QUANTUM LEAP;
Peculiar logic could take computers where no others have gone before

The Houston Chronicle

March 24, 1997, Monday, 2 STAR Edition

Section: DISCOVERY; Pg. 6

Length: 2014 words

Byline: GEORGE JOHNSON; New York Times

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 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 theoretical and experimental breakthroughs has raised hopes that just such an invention may be possible.

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

QUANTUM LEAP;Peculiar logic could take computers where no others have gone before

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.

""The NSA 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, 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 an electron hovering around
the nucleus of an atom. In 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.

QUANTUM LEAP;Peculiar logic could take computers where no others have gone before

Only when the electron is measured, or disturbed by the outside world, does the superposition break down: the particle crystallizes from the quantum haze and becomes fixed in space and time. This process, called quantum decoherence, 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.

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,'' Laflamme said.

One of the so-called 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; Feynman died in 1988. In the early 1980s, he and a few other scientists and mathematicians, began

QUANTUM LEAP;Peculiar logic could take computers where no others have gone before

toying with the idea of ***quantum computation***.

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, 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, Lloyd described how a ***quantum computer*** might be built. In a regular computer, bits - the 1s and 0s 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 Lloyd's hypothetical

quantum computer, three different kinds of atoms - call them A, B and C - are repeated to form a long chainlike m olecule, 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 laser pulse 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. It is just the kind of shuffling of binary digits that is the essence of computation.

QUANTUM LEAP;Peculiar logic could take computers where no others have gone before

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 Shor's factoring algorithm

and 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 IBM 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. If somewhere in the chain of calculations, the cluster 101 or 110 appears, it is a clue that a bit needs to be reset.

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.

Again, scientists had underestimated the strange things that are possible on the quantum realm. Landauer said no one had been as surprised as he when Shor showed in 1995 how quantum error correction could be done. Shor proved it was possible to determine whether a qubit's value was right or wrong without actually reading it and disturbing the superposition. The trick is a quantum version of redundancy, in which a cluster of nine qubits is used to encode a single bit of information.

(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,'' 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***.

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,'' 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 even if it never becomes practical to make

even small-scale ***quantum computers***, theorists such as 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.

———————————————

 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 phonomenon, called quantum
superposition, allows for more powerful computation, solving
problems that would boggle a regular digital computer.

Graphic

QUANTUM LEAP;Peculiar logic could take computers where no others have gone before

Graph: 1. The unpredictable Computer (TEXT); Photos: 2. Dr. Peter Shor; 3. Dr. Rolf Landauer; 1. Illustration by Al Granberg/N.Y. Times News Service, 3. Associated Press

Classification

Language: ENGLISH

Subject: PHYSICS (89%); ***QUANTUM COMPUTING*** (89%); QUANTUM MECHANICS (89%); SCIENCE & TECHNOLOGY (78%); MATHEMATICS (74%); INTERNATIONAL RELATIONS & NATIONAL SECURITY (71%); INTELLIGENCE SERVICES (70%); GOVERNMENT & PUBLIC ADMINISTRATION (66%); NATIONAL SECURITY (64%); SPECIAL INVESTIGATIVE FORCES (50%)

Company: MASSACHUSETTS INSTITUTE OF TECHNOLOGY (60%); MASSACHUSETTS INSTITUTE OF TECHNOLOGY (60%)

Industry: COMPUTER EQUIPMENT (90%); ***QUANTUM COMPUTING*** (89%); PUBLISHING (73%); COMPUTER SOFTWARE (72%)

Geographic: NEW MEXICO, USA (68%)

Load-Date: March 25, 1997

End of Document