Quantum Computing

GitHub Repository: https://github.com/annie2404/CS4182-project

Lakeisha Lazo 19277997

Quantum computing is a topic that is not being discussed enough amongst the general public even though it can revolutionize the entire prospect of the world. It can solve the current energy crisis, then further solving climate change. It can also transform the development of drugs and materials. It can affect several aspects of our daily lives, but what is quantum computing?

First, let's look back. The idea of quantum mechanics, the basis of quantum computing, has been around since 400BC. It was introduced by an Ancient Greek philosopher, Democritus. He believed that the entire universe is made up of atoms in a void that are always moving around because of some predetermined and understandable laws. Furthermore, he thought these atoms can hit and bounce off each other or even stick together to make bigger things which can be known as molecules now (Aaronson, 2013). It is obvious to see that this Ancient Greek philosopher had a pretty modern view of science and he is often accredited for his formulation of the theory of atoms in the universe. Fast forward a couple of thousand years, the concept of quantum computers was brought forward around the late 1970s and early 1980s. The name Richard Feynman is often brought up. He observed that particular quantum mechanical operations cannot be operated on classical computers (Polak & Rieffel, 2000). This just means that the computers that we are familiar with aren't capable of computing in the quantum realm, this is still true even with the technology we have today. However, many scientists have anticipated this idea. Paul Benioff was one of these scientists. He released a paper in 1979 that exhibited the theory of quantum computing and suggested that a quantum computer could be created. There is also Yuri Manin who displayed the core idea of quantum computing in his book *Computable and Non-Computable* published in 1980 which was written in Russian and wasn't translated until later (Gruska, 1999). It's quite interesting to think that the concept of quantum computing is relatively ancient, yet it still manages to be a modern notion.

To completely comprehend what quantum computing is, the basics are to be understood. First, it is to know what classical computing does. The computers everyone is very familiar with are models of classical computing, but there are supercomputers that are of a higher-level performance that still follow classical computing. The rudimentary building block of a computer, the bit, can store information and be represented logically by a zero, meaning off, or a one, meaning on (Bone & Castro, 1997). Then understand that quantum computing is a simulation of quantum mechanics. This deals with the behavior of atoms and fundamental particles like electrons and photons. The sight can further be extended to the likes of molecules which are a group of atoms bonded together.

Thinking about the molecule for caffeine allows further inspection in this aspect. With the existence of supercomputers, it is understandable to think that this molecule can be taken and represented exactly in a computer. However, it is near impossible to do so on a classical computer. This is because the amount of bits that store the information of a caffeine molecule possibly sums to roughly ten per cent of the number of atoms in the entire world (Sutor, 2020). With a quantum computer, you can represent this molecule with quantum bits or qubits for short. These can exist in the classical position of either 0 or 1, however, it can be in a state where it is both 0 and 1. This is called superposition. This state can be taken advantage of. Operating on a singular qubit, essentially performs the operation on both values simultaneously. Increasing the number of qubits can exponentially increase this 'quantum parallelism' obtained from the system (Bone & Castro, 1997). Trying to determine whether the qubit is 0 or 1, will collapse the superposition, forcing the qubit to be either zero or one but the outcome is

seemingly random. This is called decoherence. Scientists don't completely understand what happens but there are a lot of theories trying to explain this. In the eyes of scientists like Bone and Castro (1997), the universe is split into two parallel universes where the qubit exists as 0 in one universe and 1 in another. Unfortunately, the very reliance of the bizarre subatomic rules of quantum mechanics makes quantum computing difficult to control and fragile. Furthermore, electromagnetic waves and the temperature needs to be accounted for because it can possibly interfere with the quantum computer. Therefore, the environment must be acutely controlled (Sutor, 2020).

