Quantum Computing

CSCI 3100 Term Paper

By: James Avery King

Quantum computing holds possibly the most potential for the growth of our species than any other field of science. This mostly untapped potential will pave the way for life on this planet to truly understand the limits of our universe, or in physical reality, the limits of the human mind's conception of the universe. Quantum mechanics represents the next step in technology and understanding the world around us. From the double slit experiment to the Higgs Boson particle, quantum mechanics has mostly only given scientists and philosophers more questions to answer in the place of solving what defines us physically. With the help of quantum computation we will finally be able to define on a more universally understandable scale what existence really is by eliminating variability with concentrated precision. Imagine, instead of simply stating that a cell with a cell wall has a semi-permeable phospholipid bilayer scientists will finally be able to understand the transfer of matter and energy through these cell walls using algorithms that will finally take into account the extreme amount of variability in everyday phenomena across the spectrum of size. Knowledge in computer systems will surpass the Boolean states of true and false and become something more, something new, and something truly remarkable.

I would like to begin with a very brief history of quantum computation. This history started officially only around 40 years ago at the beginning of the 1970's. Notable practical advancements begin in 1994 with Peter Shor at Bell Labs. Shor discovered an algorithm still has the potential to decrypt most of the cryptographic algorithms in use today with the aid of quantum mechanics. That same year the United States Government organized its first workshop on quantum mechanics, and the next year the Department of Defense organized its first workshop using quantum mechanics in crypto analysis. That same year, 1995, was the year the very first quantum gate was made, the C-NOT gate, by Christopher Monroe. In 1996 Bell Labs made strides again by creating the first quantum algorithm to query a database. The first 3 qubit quantum computer was made in 1998 and was tested successfully that same year. Then, in 2000 the first 7 qubit machine was made at Los Alamos Research facility in America. And finally, to show how much research and development has progressed for quantum computers, D-Wave, the first public company to make quantum computers, has claimed to have broken the 1000 qubit barrier in this year, 2015.[3]

The first research article that I found on the internet serves the purpose of giving an overview of both the history and design of what a quantum computer should be. Published in 2002 by Archil Aviliani, the research is very optimistic about the potential of this mysterious new field. Aviliani cites Gershenfeld's predictions that the minimization of transistor size will continue to shrink at an exponential rate continuing until scientists synthesize a wire medium that is only one atom in diameter. According to Aviliani, this will occur sometime around the year 2020, and will redefine how we are able to transfer information due to the restructuring of the laws concerning data transferred through one atom. Scientists will have to terminate their prior usage of classical physics and adopt the new standard of quantum computation necessary to research and develop data transmission technologies on this new one-atom system. This one-atom system also necessitates redesigning of one of the most fundamental parts of modern computers: the computer chip. Without adequate support from the hardware of an information transmission terminal, there will be no way to make sense of this infinitesimally small medium for transferring the data.

Next, the Boolean standard of mathematics will have to be completely disregarded if scientists are to be able to calculate quantum states of matter. This standard will be replaced by the quantum quaternary standard in which the values can exist in either true, false, or in superposition in which both true and false exist simultaneously. The implications of this statement are enormous. As Aviliani stated in his research, “a computer working on a qubit rather than a standard bit can make calculations using both values simultaneously. A qubyte, is made up of eight qubits and can have all values from zero to 255 simultaneously”. This means that quantum computers will not only be able to account for the four dimensions we perceive, three dimensions of space and the linear dimension of time, but also for the possibly infinite amount of dimensions that we are unable to perceive with our five senses. The quantum quaternary standard of storing and calculating information will effectively enable the first civilization on earth to utilize its power to take into account all variables of say, an adversary in wartime, and effectively compute every possible outcome of a situation far into the future. It could take wartime game theory to a whole new level, giving an obvious advantage to whoever wields this formidable weapon of futuristic warfare.

