Comprehensive Report : Quantum Computing and Quantum Information

SATISH BHAMBRI, Masters in Software Engineering, Arizona State University

This report discusses the lectures and writings of Dr Umesh Vazirani on the subject of Quantum Computing and the book Quantum computation and Quantum Information and presents a comprehensive study of the various topics in this research..

CCS Concepts: • **Computer systems organization → Quantum systems.**

KEYWORDS

Fourier Sampling, Simon's Algorithm, Reversible Computation, Simulating Classical qubits, Recursive Fourier Sampling, Quantum Fourier Sampling, Quantum factoring, Quantum Algorithms, Quantum Gates, Quantum Circuit, Continuous quantum states, Particle in a box, Observables, Expectation values, Unitary evolution, Quantization, Quantum computing.

1 INTRODUCTION : Quantization

In last two decades, computing paradigm has seen a number of evolving phases but the one which has established altogether new roots in the computing paradigm is the quantization of classical paradigm, ie, the quantum computing. Our computing industry has been directed according to the Moore's law which predicts that the number of transistors on a Si chip doubles every 18 months to two years. But as the number of transistors are increasing, their size is decreasing only to enter the quantum realm where the classical physics' laws are no longer applicable. [1] [2] Hence, the quantum computing. Important features of Quantum mechanics which deviate from the classical paradigm are :

- Quantum mechanics' laws forbid the complete knowledge of the system's state, hence, a measurement only reveals a small amount of the information about the quantum state of the system.
- When we measure the state of a quantum system, this fundamental act disturbs the state of the system.
- Trajectories of quantum entities are not defined.
- Quantum mechanics is inherently probabilistic.
- Quantum entities behave both like waves and particles, depending on the conditions.

2 SUPERPOSITION : Young's Double Slit Experiment

Light displays dual nature (wave – particle duality), behaving as a stream of particles or corpuscles (as Newton called them) in some situations and as an electromagnetic wave in some. Young's double slit experiment, performed in early 1800's, established the wave nature of light. This experiment includes a monochromatic light source, and an equidistant, thin and identical slits, as shown in the figure, and a detecting screen. [2] When the light source is turned on, we see interference patterns on the detector screen, thereby, the wave

nature of the light is established.

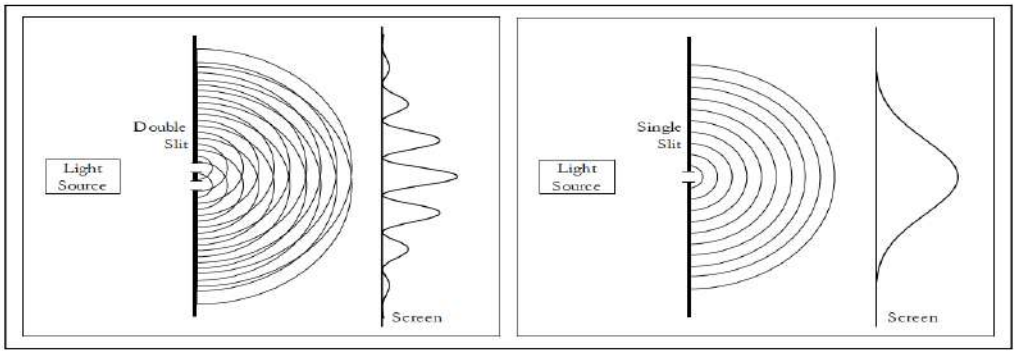
But when we decrease down the intensity of the light to very low, which Young was unable to do, when this experiment was performed originally, such that we make sure that only single photon is released every second, then what we observe is in total contrast to the intuition. And we observe similar results if we take electrons, which intuitively we consider as particles. [3] [1] [2]

A brief insight into the experiment, consider a stream of bullets, instead of the light source. Now at the detector screen, we will observe a distribution pattern. If we close one of the slits, the bullets would only be detected behind the opened one and some deflected bullets in the surrounding area. Hence, the normal distribution.

Consider a point y on the detector screen, such that P1(y) denotes the probability that the bullet lands at point y when only slit 1 is open, and correspondingly P2(y). Say, that P12(y) denotes the probability of bullet landing at point y when both the slits 1 and 2 are open.

$P12(y) = P1(y) + P2(y)$.

Considering, waves (for instance, water waves), then we see the interference pattern as shown in the figure below.



[2]

In this case, we observe dark patches where waves are out of sync and very bright patches where they are in sync and positively superimpose each other.

Calculations, in the case of waves involve the height of the waves or the Amplitudes.

$H12(y) = H1(y) + H2(y)$

Intensity at any point y would be given by the,

$I12(y) = (H12(y))^2$

Hence, the difference from the case of bullets. And hence, the interference pattern in case of waves.

