Progress towards quantum computation

Charles H. Bennett and David P. DiVincenzo
IBM Research *

Version nv06 for News and Views (Nature), 9/20/95.

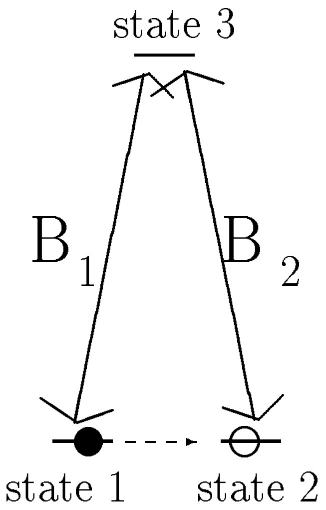
One of the paradoxes of quantum theory is how little its strange foundations obtrude into everyday life, even while supporting an edifice of chemistry and physics that explains the existence and properties of ordinary matter in exquisite detail. To marvel at the foundations themselves—in the form, say, of the two-slit experiment or the Einstein-Podolsky-Rosen effect—one must generally visit a textbook or a laboratory. However, it is becoming evident that such arcana may have rather direct and dramatic applications to the newer science of information processing.

For about ten years, there have been speculations about the vast and distinctive powers a quantum computer would have if one could ever be built. Now it appears that the subject of quantum computing is emerging from this visionary prehistory into a distinct "experimental" era. Powerful algorithms exploiting the unique capabilities of quantum computation are now widely understood, and some systematic searches for new algorithms are underway. On the hardware side, it is recognized that the implementation of the logic gates of a quantum computer is now, at some rudimentary level, within the purview of some well established experimental physics. It is still too early to tell when or whether quantum computing will advance to a third "engineering" era of routine practical exploitation.

At the most recent Workshop on Quantum Computation, held in the hospitable surroundings of the Institute for Scientific Interchange in Turin, Italy, between June 25 and July 7, the discussions, while still including "visionary era" discussions of Bel-

* Yorktown Heights, New York, NY 10598, USA; bennetc/divince@watson.ibm.com.

l's inequalities, quantum cellular automata, and the "many-worlds" interpretation, have moved on to include some concrete discussions of experimental realizations of quantum logic gates — to the extent that the paper[1] of the University of Innsbruck group, presented by T. Pellizzari, unabashedly presented a "realistic model of a quantum computer".



The scheme for implementing quantum logic which he presented builds on some of the hottest trends in atomic spectroscopy, in particular a technique called "dark-state transfer of Zeeman coherence". A Zeeman-coherent atom is one in which the wavefunction is only non-zero for one of the members of the ground state multiplet (containing "Zeeman fine structure"). This wavefunction can be moved to the other member of the multiplet if the atom is exposed to two optical beams which couple these two ground state levels to an excited state (see diagram). The rule is to first turn B_2 on, which leaves the system in state 1 but strongly couples states 2 and 3. When B_1 is turned on next, the system is transferred from 1 to the 2-3 complex, but, remarkably, because of quantum interference the amplitude of the wavefunction in the excited state 3 always remains very small. Then if B_2 is turned off, the system wavefunction is 100% in state 2; turning off B_1 completes the process.

This kind of spectroscopy has many advantages as a basic step in quantum computation. The instantaneous state is always "dark", that is, it cannot suffer spontaneous emission from the excited state, since its probability density for being in this state is vanishingly small (if the beams are turned on and off slowly enough). Thus the system always remains in a pure quantum state. If one of the beams B_2 is a single-photon state, then the spectroscopy serves to map the quantum state of that beam, which could be a superposition of zero and one photons, into the same superposition of the two Zeeman sublevels. It is this transfer capability which the Innsbruck workers have extended to solve the hardest problem of physical quantum logic gate design: moving a quantum state undisturbed from one subsystem (atom) to another.

