QUANTUM COMPUTING

Patrick Barsoum (19240058)
Richard Alexander (19270151)
Eoin Chedzey (18223796)
Elton Babela (18196497)

CS4182 Foundations of Computer Science 2

Table of Contents

Abstract

This paper researches different areas of Quantum Computing Fundamentals, History, Hardware and Applications in which this new field of research has the potential to transform the lives of everyone on earth. We first introduce the idea of Quantum Computing and how it is different from traditional computing as well as highlighting the key fundamentals, then we discuss a brief history of quantum computing, as well as the hardware making up a quantum computer, then finally highlighting the main applications and uses of quantum computing. The goal of this report is to emphasize the importance of Quantum Computing and the life changing applications that can come out of this field.

Richard Alexander (19270151)

Patrick Barsoum (19240058)

Introduction

Fundamentals of Quantum Computing

Quantum computing is the area of study focused on developing technology based on quantum theory. “The power of quantum computing is based on several phenomena and laws of the quantum world that are fundamentally different from those one encounters in classical computing”. (Gruska 2002)

Over time computers have become smaller and increased in power, however this is meeting its physical limits as computer parts are reaching the size of an atom. A transistor is the simplest form of data processor in a computer, it is a device that regulates current or voltage and acts as a switch or gate for electronic signals that can either be in the off position (no voltage) – represented by a zero, or in the on position (high voltage) represented by a one. These ones and zeros are called Bits, which is short for the phrase Binary Digits. As transistors get smaller and approach the size of an atom, quantum physics makes things complicated. Electrons might just transfer themselves to the other side of a transistor via quantum tunnelling which means there is a limit to how small we can make a transistor. It isn’t all negative though, scientists are using these unusual properties of quantum physics to their advantage by building quantum computers. (Williams, P 2011)

Instead of bits, quantum computers use qubits (quantum bits). There are several physical objects that can be used as qubit - a single photon, a nucleus or an electron and a few others. Electrons have magnetic fields, if you place them in a magnetic field they will align with that field, like a compass that aligns to the magnetic field of the earth. This is the lowest energy state, or as it’s called for the electron, spin down. You can change the electrons energy state or spin by applying some force, just like with a compass if you applied some force you could turn the needle and in principle if you aligned it perfectly against direction of the magnetic field, it would stay there, this is the high energy state or spin up. This is similar to a normal bit, it has two states, spin up and spin down like one and zero. However, qubits can be in both states at once, instead of just being on or off (spin up or spin down), qubits can also be in what’s called superposition, where they’re both on and off at the same time. Superposition is like flipping a coin, it can be either be heads or tails. But as its spinning it’s both heads and tails. Its until you measure it, by stopping the coin, you find out which it is. While it is spinning the qubits have a probability of being spin up or spin down and it is only when you measure it, does it become apparent to which it is. Four Classical bits can be in 2^4 different combinations at a time, that’s 16 combinations of which you can only use one, 4 qubits in superposition can be in all 16 combinations at once. This grows exponentially with each extra qubit added and is represented by 2^n qubits. (Hirvensalo 2001)

One of the most important concepts for quantum computing is quantum entanglement and also one of the most puzzling concepts of quantum physics. Quantum entanglement is a connection between qubits that makes the qubits react to a change in the others immediately no matter how far apart they are. This means when you measure an entangled qubit, you can find out the properties of its partners without having to look. “A pair of quantum systems in a maximally entangled state is the purest form of inherently quantum information: it is capable interconnecting two parties far apart, it cannot be copied, eavesdropped without disturbance, nor it can be used by itself to send classical messages.” (Gruska 2002)

Quantum Entanglement can assist in speeding up both classical and quantum communication. Quantum entanglement is also the main reason why quantum computers cannot be efficiently simulated by classical ones. “To describe fully a state of n-qubit register we need to write down in

general 2^n complex coefficients. Already for a small n = 100 this would require 2^100 ≈ 10^30 numbers, which is outside the potential of foreseeable classical computers." (Gruska 2002)

Boolean gates and circuits are building blocks of classical computers, and in a similar way quantum analogues are essential elements from which quantum computing devices are designed. However, the related theoretical, design and implementation of gates a vastly more complicated for quantum gates and circuits when compared to the traditional methods of classical computing. (Gruska 2002)

