem. If T is the relaxation time of a single qubit and t is the operation time of a single gate, then $R \equiv T/t$ serves as a figure of merit for the hypothetical com-

SERGE HAROCHE *and* JEAN-MICHEL RAIMOND *are professors of physics at the Ecole Normal Supérieure in Paris and at the Pierre and Marie Curie University (University of Paris VI).*

puter. If one hopes to compute with a reasonable probability of success, R must be on the order of the number of qubits times the number of gate operations.

Consider, for example, an absurdly modest application of Shor's factorization algorithm: factoring a four-bit number. Even that would require about 20 000 gate operations on 20 qubits. So R would have to be larger than about 400 000, a very optimistic figure for the best quantum optics systems we have at present. What about a more useful task—for instance factoring a 400-bit number? Then R, which scales at least as the third power of the input-number size, would have to be of order 4×10^{11}. If t is a tenth of a millisecond, as in the ion-trap gate recently demonstrated by David Wineland's group at the National Institute of Science and Technology's facility in Boulder, Colorado, then the relaxation time would have to be a year!

Not to worry!

The optimists claim that such requirements should not deter us. "There has been, after all, a lot of progress between Pascal's machine and the Pentium processor," they will say, concluding that there is no clear limit to what technology and money can do. But this view assumes that t and T can be tuned independently, in opposite directions. That is, however, not true for any system known today. The physical interaction that couples the qubits together adds its own noise, which produces random perturbation of the qubits.

In the ion-trap quantum gate, for instance, the qubits are encoded in two substates of an ion's ground level, which have, in principle, infinite lifetimes. But the qubit operation is implemented by a laser-induced Raman process that involves a virtual transition of the ion to a short-lived excited level. If one shortens the duration of the virtual transition by increasing the laser power, one also increases the probability of an unwanted real transition to the excited state, followed by a spontaneous emission that ruins the quantum coherence of the bit. It is thus impossible to shorten t without ultimately also shortening T.

Irrespective of the laser power, one can show that R for such an ion-trap gate cannot significantly exceed the inverse cube of the fine structure constant, roughly 3×10^6. This limit applies to any gate based on allowed electric-dipole optical transitions. Thus the most ambitious task one can expect an optical quantum computer to perform, if nothing is done to correct for decoherence, is the factorizing of a four-bit number!

Another point is worth mentioning. Macroscopic quantum systems such as superconducting metals, or the recently produced Bose–Einstein atomic condensates are not destroyed by decoherence. (See the column by Daniel Kleppner on page 11 and the news story on page 18.) Why then should quantum computers be so vulnerable? Because there is indeed a fundamental difference. Macroscopic condensates, even if they incorporate a large number of particles, are described by a *single* quantum state, whose information content is necessarily zero. By contrast, in a hypothetical quantum machine, the qubits could be superposed in a huge number of different states. A thousand-qubit register, for example, would span $2^{1000} \approx 10^{300}$ states, and the coherence between all these states would have to be preserved over millions of operations. Manipulating such a quantum monster would be a feat almost as difficult as keeping Schrödinger's famous cat in a superposition of its dead and alive states.

Ingenious schemes for getting around the decoherence problem have recently been put forward. They rely on a variety of "watchdog" strategies that can be simply summarized as follows: Because spontaneous emission processes are lethal bugs, let us detect them and correct for their effects, restoring the quantum coherence as it gets destroyed.

Watchdog strategies

All these schemes rely on the use of redundant information. Instead of encoding in single bits, one would encode 0 or 1 in entangled states made of three or more qubits. Whenever one bit flipped inadvertently, the accident would be recognized by a sensitive detection procedure (the watchdog) and corrected for. Let us not be deterred by the fact that such entangled states of many particles are so difficult to prepare that no one has as yet succeeded. The mere preparation of such a state will be an experimental tour de force, leading to dramatic tests of quantum mechanics. Even if technological progress one day makes such entangled states common in the laboratory, any lapse of our watchdog's attention (in other words, any detection efficiency less than 100%) will result in a loss of coherence, and any imperfection in the sequence of operations required to control the system is bound to cause additional errors. Therefore we think it fair to say that, unless some unforeseen new physics is discovered, the implementation of error-correcting codes will become exceedingly difficult as soon as one has to deal with more than a few gates. In this sense the large-scale quantum machine, though it may be the computer scientist's dream, is the experimenter's nightmare.

If a large-scale quantum computer is unrealistic, what about a small one, with a few dozen qubits? Because these computers would obey quantum logic, Seth Lloyd (MIT) argues that they would be particularly well adapted to compute the behavior of a quantum spin system made up of as many particles as the computer has qubits. (See Lloyd's article in *Scientific American*, October 1995, page 140.) This would amount to simulating a physical system by an artificial copy obeying the same equations of motion. We strongly doubt that there exist real spin problems whose study warrants the effort of performing such a challenging simulation rather than studying the original spin system itself. If one is concerned with just a handful of particles, classical computers can do the job and the need of quantum computation disappears altogether.

Even if quantum computing remains a dream, the physics of quantum information processing at the level of a few qubits is fascinating. Experiments on entangled particles with ions in a trap or atoms in a cavity will help us understand the fundamental aspects of quantum measurement theory, and they may lead to major improvements in the precision spectroscopy of simple quantum systems.

The newly discovered strategies for partially controlling the effects of decoherence, which would have been deemed impossible until very recently, greatly advance our understanding of dissipation in mesoscopic systems. Testing quantum decoherence in conceptually simple experiments is also an important and challenging task. Rather than teaching us how to build a large quantum computer, such experiments are more likely to teach us about the processes that would ultimately make the undertaking fail. It is important to advertise this fascinating subfield of quantum optics for what it really promises, which is a deeper insight into the most counterintuitive theory yet discovered by physicists.

We thank P. Zoller and I. Cirac for stimulating discussions and enlightening comments. ■