ISTANBUL TECHNICAL UNIVERSITY
FACULTY of ELECTRICAL and ELECTRONICS ENGINEERING

A STUDY ON QUANTUM COMPUTATION: COMPARISON BETWEEN CLASSICAL AND QUANTUM LOGIC GATES WITH APPLICATIONS

GRADUATION DESIGN PROJECT

Özgen Tunç TÜRKER

DEPARTMENT OF ELECTRICAL ENGINEERING

MAY 2019

ISTANBUL TECHNICAL UNIVERSITY
FACULTY of ELECTRICAL and ELECTRONICS ENGINEERING

A STUDY ON QUANTUM COMPUTATION: COMPARISON BETWEEN CLASSICAL AND QUANTUM LOGIC GATES WITH APPLICATIONS

GRADUATION DESIGN PROJECT

Özgen Tunç TÜRKER
(040120386)

Supervisor: Prof. Dr. Ş. Serhat ŞEKER
Date: 29 May 2019

DEPARTMENT OF ELECTRICAL ENGINEERING

MAY 2019

FOREWORD

First of all I thank my mother Ülker TÜRKER and my father Ahmet TÜRKER for their love and support.

I also thank my dear friend Burçak EKİTLİ for helping me to be motivated whole year. I thank my friends who create an intellectual environment around me and criticise and support me whenever I need, Ahmet Hakan DUMAN, Öner ALTINBAĞ, Celaleddin HİDAYETOĞLU, Orçun KOLAY, Eray TUNCAN, İsmail PAMİR, Yiğithan YILMAZ and many more...

Finally I thank my supervisor Prof. Dr. Serhat ŞEKER for encouraging me to start a project on a such delightful and cutting-edge subject.

May 2019 Özgen Tunç Türker

Contents

ABBREVIATIONS

NMR	:Nuclear Magnetic Resonance
SRT	:Spin Resonance Transistor
CNOT	:Controlled NOT
IBMqX	:IBM Quantum Experience
QND	:Quantum Non-Demolition

List of Tables

List of Figures

A STUDY ON QUANTUM COMPUTATION: COMPARISON BETWEEN CLASSICAL AND QUANTUM LOGIC GATES WITH APPLICATIONS

ABSTRACT

Aim of the thesis is to step the reader into quantum computation world which is the future of the computation science and also highly interested by electrical, computer and physics engineers as a cutting-edge technology. In this thesis brief explanation of quantum computation is given with basic applications and differences from the classical computation are also given in a comparative way.

The historical developments which make quantum computation happen and mathematical background of quantum physics and computation is given to prepare the reader for the quantum computation. Quantum technologies which covers quantum computers also given in a comparative way to create a visualisation and physical equivalency to what is explained mathematically. Most promised way of building quantum computation, superconductor quantum computers are examined in detail and technical details of IBM's device are also explained.

With all the information given, quantum algorithms, Shor's algorithm and Grover's algorithm and their requirements are introduced and basic simulations of them are done in the IBM's Quantum Experince cloud service. Results of the simulations are commented and improvements which may be done about them are mentioned. Finally basic comparisons between quantum computation and classical computation is done briefly and future of the quantum computation is mentioned.

KUANTUM HESAPLAMA ÜZERİNE BİR ÇALIŞMA: KLASİK VE KUANTUM MANTIK KAPILARININ UYGULAMALAR ARACILIĞI İLE KARŞILAŞTIRILMASI

ÖZET

Tezin amacı; okuyucunun, hesaplama biliminin geleceği olan ve elektrik, bilgisayar ve fizik mühendisleri tarafından son derece ilgilenilen kuantum hesaplama dünyasına adım atmasına yardımcı olmaktır. Bu tezde, uygulamalarla birlikte kuantum hesaplama konusu açıklanmaya çalışılmış ve klasik hesaplama ile arasındaki farklar karşılaştırılmalı olarak verilmiştir.

Kuantum hesaplamayı mümkün kılan tarihsel gelişmeler ve arkasında yatan matematik bilgisi okuyucuyu quantum hesaplamaya hazırlamak maksadıyla verilmiştir. Kuantum bilgisayarları konu alan kuantum teknolojileri bölümü karşılaştırmalı olarak ele alınarak konunun somutlaştırılması hedeflenmiştir. En çok gelecek vaat eden kuantum bilgisayar teknoloji süperiletken kuantum bilgisayarlar hakkında detaylı bilgi verilerek deneylerde kullanılan IBM'in süperiletken bilgisayarı hakkında da tüm teknik bilgiler tezde yer almıştır.

Tüm bu verilen bilgiler doğrultusunda Shor algoritması ve Grover algoritması ve tüm gereksinimleri verilerek bu algoritmalar IBM'in bulut servisi sayesinde erişme açtığı "Quantum Experience" kuantum bilgisayarlarında çalıştırılmıştır. Son olarak kuantum hesaplama ve klasik hesaplamada kullanılan temel mantıksal kapılar karşılaştırılmış ve kuantum hesaplamanın geleceği hakkında bilgiler verilmiştir.

1 Introduction

In 1965, Gordon Moore stated that in every two years power of computers will be doubled. That is the *Moore's law* as we know today. Moore's law was true and it was seen in fallowing years. But it is expected that in some time it will come to the end with some limitations. One of these limitation is about size.[1] As the size of components getting smaller and smaller, quantum physics started to play role in the systems, like tunnel effect. [1] Another limitation is Launder's limit, which related about heat dissipated from a computation. This limits the smallest amount of energy needed and this is calculated for a CMOS computer by James Meindl in 2000.[2] These limitation forces scientists to think about another type of computation, different from the conventional one. Quantum Computation is a one of the possible solution for these limitation. It is based on quantum mechanical principles and it is a type of reversible computation which is free from Launder's limit.[3] Moreover there is also another motivation of quantum computers which is given by Richard Feynman as he pointed out the impossibility of simulation a quantum physical system which is the part of the real the world in a classical computer. And with that way he concluded the possibility and the necessity of the quantum computer.[4, 5]

Quantum Computation is a bridge between two great achievement of science, computer science and quantum physics. Ongoing developments of science is bringing us today to merge these two important field and with the intersection of them we can create completely new type of computation.

As it is tried to explain quantum computation is built upon two important and successful field of science, computer science and quantum mechanics. Hence, it is planned that basics concepts of these two fields will take place in this project. Mathematical background to build quantum computation will be given a little deeply than basic concepts. After these two chapters, quantum algorithms and topologies compatible with applications and case studies will be given as heart of the project. In applications chapter a comparison will also be done. And finally conclusion and discussion will take place as a fifth chapter.

1.1 Definition of Quantum Computation

As it takes place in projects title, the definition of *quantum computation* should be given first. Quantum computation basically is a method of computation using quantum mechanical principles. Unlike a conventional irreversible computation, quantum computing is one of the possible reversible computation method. According to Launder's principle, irreversible computations, for example erasing a bit of information, or taking two bits as an input and resulting one bit as an output, increase the entropy of the system.[6] Hence operations can be undone. Rolf Landauer also pointed that performing an irreversible operation dissipates at least a minimum amount of energy.[7]

Quantum computers which perform quantum computation use quantum bits, namely qubits instead of bits in classical computers. Qubits have some special properties that bits don't. These properties which will be explained in detail in following chapters are based on purely quantum mechanics. Most

important ones of these properties are superposition and entanglement.[8] Superposition means that unlike classical bits states 1s and 0s qubits can be simultaneously in sate 1 and 0.[8] And the more complicated one, entanglement is kind of interaction between two *entangled* or paired systems at a distance.

To realise a quantum computer, a qubit storage system(two-level quantum system), functions to apply on the information (quantum logic gates) and measurement system are needed.[9] Some of the examples of the two-level (or two-state) quantum systems are two distinct polarisation states of a photon, two energy levels of an atomic electron, the two spin directions of an electron or atomic nucleus in a magnetic field, etc.

In classical computation bits are macroscopic states and they are continuous parameters like voltage. In this parameter space two separated region are decided to determine 1and 0 as bits. This space can also be represented as $x \in 0, 1^n$. N-bit memory can be in 2^N different states. And manipulation of data is done by a set of boolean operations. This operations use one or two bits at a time and with a set of operations any "deterministic transformation" can be done.[10]

In contrast, for a quantum bit, qubit, states are physically microscopic systems and they are defined by "a fixed pair of reliably distinguishable states".[10]

In quantum computation, qubit is a basic unit of quantum information. Here quantum information means information of a quantum state. Qubits can be found in two different energy level, $|0\rangle$ and $|1\rangle$. $|0\rangle$ level is often called *ground state* since it represents lowest energy level of this quantum system. In quantum mechanics, state of the system is represented as a ket vector in Dirac notation (Braket notation) which will be explained in the mathematical background chapter of the project. $|0\rangle$ and $|1\rangle$

1.2 Motivation

As it is mentioned before quantum computation is a subject that stands like a bridge between two vast subject of science. That's why, while studying quantum computation, every step of progression is seen directly. Through the last century, seeing and learning about the outstanding developments in science which make quantum computation happens are the key points of the motivations of this project. It is always thrilling that being busy with the topics that stands on the mountain of huge studies, achievements and developments. Dealing with huge amount of work done by countless people, is delighting as well as arduous.

On the other hand, making a connection between electrical engineering and a natural science is another point of the motivation. Here, in this project this connection is made with fundamental electrical engineering concept. Classical logic gates and circuits which has strictly connected with classical physics got a completely different and new approach with quantum physics. Showing this connection is also great motivation for the project.

And lastly there is also breathtaking possible future of quantum computers. In that future, it can be imagined quantum computers solving puzzles unsolvable so far, optimizing difficult engineering problems, diving into the big data, etc. And also there may be totally different cryptography systems and even new methods of communication. Being aware of this change is also huge motivation.

1.3 Aim

In the project, understanding and explaining Quantum computation is in the first place. After that giving its pros & cons against classical computation is aimed. To reach this goal, quantum computation will be tested based on some algorithms. These algorithms will be given as quantum circuits model of computation. And the circuits will be shown in *Quantum Composer* (Figure:1.1) which is a graphical user interface designed by IBM for programming IBM's quantum computers with using quantum logic gates via cloud server. After that relevant classical topology will be simulated in the programs like and the results will be compared and discussed.

1.3.1 Methodology

Project's applications and case studies will take place over IBM Quantum Experience (Q Experience) cloud service. In IBM Quantum Experience, there are currently 3 public devises. These are 14 qubits *IBM Q 14 Melbourne* and with 5 qubits *IBM Q 5 Tenerife* and *IBM Q 5 Yorktown*. But at the moment only *IBM Q 5 Tenerife* can be used via graphical user interface.

In *IBM Q 5 Tenerife* IBM uses fixed-frequency superconducting transmon as a qubit which is a Josephson-junction-based qubit that is insensitive to charge noise. Fixed-frequency qubits are chosen to avoid corrupt quantum information which can be caused by external magnetic field fluctuations.[11] The properties of qubits of IBM's quantum computers is always up to date in their websites devices section. (`www.research.ibm.com/ibm-q/technology/devices/`)

IBM Q Experience also presents a graphical user interface to create a topology of a quantum circuits. Quantum circuits are model of quantum computation just like quantum Turing machine. In Figure 1.1 it is seen that the screenshot of the composer of the IBM Q Experience. An example is given in the Figure 1.2

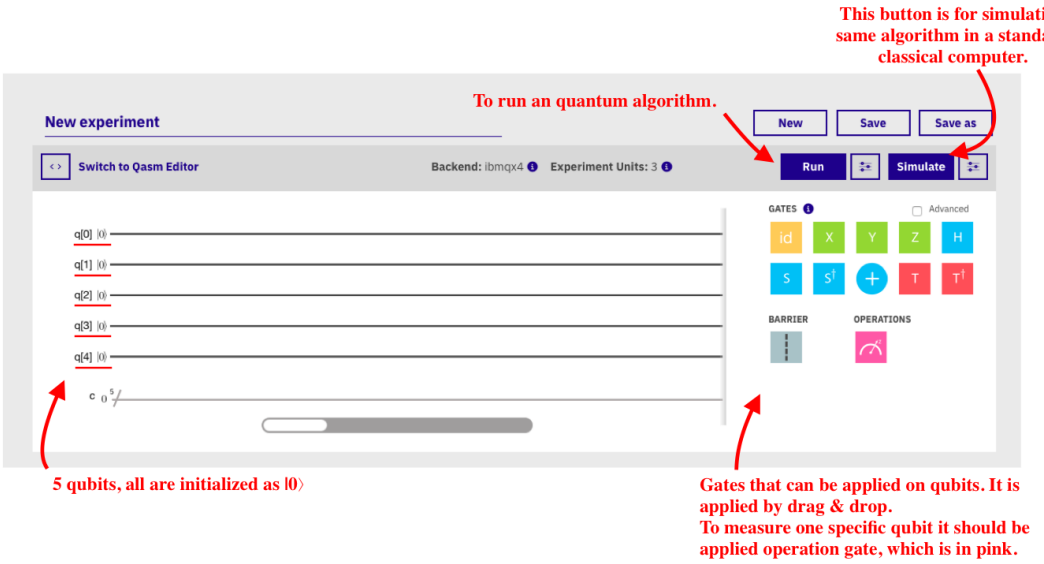


Figure 1.1: Graphical User Interface of *IBM Q 5 Tenerife*.

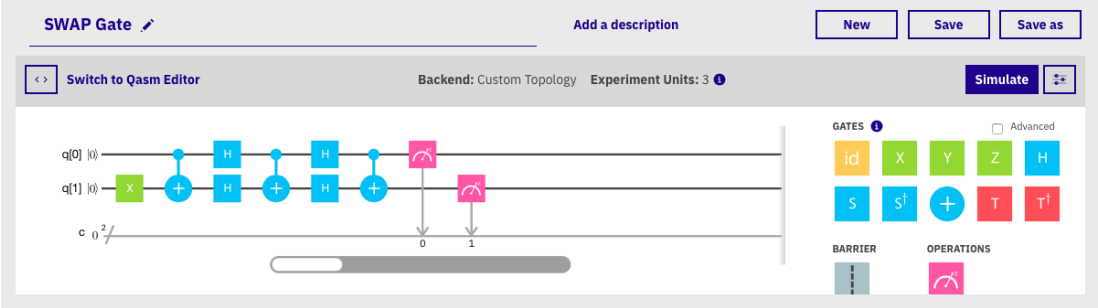


Figure 1.2: Example of a topology. Swap gate topology.

1.4 Organisation

After introduction, historical background first given in detail. In it, instead of giving history of two separate roots of quantum computation (computer science and quantum physics), the incidents made quantum computation real, will be told. Also in historical background chapter some terms which are related development of the quantum computers, will be explained. After that quantum physics will be given as chapter 3. This chapter will include mathematical and physical background and a quantum mechanical approach to the computation. For the moment, superposition, Bloch's sphere and Hilbert spaces are considered as sub topics of this chapter. Besides, some of the detail information which is needed for understanding the thesis will be in the appendix section. Then, in chapter 4, quantum technologies will be discussed. Qubits, quantum logic gates, physical realisations and detailed information of quantum computers and the one which will be used in the thesis (IBM Q 5 Tenerife) are some of the topics of the chapter. In chapter 5 quantum algorithms & topologies will be given explicitly. Additionally, applications and case studies will be done in this chapter which will become the heart of the project. These studies will be tested on IBM's quantum computer which is allowed to be used over IBM's cloud service. In this service IBM serves some of its quantum computers to the public. This issue will be discussed more in detail in the IBM's Quantum Computer subsection. Finally, conclusions and discussions will take place in the last chapter.

1.4.1 Time Planning

Time planning of the project is in the Figure 1.3. As it is shown in the figure, literature research takes 5 months time period of the project which is expected last for 9 months. During the literature searching, collected information used while determining outline of the thesis and preparation of the interim project report. Also information about the historical background and theoretical part such as mathematical equations and physical explanations of the subject will be searched in this time period. After finishing literature research, it will be continued to give theoretical information for a period. Then case studies and applications will be focused. Although literature searching seems to finish in 5 months, in any inconvenient situation it is possible to go back to it. After all according to the results, discussions will be made and all study will be reported in the final thesis.

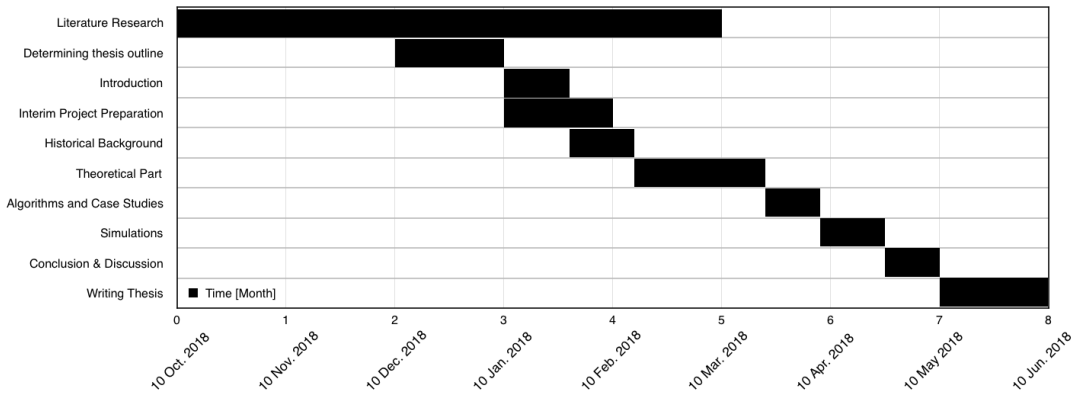


Figure 1.3: Time management.

A planned workflow chart is also given in Figure 1.4.

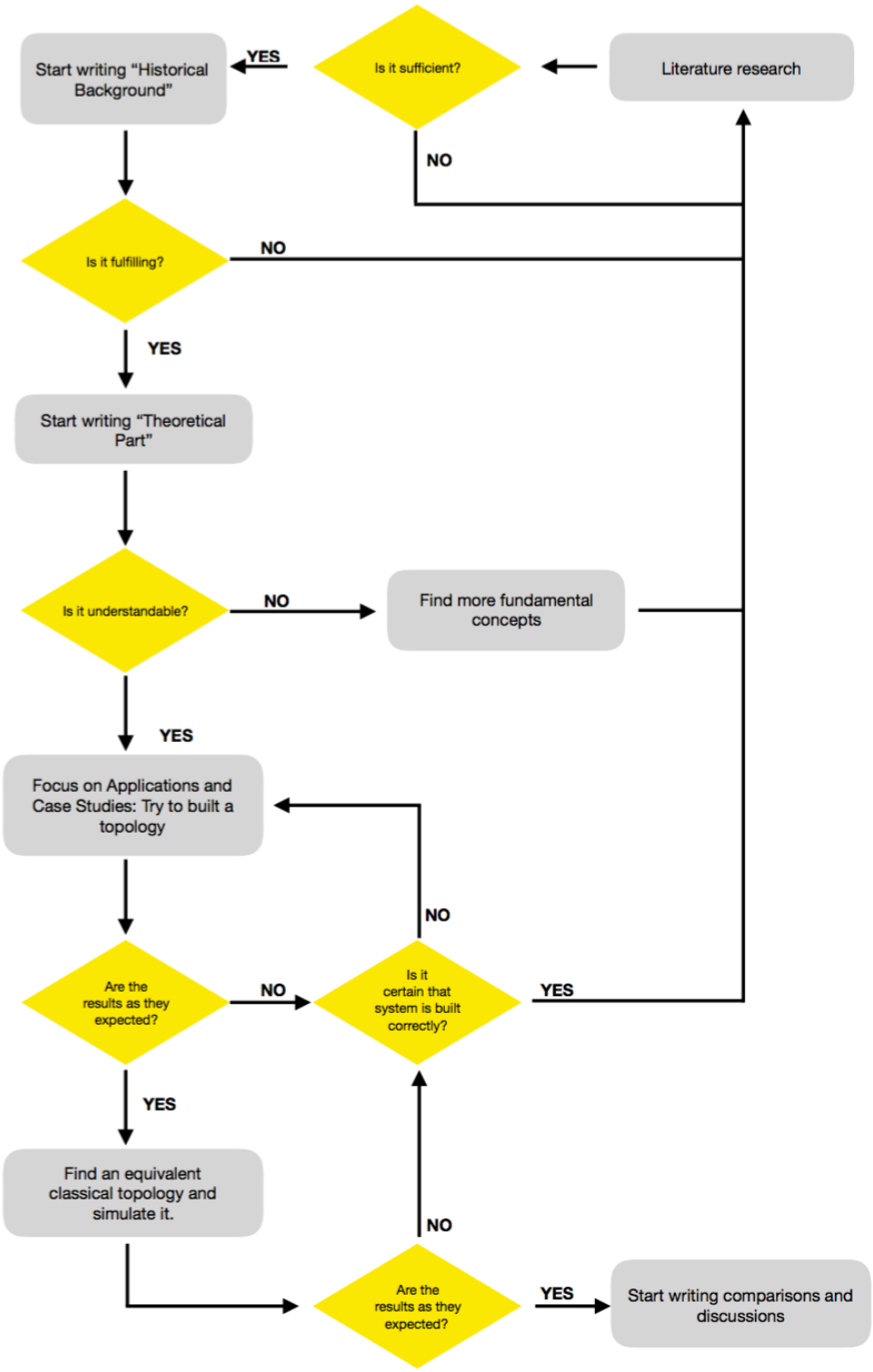


Figure 1.4: Workflow chart.

2 Historical Background

In this chapter, history of computer science and quantum mechanics will not be given but all their milestones and other incidents which make quantum computation possible will be given. To make a good start, Allan Turing and his hypothetical machine which is known as *Turing Machine* will be the best.

2.1 Turing Machine

In his paper "On Computable Numbers, with an Application to the Entscheidungsproblem"[12]Turing proposed *the universal computing machine*. Which is simple and powerful as it can be simulate any of the computer algorithms regardless its complexity.[13] 1930's are the year for the search of an concrete computational theory. Besides Turing machine there are also two main theories for formalising computation, these are the , λ*-calculus* of Alonzo Church, and *recursion theorem* of Stephen Cole Kleene.[14] Among them, Turing machine(TM) is the most popular one. One of its reason may be the success of TM on decoding German's code in the second World War. [14]

Principle of Turing machine is simple. It's structure in Figure 2.5

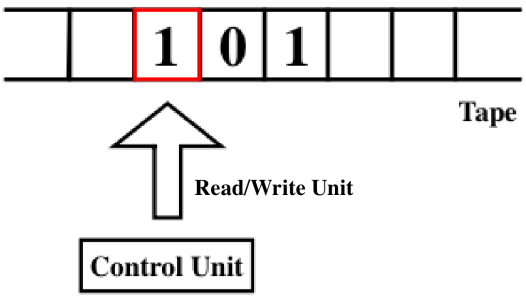


Figure 2.5: Structure of the Turing Machine.

An infinitely long tape which is divided into small squares is the equivalent of the memory of the modern classical computers. Read/write unit can move left or right but it can only make an operation for one square per time. From this it can be seen as an input/output pin of a modern computer. And control unit is a finite control unit is holding current state of the machine and it decides what to do to that square and what to do in next step. A basic Turing machine, finite state Turing machine, instructions are given below to change a set of input for example "101"(as it is shown in the Figure 2.5) to "010" and back to "101":

Table 2.1: State table of finite state Turing machine.

