Quantum Theorists Trying to Surpass Digital Computing

The New York Times

February 18, 1997, Tuesday, Late Edition - Final

Distribution: Science Desk

Section: Section C; ; Section C; Page 1; Column 4; Science Desk ; Column 4;

Length: 2198 words

Byline: By GEORGE JOHNSON

By GEORGE JOHNSON

Body

IN the never-ending effort to make sense of the universe, the human brain long ago bumped up against its limits. Unchastened, brains learned to amplify themselves with pencils and paper, slide rules, mechanical calculators and electronic computers. And the computers get faster all the time.

Eventually, humans will reach the physical limits of computation because the signals inside a computer cannot travel faster than light. But then they can put two supercomputers together in parallel, or 10 supercomputers, or a hundred, or a million, and let them work on different parts of a problem at the same time.

The mental horizon would seem limitless, except for the sobering truth that there are some problems that even the fastest conceivable digital computers are unable to solve. The problems are what mathematicians call intractable. Finding the answer would take more time than Earth -- or even the universe -- is expected to exist.

What is needed is another great technological leap: some kind of problem-solving device that on a very fundamental level is more powerful than a digital computer. In the last few years, a steady accumulation of both theoretical and experimental breakthroughs has raised hopes that just such an invention is within the realm of possibility. By harnessing the peculiar logic called quantum mechanics that governs the world inside atoms, scientists are trying to invent a radically different kind of computing: an information-processing method so powerful that it would be to ordinary computing what nuclear energy is to fire.

"Just a few years ago, it was thought that ***quantum computing*** was impossible," said Dr. Raymond Laflamme, a physicist at Los Alamos National Laboratory in New Mexico. "Now we have passed some big stumbling blocks. The possibilities are very exciting."

Theorists recently proved that by manipulating subatomic particles as though they were beads in an abacus, a ***quantum computer*** could in principle crack problems that now seem impenetrable. Buoyed by this possibility, experimenters have begun to build the first rudimentary components -- each as small as a single atom -- needed to make such a machine.

Even the fastest conventional supercomputer, primed with the cleverest software, would take hundreds of millions of years to examine a 300-digit number and find all its factors, the numbers it can be evenly divided by. But a ***quantum computer***, if one could be constructed, would perform the task in minutes.

Since the codes used to protect military and commercial secrets rely on the near-impossibility of factoring large numbers, the National Security Agency, the Government's premier code-making and code-breaking department,

has begun closely following the field. And the Defense Department's Advanced Research Projects Agency, which is famous for research on speculative endeavors like artificial intelligence, has placed a modest bet of $5 million over five years to study ***quantum computers***.

"The N.S.A. would obviously prefer that ***quantum computing*** were not possible," said Dr. Seth Lloyd, a physicist at the Massachusetts Institute of Technology. "But if it does turn out to be possible, then they need to be prepared." Although large hurdles lie ahead, Dr. Lloyd said, "***quantum computing*** is coming tantalizingly close to being something that might work." And even if the grand effort should ultimately fail, physicists say, the research is giving them a deeper understanding of the peculiarities of quantum physics than was possible before.

The key to this new kind of computation is a phenomenon called quantum superposition. Consider the case of an electron hovering around the nucleus of an atom. According to quantum mechanics, the electron cannot be said to be in a single definite position. It exists instead in a kind of limbo, a superposition that consists of every possible location it could conceivably occupy.

Only when the electron is measured, or somehow disturbed by the outside world, does the superposition break down: the particle crystallizes from the quantum haze and becomes fixed in space and time. It is this process, called quantum decoherence, that gives rise to the everyday world in which things can be in only one place at a time.

Hard as they are to imagine, quantum effects lie at the root of the most familiar phenomena. Think of a beam of light bouncing off a spot on a mirror. The angle at which the light beam strikes the mirror equals the angle at which it is reflected, a truth so basic that it is taught in high school science class. But behind the scenes, there is much more going on.

Light is made of particles called photons, and photons obey quantum rules. Defying all common sense, the photons in the light beam can be thought of as simultaneously bouncing off every single point on the mirror's surface as though they were trying out all the many possible paths. Some of these paths reinforce each other, while most cancel each other out, somewhat in the way that the positive number 5 added to a negative 5 equals 0. Ultimately, all that is left is the single trajectory that is observed.

