School of Physics and Astronomy

Quantum Computing

Senior Honour Group Project Report

A. Harun, T. Baird, H. Rathee, T. Duce, L. Kefalas, C. Panayi
Feb 2019

Abstract

This report entails a summary of the theory, technology, algorithms and applications of quantum computers. Current examples of existing quantum processors are also provided, and the potential of the field of quantum computing as a whole is discussed. We conclude that at this moment in time investment in quantum computing technology isn't preferable to current classical systems. However, in the foreseeable future quantum computers will start to outperform their classical counterparts, potentially making them desirable to investors.

Date: February 4, 2019

Supervisor: Professor A. C. Shotter

Contents

1 Introduction

The idea for a quantum computer was first introduced back in the 1980's by the famous theoretical physicist Richard Feynman [1]. This idea arose from the fact that certain problems which can't be solved by classical computers, where shown to be solvable by their quantum counterparts. There is a recent rise of interest in development of Quantum Computation technology right now by companies like IBM and Google, making this the right time to start looking into the technology behind it and its advantages. Companies like IBM have been releasing their quantum computers with better processors and it is only a matter of time when this technology of the future becomes the present.

The aim of this report is to begin with understanding the physical properties that allow for such computers to exist. These properties are found in the field of quantum physics, which describes the fundamental laws of nature at its smallest known scale, and are known as the principle of superposition, quantum entanglement and interference.

The report continues with a review of the most widely used processor technologies available today, whilst including quantum processors which are seen as having a large potential by researchers but are currently at a more theoretical level. This will contain a discussion about the difficulties and limitations of each processor type, which in turn will give us an idea of their place in the future of the field.

We also discuss the way that such quantum processors are used to solve numerical problems, giving examples of some of the most important quantum algorithms, and also providing actual examples of recent applications of quantum computers that are proven to work more efficiently than classical ones.

Finally, we include a speculation on the likely advances in the development and uses of quantum computers in years to come, along with a conclusion about whether or not such technology is worth investing in.

2 Theory

2.1 Superposition

Unlike our classical world, the quantum mechanical world is non-deterministic. This means that small particles, like electrons, can't be described by definite states, like position and velocity. They can, however, be described by a state vector which gives all the possible states, along with their respective probabilities, that the particle can be in. Therefore, before any measurements are taken, the particle is thought to be in all possible states at the same time and this is known as the principle of superposition [2]. This is indeed very counter-intuitive which is why it is better described by mathematics. State vectors are represented by the standard notation of quantum mechanics, called the Dirac notation [3, p. 78–79], and are labeled as $|\Psi\rangle$. Consider a particle which can exist in a number, N, of different possible states. We label each of these states as $|\phi_i\rangle$ and they each have a certain probability of being occupied, related to the numbers a_i. Then the state vector that describes the particle can be written as

$$|\Psi\rangle = \sum_{n=1}^{\infty} a_i \, |\phi_i\rangle$$

where the constants a_i have the property: $\sum_{n=1}^{\infty} a_i = 1$, since they are directly related to probability values.

The principle of superposition has no analogue in the classical world since the position and velocity of a classical object, for example a football, are deterministic and well-known.

2.2 Entanglement

Another property found in quantum mechanics that has no classical analogue is the entanglement between two or more particles. Entangled particles have states that can only be described with reference to each other and can't be broken down to single-particle states [4]. This means that once the particles interact in a certain way their states become correlated and a measurement of the state of one particle can affect the state of the other.

One key feature used in quantum computing, that arises from the entanglement of two qubits is quantum teleportation which describes how the information of a quantum state can be transported from one place to another, independent of their spatial separation [5, p. 26–28]. Considering two entangled particles far apart, if one of the particles is in a certain state, it can share its information to the other particle allowing it to acquire the same exact state, although no matter is teleported. It should be noted that once the receiving particle is in the desired state, the state of the initial particle is destroyed. This is due to the no cloning theorem which states that it is impossible to make a copy of a particle that is in a certain (unknown) superposition of many states. This property allows for the exchange of information through what is known as a quantum channel. However, since a classical channel is also required to utilise this information, quantum teleportation doesn't allow for faster-than-light communication.

Entanglement is also represented by the same mathematical language as seen previously in order to give a better picture of what an entangled state should look like. One frequently used example of an entangled state of a system comprised by two particles, A and B, where each can occupy two possible states, labeled as $|0\rangle$ and $|1\rangle$, is a group of states known as the Bell states [5, p. 25–26]. The choice of the given labels will be apparent in Sec. 2.4. These four states obey the mathematical restrictions of what constitutes an entangled state and are expressed as

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle - |1_A 1_B\rangle)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0_A 1_B\rangle + |1_A 0_B\rangle)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0_A 1_B\rangle - |1_A 0_B\rangle)$$

2.3 Inteference

Aside from superposition, which allows for a particle to be at many positions at once, a single particle can also interfere with its own trajectory and direction of its path. This was first shown by the famous double slit experiment in 1927. Using electrons instead of light waves, this experiment showed that small particles can behave as waves, coining the term wave-particle duality [6].

Interference can be either constructive or destructive, where the former applies to the addition of amplitudes and the latter applies to their subtraction. Since qubits are subject to interference, probabilities that are associated during and at the end of each computation don't follow the rules of classical probabilities. For example, it can be shown that an n-qubit system can be manipulated such that one of the 2^n possible states can yield a probability that is higher than the sum of all the individual state probabilities [7, p. 269–271]. This property can help in categorising and differentiating results obtained at the end of computations.

2.4 Qubits

Classical computers store information in the form of bits which can either take the value of 0 or 1, true or false respectively. This is a two state system that can be labeled as either $|0\rangle$ or $|1\rangle$. The quantum mechanical analogue of the bit is the quantum bit or qubit [8] which, due to superposition, can be in both states at the same time. Its mathematical representation is

$$|\Psi\rangle = a_0 |0\rangle + a_1 |1\rangle \,, \text{where } |a_0|^2 + |a_1|^2 = 1 \,.$$

Such systems can be physically realised by subatomic particles, like electrons or photons, which can be in a superposition of two possible states called spin up, $|0\rangle$, and spin down, $|1\rangle$.

All the possible states of a single qubit can be visualised geometrically using what is known as the Bloch sphere, which is a unit vector in a three-dimensional space whose direction depends on the values of its probability amplitudes a_0 and a_1.

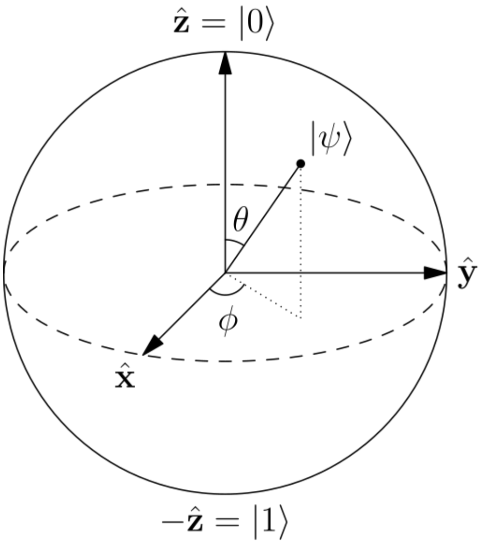


Figure 1: Geometrical representation of the qubit. In this representation the probability amplitudes a_0 and a_1 are expressed in terms of the angles, θ and ϕ, between the state vector $|\Psi\rangle$ and the x and z axis respectively [9].

Another useful representation of this two-state system is in the form of 2-dimensional vectors with each state labeled as

$$|0\rangle \to \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad |1\rangle \to \begin{pmatrix} 0 \\ 1 \end{pmatrix} .$$

The reason behind this notation will be more apparent once quantum gates are introduced.

Furthermore, a two-qubit state can be represented by a superposition of the 4 possible states as:

$$|\Psi\rangle = a_0 |00\rangle + a_1 |01\rangle + a_2 |10\rangle + a_3 |10\rangle$$

So, by following the above argument, it can be shown that an N-qubit system can be represented by a superposition of 2^N possible states, which means that the system can be in all 2^N states at once. It is apparent that such property of the qubits can make some computations exponentially faster and thus more efficient.

2.5 Quantum Gates

The building blocks of classical computers are called logic gates which are responsible for processing bits of information stored in the register. Logic gates have the form of switches and can manipulate electric currents that either allow the current to pass though $|0\rangle$ or prevent it $|1\rangle$. This shows the relation between flow and lack of flow of current to information. Such logical operations on bits is called Boolean Algebra and each operation can be represented by a truth table.

In quantum computing, quantum gates take the form of linear operators (matrices) which act on states (vectors) and the quantum register is simply a state vector depending on the number of qubits of the system. For single-qubit quantum gates the only requirement for such operators to be considered quantum gates is mathematical in nature and called unitarity [10]. This simply means that the operator, when acted upon by its inverse gives the identity matrix $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.This means that any unitary matrix can be a valid single-qubit quantum gate. Some important examples of single-qubit quantum gates, that will be further discussed in Sec. 4, are

1. The Hadamard gate H
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$
2. The three Pauli gates X, Y and Z
$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

The X Pauli gate is the quantum equivalent to the classical NOT gate.

When considering multiple-qubit gates it can be shown that they can always be broken down to a combination of the CNOT [11] gate and single-qubit gates. This is called the universality of the quantum gates [12, 13].

2.6 Measurements

In order for quantum computations to be useful they, ultimately, need to provide a final result that can be understood and may be processed even further. As seen previously, a qubit can be in a superposition of both the states $|0\rangle$ and $|1\rangle$. However, according to quantum mechanics, when one actually tries to measure this qubit it will be forced to take one of the two possible values, thus behaving like the well-known classical bit. This action of the qubit is known as the collapse of the wavefunction, and it is observed in all quantum systems upon measurement [14, p. 11–22]. The final value of the measured qubit, prior to the measurement is unknown, but the probability of either $|0\rangle$ and $|1\rangle$ occurring is given by the values $|a_0|^2$ and $|a_1|^2$ respectively, which are not necessarily known.

It might be tempting to think that one qubit contains more than one bit of information but the collapse of the wavefunction upon measurement shows that when measuring one qubit, only one bit of information is obtained. Only Nature can keep track of the values of the probability amplitudes associated with the superposition of one or more qubits and it is of great importance, for quantum computing, to understand how to utilise the information hidden in superpositions of qubits without actually measuring them.

The act of measurement can be further classified into two parts referred to as projective and Positive Operator-Valued Measure (POVM) [5, p. 87–91], with the former being the most widely used in most applications concerning quantum computing. Projective measurements are very useful in calculating averages and standard deviations. POVM, on the other hand, is a mathematical formalism that is associated with the probabilities of the individual states rather than the actual post-measurement outcome, which is useful, for example, when one considers an experiment where a measurement takes place only once.

2.7 Decoherence

A major problem in quantum computing is the fact that the system of qubits cannot be in complete isolation. This means that qubits can interact with their immediate environment causing unwanted entangled pairs and the disappearance of the qubits superposition, forcing them to have a random and probably unwanted superposition as well as completely destroying their superposition causing them to behave as classical bits [15]. This phenomenon, known as decoherence, can destroy the computational process mid-way.

The time taken for a quantum system, in superposition, to decohere completely is called decoherence time. This time interval is directly affected by the temperature of the system and its surroundings, the higher the temperature the shorter the decoherence time.

Due to the above issues quantum processors are usually kept in vacuum, inside large containers which are themselves maintained at extremely low temperatures (at about 0.01 K). In classical computing any possible errors errors that might occur during the computation can be easily minimised by having a number of copies of the qubits such that the errors won't actually affect the computation. However, as stated previously by the no-cloning theorem [16], a qubit can't be copied, so other ways had to be found to deal with errors associated with decoherence. The field of quantum error correction [17] was then developed which contains a mathematical description of manipulating quantum gates and qubits in such a way as to reduce the damage caused by possible interactions of the system and its surrounding environment.

3 Quantum Processor technologies

We shall now review the various processor technologies which have been proposed to realise a first wave of quantum computers. There are a large breadth of different approaches; however, only a few of these have actually seen production or considerable progress in development. We shall identify what are currently the most promising of the suggested processor technologies with evidence from the literature along with a description of their different operating principles and capabilities. Comments shall also be made regarding the reasons why the others appear to to be less likely to play a main role in quantum computing in the near future, with a general discussion of the difficulties in the evolution of each processor type given at the end of the relevant subsection. Prior to the discussion of individual technologies, let us briefly summarise several important concepts which are crucial for the appreciation of different processors. Firstly, all quantum computers essentially have the same fundamental requirements for operation and a particularly popular statement of these requirements was codified by the American physicist DiVincenzo, in the so called DiVincenzo criteria [18]. These criteria have become the standard basis at which experimental implementations of a quantum computer are assessed by researching groups [19]. Where possible, we refer to these criteria in our description of the different processor technologies for clarity and because their fulfillment indicates the success of that technology. The following is a brief statement of these criteria:

1. Firstly, each QC requires the use of a quantum system to constitute an individual qubit.

2. Secondly, it must be possible to set the qubits up so that they are in a well-defined reference state for beginning the computation.

3. A third criterion is that the processor possesses adequately long decoherence times so that the information stored in the QC does not become corrupted before the desired computation has been carried out.

4. The fourth of DiVincenzo's criteria demands that the processor technology in question is able to implement a universal set of quantum gates.

5. The fifth and final criterion states that the computer must have the capability of carrying out measurements of the states of individual qubits.

One should also note the implicit necessity of entangling a large number of these qubits across the registers of the computer in order to achieve the full potential of the computer in question. Therefore, the number of simultaneously entangled, fully controllable qubits boasted by a given technology is one benchmark of its power.

We go into considerable depth in describing two of the more promising processor technologies (superconducting qubits and ion-trap quantum computers) as paradigmatic examples of how these criteria are met in practice and the difficulties faced in doing so. Briefer statements are given for the other proposed technologies.

Let us briefly expound the implications of criteria 3 and 4. It has been shown that it is possible to achieve any quantum operation we require on a set of qubits in a computer by making use of a finite set of quantum logic gates. These gates are said to constitute a set of universal quantum gates and one can think of them as the quantum equivalent of the classical NAND gate from which any classical logic operation can be constructed. As mentioned previously Sec. 2.5, one such set of quantum gates is the Hadamard gate, single qubit rotation gates, and the two qubit controlled NOT gate (CNOT) . The ability of a given processor technology to implement performant versions of these gates is therefore one crucial test of its viability.

Another critical factor deciding whether or not a given processor technology is practicable is its ability to deal with decoherence. This is the phenomenon whereby the information stored in qubits becomes corrupted due to an unwanted alteration of their state and can occur, for instance, due to interaction of the qubits with their environment. There are two main measures of decoherence in quantum computing. These are the T_1 and T_2 coherence times of the qubits. The first of these, the T_1 coherence time or relaxation time gives a measure of the loss of energy from the system. It can be understood through an example. If our qubits were to adopt the form of ions and their ON/OFF states were to correspond to their electronic energy states, then their T_1 time would be the average time taken for a spontaneous decay to occur from the ion's excited state to its ground state. On the other hand, the T_2 coherence time, or dephasing time, is a measure of the time taken for randomisation of the phase difference between the qubit's logic states. To understand what is meant by this, it is best to have in mind the Bloch sphere representation of a qubit's state, already discussed in Sec. 2.4. Certain types of noise in the qubit's environment may cause the state of the qubit to swing about the equator of its Bloch sphere (corresponding to a change in the phase between its 0 and 1 components). This leads to a different probability of finding the qubit to be ON or OFF when a measurement is performed. Clearly, this is unhelpful as it leads to incorrect results in our computations. The T_2 time tells us on average how long it takes for this dephasing to become appreciable [20]. For a QC to perform correctly, these times must be lengthened by reducing the noise in the system or dealt with through a family of methods called quantum error corrections. Success on this front is judged as having the qubits remain coherent for long enough so that quantum gates can carry out their operation or measurement devices perform their readout before the stored information is reduced to gibberish. Comment will be made in the following sections regarding how successful each processor technology is at achieving these tasks.

