Andrew Rutherford

Dr. Elizabeth White

CSCI 2270

30 November 2014

Quantum Computing

Earlier this month, the Engineering Center at the University of Colorado Boulder hosted a computer science colloquium on quantum computing. The speaker, Fred Chong, touched on a variety of subjects including the major differences between quantum and digital computing, some major advantages and disadvantages of quantum computing, and why there are unprecedented levels of investment within the emerging industry today.

Fred Chong began his talk with an introduction of himself, and a background of his work and research. He received his Ph.D. from the Massachusetts Institute of Technology in 1996, and is currently the Director of Computer Engineering and Professor of Computer Science at the University of California at Santa Barbara. Chong’s research interests include emerging technologies for computing, multicore and embedded architectures, computer security, and sustainable computing. He is a recipient of the NSF CAREER award, the DARPATech Most Significant Technical Achievement Award, and has been funded by NSF, Google, DARPA, and several other large organizations. Much of Dr. Chong’s research has been for research and development within the quantum computing industry.

The main difference between quantum computing and conventional (digital) computing is the method in which data is stored and encoded. Digital computers encode data into bits, or binary digits, which are always in one of two states (0 or 1). Quantum computers encode information into quantum bits, or qubits. Similar to the bits used by digital computers, the qubit is also a two-state system. The main difference however, is that qubits exist in a state of superposition, that is, a qubit is the polarization of a single photon. It can exist in a state of horizontal polarization, vertical polarization, or anywhere between. Rather than existing in a state of either 0 or 1 like a traditional bit, qubits can exist in a state of “parallelism”, or in an array of different states based on the ratio of polarization of its vertical and horizontal poles. Two qubits can be in a superposition of 4 states, and 3 can be in a superposition of 8 states. A quantum computer with *n* qubits can be in a superposition of up to states simultaneously. This fundamental difference in how data is encoded and stored is the foundation of quantum computation.

To perform an action, a quantum computer sets an applicable amount of qubits into a controlled initial state. Quantum logic gates then manipulate certain qubits in a predetermined order. These gates are the basic unit of a quantum circuit, and are similar to the logic gates used in conventional digital computers. Chong explained how the Hadamard gate, Toffoli gate, Z gate, and Controlled gates, the most common universal quantum operators, function in a quantum computer. Each of these quantum logic gates are represented by a numerical matrix composed of qubits. The superposition of particular qubits is then manipulated, based on what problem is being solved. This process can occur very rapidly, over and over again. Quantum logic gates can perform any action of their digital counterparts, meaning a quantum circuit can perform virtually any action a digital circuit can. This is one of the main advantages quantum computation has over its digital counterpart.

The order and operation of quantum logic gates are determined by a quantum algorithm. Comparable to classical algorithms used by digital computers, quantum algorithms are essentially a predetermined set of instructions used to solve a problem. When used properly and on the same problem, computation times of quantum algorithms are almost always shorter than that of classical algorithms. Coincidentally, two of the most popular quantum algorithms: Grover’s Algorithm (used for searching an unordered database or unordered list) and Shor’s Algorithm (used for finding prime factors of an integer, *n*) are the quantum representatives of digital algorithms utilized in several CSCI 2270 projects this semester. Grover’s and Shor’s algorithms achieve speeds of O() and O(), respectively.

After the quantum algorithm has finished and produced a solution, steps of error-correction must be performed to ensure it is accurate. This is important because quantum computers are extremely sensitive to external disturbances. Quantum decoherence is created when any of these external factors affect the computation in an unwanted way. These factors can include magnetic disturbances outside of the computer itself, or the inductive interference of qubits by other qubits, within the computer. Chong summarizes this by saying “the exponential advantage from quantum computing also comes with exponential overhead.” Quantum decoherence presents a major obstacle in the progression of quantum computing; often times the added time and resources needed for error-correction can offset the gains in speed and efficiency achieved during the initial calculation. As computation times increase, so too does the time required to perform the additional error-correcting algorithms.

