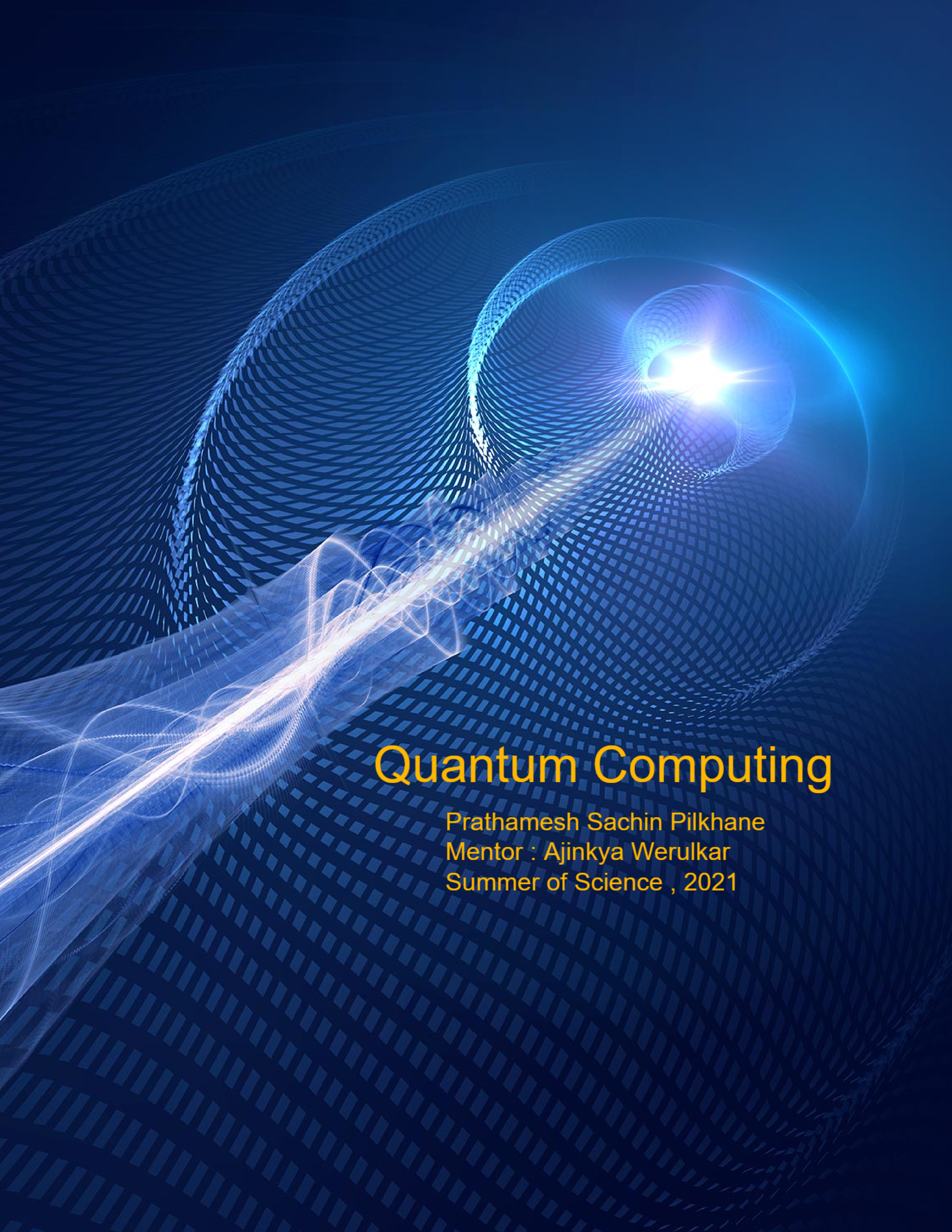

Quantum Computing

Prathamesh Sachin Pilkhane
Mentor : Ajinkya Werulkar
Summer of Science , 2021

Contents

1 Introduction and Overview

Through this Summer of Science report, we aim at building a clear picture on **Quantum Computing**, and **Quantum Error Correction**. The primary source being followed is **Quantum Computation and Quantum Information** by **Nielsen** and **Chuang**. We first cover some mathematical preliminaries, followed by the postulates of Quantum Mechanics. This will be followed by a description of special EPR pairs and two of their characteristic uses : Teleportation and Super-Dense Coding. We then cover the Quantum Fourier transform. We conclude this report by Quantum Error Correction and a small section on Quantum Cryptography.

The most important thing to keep in mind about Quantum Computing is that, we need to think out of the box, using classical methods of solving problems will only lead us to use Quantum Computing in a classical way, making the power of Quantum Computing much less than what it can be used for.

---

2 Mathematical Preliminaries

Quantum Computation depends heavily on the understanding of linear algebra and we first cover some preliminaries on the same.

2.1 Vector Spaces

The most important part of linear algebra is the notion of a vector which we will denote by the bra-ket notation, $|\cdot\rangle$. The vector is an element of a vector space which satisfies certain condition.

For a subspace of this vector-space, we can define a set of linearly independent vectors, which span the sub-space.Such a set is called a basis of the subspace.All bases

All our calculations on qubits(the quantum analogue of bit) , are essentially calculations on vectors.

