QUANTUM COMPUTING

The Advantages of Superposition

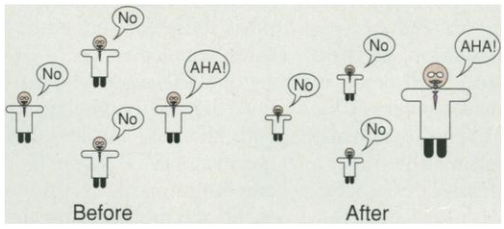
Lov K. Grover

Although transistor-based computers obey quantum mechanics, their logic states are only 1 or 0. If logic elements are allowed to be in quantum superpositions of states, however, fast solutions to hard problems are possible. One example is the exhaustive search problem: identify an item satisfying a specific property out of an unsorted list of N items. Once an item is examined, it is easy to tell whether or not it satisfies the property. However, the list has no known structure by which one can anticipate which item is more likely to satisfy the property. Under these circumstances, any classical algorithm, whether probabilistic or deterministic, will need to examine at least $0.5N$ items to succeed with a probability of 0.5. Quantum computers can be in a superposition of states and simultaneously examine multiple items; hence, there is the possibility of searching faster than with classical computers. It was recently shown that a quantum computer could search the list in less than $\sqrt{N}$ steps (*1*). This result has aroused considerable interest because several important problems are solved by an exhaustive search (*2*). Recently, fast search algorithms have been implemented in liquid ensembles of molecules through nuclear magnetic resonance [(*3*); see also the commentary by Jones on page 229 (*4*)].

The quantum search algorithm starts by setting the system to a superposition of N states corresponding to the N items to be searched. It can now examine all N items simultaneously. However, if it is programmed to immediately print out the item examined, it will only print out the right item with a probability of $1/N$ because only one of the N items examined satisfies the desired property. Instead, by carrying out a set of quantum operations, it is possible to increase the probability in the desired state at the expense of other states. After this, it will indeed print out the desired item with a high probability.

A quantum system is defined by specifying the amplitude in each state, which in general is a complex number—the probability in each state is the square of the absolute value of this amplitude. Just like classical probabilistic processes, quantum operations are required to follow their own conservation law, which leads to the constraint that all quantum operations have to be unitary; that is, they must be rigid rotations of the amplitude state vector in the N-dimensional state space. This leads to wavelike behavior of particles at the microscopic level. Two elementary quantum operations are quantum diffusions and phase rotations. In fact, the quantum search algorithm consists of an alternating sequence of quantum diffusions and phase rotations.

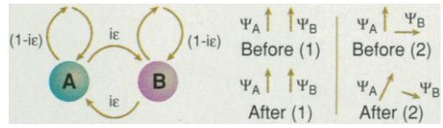
Quantum diffusion is similar to classical diffusion except for the fact that the fraction of the amplitude transferred from one state to the other is imaginary (see figure at right). If the amplitude of the system in two states is the same, then the amplitude transferred in each direction is the same and there is no net transfer. However, if the amplitude in one state is rotated with respect to the other state, then there is a net transfer from one state to the other. As a result of this transfer, the net rotation between the two states gets reduced. In Schrödinger's equation, the states are the points of an infinitesimal grid—there is a quantum diffusion between neighboring grid points along with a continuous phase rotation that is determined by the potential. As a result, there is a net transfer of amplitude into states of low potential, just as one would expect classically.



Split personality. Quantum mechanical systems can simultaneously be in multiple states and carry out multiple computations. The quantum search algorithm amplifies the probability in the desired state by a sequence of simple unitary operations.

Just like a classical computer, a quantum computer can be represented by a multitude of binary systems. Each binary system is a quantum mechanical bit, called a qubit, which is in a superposition of two states. The quantum search algorithm starts by setting the system of n qubits to a uniform superposition of all $N = 2^n$ states. An alternating sequence of quantum diffusions and phase rotations is then carried out. After about $\pi\sqrt{N}/4$ repetitions, the amplitude becomes concentrated in the desired state. A measurement then reveals the desired state with certainty.

A version of this algorithm has recently been implemented for the special case $N = 4$ through nuclear magnetic resonance technology with the use of an organic molecule as a two-qubit quantum computer (*3*, *4*). This implementation needed only a single quantum query to search an unsorted list of four items with certainty; any classical algorithm would need an average of 2.25 queries and a worst case of 3 queries.



From state to state. Quantum diffusion is the transfer of a small imaginary amplitude from one state to another. If the phase of one of the states is rotated with respect to the other, there is a net transfer from one state to the other.

Landmark developments, such as this first demonstration of an important quantum algorithm, give one an opportunity to pause and assess the state of the art. There are two sets of challenges confronting quantum computers: the hardware and the software. The hardware challenge arises from the fact that the physics of quantum computational devices is different from that of existing devices and we do not know what the ultimate structure of these will be. The hardware must satisfy somewhat contradictory requirements: first, it must be isolated to prevent environmental disturbance, and, second, different parts of the system must interact in a controllable way. Existing devices, such as transistors, are too closely coupled to their environment. Nuclear magnetic resonance satisfies both conditions to some extent. The next big hardware challenge is to increase the number of qubits from two to something on the order of five to ten; this will permit more sophisticated algorithms. The software challenge is to find applications that will justify the effort of building quantum hardware. It has been shown that the quantum search algorithm itself cannot be further improved for the application of an exhaustive search. Nevertheless, there has been considerable research on extending it to other applications.

The author is at Bell Labs, Lucent Technologies, Murray Hill, NJ 07974, USA. E-mail: lkgrover@bell-labs.com

References

1. L. K. Grover, *Phys. Rev. Lett.* **79**, 325 (1997).
2. G. Brassard, *Science* **275**, 627 (1997); G. P. Collins, *Phys. Today* **50**, 19 (October 1997).
3. I. Chuang, N. Gershenfeld, M. Kubinec, *Phys. Rev. Lett.*, in press.
4. J. A. Jones, *Science* **280**, 229 (1998).