> *The science is immature and a multi-purpose quantum computer doesn't yet exist. But that isn't stopping investors pouring cash into quantum start-ups. (Gibney, 2019)*

This perfectly describes the current state of quantum computing. We are in a 'quantum gold rush' even though this industry is in its very early stages. By the beginning of this year, at least fifty-two companies globally have been funded for their quantum technology. In 2017 and 2018, these companies received at least $450 million in private funding and venture capital took up most of this money (Gibney, 2019). Venture capital, in layman's terms, is essentially investments in private but young companies (Kortum & Lerner, 1998). This money alone excludes large companies like Google, IBM and Alibaba, that are taking apart in this international quantum race. As Machnes said on TEDx Talks (2020), we are in the 1950s of quantum computing but it is a big deal that so much money is being invested into this. The 1950s refers to a time when classical computers were only coming about and so the machines built were big, clunky and had a lot of wires all over the place. This is akin to the current state of machinery needed for quantum computers. To note, the quantum chips holding these qubits need to be colder than interstellar space. The temperature is brought down to a degree just about absolute zero, this is about -273 degrees in Celsius (Narasimhachar, 2015). Even with these limitations, companies like Google and IBM have constructed quantum computers. Surprisingly, anyone can code on a quantum computer right now. IBM has made a 5 qubit, quantum computer available for free online. Under the name "IBM Quantum Experience," there is a web interface that presents videos and tutorials for anyone at home who was interested.

On important news for quantum computing, on October 23rd, 2019, Google announced that they have achieved 'quantum supremacy' on the scientific journal *Nature*. This is the moment when a quantum computer has outstripped the capability of the world's largest supercomputer for certain tasks. Google's scientists claimed that their 53-qubit quantum processor, dubbed Sycamore, took 200 seconds to perform a completely arbitrary mathematical operation that would take supercomputers 10,000 years (Arute, et al., 2019). However, IBM took issue with the findings. They announced that this task can be performed in 2.5 days and not the 10,000 years, with greater reliability (Pednault, et al., 2019). Even so, this is an incredible milestone for the field of quantum computing and with this, it will continue to build hype for a near science-fiction future.

Clodagh Walsh 19230737

Qubits can store a value of either 0, 1 or any value in between. They reside in a three-dimensional space referred to as the Bloch Sphere. Since the qubit can occupy any state between the basis states of 0 and 1 the state of the qubit at any instance must be accompanied by a probability. The computational basis states of the qubits are denoted by the vectors |0> and |1> ,with the former being the ground state of the qubit. This notation is referred to as Ket or Dirac notation which was developed by the physicist Paul Dirac in 1939. Since the qubit can occupy a state anywhere between 0 and 1 inclusive its state is thought of as a vector in a three-dimensional sphere.

This ability of qubits to occupy a state between the basis states is known as superposition. Exploiting this capability of qubits, a quantum computer can outperform a classical computer. Despite its benefits there is one serious flaw. Upon inspection, the qubit collapses out of superposition and hence the advantages of quantum computing are lost. By Heisenberg's Uncertainty Principle the observation of a qubit alters its state. Programmers generally examine the state of their variables throughout the program, however this is not possible in quantum programming. (Mannucci, 2008)

The property of entanglement alleviates this seemingly catastrophic situation. When a set of qubits are entangled, a change in any one qubit will prompt an immediate reaction in the other regardless of the distance between them. By measuring one of the qubits the properties of the other qubit can be determined without having to inspect it. This proves very useful in maintaining the superposition of the qubit.

Programming a quantum computer involves the manipulation of qubits. This is achieved through the use of quantum gates. Quantum gates take the input in a superposition apply the given operation and output a qubit with an updated superposition and therefore updated probability. These quantum gates are availed of to construct quantum circuits which in turn perform computations.

The Swap gate takes two qubits as input and alters their states. The quantum NOT gate has the same function as the classical NOT gate, it changes the state of the qubit. The quantum NOT gate is also referred to as the Pauli X gate, as the NOT gate essentially rotates the qubit 180 degrees on the x-axis. Other rotation gates include the Pauli Y and Pauli Z gates. Where the qubit is rotated 180 degrees on the y-axis where the Pauli Y gate is applied and a rotation of 180 degrees is carried out on the qubit in the z-axis when the Pauli Z gate is implemented. The controlled Not (CNOT) gate is a two qubit version of the NOT gate composed of a control qubit and a target qubit. If the control qubit is set then a NOT operation is carried out on the target qubit. The CNOT gate produces entanglement a phenomenon crucial to the success of quantum programs. The Hadamard gate applies two rotations on the qubit. It first rotates the qubit 180 degrees on the x-axis, followed by a 90 degree rotation along the y-axis. This procedure produces the Hadamard matrix which places the qubit in superposition. Therefore, this gate is frequently used. The Toffoli gate is an extension of the CNOT gate with three inputs. If both of its two control qubits are set then a NOT operation is performed on the third qubit. The Toffoli gate is essential as it can be used to generate all other logic gates. (Mannucci, 2008)