Several recent experiments have proved that different quantum bits (or "qubits") can be made to interact controllably, in such a way that a rudimentary quantum logic gate is formed. In the work of C. Monroe and collaborators at NIST in Boulder, Colorado, it has been successfully shown that the low-lying states of Be ions in a Paul trap can be coupled spectroscopically to *phonons* (not photons), i.e., vibrational quanta of the trapped ions. Their work, inspired by a recent theoretical proposal by Cirac and Zoller[2], demonstrated the successful operation of a quantum exclusive-or or controlled-NOT gate, which flips one qubit conditionally on the state of another qubit, with an overall reliability in the initial experiments of about 80%. In another experiment by Q. A. Turchette and co-workers at Cal Tech, which was reported at the Turin meeting, the roles of the quantum information carriers are reversed: they study cavity quantum electrodynamic systems in which the interaction between different photon states is mediated by an atomic state (in this case, of a Cs atom in a beam passing through a high-finesse optical cavity). These workers have determined indirectly that this setup would provide an atomic-state dependent phase-shift (up to 16° in one experiment), from which logic gates like the exclusive-or could be built up.

These last few examples are illustrative of a general theme that pervaded both theoretical and experimental discussions at Turin (and elsewhere): a lot can be done in systems where quantum states can be controllably interconverted from one physical form to another. Fundamental new approaches to experiments involving the Einstein-Podolsky-Rosen paradox, which have implications for real quantum cryptography, may come out of these discussions. An EPR pair (made out of two photons, say) is usually a fleeting thing, lasting as long as it takes them to traverse an experimental apparatus to a detector. Suppose, instead, that the photon quantum state could be "swapped" using dark-state spectroscopy into a long-lived quantum state like the Zeeman sublevels of an atomic ground state; such a state is potentially some six orders of magnitude longer-lived than the original photon state. This capability of storing two halves of an EPR pair for a long time is a prerequisite for many novel forms of quantum information transmission. One interesting protocol introduced at Turin which has been discussed recently is a so-called "purification" process. Suppose a collection of particles, each of which is half of an EPR pair, is received and stored, but that some corruption of the quantum state (losses, decoherence) occurs during transmission or storage. In purification, this collection of particles is processed, so as to produce a smaller number of particles, each of which is a member of a now nearly perfect EPR pair. Such a technology would open up a variety of possibilities: It would provide a new way of assuring privacy in cryptographic transmissions. It would make possible the separation of EPR pairs by much greater distances, permitting quantum cryptography and teleportation[3] to be practiced over distances much farther than a typical photon can travel through an optical fiber without loss. And, it points the way to a possible error correction scheme for quantum computation.

The actual processing involved in purification is a sequence of quantum-coherent exclusive-or gates supplemented by classical messages between the two parties; thus, purification *is* itself a kind of quantum computation. Workers at Turin were encouraged that other quantum computations of fundamental interest exist besides the famous Shor prime factorization algorithm. It is also heartening that purification (and a few other quantum computations) become useful at scales far below quantum factorization: Shor's algorithm definitively surpasses classical factorization methods only for quantum computations involving perhaps millions of quantum gate operations, while for purification the number of gates may only be in the tens. Workers in field see even tens of gates as a monumentally difficult job experimentally, and no one has any idea when the "engineering" era will be entered even for this simple a computation. Needless to say, Shor factoring is much, much more remote. Still, when Peter Shor offered a wager during his seminar at Turin that the first factoring of a 500-digit number would be accomplished on a quantum computer, there were no takers on the other side.

Although Rolf Landauer was not in attendance at Turin, his work[4] throughout the "visionary era" of quantum computing exercised an influence over much of the present work. His role has been unique during this period — he has constantly challenged the "visionaries" to show a workable path to the future. He skeptically pointed out that abstract Turing-machine Hamiltonians do not make an apparatus, that dissipation and disorder are inherent in physical systems and cannot be ignored, and that computers would not be what they are without error correction. As a result, Landauer's points now serve as accepted terms of admission to the "experimental era". The serious workers in the field are proposing real apparatus, not abstraction; they are worrying about and calculating the effects of dissipation and disorder; and they are struggling with the meaning of error correction in a quantum-coherent system (so far without conclusive demonstration of success).

References

[1] T. Pellizzari *et al.*, "Decoherence, continuous observation and quantum computing: a cavity QED model", preprint (June, 1995).

[2] J. I. Cirac and P. Zoller, "Quantum computations with cold trapped ions", Phys. Rev. Lett. **74**, 4091 (1995).

[3] Tony Sudbery, "Instant Teleportation", Nature (News and Views) **362**, 586 (1993).

[4] R. Landauer, "Is quantum mechanics useful?", Trans. Roy. Soc. Lond., in press.