EPQ

Will Quantum Computing escape the Theoretical?

Contents

Abstract

Quantum Computing was originally envisaged in the 1980s as a computing technology that could be used to solve certain classes of computational problems more efficiently than is possible with traditional computing technologies.[1] This essay examines whether quantum computing could fulfil this potential, the barriers that will have to be overcome, and the challenges in doing this. The essay reviews the limitations of classical computing and describes fundamental principles of quantum computing technology. It then discusses the use of the quantum technology by specific quantum algorithms and specific areas where the use of Quantum Computing technology has greatest potential. The essay then highlights the technical barriers that need to be addressed to overcome these barriers, and the business and commercial challenges that need to be overcome for the technology to become fully established. It is concluded that there are considerable challenges for the technology to become fully realisable and that there needs to be development in the technology and progress in the commercialisation of the technology for the technology to become mature in the computing industry. However it also concludes that there is considerable ongoing investment from major organisations to enable this to happen.

Introduction

Quantum Computing was first discussed by Paul Benioff in the 1980's who proposed that quantum mechanics could be utilised to create a Turing machine (a mathematical model of a computational system). Then Richard Feynman and Yuri Manin identified that if such a system could be realised it had the potential to address certain problems much more efficiently than is possible with a classical computing system.[2] Since, there has been considerable academic, and industry focus to realise this potential. Specific applications that could benefit from the use of Quantum computing concepts have been identified but there are some barriers to realise the technology in a real-world technical and commercial environment and the introduction of real-world platforms have been tantalisingly just around the corner. This essay describes: the basic technology, the barriers to its productization: and the prognosis for the future.

The Limitations of Classical Computing

A processor is the 'brain' of the computer; it is made up of billions of tiny transistors, which control the flow of electrons and can be used to denote either 0 or 1. These transistors make up Logic Gates, e.g. AND, OR, NOT (the use and meaning of these are discussed subsequently) that perform logical tasks with binary digits. These gates used together form a circuit. The general rule is that the more transistors available in the processor to use, the more capable a processor is at performing challenging and more complex tasks. When a computer has enough of them (in the billions) it has the capability to perform tasks that a human could never do. The number of transistors needed for the processor is normally directly proportional to complexity to the task that can be performed. Over time, transistors become smaller and smaller and more can fit into one space.[3] The first modern transistor was made in 1947 and was 14 micrometres in size which is under twice the size of a red blood cell. Today, the processor manufacturer Intel mass-produces transistors to a scale of 14 nanometres which 500 times smaller than a red blood cell.

A classical computer's computational capability depends on the amount and size of transistors and, as transistors get smaller, they become closer and closer to the size of the electrons they are trying to control.[4] Additionally, as the hardware becomes smaller, the usual Standard physics model is replaced with the Quantum physics model, and this is problematic. For example, if transistors become small enough, 'Quantum Tunnelling' becomes an issue, where electrons can 'bypass' the transistor. This essentially puts a physical cap on Moore's Law which predicts that the number of transistors on a processor will double every two years.

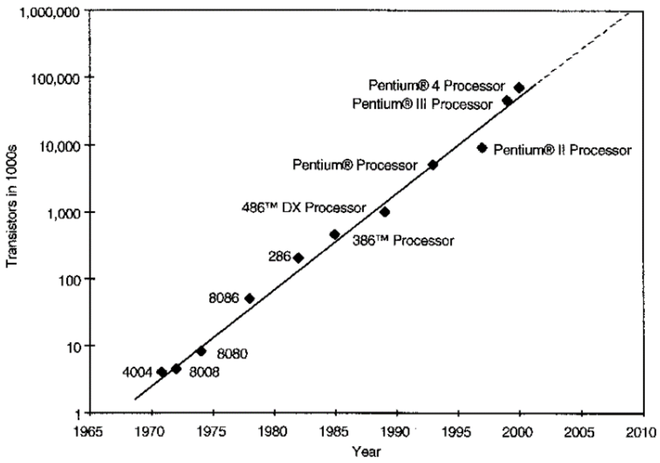


Figure 1

Quantum Computing with its ability to process and manipulate exponentially more data than Classical Computing opens up great possibilities to address problem sets that require this capability.[5]

Theoretical Basis for Quantum Computing

In Physics, many different strange phenomena occur in a Quantum Model that do not in the Standard Model. This apparent contradiction between the proven Quantum Model and the Standard Model still represents one of the greatest mysteries in Modern Physics.[6] However, there are a number of concepts in the Quantum model that are of great potential use in Quantum computing, the main ones being: superposition, interference, and entanglement. Quantum computing uses these concepts to create the 'Qubit'.[7]

In classical computing, the computational model is fundamentally deterministic, and the core object of information in the model is the 'bit' which either has a value 0 or a value 1. In Quantum computing, the computational model is fundamentally probabilistic, and the core object of information in the model is the 'Qubit' which has a value 0, 1, or a superposition of 0 and 1.[6] This non-deterministic probabilistic attribute can be exploited by specific algorithms to address problems where linear deterministic approaches can't efficiently address the vast number of scenarios that need to be modelled.

Superposition – explained using electrons

One of the most famous experiments in Physics is the Double Slit Experiment, first performed by Thomas Young.[8] When a monochromatic source (same wavelength) of light is shone through a wall with two slits in it, the light goes through both slits onto a screen on the other side and a classic 'interference' pattern is observed, where the waves from the two slits interfere with each other.

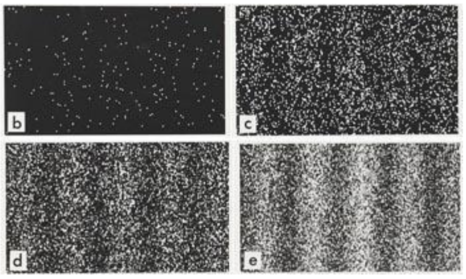


Figure 2

If this experiment was done with electrons, depending on how the electrons are observed, the outcome can show an interference pattern (implying behaviour as a wave), or a slit pattern (implying behaviour as a particle). The experiment is showing that electrons could take on two natures - this dual nature is called Wave-Particle duality. [9] Section 'e' in Figure 2 shows the interference pattern and 'b', 'c' and 'd' show a graduation towards it.

