Daniel Maxson

CSCI 2270

Colloquium Paper

Quantum Computers

Thursday November 13, engineering classroom wing - Room 265

Speaker: Dr. Fred Chong, Director of Computer Engineering and Professor of Computer Science at University California Santa Barbra. PhD from MIT 1996. Received the NSF CAREER award, the DARPATech Most Significant Technical Achievement Award, Leads the Greenscale effort for energy efficient computing, and has 5 best paper awards.

Research: emerging technologies for computing, multicore and embedded computing. Dr. Chong has been funded by: Xilinx, Altera, Mitsubishi, DARPA, IARPA, AFOSR, Google, and the NSF. Led $20 million in awards research.

The event was an explanation of large-scale quantum computer architectures from a systems perspective. I was intrigued, I have been hearing more and more about quantum computers.

Dr. Chong started out his talk with a brief overview of who he was and what he wanted the audience to learn from him. Specifically he wanted to present a basic overview of quantum computing and the problems of scaling up this architecture. He would guide us through the interworking of a quantum system and explain problems and issues that present themselves when you physically implement a quantum computer.

I maintained an understanding for about the first twenty minutes of his talk, he was still discussing current computer system adaptations to quantum architectures. Talking about controlling error rates and issues with memory scalability vs cost, and how exponentials become a major factor in implementation of a physical quantum computer when designed to tackle certain exponential algorithms. He mentioned that if we wanted to learn more about specific algorithms we could find information at <http://math.nist.gov/quantum/zoo/> , but he focused on controlling exponential cost and making sure that the problem could be solved before the cost actually became exponential. This would be achieved by implementing an architecture that could sustain computational integrity long enough to solve the algorithm. He had a nice PowerPoint slide with a proportional pyramid Venn where the three sides represented a part of a quantum computer system. Speed, reliability, cost, and he spent a few minutes talking about how if they increase speed and reduce reliability for specific algorithms they become attainable processes.

He explained that he got into quantum computers because he was tired of writing a certain type of machine code, and I admit I was too interested in what he was talking about to write down the specific type, but he found out that working with quantum computers he spent most of his time writing this exact type of code. I think it was error correction architectures. He may have been under the same assumption that I was about the error rate of quantum computers. I was not aware of the need for so much error correction in a quantum computer. I did not get the feeling that he was disappointed to be writing this type of code again, but more of an excitement that he could apply his extensive knowledge to a new type of architecture. There is a major hurdle to quantum computing in the fact that apparently observing the entangled qubits alters their physical state. My understanding of the specifics of how and why are not at any level above an enthusiastic interest in the subject so most of the talk about measuring qubits was foreign territory for me. I do not know exactly how they function but I know that there are many challenges that have to do with measuring superposition, the ability of a qubit to be in multiple states simultaneously. These states all having to sum to 1, once the measurement has taken place and the data has been error corrected.

“Quantum computation exploits the ability for a single quantum bit, a qubit, which can be implemented by the polarization states of a photon or the spin of a single atom, to exist in a superposition of the binary “0” and “1” states (simply denoted as |β› + β|1›, where  and β are probability amplitude satisfying (||² +| β|² = 1),. With *N* qubits, a quantum computer can be in 2ⁿ unique states at any given time. These states can be inter-correlated such that a single logic gate can act on all possible 2ⁿ states.” (Frederic T. Chong)

The Schrodinger’s cat conundrum. I have a grasp of this phenomenon since I have spent time trying to wrap my head around it. I could not fathom this cat being both alive and dead; it must be in one state or the other. I am still unconvinced that this is physically the case. I can understand the idea of something being uncertain and the implication that because of uncertainty, it can be in both states but I struggle with the idea that measuring or observing something changes it physically. My understanding is also discounted because I am thinking of the cat physically, not in a quantum sense. If we were to observe the cat and this radioactive poison release mechanism we would have a healthy cat until the time frame ends or the mechanism activated and the cat dies and the ‘state’ of the cat changes to ‘dead’. Now I think that in the quantum sense the cat has multiple states that can will or have existed, akin to alive or dead, young or old, fast or slow, and we know that in the past observed cats can have all of these states in different combinations. Therefore, we assume for a given cat that we have yet to observe it can be in any of these states. Once we observe or measure the cat these states are now set physically. Even while writing this I now feel like I have a better grasp of quantum states. Sometimes it takes writing down your thoughts.

Entanglement was another idea that I thought was sure to be addressed, there are concerns that entanglement would be able to break / change the c barrier (speed of light), and Dr. Chong provided an explanation. He seemed to feel that because of the error rate implicit with quantum computing and the necessity to provide error correction data with the original data that the c information barrier had not been broken. You would be by necessity forced to send the error correction data through a reliable physical medium that would not be breaking the c barrier. Because the data recorded by the entangled particles needs to be error corrected, it was not yet ‘real’ information, my association would be being apart from a friend and buying them a souvenir from your vacation and thinking they would enjoy it. You are guessing but do not know. If you call them (the reliable physical medium), you can confirm that your gift is appropriate.