Current State	Read	write	Move	New State
state X	B	B	R	state Y
state X	1	0	L	state X
state X	0	1	L	state X
state Y	B	B	R	stop state
state Y	1	0	R	state Y
state Y	0	1	R	state Y

This can be also represented by a state diagram in Figure 2.6

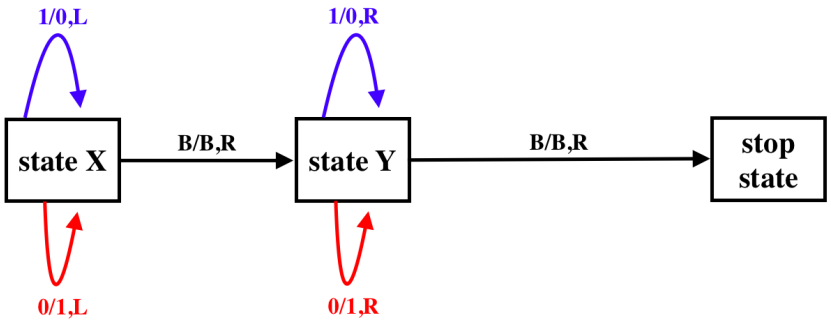


Figure 2.6: State diagram of finite state Turing machine.

In format "0/1,L", 0 is read, 1 is written values L is the left move of the tape. Red arrows show that 0 is read and blue arrows show that 1 is read. In fact, with its infinite tape, Turing machine can do more than a finite state machine, which is a abstract machine with only finite number of states, can do.

2.2 Quantum Mechanics

Quantum physics is one of the most successful achievements of physics so far. Here, only some parts which is concerned by computation will be taken. In a quantum system, a system which is small enough to observe quantum effects, evolutions are described with Schrödinger Equations which is introduced by Erwin Schrödinger in 1925 and published in 1926[15] and leads him to won the Nobel Prize in 1933. Since Schrödinger equation is linear, we have a famous property which takes important place in quantum computation, *superposition*. With his equation Schrödinger thought that the state of a quantum system can be determined certainly. But that was not the case. Max Born brought forward the probabilistic interpretation of Schrödinger equation. [16] Schrödinger equation, thus, gives only the probability to find the system in a state. With this explanation, states of a quantum system can be superposed with its probabilities. For example, consider the spin of an electron as a quantum system. So its states *spin up* and *spin down* as it is shown in Figure 2.7.

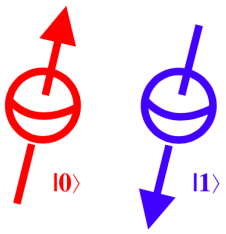


Figure 2.7: Two different state of spin of an electron. *Spin up* and *spin down*

So the probabilistic interpretation tells that finding quantum system in a state is always probabilistic. For example, for a *Spin up* state, finding spin of electron in the *Spin up* state (red one in the figure 2.7) is always 100% and similarly for a state *spin down* finding system in *Spin down* state (blue one in the figure 2.7). And these two state also added up with some probability and create a superposition state which is shown in Figure 2.8. And this time, probability of finding this new state in *Spin down* state different than finding it in *Spin up* state. Sum of these different probabilities makes 100%.

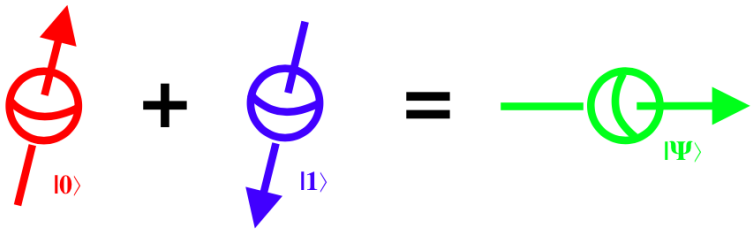


Figure 2.8: Superposition of states *Spin up* and *spin down*

This phenomena leads quantum mechanics at a "strange" point for that time. Some paired quantum states which later called *entangled* (by Erwin Schrödinger), may have some sort of instant communication which is named "spooky action at a distance" by Albert Einstein. They keep their dependency even there is a huge physical distance between them. In 1935 Albert Einstein, Boris Podolsky and Nathan Rosen published a paper about a thought experiment,"EPR" paradoxes, to show that quantum physics is not completed.[17] Their paradox basically claims that this instant communication violate the special theory of relativity, so there must be pre-determined variable between these states. Debates had been only solution for almost 30 years until John Bell introduced a theorem for testing EPR paradox.[18] And after several years, Bell's theorem is tested and proved that there is no "hidden variable" to predetermine the communication. With this progress, entanglement, with superposition, is one of key features to make quantum computation real.

2.3 Reversible Computing

One of the important feature of the the quantum computing is *reversibility*. Physically, it corresponds to more efficient way of making logic operations than the conventional irreversible computation. Also more technically, reversible computation is not limited by Landauer's Limit which stands for a energy dissipation while making an logic operation because of the information lost. Which can be explained by increasing entropy.[6] Landauer was the first one who connected logical reversibility and physical

reversibility.[19] He introduced that at least $kT \ln 2$ of energy per irreversible logical operation.($3 \times 10^{-21} J$ at room temperature)[3]

Following to Landauer's works, *reversible computation* was first introduced by Charles H. Bennett. He showed that a conventional computation which is irreversible by its nature, may be made reversible.[3] And he introduced reversible Turing machine in his work. After that, Tommaso Toffoli came up in 1980 with his idea of reversible logic gate *Toffoli Gate*.[20] And two years later, he and Edward Fredkin brought forward the idea of *billiard-ball computer* and *Fredkin gate* came up.[21] They thought that any physically deterministic system may be designed to be reversible.[22] The billiard-ball computer was an example for their idea, idealised mechanical computer which is reversible based on elastic collision in Newtonian physics. And it was also an example of *conservative logic* which is also introduced in the same paper to represent indestructible information in any set of logical operation.[22] The demonstration of the system is in the Figure 2.9 which is taken from Wikipedia and will be replaced by another original figure soon.

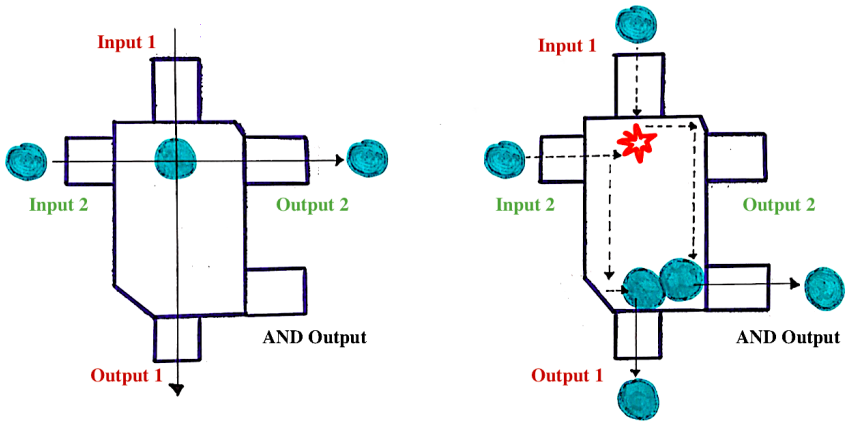


Figure 2.9: Visualisation of billiard-ball computer.

In the Figure 2.9, on the left there is only one billiard ball is coming from one of the input ports and comes out from the corresponding output port.. On the right 2 balls is coming from both input ports and they collide elastically, ideally. One of the balls comes out from the one of the output ports and the other comes out from the AND output forms.

2.4 Quantum Algorithms

Before passing the talking about the quantum algorithms there were still some problems. One of them was quantum computational representation of Turing machine. This was achieved in 1982 by Paul Benioff who showed a quantum mechanical model as representation of the Turing machine. His work was based on Bennett's reversible Turing machine description. [23] At that time Richard Feynman also published "Simulating Physics with Computers" in 1981 in which he discussed that simulating quantum problems in classical computers is not effective and he brought forward the idea of different kind of computing, quantum computing.[14, 4]

In 1985 David Deutsch introduced first quantum Turing Machine.[24] Just like, mathematical model of classical computation, Turing Machine can do any classical logical algorithms, the mathematical

model of quantum computation which is called quantum turing machine also capable to simulate any quantum algorithms.[14]

In practical manner, Peter Shor was the first one who came up with an algorithm. He showed that quantum computers can be used to factorise large numbers and give as an output its prime integers much more efficiently than classical computer. This is known as Shor's algorithm and will be discussed in detail in the project. The second important algorithm is known as Grover's algorithm, which will again be discussed in detail later on, is introduced by Lov Gorver in 1996.[14] With the potential of the use of these algorithms in the area of cryptography, search and optimisation, simulation of quantum systems or solving large linear systems, quantum computers have more power than a standard computer. [25]

2.5 Experiments

Physical realisation of quantum computers is one of the greatest challenge of the topic. Most critical requirement to built a quantum computer is making it isolated. A small interaction with the outside may cause quantum mechanically destructive process called decoherence.[26] First successful attempt was in 1998, these were the first experiments. In Oxford University by by Jonathan A. Jones and Michele Mosca[27] and in IBM's Almaden Research Center by Isaac L. Chuang realised 2 qubit quantum computer based on NMR (Nuclear Magnetic Resonance).[28]

In 2001, with the NMR technique, 7 spin-$1/2$ nuclei used as qubits in order to experimental realisation of Shor's algorithm. [29] After that an other quantum algorithm the Deutsch– Jozsa algorithm realised experimentally on an ion-trap quantum computer.[30] With same method, Grover's algorithm was implemented by using two qubits. [31] an optical method was taken place in 2009 with again Grover's algorithm realised experimentally with photons as qubits. [32] Again in 2009 first solid state based quantum processor was realised, a two-qubit superconducting processor. [33]

2.6 Modern Quantum Computers

Researches and implementations of quantum computers have variety of different approaches, atomic physics, quantum optics, nuclear and electron magnetic resonance spectroscopy, superconducting device physics, electron physics, and mesoscopic and quantum dot research. [34] In his paper DiVincenzo gives 5 requirements to make a quantum computer real. These are [34]

1. A scalable physical system with qubits characterised properly
2. The ability of initialising states of the qubits to a simple reliable state
3. Long decoherence times
4. Universal quantum gates
5. The ability of measuring specific qubits

Based on these requirements, today, companies like IBM, Google, Microsoft, D-Wave and Rigetti are currently working on quantum computers. The computer which will be used in this project is one of the machines of IBM Quantum Experience project which is a cloud service launched in 2016 to let

its members use and run experiments on quantum computers. In IBM Quantum Experience, superconducting qubits are used and the machines are actually located at the IBM T. J. Watson Research Center in New York.

Additionally, IBM announced in January 2019 world's first commercial quantum computer. 20-qubit computer, "IBM Q System One" has an integrated quantum computing system in it.

3 Mathematical Background

To better understand quantum computing, first quantum mechanics, the most accurate and complete description of the world [1], should be mentioned.

3.1 Observations in Quantum Mechanics

Unlike wave mechanics, in quantum mechanics, a state of a physical system is represented with a unit vector. Generally, these vectors are represented with a ket vector ($|\Psi\rangle$) according to the Dirac notation. Here Ψ is an arbitrary vector and ket symbol tells that the label inside it is a vector. A condition for a unit vector is normalisation condition and it is shown as follows:

$$\langle\Psi|\Psi\rangle = 1 \tag{3.1}$$

From *linear algebra* knowledge, it can be said that every vector can be written as a linear combination of the spanning set vectors of its vector space. This feature led **superposition** happen, which simply refers writing down a physical state with linear combination of other states. If these vectors are linearly independent they form a basis.

$$|\psi\rangle = a_1|1\rangle + a_2|2\rangle + a_3|3\rangle ... + a_n|n\rangle, \tag{3.2}$$

$$= \sum_i a_i|i\rangle \tag{3.3}$$

Where $|1\rangle, |2\rangle, |3\rangle ..., |n\rangle$ are vectors of the vector space which contains vector $|\psi\rangle$ and $a_1, a_2, a_3, ..., a_n$ are complex numbers. If this set of vectors is an orthonormal set then the set becomes a basis vectors set. So inner product of these vectors must be equal to 0. In quantum mechanics inner product is shown like this:

$$\langle v_1|v_2\rangle \tag{3.4}$$

according to the Dirac notation. And it is pronounce as braket of v_1 and v_2. And for basis vectors it should be

$$\langle v_i|v_j\rangle = \delta_{ij}, \tag{3.5}$$

A n-dimension vector space has a basis which consist n vectors. It can be more than one set of n vectors which can form a basis. For example if $\mathbb{R}^2$ is considered, most convenient way is to take basis

as:

$$|v_1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |v_2\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{3.6}$$

but other vectors also can be written as basis vector. Such as:

$$|v_1\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, |v_2\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}, \tag{3.7}$$

Here coefficients $\frac{1}{\sqrt{2}}$ are to make basis orthonormal.

Moreover, ket vector ($|\Psi\rangle$) which can be represented as a column vector is a *hermitian conjugate* (or conjugate transpose) of the bra vector ($\langle\Psi|$) which can be represented as a row vector.

$$|\Psi\rangle = \begin{bmatrix} \psi_1 \\ \psi_2 \\ \psi_3 \end{bmatrix}, \quad \langle\Psi| = \begin{bmatrix} \psi_1^* & \psi_2^* & \psi_3^* \end{bmatrix} \tag{3.8}$$

Now if the equation **3.2** is taken, the representation $\langle i|\psi\rangle$ can be read as the result of the state $|\psi\rangle$ which ends up in the form of $|i\rangle$. This inner product rises a number which is called amplitude. Richard Feynman interprets this inner product as "the amplitude that" [35]. He interprets right of the vertical line is initial state and the left side is final state. So again from equation **3.2**, for example $\langle 2|\psi\rangle$ can be written like this:

$$\langle 2|\psi\rangle = \langle 2|\left(a_1|1\rangle + a_2|2\rangle + a_3|3\rangle ... + a_n|n\rangle\right) \tag{3.9}$$

$$= \langle 2|a_1|1\rangle + \langle 2|a_2|2\rangle + \langle 2|a_3|3\rangle ... + \langle 2|a_n|n\rangle \quad \text{from eq. } \mathbf{3.5} \text{ all terms, except } \langle 2|a_2|2\rangle \text{ give 0} \tag{3.10}$$

$$= \langle 2|a_2|2\rangle \quad \text{and if the number } a_2 \text{ is taken outside } \langle 2|2\rangle \text{ gives 1} \tag{3.11}$$

$$= a_2 \tag{3.12}$$

So the complex number a_2 is the amplitude that the state $|\psi\rangle$ ends up with the state $|2\rangle$. This huge important feature will be discussed later in this section.

Again in linear algebra a *linear operator* is used for the following operation: $P : \vec{A} \to \vec{B}$. Here P is a *linear operator* that acts on vector space A and transform it to the vector space B. There also exists matrix representation of these linear operators, as matrices $A_{m\times n}$ which transforms a vector from vector space $\mathbf{C}^m$ to a vector from vector space $\mathbf{C}^n$.

In quantum mechanics an *observable* is also taken as an *linear operator*. Only condition for it, is that operator should be *hermitian* which equals it own *conjugate-transpose*.

$$A = \overline{A^T} \tag{3.13}$$

So every observable associated with a linear and hermitian operator. Generally it is represented with a hat over a capital letter. For example, $\hat{H}$ stands for Hamiltonian which is a energy operator. Measuring

an observable about a state means acting on that state vector (ket vector) with associated operator.

$$\hat{H} : |\Psi\rangle \rightarrow |\Psi'\rangle \tag{3.14}$$

$$\hat{H}\,|\Psi\rangle = |\Psi'\rangle \tag{3.15}$$

Besides the matrix operations, sometimes it is referred as matrix mechanics, quantum mechanics has features from wave mechanics too. An one dimension state function in wave mechanics is represented with $\psi(x)$. Its observables are associated with the operators like position, momentum and energy. In position space, these are $\hat{X} = x$, $\hat{P} = -i\hbar\frac{d}{dx}$ and $\hat{H} = \frac{-\hbar^2}{2m}\frac{d^2}{dx^2} + \hat{V}$ respectively. And they act on state function by multiplication.

$$\hat{H}\psi(x) = \frac{-\hbar^2}{2m}\frac{d^2\psi(x)}{dx^2} + \hat{V}\psi(x) \tag{3.16}$$

Here $\hat{V}$ is a potential energy operator.

There is also outer product, $|v_1\rangle\langle v_2|$. Outer products produce operator rather than a scalar value which is produced by an inner product. For basis vectors there is an important relation called *completeness relation* which helps a lot in quantum computation.

$$\sum_i |i\rangle\langle i| = I$$

Here I is the *identity vector*. The completeness relation can be derived from $\sum_i |i\rangle\langle i|$ acting on $|\psi\rangle$.

$$\left(\sum_i |i\rangle\langle i|\right)|\psi\rangle = \sum_i |i\rangle\langle i|\psi\rangle \tag{3.17}$$

$$= \sum_i |i\rangle a_i \quad \text{here } a_i \text{ can change places cause it is a scalar} \tag{3.18}$$

$$= \sum_i a_i |i\rangle \tag{3.19}$$

$$= |\psi\rangle \tag{3.20}$$

If a state for example $|\Psi\rangle$ wanted to be measured in a desired state for example $|1\rangle$ so it should be acted by an operator, P_1, and this operator called *projection operator* which refers to the projection of the state $|\Psi\rangle$ to the $|1\rangle$.

$$P_1|\Psi\rangle = |1\rangle\langle 1|\,|\Psi\rangle \quad \text{again from equation } \mathbf{3.2} \tag{3.21}$$

$$= |1\rangle a_1 = a_1|1\rangle \tag{3.22}$$

Here it is seen that the state $|\Psi\rangle$ collapsed to the state $|1\rangle$ after projection operator acted which corresponds to measuring. And a_1 is the amplitude of that collapse event.

From here *density operator* can also be introduced. It correspond to the projection operator for all basis states. If an ensemble of states is created with specific percentage, lets say p_i for example for state $|i\rangle$ then the density operator becomes:

$$P = \sum_i p_i |i\rangle\langle i| \tag{3.23}$$

Additionally, density operator or density matrix is used to represent *mixed states*. Mixed states are different then superposition states. The density of a specific state in a mixed state or an ensemble of states denoted by a real number while this is complex number in a superposition. Besides mixed states there are also *pure states* which are the ones that can be written with a ket vector, basis vectors and all other quantum superposition of them.

Now it's time to solve equations and find the result of the measurement. In quantum mechanics, the only possible results of the measurements are the eigenvalues of the operator which is associated with the observable. And after that measurement, state collapses to the eigenfunction or eigenstate of the operator. This property shows the quantumness of quantum mechanics. There are no continuous spectrum of the result, there are only discrete values results which are eigenvalues of the associated operator.

3.1.1 Measurements in Quantum Mechanics

Another beautiful and weird reality about quantum mechanics is the dependence of the measurement to the basis. It is impossible to making any measurement about states rather than the states which form basis. To get information on the states rather than basis, first it should change the basis. Than it is possible to get knowledge of the system at that basis.

To visual it polarised photons can be used. In two dimensional hilbert space, if vertical and horizontal polarised photon are selected as basis than any state $|\phi\rangle$ can be expressed as follows:

$$|\phi\rangle = \alpha\,|\updownarrow\rangle + \beta\,|\leftrightarrow\rangle$$

So to measure this state $|\phi\rangle$ which polarisation it has, best way is to multiply it with the bra vector of the basis vector. It is called projective measurement. To see whether it is vertical polarised or not calculate $\langle\updownarrow|\phi\rangle$ and its probability $\left|\langle\updownarrow|\phi\rangle\right|^2$. And same for horizontal polarisation, $\langle\leftrightarrow|\phi\rangle$ and its probability $\left|\langle\leftrightarrow|\phi\rangle\right|^2$. With these calculation, it is found that the state $|\phi\rangle$ behaves like vertical polarised with the probability of $|\alpha|^2$ and horizontal polarised with the probability of $|\beta|^2$[10]

But what if it is wanted to be measured the state with a machine which is polarised diagonally? For as it is mentioned before now state $|\phi\rangle$ should be written in diagonal polarised vectors basis. So it should be find two of them because the hilbert space of the system has two dimension. Then basis change can be a good point to start. So $|\nearrow\rangle$ and $|\swarrow\rangle$ can be selected,

$$|\updownarrow\rangle = \mu\,|\nearrow\rangle + \nu\,|\swarrow\rangle \tag{3.24}$$

$$|\leftrightarrow\rangle = \gamma|\nearrow\rangle + \lambda\,|\swarrow\rangle \tag{3.25}$$

Form here $|\phi\rangle$ can be rewritten and $\langle\nearrow|\phi\rangle$ and $\langle\swarrow|\phi\rangle$ and their probabilities can be calculated. There is also another way to do it, and it is writing down the diagonal basis in terms of horizontal and vertical ones. This method will be used in the section 3.2

This principle works when if it is wanted to see the result of the operator of an observable. In quantum mechanics, observation results always with an eigenvalue of the operator. It is seen that an operator acts on a state as shown:

$$\hat{P}\,|\Psi\rangle = p\,|\Psi'\rangle\,, \tag{3.26}$$

Here $\hat{P}$ is an arbitrary operator, $|\Psi\rangle$ is an arbitrary state and it is eigenstate of the operator $\hat{P}$ and finally p is the eigenvalue of $\hat{P}$. Here number p and vector $|\Psi\rangle$ form eigenvalue, eigenstate couple. This is because operator $\hat{P}$ is defined in the basis of $|\Psi'\rangle$ vectors. Sometimes these couples may be deformed, such that one eigenvalue can be associated with two different eigenstate. This causes *degeneracy*. A physical example of it is that, some particles, which are in different states, may have same energy level, is corresponds eigenvalues.

Only condition for making a measurement and getting an result with a probability of 100% is that the resulted state should be an eigenstate of the operator associated with the observable which is wanted to be measured. In all other cases there is always a uncertainty and the measurement results with a probability which is equal to the square of the norm of the expectation value as *Copenhagen interpretation* says.

There is also an important term, *expectation value*. Expectation value is the average of the results for an observable. Generally it is shown like this $\langle\hat{P}\rangle_\Psi$. The subscript Ψ shows the basis for which this expectation value is calculated. It is calculated as follows:

$$\langle\hat{P}\rangle_\Psi = \langle\Psi|\hat{P}|\Psi\rangle \tag{3.27}$$

From the expectation value it is also important to calculate standard deviation, σ. Which helps *the uncertainty principle* be introduced with ease.

$$\sigma_{\hat{P}} = \sqrt{\langle\hat{P}^2\rangle - \langle\hat{P}\rangle^2} \tag{3.28}$$

3.2 Qubits

To make the topic easier to understand let's consider a simple experiment of photon. In this experiment, a laser pointer and 3 different polarizers, vertical, horizontal and diagonal, are needed. First step is pointing laser beam to a screen. Then polarizers are placed between laser pointer and screen in a specific order. First it is seen that if one of any there polarizers is placed laser beam is seen on the screen. But when second polarizer is also placed, things getting complex. If first polarizer is vertical and second is horizontal or vice versa, there will be no light on the screen. However if the diagonal polarizer is placed between vertical and horizontal polarizers then it turns out that light is seen on the screen. This basic experiment holds lots of quantum mechanical features in it.

