

Quantum Computing with Molecules

By taking advantage of nuclear magnetic resonance, scientists can coax the molecules in some ordinary liquids to serve as an extraordinary type of computer

by Neil Gershenfeld and Isaac L. Chuang

Factoring a number with 400 digits—a numerical feat needed to break some security codes—would take even the fastest supercomputer in existence billions of years. But a newly conceived type of computer, one that exploits quantum-mechanical interactions, might complete the task in a year or so, thereby defeating many of the most sophisticated encryption schemes in use. Sensitive data are safe for the time being, because no one has been able to build a practical quantum computer. But researchers have now demonstrated the feasibility of this approach. Such a computer would look nothing like the machine that sits on your desk; surprisingly, it might resemble the cup of coffee at its side.

We and several other research groups believe quantum computers based on the molecules in a liquid might one day overcome many of the limits facing conventional computers. Roadblocks to improving conventional computers will ultimately arise from the fundamental physical bounds to miniaturization (for example, because transistors and electrical wiring cannot be made thinner than the width of an atom). Or they may come about for practical reasons—most likely because the facilities for fabricating still more powerful microchips will become prohibitively expensive. Yet the magic of quantum mechanics might solve both these problems.



The advantage of quantum computers arises from the way they encode a bit, the fundamental unit of information. The state of a bit in a classical digital computer is specified by one number, 0 or 1. An n -bit binary word in a typical computer is accordingly described by a string of n zeros and ones. A quantum bit, called a qubit, might be represented by an atom in one of two different states, which can also be denoted as 0 or 1. Two qubits, like two classical bits, can attain four different well-defined states (0 and 0, 0 and 1, 1 and 0, or 1 and 1).

But unlike classical bits, qubits can exist simultaneously as 0 and 1, with the probability for each state given by a numerical coefficient. Describing a two-qubit quantum computer thus requires four coefficients. In general, n qubits demand 2^n numbers, which rapidly becomes a sizable set for larger values of n . For example, if n equals 50, about 10^{15} numbers are required to describe all the

probabilities for all the possible states of the quantum machine—a number that exceeds the capacity of the largest conventional computer. A quantum computer promises to be immensely powerful because it can be in multiple states at once—a phenomenon called superposition—and because it can act on all its possible states simultaneously. Thus, a quantum computer could naturally perform myriad operations in parallel, using only a single processing unit.

Action at a Distance

Another property of qubits is even more bizarre—and useful. Imagine a physical process that emits two photons (packets of light), one to the left and the other to the right, with the two photons having opposite orientations (polarizations) for their oscillating electrical fields. Until detected, the polarization of each of the photons is indeter-