Quantum Computers

Group Members
Chelsea Richardet, David McDiarmid, Fei Ye

Group Name
Qubit

Statement of Position
Computer technology has come a very long way since the days of warehouse-sized computers. Computers have become much smaller, more advanced, and are now capable of processing information much more quickly than in the past. However, conventional computers are still not fast as we would like them to be and they tend to take too long when processing enormous amounts of information. Quantum computers take advantage of the latest physical theories of quantum mechanics and house great potential for performing calculations at a much faster rate than modern-day computers. Quantum computers will not only be faster, but will be able to store enormous amounts of memory. Our group will be doing our research project about the possible implications quantum computers may have on technology in society. The introduction will provide the history of quantum computers starting with the conception of the idea. Relevant background information and the mechanics of quantum computers (ie. how they work) will be discussed in the body. The argument of the presentation will outline potential applications and technical issues associated with quantum computing. A conclusion will summarize the major points presented about quantum computers.

History of Quantum Computing
The development of quantum computer, as well as the development of any invention started with an idea. Like some other inventions, many people get the similar idea and work on it from different angles.

In 1969 Steven Wiesner suggested quantum information processing as a possible way to better accomplish cryptologic tasks (Wiesner published his paper about it in 1983).

In 1970s, physicists and computer scientists explored the idea of a computational device based on quantum mechanics. Alexander Holevo (1973), R.P. Poplavskii (1975), Roman Ingarden (1976) and Yuri Manin (1980) were the first four people who published their papers on quantum information.

In 1982, Richard Feynman, the Nobel prize-winning physicist, thought up the idea of a ‘quantum computer’, a computer that uses the effects of quantum mechanics to its advantage. He also explained how a machine would be able to act as a simulator for quantum physics. In other words, a physicist could carry out experiments in quantum physics inside a quantum mechanical computer.

In 1985, David Deutsch, of Oxford, publishes a theoretical paper describing a universal quantum computer. Quantum
In 1994, Peter Shor, working for AT&T, published a paper in which he set out a method for using quantum computers to crack an important problem in number theory, namely factorization. In principle, his algorithm would far surpass the efficiency of any known computer when executed on a quantum computer.

With these breakthroughs, quantum computing transformed from a mere academic curiosity directly into a national and world interest.

How It Works

Quantum Computers is somewhat similar to a normal computer in some aspects, but it is much more advanced. Take the Turning machine, developed by Alan Turning in the 1930's. It is a device that has tape which is split into small square of unlimited length. Each square has a symbol that may be a zero or a one. A read-write device reads the symbols giving instructions to the machine. This is done by using bits. In a quantum computer, both the tape and also the read-write device are in a quantum state. Because it is in a quantum state the symbols of the tape can be zero, one, and anything between. This is what physicists call superstition. Because it can be multiple symbols this indicates that the quantum computer can do many tasks at a time (unlike a normal computer which can only perform one calculation at a time). Also, in a quantum computer the tape uses quantum bits, or qubits instead of bits. By exploiting the properties of quantum mechanics it has the potential to do calculations much faster then the fastest super-computer we have now.

Another aspect that a quantum computer utilizes is entanglement. When physicists try and look at atoms they have a very significant possibility that they could bump the atom which in turn could change their value completely. The problem with this is that, if one atoms value changes it could potentially change many other atoms which could then change the calculation entirely. To get away from this they wait until an atom bumps into another one on its own. When this happens the atom will choose a certain spin or value that it has. In turn the atom that it bumped will choose the opposite spin or value. This allows the physicists to see the state that the atoms are in without actually bumping them themselves. With this new technology it can support entirely a new kind of computation with new algorithms based on quantum computers.