Let's give a physical explanation of the experiment. Here it will be considered an one photon phenomena in order to make things small enough to see the quantum effects. And vector space is taken as 2 dimension Hilbert Space. Photons can be in different polarisation states. First of all basis of the experiment should be determined. Here vertical polarisation and horizontal polarisation is taken as basis, it is represented as $|0\rangle$, $|1\rangle$ respectively.

$$|vertical\,polarized\,photon\rangle = |\updownarrow\rangle = |0\rangle = \begin{bmatrix}1\\0\end{bmatrix}, \qquad |horizontal\,polarized\,photon\rangle = |\leftrightarrow\rangle = |1\rangle = \begin{bmatrix}0\\1\end{bmatrix} \tag{3.29}$$

Form these basis vectors, diagonal polarised photon can be written in terms of basis vectors.

$$|diagonal\,polarized\,photon\rangle = |\nearrow\rangle = \alpha\,|\updownarrow\rangle + \beta\,|\leftrightarrow\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{3.30}$$

It is known that in quantum mechanics all states are normalized so that

$$\langle \nearrow | \nearrow \rangle = 1 = \Big(\alpha^* \langle 0| + \beta^* \langle 1|\Big)\Big(\alpha |0\rangle + \beta |1\rangle\Big) \tag{3.31}$$

$$= \alpha^* \langle 0| \alpha |0\rangle + \alpha^* \langle 0| \beta |1\rangle + \beta^* \langle 1| \alpha |0\rangle + \beta^* \langle 1| \beta |1\rangle \tag{3.32}$$

$$= \alpha^* \alpha \langle 0|0\rangle + \alpha^* \beta \langle 0|1\rangle + \beta^* \alpha \langle 1|0\rangle + \beta^* \beta \langle 1|1\rangle \tag{3.33}$$

$$1 = |\alpha|^2 + |\beta|^2 \tag{3.34}$$

In this configuration the systems eigenstates are vertical and horizontal polarisation states. So every measurement in that basis will yield one of these basis. Now if $|\phi\rangle$ is an arbitrary polarisation state it can be written as a superposition of the basis vectors and if it is filtered with vertical polarised, $\left|\langle \updownarrow |\phi\rangle\right|^2$ will be the probability of the single photon passing through the filter. As it is mentioned in section 3.1, $\langle \updownarrow |\phi\rangle$ can be read as the amplitude that the state $|\phi\rangle$ becomes $|\updownarrow\rangle$ and its absolute value square is the probability for that event happens.If the photon success to pass the filter it will be no longer in the state of $|\phi\rangle$, it will be in the state of $|\updownarrow\rangle$ which is an eigenstate of the system.

After that, if an horizontal polarizer is applied, from the orthonormality of the basis the result will be 0, $\langle \leftrightarrow | \updownarrow \rangle = 0$. But if diagonal polarised filter is placed after the vertical filter, $\langle \nearrow | \updownarrow \rangle$, the result won't be equal to 0.

$$\langle \nearrow | \updownarrow \rangle = \Big(\alpha^* \langle 0| + \beta^* \langle 1|\Big)|0\rangle \tag{3.35}$$

$$= \alpha^* \neq 0 \tag{3.36}$$

Since a diagonal measure is done, to understand which basis the state is collapsed, another basis vectors should be defined, which includes state $|\nearrow\rangle$ as an eigenstate. This set of basis vectors is the one which it is mentioned in the equation **3.7**, vectors are $|\nearrow\rangle$ and $|\swarrow\rangle$. According to that equation α and β are equal to $\frac{1}{\sqrt{2}}$. Sp after the measurement state collapses to the eigenstate $|\nearrow\rangle$. Finally an horizontal measurement is done again $\langle \leftrightarrow | \nearrow \rangle$ will result different than zero and the photon, which finally ends up in the state $|\leftrightarrow\rangle$ can be seen in the screen.

This example shows that how qubits behave. The photon here, is seen as a basic unit of information which can be used in quantum computing, qubits.[10]

Qubits are quantum computational equivalent of classical bits. Qubits and bits have conceptional similarities however they are different mathematical. Using a quantum state as a qubit it should be *two-state system*. In two-state system, any arbitrary state can be in a superposition of the two independent state, as it seen in the above example. Another simple example for these systems may be a spin 1/2 particle such as electrons whose spins can be $+\hbar/2$ (spin up) or $-\hbar/2$ (spin down). So an arbitrary electron can be found or created in superposition of spin states up and down. These two-state (or two-level) systems are two-dimensional complex vector space.[34] For one qubit this space is denoted as "Bloch Sphere".

3.2.1 Bloch Sphere

Bloch Sphere which is introduced by Felix Bloch, is a geometrically representation of two-level quantum system whose states are $|0\rangle$, $|1\rangle$ or any complex combination of these two. Figure 3.10 shows these states clearly.[36]

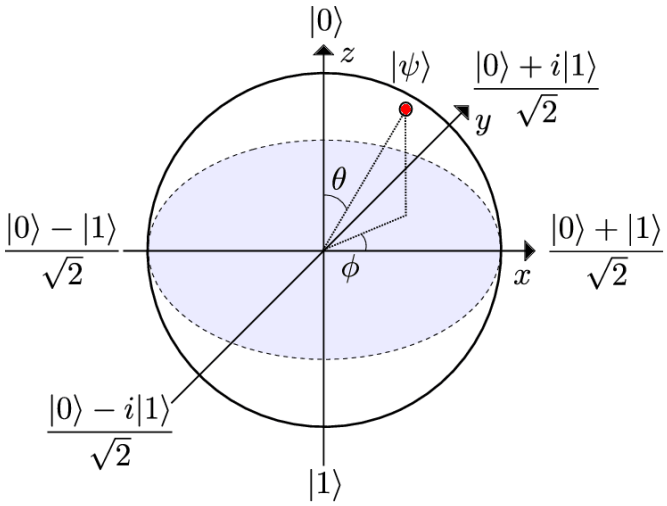


Figure 3.10: Bloch Sphere and some state of a qubit are shown on the sphere.

General representation of a state on a Bloch Sphere is

$$|\Psi\rangle = \cos(\frac{\theta}{2})\,|0\rangle + e^{i\phi}\sin(\frac{\theta}{2})\,|1\rangle\,, \tag{3.37}$$

Equation **3.37** is used to show mathematically any state of two-level quantum system.

3.2.2 Pauli Matrices

Qubits, are defined in two-dimensional *Hilbert Spaces*[37]. So observables associated with two-level systems should be defined by 2×2 matrices.

$$\hat{O} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

If basis vectors are taken as $|0\rangle$ and $|1\rangle$ then the values a, b, c and d are calculated as follows:

$$\hat{O} = \begin{bmatrix} \langle 0|\hat{O}|0\rangle & \langle 0|\hat{O}|1\rangle \\ \langle 1|\hat{O}|0\rangle & \langle 1|\hat{O}|1\rangle \end{bmatrix}$$

And any arbitrary can be written in terms of 3 *Pauli matrices* and an identity matrix. These Pauli matrices are:

$$\sigma_1 = \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_2 = \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_3 = \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{3.38}$$

3.3 Evolution of The Systems

Consider that a qubit system is realised, now the question will be how a state in this system evolves in time. Here quantum mechanics answer this question by the *Schrödinger Equation*:

$$i\hbar\frac{d|\Psi\rangle}{dt} = \hat{H}|\Psi\rangle \tag{3.39}$$

In this answer system is considered as *closed system* which means it does not interact with its environment. In fact this seems practically impossible but many cases which can be taken as very good approximation of a *closed system* may created. In equation **3.39** $\hat{H}$ plays very critical role. If the Hamiltonian of the system is known than the evolution of the system is a first order differential equation far away. From here it can be derived as follows, from time t_1 to t_2 :

$$|\Psi(t_2)\rangle = exp[\frac{-i\hat{H}(t_2-t_1)}{\hbar}]|\Psi(t_1)\rangle \tag{3.40}$$

If an operator $\hat{U}$is defined as $exp[\frac{-i\hat{H}(t_2-t_1)}{\hbar}]$ it will be unitary evolution operator of closed system.

3.4 Multiple Qubits

Just like, more than one bits needed to make on operation in classical computation, in quantum computation, more than one qubit is also needed. In quantum computation *Hilbert Space* is used as a complex vector space with finite dimension. It is known that for a two-level system like a qubit, dimension of the Hilbert space must 2. Additionally when two qubits are considered Hilbert spaces for each qubit H_1 and H_2 should be merged in order to have larger Hilbert space. This operation is done by *tensor product* which is denoted by $\otimes$.

$$H = H_1 \otimes H_2 \tag{3.41}$$

And dimension of H is the multiplication of the dimensions of two Hilbert spaces. Here it is 4 by 2×2 for two qubits system. If there exist n-qubit system then the dimension of the systems Hilbert space will be 2^n.

A state defined in H can be created by tensor product of the states defined in H_1 and H_2. If vector v_i and u_i are the basis vectors of the Hilbert spaces H_1 and H_2. Than

$$w_i = u_i \otimes v_i = v_i \otimes u_i \tag{3.42}$$

w_i is the basis vector for H. Additionally tensor product have properties like associativity, commutativity, and distributivity. Rather than using always the $\otimes$ symbol, a system of two qubits generally represented like $|\phi_1\phi_2\rangle$.

3.4.1 Entanglement

Now move forward to the one of the most critical part of the quantum computation, *quantum entanglement*. This is a feature that makes people dream about of quantum systems as a computational devices which offer an exponential speed-up over classical computation.[38]

In quantum mechanics, entanglement basically means a connection between two or more quantum states. More technically, if n entangled states are considered, measuring one of them perturb all states and rises also knowledge of all other states.

Most basic example of an entangled state is two qubit entangled state:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Here $|\Psi\rangle$ is a normalized entangled state. It can be seen the system is two qubit system and if the state of first qubit is known it is clear that second qubit will also be known.

So if polarised photons are taken as qubits, it becomes:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}|\updownarrow\updownarrow\rangle + \frac{1}{\sqrt{2}}|\leftrightarrow\leftrightarrow\rangle$$

From tensor products:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\Big(|\updownarrow\rangle \otimes |\updownarrow\rangle\Big) + \frac{1}{\sqrt{2}}\Big(|\leftrightarrow\rangle \otimes |\leftrightarrow\rangle\Big)$$

To distinguish better the qubits, subscripts can be written:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\Big(|\updownarrow\rangle_1 \otimes |\updownarrow\rangle_2\Big) + \frac{1}{\sqrt{2}}\Big(|\leftrightarrow\rangle_1 \otimes |\leftrightarrow\rangle_2\Big)$$

Now to find the amplitude that the state $|\Psi\rangle$ ends up with its first qubit vertically polarised, ${}_1\langle\updownarrow|\Psi\rangle$ should be calculated.

$${}_1\langle\updownarrow|\Psi\rangle = {}_1\langle\updownarrow|\Big[\frac{1}{\sqrt{2}}\Big(|\updownarrow\rangle_1 \otimes |\updownarrow\rangle_2\Big) + \frac{1}{\sqrt{2}}\Big(|\leftrightarrow\rangle_1 \otimes |\leftrightarrow\rangle_2\Big)\Big] \tag{3.43}$$

$$= \Big[\frac{1}{\sqrt{2}}\,{}_1\langle\updownarrow|\Big(|\updownarrow\rangle_1 \otimes |\updownarrow\rangle_2\Big) + \frac{1}{\sqrt{2}}\,{}_1\langle\updownarrow|\Big(|\leftrightarrow\rangle_1 \otimes |\leftrightarrow\rangle_2\Big) \tag{3.44}$$

The term ${}_1\langle\updownarrow|\Psi\rangle$ acts only the first term of the tensor products because it is not in the same space of the second qubits of the products. So it is easily seen that second part of the addition results zero. And the amplitude of the finding first qubit of the system in the vertical polarisation is $\frac{1}{\sqrt{2}}$ and the resultant state ends up with the state $|\updownarrow\updownarrow\rangle$. So this demonstration helps to visualise more how two qubits are connected to each other in a entangled state.

This strange phenomenon is named “spooky action at a distance” by Albert Einstein. [39] And it is subjected by him, Rosen and Podolsky. But in 1964 the reality revealed with John Bell’s proposed experiment which is realised after in few years.

4 Quantum Technologies in Quantum Computation

Quantum technologies are great collaboration of the physics and engineering. These technologies are developed by using quantum mechanical principles as it is mentioned in the section 3. In quantum computation these principles are applied on states of two-level quantum systems, qubit.

Here a quantum state can be described by the knowledge about a physical system. That knowledge is written in a ket vector or a density operator (equation **3.23**).[40] In order to realise realise a quantum computation some requirements are needed, these are known as *DiVincenzo's criteria*. A well defined qubits system is the first requirement and it is needed to initialise that qubit reliably. Then that qubit must maintain its state till the computation operations end. Also quantum mechanical operations, gates, which applied to the qubit must be defined. Finally the ability of measuring single and specific qubit is required to accomplish and trustable quantum computation. [34]

4.1 Type of Qubits

Quantum computation needs "well characterised" qubits. Here "well characterised" means the knowledge about physical parameters of the system. As it is already mentioned that any two-level quantum system can be used as an qubit, as long as they can be addressed, controlled, measured, coupled with nearby qubits and isolated from environment [41].

There are variety of different researches on realisation of quantum technologies for quantum computation. One of the main difference between the works is the qubit system they use. There are ion-traps, neutral-atoms, atoms in a lattice, photon in an optical cavity, spin states or charge state of quantum dots, superconducting devices and more.

In table 4.2 some of qubit systems is mentioned with their properties. Here Γ_Q is for decoherence time which means the time for qubit to loss its written information, distribution or noise, Γ_{op} is for the operation time of a transformation on a qubit and n_{op} is maximum number of operation. Here the 8 shown systems actually are based on 3 different qubit systems, spin, charge and photon. In ion trap and quantum dots the qubits is based on spins, in electron in gold and in gallium arsenide it is charge and finally in cavities it is photon. [1]

Table 4.2: Qubit systems and their properties.[1]

Systems	Γ_Q	Γ_{op}	n_{op}
Nuclear Spin	$10^{-2} - 10^{8}$	$10^{-3} - 10^{-6}$	$10^{5} - 10^{14}$
Electron spin	10^{-3}	10^{-7}	10^{4}
Ion trap (In+)	10^{-1}	10^{-14}	10^{13}
Electron – Au	10^{-8}	10^{-14}	10^{6}
Electron – GaAs	10^{-10}	10^{-13}	10^{3}
Quantum dot	10^{-6}	10^{-9}	10^{3}
Optical cavity	10^{-5}	10^{-14}	10^{9}
Microwave cavity	10^{0}	10^{-4}	10^{4}

4.1.1 Photons

Photons may be the one possible unit of information in quantum computation because of their ability of low loss transmission via optical fibers, make combinations with beamsplitters and delay with a phase shifters. They can also be made to interact with each other. [1]

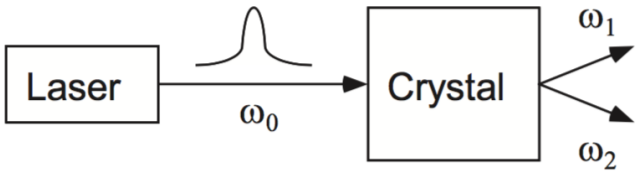


Figure 4.11: Generation of photon pairs. [1]

Scheme shown in the figure 4.11 is the concept to obtain qubits where the frequency w_o is equal to $w_1 + w_2$. And these qubits are manipulated by mirrors, phase shifters and beamsplitters which will be discussed in sec 4.4. [1]

4.1.2 Ion Traps

Ion-trap quantum computers, are first realised experimentally by J.I. Cirac and P. Zoller. [42] In this work they used N laser-cooled ions interacting with laser light and moving in a linear trap. Toy model of it is in the figure 4.12. Laser cooling method can be used with atoms to through electric dipole-dipole interaction. Ions are basic unit of information and they are manipulated by different laser beams for each ion, like it is shown in figure 4.13. Here the key part is to excite, manipulate single qubit ions must be separated from each other at a distance equal or more than wavelength of the beam. [1]

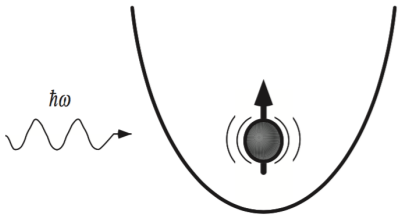


Figure 4.12: Toy model of ion in a trap.[1]

This method is the most promising quantum computation technology for realising systems of dozens of qubits in the predictable future. [43] Additionally it is more scalable in contrast to Nuclear Magnetic Resonance quantum computation has potentially has limited number of qubits.[44]

Figure 4.13: N ions, linear trap and laser for interacting with each ions.[42]

”An ion-trap quantum computer consists of a string of ions in a linear radio-frequency trap.”[43]

In *Demonstration of a Fundamental Quantum Logic Gate*, the most successful realisation in time [45], single $^9Be^+$ was used and its harmonic oscillator states and spin states were coupled to create quantum states and basis of these states were $|0\rangle|\downarrow\rangle$, $|0\rangle|\uparrow\rangle$, $|1\rangle|\downarrow\rangle$, $|1\rangle|\uparrow\rangle$. These states were manipulated by applying a pair of off-resonant laser beams.[46]

In ion-trap quantum computers, the drawback is any heat in the system can disturb the system and lead to have unreliability of the computation. [43]

4.1.3 Nuclear Magnetic Resonance

In nuclear magnetic resonance, the principle is the similar to the trapped ions, but here instead of ions molecules are trapped, which is more challenging task. Thanks to nuclear magnetic resonance technique manipulation and detection of nuclear spin states are done by using radio frequency electromagnetic waves.[1]

One of the popular physical system to do a quantum computation or build a quantum computer is the nuclear spin because it can be isolated from electronic and vibrational mechanisms which may disturb the system. [45] This method is based on the fact that the spins of each molecule of a liquid sample are independent from the spins of all other molecules. So each molecule can be considered as an quantum computer. Each molecules spins can be manipulated and the observations result the average expectation value over the ensemble, all molecules. [47]

4.1.4 Cavity Quantum Electrodynamics

In cavity QED, there is two way to represent a qubit, one is photon using nonlinear interaction with cavities atoms in it and the other one is atoms using interaction with photons.[1] Using atoms rather

than the ions has an advantage Since the neutral atoms do not have charges like ions do, their coupling with the environment is also weaker than the ions'. [48]

In the figure 4.14 neutral atoms are assumed as fixed, like trapped ions, in the quantum electrodynamic cavity and they are interacted, manipulated, with the individual laser beams.

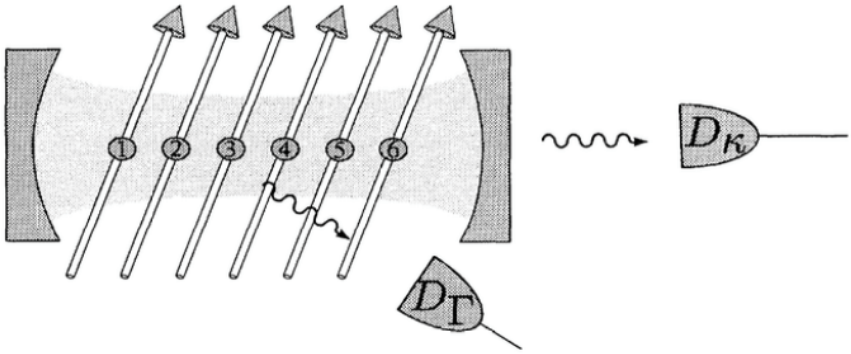


Figure 4.14: Scheme of the experimental setup of atoms in cavity.[49]

Arrows in the figure 4.14 stand for the laser beams interacting with each atoms. And D_K and D_Γ stands, respectively, for cavity photon and for simultaneously emitted photons [49] which are main source of the loss of the information.[48]

4.1.5 Spin States

By spin states most of the spin-$1/2$ states are considered; electron spin, nuclear spin. With technological developments quantum computers capabilities also rise. The methods given above are very successful for experimental usage and for several qubits systems but if 100 and more qubits are aimed then solid state computers have great potential. [50] Here qubits are electron spin states of quantum dots of the material, which refers quantum confinement, order of nanometers. In applications they are strongly coupled through a cavity.[50] In the figure 4.15, microdisk structure of experimental setup of quantum computer with quantum dots is shown. Here quantum dots are embedded in a microdisk of indium arsenide. Dots are coupled to single cavity mode. And each dot can be manipulated by a laser from a fiber tip.

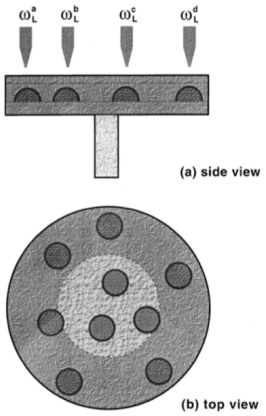


Figure 4.15: Experimental setup of embedded quantum dots.[50]

Nuclear spin states can also be used as an quantum computer in a semi-conductor, silicon. In his paper *A silicon-based nuclear spin quantum computer*, Kane explained how to make logical operations and measurements on nuclear spin qubits with controlling *hyperfine interaction* between electron and nuclear spin. [51] Kane's design which is shown in figure 4.16, is called spin-resonance transistor [52]. In the design Kane used nuclear spin of $^{31}P^{+}$ nuclei which are doped in silicon just below the "A gates" and electrons of the silicon are bounded to the $^{31}P^{+}$ nuclei. So this "A gates" controls the interaction between electron and $^{31}P^{+}$ which called *hyperfine interaction*. And there are also "J gates" which are used for the interaction between other qubits, by decreasing or increasing electrical potential barrier between them. Since the Kane's work, SRT has been designed also with different materials, germanium/silicon.[52]

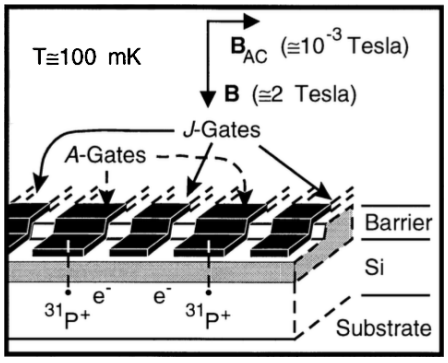


Figure 4.16: Structure of spin-resonance transistor (SRT). [51]

4.1.6 Superconductor

Imagine a qubit system realised with a classical LC oscillator circuit. The resistive effect of the circuit causes rapid decoherence and the information written will be lost. To prevent that superconducting circuits are good candidate for qubits. In superconductors charges is carried by electron pairs which are bound together via phonon interaction, which called *Cooper pairs*. Cooper pairs are a spin integer particles which can be classified as a boson. So cooling them close to the absolute zero leads to the Einstein-Bose condensation, in which all particles occupy same energy states, contrary to the fermions which are restricted by the *Pauli exclusion principle*. These cooper pairs carrier charge of 2e.[1, 53, 54]

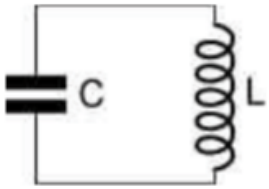


Figure 4.17: Classical LC electrical oscillator.[55]

If voltage equation is written for left side of the circuit

$$V = \frac{Q}{C}$$

and for right side

$$V = L\frac{di}{dt}$$

and with the relation $I = \frac{dQ}{dt}$ if Kirchhoff's voltage law is applied

$$\frac{Q}{C} + L\frac{di}{dt} = \frac{Q}{C} + L\frac{d^2Q}{dt^2} \tag{4.45}$$

From the equation **4.45** mathematical harmonic oscillator behaviour can be seen.

$$\frac{d^2Q}{dt^2} + \frac{1}{LC}Q = 0 \tag{4.46}$$

$$\frac{d^2Q}{dt^2} + w^2Q = 0 \tag{4.47}$$

$$w_r = \frac{1}{\sqrt{LC}} \tag{4.48}$$

LC oscillator can be seen as quantum harmonic oscillator, operators of flux and the charge stored in the system, across the inductor and the capacitor respectively, commute in a way that provides an analogy.[26]

$$[\Phi, Q] = i\hbar \tag{4.49}$$

From the equation **4.49** it can be seen that flux (Φ) is analogous of the position and charge (Q) is the analogous of the momentum for a particle. From the energy of inductor $\frac{1}{2}LI^2$ and $\Phi = LI$, from the energy of capacitor $\frac{1}{2}CV^2$ and $Q = CV$, Hamiltonian of the system can be written as follows

$$\hat{H} = \frac{\hat{\Phi}^2}{2L} + \frac{\hat{Q}^2}{2C} \tag{4.50}$$

where $\frac{\hat{\Phi}^2}{2L}$ stands for kinetic energy and $\frac{\hat{Q}^2}{2C}$ for potential energy. With the equation **4.50** evenly quantized levels of the harmonic oscillator can be easily seen.

