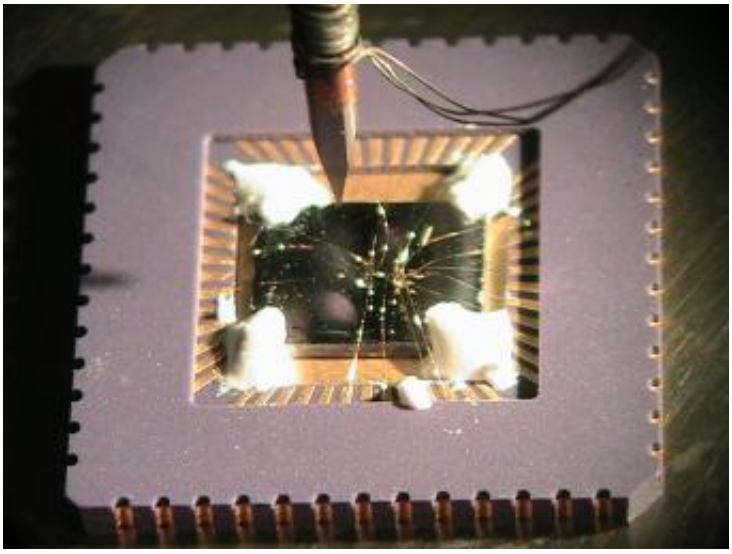
Quantum Computing Steps Forward

January 20 2006



With the University of Michigan's latest production of a quantum chip, it's another step forward for quantum computers that will someday dwarf the abilities of today's machines.

Working with individual ions or atoms – much smaller than the transistors of even the most advanced microchips - quantum computers may be both more powerful and more compact than existing computers by various orders of magnitude.

Common computers today are thousands of times more powerful and more compact than the first 30 ton behemoths, but they use virtually the

same logic. The fundamental design has gone unchanged for 50 years.

Quantum computing is whole new ball game. The secret lies in the almost magical property of quantum matter to adopt two states simultaneously. Normal integrated circuits store data using transistors which have just two states – on and off. Each quantum circuit, or qubit, can represent at least three states: on, off or both by an effect called quantum superposition. This means much more data can be stored on each individual circuit.

Actually, qubits can potentially contain many states. Dr Andrew White, Senior Lecturer in Physics at University of Queensland describes a qubit like this: “A quantum computer takes that on or off state and adds many different possible states. The first thing, if you think of the globe, let the South Pole be on, the North Pole off – that’s not a very good description of the globe. A quantum computer let’s you describe information by saying, look, you can take an arrow from Earth’s center and point it at the North Pole, South Pole or Los Angeles or London, and that’s richer description. You can fit much more information on a single qubit.”

Based on Dr. White’s description, a single qubit could replace a whole bank of conventional memory. Normal memory holds a large array of binary numbers expressed as on or off transistors – ones or zeros. Many transistors are needed to express anything more than just a simple number – hence today’s computers need for large memories. For example: you need 8 bits plus one bit for error correction to store the binary number for 256 which is expressed as 11111111. Going back to our globe example, our arrow could point to Amsterdam which could represent 256 – or any other number. A single qubit could store more information than thousands of transistors.

This compact storage leads to another advantage: speed. Without the need to access many memory locations to read data, retrieval is almost

instantaneous.

Quantum computers will represent a huge leap in processing power as well – they could execute instructions exponentially faster because there would be almost no limit to the size of the instruction. Currently, most computers use 32 or 64 bit instructions.

There is another exciting benefit to working with quantum reactions: Entanglement. It describes the ability of quantum matter to “link” two particles. Change one particle and the other changes – instantaneously, even though there is no physical connection! And distance may be irrelevant! This property – not fully understood – would enable computers to talk to each other with no time lag over long distances.

Anton Zeilinger at the Institute of Experimental Physics in Vienna, Austria, preformed an experiment to demonstrate entanglement: their group strung an optical-fiber cable in a sewer tunnel under the Danube River with an "entangled" photon at each end. They measured of the state of polarization in one photon (horizontal, vertical, etc…) establishing that the other proton immediately had an identical polarization.

