Recent developments bring quantum computers closer to implementation

Bryan Dyne
8 January 2011

Richard Feynman first seriously posed the question of designing computers based on quantum mechanics in a paper published in 1982.[1] The most recent research into this field comes from a team from the Delft University of Technology and Eindhoven University of Technology, both in the Netherlands. In a paper recently published in the scientific journal *Nature*,[2] a new technique to manipulate the fundamental building blocks of quantum computers was examined.

Inspired by basic questions about the nature of light, quantum mechanics is the study of the most fundamental particles of matter. The most advanced quantum computing application currently imagined involves utilizing the inherent link that two particles, such as electrons, can form on the most elementary level to perform specified calculations.

Current computers are based on a binary digit, called a bit. The information stored is held in two distinct states, generally referred to as 0 and 1. The basic unit of a quantum computer is called a qubit. The value of a qubit is generally based in the inherent rotation of an electron, which is either negative or positive. Unlike a classical bit, which is always one value or the other, a qubit initially has both of these values. Only when acted upon will the qubit take on a single value, and it will do so following the probabilistic laws governing quantum mechanics.

A bit has a distinct disadvantage compared to a qubit. While 1000 bits could deliver about 1000 pieces of information at a time, 1000 qubits could deliver approximately 2^1000 (or 10^300) pieces of information simultaneously. This number is so large, that it is incomprehensibly larger than the number of grains of rice it would take to fill up the Solar System.

While exponentially more powerful than classical computers, quantum computers have also proven to be exponentially more difficult to build. Quantum computers revolve around the manipulation of individual quantum particles. While dealing with 1000 bits is easy for modern-day technology, working with 1000 qubits it incredibly hard. The quantum mechanical nature of qubits can cause unwanted interaction with their physical surroundings, destabilizing the entire system. Imagine a line of dominoes falling one after the other. This issue has been the reason that quantum computers have yet to exceed their classical counterparts.

Physics simulations were the original goal for quantum computers, and the impetus for Richard Feynman to write his 1982 paper. Feynman wanted to look at the possibility of a computer being able to fully simulate physical events, not just approximate them. Quantum mechanical systems were the particular focus. Unlike the random-event generators found in classical computers, the probabilistic nature of qubit states lets a quantum system be truly represented. This lets large systems of quantum particles be studied, which is utterly beyond the capabilities of classical computing.

Success at building a quantum computer would also be the most stringent test of quantum mechanics ever devised. If quantum computers can be built to outstrip classical computers, it would be the most powerful vindication of quantum theory yet. On the flip side, a demonstration of a fundamental reason that quantum computers *cannot* be built would require a serious re-thinking of much of physics.

A consequence of this technology would be immediately felt in the field of electronic security. Most secure communications and information storage revolve around a technique called RSA encryption. The process involves multiplying two prime numbers, such as 5 and 3, and using the product, 15, to encode data.

The power of this approach is based on multiplying prime numbers so large, that the product is hundreds of digits long. Classical computers simply cannot factor such a large number in any reasonable timescale. The original information, encrypted based on the two original numbers, is thus safeguarded.

In contrast, quantum computers would be able to take advantage of a procedure known as Shor's algorithm. The essence of the formula is that, using quantum computers, even extremely large numbers could be factored in a matter of moments. This would give the user of a quantum computer the ability to break into bank accounts, private email, and decipher computer passwords at a whim.

The specific advances of the new research involve the direct manipulation of electrons through electric fields. Previous experiments used magnetic fields, which do not have the precision necessary to form large numbers of qubits into a functioning system. The precision granted by using electric fields shows potential in keeping large amounts of qubits coherent long enough to perform calculations.

What should be noted is that quantum computers will not solve all problems posed in computer science. If they ever reach fruition, the highest use will be simulating quantum physics. They will not be adept at proving mathematical theorems nor will they discover new physics. Those would still be the province of human beings.

A major drawback of quantum computers is the issue of usage. Much of the research done on the subject is funded by private institutions and nation states. Any private institution with a quantum computer would be able to break down any barriers encountered in breaking into a competitor's system in seconds, giving an unparalleled edge in development. Even more disturbing, a government with a quantum computer could access secrets held by other nations with ease. Its apparatus for electronic spying, both foreign and domestic, would be without rival.

Quantum computing is an exercise in contradictions. The technical difficulties make it difficult to achieve, and the social and political consequences give pause over whether and how fast to move forward with this effort. On the other hand, humanity's knowledge of physics itself is in many ways bound up in showing whether such tools are possible. We owe it to ourselves to find out.

Notes:

[1] R. P. Feynman. *Simulating Physics with Computers*.

[2] S. Nadj-Perge, S.M. Frolov, E.P.A.M. Bakkers, L.P. Kouwenhoven. “Spin-orbit qubit in a semiconductor nanowire.”