2.2 Linear Operators

Any function(or evolution as we will further note) which maps a vector-space **V** to a vector-space **W** and satisfies linearity i.e.

$$A(\sum a_i |\psi_i\rangle) = \sum a_i A |\psi_i\rangle$$

is considered as a linear operator. By Linear Algebra , operators on vector spaces can be defined using Matrices. The matrix which represents $A : \mathbf{V} \rightarrow \mathbf{W}$ with respect to certain basis vectors in **V** and **W** is called the Matrix of linear transformation of A

2.3 Inner and Outer products

An inner product of a vector space **V** is defined as a function from V **x** V to C if it satisfies

1. $\langle v|w\rangle = (\langle w|v\rangle)^*$
2. $\langle v| \sum_j a_j w_j\rangle = \langle \sum_j a_j v w_j\rangle$

3. $\langle v|v\rangle \geq 0$ with equality iff $|v\rangle = 0$

We define an orthonormal basis of a sub-space as a basis whose vectors, $|v\rangle$ have a length of 1 i.e. $\sqrt{\langle v|v\rangle} = 1$ and which are orthogonal to each other , $\langle v|w\rangle_{v\neq w} = 0$ Every finite dimensional vector space , has an orthonormal basis , and a basis can be found by the Gram-Schmidt Orthogonalisation process.Working in an orthonormal basis , we can define the inner product of two vectors $|v\rangle$ and $|w\rangle$ as

$$\langle v|w\rangle = \begin{bmatrix} v_1^* \; v_2^* \ldots \; v_n^* \end{bmatrix} \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix}$$

Similarly we define the outer product on an inner product space as a function which takes 2 vectors $|v\rangle$ and $|w\rangle$ and gives $|v\rangle \langle w|$, which acts on any other vector $|a\rangle$ to give $\langle w|a\rangle |v\rangle$.
The outer product notation is useful when defining matrices , as we shall further note in next section.

2.4 Eigenvalues and Eigenvectors

An eigenvector for a linear operator **A** is a non-zero vector $|v\rangle$ such that
$A|v\rangle = \lambda |v\rangle$ for some complex number λ.This complex number is called the Eigenvalue corresponding to the Eigenvector $|v\rangle$
A necessary and sufficient condition for a complex number λ to be an eigenvalue of a linear operator **A** is :

$$\det |A - \lambda I| = 0$$

An linear operator **A** is called diagonalisable if there exists an orthonormal basis composed of eigenvectors of A. Such an operator can be defined in terms of the outerproducts of thse vectors as:

$$A = \sum_j \lambda_j |v_j\rangle \langle v_j|$$

3 Qubit : The Quantum bit

The quantum analogue of the classical bit is the qubit. Like the classical bit has 2 possible values, 0 or 1 , we define two vectors:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad and \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

to represent states of qubit. However, unlike the classical bit which can exists in either of the two states at a given time , the qubit can exists in a superposition of both states. This seems natural as a qubit essentially represents a vector corresponding to the state of a system. Following the above notation of $|0\rangle$ and $|1\rangle$, we can write any single qubit state $|\psi\rangle$ as

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{1}$$

$$where \;\; |\alpha|^2 + |\beta|^2 = 1$$

for a normalized state $|\psi\rangle$ The basis of $|0\rangle$ and $|1\rangle$, as of any other vector space, is not the only basis of vectors. It is just the standard basis. We may wish to work in different basis of vectors depending on the computations involved. One another basis which we will be using is:

$$|+\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\, and\, |-\rangle = \frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle$$

We may switch between any basis , depending on the computations involved.

3.1 Bloch-Sphere representation

We can also represent equation (1) as

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle\right)$$

where γ is the overall phase constant, called global phase. We will further note that the presence of global phase doesn't alter our measurements and it suffices to perform computations on

$$|\psi\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle$$

We can denote this $|\psi\rangle$ in a unit sphere in the manner as shown in figure 1.
In the figure ,θ represents the angle from z axis and ϕ represents angle between projection of $|\psi\rangle$ on x-y plane and the x axis. This definition of θ and ϕ is well known as the polar notation in general.

The Bloch-Sphere notation is very helpful as any computation involving single qubit , can be thought of as a rotation from the original direction of $|\psi\rangle$.

3.2 Single qubit gates

As opposed to the only single bit gate in classical world , the NOT gate, Quantum computation have many possible gates. This comes from the fact that single bits can be present only in 2 possible states , while qubits are in general in a superposition of states. Also , every gate acts on the qubits

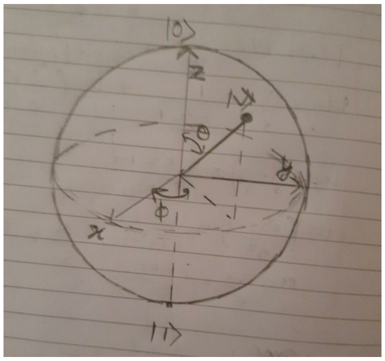

Figure 1: Bloch-sphere representation of a qubit

in a linear manner. For example, the NOT gate applied on a $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ gives the result $\alpha|1\rangle + \beta|0\rangle$.This behaviour of Quantum gates is emperical , however non-linearity of operators would imply certain improbable events such as communication faster than light.

The NOT gate described above can be realised as an operator given by

$$X \quad = \quad |0\rangle\langle 1| + |1\rangle\langle 0|$$

or equivalently, in matrix form as:

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

The output of a gate must satisfy the normalisation condition.This imposes that the gate must be a Unitary matrix $\mathbf{U}$, a matrix satisfying $U^\dagger U = I$.Thus in theory, infinitely many matrices can be used as gates.Two important gates which we will use are:

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

which has the action of leaving $|0\rangle$ untouched while flipping the sign of $|1\rangle$, and the Hadmard gate :

$$H = \frac{X+Z}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

which has the action of

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle$$

$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle$$

3.3 Multiple qubits

We define a system of more than one qubits by the tensor product of the individual qubits.We define the tensor product of 2 qubits as $|A\rangle|B\rangle = \begin{bmatrix} a_1 B \\ a_2 B \\ \vdots \\ a_n B \end{bmatrix}$ where $a_1, a_2, \ldots, a_n$ compose the vector

$|A\rangle$. We denote the tensor product of $|A\rangle$ and $|B\rangle$ by $|A\rangle\,|B\rangle$ or simply by $|AB\rangle$ Thus, like the classical 2 bit system is made up of 00, 01, 10 or 11,the 2qubit system is made up of a superposition of $|00\rangle\,, |01\rangle\,, |10\rangle$ and $|11\rangle$ and can thus can be represented as :

$$|\psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle$$

One important class of the 2 qubit system are the EPR pairs, named after the scientists **E**instein , **P**odolsky and **R**osen. The pairs are responsible for some interesting phenomenon such as Teleportation and Super Dense Coding.