In a similar way, a ***quantum computer*** would be capable of a powerful kind of parallel processing that goes far beyond what is possible with even the most advanced digital machines. In a ***quantum computer***, all the calculations needed to solve a problem could be performed simultaneously, like the photons trying out every possible path as they are reflected by a mirror. Most of these calculations would cancel out, leaving the correct answer to the problem.

Until very recently, trying to compute by using quantum mechanics was an obscure and somewhat disreputable endeavor. "It was dismissed as just a bunch of funny old guys in an office thinking about something with no practical application," Dr. Laflamme said.

One of the misfits was Dr. Richard P. Feynman, who shared a Nobel Prize in 1965 for his part in developing quantum electrodynamics, the theory explaining how electrons and photons interact; Dr. Feynman died in 1988. In the early 1980's, he and a few other scientists and mathematicians, including Dr. Paul Benioff at Argonne National Laboratories and Dr. David Deutsch at Oxford University, began toying with the idea of ***quantum computation***. But no one paid much attention.

The field languished until 1994, when Dr. Peter Shor of AT&T Labs in Murray Hill, N.J., wrote a program that would rapidly factor large numbers on a quantum machine (assuming one could be built). By simultaneously examining all the possibilities in quantum superposition -- the good answers reinforcing each other, the bad ones canceling each other out -- Dr. Shor's algorithm would rapidly solve what had long been an impenetrable problem.

But first, scientists need to build a machine to run the program. In an influential 1993 paper, "A Potentially Realizable ***Quantum Computer***," published in the journal Science, Dr. Lloyd described how a ***quantum computer*** might be built. In a regular computer, bits -- the 1's and 0's of binary code -- are manipulated by tiny switches called

logic gates. A NOT gate, for example, takes its input signal and inverts it. Give the gate a 1 and it will return a 0, and vice versa. Other gates have two inputs. An AND gate will return a 1, only if both its inputs (X and Y) are 1. An OR gate will say 1 if either of its inputs (X or Y) is 1.

Technology has managed to shrink conventional computer circuitry so millions of these gates can fit on a single chip. But the gates in a ***quantum computer*** would be so small that each would consist of a single atom, which means that they would behave quantum mechanically. In the hypothetical ***quantum computer*** that Dr. Lloyd proposed, three different kinds of atoms -- call them A, B and C -- are repeated to form a long chainlike molecule, called a polymer: ABCABCABCABCABC.

Each of these atoms' nuclei is orbited by an electron that could be manipulated to perform a computation. Normally, the electron would rest in its lowest energy state, representing the binary digit 0. But if it was struck just so by a laser, the electron would rise to a higher energy state, representing 1. A second pulse from the laser would reset the atom to 0.

Different kinds of atoms respond to different colors of light, so it would be possible to choose which atoms to switch on and off. In fact, one could tailor the laser signals to tell all A's whose neighbors had a particular value, 1 or 0, to register a 1. That is just the kind of shuffling of binary digits that is the essence of computation.

So far, what has been described is no different from a vanishingly tiny version of a conventional digital computer. Here is the crucial difference: Since this is a quantum system, each electron can also be in both states, 1 and 0, at the same time. Because of this peculiarity, the bits in a ***quantum computer*** are called quantum bits, or qubits, for short. They have more "degrees of freedom" than an ordinary bit, which can be only 1 or 0, and that allows for more powerful information processing.

For all the excitement caused by Dr. Shor's factoring algorithm and Dr. Lloyd's abstract design for a ***quantum computer***, still more obstacles must be overcome. One of the sharpest critics of ***quantum computing***, Dr. Rolf W. Landauer of the I.B.M. Thomas J. Watson Research Center, in Yorktown Heights, N.Y., is fond of noting how very delicate and error-prone a ***quantum computer*** would be.

In a conventional computer, mistakes -- a 1 that has improperly shifted to 0, or vice versa -- are kept from accumulating by error-correction schemes. The key is redundancy. Instead of writing 1, the computer writes 111; instead of 0, it writes 000. If somewhere in the long chain of calculations, the cluster 101 or 110 appears, it is a clue that a bit has gone astray and needs to be reset to its correct value.

For a long time, it was thought that with qubits, error correction would be impossible. To detect an error, it seemed obvious that one would have to read the bit in question to see whether it had flipped to the wrong value. But under the rules of quantum mechanics, measuring a qubit would instantly cause the superposition -- all those simultaneous computations -- to come undone. The calculation would be derailed as surely as if one dumped a bucket of water inside a PC.