In 2002, according to Aviliani, it took a standard supercomputer around a month to query a single phone number from the database of the entirety of the world’s phones. This would be reduced to 27 minutes or less with a quantum computer. This example just goes to show the true power of this new kind of machine. It is truly awe-inspiring to think that this sort of technology, with enough research and development, is within the grasp of the scientists of our species. Another example that Aviliani uses in his research is that a “quantum computer with 500 qubits gives 2^{500} superposition states. Each state would be classically equivalent to a single list of 500 1’s and 0’s. Such a computer could operate on 2^{500} states simultaneously…This kind of computer is equivalent to a classical computer with approximately 10^{150} processors”. Now, these are by standards of a paper written in 2002, but the raw potential is still evident in the numbers. This quantum computer with 500 qubits would, according to Aviliani, eventually condense itself into a single answer, or list of 500 1’s and 0’s, which would be calculated using the algorithms and equations of quantum mechanics. The methodology behind this computation would exemplify the fundamental difference between classical and quantum computers. Quantum computers would be able to work on every series of qubits simultaneously, whereas a classical computer could only work on one of the set of 500 1’s and 0’s at a given time, again by 2002 standards[1].

One of the most interesting points in Aviliani’s research is his application of Moore’s Law to the development of quantum computers. According to classical Moore’s Law, the number of transistors on a microprocessor doubles every 18 months. Applying this to quantum computers would, seemingly, yield the same result as for classical computers. But by adding just one more qubit, a quantum computer can effectively and at the very least double its speed. We would have to describe the rate of microprocessor capability by an equation whose slope increases by much more than an exponential rate if we wanted to apply Moore' s Law to quantum computation.

As you can probably imagine, the hardware behind a computer of this magnitude is immense to say the least. At the time of Aviliani's research, there were three main schools of thought for creating a quantum computer. The first, which was used to generate the first 2 qubit computer at a cost of one million dollars, uses nuclear magnetic resonance technology. At the time Aviliani's research was published this seemed to be the most promising of the three with successful experiments being completed at both the Massachusetts Institute of Technology and Los Alamos National Laboratory. The second was "based on ion trap", and is currently being used at colleges like the Georgia Institute of Technology to construct successful prototypes and machines. The third method is called quantum electrodynamics which uses the capture of a single photon and a synthetic atom to create the circuitry of a quantum computer using coherent coupling.

Aviliani proposes two specific areas in which quantum computation will advance our species, and one general statement about future implications of this new standard of information processing. The first, and most obvious, is in the field of cryptography. In 2002 banks were on the RSA encryption standard, which uses factoring as its main method of encrypting data and generating "randomness". This standard could be broken in centuries on a classical computer, but only in a few years using a quantum computer. Since quantum computers can simultaneously calculate equations on every qubit, it has more processing power and therefore more of an ability to break any encryption standard or pseudo-random number generator. The second field that quantum computers will be able to improve is artificial intelligence. Quantum computation will be able to increase machine learning by giving the machines the beginnings of what every sentient species has; a brain. The brain is nothing more than, to our knowledge, an organic quantum computer that grows and learns based off of evolutionary advantages and mistakes that the organism bound to it makes over the generations of that organism's species. More specifically, the human brain contains particles that are entangled in different areas of the brain at the same time to give us the conscious feeling of, for example, love. Our sensation of this attraction and understanding of an organism outside of ourselves has evolved over the millennia into an evolutionary advantage that allows us to survive on an emotional level due to the quantum entanglement of different atoms in our brains. Just as a human can learn to suckle its mother based off of trial and error, so can a machine learn to suckle at the breast of the knowledge of the human race using the same methodology, only at a faster rate with a more concentrated quantum computational device that does not delve into emotions or survival instincts.

The most interesting quotation from Aviliani's research comes from Charles Bennet of IBM. It states, "On the theory side, quantum mechanics delves deep into areas that are nearly unthinkable. For instance, it's possible that a quantum computer holds an infinite number of right answers for an infinite number of parallel universes. It just happens to give you the right answer for the universe you happen to be in at the time". The implications of this statement are a lot for anyone to stomach. This means that, in terms of what Bennett believes, we could every perceivable question in the multiverse, as well as every answer to these questions, at the exact same time once we create a quantum machine with enough processing and memory capacity.