A normal logic gate reads in a simple set of inputs and produces a single defined output. However a quantum gate manipulates the inputs of superpositions, rotates the probabilities, and produces another superposition as its output. The quantum computer sets up a set of qubits and then applies quantum gates to entangle the superpositions and manipulate the probabilities, and then finally evaluates the outcome by collapsing the superpositions into a regular sequence of ones and zeros that is in a readable format just like with a classical computer. What this means is you get all of calculations that are possible with the inputs provided, all done at the exact same time. However, you can only measure one of the results and it is probably the result you were looking for but there is a chance you will have to go back and check it again. By using superposition and entanglement efficiently this method will be exponentially more efficient the a classical computer. (Williams, P 2011)

Long before anyone had even thought of quantum computers the physicist Erwin Schrodinger worked out an equation that describes how any isolated quantum system evolves over time. This relates to quantum computing as a quantum memory register is exactly an isolated quantum system, so Schrodinger's equation must describe a quantum memory register as well. Schrodinger's equation is a linear first order deterministic partial differential equation the involves the instantaneous state of quantum memory register and a constant equal to Planck's constant divided by $2\pi r$. (Gruska 2002)

Richard Alexander (19270151)

History of Quantum Computing

Quantum computing is one of humanities next greatest technological achievements. The completion of a fully functional and reliable quantum computer would revolutionise the world as is known today. This revolutionary idea of quantum computing had been in existence" As early as 1959 the American physicist and Nobel laureate Richard Feynman noted that, as electronic components begin to reach microscopic scales, effects predicted by quantum mechanics occur—which, he suggested, might be exploited in the design of more powerful computers."(Holton 2015). This shows us just how new the quantum computing truly is, The research into quantum computing is less than 100 years old to be exact from the year 1959 to date it has only been 61 years since the American physicists and Nobel laureate Richard Feynman had noted his speculations in regards to quantum computing.

Technology is advancing at an extremely rapid pace thanks to the internet and modern digital computers. "During the 1980s and '90s the theory of quantum computers advanced considerably beyond Feynman's early speculations" (Holton 2015). Thanks to the pace at which modern computers have sped the growth of technology. Many people were involved in the development of the knowledge available on quantum computing today. Some of the people involved in this endeavour was David Deutch "In 1985 David Deutsch of the University of Oxford described the construction of quantum logic gates for a universal quantum computer" (Holton 2015) and another one was Peter Shor, Mr Shor had devised an algorithm to factor numbers that only required as few as 6 qubits, he accomplished this in the year 1994 (Holton 2015). In the space of 4 years from Peter Shors contribution to the development of quantum computing, 3 men in the year 1998 created the first quantum computer of 2 qubit that could be loaded with data and output a solution. These 3 men were "Isaac Chuang of the Los Alamos National Laboratory, Neil Gershenfeld of the Massachusetts Institute of Technology (MIT), and Mark Kubinec of the University of California at Berkeley" (Holton 2015). The quantum computer they had created was only coherent for a few nanoseconds but the importance of that first quantum computer was the principles it laid out as to how a quantum computation functions. By the year 2000, 2 other quantum computers were created. The reason for was that some key principles in quantum computing had already been established that facilitated the creation of the quantum computers created in the year 2000. In that year" Emanuel Knill, Raymond Laflamme, and Rudy Martinez of Los Alamos and Ching-Hua Tseng of MIT announced that they had created a 7-qubit quantum computer using trans-crotonic acid" (Holton 2015).

Many Researchers however are sceptical about extending magnetic techniques in quantum computing beyond 10 to 15 qubits because of the diminishing coherence amongst the nuclei. In the year 2000 "physicist David Wineland and colleagues at the U.S. National Institute for Standards and Technology (NIST) announced that they had created a 4-qubit quantum computer by entangling four ionized beryllium atoms using an electromagnetic "trap" (Holton 2015). All this prove that once the principles get to a stage of more clarity it will be possible to further refine quantum computers for efficiency and general use.

Elton Babela (18196497)

Hardware of Quantum Computers

The hardware of a quantum computer is not an easy one to pin down. Unlike building a conventional computer nowadays, there is no standard procedure for creating and assembling a machine like this. It is difficult to say whether current leading technology will be used in the future for developing these machines. “Even if very many papers have been written on potential quantum computers, a definite optimal hardware is still far from being selected” (Amico n.d.)

There are several different architectures that a quantum computer can be modelled off, the most prominent in use now being the quantum circuit using qubits and quantum logic gates. There is an abundance of qubit technologies such as superconductors, polarized photons, quantum dots, trapped ions and spinning atoms. The most widely used currently being superconducting technology but trapped ion qubits have a large potential for being more stable and reliable. However, superconductors solid-state makeup brings faster gate speeds and continue to be used in systems by IBM, D-wave, NASA and Google. “higher absolute fidelities and coherence times in the trapped ion system, with higher clock speeds for the superconducting system.” (Linke *et al.* 2017)

Focusing on the semiconductor technology, these are fundamental hardware components that are not exclusive to just this form of qubit technology but are present in most quantum systems. They can be conceptualized by breaking down a quantum computer into “four abstract layers: the “quantum data plane,” where the qubits reside; the “control and measurement plane,” responsible for carrying out operations and measurements on the qubits as required; the “control processor plane,” which determines the sequence of operations and measurements that the algorithm requires, potentially using measurement outcomes to inform subsequent quantum operations; and the “host processor,” a classical computer that handles access to networks, large storage arrays, and user interfaces.”(Kendon 2018) The host processor is what will be used to interact with the user, running an orthodox OS and UI, it will communicate with the control processor through a high-bandwidth connection.

Quantum Data Plane

The qubit hardware (Quantum Processing Unit) resides on the data plane which is cooled to near absolute zero (> 0 K). This is required as the processor here acts on subatomic particles. Thermal energy in a qubit will give it motion and causes decoherence when measuring these qubits. This along with quantum gate errors are the main contributors to creating a “noisy” superconductor, “the dominant sources of noise in current hardware are unitary gate errors and decoherence” (Kandala *et al.* 2019) This part of the system is also kept in a vacuum to not have gas particles interact with qubits, another source of decoherence. The quantum processor functions by receiving analogue signals and is how information is passed and carried around the processor, this means that almost all of the power needed to run one of these systems “slightly less than 25 kilowatts for the latest machine" (Hsu 2015) is used on cooling and servers.

Control and Measurement Plane

The control and measurement plane are the median between the control processor and the quantum data plane. It converts digital instructions from the control processor to analogue for the quantum data plane to interpret. It then converts analogue signals from the quantum data plane, converts that to digital and relays it on to the control processor for the data to be accessible to the user. The analogue frequency must be high enough as to “avoid thermally populating the qubit”(Barbara 2018) as increasing thermal energy, as shown earlier, increases decoherence.

Control Processor Plane and Host Processor

The control processor oversees identifying and triggering the appropriate quantum gates and operations. “These sequences execute the program, provided by the host processor, for implementing a quantum algorithm.” (Kendon 2018) It is also tasked with the quantum error correction algorithm. Error correction is a vital part if quantum systems want to be useful in the near future. “QPUs remain as isolated operational elements that must interact with a host HPC system using a network interface”(Britt and Humble 2017)

Eoin Chedzey (18223796)

Applications of Quantum Computing

One of the biggest applications for Quantum Computing is cryptography.

Cryptography

Introduction

One of the important areas in modern society is communicating securely. Quantum information transmission and processing contributes significantly to this. Quantum cryptography is a great example that may be the main protection against quantum codebreaking for the future. One of the new features of quantum cryptography is that the security of quantum key generation and quantum cryptographic protocols is based more on the laws of nature than classical cryptography. The security of classical cryptography is based on "unproven assumptions concerning the computational hardness of some algorithmic problems." (Gruska 2002)

Quantum Key Distribution

Quantum key distribution is a method in which quantum states are used to make a random secret key for cryptography.

Basically, Sarah tries to send qubits to Patrick and an eavesdropper Leah, tries to learn and change as much as it can without being detected. This is a difficult task for the eavesdropper as quantum states cannot be measured and copied without causing some sort of disturbance which are immediately detected. (Gruska 2002)

This is the idea of it: There are two people who are separated and want to communicate with each other. In this case, we will be using Sarah and Patrick. Sarah sends to Patrick 2n qubits which are randomly chosen from one of the states |0) , |1) , |+) , |−). Patrick measures the bits he received. He does this by using the measurement basis randomly between {|0), |1)} and {|+), |−)}. Sarah and Patrick tell each other publicly where anyone can listen to how they prepared and measured each qubit. They find out by chance that they may have used the same method which on average, happens half the time and keep those results. If there are no errors, they now "share the same random string of n classical bits." An example of this is to associate |0) and |+) with 0 and |1) and|-) with 1. This is known as *raw quantum transmission*, RQT. (Steane 1997)

So far, it is impossible to learn Patrick's measurement results by just looking at the qubits journey. Some evidence of their presence is left behind. One way for an eavesdropper of whom we will call Leah, to try and find out the key, is to catch the qubits and measure them before passing them to Patrick. On average, Leah guesses Sarah's qubits correctly not disturbing her cycle. Leah's correct guesses doesn't cause conflict with Patrick's. This causes Leah to learn the state of half of the n qubits which Sarah and Patrick trust, and interrupts the other half. Leah basically corrupts n/4 bits of the RQT. By randomly choosing n/2 bits of the RQT, Sarah and Patrick can detect the presence of Leah and so decide to publicly announce the values they have. They can be sure that no eavesdropper was present if they agree on these bits. This can be done since the probability that Leah was present and they happened to choose n/2 uncorrupted bits is (3/4)^n/2 ≃ 10^−125 for n = 1000. The secret key is the n/2 unrevealed bits. This method is used to detect eavesdropping. (Steane 1997)

Quantum computing can provide helpful advancements to human life thanks to the enormous abilities of quantum technology. Not only does it aid in security (cryptography) but also everyday jobs.

Medicine

- The research and development of medical sciences. An example is analysing a sequence of DNA which are usually large in size.
- Diseases like cancer can be diagnosed faster and more accurate.
- Producing and discovering drugs at a scale.
- Analysing and processing heavy images which bioengineering, and telemedicine rely on. (Al-maghraby 2017)

Economy and Finance

- Investment decisions can be done through the analysis and simulation of stock portfolios.
- The detection of fraud is more effective and can be viewed in real time.
- Applications for planting and agriculture. (Al-maghraby 2017)

Information Technology

- Analysing and searching data from big data warehouses.
- Testing and simulating software that is time consuming and complex for current computers.
- The fast response and analysis of massive data such as traffic management is enhanced using quantum processes. (Al-maghraby 2017)

Natural Sciences

- Use quantum computing power to study and simulate experiments that are too costly and time consuming.
- Analysing time series and forecasting. (Al-maghraby 2017)

Patrick Barsoum (19240058)

Conclusion

We discussed qubits and their superposition as well as entanglement and the quantum gates used for qubits. Quantum computers are not just a variation of our classical computers, they are more like a new piece of technology separate to how we think classical machines operate. Overall quantum physics is a mind bender, however by being clever we have turned a disadvantage of our transistors reaching their size limit into a new and exciting realm of possibilities by using the weird world of quantum physics to our advantage. There is still a lot of research and development left to do before we have a quantum computer in every household, but the transformative possibilities are not that far away.

Richard Alexander (19270151)

The history of quantum computing is relatively new. There is still much to be understood about the mechanics of quantum computing and there are still many aspects of quantum computing not yet fully comprehended. There is a rich history of Physics, Mathematics and Computing that led to the development/discovery of quantum computing. It is generally accepted that most of the foundation for quantum computing had been laid in the 80s and 90s. This is the reason why it is accepted that quantum computing properly began in the 1980s. This makes quantum computing only 40 years old but in those 40 years the knowledge about quantum computing has grown quite significantly. This significant growth in quantum computing is due to the hard work done by many great minds such as physicist Richard Feynman who was awarded a Nobel Peace Prize for his work in the scientific field and is famously known for his witty quotes such as "Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy". What is evident with quantum computing is that it is still in its early stages and there is much room for improvements and history has shown us just how much a little information can speed up the process of further developing quantum computers. In today's day and age, it is believed that we have many quantum computers prototypes and we are moving much closer towards the real thing with the many discoveries and breakthroughs achieved by Scientists.

Elton Babela (18196497)

Essentially, a quantum computer is much more than the term 'computer' can convey. It is made up of so many different devices, the QPU operating in analogue format carrying out the calculations while the HPC acts no different from a 'normal' computer digitally. The Control and Measurement plane acts as a translator between devices. All together it fits together as a whole system that has more potential than the supercomputers, we have today.

Eoin Chedzey (18223796)

Quantum computing can be used to aid in our everyday lives as well as one of its biggest applications, yet which is cryptography. Secure communication is an important aspect of everyone's lives and that is where the use of quantum computers come in to ensure that this happens. Medicine is a big part in everybody's lives ensuring that we all stay healthy and alive. Quantum computing can aid in diagnosing one of the world's most deadly disease, cancer, at a faster rate and more accurately. In terms of finance, the detection of fraud is more effective and can be viewed in real time, preventing it from even happening. These are all just a few applications of what quantum computing can do to help the world. Imagine what it would be like in the future.

Patrick Barsoum (19240058)

Bibliography

Al-maghraby, R. (2017) 'Promising Real-Life Applications of Quantum Computing', 1–5, available: http://www.onewayforward.info/Papers/Promising Real-Life Applications of Quantum Computing.pdf.

Amico, I.D.' (n.d.) *Quantum Computer Hardware*.

Barbara, S. (2018) *Metrology of Quantum Control and Measurement in Superconducting Qubits*.

Britt, K.A., Humble, T.S. (2017) 'High-performance computing with quantum processing units', *ACM Journal on Emerging Technologies in Computing Systems*, 13(3).

Gruska, J. (2002) 'Quantum computing', *Technology Review*, 70(7), 632–636, available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.397.2253&rep=rep1&type=pdf.

Hirvensalo, M. (2001) *Quantum Computing* [online], Second Edi. ed, available: https://books.google.ie/books?hl=en&lr=&id=lAmrCAAAQBAJ&oi=fnd&pg=PA1&dq=quantum+computing&ots=hTVrnB8CYc&sig=yvVfUcGbZfdQyoTu5hWR6g55uyU&redir_esc=y#v=onepage&q&f=false.

Holton, W. (2015) 'Quantum computer', available: https://www.britannica.com/technology/quantum-computer .

Hsu, B.J. (2015) 'How Much Power Will Quantum Computing Need? - IEEE Spectrum', 5–7, available: http://spectrum.ieee.org/tech-talk/computing/hardware/how-much-power-will-quantum-computing-need?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+IeeeSpectrumFullText+(IEEE+Spectrum+Full+Text).

Kandala, A., Temme, K., Córcoles, A.D., Mezzacapo, A., Chow, J.M., Gambetta, J.M. (2019) 'Error mitigation extends the computational reach of a noisy quantum processor', *Nature*, 567(7749), 491–495.

Kendon, V. (2018) *Quantum Computing: Progress and Prospects (2018)* [online], Computational Complexity, available: http://link.springer.com/10.1007/978-1-4614-1800-9_148%0Ahttps://www.nap.edu/catalog/25196.

Linke, N.M., Maslov, D., Roetteler, M., Debnath, S., Figgatt, C., Landsman, K.A., Wright, K., Monroe, C. (2017) 'Experimental comparison of two quantum computing architectures', *Proceedings of the National Academy of Sciences of the United States of America*, 114(13), 3305–3310.

Steane, A. (1997) 'Quantum computing', *Reports on Progress in Physics*, 61(2), 117–173, available: https://arxiv.org/pdf/quant-ph/9708022.pdf.

Williams, P, C. (2011) *Explorations in Quantum Computing* [online], Second Edi. ed, available: https://books.google.ie/books?hl=en&lr=&id=QE8S--WjIFwC&oi=fnd&pg=PR8&dq=quantum+computing&ots=BKKPYO-ySP&sig=HnRDjGw9lKOhX_MxD6CxJ35TkQs&redir_esc=y#v=onepage&q&f=false.