But once again, scientists had underestimated the strange things that are possible on the quantum realm. Dr. Landauer said no one had been as surprised as he when Dr. Shor showed in 1995 how quantum error correction could be done. Dr. Shor proved that it was possible to determine whether a qubit's value was right or wrong without actually reading it and disturbing the superposition. The trick involves a quantum version of redundancy, in which a cluster of nine qubits is used to encode a single bit of information. (Dr. Laflamme and Dr. Wojciech Zurek at Los Alamos have since shown that quantum error correction could be done with just five qubits.)

"I had been too pessimistic -- it's that simple," Dr. Landauer conceded. But he said he was still not convinced that the practical problems of building reliable ***quantum computers*** could be overcome. "I'm not ready to put my money in ***quantum computing***," he said.

With some of the problems solved -- on paper, anyway -- physicists have started experimenting with the tiny parts that would be needed to make a ***quantum computer***. At the National Institute of Standards and Technology in Boulder, Colo., Dr. David Wineland and his colleagues have coaxed an atom of beryllium to act like a quantum logic

gate, processing 1's and 0's. At the California Institute of Technology in Pasadena, a team led by Dr. H. Jeffrey Kimble is making quantum components using photons and cesium atoms.

So far, experimenters have managed to make single quantum logic gates. Factoring a 300-digit number would require stringing together thousands of gates, and even ***quantum computing***'s most enthusiastic supporters admit that such a goal is exceedingly daunting.

"Theory is way ahead of experiment," Dr. Kimble said. "It's like Hannibal trying to cross the Alps. We'd really like to run ahead and see what's on top, but we have all these elephants to deal with."

But in a paper published last year in Science, Dr. Lloyd showed that even a very simple ***quantum computer*** would be useful for a different kind of problem: studying the strange behavior of the subatomic world. He calculates that simulating 50 subatomic particles, interacting quantum mechanically, would take even a powerful supercomputer with trillions of logic gates many years. A ***quantum computer*** with 50 quantum gates could perform the simulation with ease.

Even if it never becomes practical to make even small-scale ***quantum computers***, theorists like Dr. Zurek at Los Alamos predict that the recent breakthroughs will lead to a more profound understanding of how the counterintuitive behavior of subatomic particles gives rise to what is quaintly called the real world.

"While trying to implement a ***quantum computer***, we are bound to learn a lot about how this transition occurs," Dr. Zurek said. "Even if we don't build a ***quantum computer***, we will learn so much by trying that the effort is worth pursuing."

Graphic

Photos: Work on using ***quantum computing*** by Dr. Peter Shor of AT&T Labs, left, has drawn skepticism from Dr. Rolf W. Landauer, an I.B.M.researcher. (Dith Pran/The New York Times; Joyce Dopkeen/The New York Times)(pg. C6)

Diagram: "The Unpredictable Computer"

In a digital computer, information - numbers, words, pictures, sounds - is coded as a long string of binary digits called bits. Each bit can be either 1 or 0. Because of the paradoxical rules of quantum mechanics, the bits in a ***quantum computer***, called qubits, can be not only 1 or 0, but 1 and 0 at the same time. This phenomenon, called quantum superposition, allows for more powerful computation, solving problems that would boggle a regular digital computer. (Illustration by Al Granberg)

Classification

Language: ENGLISH

Subject: BRAIN (89%); PHYSICS (89%); ***QUANTUM COMPUTING*** (89%); QUANTUM MECHANICS (89%); RESEARCH & DEVELOPMENT (78%); SCIENCE & TECHNOLOGY (78%); MATHEMATICS (74%); INTERNATIONAL RELATIONS & NATIONAL SECURITY (70%); INTELLIGENCE SERVICES (69%); ARTIFICIAL INTELLIGENCE (65%); GOVERNMENT & PUBLIC ADMINISTRATION (65%); NATIONAL SECURITY (64%); DEFENSE DEPARTMENTS (63%); SPECIAL INVESTIGATIVE FORCES (60%)

Company: LOS ALAMOS MONITOR (53%); LOS ALAMOS MONITOR (53%)

Industry: COMPUTER EQUIPMENT (90%); ***QUANTUM COMPUTING*** (89%); SUPERCOMPUTERS (89%); COMPUTER SOFTWARE (73%); ARTIFICIAL INTELLIGENCE (65%); DEFENSE DEPARTMENTS (63%)

Geographic: NEW MEXICO, USA (86%)

Load-Date: February 18, 1997

End of Document