3.1 Trapped ion quantum computer (TIQC)

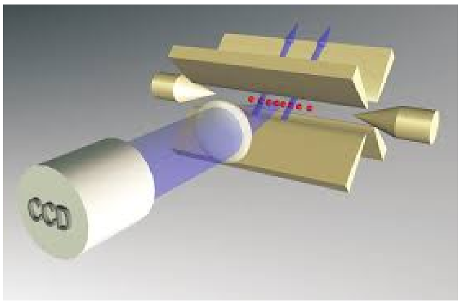


Figure 2: An individual ion trap confining a string of ion qubits [21].

Trapped ion quantum computers are another suggested approach to realizing qubits and manipulating them. In a trapped ion QC the electrically charged nature of an ion is used to confine the ion to a containment device through the use of electromagnetic fields.

Such an element (the ion in a trap) constitutes a single qubit. Pulses of light (photons) are used to manipulate the states of these qubits in order to carry out computations. As mentioned previously, two distinct states of this ion must be selected to constitute the on/off (or 0/1) states of the qubit. What is done then, is that two different energy levels of the ion are chosen to represent these states - whereby a more energetic, excited state of the ion may represent the 1 state, and a less energetic state may represent the 0 state [22, 23]. In order to have a successful quantum computer, it is imperative that **many** qubits can be simultaneously placed in an initial state, manipulated, stored, or measured. For a trapped ion QC, it has been proposed that this problem is tackled through scalable trap designs. This sees one bring together an array of ion traps (each containing one or more ions) which are interconnected so as to allow for the transfer of information from one trap to another. It also permits the storage of information in classically familiar memory locations where the qubits are incapable of being modified. Furthermore, the individual qubits are acted upon by quantum logic gates in designated interaction regions [24]. The nature of these gates is discussed later.

To meet the second of DiVincenzo's criteria, an essential part of the functioning of a trapped ion QC is the preparation of the initial states of all the qubits in a given quantum register. The most common technique used to achieve this is called optical pumping. Basically, we start out having all the ions confined to traps, but in random states. We then use a laser to repeatedly excite the ion to certain excited states by firing photons at it. Once excited, the ion subsequently radiates photons and de-excites. One special de-excited state is our chosen initial state that we want all our qubits to start out in. If the ion de-excites to this state, the laser light is by design unable to excite the ion from this state and since it is stable, the ion remains in this desired state. If the ion had de-excited to an undesirable state, the laser will go ahead and excite it again. This process continues on and on until all our qubits are in the initial state that we want. This technique has been shown to be capable of 99.9 % fidelity (i.e., carrying out the expected operation 99.9% of the time) [25].

In order to achieve the aforementioned crucial operating requirement of precise measurement of the qubit states following computation, a trapped ion QC again makes use of the individual energy levels of the confined ion in conjunction with a laser. When a measurement is performed on the ion to see what state it is in, the ion collapses into a given state - say state 0. The laser is tuned so as to cause the ion to be excited if that collapsed state is one of a particular energy. Following excitation, the ion subsequently de-excites, giving out a photon of light in the process. From this new de-excited state, the ion is once again excited by the laser and this process continues on, giving rise to a large number of photons which are gathered by a device such as a photomultiplier tube or CCD camera. Now, going back to the point of our initial measurement, if the ion collapses into another state - state 1 in our case - then the laser is tuned so as to be unable to excite the ion from this state. Therefore, such a measurement does not give rise to the release of a large number of photons. In this way, we are able to tell which state the ion is in upon measurement. The precision of this measurement is determined by the ability to discern between the 1 state, where no photons other than irrelevant noise photons are detected, and the 0 state, where many photons should be detected. The accuracy is found to be $> 99.9\%$, making this type of QC superior in this respect to most others [26]. Several different proposals for the physical implementation of single qubit rotation gates and two-qubit controlled NOT gates have been proffered over the years. Some of these have actually also seen experimental demonstration and usage in the few examples of working TIQCs. Single qubit rotation gates which use rabi flopping (the changing the state of the qubit by firing a beam of photons at it and subjecting it to an oscillating EM field) have been exhibited [27]. Moreover, it has been demonstrated that by using a highly focused laser beam it is possible to perform single qubit operations on individual ions in a chain. Such a chain is confined to a single trap and constitutes an entire qubit register [28]. To complete the universal set of gates, a design for a controlled NOT gate was put forward by Cirac and Zoller [23]. This design was realised experimentally in 2003 [29], therefore demonstrating the feasibility of meeting this criterion. The different qubits in a trapped ion QC are entangled via the use of such gates, of which there are two different major types. First are coulomb-based gates which capitalise on the fact that the ions in a trap can “feel” each other through the electrostatic Coulomb force that mediates the interaction between charged particles. Forces are applied to the ions in a trap and in analogy to a line of connected pendula, the other distinct ion qubits react in their motion - this produces what are termed motional states of the ions [30]. The second means of entangling uses photonic gates. This is an example of second-generation entanglement, whereby two or more photons are themselves entangled before being directed at ions in different traps, inducing subsequent entanglement in those ions [31, 32, 33].

Difficulties

The foremost obstacles in the way of progress in trapped ion quantum computing all essentially revolve around problems with scalability [34]. Large numbers of confined ions are required to achieve greater processing power, necessary for solving harder computational problems. Unfortunately, it is difficult to trap multiple ions in the same trap and form strings of entangled ions. For instance, it is particularly troublesome to set up the motional states of the ions in order to effect this entanglement. This is because having many ions in a single trap interacting via the Coulomb force becomes very complicated and the quantised motion (which can be thought of as units of particle-like entities called phonons) doesn’t persist for very long timescales [5]. Many proposals have been made in order to tackle this problem, such as microfabrication processes and photonic interconnects [19]. These proposals see many traps connected up together into a network so as to avoid the need for storing all the ions in a single trap. There is an issue, however, with the miniaturised ion traps produced by microfabrication as they can suffer from excessive electric field noise that causes undesireable heating at the surface of the traps, in turn inducing decoherence in the ions. This difficulty has been addressed, and the unwanted heating reduced somewhat although further improvement may potentially be necessary [19]. Decoherence of individual qubit states also poses a limiting factor on the performance of TIQCs. This manifests either in the T_1 time of the ions (the time taken for them to de-excite to their lower energy state) or in the T_2 decoherence time resulting from environmental influences. Work must be done to quicken gate operation times or to better isolate the ions [23, 35].

3.2 Superconducting Qubits

Superconducting qubits are the most widely used quantum processor. This use varies from commercial research with companies such as: IBM, Intel, and D-Wave with their quantum annealer. These will all differ preferentially but the fundamentals of their superconductive qubit will be the same in each [36, 37, 38].

As discussed in Sec. 2.4, making a qubit system on the microscopic (i.e spin state of an atom) scale is fairly easier. The challenge is then to make this an object than can be used in computation, and information processing much like a classical computer. What a superconducting qubit does is emulate an atom on a macroscopic level, via electrical circuits and a device called a Josephson junction [39].

Let us start with a circuit consisting of a parallel configuration of a inductor and a capacitor which are made from superconductors. Different conductors are used with different material properties. Superconductivity is a phenomenon where the circuit has no resistance, meaning that the circuit doesn't heat up like in normal conductors and no energy is lost.

The Hamiltonian is an equation that describes the energy of the system, where classically it would just be the energy equation. Below Eq. (1) is the Hamiltonian of the superconducting circuit system which is dependent on electrical components. Specifically the charging energy of a capacitor being the first term, and the flux energy across an inductor being the second term. This has the same form as that of a quantum harmonic oscillator shown by Eq. (2). The first term being kinetic energy and the second term potential energy.

$$H = \frac{Q^2}{2C} + \frac{\Phi^2}{2L} \tag{1}$$

$$H = \frac{p^2}{2m} + \frac{kx^2}{2} \tag{2}$$

The circuit will have distinct energy levels like a harmonic oscillator, with an energy difference between its ground state energy and the first state. This energy difference is equivalent to a frequency f (Hz), which is of the microwave spectrum chosen by design of the system which is roughly 10 GHz.

$$f_{01} = \frac{1}{\sqrt{LC}}$$

The frequency is also equivalent to a temperature roughly 0.5 K. This temperature is the energy required to excite the system to its first excited state, kept below this temperature the system will stay in its ground state. This temperature is achieved by placing the circuit in dilution refrigerators, keeping its temperature at around 10 mK. When needed the system can be excited with a microwave pulse in the circuit. This is called a gate voltage.

The superconducting circuit like the harmonic oscillator has linear energy levels. The energy difference between each ascending state is the same. When trying to create a superposition between the first states, energy can leak into other states as they have the same energy difference. Atomic energy levels which has discrete differences. The distinct energy differences prevent leakage and create a well-defined qubit. For the circuit to become a qubit it system it must have discrete energy levels. The Hamiltonian needs to be altered so that there is a non-linear difference between levels. This is achieved by changing the flux dependence on the current [41].

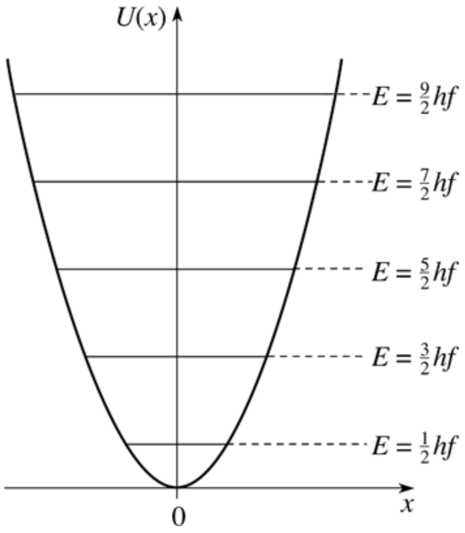


Figure 3: A harmonic potential well [40].

Flux, ϕ, is the rate of volts travelling through a circuit component, given by an integral of voltage over time. Eq. (3) is the linear dependence of the flux on the current for an inductor.

$$I = \frac{\phi}{L} \tag{3}$$

For the non-linear energy levels to be achieved the inductor is replaced by a Josephson Junction, consisting of two superconducting wires which sandwich an insulator. Below is the flux dependence of the current of a Josephson Junction.

The Josephson Juction now changes our Hamiltonian, so that it no longer resembles a harmonic oscillator with linear energy gaps. It now takes the form of a cosine, which has a definite maximums instead of continuous levels like the oscillator (see Fig. 3).

$$L_j = \frac{\Phi_0}{2\pi I_c \cos\phi_0} = \frac{L_j}{\cos\phi_0}$$

This changes the spacing between energy levels making them non-linear. Now when excited between the ground and first excited state it will form a superposition of those two states, without leakage into other states.

To understand the Josephson Junction a brief description of superconductivity and current is required. A current flowing through a conductor is the flow of negatively charged electrons through the circuit, in a superconducting current the electrons travel in pairs. These pairs are called Cooper pairs, this pairing is a quantum phenomenon but can be compared to a classical analogy by considering the lattice structure of metals. Delocalised electrons can move freely in the lattice structure of positively charged ions. Electrons mutual negative charge repel each other, while the positive charge of ions attracts the electrons. At low temperatures the attraction between delocalised electrons and ions displace the ions which increases the positive charge density in the local vicinity. The change in charge density attracts other electrons, creating a Cooper pair [42]. Quantum mechanically this is due electron-phonon interactions within the lattice but this is not necessary to delve upon.

Now with an understanding of superconductivity, a Josephson Junction as discussed previously is two superconductors (aluminum) sandwiching an insulator (aluminum-oxide) [43]. A Josephson Junction is a macroscopic example of a quantum phenomenon. Cooper pairs in the superconductors can quantum tunnel through the insulator, known as a super-current. The frequency of this tunnelling is equivalent to the Josephson energy E_j ($E = h\omega$).

The Hamiltonian of the circuit has changed with the introduction of the Josephson Junction and removal of the inductor, the flux energy term in the Hamiltonian is replaced with the Josephson energy.

$$H = \frac{Q^2}{2C} - E_j \cos \frac{2\pi\Phi}{\Phi_0} \tag{4}$$

$$\hat{H} = 4E_c(\hat{n} - n_g)^2 - E_j \cos \hat{\phi}$$

Eq. (4) can be put in terms of charge carries and E_c (energy of capacitor) and E_j. The qubit is then initialised via gates by applying a microwave voltage through the circuit, this is given by the gate charge or the number of charge carries n.

The Circuit will have electrons at the surface that will attract charged molecules to its surface which act as an external voltage. This acts as a false gate, or a gate error. This was a huge source of error and decoherence for the original charge qubit described above.

Currently the staple Superconducting qubit system is the Transmon regime which made the charge qubit obsolete.This was done by decreasing the capacitance energy, by increasing the surface area of the capacitor. This was done by adding teeth in the capacitor. By decreasing the capacitance energy the small unwanted variations in gate charges from external sources had next to negligible effect, making the Transmon qubit incredibly useful. This led to a side effect of a reduction of the anharmonicity of the system, which is essential for the qubit to work. This is expanded upon in the difficulties section below [44].

To read information off of our qubit systems Cavity Quantum Electrodynamics (QED) is used. A device called a Fabry-Perot resonator is used, which is essentially two imperfect mirrors facing each other to form a cavity. Light will transmit through the cavity if the wavelength of light is a multiple of the size of the cavity. The cavity has an electric field inversely proportional to its size, which is usually equal to the wavelength it transmits.

A cavity can be made in the circuit, which is called circuit QED. This is constrained in one dimension, the zero point electric field of the cavity can couple with that of the qubit through its large dipole moment (as it can be seen as a large artificial atom). Now with this set up a microwave voltage can be applied along the cavity opening which will flip the qubit state. Shining a photon of wavelength equivalent to that of the cavity size infers the state of the qubit by the phase difference of photons that pass through the cavity [45]. These are the fundamentals of how the qubit state is controlled and information is read from it when required.

More than one qubit can be added to the same cavity which can have unique excitation energies designed by the experimentalist so each can be controlled separately. While the photon which can infer to the user, the state of one can now tell you that of the whole system.

Difficulties

Progress in this method has been promising and this is reflected in the fact that most of the known companies prefer this technology, as stated at the start of this section, as their choice of building a quantum processor. Much of the current research is done as to allow the superconducting circuit bypass problems with the 3D geometry of the qubits. These current problems are decoherence and cross-talk that is happening between the qubits. This difficulty should be omitted if ground planes compromising the physical qubits are aligned together [46]. The circuits used in a superconducting systems operate at a few mK for systems with size of the order of 10^2. Dilution refrigeration technology is extensively used in order to keep the temperature of the system low and constant [19]. Research into room temperature superconductors may help relieve this problem [47].

Continuing from the previous section. With the decrease in capacitance energy the system starts to become more harmonic, which by definition is not a qubit. This harmonicity leads to leakage of the gate voltages, called an error per gate. Minimising this error per gate by altering gate times is a highly active field of research in physics [44].

3.3 Spin-Orbit Qubits via Quantum Dots

A Spin-Orbit qubit utilises the simple quantum system of the spin state of a single electron. A Quantum Dot is used to isolate a single electron on its own and from the environment, whilst being able to be interacted with via electrode gates.

To begin Quantum Dots are semiconductors, commonly GaAs (Gallium Arsenide) or Si (Silicon). The dot is made from enclosing a very small region of space on the micrometre scale with the semiconductor, which is filled with an electron gas. The “cage” has two gate electrodes in which current can be passed through, fine tuning the current which isolates a single electron in the Dot. This specific type of quantum dot is called a lateral quantum dot, there are many types of quantum dots but for qubits this structure type is used most commonly [48].

The analogy of an artificial atom can also be applied to the quantum dot system as it was with the superconducting circuit in Sec. 3.2. The quantum dot is effectively a potential well that confines the electron within, produced by the electrodes. Like the SCQ the system has energy levels analogous to the atomic model. Adding More Dots near each other causes a wavefunction overlap, comparable to atoms forming molecules.

What makes the Dot a good candidate for a qubit is being able to measure the charge (electron number) of the system externally, by measuring the inductance of the dot. The electron within can also have a spin state, like in an atom it can also be split with a large magnetic field. This splitting is called Zeeman splitting. Now with the splitting of the spin states into their own energy levels, the qubit system can be measured and manipulated via the electrode gates [49].