3.4 Multiple Qubit Gates

Like the single qubit gates , a multiple qubit gate must be represented by a unitary matrix. One important difference between the Classical and Quantum world is reflected in these gates. Classical gates such as 'AND' and 'OR' gates are not reversible, we cannot predict what was the input for a given output, however by postulates of Quantum Mechanics every operator must be defined by an invertible matrix which makes every operator a reversible operation.

We can however define the XOR or C-NOT (Controlled NOT) gate as a gate which leaves the second bit if the first bit is 0 while flips it if the first bit is 1. The first bit is called the control bit and the second is called the target bit. Such a gate can be given by the matrix:

$$U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

One may verify that indeed the matrix satisfies the following operations:

$$U\,|00\rangle = |00\rangle\,, U\,|01\rangle = |01\rangle\,, U\,|10\rangle = |11\rangle\,and\;\;U\,|11\rangle = |10\rangle$$

To define gates such as AND , we define the CCNOT gate, which operates on 2 bits of data and

4 Postulates of Quantum Mechanics

Quantum systems are guided by a set of 4 postulates:

4.1 State space

In all the discussions previous to this, we never actually mentioned why we referred to the qubit as a vector. The reason is the following postulate.

Postulate 1: *Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the state space of the system. The system is completely described by its state vector, which is a unit vector in the system's state space.*

This postulate tells us that any quantum system, can be described in terms of a vector spanned by some basis of vectors. This postulate doesn't tell us much on how the system manifests, it just tells us the existence of a vector which can describe a state of the system. The basis of vectors also completely depends on the system being discussed. For example , in the case of Quantum Computing we generally have the vector space spanned by qubits, in case of Quantum Mechanics for a particle in a box system , we have certain Eigenstates and particle is considered to be in superposition of those states.

4.2 Evolution of state

In section 3.2 , we noted that single qubit gates/operators must be unitary.This is true in general i.e.

Postulate 2: *The evolution of a closed quantum system is described by a unitary transformation. That is, the state $|\psi'\rangle$ of the system at time t1 is related to the state $|\psi\rangle$ of the system at time t2 by a unitary operator U which depends only on the times t1 and t2,*

$$|\psi'\rangle = U|\psi\rangle$$

The postulate also has a clause for the requirement of closed quantum system, i.e. a system without energy losses. Having systems meeting this criteria is usually difficult , and so we sometimes use a region of space beyond which the energy changes are negligible.

This postulate thus helps us write any possible evolution, whether by gates or noise or by other means, by simply Unitary operator. A more refined version of this postulate can be given to describe the evolution of a quantum system in continuous time. From the refined postulate we can get the above mentioned statement.

Postulate 2′: *The time evolution of the state of a closed quantum system is described by the Schrodinger equation,*

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

In this equation, $\hbar$ is a physical constant known as Planck's constant whose value must be experimentally determined. The exact value is not important to us. In practice, it is common to absorb the factor into H, effectively setting = 1. H is a fixed Hermitian operator known as the Hamiltonian of the closed system.

If we know the Hamiltonian then we can solve for the dynamics of the system for a given time interval. However, most systems that we consider have highly complicated Hamiltonians. However for our study, we just state the Hamiltonian for a given system without giving the derivation/ reason of the same.

4.3 Quantum Measurement

Till now we have seen the evolution of the state in a closed quantum system ,but there are times when we perform some measurements on the system. The result of measurement on the state of the system is given by the following postulate.

Postulate 3:*Quantum measurements are described by a collection M_m of measurement operators. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement then the probability that result m occurs is given by*

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle\,,$$

and the state of the system after the measurement is

$$\frac{M_m\,|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$$

The measurement operators satisfy the completeness equation

$$\sum_m M_m^\dagger M_m = I$$

The completeness equation expresses the fact that probabilities sum to one:

$$1 = \sum_m p(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle = \langle\psi| \sum_m M_m^\dagger M_m|\psi\rangle$$

The equation being satisfied by all for all $|\psi\rangle$.

Using postulate 3 we can deduce that a measurement in the computational basis by measurement operators $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$, collapses the system to either $|0\rangle$ or $|1\rangle$ upto a global phase factor.

4.4 Composite system

We now formally describe the state of system composed of multiple systems. The state of such as system is given by postulate 4.

Postulate 4:*: The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and system number i is prepared in the state $|\psi_i\rangle$, then the joint state of the total system is* $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle$

We thus define the state of system consisting of multiple states using the tensor product of the individual state vectors.

4.5 Density operator

Instead of formulating the postulates in terms of the state vector we can also reformulate them using the density operator. The density operator of system which is in one of a number of states $|\psi_i\rangle$, with a probability of p_i , is given by the equation:

$$\rho = \sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right| .$$

All postulates of quantum mechanics can be reformulated in terms of the density operator, also called as density matrix.Suppose we want to describe the postulate of evolution. If the system was in a state $|\psi_i\rangle$ with a probability of p_i then after the evolution it will be in a state U$|\psi_i\rangle$ with the same probability. The density matrix due to the evolution would change as follows:

$$\rho = \sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right| \to \sum_i p_i U \left|\psi_i\right\rangle \left\langle\psi_i\right| U^\dagger = U\rho U^\dagger$$

Measurment also can be performed in a similar way. Suppose we perform measurements described by measurement operator M_m. If the initial state was $|\psi_i\rangle$,then the probability of getting result m is:

$$p(m|i) = \langle\psi_i|M_m^\dagger M_m|\psi_i\rangle = tr(M_m^\dagger M_m \left|\psi_i\right\rangle \left\langle\psi_i\right|)$$

the overall probability being given by

$$p(m) = \sum_i p(m|i)p_i = \sum_i p_i tr(M_m^\dagger M_m \left|\psi_i\right\rangle \left\langle\psi_i\right|) = tr(M_m^\dagger M_m \rho)$$

and the density operator after the measurement m is given by :

$$\rho_m = \sum_i \frac{p_i M_m \left|\psi_i\right\rangle \left\langle\psi_i\right| M_m^\dagger}{tr(M_m M_m^\dagger \rho)} = \frac{M_m \rho M_m^\dagger}{tr(M_m M_m^\dagger \rho)}$$

.

Lastly the fourth postulate of composite systems can be formulated as the state space being defined as the tensor product of all individual density matrices.

The density matrix notation has a characteristic use which is of the reduced density operator. Given physical systems A and B , whose state is described by density operator ρ^{AB} , the reduced density operator of A is given by:

$$\rho^A = tr_B(\rho^{AB})$$

where tr_B is the partial trace of the system over system B.The partial trace is defined by :

$$tr_B(|a_1\rangle \langle a_2| \otimes |b_1\rangle \langle b_2|) = |a_1\rangle \langle a_2| \, tr(|b_1\rangle \langle b_2|)$$

It does not seem that the reduced density operator is of any relation to the system A. However, upon performing measurements, we do get the same results as what we would have otherwise got.

The density operator is a useful tool in quantum systems , especially due to the reduced density operation.

4.6 No Cloning Theorem

Though this theorem is not a postulate of Quantum Mechanics , we give a brief account of this theorem.

The theorem states that there is no Quantum circuit which can copy an unknown arbitrary quantum state.

The proof of this theorem follows from contradiction and using postulate 2 , on evolution.

Say there exists a circuit which takes a system $|\psi\rangle$, which is to be copied, and an ancilla of bits prepared in the state $|0\rangle$. The combined system of is given by $|\psi\rangle |0\rangle$. The circuit outputs the ancilla of the system in the state $|\psi\rangle$.Since the circuit is essentially an evolution, it can be represented by a unitary operator, U. So:

$$U |\psi\rangle |0\rangle = |\psi\rangle \otimes |\psi\rangle$$

Lets say there is another state $|\Phi\rangle$ to be copied then,

$$U |\Phi\rangle |0\rangle = |\Phi\rangle \otimes |\Phi\rangle$$

Taking inner products of the above equations gives:

$$\langle 0| \langle \Phi|U^\dagger U|\psi\rangle |0\rangle = \langle \Phi| \langle \Phi|\psi\rangle |\psi\rangle$$

which simplifies to

$$\langle \Phi|\psi\rangle = \langle \Phi|\psi\rangle^2$$

Now this equation is true only if $|\Phi\rangle$ and $|\psi\rangle$ were either equal or orthonormal.This is not true in general , hence a completely generalised copying circuit cannot be made. Note that we used ancilla in state $|0\rangle$, though it does not matter in what state we keep the ancilla.

5 EPR Pairs and Entanglement

The EPR pairs have a special significance in quantum computing for example in teleportation and super-dense coding. The reason of their special significance is that when a measurement is performed on a single bit, we get the information of the both the bits of the collapsed state. The EPR pairs are also called Bell states.

The EPR pairs are given by:

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

$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$|\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

An easier way to remember this is:

$$|\beta_{xy}\rangle = \frac{|0, y\rangle + (-1)^x |1, 1-y\rangle}{\sqrt{2}}$$

This also explains a way of making them, by passing of $|x\rangle$ through a Hadmard gate , followed by a CNOT gate with $|y\rangle$ as the target bit.

5.1 Teleportation

Say Alice and Bob share an EPR pair where in , Alice possess the first qubit of the pair while Bob possess the second qubit. The task of quantum teleportation implies, given an unknown $|\psi\rangle$ in possession of Alice , she must teleport it to Bob , given that she can convey only classical bits of information to him. She can do so in the following way:
Lets say the EPR pair shared by Alice and Bob is

$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

And the unknown state $|\psi\rangle$ be represented by

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle$$

Then a circuit describe by Figure 2 is essentially what we need. Proof of the teleportation circuit:
The state of the sytem just before any computation is given by:

$$|\psi\rangle = \frac{a\,|0\rangle\,(|01\rangle + |10\rangle) + b\,|1\rangle\,(|01\rangle + |10\rangle)}{\sqrt{2}}$$

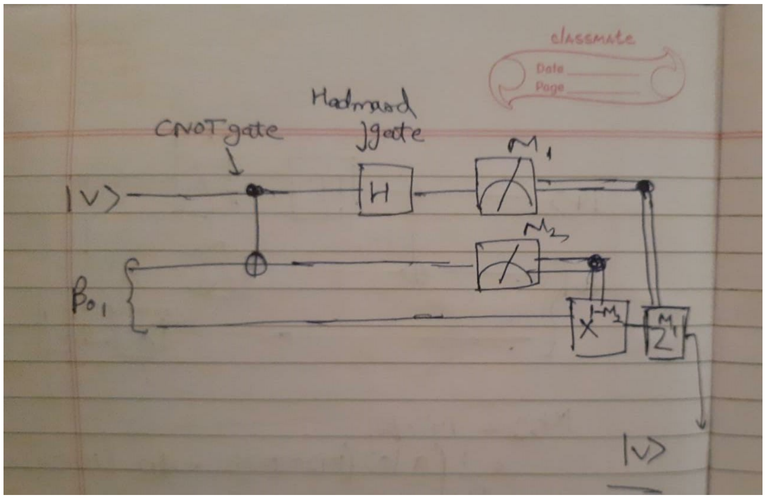

Figure 2: Quantum Teleportation with β_{01}

Here we use the convention that the first 2 bits belong to Alice , the second bit being the first bit of EPR pair, while the last bit what Bob has in possession.
After the CNOT gate, the state of the system becomes:

$$|\psi'\rangle = \frac{a\,|0\rangle\,(|01\rangle + |10\rangle) + b\,|1\rangle\,(|11\rangle + |00\rangle)}{\sqrt{2}}$$

Applying Hadmard gate to the first bit now gives us:

$$|\psi"\rangle = \frac{1}{2}\Big(a(|0\rangle + |1\rangle)(|01\rangle + |10\rangle) + b(|0\rangle - |1\rangle)(|11\rangle + |00\rangle)\Big)$$

Which can be simplified as:

$$|\psi"\rangle = \frac{1}{2}\Big(\,|00\rangle\,(a\,|1\rangle + b\,|0\rangle) + |01\rangle\,(a\,|0\rangle + b\,|1\rangle) + |10\rangle\,(a\,|1\rangle - b\,|0\rangle) + |11\rangle\,(a\,|0\rangle - b\,|1\rangle\,\Big)$$

Now when Alice measures the 2 qubits in her possession , she collapses the state $|\psi"\rangle$ into one of the four possible states. If Alice measures $|00\rangle$ then Bob's qubit is in state a$|1\rangle$ +b$|0\rangle$, which he can apply X gate and get the original —v¿ back;

If Alice measures $|01\rangle$ then Bob's qubit is in the original state $|\psi\rangle$ and he doesn't need to perform any further operations.

If Alice measures $|10\rangle$ then Bob can apply first an X gate followed by Z gate on his qubit to get back the original $|\psi\rangle$

And if Alice measures $|11\rangle$ then Bob applies the Z gate on his qubit , and thus getting $|\psi\rangle$back.

Thus, Alice was able to teleport her unknown qubit, without any information about it, to Bob via just 2 bits of information. With a few changes, it can be shown that all the EPR pairs can be used for Quantum Teleportation. Quantum Teleportation , though seems to be faster communication of information than light, isn't as such, as the conveying of information by Alice about her 2 qubits prevents this, thus Quantum Teleportation does not enable faster communication than light.

Also, it may seem that we just violated the No Cloning theorem as Bob's qubit was finally a copy of the original qubit. However, during the computation by circuit, we infact have only the target bit in state $|\psi\rangle$ while the original data ended up in one of the computational basis of $|0\rangle$ and $|1\rangle$.

5.2 Super Dense Coding

Suppose Alice wants to share two bits of information to Bob , given that they are distant away while they share an EPR pair and Alice can interact only with qubit. Is this possible?
The answer to the question is infact Yes.
Alice does so in the following way:

Suppose the state/ EPR shared by Alice and Bob is

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

where Alice is in possession of the first bit while Bob is in the possession of the second bit.
Now if Alice wishes to send the bit string '00', then she does nothing to her bit, if she wishes to send '01', then she applies a phase shift, Z gate to her bit.If she wishes to send '10', then she just applies the bit flip X gate, anf finally if she wishes to send '11' she applies X gate followed by Z gate to her bit.The result of all this can in fact be summaried as:

$$00 : |\psi\rangle \rightarrow |\beta_{00}\rangle$$

$$01 : |\psi\rangle \rightarrow |\beta_{01}\rangle$$

$$10 : |\psi\rangle \rightarrow |\beta_{10}\rangle$$

$$11 : |\psi\rangle \rightarrow |\beta_{11}\rangle$$

Indeed, we have the 4 EPR pairs. Now if Alice sends her qubit to Bob then Bob has possession of both the qubits. Notice that EPR pairs form an orthonormal basis of the two-qubit space. Hence by making a measurement in the Bell basis, Bob can identify the which bit string was sent by Alice.

6 Quantum Fourier Transform

Many of the transformations involved in mathematics or computer science involve calculations which are very difficult to be carried over classical computers. One such transformation is the discrete Fourier transform. This can be achieved in much efficient way in a quantum circuit as compared to its classical counterpart.

In usual mathematical notation , discrete Fourier transform acts on a vector of complex numbers, $x_0, x_1, \ldots, x_{N-1}$,of fixed length N, and outputs the another vector of complex numbers ,$y_0, \ldots, y_{N-1}$ given by:

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

The quantum Fourier transform is defined in a similar way.The QFT on an orthonormal basis of vector $|0\rangle, \ldots, |N-1\rangle$ is defined to be a linear operator with the following action on the basis state:

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

Equivalently , this can also be seen as

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

We can also represent the Fourier transform in another way . Consider $N = 2^n$ and the basis is the orthonormal basis given by $|0\rangle, \ldots, |2^n - 1\rangle$.The state j can be represented in binary representation as$j = j_1 j_2 j_3 \ldots j_m$.Now the quantum Fourier transform of $|j\rangle$ is given by

$$|j_1 j_2 \ldots j_n\rangle \to \frac{(|0\rangle + e^{2\pi i \; 0.j_n} |1\rangle)(|0\rangle + e^{2\pi i \; 0.j_n j_{n-1}} |1\rangle) \ldots (|0\rangle + e^{2\pi i \; 0.j_n j_{n-1} \ldots j_1} |1\rangle)}{2^{n/2}}$$

6.1 Phase estimation

The Fourier transform is a helpful technique to find the phase of a complex number. This technique, called phase estimation, is based on finding the phase ϕ of a complex number, $e^{2\pi\phi}$, which is the eigen value of an operator U corresponding to eigen vector $|u\rangle$. Using Fourier transform this can be achieved as follows.

We work with two registers , the first one contains t qubits all set to $|0\rangle$ where t is determined by the accuracy upto which we would want to estimate ϕ.

The second register begins in the state $|u\rangle$ and contains as many bits as is necessary to store $|u\rangle$. The computation starts by applying a Hadmard gate to the first register followed by Controlled-U operation (applies U to target bit if control bit is set to 1) on the second register, with U raised to successive powers of 2.The action of this is to make the system in the state:

$$\frac{1}{2^{t/2}}(|0\rangle + e^{2\pi i 2^{t-1}\phi} |1\rangle)(|0\rangle + e^{2\pi i 2^{t-2}\phi} |1\rangle) \ldots (|0\rangle + e^{2\pi i 2^{0}\phi} |1\rangle) = \frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} e^{2\pi i k\phi} |k\rangle$$

The second register is still in original state $|u\rangle$ and has not been mentioned above.

Now we apply the *inverse quantum Fourier transform* on the first register.The third stage of the phase estimation process involves the measurement of first register in the computational basis.

This process gives a good estimate of ϕ

6.2 Application : Order Finding

For a positive co-prime integers x and N,the order of x modulo N is defined as the smallest natural number r such that $x^r \equiv 1 \pmod N$. This problem is a hard problem classicaly in the sense that no alogirthm is known which can solve this in polynomial time in terms of $\log N$. We now demonstrate how phase estimation can be used to make an efficient quantum algorithm for order finding.

The quantum algorithm for order-finding is just the phase estimation algorithm applied to the unitary operator

$$U|y\rangle \equiv |xy \pmod N\rangle$$

where y $\in \{0,1\}^L$. We can also note that the states given by

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi isk/r} |x^k \pmod N\rangle$$

for$0 \leq s \leq r-1$ are eigenstates of U as:

$$U|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi isk/r} |x^{k+1} \pmod N\rangle = e^{2\pi is/r} |u_s\rangle$$

. Now using phase estimation procedure for U , we can indeed find the value of s/r to a great accuracy . With the help of continued fractions and little bit more work , we can find r with an accuracy $\geq \frac{1}{4}$

6.3 Application : Factoring (Shor's Algorithm)

One of the most powerful Quantum algorithm is the Shor's algorithm, which gives a non-trivial factor of a postive composite number N. For given N not a power of a smaller number , we can reduce the factoring problem into phase estimation problem using by using the following two theorems:

Theorem : Suppose N is a L bit composite number then and x is a non trivial solution of $x^2 \equiv 1 \pmod N$, then at least one of $\gcd(x-1, N)$ and $\gcd(x+1, N)$ is a non trivial factor of N.

Theorem : Suppose $N = p_1^{a_1} \dots p_m^{a_m}$ is the prime factorization of N.Let x be an integer chosen uniformly at random, subject to the condition that $1 \leq x \leq N-1$ and x is coprime to N. Let r be the order of x modulo N, then:

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

Combining these two theorems , we can with great certainity find a non-trivial factor for any composite N , starting with the trvival cases and finally using the phase estimation technique . The procedure can be summarised as :

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

Lets take an example , of the number 15, to explain this algorithm:

15 is neither even , nor a power of a natural number.

Choose x = 7 , then gcd(7,15) = 1, so we find the order r of x with respect to N . We create the 2 qubit-system in the state:

$$\frac{1}{2^t} \sum_{k=0}^{2^t-1} |k\rangle\, |0\rangle = \frac{1}{2^t} \Big[\, |0\rangle + |1\rangle + \ldots + |2^t - 1\rangle \,\Big]\, |0\rangle$$

By using t Hadmard gates.Say t = 11. Computing and storing x^k (mod N) in the second bit we change the qubit state into:

$$\frac{1}{2^t} \sum_{k=0}^{2^t-1} |k\rangle\, |x^k (\text{mod } N)\rangle = \frac{1}{2^t} \Big[\, |0\rangle\, |1\rangle + |1\rangle\, |7\rangle + |2\rangle\, |4\rangle + |3\rangle\, |13\rangle + |4\rangle\, |1\rangle \ldots \Big]$$

Though we should now take the Inverse Fourier Transform on first bit, we can measure the second bit giving 4 values 1,7,4 and 13 with equal probabiltity. Say we measure 1 , this collapse the state into $\sqrt{\frac{4}{2^t}} \Big[\, |0\rangle + |4\rangle + |8\rangle \ldots \Big]$

Now we perform the Inverse Fourier transform. The Inverse Fourier transform of a state $\sum y_k\, |k\rangle$ is given by $\sum x_j\, |j\rangle$ where x_j is given by :

$$x_j = \frac{1}{\sqrt{2^t}} \sum_{k=0}^{k=2^t-1} y_k e^{-2\pi ijk/2^t}$$

In our case , y_k is 0 $\forall k \neq 4 * m$, for some integer m. Hence x_j can be reduced as

$$x_j = \frac{1}{\sqrt{2^t}} \sum_m \sqrt{\frac{4}{2^t}} e^{-2\pi ij(4m)/2^t}$$

We see by simple calculations that if j is not a multiple of 512, then the summation is equal to zero, while otherwise the expression simplifies to :

$$x_j = \frac{2 * 512}{2048} = \frac{1}{2}$$

and hence after the IFT, the state is given by $\frac{1}{2}\Big[\,|0\rangle + |512\rangle + |1024\rangle + |1536\rangle\,\Big]$ Now we can measure 0,512,1024 and 1536 with equal probabilities. Say we measure as 512 , then $512/2048 = 1/4$ and hence r $= 4$ (as if there were some common factor then r≥ 8). Now it turns out that for pur choice x=7 , r is even and $x^{r/2}(\text{mod } N) = 4(\text{mod } 15) \neq -1(\text{mod } N)$ and hence one of $\text{gcd}(7^{4/2}1, 15)$ and $\text{gcd}(7^{4/2} + 1, 15)$ must be a factor of 15. We succeed with factor found as 3 (or 5 if chosen latter gcd)

6.4 Applications

The power of Quantum Parallelism is exhibited in the Quantum Fourier transform and its applications. Quantum Fourier transform also finds its applications in various possibilities such as finding discrete logarithms and period finding of a function.

7 Quantum Error Correction

Like the classical possibilities of errors in bits, Quantum computers are also susceptible to errors. In fact, Quantum computers are more prone to errors than classical digital computers because the delicate and uncontrollable nature of Quantum systems. Thus if large scale quantum computers are to be made a reality, a theory of quantum error correction is a must. Before we proceed with quantum error correction , we first begin with classical errors and their correction.

7.1 Classical Error Correction

Classical error correction theory involves:

1. Identification of type of error
2. Introduction of redundancy via encoding and
3. An error recovery procedure

The first step is to identify the type of error. Such an understanding is represented by an error model. It describes the evolution of set of bits inside a channel. A channel can be movement of bits from one place to another or storage of bits or simply the passage of time. An identity channel is one which does not cause any change in the bits , or the change in bits is the Identity function. When errors given by an error model act on a register, we show this by ξ^C acting on the same. Though in general the errors acting on bits can even be depended on each other , we analyse the simple models where we have independent errors. This is enough for our initial understanding of them.

The second part involves introducing redundancy in bits to improve error correction accuracy.This can by done by adding extra bits to a *logic bit* we wish to protect. Such a construction is called a codeword. The basic idea behind this is that even if an error occurs on a codeword , we can still recover the original bits as the other bits contain enough information of the original data.

The third part is of the error recovery. The error recovery operation must be able to unambiguously distinguish between codewords after errors have acted on them. For a set of errors ξ_i^C , to be possible to correct them , we must have

$$\xi_i^C(k_{enc}) \neq \xi_j^C(l_{enc}) \quad \forall k \neq l$$

else , the recovery operation will fail to rectify as two different errors on two different codewords give the same result, and its not possible to a priori know which error has acted. This condition is called the condition for classical error correction . Having the basics of classical error correction theory, we know see an example of the Classical three bit code method.

7.2 The Classical three bit code

Let us consider the simple bit flip channel which flips the bit with a probability of p and leave it unaffected with probability *1-p*. A simple strategy is to increase the number of bits by adding two extra bits, and encode each bit as:

$$0 \rightarrow 000$$

$$1 \rightarrow 111$$

This can be done by first adding two ancillary bits to the logical bit and then copying the first bit into the other bit.

To be able to design a recovery operation which acts on the codewords after the bit flip channel , we must have the condition of error correction to be satisfied. Thus , if we consider that at most a single bit flip occurs on each codeword, then we can recover our original register , and this is a set of correctable errors.

The recovery operation can now be understood in the following way:
Say the codeword after passing through error channel have all three bits equal to each other. Then we can be sure that the no error has occured. If otherwise, one of the bits is flipped , then we would have that other 2 bits are equal and that value must be the value of the bit before the error occured.

Thus , we have a recovery model which can easily be implemented by noting that we just need to compare any 2 distinct pairs of bits.
We now proceed with our discussion on Quantum error correction.

7.3 Error models for Quantum Computing

Like the Classical case , where in errors could have been depended on each other , we take the simpler case where they are not. However unlike the bit flip channel being the only possible channel in classical bits , qubits can have many possible errors such as rotation of phases, change of amplitudes. We describe two of such errors namely the bit flip and the phase flip.

7.3.1 Three bit quantum code for Bit flip error

The bit flip channel operating on a system can be interpreted as applying the Identity gate with a probability of 1-p and applying the bit flip , X gate with a probability of p.
Encoding:
Unlike the repetetion of bits in the classical encoding , we cannot copy every random qubit , as this would violate the no-Cloning theorem. We however can repeat the computational basis of bits , as they form an orthogonal basis. This can be done by an unary operator U, which acts on $|\psi\rangle$ tensed with two ancilla bits initially set to $|0\rangle$, to encode the into $|\psi_{enc}\rangle$ given as:

$$|\psi_{enc}\rangle = U\,|\psi\rangle\,|0\rangle\,|0\rangle$$

. The unary operator U , is similar to the classical case , where it encodes the qubit $|0\rangle$ as $|000\rangle$ and qubit $|1\rangle$ as $|111\rangle$. For the superposition of these two states , it encodes as:

$$\alpha\,|0\rangle + \beta\,|1\rangle \xrightarrow{U} \alpha\,|000\rangle + \beta\,|111\rangle$$

One may not that this is not the same as copying the qubit(that would mean $\alpha\,|0\rangle + \beta\,|1\rangle \rightarrow (\alpha\,|0\rangle + \beta\,|1\rangle)^{\otimes 3}$, thus not violating the no-Cloning theorem.

Recovery operation:
Similar to clasical case, we can apply the Toffoli gate , or the CCNOT gate , where the first bit is flipped if both the control bits (in this case the ancillary bits) are set to 1, which can be checked before using CNOT gates. This way we can rectify a bit flip error on a qubit.

The given procedure is just the classical analogue of the three bit code for single bit flip error , called as the **Three bit Quantum code.**

7.3.2 Three bit quantum code Phase flip error

The phase flip channel operating on a system can be interpreteed as applying the Identity gate with a probabilty of 1-p and applying the phase flip Z gate with a probability of p. There is no classical analogue of the phase flip , however we can in fact change a phase flip error to a bit flip error by changing our computational basis. If we work in the Hadmard basis states then we see that in fact a phase flip channel is a bit flip channel in this basis,

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \xrightarrow{Z} \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \xrightarrow{Z} \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle$$

Encoding and Recovery operation:
Based on the previous discussion , all it remains to encode in the computational basis of $|+\rangle$ and $|-\rangle$. This can be done by applying the Hadmard gates to each bit , to our previous encoding operator. Thus our encoding operation now encodes as:

$$\alpha |0\rangle + \beta |1\rangle \xrightarrow{U} \alpha |+\rangle |+\rangle |+\rangle + \beta |-\rangle |-\rangle |-\rangle$$

And similarly, the recovery operation first checks for parities of the qubits in the Hadmard basis , and then we switch back to the standard basis by applying Hadmard gates again. Thus making it almost the same as the bit flip channel.

7.4 The Nine qubit Shor code

The three qubit bit-flip and phase-flip errors can be combined to give the nine-qubit code which corrects bit-flip or phase flip on any one of the nine qubit. It also allows for the correction of simultaneous bit and phase flip on the same qubit. Thus , including the Identity error operator in the basis of errors , we can now correct all possible type of errors. Encoding for the Shor code works in two stages. First each qubit is in the three qubit phase-flip code. Next , each of the qubits in the three phase-flip code is now encode as the three qubit bit-flip code. This can be summarised as:

$$|0\rangle \xrightarrow{1^{st}} |+\rangle |+\rangle |+\rangle \xrightarrow{2^{nd}} \frac{(|000\rangle + |111\rangle)^{\otimes 3}}{2\sqrt{2}}$$

Suppose we subject these codewords to both the bit-flip and the phase-flip channels, with the restriction that there is at most one bit flip and at most one phase flip. We can view the combined effect as a single channel, whose effect is a bit flip with some amplitude, and a phase flip with some other amplitude, and a combination of both. In a way analogous to the bit-flip channel seen previously, we can see that bit flip X operator on any of the nine qubits will move the codeword to an orthogonal subspace. The phase flip Z operator on any of the qubit will also move the code to an orthogonal subspace through a sign change between the triplets of qubits. A peculiarity of this code not encountered in the three-bit codes is that applying the Z error on any member of the triplet will move the code to the same subspace. This will not prevent error correction as we only

need to know where the code has moved to undo the error. Again , if both X and Z errors act together , we get another orthogonal subspace . Thus no element of can infact belong to more than one error , and thus we satisfy the Condition of error correction.
Continuing , the recovery operation can again be performed by noticing now that to recitfy the bit flip error we need to check the parity of the individual subset of the three qubits , while for phase flip , we need to check the parity of the entire subset and compare it with others , and thus we can make a circuit which implements exactly this.

8 Conclusion

Before concluding , I want to discuss an interesting branch of Quantum Computation , namely Quantum cryptography. My interest in Teleporation and Quantum Error correction made me read about certain protocols in Cryptography. One of them is the BB84 protocol.
BB84 protocol:
Say Alice wants to send a private key to Bob. To do this she starts with a bit string **a**. Alice then encodes **a** with a bit string **b** and sends the qubit:

$$|\psi\rangle = \otimes_{i=1}^{n} |\psi_{a_i b_i}\rangle \, ;$$

where $\psi_{a_i b_i}$ is the encoded string in different basis based on a_i and b_i as:

$$|\psi_{00}\rangle = |0\rangle$$

$$|\psi_{10}\rangle = |1\rangle$$

$$|\psi_{01}\rangle = |+\rangle$$

$$|\psi_{11}\rangle = |-\rangle$$

Note that the bit b_i is what decides which basis a_i is encoded in (either in the computational basis or the Hadamard basis). The qubits are now in states that are not mutually orthogonal, and thus it is impossible to distinguish all of them with certainty without knowing **b**. Now Alice sends the qubit through a public channel ξ to Bob. If Bob receives the same then he can be sure that an eavesdropping agency, Eve cannot be having the exact same copy of the (due to the No-Cloning Theorem as qubits are in non-orthogonal states).

Now Bob generates a string $\mathbf{b}'$ of the same length as **b** and then measures the qubits he recieved from Alice, in the space of classical or Hadmard basis based on his **b'** , making a bitstring $\mathbf{a}'$. He now announces that he received Alice's message. Now Alice anounces her string **b** , and now Bob and Alice discard all the bits of **a**and **a'** and discard bits where **b**and $\mathbf{b}'$ do not match.

From the remaining k bits where both Alice and Bob measured in the same basis, Alice randomly chooses k/2 bits and discloses her choices over the public channel. Both Alice and Bob announce these bits publicly and run a check to see whether more than a certain number of them agree. If this check passes, They now have a private key to use for information reconciliation and privacy amplification techniques to create some number of shared secret keys. Otherwise, they cancel and start over.

With this we conclude our report. Surely there is no end to the fascination provided to us by Quantum Mechanics , and in specific, to Quantum Computing!

9 Bibliography

- Quantum Computation and Quantum Information - Nielsen and Chuang
- An introduction to Quantum Computing - Kaye, Laflamme and Mosca
- https://www.youtube.com/watch?v=X8jsijhllIA
- https://www.youtube.com/watch?v=b3NxrZOu_CE
- https://www.youtube.com/watch?v=CBrsWPCp_rs
- https://www.idquantique.com/quantum-safe-security/overview/quantum-key-distribution/