Brandon Fieger
CSE300

Stacey Suver

3 November 2016

A New Era in Computing: Quantum Computing

Over the past few decades technology has exponentially increased in computing power while retaining smaller and smaller physical systems. Co-founder of Intel, Gordon Moore, proposed a theory that the number of transistors per square inch on an integrated circuit doubles every year. Up until the 21st century this theory held true, however, traditional silicon based computing devices has reached an upper physical limit. We are reaching hardware limits that can only provide so much power and memory in an area without running into energy consumption and heat dissipation issues. If Moore’s law continues to be true, a new technology must be developed that overcomes our physical limits. One promising and highly researched technology is quantum computers. Using properties of quantum mechanics we are able to encode and process information in subsystems and perform simultaneous computations within these subsystems. If a perfect implementation of a quantum computer was achieved, it would be magnitudes of millions times faster and more powerful than our current fastest supercomputer in Sunway TaihuLight.

Quantum computing is an exciting new era of technology that touches on both theoretical computations and quantum physics. The idea of quantum computing has been around for decades, but a concrete model to simulate computations was hard to come by. “Strengths and weaknesses of quantum computing” by Bennett C, Bernstein E, Brassard G and Vazirani U was one of the founding studies written in the 1990’s. One of the early developers in quantum computers, Deutsh, had come up with an efficient universal QTM that could run off of quantum circuits. “The computational power of QTMs has been explored by several researchers. Early work by Deutsch and Jozsa showed how to exploit some inherently quantum mechanical features of QTMs. Their results, in conjunction with subsequent results by Berthiaume and Brassard established the existence of oracles under which there are computational problems that QTMs can solve in time with certainty; whereas if we require a classical probabilistic” (Bennett 1512). At the core of quantum computers lies a qubit, a two-state quantum-mechanical system to encode information. Qubits are similar to regular transistors in that they encode if an electron exists or not, 1 or 0, however, due to the properties of quantum physics they can be entangled with each other. A qubit also has a special, not fully understood property called the superposition. The spin of the qubit can either align with a field, known as a spin-up field, or opposite of a field, known as a spin-down state. The authors state that qubits are extraordinary special because they can occupy both positions simultaneously, and can transfer data between other qubits instantly through quantum entanglement. The article explains how quantum entanglement is one of the many “spooky” phenomenons that occur when reaching sub-atomic sizes. They suggest that because qubits can be in multiple superpositions at the same time, can be entangled with other qubits, and can store binary information, a model to simulate computations can be formed. They further explain how a turning machine implementation using qubits can be devised, and the strengths and weaknesses of the model. Since the article was written in the 90’s much of the information is dated and has been developed upon. The theoretically limitations of quantum computer however has not changed and has been kept the same over the decade.

Microsoft Researcher and specialist in quantum architecture, Krysta Svore, recently wrote “The Quantum Future of Computation”. Svore explains how quantum computers are superior to classical computers because of quantum algorithms. These quantum algorithms can solve a range of problems better than the best known classical algorithms. She later explains that because of the superposition of qubits, various algorithms can be implemented to exceed running time and performance verses classical computers. Varying algorithms such as the Grover search, period finding and quantum walks will perform magnitudes faster on a quantum computer rather than a traditional one. The article also explains how simple tasks such as linear searches and sampling from a distribution can be performed in significantly less time. Although the article speaks in uncertainty and about the future, it does go over today’s technology and current work. “Experimental development of qubits has progressed to the point where scalable qubit technology already exists—within the next few years, we can expect to see the development of small quantum computers with more than 100 physical qubits” (Svore 28). With the recent release of the D-Wave system her claims about the future and present progress of quantum computers has been accurate.