With the combination of charge detection and the Zeeman splitting of the spin states, the qubit can be activated and information can be read out. Zeeman splitting lowers the energy of one of the states while the other increases. By applying voltages to the gates of the dot the two spin states can be tuned such that the spin up state is lower than the fermi sea energy level of the semiconductor while spin down state is above(the fermi sea energy level is the minimum energy of the ’sea’ of electrons in the semi-conductor). This makes it energetically favourable for an electron to transition to the spin up state from the fermi sea. With an electron in the spin up state, it can be excited with a gate voltage and the qubit system will be initialised. There will be a superposition of the spin up and spin down state of the electron.

After oscillations of the spin states, the final state needs to be determined without prematurely collapsing the system. To detect its final spin state, spin to charge conversion is used. This is done by having the Zeeman split energy levels sit as they were for initialisation, spin up below the fermi energy while spin down above. If the system is in spin down state it will be energetically favourable to travel into the fermi sea, causing a change in charge from $-q$ to 0. If in spin up there will be no change. The charge value infers the final state of the system, therefore allowing the user to read information of the qubit.

Now the next challenge is control the spin state. This is done by a technique called Electron Dipole Spin resonance (EDSR). EDSR controls the spin state of an electron by spin orbit coupling of an electric field. The electric field is created by applying small voltages at the electrodes, producing an effective magnetic field. The magnetic field couples to the electron spin, and can rotate the spin state with manipulation. In qubits its desirable to be able to change spin states multiple times before decoherence [50, 51].

While these Qubit system seems quite pure, theyfaces many decoherence sources: Electron-phonon coupling, Hyperfine interactions, charge dephasing and spin-orbit interactions. Some of these issues are expanded upon in the difficulties section below. On going research is trying to reduce these sources of error by trying different materials to make the quantum dot out of, and even structural design. For instance, using Graphene as the semiconductor [52].

Difficulties

The Quantum Dots technology is limited by the control mechanism of the qubits [53]. Many physical qubits have to be encoded such that a logical qubit may be realised. The exchange times in which the physical qubits interact have to be controlled precisely [53]. The qubits have low coherence time and the temperature of the System is low, around 4 K [54]. Since the interaction between the dots is short ranged this puts an extra constraint in using the quantum error correction codes needed for building a large scale quantum computer [54]. Many materials are yet to be tried such that the fidelity of the two-qubit gate is improved, since it is currently not up to the standard required of QC, and the materials are to be eliminated such that the best candidate is found [34]. In order to eliminate that, qubits have as low coherence as possible the donor atoms placed on the quantum dots must be positioned precisely such that the atoms are as much pure as possible. Low purity would interfere with the qubits performing actual quantum computation [34]. A future direction of this method is to eliminate the short distance interaction problem of the qubits by producing self-assembly quantum dots in which they will have the feature that their optical characteristics are different from currently produced quantum dots. Such a solution to this problem is given by fabrication and dot tuning techniques [54].

3.4 Linear Optical Quantum computer

In LOQCs, one makes use of photons of light to act as qubits. Some mode, or property, of the photons is chosen so that its value at a given moment determines whether or not the qubit is in the ON state or the OFF state. For example, it could be decided that if the photon is polarized vertically then it is in the ON state and if it is polarized horizontally, then it is the OFF state.

There are several techniques which have been developed to produce individual photons in initial reference states. One such method is called spontaneous parametric down-conversion (SPDC). This works by firing an initial, high energy photon at a non-linear crystal which, with some small probability, splits the photon up into two lower energy output photons. One of these output photons ("the idler" photon) is said to "herald" the other "signal" photon's presence as if we observe the production of the idler, we can deduce from energy conservation that the signal has also been produced. The only issue with such a process is that, due to its probabilistic nature, the outputted photons are not produced very rapidly. This is a bottleneck as for efficient computing, large numbers of initialised photons are required on demand [55, 56].

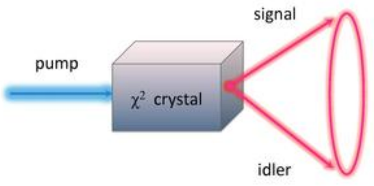


Figure 4: Schematic of SPD using a non-linear crystal [57].

Measurements are performed in LOQCs via the use of single-photon detectors. A specific example of such a detector is a superconducting nanowire single-photon detector (SNSPD). A SNSPD consists of a square array of superconducting nanowires which are held at a temperature below which they go superconducting. Furthermore, a bias current is applied to the array which is just slightly below the superconducting critical current, I_c of the wires (if the current flowing in a superconductor is below I_c then it is in its superconducting state, otherwise it is non-superconducting). This bias current makes the SNSPD very sensitive to incoming photons which impact cooper pairs in the wire and cause the irradiated region to undergo a dip in its critical current. Consequently, the region in question becomes non-superconducting and as a result its electrical resistance takes on a non-zero value which allows one to confirm the presence of a photon via a concurrent voltage pulse [58].

Since it is photons which act as the qubits here, there should not be a problem with the photons decohering as a result of their coupling with the computer's environment - this coupling is extremely weak for photons. Let us clarify what is meant by this. Firstly, it is known that photons do not self interact (two photons which are fired directly at each other would simply pass straight the other photon) [60]. Moreover, when we talk of

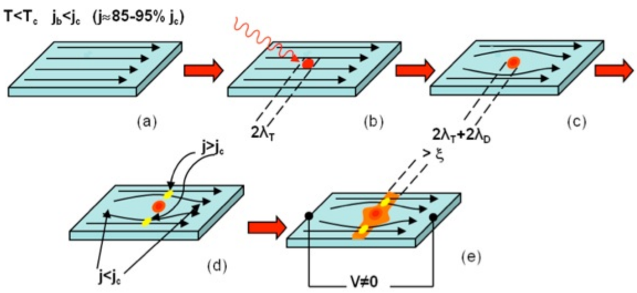

T<T_c j_b<j_c (j≈85-95% j_c)
(a)
2λT
(b)
2λT+2λD
(c)
j>jc
> ξ
j<jc
(d)
(e)
V≠0

Figure 5: Operation of a SNSPD [59].

photons' "environment", we typically mean unwanted sources of heat and other sources of electromagnetic radiation which is made up of photons. Therefore, it can be understood that photons should be resilient to decoherence resulting from this "environment". Other types of contaminants (the matter kind) can much more easily be removed as sources of interference. With this being said, there are other possible sources of decoherence which typically see photon's being lost during computation. For instance, if there are imperfections in the optical elements (beam splitters, mirrors, phase shifting elements) which make up the computer, then it is possible that some fraction of the photons don't make it to where they've supposed to [61, 62, 63].

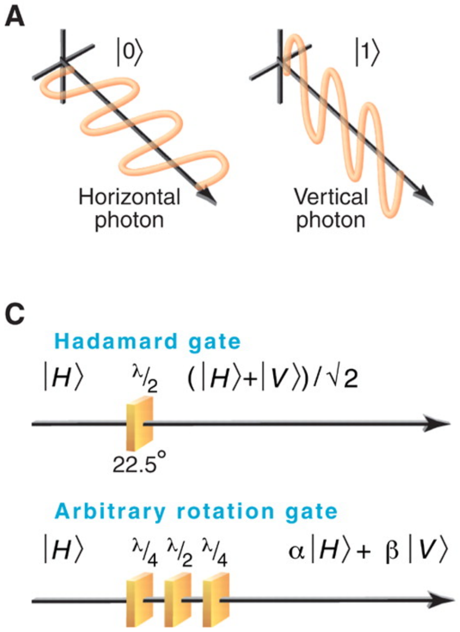


Figure 6: The 2 different polarisation states of a photonic qubit and the action of a Hadamard gate on an incident photon [64].

Manipulation of the photons state is effected by optical instruments such as beam splitters, phase shifting elements like quarter-wave plates and mirrors) [65] - these therefore constitute the quantum logic gates for this particular technology. This would ostensibly stand to be one of the benefits of this particular technology - optics is a well understood and developed area and so using optical elements as the computer's machinery should pose less difficulties and superior modularity than alternative, more convoluted QC technologies. Comparison could be made with attempts to connected up components in ion trap quantum computers - the latter proves to be a much more difficult task [66].

For an example of how single-qubit gate is implemented, consider the action of a quarter-wave plate on an initially vertically polarized wave, as shown in Fig. 6. This optical element acts like a Hadamard gate in this usage as it splits the vertically polarized (ON state) photon into a combination of vertical and horizontal components - essentially a superposition of ON and OFF states.

When it comes to two-qubit gates, the aforementioned point about the lack of photon self interactions gives rise to certain obstacles. Since it is necessary to realise two qubit logic gates in order to have universal computation, we must have some way of taking in two photons, looking at what each of their states are and determining a corresponding output. This would ordinarily be achieved by having the two qubits (photons) interact so as to "communicate" their states to the other. However, we have just noted that this is impossible. A workaround to this problem was devised by Knill, Laflamme and Milburn [65]. They described a procedure which makes use of entanglement and ancillary qubits in order to introduce an "effective interaction" between photon qubits. The only issue with this procedure is that the gates which carry it out are non-deterministic meaning that in order to achieve a sufficiently high probability of the gate functioning as desired, many entangled qubits must be used (corresponding to a great amount of resources) [60, 67, 68].

Difficulties

Complete architectures exploiting this method have not been developed and not much investment has been made in the source and detector technologies needed for developing and entangling the photons. High fidelity of multi-photon qubits has not been reached and this is important for implementing the cluster state architecture which is one of the two most promising architectures for exploiting this method. An upcoming challenge for this approach is to improve the physical models of quantum photonic components [19]. It is still to be understood what it is possible to be achieved with the current linear optical technology and the design for scaling an integrated device using this method is yet to be developed [69]. Large amount of photons are needed to achieve low error rates and this increases the complexity of the system as well as the the cost of developing it [66]. Like trapped ion quantum computers, LOQCs suffer from a scalability problem. This problem is actually more pronounced for LOQCs however. One work cites a resource dependence that can be as great as 5 orders of magnitude greater than that of a QC approach such as trapped ions. This problem stems from the point mentioned previously about photons weak self interaction. To counteract this, a scheme involving large numbers of simple optical instruments is used. Moreover, due to the noted stochasticity involved in this implementation of quantum gates, an even multitude of components is necessitated. One research group even provides calculations indicating that 10^{11} components may be required to run a LOQC for practical purposes [70].

3.5 Topological quantum computers (TQCs)

TQCs are a further suggested approach to quantum computing. Out of all the processor technologies mentioned, this type is the least developed. However, we discuss its premise briefly as it has a few unique and promising features. In these computers, qubits are

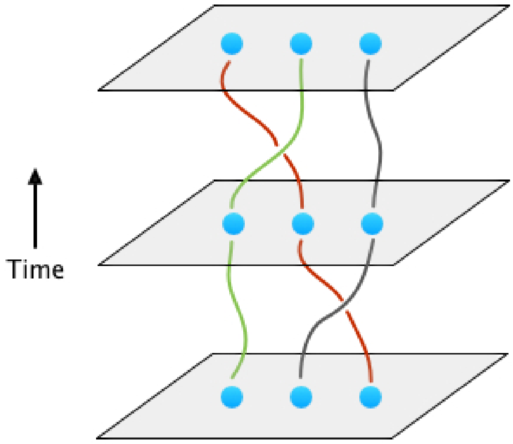


Figure 7: Image of qubit braiding [71].

realised by what are called non-abelian anyons, produced for instance when flakes of gallium arsenide are magnetised and cooled. These so-called quasiparticles are used to carry out computation by manipulating them so that they flow through spacetime and become entwined in specific ways (braided) - this is illustrated in Fig. 7. The specific braiding pattern encodes corresponding computational information and the non-abelian nature of the anyons means that the patterns are uniquely determined by the braiding order. To elaborate, let us think of the braids as analogous to a knot of wires. If anyon A is the red wire and anyon B is the blue wire then if we cross the red wire over the blue wire we achieve a different braid to crossing the blue wire over the red wire. This is what non-abelian means. The great advantage of topological QCs is the fact that, like a tangle of wires which is very hard to unknot using random pulls and tugs, a braiding of anyons is superbly resilient to outside noise and this gives rise to the possibility of long coherence times of these computers (purportedly of the order of weeks instead of microseconds) [72, 73].

Difficulties

So far topological quantum computers are still in the development stage. The existence of the crucial ingredient of non-abelian anyons have yet to be conclusively demonstrated experimentally. It is believed that this shall be achieved soon however [74]. Following this, it is planned for systems to be developed to braid the anyons, manipulate the qubits and perform measurements of the qubit states. Acknowledgement is evident in the literature regarding the engineering challenges associated with such tasks as the physical realisation of quantum gates, however [75]. It is also forecast that development of hybrids between topological and non-topological systems will be developed simultaneously with that of pure topological QCs. This should lead to swifter initial progress in the field, simultaneously incorporating the error-resistant properties of topological QCs and utilising the more developed approaches of other technologies. Finally, research is being carried out into other, perhaps more easily produced, physical systems (other than cooled and magnetised gallium arsenide) which are capable of giving rise to non-abelian anyons

[76, 77].

3.6 NMR

In an NMR quantum computer, a qubit's two logic states (on and off) correspond to two quantum mechanical spin states of the nucleus of an atom (call the states spin up and spin down respectively). These atomic spins may either be present in dissolved molecules in liquid NMR quantum computers (LNMRQCs) or exist in some crystalline lattice in solid-state NMR QCs (SSNMRQCs). As shall be discussed shortly, the former of these two approaches is generally considered to be non-viable due to scalability problems. However, the principle of operation is the same for both and so we give a general explanation now. To expand upon the point about the qubit logic states: one can imagine a classical picture where the atomic nuclei are like little spinning tops that are either spinning clockwise (which we call a spin $+\frac{1}{2}$ state) or anticlockwise (which we call a spin $-\frac{1}{2}$ state). To map our idea of a logical 0 and logical 1 from classical computing to this quantum system, we think of the spin $+\frac{1}{2}$ state as logical 0 and spin $-\frac{1}{2}$ state as logical 1 [78, 79].

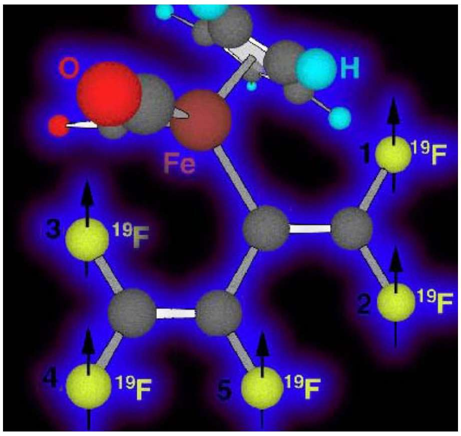


Figure 8: Diagram of one liquid molecule with 5 different nuclear spin sites. Along with many other copies of this molecule in the sample to permit averaging, this represents 5 qubits [80].

Now, how do we go about addressing these qubits as is required when we perform computations? This is where the concept of nuclear magnetic resonance is taken advantage of. When these molecules (and their composite spinning nuclei) are placed in a magnetic field, the spin $+\frac{1}{2}$ and spin $-\frac{1}{2}$ states react differently. The state which opposes the direction of the magnetic field becomes more energetic whilst the other state takes on a reduced energy state (see Fig. 8). It is found that if one pulses a signal of a precisely chosen radio frequency at the nucleus in the magnetic field, the nucleus can be coerced into switching from its low energy state to its higher energy state. And just like that, we have managed to flip a logical $|0\rangle$ (spin $+\frac{1}{2}$, or high energy state) to a logical $|1\rangle$ (spin $-\frac{1}{2}$, or low energy state). This forms the basis of NMR quantum computation [81].

The next problem is that of addressing multiple qubits at once. It is clear that we cannot have wires leading to all the individual nuclei within our sample of molecules. The solution makes use of the following facts. The exact energies of the different spin states of the atomic nuclei when placed in a magnetic field depends on the exact identity of the nucleus in question, for example if it is a hydrogen nucleus or oxygen nucleus. The energies also depend on what the neighbourhood of the nucleus within the molecule looks like. For instance, if it is at the surface of the molecule or stuck in the middle. Therefore, to make a specific nucleus perform its spin flip operation, we must fire a certain frequency of radio waves at it; for a different nucleus another different frequency of radio waves must be used. Importantly, the radio waves of one frequency (for nucleus A for instance) cannot affect a different nucleus (nucleus B). This energy dependence is leveraged so that we can indiscriminately fire pulses of all the different required radio frequencies through our sample of molecules, simultaneously addressing all the different nuclei without getting our instructions mixed up [22].

Unlike the processor types discussed previously, an NMR QC falls under the category of an ensemble quantum computer. In this case, this essentially means that instead of qubits being individual elements, a large number (for instance 10^{20}) of individual nuclear spins correspond to a single qubit. Essentially, we have a whole bunch of identical molecules (the molecules may be non-uniform themselves). Say each molecules has 3 spin sites (nuclei) in it: site A, B and C. All of the A sites throughout the whole sample (ensemble of molecules) constitute a single qubit of the ensemble. The large number of identical spin sites is used to obtain an ensemble average [82].

Difficulties

It is generally accepted that LSNMR quantum computers are not viable candidates for large scale quantum computing owing to the aforementioned difficulties in scaling them up to solve harder problems and the challenge of effectively initialising [83]. However, one slightly different take on the approach, solid state NMR quantum computing (SSNMRQC), has been put forward as a promising alternative. In SSNMRQC, instead of using molecules dissolved in some fluid solution, qubits take the form of components of some solid (for example, nitrogen vacancy centers in diamond). The same NMR techniques for qubit addressing, manipulation and readout are used except in the solid-state case, it is possible to avoid the shortcomings of LSNMR. For example, as the atoms of a solid are fixed in place, it is possible to avoid the decoherence that occurs when the molecules in a liquid diffuse throughout its volume. When this occurs, the nuclear spins present in those molecules "see" a different magnetic field (because this varies throughout the sample) as they move away from their initial position. This can mess with the state of those spins. Furthermore, when using a solid it is possible to cool the sample down to lower temperatures which means that prevention of decoherence resulting in the breakdown of ion entanglement can be facilitated. Finally, additional control over the spins in a solid and the capability of achieving greater polarisation since the spins are more faithfully aligned in the magnetic field direction means that the problem of initialisation associated with LSNMR can be tackled [84, 85].

Although the future of solid state NMR is promising, as already stated previously, several difficulties have to be overcome to make this a potentially viable method for building a large-scale QC. The signal that can be detected in solid state NMR is exponentially inversely proportional with the number of spins that the system includes. This puts a constraint on the number of spins that can be used to build a quantum processor and is a consequence of the fact that pseudo-pure states are used to prepare the qubits [86]. Pseudo-pure states are quantum states which consist of a pure state which we want to use in our computation plus a smaller mix of other states. These pseudo-pure states are necessary in NMR as ideal initialization into pure states is impossible in such systems. Having an upper bound on the number of spins poses a scalability difficulty. Two approaches have been used to circumvent this problem. Modified algorithms that dont require pure states (as opposes to pseudo-pure states) and working with molecules that are extremely highly polarised. For the latter approach, such a polarisation cannot be currently experimentally achieved [22]. It seems that for the time being, solid state NMR hasnt stood up to the expectation of using SSNMR to advance the general method of NMR for building a QC and as a result researchers are debating whether further research would produce any useful results for the future of experimental quantum computing [79, 87].

4 Algorithms

We are now going to focus on how the Quantum Computers actually solve numerical problems using the qubits and gates provided by the quantum processor technologies. For this we are going to look at some of the known quantum algorithms that have been realised and built up until now.

There are only a few known quantum algorithms. This is because designing algorithms for quantum computers is difficult for two reasons:

1. Quantum Mechanics is not very intuitive for our minds which are better suited at processing the classical world. Since, part of new algorithm design relies on the intuition on how the algorithm works, this is difficult to achieve for quantum algorithms and thus new and innovative ways of thinking and special insights are required to develop new quantum algorithms.

2. We don't just need to develop algorithms that solve a particular problem. We need algorithms that solve problems that either have no known classical algorithm that solves them or if there is a known classical algorithm, we need the quantum algorithm to be more efficient than the classical counterpart.

There are two main models of Quantum Computation that we are going to focus on:- The Universal Gate/Quantum Circuit model and the Quantum Annealing Model. There are other models of quantum computation that have been proposed but they are essentially equivalent to the Quantum Circuit Model. That is, in the sense that they require the same resources to solve the same problems. For example, the Quantum Turing Model of computation which is a quantum generalization of the Turing Model of classical computation has been shown to be equivalent to the model based on quantum systems [88].

4.1 Quantum Circuit Model

We now begin by looking at the Quantum Circuit Model for Quantum Computing. There are five key features of this model:

1. A quantum computer in practice has classical part as well. In principle, it is possible for classical computations to be performed by a quantum computer but it is usually more convenient and efficient to do some calculations on a classical computer. For example, many schemes for quantum error correction involve classical computation for increased efficiency.

2. A quantum circuit acts on a n qbit system. This system belongs in a state space of 2^n-dimensional complex Hilbert Space. The product space forms the computational basis states and are of the form $|x_1, x_2, \ldots, x_n\rangle$ where $x_i = 0, 1$. This is represented by the state $|x\rangle$, where x is a number with binary representation $x_1 \ldots x_n$.

3. This is the assumption that it takes at most n steps to prepare any state $|x_1, x_2, \ldots, x_n\rangle$. The state $|x_1, x_2, \ldots, x_n\rangle$ is essentially a tensor product of the states of all the qbits in the system.

$$|x_1, x_2, \ldots, x_n\rangle = |x_1\rangle \otimes |x_2\rangle \cdots \otimes |x_n\rangle$$

4. Quantum Gates can be performed to any subset of qbits as is desired. They are explained in Sec. 2.5.

5. Measurement in computational basis can be performed on any number of qbits. Generally Measurement destroys the quantum information and replaces it with classical information and is irreversible.

Frequently used quantum gates and circuit symbols are provided in Appendix A.

4.1.1 Algorithms for Circuit Model

There are three major classes of algorithms for the Quantum Circuit Model:- Shor's Quantum Fourier Transform, Grover's Quantum Search Algorithm and Quantum Simulation of physical systems. The ability of quantum algorithms to outperform classical algorithms comes from three main properties of quantum systems:-

1. **Superposition:** Since qbits can exist in a state of superposition of states as described in Sec. 2.1. Thus, when a transformation is applied to a state, it is simultaneously applied to all the states in the superposition. This is known as Quantum Parallelism [89]. This is a feature of many algorithms especially the class of Shor's Quantum Fourier Transform. The qbits can be prepared in a superposition by using the Hadamard transform (H) and then the function can be applied to all the possible states.

   However, this is not immediately useful since in a way, the information is hidden because when we make a measurement, the superposition collapses to one of the states. Thus to retrieve useful information from the superimposed states, we have to find some clever ways to manipulate the state to get the desired result, or in cases where it cannot be done, we can we can make multiple similar states and measure them forming a statistical distribution.

2. **Entanglement:** This property of quantum systems as described in Sec. 2.2 is useful in applications like quantum teleportation and quantum error correction as well as in quantum communication [90].

3. **Probability Amplitudes:** The third way quantum algorithms have an edge over the classical ones is that complex numbers describing a quantum system grows exponentially unlike classical systems that grow linearly. This power up is immediately useful when trying to simulate quantum physical systems. Since, for a system of n particles, if we were to simulate it classically, we would need to keep track of c^n complex numbers describing the system. But, when simulating the system on a quantum computer, we just need n qubits and their interactions keep track of the exponential complex numbers describing the system. Although we can evolve the system in a quantum computer, we need to find clever ways to extract the information hidden in the states as it is not directly available to us.

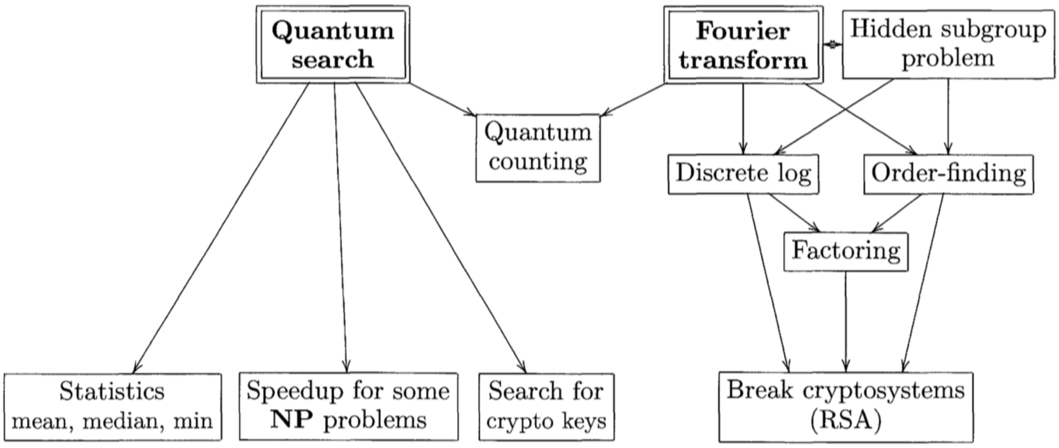


Figure 9: Main Quantum Algorithms and their relationships along with notable applications [5, p. 173].

4.1.2 Quantum Simulation

We now look at the quantum algorithm for simulating physical quantum systems on a quantum computer. At the heart of simulation is the solution to differential equations that capture the physical paws that govern the dynamics of a system, for example Newton's equation and Poisson's equation. For quantum systems, the dynamics is governed by the Schrodinger equation

$$i\hbar\frac{d}{dt}\left|\psi\right\rangle = H\left|\psi\right\rangle$$

Where, H is the Hamiltonian according to which the system evolves. Simulating quantum systems on a classical computer is possible but often very inefficient. The main problem with simulating quantum systems is that the number of differential that needed to be solved grows exponentially with the number of particles in the system being simulated. Sometimes, some approximations might help reduce the number of equations to be solved, but there are many problems for which no such approximations are known like the Hubbard Model [91] or the Ising Model [92]. Quantum Computers can efficiently simulate quantum systems for which there is no known efficient classical simulation [93].

We start by looking at problem where H is time independent, in which case the differential equation to be solved is

$$\left|\psi(t)\right\rangle = e^{-iHt}\left|\psi(0)\right\rangle$$

(Refer to Appendix C)

Most simple Hamiltonians can be approximated using quantum gates. For more complicated Hamiltonians, they can be simplified using Trotter Formula[94]. The algorithm for quantum simulation then includes choosing a starting quantum state and updating the state for small time intervals by applying the time evolution operator and iterating the step until we get the desired result. An example of Hamiltonians being approximated using quantum gates are given in Appendix-D.

At each iteration of the algorithm, a new quantum state is formed and the old one is destroyed. Thus, many physically interesting problems can be simulated in this way like the Hubbard and the Ising model, also problems involving global symmetries from particle statistics(indistinguishable particles) [95]. Quantum simulation can be used to understand a lot of interesting physical systems like in chemistry, where quantum simulation will make simulation and study of molecules much easily accessible.

4.1.3 Shor's Quantum Fourier Transform

Now we look at another important class of quantum algorithms that depend on fast quantum Fourier transform. A quantum algorithm for Fourier Transform acts as a major ingredient in developing many other useful algorithms for tasks like factoring, discreet logarithm etc..

A useful method of solving problems in mathematics and computer science is to first transform them into another problem for which the solution is known. An amazing achievement of Quantum Algorithms is that it makes some of those transforms much faster to compute compared to classical algorithms. One of these transformations is the discreet Fourier Transform. In a mathematical sense, a discreet Fourier transform takes a vector of complex numbers $x_0, x_1, ..., x_{N-1}$ and transforms them into $y_1, y_2, ..., y_{N-1}$ where the transformation is given by

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi ijk/N}$$

The quantum Fourier Transform is essentially the same transformation with a slightly different notation. It acts on an orthonormal basis $|0\rangle, ..., |N-1\rangle$ and the transformation is defined by

$$|k\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi ijk/N} |j\rangle$$

Thus an arbitrary state is transformed as

$$\sum_{j=0}^{N-1} x_j |j\rangle \longrightarrow \sum_{jk0}^{N-1} y_k |k\rangle$$

This transform is defined by a Unitary transformation and thus can be efficiently implemented on a quantum computer [96, 97]. The quantum circuit for Fourier Transform is given in Appendix B.1.

This circuit performs the QFT using $\mathcal{O}(n^2)$ number of gates, whereas the best known classical algorithm,like Fast Fourier Transform, for performing the discreet Fourier Transform uses $\mathcal{O}(n2^n)$ number of gates. Thus, the quantum algorithm provides an exponential speed up over the classical algorithm. But, unfortunately, quantum computation cannot be directly used to speed up classical Fourier transforms as the amplitudes of the transformed states cannot be accesses directly using measurement. Thus, to be able to use the speedup provided by the quantum algorithm for Fourier transformation, we need a more clever way to exploit it. It turns out that the QFT algorithm can be used to perform a general procedure called Phase estimation [98] which in turn is an important part of many useful quantum algorithms. Phase estimation allows us to estimate the value of φ for a Unitary operator U with eigenvector $|u\rangle$ and eigenvalue $e^{2\pi i\varphi}$. Phase estimation process utilizes two registers. The first register contains t qbits in state $|0\rangle$ and the second register encodes the state $|u\rangle$ The process takes place in two parts. The first part uses unitary quantum gates to produce the state

$$\left(\frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1} e^{2\pi i\varphi k}|k\rangle\right)\otimes|u\rangle$$

The second part of the algorithm includes performing an inverse Fourier transform on the first register which gives the state

$$\frac{1}{2^{t/2}}\sum_{j=0}^{2^t-1} e^{2\pi i\varphi j}|j\rangle|u\rangle \rightarrow |\widetilde{\varphi}\rangle|u\rangle \tag{5}$$

And now, the first registered can be measured to give a good estimator of φ. This algorithm produces the value of φ [98]. The circuits for the two parts of phase estimation are given in Appendix B.2. Phase Estimation can be used to solve other problems that can be reduced to the problem of Phase Estimation. We look at two of those problems; Order-Finding and Factoring.

1. Order Finding: For positive integers x and N, $x < N$, with no common factors, the order of x modulo N is defined to be the least positive integer, r, such that $x^r = 1(modN)$. The problem of order finding is to find the order for some specified x and N. This is a hard problem since no classical algorithm is known that can solve this using resources polynomial in $L \equiv \log N$. It turns out that the quantum algorithm for order finding is just phase estimation applied to the operator [97, 99].

$$U|y\rangle \equiv |xy(modN)\rangle \tag{6}$$

It can be shown that the eigenstates for this operator are

$$|u_s\rangle \equiv \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} exp[\frac{-2\pi isk}{r}]|x^k modN\rangle$$

and the corresponding eigenvalues are $exp[\frac{2\pi is}{r}]$. Modular exponentiation is used to implement the controlled-U^{2^j} operation for any integer j. Now, preparing the state $|u_s\rangle$ requires the knowledge of r which is what we want to find. We can circumvent this problem by preparing a superposition of the eigenstates for the operator. Now, it can be shown that

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = |1\rangle$$

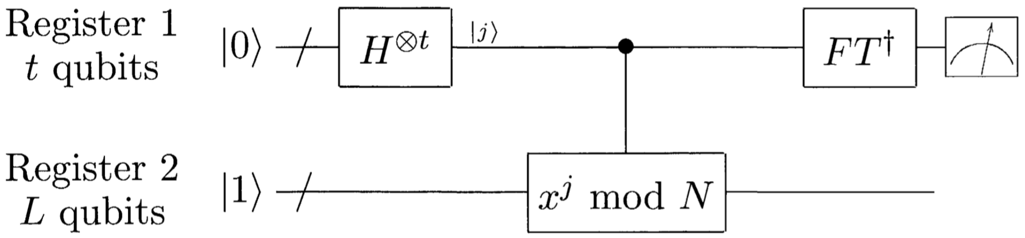


Figure 10: The quantum circuit diagram for the order finding algorithm. This circuit can also be used for factoring. $FT^\dagger$ stands for inverse Fourier Transformation [97].

Thus, we only need to prepare the second register in the state $|1\rangle$. Now, we can apply the phase estimation procedure and if we use t $= 2L + 1 + [log(1 + \frac{1}{2\epsilon})]$ for the first register, we can obtain the estimate for the phase $\varphi \approx \frac{s}{r}$. The circuit diagram for the algorithm is given in the Fig. 10. we can not obtain the desired answer,r, from $\varphi \approx \frac{s}{r}$ using the continued fractions algorithm [100, Chap 10], which produces a fraction closest to φ [5, p. 230].

2. Factoring: The problem of factoring can be stated as- given a composite integer N, what prime numbers when multiplied together equal it. This problem is of great interest from a practical standpoint as efficient algorithms for order-finding and factoring can be used to break the RSA public-key cryptosystem[101]. The most efficient classical algorithm for factoring is number field sieve[102] and it is exponentially less efficient than quantum analogue. It turns out that a fast algorithm for order finding can be turned into a fast algorithm for factoring. There are two theorems in Number theory on which this algorithm relies on[103]. They are stated below:

Theorem 1 *Suppose N is an L bit composite number, and x is a non-trivial solution to the equation $x^2 = 1(modN)$ in the range $1 \leq x \leq N$, that is, neither $x = 1(modN)$ nor $x = N-1 = -1(modN)$. Then at least one of gcd(x-1,N) and gcd(x+1,N) is a non-trivial factor of N that can be computed using $O(L^3)$ operations.*

Theorem 2 *Suppose $N = p_1^{\alpha_1}.....p_m^{\alpha_m}$ is the prime factorization of an odd composite positive integer. Let x be an integer chosen uniformly at random, subject to the requirements that $1 \leq x \leq N-1$ and x is co-prime to N. Let r be the order of x modulo N. Then*

$$p(r\ is\ even\ and\ x^{r/e} \neq -1(\mod N)) \geq 1 - \frac{1}{2^m}$$

The algorithm for factoring is summarised below'[5, p. 233]'-

Inputs: A composite number N

Outputs: A non trivial factor of N

Procedure:

1. If N is even, return the factor 2.

2. Determine whether $N = a^b$ for integers $a \geq b$ and $b \geq 2$, and if so return the factor a.
3. Randomly choose x in the range 1 to N-1. if gcd(x,N) > 1 then return the factor gcd(x,N)
4. Use the order finding subroutine to find the order r of x modulo N.
5. If r is even and $x^{r/2} \neq$ -1(mod N) then compute gcd($x^{r/2} - 1$,N) and gcd($x^{r/2} - 1$,N), and test to see if one of these is a non trivial factor, returning the factor if so. Otherwise, the algorithm fails.

Hidden Subgroup Problem: The hidden subgroup problem [104, 98] is a general problem in group theory in mathematics. This set of problems includes all the known 'exponentially fast' applications of quantum Fourier Transform. Some of the examples of this type of the problem are - period finding [105, 106], discreet logarithm, Deutsch-Josza oracle [107].

4.1.4 Grover's Quantum Search Algorithm

The quantum search algorithm works by searching a space of elements and looking for a solution to the search problem [108, 109]. The quantum search algorithm provides a quadratic speedup over the classical search algorithm. The Grover search algorithm is the most optimal possible quantum search algorithm and the quadratic speedup provided by it is the best that can be achieved using quantum computing [110].

The working of the algorithm can be visualised as a rotation in a two-dimensional space spanned by the starting vector $|\Psi\rangle$ and the state formed by a uniform superposition of the solutions to the problem. Where, $|\Psi\rangle = \frac{1}{N^{1/2}} \sum_{x=0}^{N-1} |x\rangle$. The algorithm works by applying the Grover Iteration(G) repeatedly on the initial state, that rotates the state closer to the state $|\beta\rangle$ which is a superposition of the states which are a solution to the search problem. The angle of rotation by each iteration is θ given by

$$\cos\theta/2 = \sqrt{(N-M)/N} \tag{7}$$

where, N is the number of items to be searched and M is the number of solutions to the search problem. Thus, each application of the Grover iteration(G) rotates the state by angle θ[111] and rotates it closer to the state $|\beta\rangle$ and then a measurement in the computational basis, produces with a high probability, one of the states encoded in $|\beta\rangle$, that is, a solution to the search problem. $\mathcal{O}(\sqrt{N/M})$ iterations of G must be applied to obtain a solution with a high probability which is a quadratic improvement over the classical $\mathcal{O}(N/M)$ operations . The Grover iteration is a unitary transform G that can be applied using quantum gates and is given in B.3. The action of G as a rotation is given in Fig. 11. Where the states $|\alpha\rangle$ and $|\beta\rangle$ are

$$|\alpha\rangle \equiv \frac{1}{\sqrt{(N-M)}} \sum_x {}'' |x\rangle \tag{8}$$

$$|\beta\rangle \equiv \frac{1}{\sqrt(M)} \sum_x^{\prime} |x\rangle \qquad (9)$$

Here, $\sum_x^{\prime}$ indicates sum over all the states that are solutions to the search problem and $\sum_x{}''$ indicates sum over all states that are not solutions to the problem. This algorithm has one drawback that we need to know the number of solutions to the problem to know how many iterations need to be applied to get a solution with a high probability. This, can be overcome by using one of the applications of the quantum search algorithm-Quantum Counting.

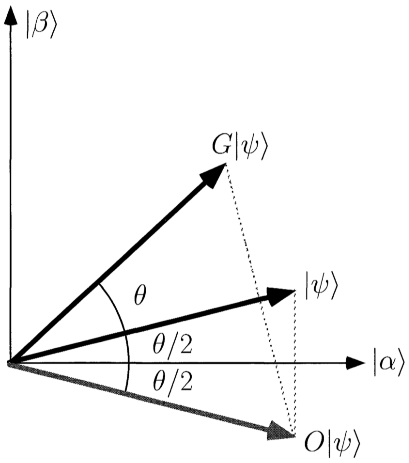


Figure 11: The rotating action of Grover iteration G on a state. The states $|\alpha\rangle$ and $|\beta\rangle$ are given by Eq. (8) and Eq. (9)

Quantum Counting: Quantum Counting is an application that combines Grover's Algorithm and phase estimation. It works by estimating the eigenvalues og the Grover Iteration G, which gives us the number of solutions M to the search problem. If $|a\rangle$ and $|b\rangle$ are two eigenvectors of the Grover iteration and θ is the angle of rotation, then it can be seen that $e^{i\theta}$ and $e^{i(2\pi-\theta)}$ are the corresponding two eigenvalues. Then, once we use phase estimation to estimate the value of θ, we can estimate the number of solutions, M, using the equation

$$\sin^2 \theta/2 = \frac{M}{2N}$$

which follows from the equation-7. This technique can also be used to find the number of solutions to a search problem, which then allows us to use the Grover's routine to find the solutions thus overcoming the drawback of Grover's algorithm. Quantum computing also has applications in solving NP-complete problems, which may be phrased in terms of the existence of a solution to a search problem.

4.2 Quantum Annealing

Now we turn out attention from the Quantum Circuit model of Quantum computation and turn to the Quantum Annealing model. It is not a universal use model unlike its Quantum Gate counterpart. It can be be used to solve a specific set of optimization problems. It is an example of a meta heuristic for finding the global minimum of a given objective function. We start with a little background on simulated annealing which inspired the simulated Quantum Annealing algorithm which in turn inspired the Quantum Annealing model of Quantum Computation.

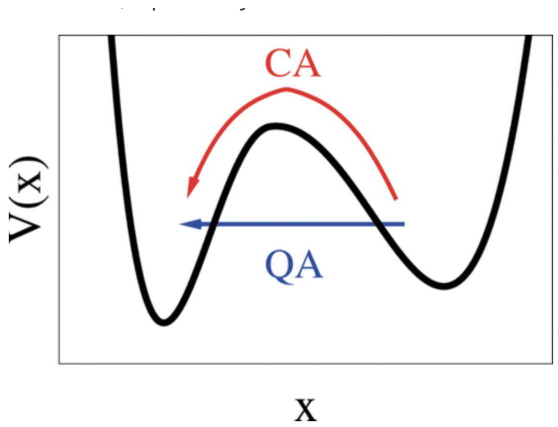


Figure 12: The comparison of QA and a classical algorithm like SA. SA needs to jump over the cost function, whereas QA can just tunnel through using Quantum Tunneling [112].

Simulated Annealing(SA)[113] is an example of a heuristic algorithm, i.e. an algorithm that is capable of finding solutions quickly on many types of inputs. It is based on an experimental technique known as annealing [113] whose purpose is to find the lowest energy equilibrium state of a system in low temperature limit. The algorithm is based on this property of annealing which resembles the behaviour of a optimization problem. The algorithm finds the minimum value of a variable(energy) given fluctuations in other variable(temperature).

Quantum Annealing [114] is also a heuristic algorithm inspired by SA but instead of using thermal fluctuations, it uses quantum field fluctuations and quantum tunneling to move through the landscape associated with the cost function associated with the optimization problem. A diagrammatic comparison of the two processes is shown is Fig. 12. The Hamiltonian used for QA can be written as

$$H = H_F + \Gamma(t) H_D \tag{10}$$

Where, H_F encodes the function to be optimised, H_D is a Hamiltonian that introduces an external transverse field and Γ is the transverse field coefficient used to control the intensity of the external field [115]. The process of QA involves evolving a system according to the Hamiltonian given in Eq. (10) and if the system evolves slowly, it will settle in a ground state which corresponds to the optimal value of the function encoded in H_F.

Simulated Quantum Annealing (SQA) is a classical algorithm to implement the techniques of QA [117]. It uses the software run on classical hardware to simulate quantum mechanics using Quantum Monte Carlo Methods [112]. Simulating quantum phenomenon

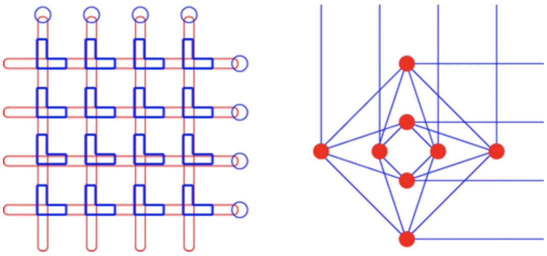


Figure 13: The physical layout of qbits(right) and their corresponding graphical representation(left).The red dots represent qbits and blue lines are couplers [116].

on classical machines utilizes a lot of resources making these algorithms inefficient [118]. In contrast, it has been shown that quantum hardware can efficiently simulate quantum phenomenon like tunneling [119]. This is the idea behind the Quantum Annealing Model of Quantum Computing. A quantum computer based upon quantum annealing uses a quantum processing unit (QPU) which contains qbits that interact and behave like quantum systems and thus exhibit properties like tunneling and superposition. These properties are exploited to find low energy states that correspond to low-cost solutions to optimisation problems. One of the drawbacks is that to be able to solve a problem, it first needs to be converted to match the QPU's architecture so it can be mapped onto the qbits. This means that the set of problems that cannot be converted to a certain model cannot be solved by the corresponding QPU. D-Wave is one company that produces Quantum Computers based on this technology and their QPU's implement an Ising spin glass model [116]. Converting to an Ising model is done through techniques of NP-completeness theory [120]. An example of physical layout of qbits is shown in Fig. 13.

In D-Wave systems, the quantum system of qbits is evolved according to the Hamiltonian

$$H(t) = A(\tau)H_1 + B(\tau)H_p$$

where, H_1 encodes the initial conditions and H_p is the problem hamiltonian of the form described in Eq. (10) and $\tau = t/t_a(t_a$ is the annealing time). $A(\tau)$ and $B(\tau)$ are defined such that at $\tau = 0$, H_1 is dominant over H_p and as the process of annealing proceeds, influence of H_1 fades away while that of H_p increases. At the end of the process, qbits have states which corresponds to the lowest energy of the problem Hamiltonian. Thus, the qbits values are read, providing the solution to the problem.

5 Applications

Due to the hardware limitation of the current quantum technologies, there are still not many real world uses of quantum computing and most of its applications require the hybrid classical-quantum algorithm to be put in practise. Nonetheless, the development of quantum computing is still in its early stage, compared to that of classical devices. The emergence of this field is due to the known Moore's law reaching its limit as the current size of transistor reaching the size of atom [121]. In the long run, quantum computing has a high chance in leading the technology development of our world, surpassing the classical computing. Most of the world leading companies such as IBM, Google, NASA, Microsoft and many more have already started building their own quantum computing team and work on researching the capabilities of this exciting field [122].

5.1 Discovery of the quantum advantage with constant depth circuits.

Many theories regarding quantum computing have been proposed and one of them proved that quantum computers could provide a computational advantage over the classical computers. This work of S. Bravyi, D. Gosset and R. Konig revealed that quantum circuits with a constant depth can easily outperform the classical circuits that is subjected to the same constraint. In this context, the depth represents the number of computational operation performed by the computer and each of the operations applied to the qubits will take some time. Since today's qubits have small error rate and can only exist within the coherence time, this results in the consideration of depth limit.

The most interesting fact in this exertion is that the depth of quantum circuits remains constant even with an increasing number of input qubits. This does not apply for classical circuits as its depth grows larger when the input of classical bits increases. The process of increasing the number of input bits plays a crucial role in improving the circuit as the potential computational power doubles through entanglement each time a qubit is added [123]. The team found certain computational algorithms that can be used by an appropriate fixed shallow-depth quantum circuit. One of them is known as the Beinstein-Vazirani algorithm where this algorithm has lots of potential implementations such as attacking the block cipher and also determining an unknown homomorphism [124, 125].

The IBM Q team is currently working on showing the examples of this advantage through their open-source quantum computing software development framework which is known as Qiskit [126].

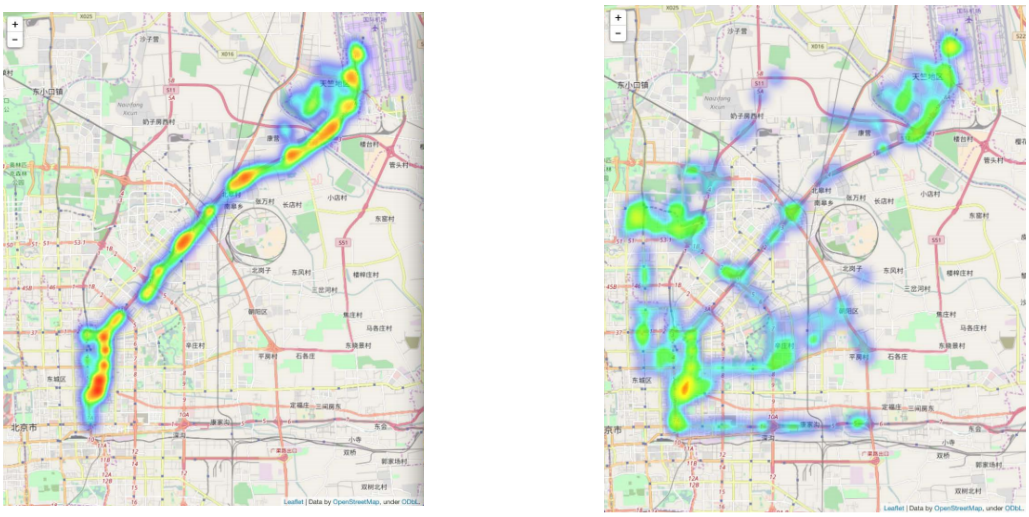
5.2 Optimisation

5.2.1 Traffic flow optimisation by Volkswagen

One of the current actual examples of problems being solved more efficiently than classical computers is the traffic flow optimisation by Volkswagen, a well-known German automaker. With the D-Wave Systems quantum processing units (QPUs) running side-by-side with the classical ones, Volkswagen developed a cloud platform that could predict the traffic outcomes up to an hour in advance and it was tested in Beijing with approximately 10,000 taxis. This quantum annealing technologies are designed to solve the quadratic unconstrained binary optimisation (QUBO) problems, where QUBO is a type of mathematical optimisation problem that maximizes a quadratic objective function. What the platform actually does behind the scene is minimising the time for the cars travelling between their individual initial locations and destinations. QUBO can be expressed generally as

$$Obj(x, Q) = x^T \cdot Q \cdot x$$

where x is the a vector of n binary variables (0 or 1) and Q is the symmetric n by n matrix. With classical computing, the platform first pre-processes the map and GPS data and identifies the regions where traffic congestion occurs. The possible valid alternative routes for every car are then determined temporally and spatially. The quantum computing process comes in after the platform has already constructed the traffic flow optimisation in the form of QUBO in order to find the solution that minimises the traffic congestion among route allocations in the whole traffic graph. The route assignment for every car are then revamped according to the results obtained and these processes are iterated until zero traffic congestion is confirmed [127].