One of the last prospects that Aviliani touches upon in his research is the implication of what kind of speed a quantum computer could process at. Aviliani asserts that we may be able to break the barrier of transferring information at the speed of light, as is the barrier in classical computers, with quantum entanglement. Even Einstein himself could not fully explain this phenomenon, stating that "hidden parameters" could be at work that we are not capable of perceiving. It is going to take another Tesla to be able to figure out how to manipulate quantum entanglement to the point where coherent data can be transferred over long distances, but according to quantum mechanics, anything is possible.

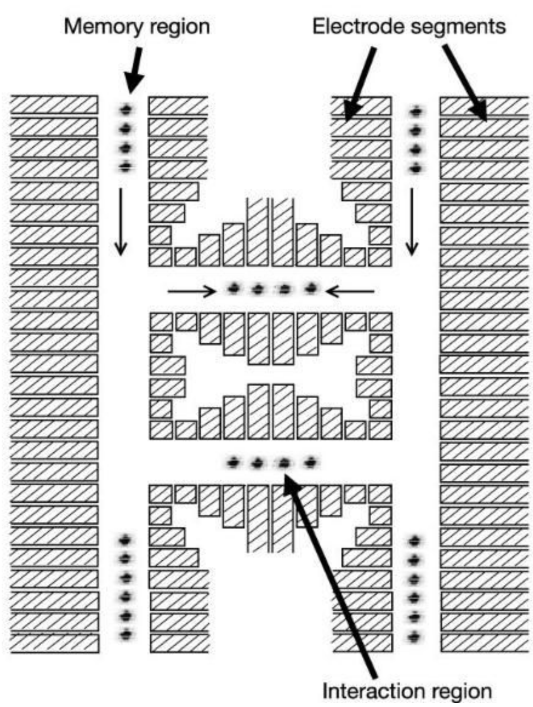
The second research article that I chose concerns the architecture of a modern day quantum computer[2]. According to Kielpinski, Monroe, and Wineland, "a quantum computer is a device that prepares and manipulates quantum states in a controlled way, offering significant advantages over classical computers in tasks such as factoring large number and searching large databases". This reaffirms Aviliani's assertion in 2002 that quantum computing would completely revolutionize our classical cryptographic systems. More specifically, the second article focuses on creating a large-scale ion-trap computer. Normally, the qubits in a quantum computer are linked by coupling in a Coulomb interaction. According to Kielpinski, Monroe, and Wineland, there are numerous technical and physical difficulties getting in the way of creating a large-scale machine with more than 2 or 3 qubits due to entanglement, as well as environmental factors such as keeping the qubits below the threshold temperature for optimal performance without any interaction with outside variables. This can be circumvented using a decoherence-free subspace, which will "significantly reduce decoherence during ion transport", and "removes the requirement of clock synchronization between the interaction regions".

Kielpinski, Monroe, and Wineland state in their research that "the power of quantum computing derives from its scaling properties: as the size of these problems grows (database query and cryptanalysis), the resources required to solve them grow in a manageable way. Hence a useful quantum computing technology must allow a large number of quantum systems, composed of thousands or millions of qubits". Thinking in classical terms this does not seem like so much of a radical idea since our modern day portable laptops have millions of individual bits inside of them. In realistic terms, this is one of the most game-changing concepts in quantum computing. Up until this time researchers had only been building computers with 2-7 qubits. As stated in my condensed timeline of this subject, the first 7-qubit computer was not built until the year 2000. This research paper published by Kielpinski, Monroe, and Wineland was, like Aviliani's research, published in 2002. The difference between the two articles is Aviliani gives an overview of quantum computing while Kielpinski, Monroe, and Wineland revolutionized scientists' entire idea of what quantum computing meant by presenting a solution to an architectural problem.