Heisenberg tried to measure the position of electrons by using photons. However, when the photons reach the electrons, the electrons changed velocity and moved to an excited state, showing that it is impossible to measure the location and the velocity of an electron at the same time. This is known as the observer effect. [10]

Electrons also have a property called ‘spin’, which was investigated in a series of experiments by Otto Stern and Walther Gerlach. They found that the isotopic spin was either upwards or downwards. However, as a Quantum particle, the electron can have a certain probability of spin up, and a certain probability of spin down, a phenomenon known as superposition**.** If the spin of the electron is measured the electron would ‘jump’ to either spin direction or the other, which direction is entirely random. [6]

Another property of electrons is that the state of spin is related to other electrons, even those far away. This concept is totally alien to classical physics but intrinsic to Quantum Theory. This property is called entanglement and has applications in Quantum Information theory, in that it allows for the ability to perform multiple calculations simultaneously but in a manner which is related to each other.[11]

The ability of a quantum particle such as an electron to have an up (‘0’) a down (‘1’) and a superposition, as well as demonstrating entanglement properties, is a very accurate model for a ‘Qubit’. [6]

Uses of Quantum Computing

In classical Computing, the solution to a problem that involves different pathways/outcomes, is found by consecutively testing each pathway until the preferred outcome has been found. This method is incredibly inefficient if the problem concerned involves millions of pathways and can it impossible for classical computers to find solutions to problems in a sensible time scale.

For these types of problems, the development of Quantum Computing is promising. The ability to have Qubits to be super positioned and entangled in many positions at once allows exponential increase in computing speed. This allow problems to be addressed that were beyond the capabilities of Classical Computing, and solution to these problems can literally change the world. Some of the potential applications are described below.

Quantum Chemistry Modelling

In Material Science and Medicine, how molecular bonds are formed and change the characteristics of that molecule defined the whole basis for the science. Simulating a molecular composition or a chemical reaction is hard for classical computers.

A key use of molecular simulation is about finding the compound's ground state where the molecules are in the lowest energy state, and this depends on finding the most stable configuration of the electrons. For classical computers, this is difficult, as they need to simulate all the possible configurations and energy levels of the electrons in each atom interacting with others that also have multiple configurations, along with the separate outcomes of Quantum Mechanics, which would also affect events that occur. This problem becomes exponentially difficult in time complexity as the size of the atom or compound increases. "If you have 125 orbitals and you want to store all possible configurations, then you need more memory in your classical computer than there are atoms in the universe," says Matthias Troyer (Microsoft Research in Zurich). In comparison, a Quantum Computer with 250 qubits could model this system.

Tech giants such as Google have backed this idea. Their 54 superconducting qubit computer called Sycamore achieved quantum supremacy in 2019. It carried out a calculation that would be impossible for a classical computer to perform in a reasonable amount of time. This simulated the molecule called diazene, which consists of two nitrogen and two hydrogen atoms. The problem took 200 seconds to complete when in comparison, Google stated that the world's fastest current classical computer called the Summit would take 10,000 years to solve the same problem.[17]

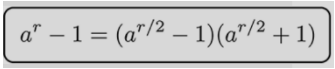
In this application of computing, Quantum machines appear to have significant advantage over Classical options because of their unique architecture.

Other practical examples for the of such an approach, would include (amongst many other examples):

- enabling a full understanding of the enzymes that underlie photosynthesis and the nitrogen cycle[18][19]
- the discovery of high-temperature superconductors and new materials for solar cells[17]

Quantum Code Breaking

The norm for sending data over the internet is to 'encrypt' it. This means that a message containing 0110 can be converted using a secret key that only Alice and Bob know to be Ae8K. If Eve does intercept the message, all she gets is Ae8K – this is called Ciphertext. She does not know what key it was encrypted with – so she cannot read the message at all even though she has intercepted it. When Bob receives the Ae8K, he uses his correlating key to decrypt it back into 0110.[17] Standards keys are usually 128 to 256 bits long, making it impossible for computers to try and 'crack' the encryption process. Trying every combination possible for a 128-bit key with 2128 possibilities, this would lead to 340,282,366,920,938,463,463,374,607,431,768,211,456 different combinations. If brute force was used to crack this key (try every combination possible until answer is found), a normal computer that could test 240 different combinations a day would crack this key for 847,904,136,496,835,804,725,427 years. This shows that encryption can be extremely secure. However, the rise of Quantum Computing puts these forms of classical encryption at risk. Algorithms like Shor's Algorithm can be applied to breaking codes.



$$a^r - 1 = (a^{r/2} - 1)(a^{r/2} + 1)$$

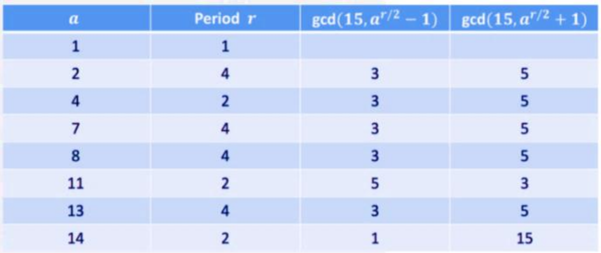
Figure 3

E.g. the powers of three
- 3,9,27,81,243,729,2187,6561
Modulus to 20
- 3,9,7,1,3,9,7,1
Has a period of 4 (r)

For example, Shor’s algorithm can be used to find the factors of an arbitrarily big number N needed to be found. If a random number 'a' was defined, that number might be a factor of N (providing a $<$ N). The number a is likely not to be a factor of N, however $a^{r/2} + 1$ is much likely going to be a factor of N.

When multiplying a by a factor of x and then modulus of N ($a^x \ mod \ N$), there will be a periodic sequence associated with it.

By using the identity above, factors are more likely to be found rather than via a brute force route. The table below shows how trying to find the factors of N = 15 can still garner results even though the guess a is not a factor. [20]



a	Period r	$\gcd(15, a^{r/2} - 1)$	$\gcd(15, a^{r/2} + 1)$
1	1		
2	4	3	5
4	2	3	5
7	4	3	5
8	4	3	5
11	2	5	3
13	4	3	5
14	2	1	15

Figure 4

Finding the periods of a function can be implemented on a classical computer. However, using the Quantum Fourier Transform is responsible for the quantum speedup.

To find the periods of a function on a Quantum computer, you need to create a superposition of the states. Usually, this is done by applying Hadamard gate to every qubit. Instead, a Quantum Fourier Transform (QFT) is applied These speeds up the algorithm by only using O((log(N)^2)) gates. QFT acts on an input qubit and maps it to a vector y_k in accordance with the formula. [21]

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \omega_N^{jk}$$

Figure 5

In this section we have seen that Quantum Algorithms can break current encryption methods by finding keys that are beyond the reach of Classical Computing, thereby posing a significant security risk.