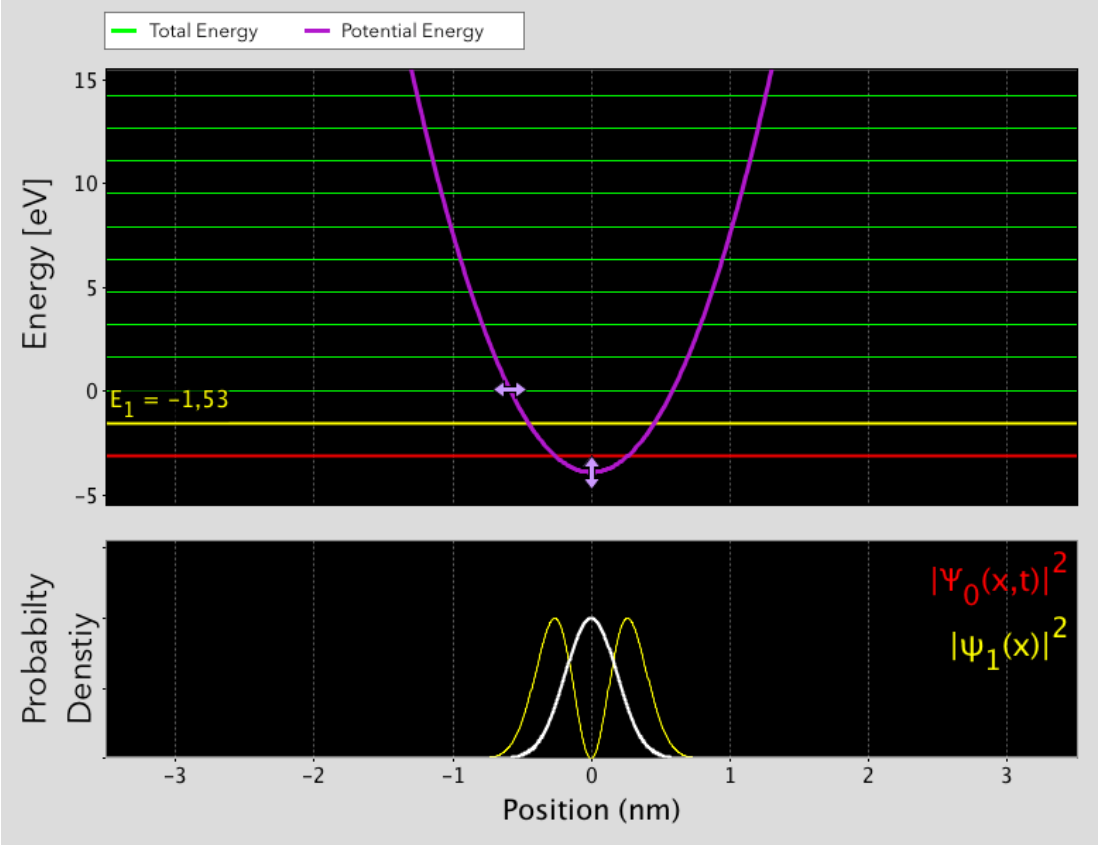


Figure 4.18: Quantum harmonic oscillator energy levels and probability density function.

The simulation in the figure 4.18 is done in "Quantum Bound States" simulation of the "Physics Education Technology project" (PhET) of the University of Colorado Boulder. In the figure 4.18 position axis can be seen as flux in the LC circuit case. Energy levels are separated evenly with value $\hbar w_r$

Now an anhormonicity is needed to create unevenly separated levels to use lowest two of them in quantum computing process. And this is done by *Josephson junctions*. Josepshon junction consist a thin layer of insulator between the superconductor material, see the figure 4.19[26].

Leftmost of the figure 4.19 physical scheme of the Josepshon junction is shown. Here Cooper pairs are seen, n stands for electron density of superconductors and ϕ for superconducting phase. On the middle simple version of the scheme is given where junction current I and junction capacitance C are depend on the thickness of the junction. Finally rightmost picture simplest way to represent a Josephson junction, which is X.

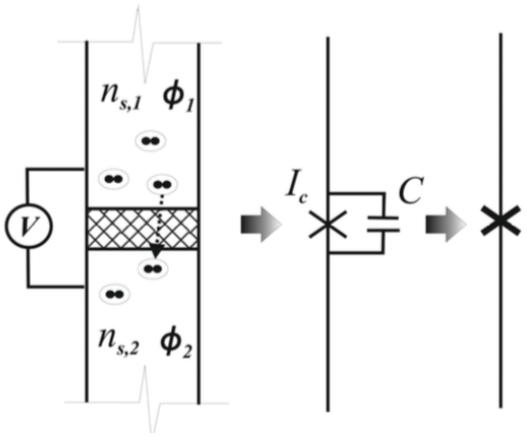


Figure 4.19: Representation of Josepshon junction.[56]

In superconductor circuits, cooper pairs can be manipulated by macroscopic elements like inductor and capacitor in a way that qubits can be constructed. Superconductors coupled with *Josephson tunnel junction* shows *quantum tunnelling* effect. With which junction provides quantized tunnelling of charges. So two level quantum system can be created only if the transition frequency between the energy levels 0 and 1 different than the those between 1 and 2.

There

In a superconductor circuit, qubits can be in 6 different types, there of them are fundamentals charge, phase, flux, their circuit representation is given in figure 4.21. There are also extended versions quantronium, fluxonium and transmon qubits. Potential energies and qubit states of three fundamental superconductor qubits are given in figure 4.20.

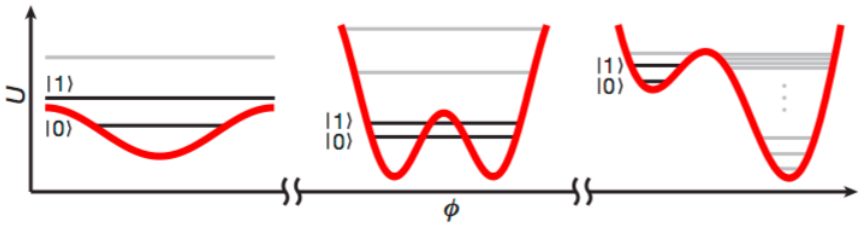


Figure 4.20: Potential energies of fundamental superconductor qubits. Left to right, charge qubit, flux qubit and phase qubit.[26]

There is an important ratio E_j/E_c where E_c stands for charging energy of the junction and the E_j for the junctions energy. This ratio shows the sensitivity of the qubit to flux and charge fluctuations. This ratio is much lower than 1 for charge qubits. In flux qubit, (also called persistent-current qubit) circuit has design in order to create double-well potential. [26]

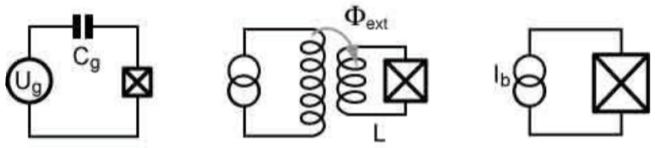


Figure 4.21: Circuit representation of fundamental superconductor qubits, Left to right, charge qubit, flux qubit and phase qubit.[55]

4.2 Initialisation

Then there is second requirement which is about initialising the quantum states. This one is based on the reliability of the qubit. The initial state of the qubit must be well known before starting the computation. This initialisation can be done in many different ways according to type of the qubit of the system. In a qubit systems realised with quantum dots use a large voltage difference is applied to equalise the charge distribution. [57] Initialisation problem is the one of the biggest challenge of the quantum computational systems. Daniel Loss and David P. DiVincenzo mentioned this problem as "state-preparation problem". In their paper the problem, initialising all spins of the quantum dots as spin-up, is done by cooling the system in *cryogenic temperatures* (at or below $150^{\circ}C$)[58] Cooling method is very popular method to prepare qubits in their ground state which also used in ion trap computers, QED qubits and nuclear magnetic resonance computers[45, 42, 48]. In addition, in nuclear spin qubit state in a semiconductor as it is shown in figure 4.16 initialisation is done by calibrating A and J gates. [51]

4.3 Decoherence

Decoherence times characterise the dynamics of a qubit or any quantum system in contact with its environment.[34] In practice every quantum system is open, they can never be perfectly isolated.[53] Longer decoherence times, longer than the gate operations are third requirement of realisation a quantum computer. By explaining these requirements, David P. DiVincenzo gave a definition of decoherence which corresponds the time for an arbitrary state $|\Psi\rangle = a|0\rangle + b|1\rangle$ transform to the mixture $\rho = |a|^2 |0\rangle\langle 0| + |b|^2 |1\rangle\langle 1|$.[34] The term decoherence which corresponds *quantum-noise* also provides the difference between quantum and classical world. With a certain decoherence times quantum systems start to show classical properties. This is one of the explanation of why quantum mechanical features do not seen in daily life. [53]

For example in ion trap quantum computer, simultaneously emitted photons destroy the coherence of the system, just like D_{Γ} in th example of neutral atoms in cavity (figure 4.14).[53]

Decoherence may lead the amplitudes change of a superposition state and other quantum states of the system may arise. These are form of state decay and in terminology it is called *leakage*. [34] Decoherence also may destroy the quantum interference which is essential for computation. [46]

Decoherence time mentioned here must be relevant with the qubit. For example it is irrelevant to talk about spin decoherence time of an electron if its charge is used as a qubit. Here quantum computation has nothing to do with electrons spin decoherence.

Different types of decoherence, bit flip or phase flip, may also be described by basic unitary gates which will be mentioned in the section 4.4.

Long decoherence times are essential for quantum computation. Otherwise decoherence may lead

to lose quantum features of the computation. Decoherence time must be long and how long must it be depend on qubit system and the quantum error correction technique of the system. With quantum error correction, accepted decoherence time can be calculated within the limits of fault tolerant quantum computation. [34]

4.3.1 Quantum Error Correction

Quantum error correction has some differences from the classical error correction. In classical, *Shannon's noisy-channel coding theorem* shows how to reduce errors in a channel by increasing amount of the information transmitted.[59] So, in classical error correction copying an information is used frequently but in quantum error correction this technique can not be used due to the no-cloning theorem. That is to say there is no perfect duplication of an unknown state in quantum computation. [60] Classical error correction also includes full knowledge of every information transmitted but in quantum mechanics that leads to collapse of the system to the measurement basis.[54]From here it can be understand that quantum error correction must be done in a way that any of the information in a quantum state is not measured, detected or determined. From the decoherence, it is known that error in quantum computation is something more than the one in classical computation since in quantum computation error may be occur in phase or amplitude of a qubit and it may also flip the qubit just like in classical computation.

To overcome quantum mechanical restrictions in error correcting techniques, Quantum error correction uses a technique which maps needed minimum Hilbert space to a Hilbert space with larger dimension. Basics of quantum error correction can be explained in three different section, these are *the three-qubit bit flip code*, *the three-qubit phase flip code* and *the nine-qubit Shor code*. There also different techniques of quantum error correction which will not be mentioned here.

The three-qubit bit flip code
Consider a superposition state of $|\Psi\rangle$

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

To protect this state, basis vector are encoded in *logical states*, $|0_L\rangle$ and $|1_L\rangle$. Here Logical states (also called as *codewords*) are defined with two additional qubit.

$$|0\rangle \mapsto |0_L\rangle \qquad |1\rangle \mapsto |1_L\rangle \tag{4.51}$$

Then superposition state turns to

$$|\Psi\rangle = \alpha|0_L\rangle + \beta|1_L\rangle \tag{4.52}$$

Here $|0_L\rangle$ and $|0_L\rangle$ are equal to the vectors $|000\rangle$ and $|1111\rangle$, respectively. This encoding is physically done by two CNOT gates and two qubits which are initially set up to their ground state as it is shown in figure 4.22.

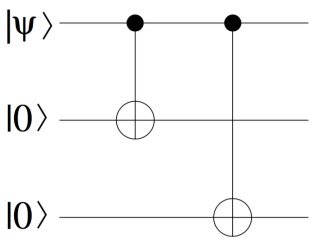


Figure 4.22: Encoding single qubit into three.[53]

With the given topology $|\Psi\rangle$ transform to the $|\Psi_L\rangle$

$$|\Psi_L\rangle = \alpha\,|000\rangle + \beta\,|11\rangle \tag{4.53}$$

If the state $|\Psi_L\rangle$ is exposed to a decoherence. say that single qubit flip probability is ε. Now all possible errors and its possibilities are given in the table 4.3

Table 4.3: State table of finite state Turing machine.

	Outcome states	**Probability**
No Error	$\alpha\,\|000\rangle + \beta\,\|111\rangle$	$(1-\varepsilon)^3$
Error 1	$\alpha\,\|100\rangle + \beta\,\|011\rangle$	$\varepsilon(1-\varepsilon)^2$
Error 2	$\alpha\,\|010\rangle + \beta\,\|101\rangle$	$\varepsilon(1-\varepsilon)^2$
Error 3	$\alpha\,\|001\rangle + \beta\,\|110\rangle$	$\varepsilon(1-\varepsilon)^2$
Error 4	$\alpha\,\|110\rangle + \beta\,\|001\rangle$	$\varepsilon^2(1-\varepsilon)$
Error 5	$\alpha\,\|101\rangle + \beta\,\|010\rangle$	$\varepsilon^2(1-\varepsilon)$
Error 6	$\alpha\,\|011\rangle + \beta\,\|100\rangle$	$\varepsilon^2(1-\varepsilon)$
Error 7	$\alpha\,\|111\rangle + \beta\,\|000\rangle$	ε^3

The number of qubit which can be corrected, t, is related to the *binary distance*, d, between two logical state. [60]

$$t = \left\lfloor (d-1) \times \frac{1}{2} \right\rfloor \tag{4.54}$$

which results 1 in this case.

So, if only single bit-flip error is considered only first 4 outcome of the table 4.3 will be taken into account. Two correct the error two ancillary qubits must be introduced with 4 additional CNOT gates as it is shown in figure 4.23. In the figure D_0 and D_1 are the measurement units of the qubits and they result x_0 and x_1 as classical bits 0 and 1.

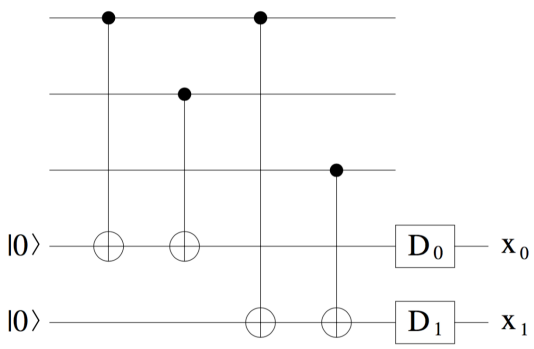


Figure 4.23: Ancillary qubits to detect the bit-flip error. [53]

Now let's see what how does it work on examples. Table 4.4 gives results of x_0 and x_1 and action must done to correct the error for the encoded state $|\Psi_L\rangle$ ends up with the error 1,2 and 3 in the table 4.3.

Table 4.4: Results of error correction.

Error No	x_0	x_1	**Action**
No Error	0	0	nothing
1	1	1	X gate to third qubit
2	1	0	X gate to second qubit
3	0	1	X gate to first qubit

With the action noted in table 4.4 the state $|\Psi_L\rangle$ remains unchanged than with a reverse operation of the gates shown in figure 4.22 the state $|\Psi\rangle$ will be save by bit-flip errors .

The three-qubit phase flip code The method seen above has nothing to do with the phase of the qubits. To correct a phase flip occurred to a superposition state first two different basis vectors are introduced.

$$|+\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big) \qquad |-\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big) \tag{4.55}$$

Relative phase flip in the basis $+,-$ corresponds to bit-flip $|+\rangle \mapsto |-\rangle$ and $|-\rangle \mapsto |+\rangle$. If initial state is same as above $|\Psi\rangle$ the encoded state $|\Psi_L\rangle = \alpha|+++\rangle + \beta|---\rangle$ should be created. And it is done by the quantum circuit given in the figure 4.24

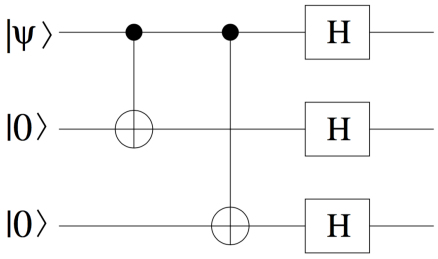


Figure 4.24: Encoding for phase-flip correction. [53]

The nine-qubit Shor code Shor code can be used to correct either of bit-flip or phase-flip errors or even for both of them. Quantum circuit of encoding in Shor code is shown in figure 4.25

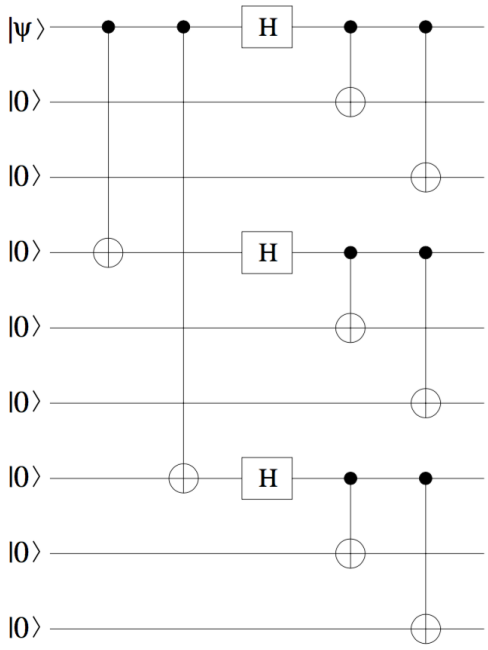


Figure 4.25: Encoding for Shor-code. [53]

The circuit in the figure 4.25 can be seen as the composite of the circuits in figure 4.22 and 4.24. Here first qubits $|0\rangle$ and $|1\rangle$ is mapped with a three qubit phase-flip code $|0\rangle \mapsto |+++\rangle$ and $|1\rangle \mapsto |---\rangle$. Then every qubit in these 3 qubits is encoded by three qubit bit-flip code $|+\rangle \mapsto (|000\rangle + |111\rangle)\sqrt{2}$ and $|-\rangle \mapsto (|000\rangle - |111\rangle)\sqrt{2}$.[1] So final result is

$$|0\rangle \mapsto |0_L\rangle = \frac{\Big(|000\rangle + |111\rangle\Big) \otimes \Big(|000\rangle + |111\rangle\Big) \otimes \Big(|000\rangle + |111\rangle\Big)}{2\sqrt{2}} \tag{4.56}$$

$$|1\rangle \mapsto |1_L\rangle = \frac{\Big(|000\rangle - |111\rangle\Big) \otimes \Big(|000\rangle - |111\rangle\Big) \otimes \Big(|000\rangle - |111\rangle\Big)}{2\sqrt{2}} \tag{4.57}$$

From here the encoded state $|\Psi_L\rangle$ will be

$$|\Psi_L\rangle = \frac{\alpha}{2\sqrt{2}}\Big(|000\rangle + |111\rangle\Big) \otimes \Big(|000\rangle + |111\rangle\Big) \otimes \Big(|000\rangle + |111\rangle\Big) + \tag{4.58}$$

$$\frac{\beta}{2\sqrt{2}}\Big(|000\rangle - |111\rangle\Big) \otimes \Big(|000\rangle - |111\rangle\Big) \otimes \Big(|000\rangle - |111\rangle\Big) \tag{4.59}$$

To correct the single qubit error occurred the correction circuit which is seen in figure 4.26 must be realised.

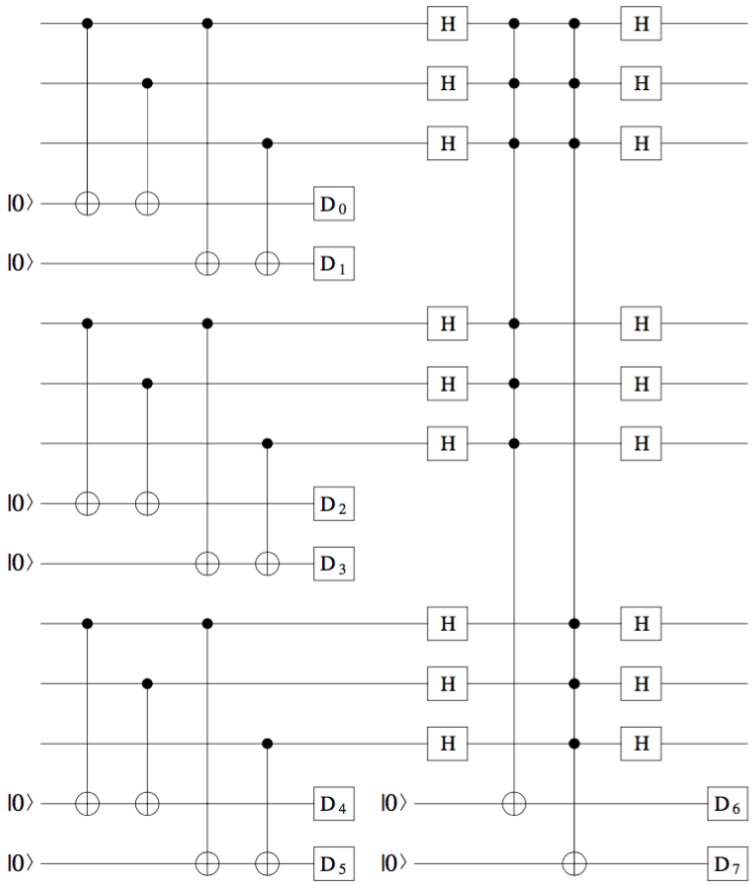


Figure 4.26: Correction circuit for Shor-code. [53]

4.4 Quantum Logic Gates

Quantum systems evolves in time respected to its hamiltonien as it is shown in section 3.3. Here the challenge is to control their hamiltonien as wished. Quantum logic gates are basic operation units that take places on quantum circuits. Just like their classical pairs performing on classical circuits.

Quantum circuits are one of the quantum computing models and this model will be taken as a base of this thesis. Other models are :

1. Measurement based quantum computation
2. Adiabatic quantum computation
3. Topological quantum computation

Quantum Turing Machine is also a model for quantum computation but its physical realisation can not be done for so far.

So for this thesis quantum circuits will take place. In quantum circuits computation is done by set of quantum logic gates.