The entire premises of Kielpinski, Monroe, and Wineland's findings centered around "confining a string of ions in a single trap". By using the spin orientation of the particle's electrons, the researchers proposed that one could store data in the form of qubits. Also, by generating a mutual Coulomb interaction, the researchers would be able to successfully transfer quantum information between the ions. Before this research was published, it was thought that "this scheme was limited to computations on tens of ions". Kielpinski, Monroe, and Wineland state that this is not true, asserting that the physical limitations of the first quantum computers could be overcome with "a number of small ion-trap quantum registers". The most advantageous part of the entire research piece for scientists was that, at the time, Kielpinski, Monroe, and Wineland used known and tested methods to make their claims, unlike the photon coupling or spin-dependent Coulomb interactions that only existed in theory.

According to Kielpinski, Monroe, and Wineland, in order to create a large-scale quantum machine, one must acquire a "quantum charge-coupled device architecture consisting of a large number Figure 1
of interconnected ion traps". In order to transfer information between the ion traps, the researchers state that different voltages can be used to achieve this task. With speeds never seen before in classical computers, quantum computers will be able to use these voltage differences in transferring data at a small fraction of the computer clock cycle compared to our modern computers.

The figure that I have included on this page, figure one, is an illustration of what this quantum charge-coupled device would look like. As you can see, there are different regions that are associated with different voltages and different tasks necessary to manipulate and store data in the ions. There is a memory region in which the ions would not be manipulated so that they may store the data necessary for computations in the computer. There is also an interaction region in which the data in the ions would be manipulated using different logical gates that are specific to quantum mechanics. In this region, "relevant ions" are moved "into an interaction region by applying appropriate voltages to the electrode segments…the ions are held close



together, enabling the Coulomb coupling necessary for entangling gates. Lasers are focused through the interaction region to drive gates”. Furthermore, the ions are put into place in the different regions by the electrode segments. These manipulate the ions by causing their orientation and physical position to change based off of the amount of voltage being passed through them at a given time. According to Kielpinski, Monroe, and Wineland, the geometry among these different regions and electrodes allows for “stable transport of the ions around “T” and “X” junctions, so one can build complex, multiply connected trap structures”.

The progress of the electrode structures for the quantum-charged coupling device is astounding. It really makes one see how far our species has come from inventing the wheel or gunpowder. The research article states that multiple ion traps have been successfully built and test using laser-machining slits with aluminum wafers and “evaporating gold electrodes onto the aluminum”. Kielpinski, Monroe, and Wineland state that the gold and aluminum traps have the same sort of geometrical structure as the quantum-charged coupling device in figure one above. They also have specific spaces between different kinds of electrodes, static and radio frequency that are “fractions of a millimeter”. This allows confinement frequencies of up to 20 megahertz.

Kielpinski, Monroe, and Wineland touch on the research of the National Institute of Standards and Technology to show the different devices that have led up to a quantum-charged coupling device capable of withstanding operations on multiple qubits. The first device of this kind was made using a pair of interconnected ion traps, which were made with the same configuration as those in the figure above. NIST demonstrated “efficient coherent transport” between the qubits with an experimental error of less than 0.6%. This experiment yielded some amazing results. The “transport times were as short as 50 nanoseconds” and “transport did not cause any heating of the ion motion or shortening of ion lifetime in the trap”. If the same experiment was conducted on a quantum-charged coupling device with, say, 100 qubits, the results may have been quite different due to the entanglement of the particles as well as the heat generated by so many qubits being manipulated and interacting with each other at the same time. But, since there were only two qubits in this initial experiment, the results were very promising in terms of the potential of using multiple qubits in a quantum machine.

The largest problem that scientists face, according to Kielpinski, Monroe, and Wineland, is that of decoherence during ion transport. Decoherence is the process in which there is a loss of the phase angles between the components of a system in a quantum superposition. In terms of quantum computing this amounts to loss of data during the transfer of the ions in the computer from one location to another. Without the proper orientation, the ion cannot effectively transmit data. This decoherence could be caused by any number of things but the most common cause would be magnetic fields outside of the system interacting with the ions that are used for transmitting information.