Quantum Computers: Applications and Technical Issues

Proposed Applications of Quantum Computers: -Mathematical problems could be solved much faster (Häffner et al., 2008), or exponentially faster depending on the problem (O'Brien, 2008). It has been suggested that quantum computers could be 'millions of times more powerful' than modern-day computers (Boyle, 2004). -Physical problems could be solved in greater detail and with more input variables (O'Brien, 2008) and solutions to problems involving quantum mechanics could be generated (Häffner et al., 2008). -Enormously large numbers can be factored much more quickly (Shor, 1994). This is because quantum computing has an extremely fast rate of 'polynomial time factoring' which would speed up the calculations (Hirvensalo, 2001). -Quantum computers have the ability to run quantum algorithms (Gea-Banacloche, 2003), such as Peter Shor's algorithm (Shor, 1994). -It would be easier to crack encrypted codes with quantum computation (Gea-Banacloche, 2003). For example, RSA encryption, which requires enormous processing power, could be implemented with quantum computers (West, 2000). Therefore, quantum computing also allows for greater security (Hirvensalo, 2001). -Two bits of data can be sent in a single quantum bit (Hirvensalo, 2001) because of the phenomenon of entanglement where two quantum particles interact with one another (Boyle, 2004). -A potential application of quantum computing relates to the highly specific field of protein folding (Johnson, 2004). -Increased networking security by employing quantum communication (O'Brien, 2008).

Technical Issues Associated with Quantum Computers: -Physical constraints and limitations of employing the theory are evident (Häffner et al., 2008) and the hardware architecture is very difficult to construct (West, 2000). -It is very difficult to meet the criteria, set by DiVincenzo, required to make a truly universal quantum computer (Häffner et al., 2008). -Quantum computers aren't ideal for performing general-purpose tasks (Gea-Banacloche, 2003). -Greater energy consumption per logical operation than a conventional computer would require (Gea-Banacloche, 2003). -Physical systems would have to encode the bits of information in an unconventional form, such as photons (O'Brien, 2008). -Outside interference from environmental 'noise' has the tendency to disrupt the quantum particles, used to store information, which would cause errors in the calculations (Unknown author, 2006). These errors are caused when the quantum computer interacts with its environment and goes into a 'incoherent state' (West, 2000). -According to Deutsch, the arrival of a practical quantum computer is at least another five years away (Cho, 2006). Currently only two-qubit computer systems have been manufactured in the lab (Quantiki, 2007). -It is difficult to manipulate one qubit without altering the state of another one due to the close proximity of the qubits (Cho, 2006). -It is probable that quantum computers will be expensive because they will employ high-tech lasers, and precisely crafted microscopic components.

Conclusion
Quantum computers give a new model for universal computation, using physical systems to simulate physical systems. Though there are some challenges to make this tentative idea be realized, we all believe that quantum computers are going to replace conventional computers in the future! We already have big improvement on that field. For example, in 2001, a 7 qubit machine was built and programmed to run Shor’s algorithm to successfully factor 15. Even though today quantum computing is still in its early stages, there are great possibilities for it. Maybe one day you will be choosing a quantum computer instead of the one you have now.

References

David:


Quantiki: Quantum Information wiki and portal. 2007 May 8. What is quantum computation? [Internet]. Available from: http://www.quantiki.org/wiki/index.php/What_is_Quantum_Computation%3F#Why_is_it_difficult_to_build_a_quantum_computer

Chelsea:

http://computer.howstuffworks.com/quantum-computer.htm
http://computer.howstuffworks.com/quantum-computer1.htm
http://www.cs.caltech.edu/~westside/quantum-intro.html


Fei:

http://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol4/spb3/  
http://www.pnas.org/content/98/21/11847.full#xref-ref-2-1
http://www.cs.caltech.edu/~westside/quantum-intro.html#problems
http://en.wikipedia.org/wiki/Quantum_computing
http://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol2/mjc5/#Conclusion
http://thefutureofthings.com/column/5/what-is-a-quantum-computer.html
http://computer.howstuffworks.com/quantum-computer.htm
The University of Calgary (U of C or UCalgary) is a public research university located in Calgary, Alberta, Canada. The University of Calgary started in 1944 as the Calgary branch of the University of Alberta, founded in 1908, prior to being instituted into a separate, autonomous university in 1966. Looking for Wiki U Ca Lgary popular content, reviews and catchy facts? Here we go: we found that wiki.ucalgary.ca has neither Alexa ranking nor estimated traffic numbers. However, we managed to discover that the most significant portion of the traffic comes from Canada (51.2%). This domain has a very good reputation, so you can visit it safely. Domain information. created by University of Calgary students, staff and faculty. This is a wiki, to provide collaborative content management in the context of teaching and learning to the University of Calgary community. Websites with a comparable popularity level. alcovemusic.50megs.com. uofczine.ucalgary.ca. The Information Technologies department provides c sparky.rice.edu.