These gates are

4.4.1 Hadamard (H) gate

Hadamard gate is a transformation acting on a qubits $|0\rangle$ and $|1\rangle$ and maps them to two different super position states, $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$.

$$\begin{aligned} H|0\rangle &= \frac{|0\rangle+|1\rangle}{\sqrt{2}} = |+\rangle \\ H|1\rangle &= \frac{|0\rangle-|1\rangle}{\sqrt{2}} = |-\rangle \end{aligned} \tag{4.60}$$

These superposition states generally noted as $|+\rangle$ and $|-\rangle$ respectively. These states can be seen clearly in the figure **3.37**. So it can be seen that Hadamard transformation is a unitary transformation which is a property of a quantum logic gate and it flips the initial state on a Bloch sphere on a way that the initial state vector can point the one of the super position state.

From the equations **4.60**, it can be derived the matrix representation of the Hadamard gate. To do that, $\langle 0|H|0\rangle$, $\langle 1|H|0\rangle$, $\langle 0|H|1\rangle$ and $\langle 1|H|1\rangle$ should be calculated. Then it can be written in the matrix form in the basis of $\{|0\rangle, |1\rangle\}$ according to the equation **4.60**.

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{4.61}$$

Hadamard gate is a single qubit operation. In IBM's Q experience (IBMqx) service, H (Hadamard) gate represented as a small blue square and after that to see what H gate did the qubit should be measured and it is done with a small pink square on the same qubit, shown in figure 4.27.

Figure 4.27: IBMqx composer, H gate acting on the first qubit which is in its ground state, $|0\rangle$.

After the setting up the topology, the circuit can be run to see the measurement result. After the measurement is done, IBM Q experience shows up a screen of quantum results. In that screen the result of the experiment is shown in a histogram like it is shown in the 4.28.

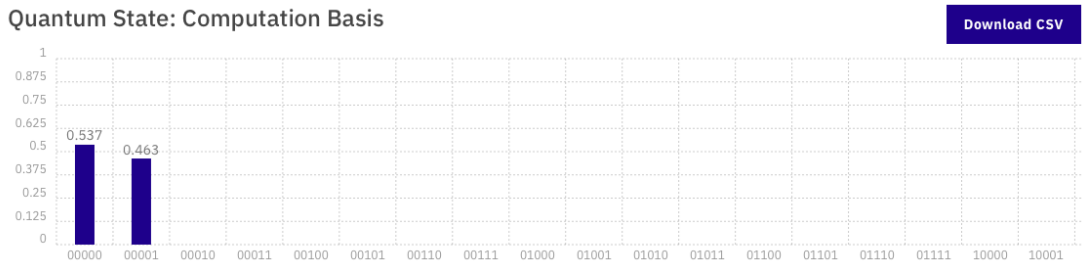


Figure 4.28: Result of the experiment shown in figure 4.27.

From figure 4.28, it can be understood that the result of the experiment is $|00000\rangle$ with a probability of 0.537 and $|00001\rangle$ with a probability of 0.463. This is very close to the theoretical result obtained by $H|0\rangle$ operation,

$$H|00000\rangle = \psi = \frac{1}{\sqrt{2}}|00000\rangle + \frac{1}{\sqrt{2}}|00001\rangle \tag{4.62}$$

$$P(\psi = |00000\rangle) = (\frac{1}{\sqrt{2}})^2 = 0.5 \tag{4.63}$$

$$P(\psi = |00001\rangle) = (\frac{1}{\sqrt{2}})^2 = 0.5 \tag{4.64}$$

This transformation can is shown in a Bloch Sphere in figure 4.29. Here initial state is seen in the left sphere and Hadamard gate is a rotation 180° rotation about the dotted axis shown which is $\frac{\hat{x}+\hat{z}}{\sqrt{2}}$.

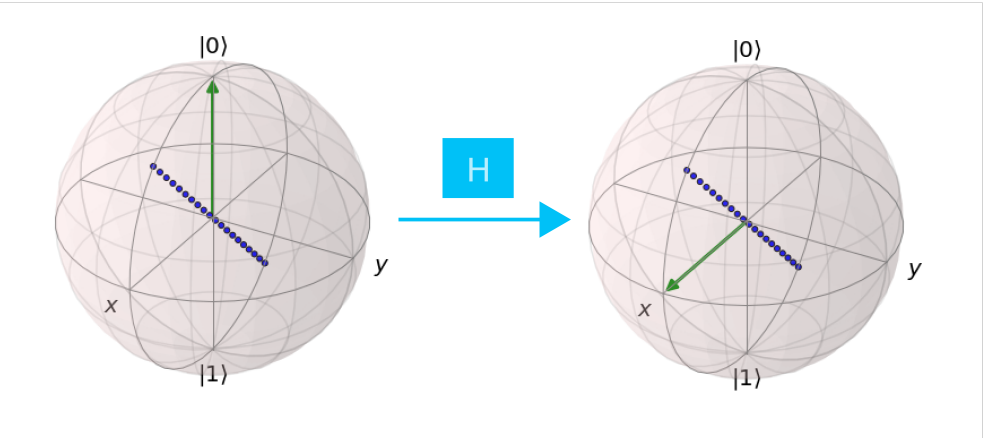


Figure 4.29: Hadamard gate transformation on a Bloch sphere.

4.4.2 Pauli-X gate

Pauli X gate has a direct classical equivalent which is a not-gate. Transformation done by X gate is mapping basis on to another, $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$ which can be also seen easily from its matrix representation, the equation **4.65**.

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{4.65}$$

This gate is applied and measured as it is shown in the figure 4.30 in the IBM Q experience and its result is in the figure 4.31.

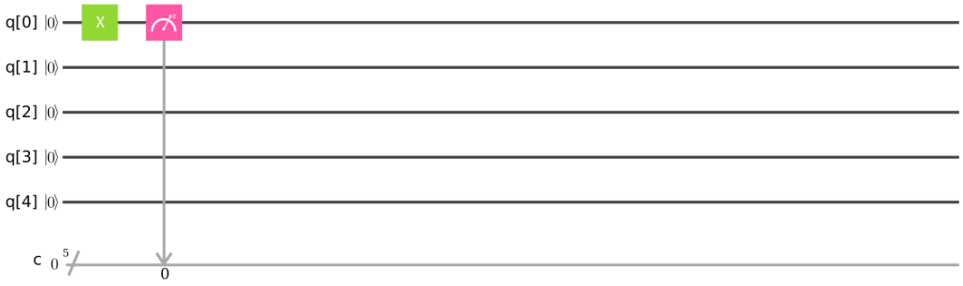


Figure 4.30: X gate on the IBMqx composer.

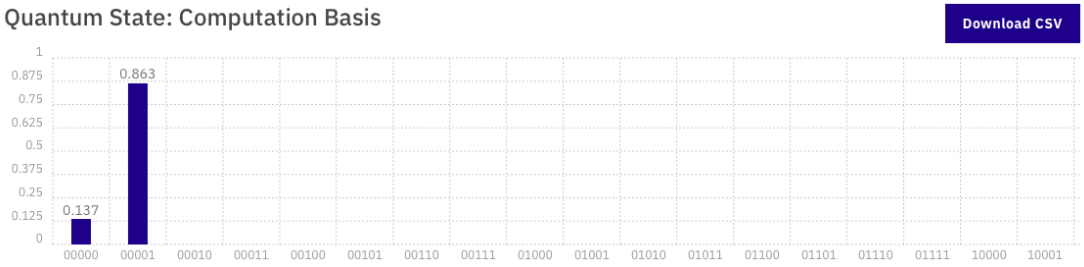


Figure 4.31: Result of the experiment.

Again this unitary transformation can be shown in the Bloch sphere in the figure 4.32. Dotted axis is the rotation axis, X gate transformation is 180° rotation about that axis.

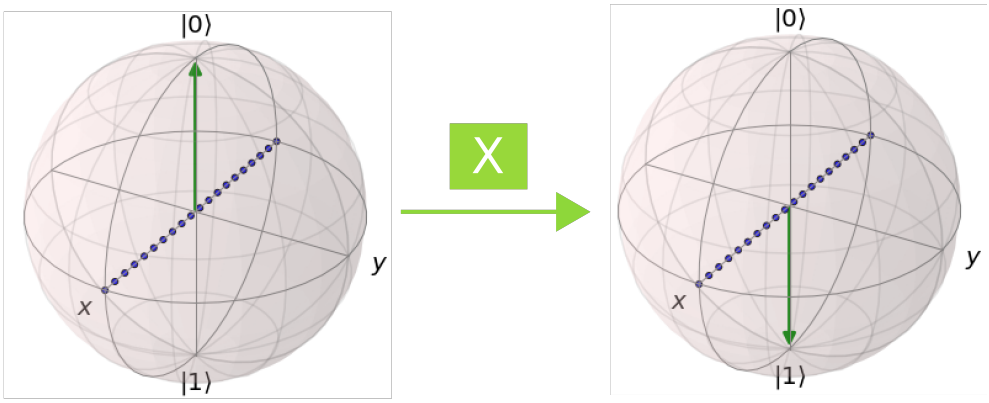


Figure 4.32: X gate transformation on a Bloch sphere.

4.4.3 Pauli-Y gate

Similar to X gate Y gate is a rotation transformation around Y-axis with an angle equals to 180°. Matrix representation of the gate is shown.

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \tag{4.66}$$

As it is understood from the matrix Y gate transforms the state $|0\rangle$ to $i|1\rangle$ and the state $|1\rangle$ to $-i|0\rangle$

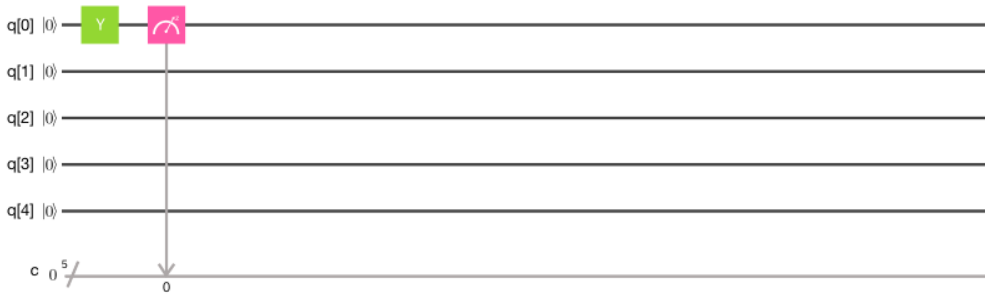


Figure 4.33: Y gate application on IBMqx.

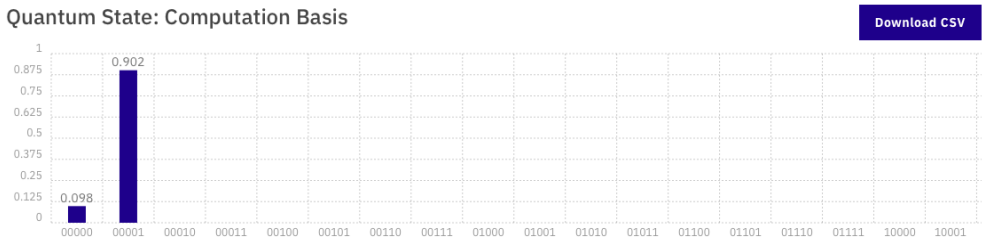


Figure 4.34: Y gate applications results.

4.4.4 Pauli-Z gate

Z gate is a rotation around Z-axis which leaves ground state ($|0\rangle$) unchanged and changes phase of the excited state ($|1\rangle$) to $-|1\rangle$.

$$Z = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{4.67}$$

Like all other Pauli gates Z gate is also one qubit gate and it is unitary. Quantum circuit representation of the Z gate is shown in the figure 4.36

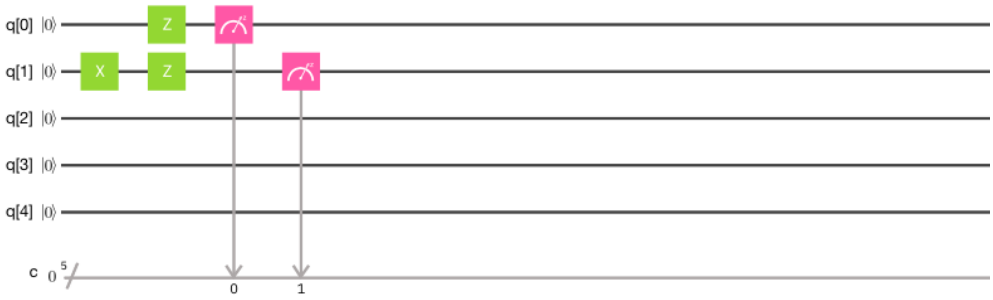


Figure 4.35: Z gate application on IBMqx.

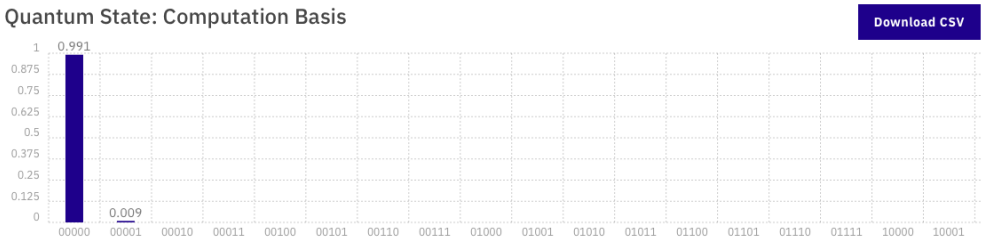


Figure 4.36: Z gate applications results.

In the application first qubit in the state $|0\rangle$ is applied with Z gate which leave the state unchanged and the second qubit which flipped to the state $|1\rangle$ applied with Z gate and its phase is changed. But in the measurement phase is not seen so in the figure 4.36 it seen seen that both gate are kept unchanged.

4.4.5 Phase shift

Phase shift gate is a single qubit gate which does nothing to the state $|0\rangle$and rotates the state $|1\rangle$ around Z-axis with an angle ϕ. It's matrix representation is as follows

$$R_\phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix} \tag{4.68}$$

With this transformation probabilities to find the states do not change because this transformation only changes the phases of the amplitude which is cancelled when the absolute square is calculated.

Pauli Z gate is indeed a phase shift gate with the rotation angle $\phi = 180^\circ$ ($Z = R_\pi$). Other common rotations are $\phi = 90^\circ$ and $\phi = 45^\circ$ which have special names like **S gate**($R_{\frac{\pi}{2}}$) and **T gate**($R_{\frac{\pi}{4}}$), respectively.

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \qquad T = \begin{bmatrix} 1 & 0 \\ 0 & \frac{(1+i)}{\sqrt{2}} \end{bmatrix} \tag{4.69}$$

4.4.6 Controlled NOT Gate

Controlled NOT gate, unlike previous gates, is a two qubits gate. It should be two qubit system before applying Controlled Not gate. The truth table of the controlled NOT gate is given below.

Initial State	Final State
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$

Matrix representation of C_{NOT} is

$$C_{NOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{4.70}$$

C_{NOT} transformation can be represented mathematically

$$C_{NOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X \tag{4.71}$$

where I is the identity matrix and the X is the Pauli X gate matrix.

C_{NOT} is also capable to create entangled state from unentangled state and since its reverse is also equal to itself, it can also create an unentangled state from an entangled state. Let's see this from with an example, let's say a superposition state is created with a Hadamard gate acted on a ground state $|0\rangle$. Then the state $\sqrt{\frac{1}{2}}(|0\rangle + |1\rangle)$ is obtained. Now if an other qubit take into account with its initial ground state, obtained state must be tensor product of previous state and $|0\rangle$.

$$|\Psi\rangle = \left[\sqrt{\frac{1}{2}}(|0\rangle + |1\rangle)\right] \otimes |0\rangle \tag{4.72}$$

$$= \sqrt{\frac{1}{2}}(|00\rangle + |10\rangle) \tag{4.73}$$

Now act this unentangled state with C_{NOT} gate.

$$\begin{aligned} C_{NOT}|\Psi\rangle &= C_{NOT}\sqrt{\frac{1}{2}}(|00\rangle + |10\rangle) \\ &= \sqrt{\frac{1}{2}}(|00\rangle + |11\rangle) \end{aligned} \tag{4.74}$$

And entangled state is obtained. This example can be simulated in IBMqx as follows:

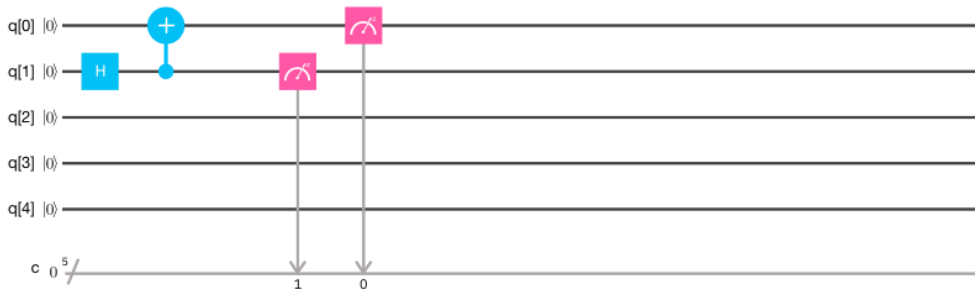


Figure 4.37: Creating entangled state.

Here q[1] is first qubit which Hadamard gate is applied then controlled with a C_{NOT} gate and q[0] is the second qubit which is flipped when the first qubit is in the state 1. The results can be seen when the circuit run.

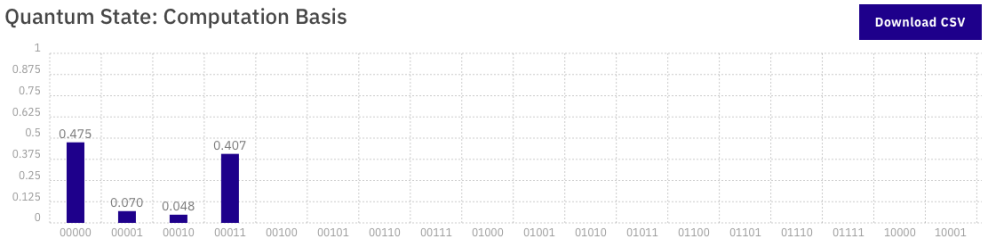


Figure 4.38: Result of the example.

From the results in the image 4.38 show that the final state is same as it is calculated before in the equation **4.74**. This state also known as Bell state and Hadamard gate with C_{NOT} gate together can be named as Bell gate which is named after the British physicist John Stewart Bell who proved that quantum physics does not have a hidden variable, like it is assumed in EPR theorem.

4.4.7 Controlled gates

Controlled gate is not always a controlled not gate. It can be a controlled-X , Y or Z too. It is also exist a controlled rotation gate. So it can be understood that the function of controlled gate can be changed. Control step is done always in the same way and controlled qubit does not effect but second qubit can be acted by different function. So if it is generalised

$$C_f = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & f_{00} & f_{01} \\ 0 & 0 & f_{10} & f_{11} \end{bmatrix} \tag{4.75}$$

This matrix can be represented mathematically

$$C_f = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes f \tag{4.76}$$

4.5 Measurement

Final requirement is the ability of read out a specific qubit. In quantum mechanics there is no possible way to observe a state directly. In other words there is no way to know the parameters α and β in a superposition state $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$. [37]

Measurement in quantum system does not need to be a unitary transformation like in quantum gates. Since the measurement gates can be used as the final step of the calculation, destroying the state would not be a problem for the calculation done.[54] Measurement gates can be also used in another role in quantum computation which is *state preparation*. Rather than producing digital (classical bit) result of a measured qubit wave-function collapse of measurement phenomena lead to find the state in a well-defined /well-known state which is one of the eigenvalues of the system in the basis of measurement.[61]

Measurement also plays an important role in initialising a quantum state. To [62] Unlike it is mentioned above unknown quantum states can be estimated statistically. For this identical copies of the state must be prepared and they must be measured with several observables. This process called *quantum state tomography*. And set of observables for a complete determination of the density matrix of the state is called *quorum*.[63] In first sight, the idea of creating identical copies of a quantum state may be seen contradictory with the theorem of no-cloning of quantum mechanics. But the theorem do not prohibit copying a quantum state probabilistically.[64] With the impossibility of an ideal copy of a state, the rising question is how close the copy of the state will be to the original one. [65]

If the density matrix of a qubit is given as follows,

$$\rho = p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1| + \alpha|0\rangle\langle 1| + \alpha^*|1\rangle\langle 0|$$

It can also be written in the form of matrix

$$\rho = \begin{bmatrix} p & \alpha \\ \alpha^* & 1-p \end{bmatrix}$$

a measurement in the base of $|0\rangle, |1\rangle$ will result "0" with the probability of p and "1" with the probability of $1-p$. So the measurement nothing to do with the offdiagonal elements of matrix which emphasise decoherence of the mixed state.

There are also type of measurement which do not effect the quantum state which is measured. These are called *quantum non-demolition* measurement. QND measurements are aimed feedback-controlled initialisations and repeated readouts. [66] QND is used based on the design of the interaction between the measurement device and measured state in which the eigenstates of the measurement quantity's operator do not change while the measurement done. [67]

4.6 IBM's Quantum Computer

In the project IBM's quantum computers will be used for quantum computation applications. The devices are located in the IBM research lab and they can be reached via a cloud server.

In IBM's quantum computers physical qubit is fixed-frequency superconducting transmon qubit which is a Josephson-junction-based qubit that is insensitive to charge noise.[68] Transmon qubits are one type of charge qubit but its E_j/E_c ratio is unlike standard charge qubit (charge states), much greater than 1. This feature explains why they are insesitive to charge fluctuation. Fixed frequency is chosen in

order to reduce decoherence effect from the external magnetic field. [68]

The structure of the devices are silicon wafers with superconducting metals such as aluminium and niobium.[68]

The properties of the qubit such as gate errors, readout errors, relaxation time (T1) and coherence time (T2) are given in the composer section of the website, `https://quantumexperience.ng.bluemix.net`. Figure 4.39 and figure 4.40 are screen shots from composer page of the IBM's Quantum Experience.

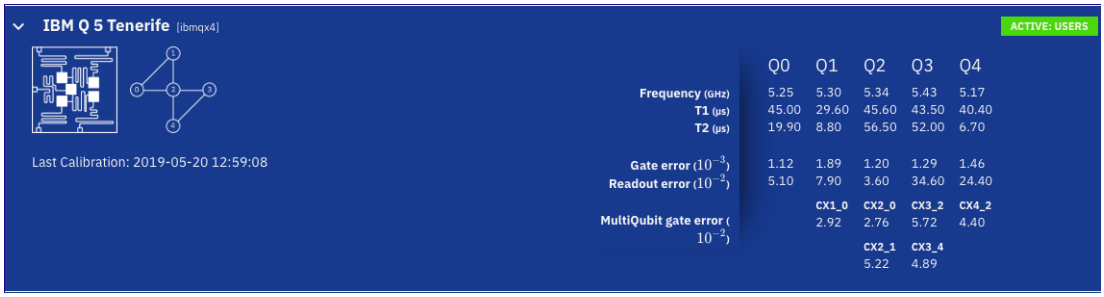


Figure 4.39: Properties of quantum computer, IBM Q 5 Tenerife (ibmqx4).