Kielpinski, Monroe, and Wineland state that the problem of decoherence can be overcome by creating a decoherence-free subspace of two ions for every qubit in the quantum computer. This subspace would act as a buffer between the qubits and the different electrical fields existing outside of the system. Another solution to the problem of decoherence is to cool down the quantum computer to a temperature that helps keep the ions in place despite interactions with outside electrical fields, as well as keeping the entire quantum computer in a room that is sealed to the point where no outside interference could penetrate its walls. With this solution, early quantum computers could potentially put us back at square one in terms of how much area the computer takes up, with each qubit being contained inside of one room, multiple rooms in a building, and a connecting pathway between the rooms. Early quantum computers wouldn't be quite as dangerous as the vacuum tubes that early classical computers were made of, but they would definitely rival and possibly surpass the early classical computer's size. Including the DFS would, according to the authors of the research article, "remove the requirement of clock synchronization between logic gates, a major but little-recognized obstacle to large-scale parallel quantum computation". This is a truly amazing feature of a large-scale quantum computing device. If you can imagine a computer that would not have to synchronize its logical gates with an internal clock and effectively use every single gate simultaneously on every single qubit, you have an accurate conception of what the future of computing will be.

There are no disadvantages to any of the advancements in quantum computing except for possibly the groups of people who are ethically against creating artificial intelligence, and those who fear that their data may be compromised by the cryptanalysis methods implemented by a quantum computer. As the Catholic Church treated Copernicus when he proved mathematically that the Earth revolved around the sun, so will the portion of our species infected with stupidity actively pursue the crucifixion of new technology. These people are thankfully in the minority and can do nothing to halt the snowball effect of scientific progress, even in the field of quantum computation.

There are numerous advantages in creating a quantum computer with enough qubits to sustain complex computations. The possibilities are literally endless. As I stated in the introduction, biology and chemistry will be revolutionized after computations that take into account every known variable simultaneously to calculate the most precise results to problems we have been grappling with as a species. There is a new field of biology that incorporates quantum mechanical concepts called quantum biology that will flourish with the help of the proper mechanisms for calculating such rigorous problems as the permeability of the cell wall. Chemists will finally be able to take into account all of the particles of an atom, protons, neutrons, electrons, and their components, and create a working model of complex interactions at this level of understanding. There is one field in particular that will benefit the most from the conception of a quantum computer's capability of calculation. Neuroscience is a very old subject, but our understanding of its complexity is still on the rudimentary level, just like our understanding of quantum computations. With the help of a quantum computer neuroscientists would finally be able to account for quantum entanglement in the human brain that allows for our conscious existence. Neuroscientists would finally be able to pinpoint the exact locations of the atoms whose entanglement gives us the simultaneous experience of emotion in the amygdala, memory in the hippocampus, reasoning in the frontal lobe, and so on.

One of the most intriguing parts of quantum computation is its future. We exist in a time where we have mathematically proven through quantum mechanics that anything is possible. The growth rates of qubits processing power, and memory in quantum computer are growing at a rate that goes above and beyond our conventional ideas of development in classical computers. There are numerous ideas for the design patterns for a quantum processor, as was discussed in the research by Aviliani. There is really no way to tell at this point which will be the most successful or if we will invent an entirely new way to store, transmit, and manipulate information using quantum mechanics. We have created a snowball effect of discovery in this new field that is growing by the day, constantly being updated with new information, research, and ideas.

I chose this topic because eventually I would like to get into research with quantum computation at the Georgia Institute of Technology. It is a very hot field right now and its purpose, which is not yet completely known, is a concept that I have thought about every single day since I discovered the topic for myself. I have been fortunate enough to be born at the dawn of modern civilization, and I plan to do everything within my power to ensure a promising future for posterity.

Works Cited

[1] Aviliani, Archil. "The Quantum Computer." *Introduction to Quantum Computers* (1998): 20-30. *Arxiv.org*. 1998. Web. 2 Dec. 2015.

[2] Kielpinski, D., C. Monroe, and D. J. Wineland. "Architecture for a Large-scale Ion-trap Quantum Computer." *Nature* 417.6890 (2002): 709-11. Web.

[3] Rieffel, Eleanor, and Wolfgang Polak. *Quantum Computing: A Gentle Introduction*. Cambridge, MA: MIT, 2011. Print.