Quantum Algorithms

Quantum Speedup and Query Complexity

A method of proving that the validity of Quantum Computing is superior to Classical Computing is to reference Quantum Speedup. Quantum Speedup is the ratio of the time for convergence for solution to the problem when using a Quantum algorithm when compared with the best conventional algorithm.[12]

Most algorithms are superior to do on a classical computer and therefore have a speedup less than 1. However, certain tasks are much better suited to solutions on a Quantum computer the algorithms in this case would have a very high Quantum speedup.[13] An example of one such task is trying to find a specific unique value in an unordered list. The only way to do this classically is to force a search of the entire list – searching every value consecutively until the right one is found. Let's say, on average. It takes 1 million steps. When a specific algorithm defined by Grover is used on a quantum computer, the time taken to search the list is, on average, a thousand steps. [14]

Query Complexity allows for the analysis of algorithm types and classifies them into different classes to help designate the amount of resource and time for the solution to be achieved.

One of the classes is 'P '. 'P' classifies problems that are solvable in deterministic polynomial time, usually decision-based problems such as a forced search. A classical computer can generally solve these problems with ease. [15] However, there are circumstances e.g., cryptography, where it still cannot be solved without a significant amount of computational time.

Another example of a complexity class is 'NP.' 'NP' problems are solvable in non-deterministic polynomial time, which includes issues that are solved usually in exponential time. These are problems that can be verified in polynomial time, e.g., finding prime factors of a number. Due to these problems being non-deterministic, many different actions could be performed on a single input (a good example of these type of problem sets are computer simulations. Classical computers find it hard to solve these problems effectively, however, Quantum computers have the capability to solve some NP problems. [12]

Database Searching and Grover's Algorithm

A database is where data is collected, stored, and organised in a contextual way that fits the database's purpose. It can also be accessed and searched. However if the database has a million items to search, the time taken to find something is directly proportional to a database’s size, and therefore as a solution, it does not scale. Algorithms have been created to counter this, such as the algorithm ‘Binary Search’. This takes the midpoint of the data and, depending on whether the value query is above or below the median value, discards the half of the data that is not needed and repeats the process. This delivers a significant time improvement compared to checking every value in order until it is found (called a Linear Search). In terms of time complexity, it's O(n) for linear search and O(log n) for binary search, the importance of this speedup can be seen in the graph in Figure 3. [16]

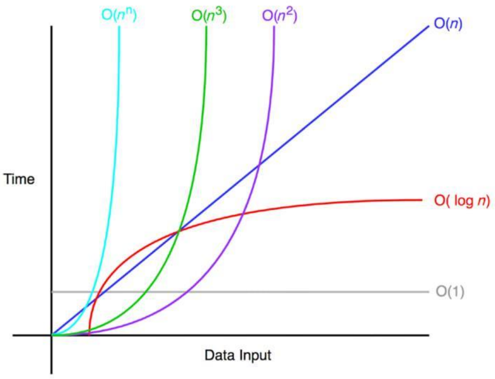


Figure 6

However, a binary search assumes that the list is ordered, and this is not always known. The aim of Grover's algorithm is to address the problem in a different manner. If, for example, there are four strings that hold the values 00,01,10,11. Then this represents a function that returns one of the strings as true and three false, e.g. 01 was returned the true value. As Grover’s is a Query Complexity algorithm, the function provides the answer, and the question is, ‘what value returned true’.

Using two qubits in a superposition of all possible values (using a Quantum computing function called a Hadamard Gate), every state would have the same probability amplitude of$\frac{1}{\sqrt{2^n}}$, where n depends on the length of the string. Applied to this problem, each amplitude would be $\frac{1}{\sqrt{4}}$ which equals $\frac{1}{2}$ The sign of the probability amplitude for the queried value amplitude is flipped from$\frac{1}{2}$ to -$\frac{1}{2}$. If the queried value is measured as well as the other values, this will bring up the same answer $(\frac{1}{2})^2 = (-\frac{1}{2})^2 = \frac{1}{2}$. To further differentiate the queried value, a function called Grover's Diffusion Operator is used, which amplifies the amplitude. This is done by 'inversion about the mean'. The mean of the amplitudes is taken, and the difference between the value and the mean is identified. If the value is below the mean, it is upwards by adding the mean and the difference. If above the mean, then it is flip downwards by subtracting the difference from the mean. For example, if there are four numbers [1,1,1,-1] (one flipped as it's the queried value), the mean would be$\frac{1}{2}$. The difference for 1 -$\frac{1}{2}$ = $\frac{1}{2}$ and the value 1 is above the mean$\frac{1}{2}$ Meaning this should be flipped below the mean; it now becomes 0. For the value -1, the difference between the mean is$\frac{3}{2}$ and the value is below the mean, so when it is flipped upwards, it becomes 2. This process has amplified the amplitude for the true value.

Applying this to the binary string problem, the Superposition would be represented as:

$\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$

Then the queried value is flipped:

$\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle$ - $\frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$

Then the probability amplitudes are flipped

$0|00\rangle + 0|01\rangle + 1|10\rangle + 0|11\rangle$ which equals $|10\rangle$

For a bigger data set, amplitudes would need to be repeatedly amplified to get to the answer.

Even though there is a quadratic speedup of using Grover's algorithm in comparison to linear search, the implementation in the real world is challenging. The oracle needs to be implemented, making sure it's reversible and no information is lost. This means that the complexity of the overhead of the Algorithm actually leads to the situation that in simple cases it can be slower than a 'classical' algorithm. [17]

This leads to us to the conclusion that Quantum Computing provides potential benefits and advantages over Classical Computing. This is only fully realised when the problem is significantly complex. When problems are simpler, the overheads required for the implementation of Grover’s Algorithm will means Classical solutions available today are quicker in comparison.

Implementation Considerations

Physical Realisation of a Qubit[25]

A Qubit can be anything that can possesses a binary state and the property of superposition. A range of technologies have been investigated as they demonstrate the necessary quantum level behaviour. Choosing which technologies to use for a qubit is dependent on considerations relating to the stability and the logistics of that qubit. The two main considerations are Coherence Time and Gate Time. The Coherence Time is the lifetime of the qubit for which it will maintain its intended state. This is important because over time, the qubit will interact with its environment (called interference), which will change its spin state, making the qubit useless. (electrons are notorious for interacting with their environment making them hard to use). Gate Time is the time required for a single gate operation until an error occurs.

A measure for the utility of a Qubit is the Gate Fidelity, which is essentially a measure of repeated accuracy of the Qubit . In Figure 7, various Quantum technologies were plotted against Gate Fidelity (the number of operations before an error) and the gate's speed. The dashed line indicates the error threshold – where the error rates become so high that adding more error-correcting qubits does not help the accuracy of the gate.

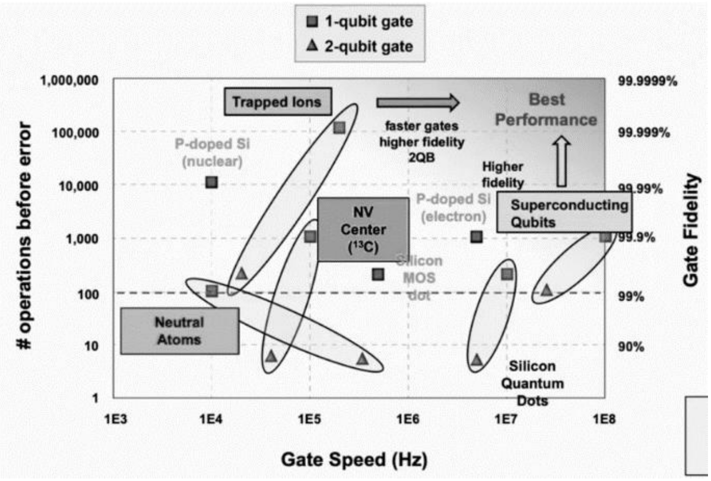


Figure 7

From the graph, the most promising technologies are for the Superconducting Qubits and for Trapped Ions Qubits. Superconducting qubits have a rapid gate speed – but a higher error rate. Trapped Ions already have a lower gate speed but are more accurate. Both are described in more detail below.

Superconducting Qubits

The use of Superconducting Qubits is one of the most common implementations of qubits. Industry giants such as IBM and Google are using this method.[23] This involves decreasing the temperature of a superconductor material to near absolute zero. Once the material is cooled below its critical temperature, there is no electrical resistivity; a benefit of this is that an electrical current can flow through that material indefinitely without a power source.[24]

This phenomenon is due to Cooper Pairs, where an electron interacts with an ion that creates a potential disturbance or phonon; Another electron then becomes attracted to the phonon, and the electrons indirectly interact with each other. This interaction drops the electron into a lower energy state which let the electrons move freely and superconduct.[25][13]

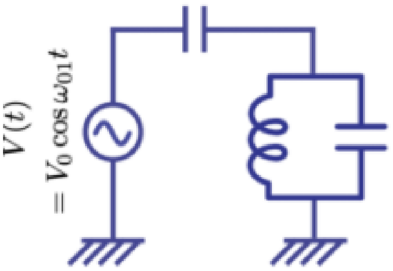


Figure 8

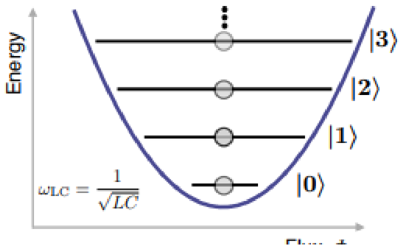


Figure 9

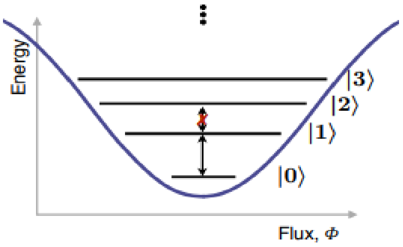


Figure 10

A $|0\rangle$ or $|1\rangle$ is represented in the qubit as energy states; spin-down is the lowest energy state, and spin-up is the higher energy state. A' Superconducting circuit' is used to manipulate and retain the qubits state. They are comprised of a capacitator and Josephson junctions.[26] To explain the Josephson Junction, consider an LC circuit (Figure 8) consisting of an inductor and a capacitor. The inductor is made from a conductor that is wound into a coil which the current flows through, generating a magnetic field. The capacitator is made up of two conductors separated by an insulator that is used to store energy electrostatically in an electric field. This is results in a positive charge building upon one of the conductors and a negative on the other, which stops the flow of current. The only way for a current to flow is for an alternating voltage to be applied. This is significant because the two components create a 'loop'. The capacitator would store all the charges and stop the flow in the circuit until a voltage is passed through and releases a current. This current comes into the inductor and creates a magnetic field and creates a voltage. This voltage then triggers the capacitor to recharge, and the cycle continues. The oscillation of energy between the two components can manipulate the energy state of the qubit. This is a Harmonic oscillator.[27]

The energy state levels are represented in Figure 9 but it should be noted that the energy gaps are all uniform which means that to go up one state and down to mean a $|0\rangle$ or a $|1$. To avoid multiple state level jumps introducing increasing errors, Josephson Junctions are used. This type of junction comprises two Aluminium superconducting electrodes separated by a thin insulator, and it behaves as a non-dissipating and a non-linear inductor, which means that the energy level is spaced in a way that limits the chances that the qubits state is invalid. See Figure 10.

The drawbacks with Semiconductor qubits are that the quantum states are very sensitive and therefore the system has to be kept at extremely low temperatures, and that interference expands greatly with an increasing number of Qubits. The first problem limits the number of physical deployments of the system, the latter problem limits the power of the Quantum computers that can be created.[26]

Trapped Ion Qubits

Another technology for making Qubits is by using Trapped ions; this is an approach championed by IonQ and Honeywell. Trapped ions are isolated atoms that have a charge, which can then be individually manipulated and measured. An ion is an atom with an electric charge.[28] The most common used atom is Calcium, which has two electrons on its outer shell.

The ions are 'trapped' between four electrodes. The electrodes create an electric field oscillating in two directions at a Radio Frequency, (RF) to be to trap the ions in all three dimensions in accordance with Earnshaw's theorem. This creates a 'saddle-shaped' electric field that keeps the ions in place.

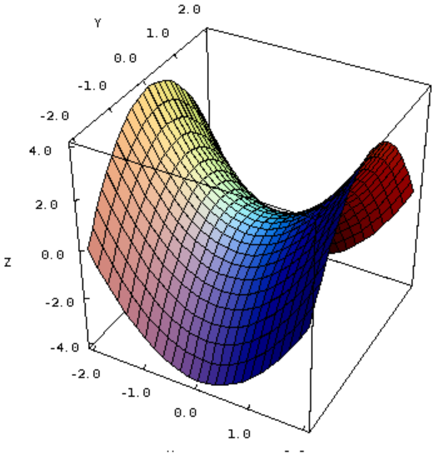


Figure 11

Qubits can still move around in this confined space, and they need to be approximately stationary so that they can be manipulated and measured. To do this, Laser Cooling is used to control the Kinetic energy of the qubits by emitting single photons that have momentum in the opposite direction the qubit's movement is, which inevitably cancels out the qubit's velocity. Doppler effect measurement is used to make sure the ion absorbs the photon and is used to detect the energy level of the ion which indicates whether the qubit is in the state |0⟩ or a |1⟩.