It is important to note that the state of the qubit is found or measured at the very end of the program. When the state of the qubit is inspected it loses its superposition therefore inspection of the qubit is reserved until the end to obtain maximum benefit from quantum computing. When measured the result is stored in a classical register. This is possible as the result is either a 0 or 1, which is a traditional bit. However, there is a slight difference in that the result here comes with a probability attached as the state of the qubit cannot be known for certain. The measurement gate accepts a qubit in a superposition of states and generates a classical bit as described above.

The IBM Q Experience is a cloud-based platform for designing and testing quantum programs. It is a visual editor where users build quantum circuits by selecting quantum gates represented graphically as blocks. The user builds their quantum circuit in the Composer workspace. Completed circuits named Scores are then run on either on a simulator or an actual quantum processor. However, access to the quantum processors is limited as they are in high demand. The number of qubits available to work with depends on the quantum processor selected.

Quantum programs can be written in Python with the aid of the QISKIT SDK for Quantum Computing. To set up the environment the programmer first imports the Quantum Computing library. Following that generate the required number of qubits and classical registers. There should be a classical register

for each qubit. Set up a circuit in which to place necessary gates. Call quantum gates on chosen quantum register. Apply the measurement gate. As previously mentioned, the outcome will be stored in a classical register. Even though programming in a High Level Language the programmer relies entirely on the use of gates to execute their commands. Such details are abstracted from the programmer of a classical program. (Silva, 2018)

QASM is the quantum assembly language. Programs written in Python and circuits designed on the IBM platform are translated into QASM and then run on a quantum processor. Note that it is more efficient to write a program using QASM than in Python.

Quantum supremacy is the term used to describe the ability of a quantum computer to carry out a task impossible to a classical computer (Preskill, 2012). The term was originally proposed by physicist John Preskill in 2012. This concept has gained much interest and attention since. Quantum supremacy is defined as a super polynomial speedup. In reality very few algorithms produce super polynomial speed up. However, a quadratic speed up is achievable for search problems. Google in collaboration with NASA conducted tests providing experimental evidence of quantum supremacy. The program which randomly generated numbers ran on a 53-qubit quantum processor named Sycamore. It is estimated that it would take 10,000 years to simulate this program on a classical machine in comparison to the 3 minutes and 20 seconds it took for the quantum processor to execute the program. Despite this remarkable advancement in quantum technology, quantum supremacy could be disproved if there was an improvement in the classical algorithms. Though proving the existence of quantum supremacy is a challenge in its own right since it is difficult to simulate these quantum programs on classical machines. This bench marking is a necessary part of the process of demonstrating the arrival of quantum supremacy. (Arute, et al., 2019)

Tito Etimiri 19248547

At this point in time, there are many known applications for quantum computing, Cryptography, Cybersecurity, Drug Development, Climate change, and Artificial Intelligence, to name a few. The possibilities are almost endless for how Quantum Computing will change the world we live in as we know it (Meyers & Deacon, 2004).

According to many researchers, the quantum computer will bring about the end for the need for cryptography. This is an unrealistic expectation however, because the current models of the quantum computer have been unable to perform complex calculations without the aid of cryptography. The strength of the current functional quantum computers relies on cryptographic keys and complex mathematical algorithms (Wright, 2000). Quantum computing could pose a threat to the well-established industry of cybersecurity. Once scientists can find a way to bypass the current lack of power needed for the quantum computer models to break encryptions and bypass security measures, the world of cybersecurity will never be the same. The drug development industry is going to benefit from the completion and commencement of operation of the quantum computer. Currently drug development is a time-consuming endeavour, that entails the draining process of enhancing the drugs currently available and discovering new drugs that could assist the medical field and provide medical developments for humanity. It has been rumoured that the development of the quantum computer would be a key factor in the production of climate-changing agents that could potentially reverse centuries worth of damage, allowing humanity to rethink our choices and save our dying planet. With the aid of the quantum computer, we would not only be able to reverse but also redirect the damage done to the earth into a useful resource, potentially a resource like energy (Cassella, 2017). A lot of this is still speculation of course and will only be confirmed and or denied upon the completion of the quantum computer. Artificial Intelligence will be one of the applications that will benefit from the quantum computer the most. The combination of the similar characteristics of Artificial Intelligence

and the quantum computer would prove beneficial to the advancement of technology. AI combined with quantum computing could also potentially prove beneficial to the financial sector.

> *"In the financial sector, the combination of AI with quantum computing may help improve and combat fraud detection (Lorenzo, 2020)."*

It seems we should not get too excited for the completion of a full scale, impervious quantum computer just yet because scientists are still a way off from properly executing this phenomenon entirely. The computer scientists of the world are in a race to successfully create the first meaningful quantum computer. Statistically speaking such a feat will take another ten years to accomplish, however, an article from Scientific American, states,

> *"IBM, Microsoft, Google, Intel, and other tech heavyweights breathlessly tout each tiny, incremental step along the way. (Jaeger, 2018)."*

These tech companies are vying for the first position. They are paving the way to the advancement of the world and hopefully soon we will bear witness to the development's quantum computing has to offer the world.

At present there are many models of the quantum computer available. The models have been classed, to separate their functions. The models being explored now are the mathematical, machine, circuit, and the algorithmic models. (Ömer, 2003). The progress models developed all over the world include, the quantum Turing machine, quantum circuit model, one-way quantum computer, and the adiabatic quantum computer. The models that have been developed revolve around the most established physical implementations of the quantum computer, which are digital and analogue.

The quantum Turing Machine is a quantum adaptation of the original Turing machine developed as a mathematical model of computation. The principle behind the QTM is to replace bits with qubits. The QTM is hoped to provide a measure for execution times, to speed calculation processes. This application could potentially move computational mathematics forward decades. Quantum circuits, another application in development, are the quantum computer equivalent to classical Boolean feed-forward networks. Essentially, the quantum circuits would carry out matrix operations on quantum bits. Quantum circuits make use of basic quantum gates. Fundamentally, the use of quantum gates makes the manipulation of the quantum system less time consuming and more cohesive. Examples of quantum gates include the NOT (N) gate, Hadamard (H) gate, and the Controlled-Not (CN) gate. (Yi-Lin Ju, 2007). The one-way quantum computer, also known as the measurement-based quantum computer, (MBQC). This model of the quantum computer relates deeply to the aforementioned Quantum Circuit Model. This concept is still in the experimental stages. The one-way quantum computer notion would convey the implementation of qubit measurements used to alter the quantum circuit, thus destroying the connections it has at the same time (Raussendorf, 2001). Adiabatic quantum computing (AQC), is another form of quantum computing that relies on the adiabatic theorem, which is a concept in quantum mechanics, to do calculations (Anon., 2020). AQC was developed to assist with the reduction of time spent and to increase the accuracy of problems, and it has since evolved to be an important application of universal importance. AQC deals with various aspects of complex computational theory, and thus despite being incomplete in its not being the final model of the quantum computer, it has proved very useful and important with the research and further development of the final quantum computer (Albash, 2016).

The mathematical model of the quantum computer describes quantum bits, also known as qubits. The mathematical model is needed for measuring devices and their interaction with quantum bits.

The precise nature of these mathematical formalisms provides a means of working with quantum concepts before fully understanding them. Intuition for quantum mechanics and quantum information processing will develop from playing with the formal mathematics. (Polak, 2011)

The mathematical side of quantum computing has been nicknamed q-processing or q-computations. The mathematics of quantum computing deals with various mathematical applications, from complex linear algebra to basic probability theory. The mathematical approach has been ground-breaking thus far, due to the tireless work of engineers, physicists, and mathematicians at the frontline of this development (Juanjo Rué, 2011).