What will be the difference to normal computer users? Try instant access to any type of data – whether it is in your computer or on the other side of the planet. As for processing power, few users rarely exceed the abilities of today’s computers. Much computer hardware is used to generate the fancy graphical interface we call Windows – with plenty left over in reserve.

Those not familiar with computer science are often surprised to learn there are still a few applications that cannot run easily on today’s computers. They lack of sufficient processing power to do climate modeling, artificial intelligence or break strong encryption.

The NSA (National Security Agency) would love to be able to break many a foreign power's encrypted communications, but has been stymied by the lack of a sufficiently fast computer for the job. Experts estimate it would take more than the lifetime of the Universe using all the computers in the world to break a 1024 bit encryption key – the current standard for serious encryption applications. It's worth noting that most commercial encryption only uses a 40 bit key. A quantum computer has the potential to break any encryption in a few days.

Scientists who study global warming and climate would like to have finer-grained models to be able to predict the weather more effectively and determine the real impact man's activities have over the planet. Current computers, although fast, still take hours or days to produce weather simulations that lack detail.

Artificial intelligence is another field that could use the extra processing power. Current algorithms simply can't be processed fast enough and, admittedly, may need more refining. However, a quantum computer could theoretically contain more processing power than the human brain in a smaller space – making true AI possible.

In fact, more powerful computers often come along well before a use is found for them. In the future, more uses will be found for quantum machines as their tremendous processing power becomes available.

But having the machine is not enough. All of today's software is based on the silicon technology it runs on. New software is already being written to take advantage of quantum computation.

One of the most important steps is to write software for error checking. All computers use some type of system to make sure a bit hasn't accidentally "flopped" from a one to a zero. Quantum computer components, because of their atomic size, will be very susceptible to

errors. In fact, one of the biggest problems faced by the scientists working on quantum computing is the problem associated with checking the state of an object so small. How does one check the value of a qubit without changing it? Error checking will be of critical importance and computer scientists have already developed some ideas to insure accuracy in quantum systems.

They have also already developed algorithms and equipment for super strong quantum encryption designed to allow hacker-proof security for communications. The National Security Agency and Federal Reserve banks can now buy a quantum cryptographic system from several companies. Anyone who intercepts and tries to read the stream of photons used will disturb the photons in a way that is detectable to both sender and receiver.

Quantum encryption represents the first major commercial implementation for what has become known as quantum information science - a blending of quantum mechanics and information theory.

As for the software you use in day-to-day computing, no changes will be necessary. Just as software emulators permit Apple users to run Windows and Windows software on the Mac's Power PC processor – albeit sacrificing some speed – an emulator could quite easily run any programs today at speeds that make the today's fastest processors look frozen. So you won't need to run out and buy Microsoft Office 2030 for Quantum Computers – although Bill Gates, if he's still alive, might like that.

It may also change the way we do computing. Like times past when computers were very expensive, we may share a large, centralized quantum computer – one that has the capacity to handle quadrillions of transactions. Connections would be via fiber optic connections and personal data – a whole lifetimes worth – could be stored on a quantum

USB-type memory the size of a credit card. This would eliminate the need to have millions of PCs that require upgrading every few years.

Don't expect any of this to happen tomorrow. Scientists are still struggling with some tough problems. Which is the best material from which to make quantum systems? How to check qubit values and not lose the information at the same time? What mechanisms are involved in entanglement? Some experts predict it will be 20 years before we see the first fully functional computers that use quantum materials.

No mater how long it takes, money will continue to flow into research efforts. Silicon-based processors are beginning to near the physical limit of smallness and speed. Intel's best processors currently fabricated using .15 micron process and run 3GHZ.

One day we may have more processing power than we know what to do with. It will be up to our imaginations – something no computer may ever accurately match - to think of new problems for these enormously powerful machines to solve.

by Philip Dunn, Copyright 2005 PhysOrg.com