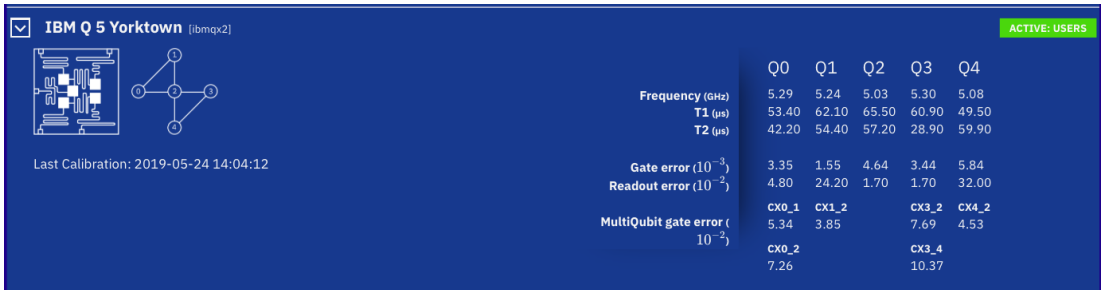


Figure 4.40: Properties of quantum computer, IBM Q 5 Yorktown (ibmqx2).

Qubits frequencies different from each other in order to addressing each of them individually. Fidelities of Single-qubit readout are $\sim 96\%$and $\sim 80\%$ for the average fidelity of readout for an arbitrary 5-qubit state. And 99.7% and 96.5% are for fidelities of typical gates for single- and 2-qubit gates, respectively. Gate times are 250–450 ns for 2-qubit gates and 130 ns for single, while coherence times are $\sim 60\mu s$ for both relaxation (T1) and coherence time (T2).[69]

Table 4.5: Characteristics of qubits, IBM Q 5 Tenerife (ibmqx4)

Qubit	$w_i^R/2\pi$ (GHz)	$w_i/2\pi$ (GHz)	$\delta_i/2\pi$ (MHz)	$\chi/2\pi$ (kHz)	$\kappa/2\pi$
Q_0	6.52396	5.2461	-330.1	410	-
Q_1	6.48078	5.3025	-329.7	512	-
Q_2	6.43875	5.3562	-323.0	408	-
Q_3	6.58036	5.4317	-327.9	434	-
Q_4	6.52698	5.1824	-332.5	458	-

Table 4.6: Characteristics of qubits, IBM Q 5 Yorktown (ibmqx2)

Qubit	$w_i^R/2\pi$ (GHz)	$w_i/2\pi$ (GHz)	$\delta_i/2\pi$ (MHz)	$\chi/2\pi$ (kHz)	$\kappa/2\pi$
Q0	6.530350	5.2723	-330.3	476	523
Q1	6.481848	5.2145	-331.9	395	489
Q2	6.436229	5.0289	-331.2	428	415
Q3	6.579431	5.2971	-329.4	412	515
Q4	6.530225	5.0561	-335.5	339	480

The table 4.5 and 4.6 are taken from `https://github.com/Qiskit/ibmq-device-information`. In the tables, $w_i^R/2\pi$ is the resonance frequency of the readout resonator. $\delta_i/2\pi$ is the anharmonicity, the difference between the frequency of the transition from level 1 to 2, vice-versa and the transition from 0 to 1,vice-versa. $\chi/2\pi$ and $\kappa/2\pi$ are for the strength of the couplings the qubit-cavity and cavity to its environment, respectively.

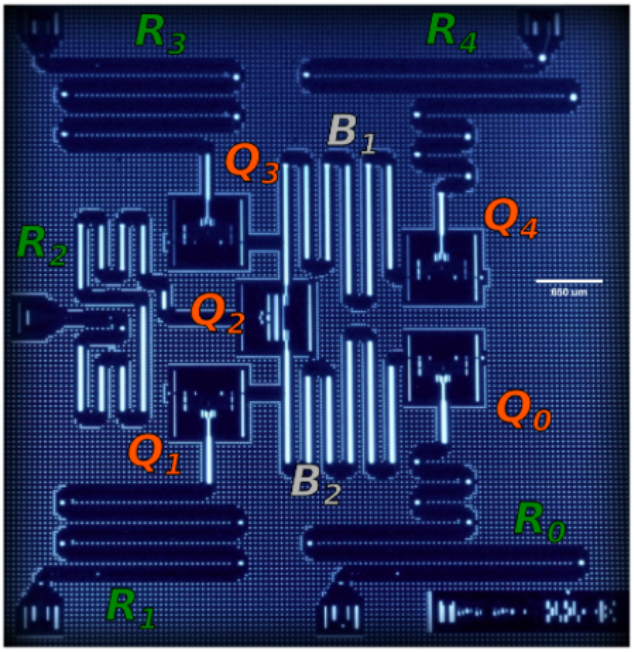


Figure 4.41: Quantum computing chip layout of both IBM Q 5 Tenerife (ibmqx4) and IBM Q 5 Yorktown (ibmqx2).

Figure 4.41 (`https://github.com/Qiskit/ibmq-device-information`) shows that how qubits are located physically. Here R_i for $i = 0, ..., 4$ represents coplanar waveguide (CPW) resonators to state preparation, readout and control qubits. Coupling between the qubits are provided by B_1 and B_2 with frequencies 6.6GHz and 7.0GHz, respectively.

In IBM Q experience measurements do not destroy the qubit's quantum state. So measurements are done by coupling weakly qubits to a microwave resonator. The resonance characteristic of the resonator is depend on the state of the qubit. So when "run" button is pushed quantum algorithm works and at the end of the process a microwave tone is send to qubit's resonators and the signal reflected back is analysed. The phase and the amplitude of the signal changes according to state of the qubit reflects

it. Before analysis the signals are amplified inside the dilution refrigerator which consist of quantum-limited amplifier at 15mk and a high-electron mobility transistor amplifier at 4 K.[68]

IBM's quantum experience cloud server has some rules. First of all to have an access to the quantum circuit composer it has to be a user. Every one can become a user and play in composer in order to explore quantum computation or search on quantum algorithms. One of the most useful feature of the IBM's quantum experience is that it can be rerun the experiments which are previously realised. The cached result from previously experiments prevent users to keep busy the real device. If someone is willing to run his/her circuit topology in the real device without using older experiments than there is a queue system which the eq/user should wait for his/her time to come up for the realisation of the experiment. When it is done, a notification system works to inform the experimentalist. This organisation works with units currency system. Every user have 15 units and the experiment value is depend on the shots wanted to run. Here shots emphasise how many times the experiment will be measured. There is also expert user mode which provides more credits and advanced features parallel with the systems development.

In the figure 1.1 IBM's quantum circuit composer is seen. To start from the bottom it must be said that quantum circuit diagram is one of the representation of quantum circuits, others are high level quantum languages and quantum assembly languages. [70] Here time goes from left to right and every line represent different timeline of a qubit. Another point needed to be mentioned is the connection or in other words coupling of the qubits in the system. The architecture of the qubits is shared by IBM (`https://github.com/Qiskit/ibmq-device-information`). In figure 4.42 and 4.43 relations between qubits are seen. Allowed two-qubit operations can be understood by this schemes in 4.42 and 4.43.

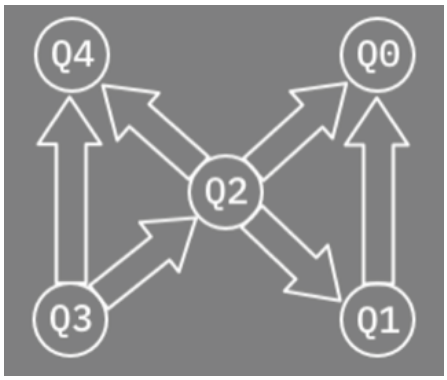


Figure 4.42: Architecture of the device IBM Q 5 Tenerife (ibmqx4).

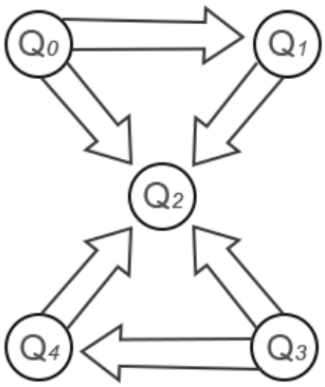


Figure 4.43: Architecture of the device IBM Q 5 Yorktown (ibmqx2).

Man-made quantum circuits of IBM's quantum computer can be seen as artificial atoms. They uses transmon qubits or the "superconducting islands" which are connected by shunt capacitors and Josephson junctions. Charge states superposition which are insusceptible to charge fluctuation can be created by this configuration.[69]

Other than ibmqx4 and ibmqx2 there is also *IBM Q 14 Melbourne* which has 14 qubits and available for public usages.

In its quantum computer IBM uses fixed-frequency superconducting transmon as a qubit which is a Josephson-junction-based qubit that is insensitive to charge noise. Fixed-frequency qubits are chosen to avoid corrupt quantum information which can be caused by external magnetic field fluctuations.

The properties of qubits which are given here, always up to date in devices section of IBM's Quantum Experience website, (`https://www.research.ibm.com/ibm-q/technology/devices/`).

5 Quantum Algorithms & Applications

5.1 Introduction to Quantum Algorithms

Quantum algorithms are step by step function which run on a quantum computer just like classical algorithms run on a classical computer. The distinguish between classical and quantum algorithms depend on the algorithms' requirement of a quantum mechanical features, like it is explained in section 3.

When the steps of an algorithms increase polynomial respect to the size of input, then it is classified as an efficient algorithm by the computer scientists. And the problems solved by these efficient algorithms are classified with the letter "P". There are also different classes, PSPACE, NP, BPP, $P^{\#P}$[71]. Definition of these classes is given in the table 5.7

Table 5.7: Some classes of problems and their definitions.

Problem Class	**Definition**
P	solved in polynomial time
PSPACE	solved in polynomial space
NP	solvable in polynomial time if solution is known otherwise it requires exponential space
BPP	solvable with a bounded probability of error time
$P^{\#P}$	solvable in polynomial time if sums of exponentially many terms could be computed efficiently

With the table 5.7, the equation **5.77** is derived.

$$\begin{aligned} P &\subseteq BPP \\ NP &\subseteq P^{\#P} \subseteq PSPACE \end{aligned} \tag{5.77}$$

The relation between BPP and NP is unknown. [71] With quantum algorithms one more class arises which is BQP, solvable by a quantum machine with a bounded probability of error time. This classification was the start point of the idea of powerful computing with quantum computers. In their paper, Ethan Bernstein and Umesh Vazirani became first who showed a problem which can be solved in polynomial time by a quantum computer and in super-polynomial time by a classical computer.[72] Here *integer factoring* and *discrete logarithms* problems come in sight. These problems don't have a polynomial-time solution in BPP but in BQP they have. [71]

5.2 Quantum Fourier Transform

Before passing the algorithms, a key concept must be introduced, Quantum Fourier Transform which enables transformations much faster than their classical pairs. Quantum Fourier Transform can be seen

same as *discrete fourier transform*.[1]

A quantum state $|\Phi\rangle = \sum_{j=0}^{N-1} |j\rangle$ can be transform as follows[73]:

$$|\Phi\rangle = \sum_{j=0}^{N-1} |j\rangle \longmapsto \sum_{j=0}^{N-1} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{-2i\pi jk}{N}} |k\rangle \tag{5.78}$$

so basis states transformation:

$$|j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{-2i\pi jk}{N}} |k\rangle \tag{5.79}$$

And operator for this transformation is given as

$$F_N = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{-2i\pi jk}{N}} |k\rangle \langle j| \tag{5.80}$$

For qubit systems where N is equal to 2^n where n is number of the qubit, state vectors can be represented like $|j_1 j_2 j_3 ... j_n\rangle$ so if these are put in the equation **5.79**

$$|j\rangle \mapsto \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{-2i\pi jk2^{-n}} |k\rangle \tag{5.81}$$

$$= 2^{-n/2} \sum_{k_1=0}^{1} \sum_{k_2=0}^{1} ... \sum_{k_n=0}^{1} e^{-2i\pi j(\sum_{m=0}^{n} 2^{n-m}k_m)2^{-n}} |k_1 k_2 ... k_n\rangle \tag{5.82}$$

$$= 2^{-n/2} \sum_{k_1=0}^{1} \sum_{k_2=0}^{1} ... \sum_{k_n=0}^{1} e^{-2i\pi j(\sum_{m=0}^{n} 2^{-m}k_m)} |k_1 k_2 ... k_n\rangle \tag{5.83}$$

It is also known that

$$|n_1 n_2 n_3 ... n_j\rangle = |n_1\rangle \otimes |n_2\rangle \otimes |n_3\rangle ... \otimes |n_j\rangle$$

and with binary fraction

$$0.j_1 j_2 j_3 ... j_n = j_1 \times 2^{-1} + j_2 \times 2^{-2} + j3 \times 2^{-3} ... + j_n 2 \times 2^{-n}.$$

finally transformation result as follows

$$|j\rangle \mapsto 2^{-n/2} \bigotimes_{m=1}^{n} \sum_{k_m=0}^{1} e^{-2i\pi j2^{-m}k_m} |k_m\rangle \tag{5.84}$$

$$= 2^{-n/2} \bigotimes_{m=1}^{n} (|0\rangle + e^{-2i\pi j2^{-m}} |1\rangle) \tag{5.85}$$

$$= 2^{-n/2} \Big[(|0\rangle + e^{-2i\pi j2^{-1}} |1\rangle) \otimes (|0\rangle + e^{-2i\pi j2^{-2}} |1\rangle) ... \otimes (|0\rangle + e^{-2i\pi j2^{-n}} |1\rangle) \Big] \tag{5.86}$$

$$= 2^{-n/2} \Big[(|0\rangle + e^{-2i\pi 0.j_n} |1\rangle) \otimes (|0\rangle + e^{-2i\pi 0.j_{n-1}j_n} |1\rangle) ... \otimes (|0\rangle + e^{-2i\pi 0.j_1 j_2 j_3 ... j_n} |1\rangle) \Big] \tag{5.87}$$

Such transformation can be realised by some basic quantum logic gates such as Hadamard and

rotation transformation which is given in section 4.4.

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i 2^{-k}} \end{bmatrix} \tag{5.88}$$

5.3 Shor's Algorithm

An important quantum algorithm, known as Shor's Algorithm is indeed a factorisation algorithm. An exertion, since almost the humanity starts to deal with the numbers, always is interested by mathematicians. Carl Gauss describe factorisation as "one of the most important and useful in all of arithmetic". [74]

Prime factorisation is a NP-class problem which has strong relations with cryptography. Cryptography will be examined in detail in section 6.2[75] Factorisation algorithms are one-way functions . Classically most efficient algorithm known to factoring an integer is *the number field sieve* which takes

$$\exp(c(\ln n)^{\frac{1}{3}}(\ln\ln n)^{\frac{2}{3}})$$

running time with some constant c.[76] Shor's algorithm do same task in polynomial time, exponentially faster than a classical equivalent.[1, 77] This speedup is illustrated in the figure 5.44

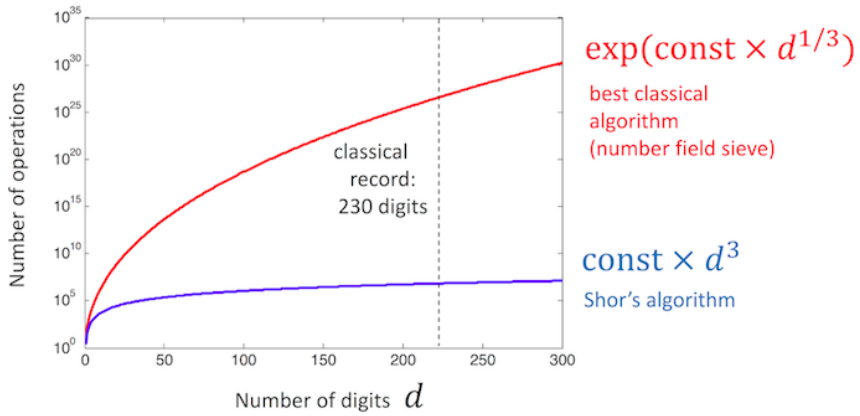


Figure 5.44: Quantum Factoring vs. Classical Factoring.[78]

Before moving on the quantum side of the algorithm basic concepts for number factorisation, *Euclid's algorithm* should be known. To start with, let's have a large integer N to be factorise. And take the number k such as $gcd(N,k) \neq 1$. So N and k are not coprime. So what Euclid's algorithm says that $gcd(N,k)$ is equal to greatest common divisor of the k and remainder of the calculation N/k, equation **5.89**.

$$\begin{aligned} gcd(N,k) &= gcd(k,r) \\ N &= k \times q + r \end{aligned} \tag{5.89}$$

And this procedure continues with k and r so that greatest common divisor of the r and the remainder of k/r calculation equals to $gcd(k,r)$. This iteration stops when the remainder of the division will rise 0.

For example let's take 147 as N and 66 as a. The steps of the calculation is given in the table 5.8

Table 5.8: Example of Euclid's algorithm.

Step	Equation	Values	Looking For
1	$147 = q \times 66 + r$	$q = 2,\ r = 15$	$gcd(147, 66)$
2	$66 = q' \times 15 + r'$	$q' = 4,\ r' = 6$	$gcd(66, 15)$
3	$15 = q'' \times 6 + r''$	$q'' = 2,\ r'' = 3$	$gcd(15, 6)$
4	$6 = q''' \times 3 + r'''$	$q''' = 2,\ r''' = 0$	$gcd(6, 3)$

From the table it is found that $gcd(147,66) = gcd(6,3) = 3$. Let's move on factorising, to do so a building block is needed, which is *modular exponentiation* from number theory. [54] If N and k are taken as coprime ($gcd(N,k) = 1$), there is always a number r which satisfy

$$k^r \bmod N = 1 \tag{5.90}$$

smallest r satisfy the equation **5.90** called *order* of the "k mod N". The equation can be rewrite as follows

$$\begin{aligned} k^r &= m \times N + 1 \\ k^r - 1 &= m \times N \\ (k^{r/2} - 1)(k^{r/2} + 1) &= m \times N \end{aligned} \tag{5.91}$$

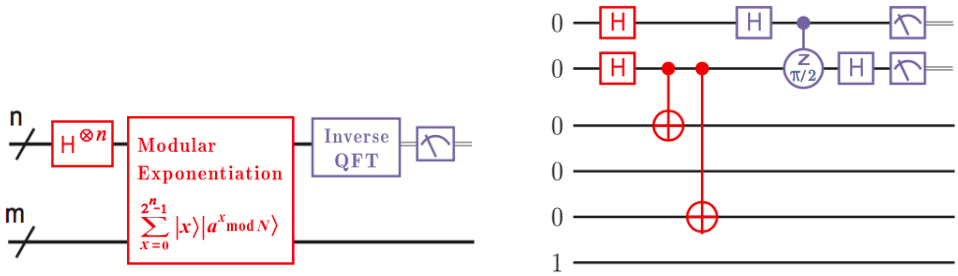
From the equation **5.91**, it is seen that either $(k^{r/2} - 1)$ or $(k^{r/2} + 1)$ can be one of the factors of the N. Otherwise there must be common divisors between $(k^{r/2} + 1)$ (or $(k^{r/2} - 1)$) and N. So it seems that if the value r can be calculated then the factors of N will be found easily. Number r is also period of the modular exponentiation function which is introduced in the equation **5.90**. It is called period cause it seen that $k^r \bmod N = 1$ also valid for k^{2r} or k^{nr} where n is a non-zero positive integer.

Let's try the algorithm so far by the integers relatively small. For example let's try to find the factors of 42, and let's have a first guess, 13. First condition $gcd(42,13) = 1$ is validated. So first thing is to find r.

$$\begin{aligned} 13^0 &= 1 \bmod 42 \\ 13^1 &= 13 \bmod 42 \\ 13^2 &= 1 \bmod 42 \end{aligned}$$

So it is found that r is equal to 2 and so $(k^{r/2} + 1)$ and $(k^{r/2} - 1)$ is equal to 14 and 12 respectively. So $gcd(42,14) = 7$ and $gcd(42,12) = 6$ rises the factors of the 42, $42 = 7 \times 6$.

From this basic example, it can be seen that quantum algorithms provide speedup where r is searched. So putting in a superposition all the numbers up to the 42 and find the module 42 of them and in the final step it should be find the frequency of the pattern repeated which is done with a inverse quantum Fourier transform (section 5.2).



(a) Outline of the algorithm

(b) Details of the algorithm. N=15, k=11

Figure 5.45: Shor's quantum factorising algorithm representation.[79]

Because of the technical restrictions Shor's algorithm cannot be done as an experiment in the IBM's Q experience service. But the *Modular exponentiation* part of the algorithm can be tested in the simulation of the service. This simulation is done based on the work of Markov and Saeedi [77].

The algorithm shown in figure 5.46 (called operator U_{13}) uses the equation $f(x) = 13x \bmod 15$ since $gcd(15, 13) = 1$. And it maps the input basis $|x\rangle$ to the state $|f(x)\rangle$.

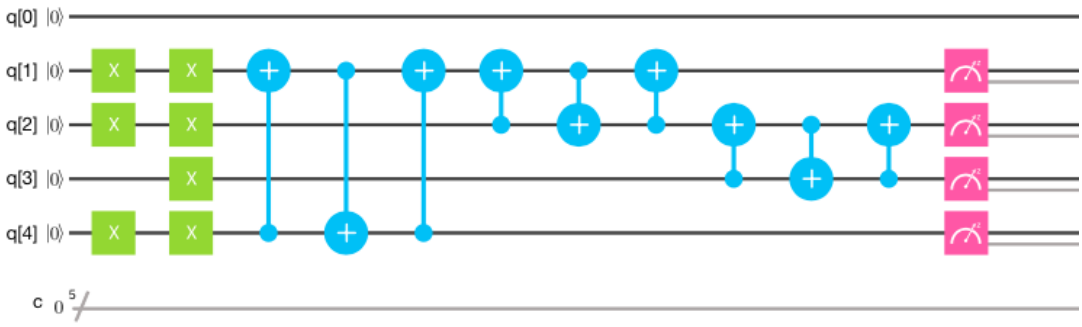


Figure 5.46: Modular exponentiation part of the Shor's algorithm. N = 15, k = 13.

The result of the simulation rises the state $|0100\rangle$ shown in figure 5.47

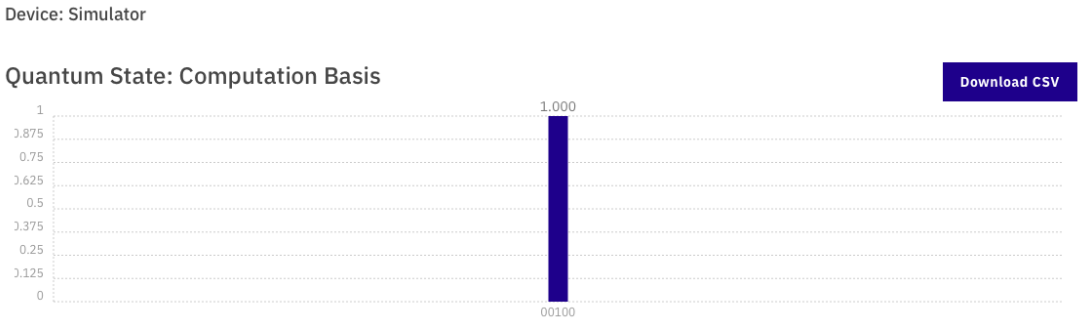


Figure 5.47: Result of the modular exponentiation simulation

Similarly, the function (operator U_{11}) can be shown. See figure 5.48 and 5.49

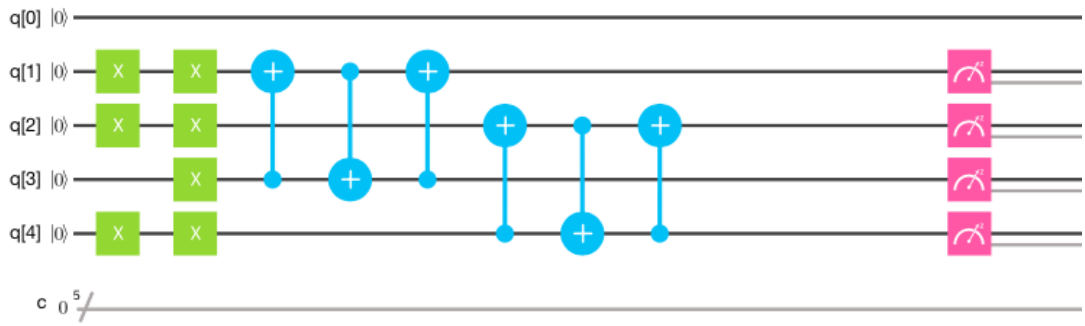


Figure 5.48: Circuit of the operator. $f(x) = 11x \bmod 15$, here x equals 13.