Annie Reeves 19258933

It is quite clear that a quantum computer is more superior than a classical computer. There are certain tasks that a classical computer cannot execute without the need of absolute force. Factoring being one of them. A classical computer can only factorise small numbers, but it still requires a huge amount of force to execute this calculation. Thanks to Shor's factoring algorithm for quantum computers larger numbers can now be factorised and do not require force in order to be executed. No one really knows what aspect of computing allows Shor's algorithm to work faster than any possible algorithm for factoring. One aspect considered is entanglement, which was explained earlier. Classical computers are local and therefore require some time to resolve contingencies, this in turn wastes a lot of time to execute the task at hand. This is not the case with quantum mechanics and so quantum computers have no need to resolve these problems and waste no time in doing so. Therefore, algorithms are executed twice as fast and larger numbers in large quantities can be factorised. Inside a classical computer, atoms move around slowly and so tasks are performed at a slow rate. That is not the case with a quantum computer (Jaeger, 2018). Atoms move and change much quicker inside a quantum computer allowing each task that a classical computer executes to be performed faster. Atoms don't follow the rules of physics as they can move forwards or backwards in time. They can be in two places at the same time and even have a chance of teleportation. This provides a huge advantage for quantum physics and future computing. Qubits are used in a quantum computer which causes exponential speedup and a larger number of calculations to be performed with ease. The outcomes of measurement of a qubit contains a value of either 0,1 or any value in-between (P.Williams, 2011). A bit can only have one of the two outcomes, 0 or 1, but a qubit can have both and hence store twice as much information. This in turn allows a quantum computer to handle greater amounts of calculations and solve parallel problems at the same time.

There are so many advantages with quantum computing and it is nearly impossible to think of the obstacles that could potentially prevent this masterpiece from becoming a reality. There would be a lot of things that would have to change for us to have the ability to use a quantum computer. Quantum decoherence is the biggest obstacle scientists and physicists have come upon (Fujikawa & Ono, 2000). Working with an electron isn't easy. When the electron is affected by the atmosphere it gets damaged and is no longer useable. This would mean we would have to isolate the system from its environment. The equipment required to preserve the electron is not yet available and we also require superconducting cables, which are only produced by one company in Japan. Decoherence is irreversible and is something that should be highly controlled or completely avoided. When you put it into perspective about how much equipment is needed you start to notice the cost for all this equipment. Technology doesn't come cheap and is often irreplaceable. There are so few companies that produce the products required to run a quantum computer and along with that comes a price since there are so few. Even tech producers need to make a profit. It would simply just cost too much

to produce a quantum computer and the resources are already scarce as it is. Businesses would make a huge profit with one of these computers by their side but is it worth breaking the banks for one. Above the cost and the equipment, what about the people who will have possession over this machine? With a quantum computer a person would become untraceable due to the cryptography elements inside this computer. As it is a classical computer doesn't have the necessary security to help keep private information safe or prevent networks from being hacked. In the wrong hands this machine could become the deadliest weapon known to man. The person would be in and out of a network system without anyone even knowing until it's too late. Mass destruction could be caused and countries turning against each other.

Quantum computing will be part of our future and will forever be changing the way in which we live. As well as providing ways to improve the development of drugs and helping to preserve our agriculture, it will provide a strong income for our economy. It may take time for this process to begin but once it does there will be changes unlike no other. Financial, pharmaceutical and security industries will be the first ones to witness most of these changes in a short space of time. Once these sectors begin to change so will everything else. Products will be produced faster, and customers will have access to these goods as soon as possible. Hence forth more money will be spent on goods and businesses will begin to make a larger profit than before. This in turn will boost the economy and we will begin to see a decrease in the number of local and global businesses closing. Every government will have the funds, through taxes, to build essential facilities like schools, hospitals and economical factories along with essential services like paramedics, firefighters and the gardai. More and more children will have the chance to go to school and hospitals will no longer be over-crowded. We will be able to save more lives on the roads with an ambulance station set up in every town and village. Quantum computing is the way to go and will be one of the greatest discoveries ever made. It will change our perspective on life and change the way in which we live our lives. The only way is up.

Clodagh Walsh 19230737

Quantum computing is greatly impacting the field of Computer Science. It has put modern cryptography methods and cybersecurity defenses in peril. The development of quantum algorithms has prompted experts to review classical algorithms. Developments in this field contribute to advancements in other emerging fields in Computer Science namely Artificial Intelligence. Ultimately this technology is redefining storage capacities and processing time beyond what Computer Scientists once thought was possible.

Works Cited

Aaronson, S., 2013. *Quantum Computing Since Democritus.* s.l.:s.n.

Albash, T., 2016. Adiabatic Quantum Computing. *arXiv,* Volume 3, pp. 2-3.

Anon., 2020. *Adiabatic quantum computation.* [Online]
Available at: https://en.wikipedia.org/wiki/Adiabatic_quantum_computation
[Accessed 2013 April 2020].

Arute, F. et al., 2019. Quantum supremacy using a programmable superconducting processor. *Nature.*

Bone, S. & Castro, M., 1997. *A Brief History of Quantum Computing.* [Online]
Available at:
http://www.academia.edu/download/31815018/A_BRIEF_HISTORY_OF_QUANTUM_COMPUTING_1.docx
[Accessed 01 May 2020].

Cassella, A., 2017. *Re-directing Climate Change and Terrorism by Allying Classical with Quantum Neural Computing,* Melbourne: Redframe Publishing.

Fujikawa, K. & Ono, Y., 2000. *Quantum Coherence and Decoherence.* 1st ed. North Holland: Elsevier Science.

Gibney, E., 2019. The quantum gold rush. *Nature,* pp. 22-24.

Gruska, J., 1999. *Quantum computing.* s.l.:s.n.

Jaeger, L., 2018. *The Second Quantum Revolution.* 1st ed. Switzerland: Springer.

Juanjo Rué, S. X., 2011. *Mathematical Essentials of Quantum Computing.* [Online]
Available at: https://web.mat.upc.edu/sebastia.xambo/QC/qc.pdf
[Accessed 8 May 2020].

Kortum, S. & Lerner, J., 1998. *Does venture capital spur innovation?.* s.l.:National Bureau of Economic Research.

Lorenzo, F., 2020. *How may quantum computing affect Artificial Intelligence.* [Online]
Available at: https://www.bbva.com/en/how-may-quantum-computing-affect-artificial-intelligence/
[Accessed 20 January 2020].

Mannucci, N. S. Y. a. M. A., 2008. *Quantum Computing for Computer Science.* s.l.:Cambridge University Press.

Meyers, R. E. & Deacon, K. S., 2004. *Simulation of applications in quantum computing.* [Online]
Available at: https://spiedigitallibrary.org/conference-proceedings-of-spie/5551/1/simulation-of-applications-in-quantum-computing/10.1117/12.564279.full
[Accessed 5 5 2020].

Narasimhachar, V., 2015. *Low-temperature thermodynamics with quantum coherence.* s.l.:Nature communications.

Ömer, B., 2003. *Models of Quantum Computation.* [Online]
Available at: http://tph.tuwien.ac.at/~oemer/doc/quprog/node9.html

P.Williams, C., 2011. *Explorations in uantum Computing.* 2nd ed. California: Springer.

Pednault, E., Gunnels, J., Maslov, D. & Gambetta, J., 2019. *IBM Research Blog.* [Online]
Available at: https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/
[Accessed 04 May 2020].

Polak, E. R. a. W., 2011. *Quantum Computing - A Gentle Introduction.* Cambridge, Massachesetts,London: The MIT Press.

Polak, W. & Rieffel, E., 2000. *An Introduction to Quantum Computing for Non-Physicists.* s.l.:s.n.

Preskill, J., 2012. *Quantum Computing and the Entanglement Frontier,* s.l.: John Preskill of Institute for Quantum Information and Matter California Intitute of Technology.

Raussendorf, R., 2001. A One-Way Quantum Computer. *ResearchGate,* 86(22), pp. 5188-5189.

Silva, V., 2018. *Practical Quantum Computing for Developers : Programming Quantum Rigs in the Cloud using Python, Quantum Assembly and IBM Q Exxperience.* s.l.:Apress.

Sutor, R., 2020. *The Hype Over Quantum Computers, Explained* [Interview] 2020.

TEDx Talks, 2020. *Quantum computers - a revolution in the making | Shai Machnes | TEDxSavyon.* [Online]
Available at: https://youtu.be/eVjMq7HlwCc
[Accessed 01 May 2020].

Wright, M. A., 2000. The Impact of Quantum Computing on Crytography. *Network Security,* 2000(9), pp. 13-15.

Yi-Lin Ju, I.-M. T. S.-Y. K., 2007. Quantum Circuit Design and Analysis for Database Search Applications. *Circuit and Systems I: Regular Papers, IEEE Transactions,* Volume 54, pp. 2552-2554.