I wondered if you kept these ions under observation, do they still behave identically or is the entanglement lost? If you could keep both under observation and transport them, far enough apart would you not be able to change the c barrier? Is the information transmitted not considered information because of the inability to error correct? Does that mean that the c barrier is only for information and we can break it only with useless chaos that needs error correction? Wouldn’t we be able to send an on/off signal and transmit information with these entangled particles? My grasp of the detailed interworking of quantum computers does not allow me to dismiss obvious idea that have already been discounted. An outside perspective can often see what those inside miss. I might spend more time studying entanglement so that I can at least understand why the obvious are not plausible.

Dr. Chong continued and I picked up a few interesting things in-between all the PhD quantum probability mathematics. One interesting idea was the ability of a quantum computer to break encryption. From his paper, A quantum Logic Array Microarchitecture: Scalable Quantum Data Movement and Computation, 5. QLA performance pg. 9

“In this section we estimate the performance of QLA when executing a general quantum application through the specific example of Shor’s factoring algorithm, which is designed to break the widely used RSA public-key cryptosystem. RSA’s security lies at the assumption that factoring large integers is very hard, and as the RSA system and cryptography in general have attracted much attention, so has the factoring problem. The efforts of many researchers have made factoring easier for numbers of any size, irrespective of the speed of the hardware. However, factoring is still a very difficult problem. The best classical algorithm known today [51] has complexity of exp((1.923+*o*(1))(log*N*)1/3 (log log*N*)2/3) for an N-bit integer. Using this algorithm Reference [52] has demonstrated the factorization of a 512 -bit number in seven calendar months on 300 fast workstations, two SGI Origin 2000 computers, and one Cray C916 Supercomputer - a process which amounts to 8400 MIPS years.” (Frederic T. Chong)

Cont.,

“For a 128 bit number, modular exponentiation requires 63730 Toffoli gates with 21 error correction steps per Toffoli. The error correction steps of the entire algorithm amount to (21 x 63730 + QFT = 1.34 x 106). Since 0.043 seconds are required to perform one error correction at level 2 recursion, it will take approximately 16 hours to complete the factorization of a 128-bit number. However, assuming success of all the gates, the circuit is repeated on average 1.3 times [56], so the total time to factor a 128-bit number would be around 21 hours. Similar calculations lead to the execution times of the factorization of larger integers shown in Table 2; however, the sheer sizes of the ion-trap chips required make the physical realization of such a systems a considerable engineering challenge, which may be impractical for N 128 , with current single chip technology.” (Frederic T. Chong)

His table 2, mentioned above, shows us the estimated key time factorization for a few keys.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | N = 128 | N = 512 | N = 1024 | N = 2048 |
| Logical Qubits | 37,971 | 150,771 | 301,251 | 602,259 |
| Toffoli Gates | 63,729 | 397,910 | 964,919 | 2,301,767 |
| Total Gates | 115,033 | 1,016,295 | 3,270,582 | 11,148,214 |
| Area (m2) | 0.11 | 0.45 | 0.90 | 1.80 |
| **Time (days)** | 0.9 | 5.5 | 13.4 | 32.1 |

(Frederic T. Chong)

A month to break what we consider overkill for encryption? This will either motivate a new type of quantum encryption or the perceived unimportance of encryption and the use of more secure communication channels. Although cooling almost 2 meters of essentially CPU chip might prove to be an issue if this type requires Helium-3 and near absolute 0˚ Kelvin temperatures.

The talk concluded and I felt overwhelmed by the understanding of this subject by one person. I have a casual interest in anything scientific and learning from someone who seems like he has mastered it was a humbling experience. I am glad that I took the time to attend this colloquium. I took away a refreshed interest in many subjects that I had not associated with each other before, specifically the use of regular physical computer science and its’ applicability in the quantum-computing world. I have a work history with the Department of Homeland Security and know a few colleagues who are starting to work with quantum computers and specifically encryption. When I graduate and continue with my career, I hope to apply some of the concepts from this colloquium to working with or helping these colleagues. I am grateful that I can attend CU Boulder and have access to these types of talks and information.

# References

*~chong*. n.d. <http://www.cs.ucsb.edu/~chong/>.

*~chong/pubs.html*. n.d. <http://www.cs.ucsb.edu/~chong/pubs.html>.

Frederic T. Chong, Tzvetan S. Metodi, Darshan D. Thaker, Andrew W. Cross, Isaac L. Chuang. "A quantum Logic Array Microarchitecture: Scalable Quantum Data Movement and Computation." n.d. *http://www.cs.ucsb.edu.* html. <http://www.cs.ucsb.edu/~chong/papers/micro05.pdf>.

P.S. I didn’t get a copy of the PowerPoint presentation so I couldn’t recall exactly where this was used but there was a very interesting crossover to inorganic chemistry and using NMR (nuclear magnetic resonance) to ‘observe’ a pentafluorobutadienylcyclopentadienylcarbonyliron complex molecule. I think this complex was used for entanglement.