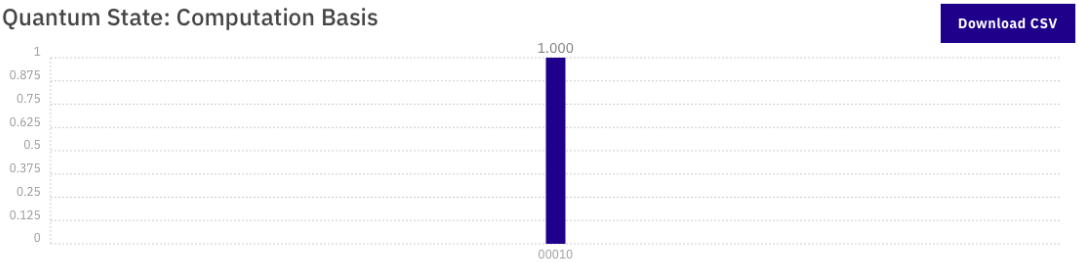


Figure 5.49: Result of the operator $U_1 1\,|1011\rangle$.

In the circuits first column of the X matrices define x of the function. Second column stands for $15(|1111\rangle)$ in both cases. The rest of the circuit is the configuration taken from the ref. [77], they are different for 13, 11 or 7.

In order to find the period of the $13^r \bmod 15$ with a good probability the operator U_j must be applied where $j = 0, 2, 4.., 2(2n-1)$, n is equal to number of the digits of $N = 15$. This algorithm is also shown in figure 5.50

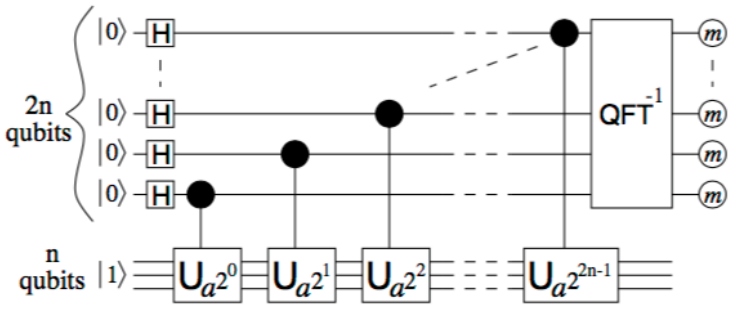


Figure 5.50: Period finding algorithm, the quantum mechanical side of the Shor's factorising algorithm.

5.4 Grover's Algorithm

One of the superiority of quantum computers is making search in a database. It is also called *quantum search algorithm* but the name Grover's algorithm which is refered to the Lov K. Grover who discov-

ered the algorithm in 1997. Grover's search algorithm can also be potentially used in NP-complete problems.[80].

Consider that there is an unstructured list and one element of the list wanted to be found. Say that there is N elements and they are numbered as it is seen in figure 5.51.

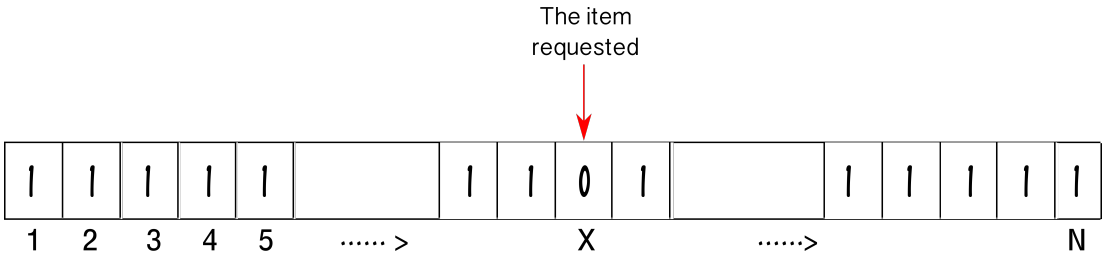


Figure 5.51: Unstructured List.

Classically to find the item requested on average $N/2$ trials will be sufficient. Grover's algorithm shows that it can solve this in $\sqrt{N}$ trials. In computer science terminology the problem which takes $O(N)$ computation times is converted to the problem which takes $O(\sqrt{N})$ computational times with the quantum search algorithm.[80]

To tell more about Grover's algorithm it is needed to understand how it works. First term it is encountered is the *black box* or *oracle*. In the searching problem oracle function is a function which maps to qubit label to the qubits value itself.[80]

$$f(x) = \begin{cases} 1, & \text{if x is the index of the item requested.} \\ 0, & \text{if x equal to any other index.} \end{cases} \tag{5.92}$$

So it is times to convert oracle function to a unitary matrix, which is represented here with a operator $\hat{U}_f$. Consider a state of the index x, $|x\rangle$ and an additional qubit (oracle qubit), $|q\rangle$.

$$\hat{U}_f |x\rangle |q\rangle = |x\rangle |q \oplus f(x)\rangle \tag{5.93}$$

where $f(x)$ is the oracle function which is given in equation **5.92**. When additional qubit set in a superposition state,

$$|q\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{5.94}$$

then the application of the $\hat{O}$ will give

$$\hat{U}_f |x\rangle |q\rangle = \hat{U}_f |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{5.95}$$

$$= (-1)^{f(x)} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{5.96}$$

So if the additional qubit is ignored then

$$\hat{U}_f |x\rangle = \begin{cases} |x\rangle, & x \neq x_0 \\ -|x\rangle, & x = x_0 \end{cases} \tag{5.97}$$

where x_0 is the item requested. It can be seen that phase of the solution is experienced a phase flip operation. Form here an operator $\hat{U}_{x_0}$ can be defined as $\hat{U}_{x_0} = \mathrm{I} - 2|x_0\rangle\langle x_0|$ where I is the identity matrix.

Now another operator must be introduced. But before that a state of superposition must be created.

$$|\psi\rangle = H^{\otimes n}|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \tag{5.98}$$

Equation **5.98** defines uniform superposition of all states. For example, say that there are 2 qubits. Than $|\psi\rangle$ is

$$|\psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \tag{5.99}$$

An operator $\hat{U}_\psi$ can be defined as $\hat{U}_\psi = 2|\psi\rangle\langle\psi| - \mathrm{I}$ where I is the identity matrix. With these information Grover's operator is introduced as follows,

$$\hat{G} = \hat{U}_\psi \hat{U}_{x_0} \tag{5.100}$$

Here the operator $\hat{U}_{x_0}$ changes the phase of the qubit to the minus and the operator $\hat{U}_\psi$ amplifies the solutions amplitude whereas reduces those of others. Repeating this operator several times make the amplitude of the solution greater.

One important part of quantum algorithms can be shown in Grover's algorithm. Let's say $|\psi'\rangle$ is a state which is perpendicular to the state $|x_0\rangle$. Now the action of the operator $\hat{U}_{x_0}$ can be seen as a reflection about $-|x_0\rangle$ and the action of the $\hat{U}_\psi$ corresponds the rotation about k axis which is shown in figure 5.52

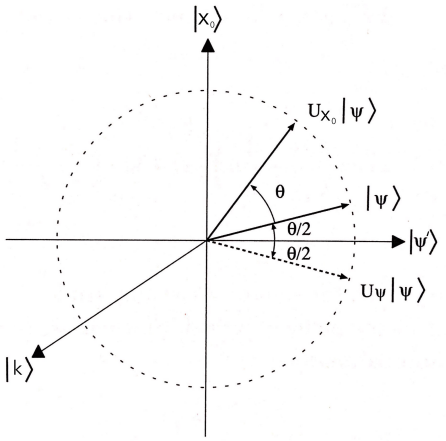


Figure 5.52: Grover searching operators seen as rotation on the qubit.[80]

Let's see mathematical example of Grover's algorithm for N=2:

$$|\psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \tag{5.101}$$

$$\hat{U}_{x_0} = \mathrm{I} - 2|11\rangle\langle 11| \tag{5.102}$$

$$\hat{U}_{\psi} = 2(|00\rangle + |01\rangle + |10\rangle + |11\rangle)(\langle 00| + \langle 01| + \langle 10| + \langle 11|) - \mathrm{I} \tag{5.103}$$

$$= 2\Big(|00\rangle\langle 00| + |00\rangle\langle 01| + |00\rangle\langle 10| + |00\rangle\langle 11| \tag{5.104}$$

$$+ |01\rangle\langle 00| + |01\rangle\langle 01| + |01\rangle\langle 11| + |01\rangle\langle 11| \tag{5.105}$$

$$+ |10\rangle\langle 00| + |10\rangle\langle 01| + |10\rangle\langle 10| + |10\rangle\langle 11| \tag{5.106}$$

$$+ |11\rangle\langle 00| + |11\rangle\langle 01| + |11\rangle\langle 10| + |11\rangle\langle 11|\Big) - \mathrm{I} \tag{5.107}$$

So from here $\hat{G}$ will be

$$\hat{G} = \hat{U}_{\psi}\hat{U}_{x_0} \tag{5.108}$$

$$= 2\Big[|00\rangle + |01\rangle + |10\rangle + |11\rangle)(\langle 00| + \langle 01| + \langle 10| + \langle 11|)\Big] \tag{5.109}$$

$$- 4\Big(|00\rangle + |01\rangle + |10\rangle + |11\rangle\Big)\langle 11| - \mathrm{I} + 2|11\rangle\langle 11| \tag{5.110}$$

If $\hat{G}|\psi\rangle$ is solved, for every term except the last one ($|11\rangle$) will rise 0. So for the 2 qubit data searching algorithm $\hat{G}|\psi\rangle$ will rise the amplitude of 1, this means the algorithm find the cached value which is written with the oracle function, in its first trial. On the other hand classical algorithms will rise the same result in a $N/2$ average trials.

Application of the Grover's algorithm in the IBM Q 5 Tenerife (ibmqx4) is shown in the figure 5.53.

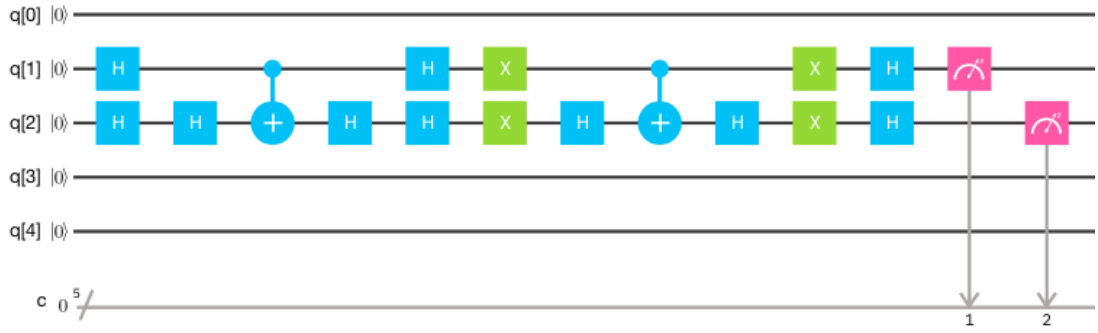
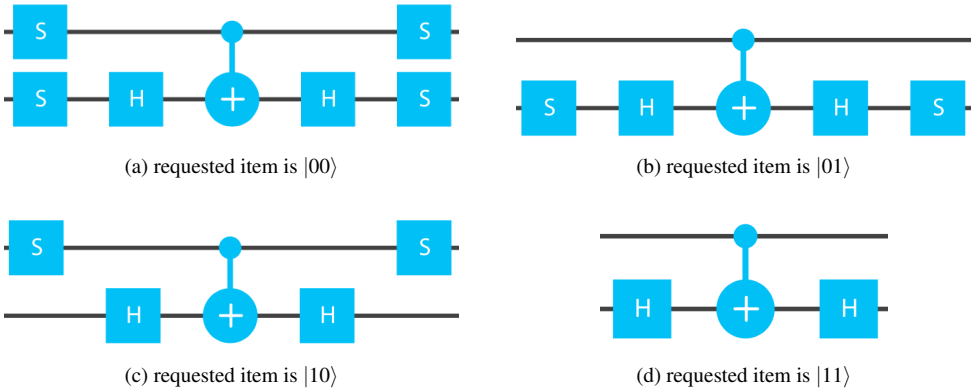


Figure 5.53: Grover's quantum search algorithm for N=2, requested item in this circuit is the state $|11\rangle$.

Here first H gates do the uniform superposition task of the $H^{\otimes n}|0\rangle$. Second part of the circuit is the oracle function which rises minus phase of the requested item which is $|11\rangle$ in this case. Other configuration for other requested items are given in the figure 5.54. This is part is denoted as U_{x_0} in above equations.



(a) requested item is $|00\rangle$ (b) requested item is $|01\rangle$

(c) requested item is $|10\rangle$ (d) requested item is $|11\rangle$

Figure 5.54: Oracle functions for requested item is $|00\rangle, |01\rangle, |10\rangle, |11\rangle$

Third and last part of the equation is implementation of U_ψ. Again Hadamard gates for uniform superposition (Figure 5.55).

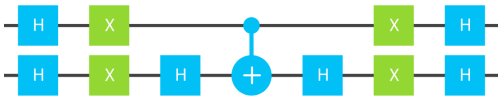


Figure 5.55: Grover operator part of the circuit.

The part of the circuit shown in the figure 5.55 is the heart of the algorithm and it is repeated to find the solution $O\sqrt{N}$ times. When this algorithm run on the IBM Quantum experience cloud server for the 1 shot,

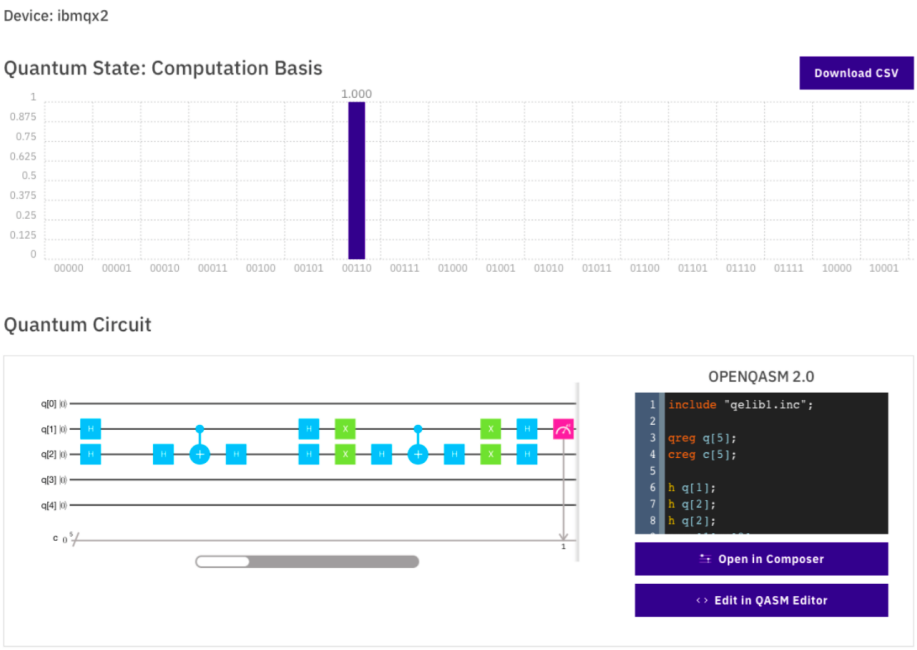


Figure 5.56: Result of the Grover's algorithm.

the exact result always come up with the amplitude of 1. The result window is shown in the figure 5.56

6 Discussions, Conclusions & Future Work

6.1 Comparison between classical and quantum logic gates

As it is already mentioned in introduction most of the classical logic gates are irreversible. It means that after the computation they lost information and it is impossible to know the state before the calculation from the output. This lost is goes to the environment as an amount of energy, so this shows that there is a thermodynamic limit for computation.[81]

With the invention and development of the reversible computation this limit is dismissed. Certain reversible computational methods proposed in the period, quantum computation was one of them.[82] On the way of searching reversibility, the classical logic gates were also questioned and some other reversible gates were proposed.[19]

6.1.1 NOT gate

First of all let's talk about a purely reversible classical gate, which is NOT gate. Because of its reversibility, in quantum computation, there is complete equivalent of NOT gate, which is Pauli-X matrix. (section 4.4.2) In the table 6.9 equal classical and quantum computational truth table is given.

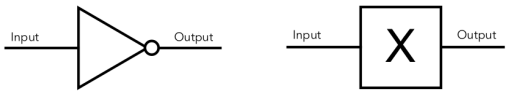


Table 6.9: Truth table of the two equivalent logic gates, NOT and Pauli-X

Input	**Output**
$1 = \|1\rangle$	$0 = \|0\rangle$
$0 = \|0\rangle$	$1 = \|1\rangle$

6.1.2 Exclusive or gate

Exclusive or gate (XOR gate) is a irreversible gate just like AND or OR gates. But there is a version of XOR gate which is reversible. And since it can be realised irreversibly, that version has a quantum computation equivalent which is controlled-NOT gate (CNOT).

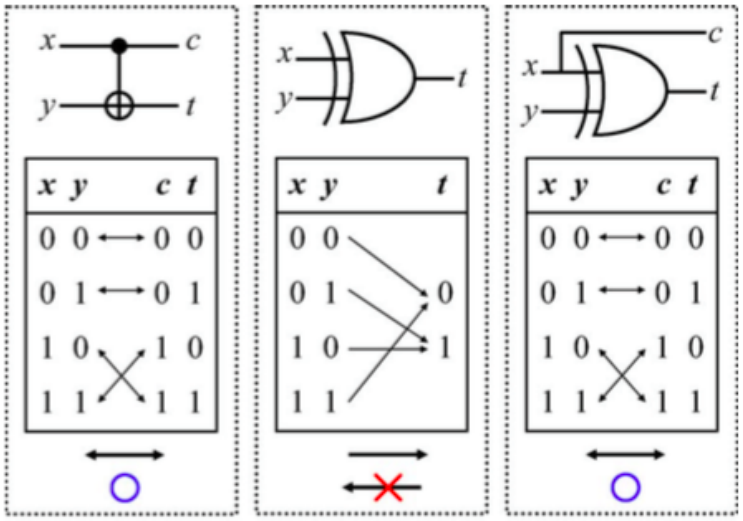


Figure 6.57: Comparison between CNOT, XOR and reversible XOR.[83]

In the figure 6.57 CNOT gate, XOR gate and reversible XOR gate is given from left to right. It is seen that every gate takes 2 input x,y but only XOR gate gives one bit. So there is lost of an information. However, taking x input to the output as an extra bit fixes the irreversibly and make the gate reversible. The signs under the truth tables refer the reversibility of the gate.

6.2 Quantum Cryptography

Cryptography always have critical importance on the side of military, diplomacy or even commerce. Oldest known cryptography technique is the *Caesar cipher* in the Roman Empire. This method encodes message by shifting every character with a fixed unit and decodes it same way, figure 6.58. [80]

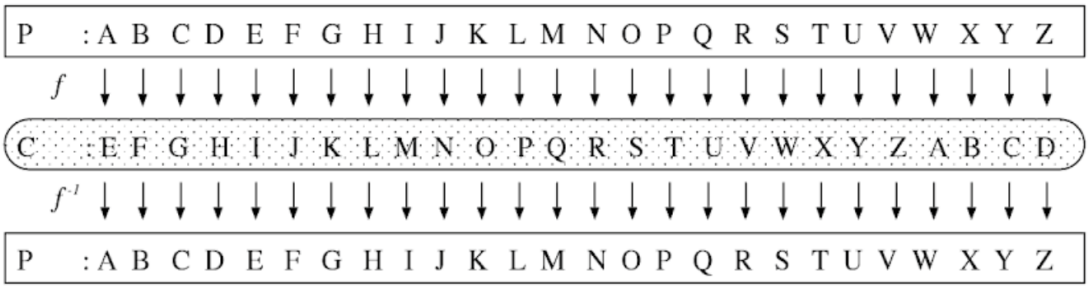


Figure 6.58: Shor's quantum factorising algorithm representation.

In that technique secret key is everything. It should only be known by sender and receiver. If it is known by third person, message can be also known easily. Thus this method is classified as *secret key cryptography*. However there is also *public key cryptography* which has widely range of usage, for example *RSA cryptography*. In public key cryptography, encryption key is shared publicly but this does not make the decryption key find easily. So it may seen as a one-way function which is easy to calculate $f(x)$ but far more difficult to find $f^{-}1(x)$. Difficulty to break RSA cryptography is based

on factorisation. Multiplying two integer is a trivial calculation but finding the factors of a very large integer is sometimes may last more than the age of the universe.[80]

In the quantum era, with the help of the powerful factorisation algorithm, Shor's algorithm (section 5.3) RSA keys becomes breakable in polynomial time. In 25 Jun 2017, a group of scientist factor the number 291311 which is larger number factorised by quantum algorithms, so far. [84] But RSA numbers are much more larger than 291311, for example RSA-2048 has 617 decimal digits.

$$\begin{aligned}\text{RSA-2048} =& 25195908475657893494027183240048398571429282126204032027777137836043662020\\ & 70759555626401852588078440691829064124951508218929855914917618450280848912\\ & 00728449926873928072877767359714183472702618963750149718246911650776133798\\ & 59095700097330459748808428401797429100642458691817195118746121515172654632\\ & 28221686998754918242243363725908514186546204357679842338718477444792073993\\ & 42365848238242811981638150106748104516603773060562016196762561338441436038\\ & 33904414952634432190114657544454178424020924616515723350778707749817125772\\ & 46796292638635637328991215483143816789988504044536402352738195137863656439\\ & 12120103971228221207203 57\end{aligned}$$

Now if quantum computers threaten the standard public key encryption, let's see what quantum mechanics proposes instead of it. So it's time to talk about *quantum key distribution*. As it is mentioned in the mathematical background section, measurement disturbs, even destroys the quantum states. Due to this fact quantum key distribution systems can be detected if any interruption occurs between sender and receiver. For this purpose there are different protocols.

6.2.1 BB84

Protocol BB84 is the first protocol which was introduced in 1984 by Gilles Brassard and Charles Bennett [85]. In the BB84 protocol photon is used as a qubit in 4 different state in 2 different basis.

$$\underbrace{|\updownarrow\rangle, |\leftrightarrow\rangle}_{\text{Horizontal-Vertical Basis}} \qquad \underbrace{|\nearrow\rangle, |\searrow\rangle}_{\text{Diagonal Basis}}$$

States in both basis represents either 1 $\left(|\updownarrow\rangle, |\nearrow\rangle\right)$ or 0 $\left(|\leftrightarrow\rangle, |\searrow\rangle\right)$.