Quantum computers are a gateway to solve various difficult computer science and everyday problems, one being data mining. “Quantum Machine Learning: What Quantum Computing Means to Data Mining” written by Péter Wittek is a core study in data mining. Wittek explains that one of the limitations of classical computers is that it can only analyze data in a linear fashion. With an era of big-data he explains how this causes various issues. In order to learn from big data sets an ordered squared algorithm must be performed, which often takes days, if not weeks to compute. With quantum computers simultaneous calculations can be performed and pipelined together to optimize big-data algorithms. He later explains how high-dimensional feature spaces that correspond to quantum states can be built to satisfy various algorithms. These feature spaces are an abstraction on top of quantum spaces to better aid when writing these algorithms. Although Wittek explains the limitations of analyzing big data on traditional computers, he does not explain use-cases or real life examples that demonstrate the limitations. He also does not explain how the transition from traditional computers to quantum computers will take place and if current algorithms can be ran on quantum computers.

With the exponential growth of technology security in our systems and architectures are constantly under attack. Padamvathi V, Vardhan B and Krishna A, authors of “Quantum Cryptography and Quantum Key Distribution Protocols: A Survey”, explain a new technology to help in cyber security, quantum cryptography. They explain how cryptography allows us to encode visible text into an incomprehensible form which can only be decrypted by certain parties. Dating back to the early seventies, strong cryptographic functions have been developed which can only be broken by a brute force approach. As stated by the article, what was once a secure system, cryptography is becoming less and less secure as computers are becoming more powerful at computing permutations of cryptographic hashes. The authors later suggest a solution which can provide a true, non-mathematical and probabilistic approach to cryptography, quantum cryptography. Using quantum computers, photons or quantum particles can be quantized and the properties about them can be used to encode information. The transmission of this encoded information is secure and is theoretically impossible to crack because of the inalienable quantum mechanics laws. The article explains how a communication protocol can be established and how information can be exchanged over quantum networks and tunnels. One issue the article does not address is how normal cryptography falls under quantum cryptography; could normal cryptography be encoded using quantum cryptography or is it mutually exclusive.

The gap between the theoretical implementation and physical implementation of quantum computers is large. Transitioning memory into a quantum form theoretically is possible, but is hard to achieve. The article “«Quantum» processor for digital systems analysis “ written by Hahanov V, Shcherbin D, Gharibi W and Iemelianov I, proposes an idea that can be used for simulation and verification of digital systems using quantum memory. The idea revolves around transactions between addressable memory components which can be used for a wide variety of applications. Specifically, a vector form of combinational and sequential structures will be implemented into the memory hardware. They explain how using a technique such as this will allow us to utilize quantum hardware and the parallel computations provided from qubits. The article also mentions the benefits of quantum memory, such as an increase in yield, along with enhanced reliability and human-free repairing in remote and online modes. Unlike other articles, this one proposes a solution to implement backwards compatibility for traditional computers.

It is without a doubt that technology will continue to grow and quantum computers will emerge as a dominating factor in the near future. However, will quantum computers replace traditional computers for our everyday consumer needs? The conditions in which quantum computers must operate makes is significantly hard to compact in size and the short-lived computation planes makes it near impossible to store lasting information. Although it has been theorized that it is possible to replicate a traditional computer in a single quantum plane, it has not been physically implemented which is a key stepping stone for the future of quantum computers.

Works Cited

Bennett, C. H., et al. "Strengths and Weaknesses of Quantum Computing." *SIAM Journal on Computing* 26.5 (1997): 1510-23. *SCOPUS.*Web. 25 Oct. 2016.

Hahanov, V., et al. "«Quantum» Processor for Digital Systems Analysis".*Proceedings of 2015 IEEE East-West Design and Test Symposium, EWDTS 2015. SCOPUS.*Web. 25 Oct. 2016.

Padamvathi, V., B. V. Vardhan, and A. V. N. Krishna. "Quantum Cryptography and Quantum Key Distribution Protocols: A Survey".*Proceedings - 6th International Advanced Computing Conference, IACC 2016. SCOPUS.*Web. 25 Oct. 2016.

Svore, K. M., and M. Troyer. "The Quantum Future of Computation." *Computer* 49.9 (2016): 21-30. *SCOPUS.*Web. 25 Oct. 2016.

Wittek, P. "Quantum Machine Learning: What Quantum Computing Means to Data Mining." *Quantum Machine Learning: What Quantum Computing Means to Data Mining.*, 2014. 1-163. *SCOPUS.*Web. 25 Oct. 2016.