Another interesting aspect of quantum computing Chong discusses is that of quantum teleportation. This exciting new technology is a process by which qubits in superposition use forms of existing communication mediums (e.g. fiber optic line) to travel from one location to another. Despite the name containing “teleportation,” the information is not actually teleporting, but instead travelling at the speed of light. Additionally, because a qubit is just a photon, no physical matter is actually being transferred. Therefore, the only thing being transferred is information, not material. Quantum teleportation is still being rigorously researched and developed. Scientists are currently testing ways to attach individual photons to molecules to allow for the transfer of actual material at light’s speed.

As technology marches forward, quantum computers will continually be redesigned around what Chong calls the “Three Axes of Quality”: area, speed, and reliability. The design pyramid visually represents the optimal quantum computational environment as one with a small area, high speed, and high reliability. The first quantum computers performed very fast, but were also very unreliable, and very large. As development into quantum technology continues, large emphasis will be placed in improving the accuracy of quantum data, and lowering the overall size of the machine. In order to improve accuracy, new methods to impede quantum decoherence, and magnetic interference will need to be developed. Reducing the overall size of the machine, however will make data more prone to disturbance, and possibly lower accuracy. This paradox presents a major obstacle for researchers and developers working with quantum computers today.

Despite the technological and economical limitations of quantum computing, unprecedented amounts of investment for research and development are being introduced into the field. Major organizations such as Google, IBM, Microsoft, and the U.S. military are taking part and collaborating in new technologies that utilize quantum computers.

In 2009, Google began working with D-Wave Systems, a company who claims it developed the first quantum computer for commercial use. With the help of researchers from the University of California Santa Barbara, Google hopes to utilize the new technology to redesign the ways it indexes the internet. Quantum computing will enable Google to index websites and databases much faster and more efficiently. This may change how people use technology to access information in a variety of new ways, such as on smartphones, tablets, and possibly even their “Google Glass” initiative.

The NSA (National Security Administration) is also investing large amounts of money into developing a “quantum supercomputer.” Originally disclosed by Edward Snowden of Wikileaks, the agency aims to use the technology to aid in breaking previously unbreakable coding encryptions. A quantum computer would also allow the NSA to more effectively monitor the encrypted communications of anyone they deemed worthwhile. $79.7 million is said to have already been invested by the NSA into the development of a quantum supercomputer, but that does not include any additional undisclosed amounts.

As the development of quantum computing continues, and the industry continues to emerge, this new technology could prove to truly revolutionize the way we create and send information. With the rise of smartphones and tablets, technology is already deeply integrated into many people’s lives. Quantum computing may signal the beginning of a transition of technology based on digital encoding to quantum encoding. If the changes brought on by the analog to digital revolution are any indication, quantum technology has the potential to fundamentally change the way we interact with technology.

Works Cited

Anthony, Sebastian. "The NSA Is Building a Quantum Computer to Crack Almost Every Kind of Encryption | ExtremeTech." *ExtremeTech*. N.p., 03 Jan. 2014. Web. 30 Nov. 2014.

Chong, Fred. "Quantum Computing." University of Colorado Boulder, Boulder. 13 Nov. 2014. Lecture.

Chong, Fred. "Fred Chong." University of California Santa Barbara, n.d. Web. 30 Nov. 2014. <http://www.cs.ucsb.edu/~chong/>.

"D-Wave Systems." *The D-Wave Two™ System*. N.p., n.d. Web. 28 Nov. 2014. <http://www.dwavesys.com/d-wave-two-system>.

Gershenfeld, Neil, and Isaac L. Chuang. "Quantum Computing with Molecules." *Scientific American* (1998): n. pag. Web.

Simonite, Tom. "Google Hires Leading Researcher to Build a Quantum Computer | MIT Technology Review." *MIT Technology Review*. N.p., 03 Sept. 2014. Web. 30 Nov. 2014. <http://www.technologyreview.com/news/530516/google-launches-effort-to-build-its-own-quantum-computer/>.