So now there is a message wanted to transmit, it is coded in both basis state randomly. But when it is coded, sender knows which basis uses for which qubit, so there is a order of the measurement basis. When the states measured with different basis it is known that with the probability of %50 it will result wrong cause both basis can be written in the superposition of the other one. When receiver get the message qubit by qubit, he/she applies its measurement to the message. Once it is applied, receiver have a message which may be different than whats transmitted. But after than sender shares its order of measurement publicly. And now both sender and receiver communicates through the public channel to agree on the set of b by discarding ith measurements which is not equal. By this way they create a safe, encrypted channel to communicate.[80]

6.2.2 B92

In B92 protocol which was introduced by Charles H. Bennett in 1992, [80] 2 non-orthogonal basis state ($|\updownarrow\rangle, |\nearrow\rangle$) within 4 basis of BB84. The non-orthogonal basis avoid the cloning of the state (no-cloning theorem). Unlike BB84 where receiver applies randomly ordered measurement, in B92 receiver applies randomly ordered projection measurement operators which are defined as follows,

$$P_0 = 1 - |\nearrow\rangle\langle\nearrow| \tag{6.111}$$

$$P_1 = 1 - |\updownarrow\rangle\langle\updownarrow| \tag{6.112}$$

Operator P_0 projects the bit value 0 ($|\updownarrow\rangle$) and P_1 ($|\nearrow\rangle$) projects 1. And projection measurements leads the state measured as follows, (note that $\langle\nearrow|\updownarrow\rangle = \frac{1}{\sqrt{2}}$)

$$\langle\updownarrow| P_0 |\updownarrow\rangle = 1 - \frac{1}{\sqrt{2}}\langle\updownarrow|\nearrow\rangle = \frac{1}{2} \tag{6.113}$$

$$\langle\updownarrow| P_0 |\nearrow\rangle = \langle\updownarrow|\nearrow\rangle - \langle\updownarrow|\nearrow\rangle = 0 \tag{6.114}$$

$$\langle\nearrow| P_1 |\updownarrow\rangle = \langle\nearrow|\updownarrow\rangle - \langle\nearrow|\updownarrow\rangle = 0 \tag{6.115}$$

$$\langle\nearrow| P_1 |\nearrow\rangle = 1 - \frac{1}{\sqrt{2}}\langle\nearrow|\updownarrow\rangle = \frac{1}{2} \tag{6.116}$$

With this protocol, when the receiver has a signal the probability of receiving right value is %50. If value 1 is received then the state is $|\nearrow\rangle$ and if its 0 then the state is $|\updownarrow\rangle$. So when the signal is received this is the right value. From here a safe and encrypted channel is built.[80]

6.2.3 E91

Protocol E91 is named after Artur Ekert with his work in 1991. Unlike the other two protocol which are fundamentally protected by no-cloning theorem, E91 protocol uses another fundamental feature of quantum mechanics which is entanglement.[80] The procedure is more or less same.

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0_1 1_2\rangle + |1_1 0_2\rangle) \tag{6.117}$$

The subscripts represent the qubit number and these qubits are transfered two parties. Let's say these qubits are spin-1/2 then the measurements done in the same basis will rise the same result however others will be discarded. So sharing publicly the sequence of the measurement they do without giving information about results, they can built encrypted channel.[54]

6.3 Future of The Quantum Computer

On 8th January 2019 IBM announced its commercial 20 qubit quantum computer for the first time. And with lower operation quality, quantum computer of the the company named D-Wave Systems which is also known as quantum annealers which are used for specific optimisation problems, has been out on the market since 2011, and now with 2000 qubits.[86]

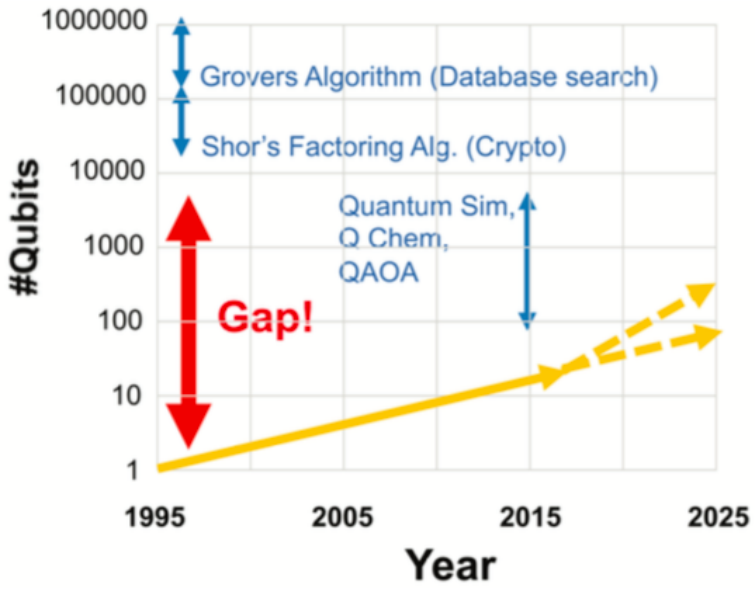


Figure 6.59: Algorithm to machine[87]

Although the quantum computers have huge potential in usage of some algorithms the implementation of the these reliably computers with high number of qubits is still questioning people's mind. In his article Mikhail Dyakonov asks about useful quantum computers, when they will appear? As an answer his own question, the figure 6.60 is shown[88].

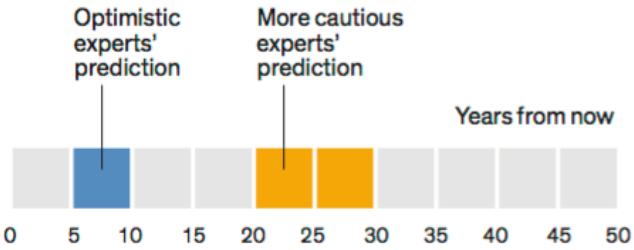


Figure 6.60: Time estimations to have an useful quantum computer.[88]

In his article Dyakonov explains "useful" quantum computer with the words, "one that could compete with your laptop in solving certain kinds of interesting problems" between 1,000 and 100,000 is needed.[88] Inspite of the large gap academic studies on the subject increase year to year, see figure 6.61

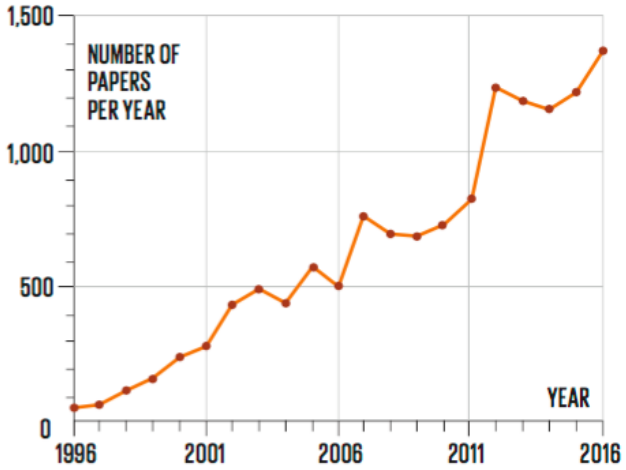


Figure 6.61: Academic Studies on Quantum Computers.[88]

Besides academic studies, a survey tells that 40 percent of its respondents which consist of more than 5,400 business and IT executives, makes their planing in order to move towards to quantum computation and 36 percent of them invests quantum technologies in the following two years. Finance, life science and supply chain are just few industries who are planning to put quantum computation to forefront. [86]

So finally, quantum computation will have huge impact on earth with dramatic changes in computation science which proposed by its specialised algorithms. Soon or late, this change will be integrated in every field of science and engineering. To be a part of it, today is the best time to involve in.

References

[1] M. A. Nielsen and I. Chuang, *Quantum computation and quantum information*. AAPT, 2002.

[2] S. K. Moore, "Computing's power limit demonstrated," *IEEE Spectrum*, vol. 49, pp. 14–16, May 2012.

[3] C. H. Bennett, "Logical reversibility of computation," *IBM journal of Research and Development*, vol. 17, no. 6, pp. 525–532, 1973.

[4] R. P. Feynman, "Simulating physics with computers," *International journal of theoretical physics*, vol. 21, no. 6-7, pp. 467–488, 1982.

[5] R. P. Feynman, *Feynman lectures on computation*. CRC Press, 2018.

[6] C. H. Bennett, "Notes on landauer's principle, reversible computation, and maxwell's demon," *Studies In History and Philosophy of Science Part B: Studies In History and Philosophy of Modern Physics*, vol. 34, no. 3, pp. 501–510, 2003.

[7] R. Landauer, "Irreversibility and heat generation in the computing process," *IBM journal of research and development*, vol. 5, no. 3, pp. 183–191, 1961.

[8] N. Gershenfeld and I. L. Chuang, "Quantum computing with molecules," *Scientific American*, vol. 278, no. 6, pp. 66–71, 1998.

[9] J. I. Cirac and P. Zoller, "A scalable quantum computer with ions in an array of microtraps," *Nature*, vol. 404, no. 6778, p. 579, 2000.

[10] C. H. Bennett and D. P. DiVincenzo, "Quantum information and computation," *Nature*, vol. 404, no. 6775, p. 247, 2000.

[11] I. Research and the IBM QX team, "User guide - frequently asked questions." `https://quantumexperience.ng.bluemix.net/proxy/tutorial/full-user-guide/000-FAQ/000-Frequently_Asked_Questions.html`, 2017.

[12] A. M. Turing, "On computable numbers, with an application to the entscheidungsproblem," *Proceedings of the London Mathematical Society*, vol. s2-42, no. 1, pp. 230–265, 1937.

[13] R. Mullins, "Introduction: What is a turing machine?." https://www.cl.cam.ac.uk/, 2012.

[14] S. Akama, *Elements of Quantum Computing*. Springer, 2015.

[15] E. Schrödinger, "An undulatory theory of the mechanics of atoms and molecules," *Physical review*, vol. 28, no. 6, p. 1049, 1926.

[16] M. Born, "Quantum mechanics of collision processes," *Zeit fur Phys*, vol. 38, p. 803, 1926.

[17] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?," *Physical review*, vol. 47, no. 10, p. 777, 1935.

[18] J. S. Bell, "On the einstein podolsky rosen paradox," *Physics Physique Fizika*, vol. 1, no. 3, p. 195, 1964.

[19] K. Morita, "Reversible computing and cellular automata—a survey," *Theoretical Computer Science*, vol. 395, no. 1, pp. 101–131, 2008.

[20] T. Toffoli, "Reversible computing," in *International Colloquium on Automata, Languages, and Programming*, pp. 632–644, Springer, 1980.

[21] E. Fredkin and T. Toffoli, "Conservative logic," *International Journal of theoretical physics*, vol. 21, no. 3-4, pp. 219–253, 1982.

[22] J. S. Hall, "An electroid switching model for reversible computer architectures," in *Workshop on Physics and Computation*, pp. 237–247, IEEE, 1992.

[23] P. Benioff, "Quantum mechanical hamiltonian models of turing machines," *Journal of Statistical Physics*, vol. 29, no. 3, pp. 515–546, 1982.

[24] D. Deutsch, "Quantum theory, the church–turing principle and the universal quantum computer," *Proc. R. Soc. Lond. A*, vol. 400, no. 1818, pp. 97–117, 1985.

[25] A. Montanaro, "Quantum algorithms: an overview," *npj Quantum Information*, vol. 2, p. 15023, 2016.

[26] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien, "Quantum computers," *Nature*, vol. 464, no. 7285, p. 45, 2010.

[27] J. A. Jones, M. Mosca, and R. H. Hansen, "Implementation of a quantum search algorithm on a quantum computer," *Nature*, vol. 393, no. 6683, p. 344, 1998.

[28] I. L. Chuang, N. Gershenfeld, and M. Kubinec, "Experimental implementation of fast quantum searching," *Physical review letters*, vol. 80, no. 15, p. 3408, 1998.

[29] L. M. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, "Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance," *Nature*, vol. 414, no. 6866, p. 883, 2001.

[30] S. Gulde, M. Riebe, G. P. Lancaster, C. Becher, J. Eschner, H. Häffner, F. Schmidt-Kaler, I. L. Chuang, and R. Blatt, "Implementation of the deutsch–jozsa algorithm on an ion-trap quantum computer," *Nature*, vol. 421, no. 6918, p. 48, 2003.

[31] K.-A. Brickman, P. Haljan, P. Lee, M. Acton, L. Deslauriers, and C. Monroe, "Implementation of grover's quantum search algorithm in a scalable system," *Physical Review A*, vol. 72, no. 5, p. 050306, 2005.

[32] P. Kwiat, J. Mitchell, P. Schwindt, and A. White, "Grover's search algorithm: an optical approach," *Journal of Modern Optics*, vol. 47, no. 2-3, pp. 257–266, 2000.

[33] L. DiCarlo, J. Chow, J. Gambetta, L. S. Bishop, B. Johnson, D. Schuster, J. Majer, A. Blais, L. Frunzio, S. Girvin, *et al.*, "Demonstration of two-qubit algorithms with a superconducting quantum processor," *Nature*, vol. 460, no. 7252, p. 240, 2009.

[34] D. P. DiVincenzo, "The physical implementation of quantum computation," *Fortschritte der Physik: Progress of Physics*, vol. 48, no. 9-11, pp. 771–783, 2000.

[35] R. Feynman, R. Leighton, and M. Sands, *The Feynman Lectures on Physics, Vol. III: The New Millennium Edition: Quantum Mechanics*. The Feynman Lectures on Physics, Basic Books, 2011.

[36] A. Frisk Kockum, *Quantum optics with artificial atoms*. PhD thesis, 12 2014.

[37] D. McMahon, *Quantum computing explained*. John Wiley & Sons, 2007.

[38] R. Jozsa and N. Linden, "On the role of entanglement in quantum-computational speed-up," *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 459, no. 2036, pp. 2011–2032, 2003.

[39] J. S. Bell and J. S. Bell, *Speakable and unspeakable in quantum mechanics: Collected papers on quantum philosophy*. Cambridge university press, 2004.

[40] A. I. Lvovsky and M. G. Raymer, "Continuous-variable optical quantum-state tomography," *Reviews of Modern Physics*, vol. 81, no. 1, p. 299, 2009.

[41] T. Orlando, J. Mooij, L. Tian, C. H. Van Der Wal, L. Levitov, S. Lloyd, and J. Mazo, "Superconducting persistent-current qubit," *Physical Review B*, vol. 60, no. 22, p. 15398, 1999.

[42] J. I. Cirac and P. Zoller, "Quantum computations with cold trapped ions," *Physical review letters*, vol. 74, no. 20, p. 4091, 1995.

[43] S. Schneider, D. F. James, and G. J. Milburn, "Method of quantum computation with"hot"trapped ions," *arXiv preprint quant-ph/9808012*, 1998.

[44] A. Sørensen and K. Mølmer, "Quantum computation with ions in thermal motion," *Physical review letters*, vol. 82, no. 9, p. 1971, 1999.

[45] N. A. Gershenfeld and I. L. Chuang, "Bulk spin-resonance quantum computation," *science*, vol. 275, no. 5298, pp. 350–356, 1997.

[46] C. Monroe, D. Meekhof, B. King, W. M. Itano, and D. J. Wineland, "Demonstration of a fundamental quantum logic gate," *Physical review letters*, vol. 75, no. 25, p. 4714, 1995.

[47] D. G. Cory, A. F. Fahmy, and T. F. Havel, "Ensemble quantum computing by nmr spectroscopy," *Proceedings of the National Academy of Sciences*, vol. 94, no. 5, pp. 1634–1639, 1997.

[48] G. K. Brennen, C. M. Caves, P. S. Jessen, and I. H. Deutsch, "Quantum logic gates in optical lattices," *Physical Review Letters*, vol. 82, no. 5, p. 1060, 1999.

[49] T. Pellizzari, S. A. Gardiner, J. I. Cirac, and P. Zoller, "Decoherence, continuous observation, and quantum computing: A cavity qed model," *Physical Review Letters*, vol. 75, no. 21, p. 3788, 1995.

[50] A. Imamog, D. D. Awschalom, G. Burkard, D. P. DiVincenzo, D. Loss, M. Sherwin, A. Small, *et al.*, "Quantum information processing using quantum dot spins and cavity qed," *Physical review letters*, vol. 83, no. 20, p. 4204, 1999.

[51] B. E. Kane, "A silicon-based nuclear spin quantum computer," *nature*, vol. 393, no. 6681, p. 133, 1998.

[52] R. Vrijen, E. Yablonovitch, K. Wang, H. W. Jiang, A. Balandin, V. Roychowdhury, T. Mor, and D. DiVincenzo, "Electron-spin-resonance transistors for quantum computing in silicon-germanium heterostructures," *Physical Review A*, vol. 62, no. 1, p. 012306, 2000.

[53] G. Benenti, G. Casati, and G. Strini, *Principles of quantum computation and information: Volume II: Basic Tools and Special Topics*. World Scientific Publishing Company, 2007.

[54] J. Stolze and D. Suter, *Quantum computing: a short course from theory to experiment*. John Wiley & Sons, 2008.

[55] M. H. Devoret, A. Wallraff, and J. M. Martinis, "Superconducting qubits: A short review," *arXiv preprint cond-mat/0411174*, 2004.

[56] A. Zagoskin and A. Blais, "Superconducting qubits," *arXiv preprint arXiv:0805.0164*, 2008.

[57] T. Tanamoto, "Quantum gates by coupled asymmetric quantum dots and controlled-not-gate operation," *Physical Review A*, vol. 61, no. 2, p. 022305, 2000.

[58] D. Loss and D. P. DiVincenzo, "Quantum computation with quantum dots," *Physical Review A*, vol. 57, no. 1, p. 120, 1998.

[59] S. Barnett, *Quantum information*, vol. 16. Oxford University Press, 2009.

[60] S. J. Devitt, W. J. Munro, and K. Nemoto, "Quantum error correction for beginners," *Reports on Progress in Physics*, vol. 76, no. 7, p. 076001, 2013.

[61] N. D. Mermin, *Quantum computer science: an introduction*. Cambridge University Press, 2007.

[62] R. Blume-Kohout, "Optimal, reliable estimation of quantum states," *New Journal of Physics*, vol. 12, no. 4, p. 043034, 2010.

[63] G. M. D'Ariano, M. G. Paris, and M. F. Sacchi, "Quantum tomography," *Advances in Imaging and Electron Physics*, vol. 128, pp. 206–309, 2003.

[64] H. Fan, Y.-N. Wang, L. Jing, J.-D. Yue, H.-D. Shi, Y.-L. Zhang, and L.-Z. Mu, "Quantum cloning machines and the applications," *Physics Reports*, vol. 544, no. 3, pp. 241–322, 2014.

[65] V. Bužek and M. Hillery, "Quantum copying: Beyond the no-cloning theorem," *Physical Review A*, vol. 54, no. 3, p. 1844, 1996.

[66] T. Nakajima, A. Noiri, J. Yoneda, M. R. Delbecq, P. Stano, T. Otsuka, K. Takeda, S. Amaha, G. Allison, K. Kawasaki, *et al.*, "Quantum non-demolition measurement of an electron spin qubit," *Nature nanotechnology*, p. 1, 2019.

[67] A. Lupaşcu, S. Saito, T. Picot, P. De Groot, C. Harmans, and J. Mooij, "Quantum non-demolition measurement of a superconducting two-level system," *Nature Physics*, vol. 3, no. 2, p. 119, 2007.

[68] M. Madeddu, "Quantum computing." `https://made2591.github.io/matteo_madeddu_quantum_notes.pdf`, January 2018.

[69] N. M. Linke, D. Maslov, M. Roetteler, S. Debnath, C. Figgatt, K. A. Landsman, K. Wright, and C. Monroe, "Experimental comparison of two quantum computing architectures," *Proceedings of the National Academy of Sciences*, vol. 114, no. 13, pp. 3305–3310, 2017.

[70] A. Zulehner, A. Paler, and R. Wille, "Efficient mapping of quantum circuits to the ibm qx architectures," in *2018 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 1135–1138, IEEE, 2018.

[71] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*, pp. 124–134, Ieee, 1994.

[72] E. Bernstein and U. Vazirani, "Quantum complexity theory," *SIAM Journal on computing*, vol. 26, no. 5, pp. 1411–1473, 1997.

[73] F. X. Lin, "Shor's algorithm and the quantum fourier transform," *McGill University*, 2014.

[74] D. Bacon, "Cse 599d - quantum computing shor's algorithm." `https://courses.cs.washington.edu/courses/cse599d/06wi/lecturenotes11.pdf`, 2006.

[75] A. Dash, D. Sarmah, B. K. Behera, and P. K. Panigrahi, "Exact search algorithm to factorize large biprimes and a triprime on ibm quantum computer," *arXiv preprint arXiv:1805.10478*, 2018.

[76] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

[77] I. L. Markov and M. Saeedi, "Constant-optimized quantum circuits for modular multiplication and exponentiation," *arXiv preprint arXiv:1202.6614*, 2012.

[78] I. Research and the IBM QX team., "User guide - quantum algorithms - shor's algorithm." `https://quantumexperience.ng.bluemix.net/proxy/tutorial/full-user-guide/004-Quantum_Algorithms/110-Shor's_algorithm.html`, 2017.

[79] C.-Y. Lu, D. E. Browne, T. Yang, and J.-W. Pan, "Demonstration of a compiled version of shor's quantum factoring algorithm using photonic qubits," *Physical Review Letters*, vol. 99, no. 25, p. 250504, 2007.

[80] H. Sagawa and N. Yoshida, *Fundamentals of quantum information*. World Scientific, 2011.

[81] B. Lambson, D. Carlton, and J. Bokor, "Exploring the thermodynamic limits of computation in integrated systems: Magnetic memory, nanomagnetic logic, and the landauer limit," *Physical review letters*, vol. 107, no. 1, p. 010604, 2011.

[82] M. P. Frank, "Introduction to reversible computing: motivation, progress, and challenges," in *Proceedings of the 2nd Conference on Computing Frontiers*, pp. 385–390, ACM, 2005.

[83] Y.-H. Chou, I.-M. Tsai, and S.-Y. Kuo, "Quantum boolean circuits are 1-testable," *IEEE Transactions on Nanotechnology*, vol. 7, no. 4, pp. 484–492, 2008.

[84] Z. Li, N. S. Dattani, X. Chen, X. Liu, H. Wang, R. Tanburn, H. Chen, X. Peng, and J. Du, "High-fidelity adiabatic quantum computation using the intrinsic hamiltonian of a spin system: Application to the experimental factorization of 291311," *arXiv preprint arXiv:1706.08061*, 2017.

[85] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing.," *Theor. Comput. Sci.*, vol. 560, no. 12, pp. 7–11, 2014.

[86] M. Ziegler and T. Leonhardt, "Quantum computing. applied now," *Digitale Welt*, vol. 3, no. 2, pp. 50–52, 2019.

[87] M. Martonosi and M. Roetteler, "Next steps in quantum computing: Computer science's role," *arXiv preprint arXiv:1903.10541*, 2019.

[88] M. Dyakonov, "When will useful quantum computers be constructed? not in the foreseeable future, this physicist argues. here's why: The case against: Quantum computing," *IEEE Spectrum*, vol. 56, no. 03, pp. 24–29, 2019.

BIOGRAPHY

Ad Soyad: Özgen Tunç Türker
Doğum Yeri ve Tarihi: İstanbul, 11 Ocak 1994
Adres: Bağarası Caddesi no:9/1 Göltürkbükü Mahallesi Bodrum/Muğla
Lisans Üniversite: İstanbul Teknik Üniversitesi
Yayın Listesi: