Quantum Computing – Mid Term Report

Prathamesh Sachin Pilkhane

Roll number:200050109

Mentor:Ajinkya Werulkar

Extended Plan of Action:

Week 12June – 26Jun: Endsem Preparation + Endsems

Week 26Jun - 3July:Lesson 10 Quantum Error correction from Quantum Computation and Quantum Information - Nielsen and Chuang.

Week 3July – 10July : Learning Q# and if time permits Quantum Information Theory from Quantum Computation and Quantum Information - Nielsen and Chuang.

Topics covered till date:

1. Introduction and Overview
2. Quantum Preliminaries
3. Postulates of Quantum Mechanics
4. Quantum Gates
5. Quantum Fourier Transform

1.Introduction and Overview

Through this Summer of Science report, we aim at building a clear picture on Quantum Computing ,Quantum Error Correction and Quantum Information Theory.The primary source being followed is Quantum Computation and Quantum Information - Nielsen and Chuang. The report starts with some basic Mathematical Preliminaries followed by postulates of Quantum Mechanics. By the end of this mid term report we also cover some Quantum Algorithms based on Quantum Fourier transforms. 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.Also , unlike the classical bits , which can be only present in either the state of 0 or 1 , Quantum Computation uses special bits, called qubits, which can be in more than one state simultaneously.(strictly speaking , we say a qubit is in a superposition of basis vectors, whose coefficients can only be measured given some information or measurement.)

2.Quantum Preliminaries:

2.1. Vector Spaces:

Quantum Computation depends heavily on the understanding of Vectors and Hermitian Matrices.

Though any basis of vectors works for our Computations,we in general stick to the notation of two basis vectors as:

|0> = $\begin{pmatrix}1\\0\end{pmatrix}$ and |1> = $\begin{pmatrix}0\\1\end{pmatrix}$

This particular choice of basis is just for convenience. However , we can always choose any other basis for our computation. One such example is :

|+> = (|0> + |1>)/√2 and |-> = (|0> - |1>)/√2

Any vector/qubit now can be represented as

|v> = a|0> + b|1> (1.1)

Where |a|^2 is the probability of observing |0> in measurement and |b|^2 is the probability of observing |1> in a measurement.

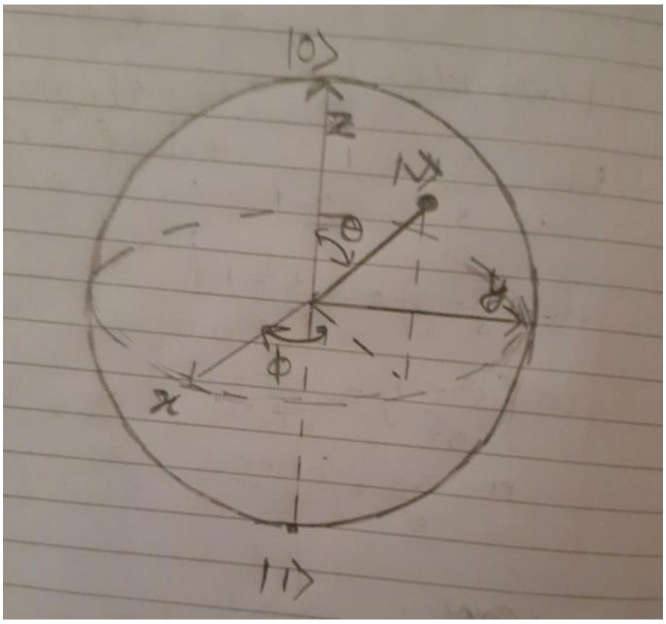
|a|^2 + |b|^2 = 1, as total probability of measuring either states is 1.
We may also note that after the measurement of a qubit, the qubit collapses into a particular state.

2.2 Bloch-Sphere Representation:

Eq 1.1 can also be written as

|v> = (cos θ/ 2) |0> + e^{iphi} (sin θ /2) |1>

Which is correct upto a global phase factor(any measurement made on this qubit , is equivalent to making a measurement on this qubit times some phase factor)
Now, we can represent |v> on a unit sphere with theta and phi as coordinates as:



As we shall further see in Quantum Gates, any operation on qubits essentially changes these coordinates.

This representation thus helps us understand what is happening, making it easier for us to imagine than doing rigorous mathematics each time.

However this representation is only for a single qubit.

2.3 Multiple Qubits:

A system of 2 bits classically can have four possible configurations(00 , 01 , 10 ,11).Similarly if we have a system with 2 qubits , it can be represented as

|v> = a1|00> + a2|01> +a3|10> +a4|11>

Where |xy> represents the tensor product of two vectors x and y

As in the single qubit system,here as well we must have the sum of squares of magnitudes of coefficients as 1.

An important 2 qubit system is the Bell state:

$$|v\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$$

This state is responsible for some interesting phenomenon as the Quantum Teleportation and Super Dense coding.

The speciality of this gate is that measuring either of the qubits collapses the state such that both qubits have the same value.

3. The Postulates of Quantum Mechanics:

Quantum systems are guided by a set of 4 postulates:

3.1 State Space:

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.

3.2 Evolution of State:

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,

$$|v'\rangle = U|v\rangle$$

In the study quantum computing, we would be using certain gates(similar to the classical gates like AND,OR,NAND,etc.).This postulate helps us in writing a unitary operator for the quantum gates, as applying a quantum gate is the same as the system evolving under certain conditions.

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.

3.3 Measurement:

Postulate 3: Quantum measurements are described by a collection {Mm} 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 $|\psi>$ immediately before the measurement then the probability that result m occurs is given by

$$P(m) = < \psi|M_m^\dagger M_m| \psi>$$

and the state of the system after the measurement is

$$M_m|\psi >/ \sqrt{}(<\psi|M_m^\dagger M_m|\psi>)$$

The measurement operators satisfy the completeness equation,

$$\sum M_m^\dagger M_m = I$$

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

This postulate thus tells us about the collapsing of state of system after a measurement is performed on the system.
We perform measurements with the help of Measurement operators, which by this postulate ,is a collection of all possible measurement of a given measurements. Sum of all probabilities of all possible measurements is 1.

3.4 Composite Quantum Systems:

Postulate 4. The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. If the state of the ith component is |ψi> and total we have n components then the net state is given by

$$|\psi 1> \otimes\ |\psi 2> \otimes \cdots |\psi n>$$

Here ⊗ denotes the tensor product.

This notion helps in working with more than 1 qubits at the same time. We already encountered an example in the multiple qubit system.

4.Quantum gates:

Like the classical bit gates such as AND, OR, etc., we also have similar gates in Quantum Computing.However, unlike the gates AND, OR which are irreversible i.e. we cannot get information of the original state of system, Quantum Gates must be reversible by Postulate 2.

This is since a Unitary operator always has an inverse and so it must always be possible to get the original state from the new state.

Some standard Single qubit gates are:

1)$\mathrm{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, the identity gate, also represented as

$\mathrm{I} = |0><0| + |1><1|$

2)X = $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, Y = $\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ and Z = $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

3)Hadmard gate H = $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}/\sqrt{2}$

4.1 Multiple qubit gates:

The most used gate in multiple qubit system is the controlled-NOT gate or CNOT gate. The gate works on two bits, the first is called the control bit and the second is called the target bit.The action of this gate can be described as negating the target bit if the control bit is 1.

$$|A,B\rangle \rightarrow |A, B \oplus A\rangle$$ where $\oplus$ denotes addition modulo 2.

This gate is analogue of XOR classical gate. We can further modify this gate as instead of negating the second bit, we apply some Unitary operator U on the target bit, if the control bit is set to 1.

Another quantum gate is the CCNOT gate or the Toffoli gate takes in 3 inputs, and negates the 3rd qubit based if and only if both the other qubits are set to 1.

This gate, if 3rd bit is set to |0>, computes the AND of the other 2 qubits.

The CCNOT gate is a universal gate i.e. any standard gate AND,OR,NAND , can be efficiently transformed into a reversible one, given that we use some garbage inputs(like the 3rd bit being |0> in the AND gate describe above)

4.2 No-cloning theorem

There exists no circuit which can copy a n qubit system. This is contrast to the classical picture. The proof of this statement follows by contradiction:

Suppose there did exist a circuit which could copy a n bit system.

Say our original state to be copied is A given by |v> , an unknown but pure quantum state, and a target slot B , initially started given by |s> .Then the state of this system in the start is given by:

$$|v\rangle \otimes |s\rangle$$

So the circuit, essentially being a Unitary operator must act as:

$$U(|v\rangle \otimes |s\rangle) = |v\rangle \otimes |v\rangle$$

Consider another state A given by |u> , then circuit applied on this gives:

$$U(|u\rangle \otimes |s\rangle) = |u\rangle \otimes |u\rangle$$

Taking inner product of these two equations gives:

$$\langle v|u\rangle = \langle v|u\rangle^* \langle v|u\rangle.$$

But this means , either <v|u> is one, i.e. |v> = |u> or <v|u> = 0, i.e |v> is orthogonal to |u>. So any circuit which is supposed to clone a random state, can only clone states which are orthogonal to each other, and thus a general cloning circuit is impossible.

4.3 EPR pairs and Quantum Teleportation:

Consider a circuit which acts on 2 qubits , circuit being a Hadmard gate applied to the first qubit followed by a CNOT gate.

Given the four possible inputs , $|00>$ $|01>$ $|10>$ and $|11>$ we get the corresponding outputs as:

$|00> \rightarrow (|00> + |11>)\sqrt{2}$

$|01> \rightarrow (|01>+|10>)/\sqrt{2}$

$|10> \rightarrow (|00> - |11>)/\sqrt{2}$

And $|11> \rightarrow (|01> - |10>)/\sqrt{2}$

These four states are called Bell states, sometimes as EPR pairs after some of the people : Bell , Einstein , Podolsky and Rosen, pointed out the strange behaviour of these states.

Quantum 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 $|v>$ 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:

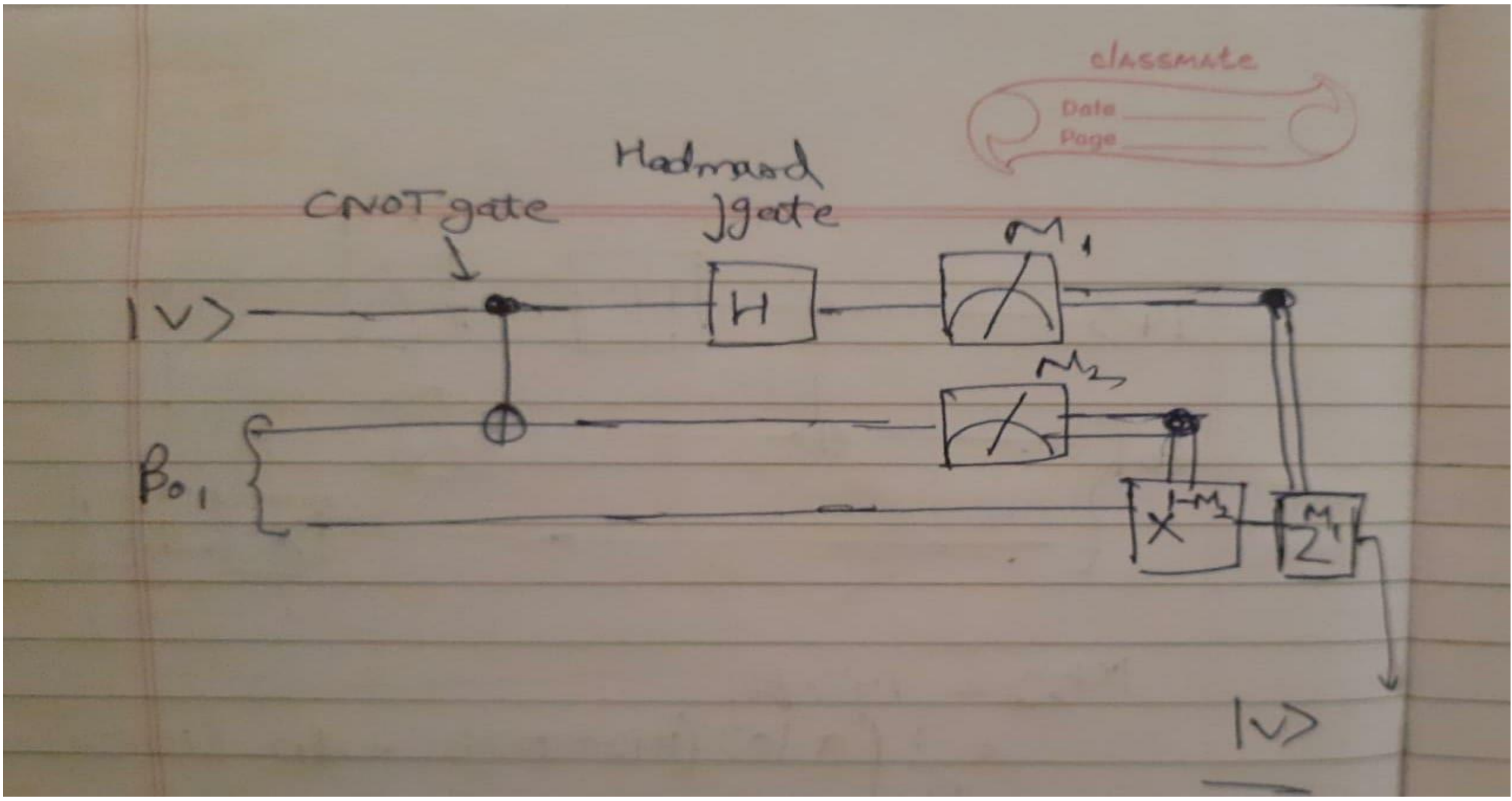
Lets say the EPR pair shared by Alice and Bob is

$(|01>+|10>)/\sqrt{2} = b_{01}$

And the unknown state $|v>$ be represented by

$|v> = a|0> + b|1>$

Then , a circuit described as:



is the Quantum Teleportation circuit for this pair.

Proof:

The state of the pair just before any computation is:

$$|u\rangle = 1/\sqrt{2}(a|0\rangle(|01\rangle+|10\rangle) + b|1\rangle(|01\rangle+|10\rangle)$$

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:

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

Applying Hadmard gate to the first bit now gives us:

$$|u''\rangle = ½[(a(|0\rangle+|1\rangle)(|01\rangle+|10\rangle) + b(|0\rangle-|1\rangle)(|11\rangle+|00\rangle)]$$

Which can be simplified as:

$$|u''> = \frac{1}{2}[|00> (a|1> +b|0>) + |01>(a|0>+b|1>)+|10>(a|1>-b|0> + |11>(a|0>-b|1>)]$$

Now when Alice measures the 2 qubits in her possession , she collapses the state |u''> into one of the four possible states.

If Alice measures |00> then Bob's qubit is in state a|1> +b|0>, which he can apply X gate and get the original |v> back;

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

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

And if Alice measures |11> then Bob applies the Z gate on his qubit , and thus getting |v> 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 making Quantum Teleportation does not enable faster communication than light.

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