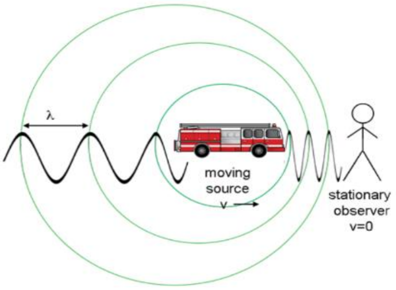


Figure 12

To measure the qubit, a laser with a specific frequency is shone on the electron and the result changes depending on the state. The laser frequency used depends on what is required to excite the ion at that specific state. The outcome will be that the qubit is excited and de-excited continuously when shone on. If the qubit is not in the state when being measured, the ion will not be excited by the laser. Whether the ion is being excited and de-excited is indicated by photons which are captured by a CCD camera.[29]

Error Correction[30]

When transferring data across locations classically, certain bits will be corrupted and changed. These changes could have dire consequences on the message being sent. In a quantum system,

qubits are more prone to the encoded information being lost in transmission. The amount of environmental interference that the Qubit may suffer is called 'the amount of noise in a communication channel'. To avoid this noise, the least error-prone type of qubit technology is preferred and error correction tools are incorporated when transmitting qubits. This is called noise suppression and a common method for this is described below. The reality is that any noise suppression can only handle a certain level of 'noise' and so the Qubit technology that is chosen, and its implementation, needs to drive the noise as low as possible.

Repetition Code

A way to recognise qubit errors is called Repetition Code. Where each qubit is repeated three times consecutively, e.g. 010 would be repeated as 000111000. Therefore, if I sent a message to Bob, he would expect to receive a sequence of three 0s and 1s. However, if he received a 101, he knows that an error has occurred. It should have been either 000 or 111. If it was 111, then one error must have happened, and if it was 000, then two errors must have occurred. By balance of probability, it is more likely that one error occurred than two. Therefore, Bob corrects that qubit to 1 for it to become 111.

This method is fine for a Classical system but not for a Quantum system as the qubits cannot be read without them jumping to a state. A way to get around this is to perform Parity Tests.

Imagine Bob receives three bits (b_1, b_2, b_3). He expects them all to be the same. The Qubits cannot directly be measured to see whether they are the same, so instead, they are put through the CNOT gate. This is because a CNOT gate returns a 1 when two qubits are different values from one another.

$b_0 \oplus b_1 = 0$ and $b_0 \oplus b_2 = 0$ then together 00 Bob will flip nothing

$b_0 \oplus b_1 = 0$ and $b_0 \oplus b_2 = 1$ then together 01 Bob will flip b_2

$b_0 \oplus b_1 = 1$ and $b_0 \oplus b_2 = 0$ then together 10 Bob will flip b_1

$b_0 \oplus b_1 = 1$ and $b_0 \oplus b_2 = 1$ then together 11 Bob will flip b_0

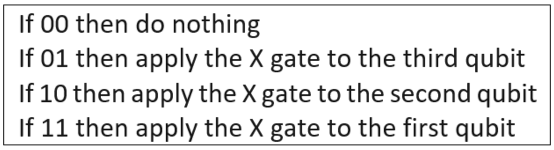
Quantum Bit Flip Correction

Quantum Bit Flip Correction builds on top of Repetition Code. Two more qubits called Ancilla qubits are inserted into the algorithm. The Ancilla qubits are qubits used to test the authenticity of qubits without measuring them. This is done by collecting information about the noise in the communication channel. They are not fundamentally needed when finding errors; however, it is necessary when fault-tolerant methods are required.

Imagine Alice needs to send a qubit of information to Bob. She does it the previous way and sends three copies of the same qubit to Bob, e.g. she would like to send the qubit $|0\rangle$, it goes to the state $\alpha|0\rangle + \beta|1\rangle$ then to $\alpha|000\rangle + \beta|111\rangle$.

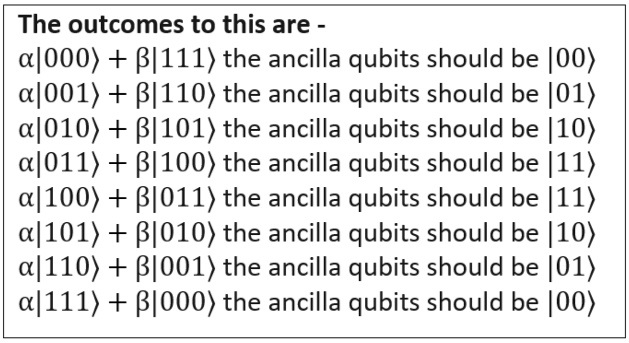
Once Bob has received the qubit, he introduces a pair of ancilla bits. He first carries out CNOTs from the first and second received qubits to the first ancilla qubit, then from the first and third received qubits to the second ancilla bit.

For there to be no errors, the outcome should be $|00\rangle$, therefore if anything else is observed then an error has occurred in transmission.



If 00 then do nothing
If 01 then apply the X gate to the third qubit
If 10 then apply the X gate to the second qubit
If 11 then apply the X gate to the first qubit

Pauli's X Gate is used to flip any wrong bits.



The outcomes to this are -
$\alpha|000\rangle + \beta|111\rangle$ the ancilla qubits should be $|00\rangle$
$\alpha|001\rangle + \beta|110\rangle$ the ancilla qubits should be $|01\rangle$
$\alpha|010\rangle + \beta|101\rangle$ the ancilla qubits should be $|10\rangle$
$\alpha|011\rangle + \beta|100\rangle$ the ancilla qubits should be $|11\rangle$
$\alpha|100\rangle + \beta|011\rangle$ the ancilla qubits should be $|11\rangle$
$\alpha|101\rangle + \beta|010\rangle$ the ancilla qubits should be $|10\rangle$
$\alpha|110\rangle + \beta|001\rangle$ the ancilla qubits should be $|01\rangle$
$\alpha|111\rangle + \beta|000\rangle$ the ancilla qubits should be $|00\rangle$

Industry/ Business Context for the Technology?

Most of the discussion in this essay has been on the theoretical plane and discussion of platform technology. Governments have funded considerable amounts of research (to name but one - UK Government has launched a 10-year investment scheme into building multiple quantum network hubs to propel and grow the industry in the UK) and private companies have invested considerable resources to realise the physical realisation of computer platforms than can be used to solve real problems.[31] According to IDC predictions, 25 percent of the Fortune Global 500 will gain a competitive edge from quantum computing by 2023, it is therefore a sector that the large computing platform companies can't ignore as it risks being a very disruptive technology.[36] McKinsey Consulting project that market to be worth $1 Trillion by 2035, with the lead sectors being Finance, Materials, Pharma and Telecom.[34]

It is clear that there is a perceived opportunity for the technology to be applied, the open question is whether Quantum computing product will get to market to address the opportunity and if it does, how will it get to market.

At present it is still not clear if one dominant technology will emerge or whether a number of different technologies will emerge, each looking to address the challenges of bringing useful 'Qubits' to market.

In terms of actual announcements Google has perhaps been the most vocal with the announcement of Google Supremacy in October 2019. Google claimed that their Sycamore system had 53 Qubits (based on Semiconductor Qubits) and they had created the first quantum computer that could perform a calculation that is impossible for a standard computer, specifically Sycamore had taken only 200 seconds to perform a calculation that their researchers estimated would have taken a state-of-the-art supercomputer 10,000 years to compute (*SN Online: 10/23/19*). Google claim to be working on Qubit error correction which will enable greater stability of the system and lead to larger systems.

IBM dispute certain elements of the announcement and also claim 53 Qubit systems. They also have announced in September 2020 chips of 500 Qubits and 100+ Qubits to be coming to the marketing in before 2023, with the claim that there will be further error correcting initiatives.

What is clear is that the large computing platform companies view Quantum Computing as a strategic area that they will be active in with considerable resources deployed. Both Google and IBM are heavily invested in the superconducting Qubit approach and they are focussed on bringing products to market which will address the known barriers in the deployment of such technology. Given the present delicacy of the technology it is likely that the capability provided to the marketplace will be a Cloud offering with capacity rented to end customers. If the large companies are able to bring products to market, the potential of the capability can then be explored by end customers to assess how their computing problems that presently cannot economically be addressed using supercomputers, can be solved using Quantum computing technology. Companies such as Rigetti Computing, have been providing a 31-qubit computer on a cloud service for some time. Additionally, IBM has set up an online IDE (Integrated Development Environment) which allows users to make their own Quantum Algorithms as an aid to learning about Quantum Computing. [34]

It is worth noting that there may be challenges to the superconducting Qubit approach, from different technologies being applied to Quantum computing. A Chinese research project has recently announced a Photon based Quantum Computer consisting of 113 Qubits (IEEE Spectrum 6th November 2021). Also, a far eastern company claims some success using a technology called nuclear magnetic resonance, which works by manipulating specially selected molecules in a powerful magnetic field. These technologies have the potential to be more robust and capable of on-site installation. This highlights the fact that the sector is far from mature and there could well be highly disruptive technological advances that could completely change the commercial models in the market in the future.

Conclusion

Quantum Computing has matured greatly as a technology in the 40 years since its inception. There is now considerable understanding of the theoretical model and how it can be applied to real world problems. A considerable amount of investigation has taken place into candidates to be the core underlying technology, prototyping has taken place and the investigation into the multiple candidates is continuing. Initial products are starting to be introduced and first phase customers engaged. At present it is still not clear if one dominant technology will emerge or whether a number of different technologies will emerge, each looking to address the issues of Qubit Coherence, Error Rates and Gate Speed. It is also not clear whether Quantum Computing will be installed on site or whether it will remain, as it is at present, a cloud-based solution.

The large computing platform industry giants are fully engaged in a race to make the technology a reality, and they are backed by governments of the large economies who view Quantum Computing as extremely strategic. With this amount of focus it is highly likely that technological progress will continue, and Quantum Computing platforms will appear into what is still a nascent market.

There are undoubted problem sets that Quantum Computing can be applied to, and that these applications have the potential to broaden once the power of the Quantum Computing platforms can be more widely accessed by industry and academia.

Evaluation

I decided to undertake an EPQ as I wanted to challenge my motivation, focusing on a challenging topic that complements my aspirations in the Technology Industry. Furthermore, an EPQ helps progress my understanding of the subject outside the A-Level syllabus, and this will significantly help me when reviewing other topics like this in the future.

Throughout the completion of the EPQ, I have acquired a wide variety of skills that serve to benefit me. An example of this is to reflect on the project and on myself systemically. The increased perception gives me the ability to have an objective view of my work. At the start of my project, I did not reflect on myself consistently. Instead, I made mistakes when planning my dissertation, which forced me to consider alternate methods of success. Likewise, my mentor gave me new approaches to the structure of my EPQ and the encouragement for the procurement of my external mentor.

By actively seeking out an external mentor, my confidence in speaking and starting a rapport with others increased significantly, and I put myself out of my comfort zone and succeeded. My external mentor was extremely helpful when considering the direction of my EPQ and helped me realise the importance of experts as a form of primary research and made me aware of several other avenues for research that I did not recognise previously.

I believe that my organisational skills have improved immensely by completing my EPQ. It forced me to plan out and be accountable through deadlines set by my mentor. I had to keep track of my work and what needed to be done, entering my activities through the activity log. The log helped me be accountable for my performance and limited the tendency of procrastination. If I were to do another project, I would include an Activity Log to make sure I hold myself culpable for the work done. Additionally, I would be more aware of my capabilities and the time needed for the work necessary. I would actively consider if I can meet the expectations that I have set at each stage of the project and makes the required amendments if necessary

After looking back on my objectives in my Project Proposal Form, I believe that I largely kept to my aims. The room for improvement lies with my language being too broad. I was too ambitious with my aims when considering that my EPQ has a finite length. To the extent where my mentor suggested reducing the scope. For example, I state that I will research into the 'proposed solutions this sector could answer which Classical Computing cannot'. The language suggests too large of a scope where most cases are assumed to be included. Instead, with help from my mentor, I decided to focus on two of the main applications for Quantum Computing where I could go into detail and still be able to cover the main objectives. Overall, this wasted time, as I had already researched multiple different utilisations of Quantum Computing to use only two of them. On the other hand, I recognise that from the further research, I acquired a deeper understanding of the industry which helped me reach a concluding statement for my dissertation. If I had the opportunity to do the project again, I would want to explore other implications that Quantum Computing would have on society in more detail for the reasons listed above.

When researching the project, I decided to write up the research whilst exploring the successive sections of the project. I think it worked both for and against me. It helped break up the project into two smaller tasks, which would make the project less monotonous as I could have a variety of activities. This kept me enthusiastic. When deciding to start my project, I was aware that procrastination could be an issue for me. I recognised that it could have been detrimental to the completion of the project and made the necessary alteration to suit me. However, this method made me less efficient with my time writing the dissertation. From reading into other sections linked with prior sections, I would realise that I had more points and arguments to add and then would have to make the necessary revisions and additions to my dissertation. This meant I had many drafts of work that would need to be rechecked for grammar and ensure that everything was factually correct. It wasted a considerable amount of time and effort. If I were to go back, I would use another method to break up the work. This can be breaking the research into logical sections that I can concurrently work on without needing other research. This would require more planning and organisation in the initial stage of the project.

The skills and lessons I have discussed above will help me greatly in my future life. I want to pursue to do Computer Science at University. Skills of reflection, organisation and time management will help me to partake in independent learning with ease. A computer science course and the industry rely on students learning programming languages proactively and having the knowledge of current affairs. These skills will be highly applicable. Additionally, the writing of my EPQ will aid in future essay writing at university.

References

[1] Andreas Baumhof. (2019). ‘Quantum leap: why the next wave of computers will change the world’, *World Economic Forum*. 29th October. [Online]. Available at: https://www.weforum.org/agenda/2019/10/quantum-computers-next-frontier-classical-google-ibm-nasa-supremacy/ (Accessed: 24/11/2021)3

[2] The Recommender. (2021). ‘Quantum Computing’, *The Recommender*. [Online]. 28th October. Available at: https://www.therecommenderjr.com/article-quantum-computing/ (Accessed: 14/11/2021)

[3] Torrie William. (n.d.). ‘Advantages of Quantum Computing over Classical Computing’, *CSEstack.org*. [Online]. Available at: https://www.csestack.org/advantages-of-quantum-computing-over-classical-computing/ (Accessed: 15/11/2021)

[4] Arnab Hazari. (2016). ‘The future of electronics is light’, *The Conversation*. [Online]. Available at: https://theconversation.com/the-future-of-electronics-is-light-68903 (Accessed: 15/11/2021)

[5] Benjamin Stafford. (2019). ‘What will we do when Moore’s Law is no more?’, *Matmatch*. [Online]. Available at: https://matmatch.com/resources/blog/what-will-we-do-when-moores-law-is-no-more/ (Accessed: 15/11/2021)

[6] Chris Bernhardt. (2019). ‘Chapter 5 - Bell’s Inequality’. *Quantum Computing for Everyone*, Cambridge (Massachusetts): MIT Press. pp 71-87

[7] Martine Giles. (2019). ‘Explainer: What is a quantum computer?’, *MIT Technology Review*. [Online]. 29th January. Available at: https://www.technologyreview.com/2019/01/29/66141/what-is-quantum-computing/ (Accessed: 14/11/2021)

[8] Andrew Zimmerman Jones. (2019). ‘Young’s Double Slit Experiment – The Original Experiment’, *ThoughtCo*. [Online]. 29th January. Available at: https://www.thoughtco.com/youngs-double-slit-experiment-2699034 (Accessed: 14/11/2021)

[9] Marianne (n.d.). (2020). Physics in a minute: The double list experiment, *+plus magazine*. [Online]. 19th November. Available at: https://plus.maths.org/content/physics-minute-double-slit-experiment-0 (Accessed: 14/11/2021)

[10] Wikibooks. (n.d.). The Quantum Model, *General Chemistry*. [Online]. Available at: https://en.wikibooks.org/wiki/General_Chemistry/The_Quantum_Model (Accessed: 15/11/2021)

[11] Stephen M. Barnett (n.d.). ‘Introduction to Quantum Information’*, School of Physics and Astronomy, University of Glasgow*. [Online]. Available at: https://www.gla.ac.uk/media/Media_344957_smxx.pdf (Accessed: 14/11/2021)

[12] Chris Bernhardt. (2019). ‘Chapter 8 – Quantum Algorithms’. *Quantum Computing for Everyone*, Cambridge (Massachusetts): MIT Press. pp 141-170

[13] Rio ICM2018. (2018). ‘*Understanding quantum algorithms via query complexity – Andris Ambainis – ICM2018’*. [Video]. 28th September. Available at: https://www.youtube.com/watch?v=v2Y7KkvpmVw&ab_channel=RioICM2018 (Accessed: 21/11/2021)

[14] Craig Gidney (2013). ‘Grover's Quantum Search Algorithm’, *Twisted Oak*. Weblog. [Online]. 5th March. Available at: http://twistedoakstudios.com/blog/Post2644_grovers-quantum-search-algorithm (Accessed: 21/11/2021)

[15] Udacity. (2015). ‘*P and NP – Georgia Tech – Computability, Complexity, Theory: Complexity’*. [Video]. 23rd February. Available at: https://www.youtube.com/watch?v=n0zd5hcOSQI&list=WL&index=49&ab_channel=Udacity (Accessed: 23/11/2021)

[16] Andy Matuschack, Michael Nielson. (2019). ‘How does the quantum search algorithm work?’, *Quantum Country*. [Online]. 16th April. Available at: https://quantum.country/search (Accessed: (Accessed: 21/11/2021))

[17] Chris Bernhardt. (2019). 'Chapter 9 – Impact of Quantum Computing'. *Quantum Computing for Everyone*, Cambridge (Massachusetts): MIT Press. pp 171-189

[18] Witold W. Kowalczyk. (n.d.). 'Let's make Quantum Computing about Sustainability', *Zapata*. Weblog. [Online]. Available at: https://www.zapatacomputing.com/lets-make-quantum-computing-about-sustainability/ (Accessed: 5/11/2021)

[19] Frederik Kerling. (2017). 'Could quantum hold the key to saving the environment?', *Atos.* Weblog. [Online]. 11th October. Available at: https://atos.net/en/blog/quantum-hold-key-saving-environment (Accessed: 5/11/2021)

[20] IMB Quantum Computing (n.d.). 'Shor's Algorithm', *IMB Quantum Computing*. [Online]. Available at: https://quantum-computing.ibm.com/composer/docs/iqx/guide/shors-algorithm (Accessed: 21/11/2020)

[21] Qiskit (n.d.). 'Quantum Fourier Transform', *Qiskit*. [Online]. Available at: https://qiskit.org/textbook/ch-algorithms/quantum-fourier-transform.html (Accessed: 21/11/2020)

[22] QC Ware (Speaker: William Oliver). (2020). '*Q2B 2019 | Introduction to Quantum Computing | William Oliver| MIT*'. [Video]. 16th April. Available at: https://www.youtube.com/watch?v=ZuHHgoe2B0o (Accessed: 29/10/2021)

[23] Alexandre Blais. (2015). 'Superconducting qubits', *QIP 2015*. [Presentation]. Available at: http://www.quantum-lab.org/qip2015/slides/QIP2015-Alexandre%20Blais.pdf (Accessed: 18/11/2021)

[24] Philip Krantz, Morten Kjaergaard, Fei Yan, Terry P. Orlando, Simon Gustavsson, William D. Oliver. (2019). 'A Quantum Engineer's Guide to Superconducting Qubit', *Applied Physics Reviews.* [Online]. 6 (2) pp 6. Available at DOI: https://doi.org/10.1063/1.5089550 (Accessed: 19/11/2021)

[25] Superconductivity. (n.d.). 'BCS Superconductivity Theory'. [Online]. Available at: http://www.chm.bris.ac.uk/webprojects2000/igrant/bcstheory.html (Accessed: 18/11/2021)

[26] Jonathan Hui. (2019). 'QC - How to build a Quantum Computer with Superconducting Circuit?', *Medium*. Weblog. [Online]. 7th January. Available at: https://jonathan-hui.medium.com/qc-how-to-build-a-quantum-computer-with-superconducting-circuit-4c30b1b296cd (Accessed: 18/11/2021)

[27] Electrical4U. (2021). 'LC Circuit Analysis: Series, Parallel, Equations & Transfer Function', *Electrical 4 U*. Weblog. [Online]. 4th July. Available from: https://www.electrical4u.com/lc-circuit-analysis/ (Accessed: 20/11/2021)

[28] Andrew Steane. (n.d.). 'Introduction to Ion Trap Quantum Computing', *Department of Physics, University of Oxford* . [Online]. Available at: https://www2.physics.ox.ac.uk/research/ion-trap-quantum-computing-group/intro-to-ion-trap-qc (Accessed: 8/11/2021)

[29] Jonathan Hui (2019). 'QC – How to build a Quantum Computer with Trapped Ions?', *Medium*. Weblog. [Online]. 14th January. Available at: https://jonathan-hui.medium.com/qc-how-to-build-a-quantum-computer-with-trapped-ions-88b958b81484 (Accessed: 8/11/2021)

[30] Chris Bernhardt. (2019). 'Chapter 7 – Quantum Gates and Circuits'. *Quantum Computing for Everyone*, Cambridge (Massachusetts): MIT Press. pp 117-140

[31] Quantum Technologies Strategic Advisory Board. (2015). 'National strategy for quantum technologies - A new era for the UK'*, UK National Quantum Technologies Programme*. Innovate UK and the Engineering and Physical Sciences Research Council. [Online]. March. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/414788/Strategy_QuantumTechnology_T15-080_final.pdf (Accessed: 6/11/2021)

[32] Eric Burgener. (2019). 'Top 10 Worldwide Enterprise Infrastructure 2020 Predictions', *IDC*. [Online]. 2nd December. Available at: https://blogs.idc.com/2019/12/02/top-10-worldwide-enterprise-infrastructure-2021-predictions/ (Accessed: 2/11/2021)

[33] Consultancy.uk. (2020). 'Quantum computing market to reach $1 trillion by 2035', *Consultancy.uk*. [Online]. 15th April. Available at: https://www.consultancy.uk/news/24361/quantum-computing-market-to-reach-1-trillion-by-2035 (Accessed: 2/11/2021)

[34] David Matthews. (2021). ‘How to get started in quantum computing’, *nature*. [Online]. 1st March. Available at: https://www.nature.com/articles/d41586-021-00533-x (Accessed: 14/11/2021)

List of Figures

Figure 1:

John H. Vanston. (2022). ‘Enhance the validity and credibility of your forecasts by structuring them in accordance with the five different ways people view the future’. *Research Technology Management*. Ch.Make Better Forecasts. Available at: https://www.researchgate.net/figure/This-graph-of-Moores-law-shows-the-regularity-of-improvements-in-transistors-over-a_fig1_239580581

Figure 2:

Dr Tonomura & Belsazar. (2012). ‘Double-slit experiment results in Tanimura’, *Wikipedia Commons*. [Online Image]. Available at: https://commons.wikimedia.org/wiki/File:Double-slit_experiment_results_Tanamura_four.jpg

Figure 3:

Bonvic Bundi. (2019). ‘Understanding Big-O Notation With JavaScript’, *DEV Community*. [Online Image] 10th October. Available at: https://res.cloudinary.com/practicaldev/image/fetch/s--NR3M1nw8--/c_limit%2Cf_auto%2Cfl_progressive%2Cq_auto%2Cw_880/https://thepracticaldev.s3.amazonaws.com/i/z4bbf8o1ly77wmkjdgge.png

Figure 4:

IMB Quantum. (n.d.). ‘Shor's Algorithm’, *IBM Quantum*. Available at: https://iqx-docs.quantum-computing.ibm.com/_images/shor-equation1vm27qee4bcma38fr2.png

Figure 5:

IMB Quantum. (n.d.). ‘Shor's Algorithm’, *IBM Quantum*. [Online Image]. Available at: https://iqx-docs.quantum-computing.ibm.com/_images/shor-table9nl8715xk3d3rf6r2.png

Figure 6:

Qiskit. (n.d.). Quantum Fourier Transform. *Qiskit*. [Online]. [Online Image]. Available at: https://qiskit.org/textbook/ch-algorithms/quantum-fourier-transform.html

Figure 7:

QC Ware (Speaker: William Oliver). (2020). ‘*Q2B 2019 | Introduction to Quantum Computing | William Oliver| MIT*’. [Video] Time: 18:42. 16th April. Available at: https://www.youtube.com/watch?v=ZuHHgoe2B0o (Accessed: 29/10/2021)

Figure 8:

Alexandre Blais. (2015). ‘Superconducting qubits’, *QIP 2015*. [Presentation]. Slide 20. Available at: http://www.quantum-lab.org/qip2015/slides/QIP2015-Alexandre%20Blais.pdf

Figure 9:

Alexandre Blais. (2015). ‘Superconducting qubits’, *QIP 2015*. [Presentation]. Slide 20. Available at: http://www.quantum-lab.org/qip2015/slides/QIP2015-Alexandre%20Blais.pdf

Figure 10:

Alexandre Blais. (2015). ‘Superconducting qubits’, *QIP 2015*. [Presentation]. Slide 24. Available at: http://www.quantum-lab.org/qip2015/slides/QIP2015-Alexandre%20Blais.pdf

Figure 11:

Mathspig (2015). ‘Maths Mystery Box 8: Junk Food’, *Mathspig*. Available at: https://mathspig.files.wordpress.com/2015/02/pic-2-graph_hyperbolic_paraboloid-mathinsight.png

Figure 12:

The Imagine Team. (n.d.). ‘Doppler Shift’, *National Aeronautics and Space Administration*. Available at: https://imagine.gsfc.nasa.gov/features/yba/M31_velocity/spectrum/images/siren_stationary.png