(a) Unoptimised traffic

(b) Optimised traffic

Figure 14: Traffic heatmap analysis in Beijing to study the performance of the optimisation [128].

Following this event, Volkswagen and D-Wave Systems are currently partnering with a telco company, Orange and also a Swiss data analytic startup, Teralytics to create a traffic management system around Barcelona. With Orange providing the raw data obtained from their users anonymously in the area of Barcelona, Teralytics enhances the structure of the data in a way that machine learning algorithm can be used. These processed data are then obtained and fed into the deep neural network model running on the D-Wave Systems quantum annealer to optimise the traffic flow by predicting the areas that have a high demand for taxis at a given time followed by moving the taxis to these areas before the traffic congestion even occurs [129].

5.3 Machine Learning

5.3.1 Election Forecasting using Quantum Deep Learning by QxBranch

In the US 2016 Presidential Election, Mr.Donald Trump was predicted to be losing to Hillary Clinton in the election. However, the election ended up with Trump claiming the victory. Many studies have been done to investigate the reason behind the failure of these traditional political forecasting models that have been used to give a high accuracy prediction in every US presidential race since Ronald Reagan in 1980 [130].

The post-election analysis revealed that the models failed to take in consideration the correlations between individual states predictions into account. Nevertheless, creating a fully-connected graphical model (connecting all the individual states) requires a powerful computational method for training the model in which the cost in implementing the method using classical devices is too expensive. This issue has lead a collaboration between Standard Cognition and QxBranch to utilise the D-Wave Systems quantum annealing technologies to solve the matter.

Implying the quantum deep learning, an incredibly robust fully-connected graphical model known as the Boltzmann Machine was built and expressed in terms of the Ising Model [92] in statistical physics. The energy function is described as

$$E[\mathbf{s}] = -\sum_{\mathbf{s}_i \in \mathbf{S}} b_i s_i - \sum_{\mathbf{s}_i, \mathbf{s}_j \in \mathbf{S}} W_{ij} s_i s_j \tag{11}$$

where s are the two possible states of the superposed qubits, which are $|0\rangle$, $|1\rangle$. b_i and W_{ij} are the field strength and coupling constants, respectively. The first term of the Eq. (11) is linear and tolerable to be handled by classical computers. The problem lies in handling the second term classically due to reason of being computationally costly [131]. This leads to the use of the D-Wave Systems quantum annealer in order to train multiple fully-connected Boltzmann Machines for every two weeks starting from June 30, 2016 until November 11, 2016, thus obtaining the correlation between individual states predictions. As a result, the predictions of these models where more agreeable with the actual results of the election giving Mr. Trump a predicted percentage of around 40% of winning the election. These exertions revealed that the quantum technologies could solve complex problems such as political modelling, more efficient than classical devices.

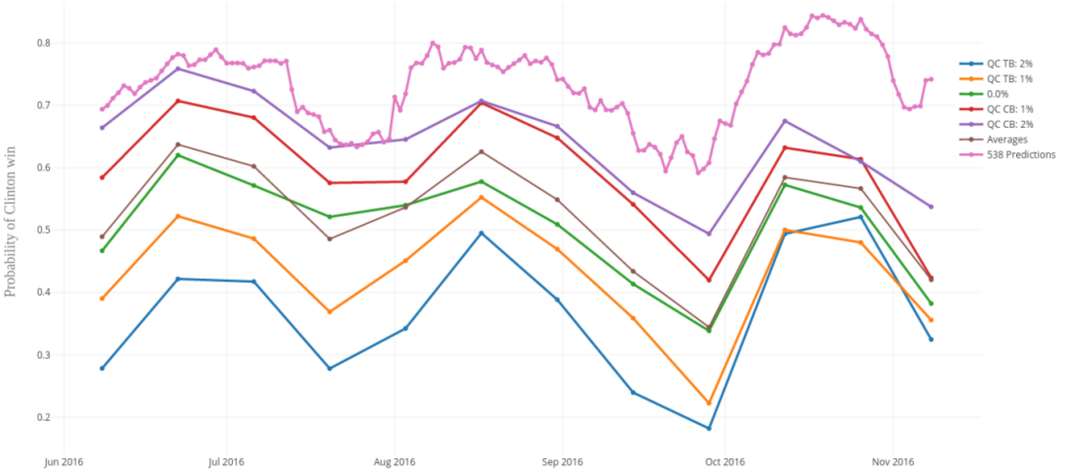


Figure 15: Comparison between quantum Boltzman Machine election forecasting model by *QxBranch* with *Standard Cognition* and the classical model by *FiveThirtyEight* [131].

5.3.2 Graph partitioning through Quantum Annealing by Los Alamos National Laboratory (LANL)

Recent studies on graph-based methods for quantum molecular dynamics (QMD) simulation have led to the implementation of graph clustering methods such as 2-partitioning, k-concurrent, recursive bisection, multi-level with refinement and community detection to be running on D-Wave Systems quantum annealer. The objective of these methods is to lessen the graph complexity in order to improve the computational efficiency.

The graph is partitioned into numbers of equal parts in order to minimise the number of edges whose end points are in different partitions which is also known as the cut edges. For every quantum or quantum-assisted methods that are implemented, the graph partitioning problem is reformulated in the form of QUBO, already discussed previously in Sec. 5.2.1, in order for it to be able to run on the quantum annealer. All the results corresponding to those methods are revealed to be comparable and sometimes better than the methods running on the existing classical graph clustering tools [132].

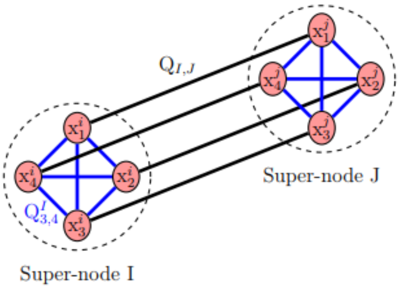


Figure 16: Graph partitioning by one of the graph clustering methods which is known as *k-Concurrent*, with super-node concept being implemented [132].

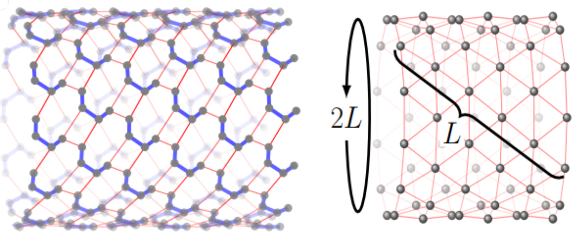


Figure 17: The simulation of quantum magnetic system using D-Wave Systems quantum annnealer(*left*) and the theoretical framework developement for the triangular lattice(*right*) [133].

5.4 Quantum Chemistry Simulation

5.4.1 Demonstration of Topological Phenomenona by D-Wave

The 2016 Nobel Prize was awarded to scientists responsible of the discovery of, what was later to be identified as, the Kosterlitz-Thouless phase transition where exotic phases of matter are governed by the topological properties of low dimensional materials such as graphene, layered semiconductors and insulators. This phenomenon does not exist classically due to the absence of a rotational degree of freedom, thus resulting in the inability of the classical devices to simulate the phenomenon. Nevertheless, with the addition of a transverse field Ising model, the simulation of this phenomenon can be demonstrated in the programmable D-Wave System quantum annealer due to the presence of frustration and quantum fluctuations. These results have been validated by the strong agreement between D-Wave quantum simulation and that of its classical counterpart [134]. On the other hand, the use of this programmable D-Wave System quantum annealer has further led to a simulation of three dimensional simple cubic lattices of up to 512 quantum spins by studying the tranverse Ising model [135]. Both of these exertions revealed the flexibility of D-Wave Systems quantum annealer to work on a larger scale in the field of quantum chemistry.

5.4.2 The Determination of Molecular Ground State Energies

Trapped ion quantum computers have recently been used in quantum chemistry applications where they implement simulations of simple molecules. Specifically, in these simulations, a quantum algorithm called the Variational quantum eigensolver (VQE) is implemented to obtain the energy levels of the molecules H_2, LiH and BeH. Such tasks are within the capabilities of current state of the art classical supercomputers but the hope is that quantum simulators will soon be able to outperform classical computers for the specific task of molecular simulation. This is because the calculation time for molecular energies scales polynomially on a QC using VQE but exponentially on a classical computer [136]. This is important as the modelling of new molecules plays a central role in the development of novel pharmaceutical products or industrial catalysts for instance. Being able to perform a simulation to see if a chemical product behaves desirably and exhibits advantageous properties, saves a lot of money and time for pharmaceutical and chemical companies in the R&D stage. This is, therefore, one example where the supply of quantum computing services is likely to be in high demand in the future.

5.5 Skepticism in Quantum Annealing applications

The advances in optimisation, machine learning and simulations in quantum chemistry made by D-Wave Systems quantum annealer has boosted the development of technology drammatically. On the other hand, with the inspiration of the D-Wave Systems quantum annealing technologies, a silicon-based classical architecture known as digital annealer is built by a collaboration work between University of Toronto in Canada with a Japanese IT equipment and services company called Fujitsu. This digital annealer consists of 1,024 updating bit blocks and built with on-chip memory that enable the process of manipulating bits. By imitating the process quantum tunneling and performing a stochastic search and evaluation of states, Fujitsu's digital annealer is capable of boosting the computational speed for combinatorial optimisation [137]. On the contrary, quantum annealing finds the best solution in a massively parallel way while simultaneously taking all the states into consideration and this implies that quantum annealing would be performing better in the long run [138].

Nonetheless, this digital annealer is able to run under normal room temperature and its also noise-proof, thus resulting in a less computational cost than that of the quantum architecture since it is necessary for previous quantum technologies to be in an extreme cryogenic environment in order to be functional [139]. The advantage over the quantum architecture can also be drawn from the capability of this digital annealer being built to be small enough such that it could easily fit in the circuit board of a data center. With the latest evolution of Fujitsu's digital annealer to their new generation consisting 8,192 updating bit blocks, this enhances the performance and precision for the optimisation process and thus enabling the technology to be applied on a larger scale of problems. Due to the capability of this digital annealer in handling the strong intercoupling strength between the bits, it can solve complex problems that are hardly solvable by current quantum annealing technologies [140].

The development in quantum technologies has clearly intensified the competitive rivalry between classical and quantum computing, leading to the rapid development in the research on computational speed. The existence of the digital annealer has led to a conclusion that it is not a good idea to invest in the quantum annealing machine such as D-Wave Systems. This is because it is much better to invest in digital annealing machines since they are capable of producing a similar or better result with a lower cost in the process than that of quantum annealing technologies. Rather than spending money in quantum annealing machines, it would be more profitable to invest on a universal quantum machine, even though such technology doesn't exist currently, as these would lead to a greater computational benefit.

6 Conclusion

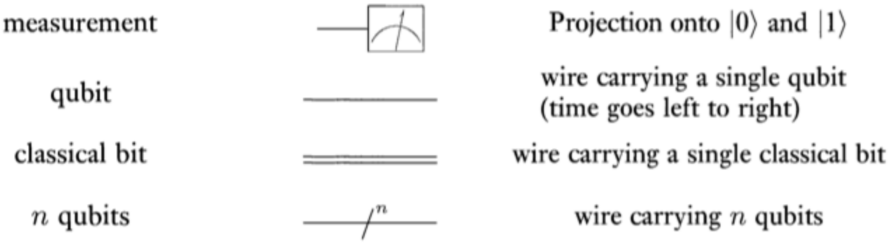
In conclusion, we see that although quantum computers may be far from being commercially available for general tasks, they promise performance improvements over their classical counterparts for specific objectives. As mentioned in Sec. 3 there are many technical and engineering obstacles standing in the way of the development of large scale QCs. This is necessary for their scaling to levels which permit the tackling of practical and important problems. Concurrently, algorithms which leverage the increased computational power of quantum computers must be developed.

As was discussed in Sec. 5, it has already become clear that areas such as quantum chemistry simulation, optimisation and machine learning can benefit tangibly from quantum technologies. With that being said, the aforementioned rise of the digital annealer demonstrates that there are still areas where applying a quantum approach is unnecessarily expensive as classical computing still remains a close competitor for the specific tasks. With the advancements made in the various fields contributing to the technological bases of the various processor types, such as research into room temperature superconductors mentioned in Sec. 3.2, refinement of the fidelities of quantum gates and readout devices, and miniaturisation of components to permit scalability, QCs look promising assuming that our current state of technology is developed significantly during the next 10-20 years.

Considering these facts, QCs should not be treated as a replacement to classical computers but should be regarded as a complementary add-on which increases their efficiency when dealing with certain problems. With these in mind, we conclude that there is no clear advantage of investing in such technology, especially over the course of the next two decades.

Appendix A Frequently Used Quantum Gates and Circuit Symbols

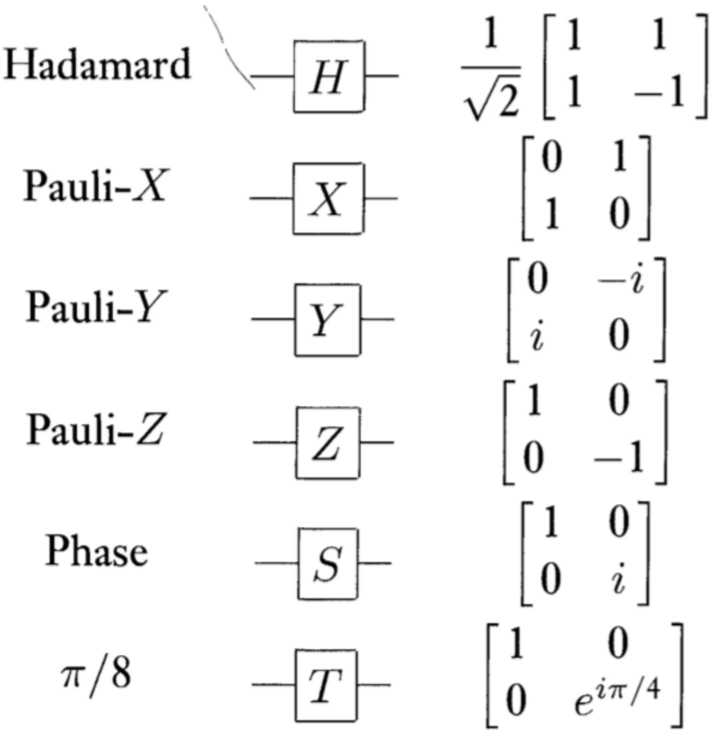
The most commonly used circuit symbols are given below



measurement		Projection onto $\|0\rangle$ and $\|1\rangle$
qubit	—	wire carrying a single qubit (time goes left to right)
classical bit	═	wire carrying a single classical bit
n qubits	$/^{n}$	wire carrying n qubits

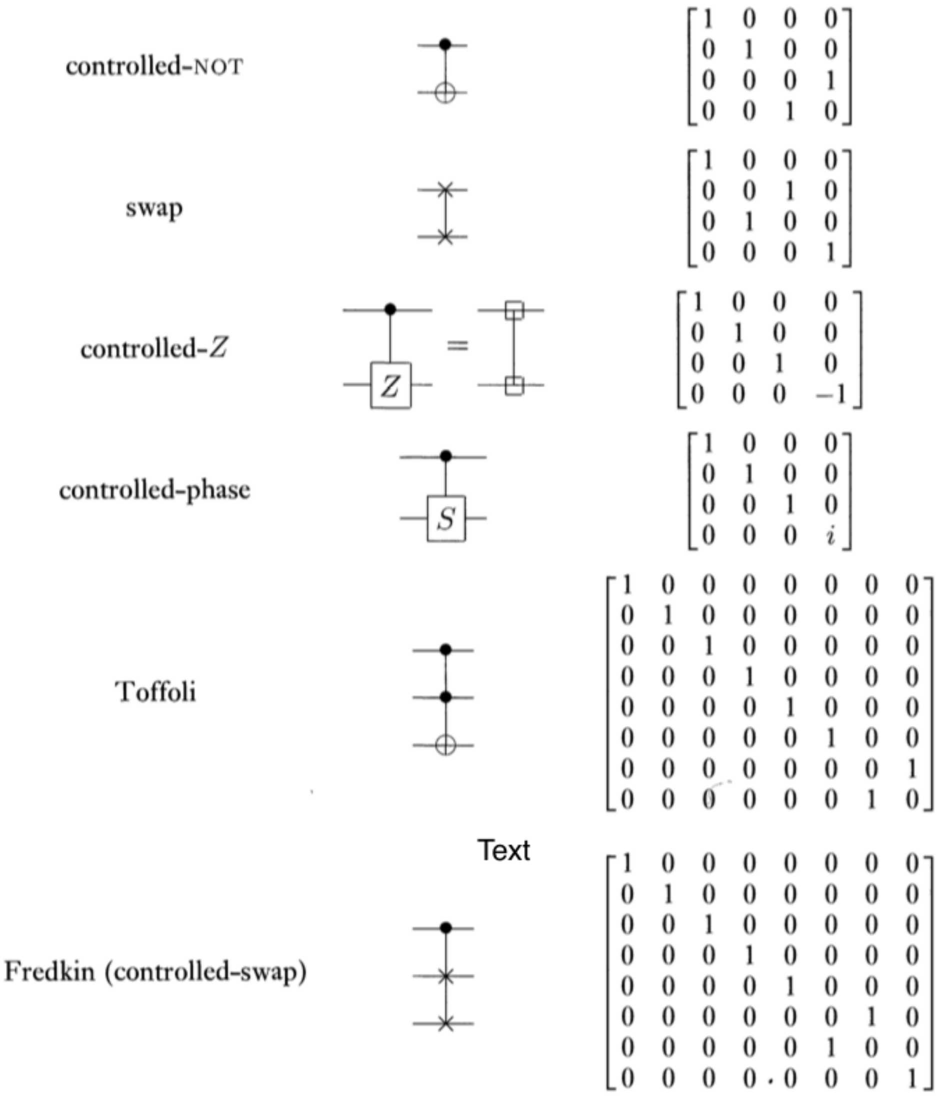
The circuits are read from left to right and each line represents a wire.

The most commonly used single-qbit gates are given below



Hadamard	$\boxed{H}$	$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$
Pauli-X	$\boxed{X}$	$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$
Pauli-Y	$\boxed{Y}$	$\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}$
Pauli-Z	$\boxed{Z}$	$\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$
Phase	$\boxed{S}$	$\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$
$\pi/8$	$\boxed{T}$	$\begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix}$

The most commonly used multiple-qbit gates are given below



controlled-NOT	$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}$
swap	$\begin{bmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{bmatrix}$
controlled-Z	$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&-1\end{bmatrix}$
controlled-phase	$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&i\end{bmatrix}$
Toffoli	$\begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0\end{bmatrix}$
Fredkin (controlled-swap)	$\begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1\end{bmatrix}$

Appendix B Quantum Circuits

B.1 Fourier Transform Circuit

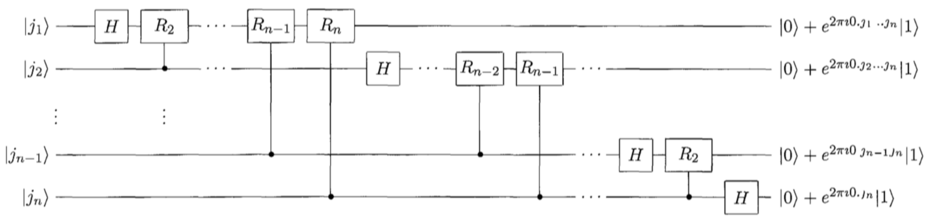

$|j_1\rangle$
$|j_2\rangle$
$|j_{n-1}\rangle$
$|j_n\rangle$
H
R_2
R_{n-1}
R_n
R_{n-2}
$|0\rangle + e^{2\pi i 0.j_1 \cdots j_n}|1\rangle$
$|0\rangle + e^{2\pi i 0.j_2 \cdots j_n}|1\rangle$
$|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle$
$|0\rangle + e^{2\pi i 0.j_n}|1\rangle$

Figure 18: An efficient quantum circuit to perform a Quantum Fourier Transform on a quantum computer. At the end there are swap gates which are not shown [141].

Here, the gate R_k denotes the unitary transformation given by

$$R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix} \tag{12}$$

B.2 Phase Estimation Circuit

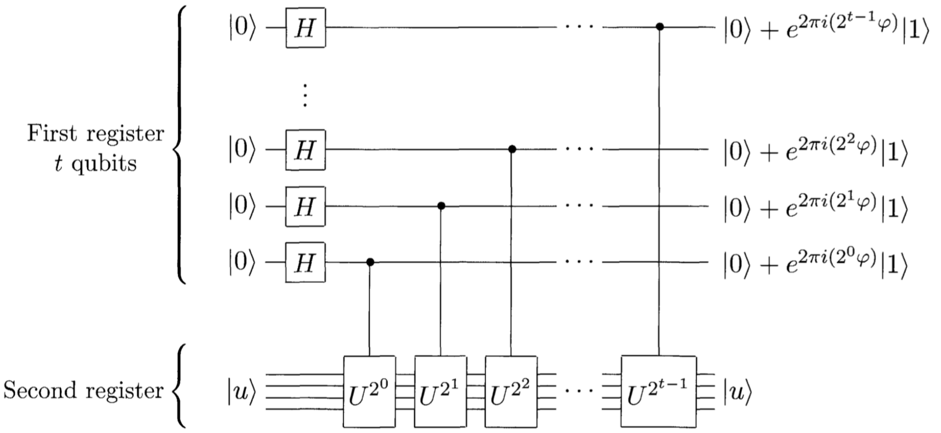

First register
t qubits
Second register
$|0\rangle$
H
$|u\rangle$
U^{2^0}
U^{2^1}
U^{2^2}
$U^{2^{t-1}}$
$|0\rangle + e^{2\pi i(2^{t-1}\varphi)}|1\rangle$
$|0\rangle + e^{2\pi i(2^2\varphi)}|1\rangle$
$|0\rangle + e^{2\pi i(2^1\varphi)}|1\rangle$
$|0\rangle + e^{2\pi i(2^0\varphi)}|1\rangle$
$|u\rangle$

Figure 19: The circuit for performing the first part of the Phase Estimation process. Normalisation has been omitted [142].

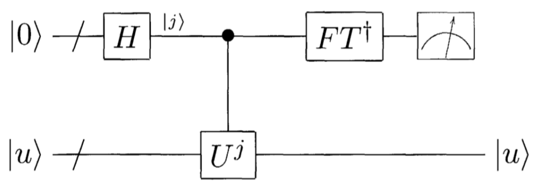


Figure 20: The complete circuit for performing the Phase Estimation [142].

The gate U^x means that U is applied x number of times.

B.3 Grover Iteration

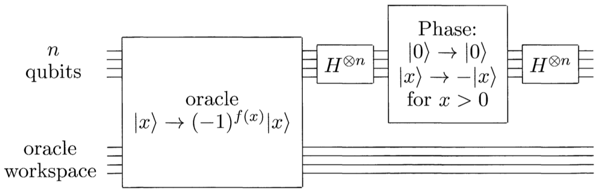

n qubits
oracle workspace
oracle
$|x\rangle \to (-1)^{f(x)}|x\rangle$
$H^{\otimes n}$
Phase:
$|0\rangle \to |0\rangle$
$|x\rangle \to -|x\rangle$
for $x > 0$
$H^{\otimes n}$

Figure 21: Schematic Circuit for Grover Iteration(G) [5].

Appendix C Exponential of Operators

The exponential of operators is defined by its power series expansion. This means,

$$e^{A} = 1 + \frac{A}{1} + \frac{A^2}{2!} + \frac{A^3}{3!} + ...$$

Here, A is an operator.

Appendix D Quantum Simulation

D.1 Approximating Hamiltonians using Unitary Gates

An example of a Hamiltonian that can be approximated using quantum gates is

$$H = Z_1 \otimes Z_2 \otimes ..... \otimes Z_n.$$

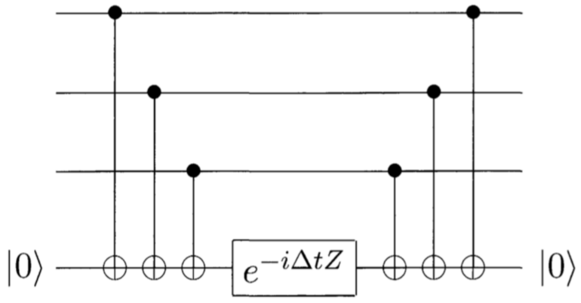


Figure 22: Quantum Circuit of Simulating the Hamiltonian $H = Z_1 \otimes Z_2 \otimes Z_3$ [5].

Where, Z is the Z Pauli matrix. This Hamiltonian can be approximated using quantum gates for any integer value of n. An example of which is given in Fig. 22

References

[1] R. P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6):467–488, Jun 1982.

[2] E. Schrdinger. Discussion of Probability Relations between Separated Systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, 31(4):555563, 1935.

[3] A. Peres, editor. *Complex Vector Space*, pages 78–79. Springer Netherlands, Dordrecht, 2002.

[4] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81:867, Jun 2009.

[5] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, Cambridge, 2000.

[6] O. Carnal and J. Mlynek. Young's double-slit experiment with atoms: A simple atom interferometer. *Phys. Rev. Lett.*, 66:2689–2692, May 1991.

[7] R. Shankar. *Principles of quantum mechanics.* Springer, 2014.

[8] B. Schumacher. Quantum coding. *Phys. Rev. A*, 51:2738–2747, Apr 1995.

[9] Bloch Sphere. Available at https://commons.wikimedia.org/wiki/File:Bloch_Sphere.svg.

[10] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Phys. Rev. A*, 52:3457–3467, Nov 1995.

[11] A. Ekert, P. M. Hayden, and H. Inamori. Basic concepts in quantum computation. In R. Kaiser, C. Westbrook, and F. David, editors, *Coherent atomic matter waves*, pages 661–701, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[12] A. Barenco, D. Deutsch, A. Ekert, and R. Jozsa. Conditional Quantum Dynamics and Logic Gates. *Phys. Rev. Lett.*, 74:4083–4086, May 1995.

[13] P. O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan. On Universal and Fault-Tolerant Quantum Computing, 1999.

[14] H. Wimmel. *Quantum Physics and Observed Reality.* WORLD SCIENTIFIC, 1992.

[15] M. Schlosshauer. Decoherence, the measurement problem, and interpretations of quantum mechanics. *Rev. Mod. Phys.*, 76:1273–1274, Feb 2005.

[16] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[17] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, Aug 1996.

[18] D. P. DiVincenzo and IBM. The Physical Implementation of Quantum Computation. 2000.

[19] Quantum Technologies Roadmap. https://qt.eu/app/uploads/2018/04/QT-Roadmap-2016.pdf. Accessed: 2019-01-29.

[20] Sources of Decoherence - Quantum Device Lab. https://qudev.phys.ethz.ch/content/courses/QSIT11/QSIT11_V08_slides.pdf. Accessed: 2019-01-30.

[21] F. Rohde and J. Eschner. Quantum computation with trapped ions and atoms. 05 2011.

[22] J. Stolze and D. Suter. *Quantum computing: a short course from theory to experiment.* Wiley-VCH, 2008.

[23] J. I. Cirac and P. Zoller. Quantum Computations with Cold Trapped Ions. *Physical Review Letters*, 74(20):40914094, 1995.

[24] D. Kielpinski, C. Monroe, and D. J. Wineland. Architecture for a large-scale ion-trap quantum computer. *Nature*, 417(6890):709711, 2002.

[25] Philipp Schindler, Daniel Nigg, Thomas Monz, Julio T. Barreiro, Esteban Martinez, and et al. A quantum information processor with trapped ions. 2013.

[26] G. PopkinDec, J. MervisJan, P. BaglaJan, D. NormileJan, J. Brainard, and D. Rochmyaningsih. Scientists are close to building a quantum computer that can beat a conventional one, Jul 2017.

[27] C. J. Ballance, T. P. Harty, N. M. Linke, M. A. Sepiol, and D. M. Lucas. High-fidelity quantum logic gates using trapped-ion hyperfine qubits. 2015.

[28] H. C. Nägerl, D. Leibfried, H. Rohde, G. Thalhammer, J. Eschner, F. Schmidt-Kaler, and R. Blatt. Laser addressing of individual ions in a linear ion trap. *Phys. Rev. A*, 60:145–148, Jul 1999.

[29] F. Schmidt-Kaler, H. Hffner, M. Riebe, S. Gulde, G. P. T. Lancaster, T. Deuschle, C. Becher, C. F. Roos, J. Eschner, R. Blatt, and et al. Realization of the CiracZoller controlled-NOT quantum gate. *Nature*, 422(6930):408411, 2003.

[30] R. Blatt and D. Wineland. Entangled states of trapped atomic ions. *Nature*, 453(7198):10081015, 2008.

[31] J. J. Garcia-Ripoll, P. Zoller, and J. I. Cirac. Fast and robust two-qubit gates for scalable ion trap quantum computing. 2003.

[32] C. Monroe and J. Kim. Scaling the Ion Trap Quantum Processor. *Science*, 339(6124):1164–1169, 2013.

[33] Ion-Photon Quantum Networks. http://iontrap.umd.edu/research/ion-photon-quantum-networks/. Accessed: 2019-01-30.

[34] A. Acín, I. Bloch, H. Buhrman, T. Calarco, C. Eichler, J. Eisert, D. Esteve, N. Gisin, S. J. Glaser, F. Jelezko, and et al. The quantum technologies roadmap: a European community view. *New Journal of Physics*, 20(8):080201, 2018.

[35] H. Haeffner, C. F. Roos, and R. Blatt. Quantum computing with trapped ions. 2008.

[36] Y. Wang, Y. Li, Z. Yin, and B. Zeng. 16-qubit IBM universal quantum computer can be fully entangled. *arXiv preprint arXiv:1801.03782*, 2018.

[37] M. Möller and C. Vuik. On the impact of quantum computing technology on future developments in high-performance scientific computing. *Ethics and Information Technology*, 19(4):253–269, 2017.

[38] D. M. Newns and C. C. Tsuei. Quantum computing with d-wave superconductors, December 17 2002. US Patent 6,495,854.

[39] J. Koch, M. Y. Terri, J. Gambetta, A. A. Houck, D. Schuster, J. Majer, A. Blais, M. H. Devoret, S. M. Girvin, and R. J. Schoelkopf. Charge-insensitive qubit design derived from the Cooper pair box. *Physical Review A*, 76(4):042319, 2007.

[40] PHYS 11.2: The quantum harmonic oscillator. Available at http://www.met.reading.ac.uk/pplato2/h-flap/phys11_2.html.

[41] D. Vion, A. Aassime, A. Cottet, P. Joyez, H. Pothier, C. Urbina, D. Esteve, and M. H. Devoret. Manipulating the quantum state of an electrical circuit. *Science*, 296(5569):886–889, 2002.

[42] J. Bardeen, L. N. Cooper, and J. R. Schrieffer. Microscopic theory of superconductivity. *Physical Review*, 106(1):162, 1957.

[43] B. D. Josephson. Possible new effects in superconductive tunnelling. *Physics letters*, 1(7):251–253, 1962.

[44] J. M. Chow, L. DiCarlo, J. M. Gambetta, F. Motzoi, L. Frunzio, S. M. Girvin, and R. J. Schoelkopf. Optimized driving of superconducting artificial atoms for improved single-qubit gates. *Physical Review A*, 82(4):040305, 2010.

[45] A. Wallraff, D. I. Schuster, A. Blais, L. Frunzio, R. Huang, J. Majer, S. Kumar, S. M. Girvin, and R. J. Schoelkopf. Strong coupling of a single photon to a superconducting qubit using circuit quantum electrodynamics. *Nature*, 431(7005):162, 2004.

[46] J. M. Gambetta, J. M. Chow, and M. Steffen. Building logical qubits in a superconducting quantum computing system. *npj Quantum Information*, 3(1):2, 2017.

[47] Why the Discovery of Room-Temperature Superconductors Would Unleash Amazing Technologies, Jan 2019. Available at =https://m.phys.org/news/2019-01-evidence-superconductivity-room-temperature.html?fbclid=IwAR1AcTAt$_{X}mnkVIp2ClZRoGAET5HZMu6YCFdD67_{B}-$ $q7-7dFxaIHNDhp$740.

[48] I. Aleiner and V. I. Fal'Ko. Spin-orbit coupling effects on quantum transport in lateral semiconductor dots. *Physical review letters*, 87(25):256801, 2001.

[49] J. Petta and D. Ralph. Studies of spin-orbit scattering in noble-metal nanoparticles using energy-level tunneling spectroscopy. *Physical review letters*, 87(26):266801, 2001.

[50] E. Rashba and A. L. Efros. Orbital mechanisms of electron-spin manipulation by an electric field. *Physical review letters*, 91(12):126405, 2003.

[51] F. H. Koppens, C. Buizert, K. Tielrooij, I. T. Vink, K. C. Nowack, T. Meunier, L. Kouwenhoven, and L. Vandersypen. Driven coherent oscillations of a single electron spin in a quantum dot. *Nature*, 442(7104):766, 2006.

[52] P. Recher and B. Trauzettel. Quantum dots and spin qubits in graphene. *Nanotechnology*, 21(30):302001, 2010.

[53] R. V. Meter and M. Oskin. Architectural implications of quantum computing technologies. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 2(1):31–63, 2006.

[54] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. OBrien. Quantum computers. *Nature*, 464(7285):45, 2010.

[55] M. Barbieri, T. J. Weinhold, B. P. Lanyon, A. Gilchrist, K. J. Resch, M. P. Almeida, and A. G. White. Parametric downconversion and optical quantum gates: twos company, fours a crowd. *Journal of Modern Optics*, 56(2-3):209214, 2009.

[56] R. Krischek, W. Wieczorek, A. Ozawa, N. Kiesel, P. Michelberger, T. Udem, and H. Weinfurter. Ultraviolet enhancement cavity for ultrafast nonlinear optics and high-rate multiphoton entanglement experiments. *Nature Photonics*, 4(3):170173, 2010.

[57] Spontaneous parametric down-conversion. Available at https://www.wikiwand.com/en/Spontaneous_parametric_down-conversion.

[58] C. M. Natarajan, M. G. Tanner, and R. H. Hadfield. Superconducting nanowire single-photon detectors: physics and applications. *Superconductor Science and Technology*, 25(6):063001, 2012.

[59] Superconducting detectors. Available at https://seis.bristol.ac.uk/~phmgt/quantip/Tuto_SSPD.html.

[60] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn. Review article: Linear optical quantum computing. 2005.

[61] J. L. O'Brien. Optical Quantum Computing. *Science*, 318(5856):1567–1570, 2007.

[62] J. M. Lukens and P. Lougovski. Frequency-encoded photonic qubits for scalable quantum information processing. *Optica*, 4(1):8, 2016.

[63] N. Savage. Building Quantum Computers With Photons, Sep 2018.

[64] J. L. O'Brien. Optical Quantum Computing. *Science*, 318(5856):1567–1570, 2007.

[65] E. Knill, R. Laflamme, and G. J. Milburn. A scheme for efficient quantum computation with linear optics. *nature*, 409(6816):46, 2001.

[66] T. B. Pittman, B. C. Jacobs, and J. D. Franson. Quantum computing using linear optics. *arXiv preprint quant-ph/0406192*, 2004.

[67] T. C. Ralph and G. J. Pryde. Optical Quantum Computation. 2011.

[68] I. A. Walmsley and M. G. Raymer. Toward quantum-information processing with photons. *Science*, 307(5716):1733–1734, 2005.

[69] R. Hughes, G. Doolen, D. Awschalom, C. Caves, M. Chapman, R. Clark, D. Cory, D. DiVincenzo, A. Ekert, P. C. Hammel, and et al. A quantum information science and technology roadmap, part 1: Quantum computation. *Report of the Quantum Information Science and Technology Experts Panel, Version*, 2, 2004.

[70] Y. Li, P. C. Humphreys, G. J. Mendoza, and S. C. Benjamin. Resource costs for fault-tolerant linear optical quantum computing. *Physical Review X*, 5(4):041007, 2015.

[71] The Future of Quantum Computing Could Depend on This Tricky Qubit. Available at https://www.wired.com/2014/05/quantum-computing-topological-qubit/.

[72] V. Lahtinen and J. Pachos. A short introduction to topological quantum computation. *SciPost Physics*, 3(3):021, 2017.

[73] Introduction to topological quantum computation. http://theory.leeds.ac.uk/wp-content/uploads/sites/55/2017/06/IntroTQC.pdf. Acessed: 2019-01-30.

[74] R. Willett, C. Nayak, K. Shtengel, L. Pfeiffer, and K. West. Magnetic-field-tuned aharonov-bohm oscillations and evidence for non-abelian anyons at ν= 5/2. *Physical review letters*, 111(18):186401, 2013.

[75] N. E. Bonesteel, L. Hormozi, G. Zikos, and S. H. Simon. Braid Topologies for Quantum Computation. 2005.

[76] A. Stern and N. H. Lindner. Topological quantum computationfrom basic concepts to first experiments. *Science*, 339(6124):1179–1184, 2013.

[77] Natalie Wolchover and Quanta Magazine. Construction Begins of Topological Qubit, Route to Quantum Computer.

[78] J. Jones. Nuclear magnetic resonance quantum computation. In *Les Houches*, volume 79, pages 357–400. Elsevier, 2004.

[79] J. A. Jones. Quantum computing and nuclear magnetic resonance. *PhysChemComm*, 4(11):49–56, 2001.

[80] 5-Qubit NMR Quantum Computer. Available at https://deliveryimages.acm.org/10.1145/2100000/2090288/figs/f1.html.

[81] M. Barbieri, T. J. Weinhold, B. P. Lanyon, A. Gilchrist, K. J. Resch, M. P. Almeida, and A. G. White. Parametric downconversion and optical quantum gates: twos company, fours a crowd. *Journal of Modern Optics*, 56(2-3):209214, 2009.

[82] D. G. Cory, A. F. Fahmy, and T. F. Havel. Ensemble quantum computing by NMR spectroscopy. *Proceedings of the National Academy of Sciences*, 94(5):1634–1639, 1997.

[83] W. S. Warren. The usefulness of NMR quantum computing. *Science*, 277(5332):1688–1690, 1997.

[84] T. Xin, B. Wang, K. Li, X. Kong, S. Wei, T. Wang, D. Ruan, and G. Long. Nuclear magnetic resonance for quantum computing: Techniques and recent achievements. *Chinese Physics B*, 27(2):020308, 2018.

[85] D. G. Cory, R. Laflamme, E. Knill, L. Viola, T. Havel, N. Boulant, G. Boutis, E. Fortunato, S. Lloyd, R. Martinez, and et al. NMR based quantum information processing: Achievements and prospects. *Fortschritte der Physik: Progress of Physics*, 48(9-11):875–907, 2000.

[86] J. A. Jones. NMR quantum computation: a critical evaluation. *Fortschritte der Physik: Progress of Physics*, 48(9-11):909–924, 2000.

[87] W. S. Warren. The usefulness of NMR quantum computing. *Science*, 277(5332):1688–1690, 1997.

[88] A. Chi-Chih Yao. Quantum Circuit Complexity. In *Proceedings of the 1993 IEEE 34th Annual Foundations of Computer Science*, SFCS '93, pages 352–361, Washington, DC, USA, 1993. IEEE Computer Society.

[89] M. Lanzagorta and J. Uhlmann. Is quantum parallelism real?, 2008.

[90] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, Mar 1993.

[91] F. H. L. Essler, H. Frahm, F. Ghmann, A. Klmper, and V. E. Korepin. *The One-Dimensional Hubbard Model.* Cambridge University Press, 2005.

[92] B. M. McCoy and T. T. Wu. *The Two-Dimensional Ising Model.* HARVARD UNIVERSITY PRESS, 1973.

[93] R. P. Feynman. Feynman and Computation. chapter Simulating Physics with Computers, pages 133–153. Perseus Books, Cambridge, MA, USA, 1999.

[94] H. F. Trotter. On the Product of Semi-Groups of Operators. *Proceedings of the American Mathematical Society*, 10(4):545–551, 1959.

[95] D. S. Abrams and S. Lloyd. Simulation of Many-Body Fermi Systems on a Universal Quantum Computer. 1997.

[96] D. Deutsch. Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 400, 07 1985.

[97] P. W. Shor. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, SFCS '94, pages 124–134, Washington, DC, USA, 1994. IEEE Computer Society.

[98] J. Smith and M. Mosca. Algorithms for Quantum Computers, 2010.

[99] Peter W. S. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. 1995.

[100] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers.* Oxford university press, 1979.

[101] M. Calderbank. The RSA Cryptosystem: History, Algorithm, Primes, 1007.

[102] A. K. Lenstra and H. W. Jr. Lenstra. *The Development of the Number Field Sieve.* Springer-Verlag, 1999.

[103] A. Ekert and R. Jozsa. Quantum computation and shor's factoring algorithm. *Reviews of Modern Physics*, pages 733 – 753, 1996.

[104] M. Mosca and A. Ekert. The hidden subgroup problem and eigenvalue estimation on a quantum computer, 1999.

[105] D. R. Simon. On the power of quantum computation. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, SFCS '94, pages 116–123, Washington, DC, USA, 1994. IEEE Computer Society.

[106] D. R. Simon. On the power of quantum computation. *SIAM J. Comput.*, 26(5):1474–1483, October 1997.

[107] R. Jozsa. Quantum algorithms and the fourier transform. 1997.

[108] *STOC '96: Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*, New York, NY, USA, 1996. ACM.

[109] L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. 1997.

[110] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. Strengths and weaknesses of quantum computing, 1997.

[111] D. Stauffer. *Front Matter*, pages i–vii.

[112] D. A. Battaglia and L. Stella. Optimization through quantum annealing: theory and some applications. *Contemporary Physics*, 47(4):195–208, 2006.

[113] S. Kirkpatrick, C. D. Gelatt, and M. P. Vecchi. Optimization by simulated annealing. *science*, 220(4598):671–680, 1983.

[114] T. Kadowaki and H. Nishimori. Quantum annealing in the transverse ising model. *Phys. Rev. E*, 58:5355–5363, Nov 1998.

[115] C. C. McGeoch. Adiabatic quantum computation and quantum annealing: Theory and practice. *Synthesis Lectures on Quantum Computing*, 5(2):1–93, 2014.

[116] S. E. Venegas-Andraca, W. Cruz-Santos, C. McGeoch, and M. Lanzagorta. A cross-disciplinary introduction to quantum annealing-based algorithms. *Contemporary Physics*, 59(2):174–197, 2018.

[117] E. Crosson and A. W. Harrow. Simulated quantum annealing can be exponentially faster than classical simulated annealing. In *Foundations of Computer Science (FOCS), 2016 IEEE 57th Annual Symposium on*, pages 714–723. IEEE, 2016.

[118] E. F. Galvao and L. Hardy. Substituting a qubit for an arbitrarily large number of classical bits. *Physical review letters*, 90(8):087902, 2003.

[119] A. T. Sornborger. Quantum simulation of tunneling in small systems. *Scientific reports*, 2:597, 2012.

[120] A. Lucas. Ising formulations of many np problems. *Frontiers in Physics*, 2:5, 2014.

[121] W. Kenton. Moore's Law, Dec 2018. Available at https://www.investopedia.com/terms/m/mooreslaw.asp.

[122] U.S. Presidential Election Model: Final Call, Jan 2019. Available at https://en.wikipedia.org/wiki/List_of_companies_involved_in_quantum_computing_or_communication.

[123] S. Bravyi, D. Gosset, and R. König. Quantum advantage with shallow circuits. *Science*, 362(6412):308–311, 2018.

[124] Huiqin Xie and Li Yang. Using Bernstein-Vazirani Algorithm to Attack Block Ciphers, 2017.

[125] M. Bonanome, M. Hillery, and V. Bužek. Application of quantum algorithms to the study of permutations and group automorphisms. *Phys. Rev. A*, 76:012324, Jul 2007.

[126] Qiskit. https://github.com/Qiskit/qiskit, 2018.

[127] F. Neukart, G. Compostella, C. Seidel, D. von Dollen, S. Yarkoni, and B. Parney. Traffic flow optimization using a quantum annealer, 2017.

[128] M Henderson. Quantum Machine Learning for Election Modeling, April 2018. Available at https://www.dwavesys.com/sites/default/files/2018-04-04%20-%20Max%20Henderson%20-%20Quantum%20Machine%20Learning%20for%20Election%20Modeling.pdf.

[129] A. Krok. VW wants to use quantum computing for traffic management, Nov 2018. Available at https://www.cnet.com/roadshow/news/vw-quantum-computing-traffic-management/.

[130] D. White. U.S. Presidential Election Model: Final Call, Nov 2016. Available at https://www.economy.com/dismal/analysis/commentary/286493/US-Presidential-Election-Model-Final-Call.

[131] M. Henderson, J. Novak, and T. Cook. Leveraging Adiabatic Quantum Computation for Election Forecasting, 2018.

[132] H. Ushijima-Mwesigwa, C. F. A. Negre, and S. M. Mniszewski. Graph Partitioning using Quantum Annealing on the D-Wave System, 2017.

[133] D-Wave Systems Inc. D-Wave breakthrough in quantum simulation reveals exotic phase of matter. Available at https://www.dwavesys.com/sites/default/files/kt_synopsis_0.pdf.

[134] A. D. King, J. Carrasquilla, J. Raymond, I. Ozfidan, E. Andriyash, and et al. Observation of topological phenomena in a programmable lattice of 1,800 qubits. *Nature*, 560(7719):456–460, 2018.

[135] R. Harris, Y. Sato, A. J. Berkley, M. Reis, F. Altomare, and et al. Phase transitions in a programmable quantum spin glass simulator. *Science*, 361(6398):162–165, 2018.

[136] A. Aspuru-Guzik, A. D. Dutoi, P. J. Love, and M. Head-Gordon. Simulated Quantum Computation of Molecular Energies. 2006.

[137] Dr. J. Reger. Steps towards Quantum Computing, Nov 2017. Available at https://blog.global.fujitsu.com/steps-towards-quantum-computing/.

[138] J. Boyd. Silicon chip delivers quantum speeds [News]. *IEEE Spectrum*, 55(7):10–11, July 2018.

[139] Fujitsu to Showcase Latest Advances in Quantum-Inspired Computing at Mobile World Congress 2018, Feb 2018. Available at http://www.fujitsu.com/fts/about/resources/news/press-releases/2018/emeai-20180215-fujitsu-to-showcase-latest-advances-in.html.

[140] Fujitsu Launches Next Generation Quantum-Inspired Digital Annealer Service, Dec 2018. Available at http://www.fujitsu.com/global/about/resources/news/press-releases/2018/1221-01.html.

[141] D. Coppersmith. An approximate Fourier transform useful in quantum factoring, 2002.

[142] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca. Quantum Algorithms Revisited. 1997.