Now, coming back to our point of decreasing the intensity of light such that only one photon passes through, we intuitively expect the nature of distribution to resemble the distribution pattern of the bullets. In this case, photodetectors on our detector screen would report the photon every second, and only one photodetector would do so every second. [2] [1]

Logically, one photon should go through one slit at a time, producing the bullet pattern, but in this case, we still observe the interference pattern. The explanation is that, since the trajectories of a quantum system is not defined, hence photon goes through both the slits and interferes with itself. [3] [2] [1]

If we try to close one slit, then the interference pattern goes away and we get normal distribution. This reflects the measurement principle of the Quantum paradigm, wherein measuring the system alters the state of the system.

This experiment with the stream of electrons yield the same results following the following amplitude equations.

$A12(y) = A1(y) + A2(y)$

$P12(y) = |A12(y)|^2$.

Where, A12(y) represents the amplitude of the resultant wave after interference at any point y and P12(y) represents the Probability that the photon is detected at the point y, when both slits 1 and 2 are open.

3 AXIOMS, QUBITS AND KET NOTATION

Following are the basic axioms of Quantum Mechanics and hence the quantum computing [3]:

- The Superposition principle: This principle describes how a particle can be superimposed among multiple state at the same time.
- The Measurement principle: This principle describes how the measurement of a particle, changes it's state and the amount of information that we can access from a particle.
- The Unitary evolution: This axiom states the evolution of a quantum system in time.

3.1 The Superposition principle:

Let's take a system, such as hydrogen atom, with k different states. In this case, an electron of the hydrogen atom is allowed to be in one of the discrete set of energy levels, beginning from the ground state, the first excited state, the second excited state and so on. We denote the k different levels of our hydrogen atom or k different states as $|0\rangle$, $|1\rangle$, …, $|k-1\rangle$, being the ground state, first excited state, .., $(k-1)^{th}$ excited state, respectively.

Superposition principle tells us that the state of the electron is given by :

$$|\psi\rangle = \alpha 0|0\rangle + \alpha 1|1\rangle + \ldots. + \alpha k\text{-}1|k\text{-}1\rangle$$

Where ψ represents the wave function, describing the system, and $\alpha 0$, $\alpha 1$, $\alpha k\text{-}1$ the normalized, complex coefficients complex coefficients such that $\Sigma_j |\alpha_i|^2 = 1$.

This notation, $|\psi\rangle = \alpha 0|0\rangle + \alpha 1|1\rangle + \ldots. + \alpha k\text{-}1|k\text{-}1\rangle$, is called the Dirac's Ket notation and the normalization on the complex amplitudes means that the state is a unit vector in a k dimensional complex vector space, known as, Hilbert space. [2] [1] [3]

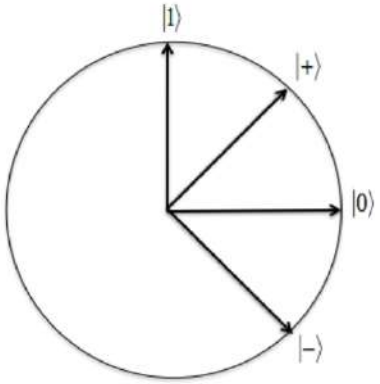


Figure 1.2: Representation of qubit states as vectors in a Hilbert space.

Mutually orthogonal vectors can also be written as:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad |k-1\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

These k mutually orthogonal unit vectors, in k-dimensional complex vector space form the orthonormal basis for that state space, and are called the standard basis. Hence, given any two states α0 |0> + α1 |1> + • • • + αk−1 |k – 1>, and β|0> + β|1> + • • • + β|k – 1>, we can compute the inner product of these two vectors, which is Σα*jβj. Hence, for orthogonal vectors, their inner product needs to be zero, as the absolute value of the inner product is the cosine of the angle between these two vectors in Hilbert space. [2]

Consider a state of the system given by :

$$|\psi\rangle = \sum_k a_k |k\rangle ,$$

where the kets |k> form the basis as :

$$|\psi\rangle = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{N-1} \end{pmatrix}$$

Then, the inner product of this state with itself is given by:

$$\langle \psi, \psi \rangle = \begin{pmatrix} a_0^* & a_1^* & \cdots & a_{N_1}^* \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{N-1} \end{pmatrix} = \sum_{k=0}^{N-1} a_k^* a_k = \sum_{k=0}^{N-1} |a_k|^2$$

Dirac introduced a better representation of this inner product, by defining a the conjugate transpose of a ket as “bra”, and represented by [2] [1] :

$$\langle \psi | = |\psi\rangle^\dagger = \sum_k a_k^* \langle k| \,.$$

This object acts on the ket as a function and gives a number. Hence the inner product now can be calculated as :

$$\begin{aligned} \langle \psi | \psi \rangle &= \left(\sum_j a_j^* \langle j| \right) \left(\sum_k a_k |k\rangle \right) \\ &= \sum_{j,k} a_j^* a_k \langle j|k\rangle \\ &= \sum_{j,k} a_j^* a_k \delta_{jk} \\ &= \sum_k |a_k|^2 \end{aligned}$$

Now we can write the inner products of any two states as follows :

$$\langle \psi | \phi \rangle = \sum_{j,k} a_j^* b_k \langle j | k \rangle = \sum_k a_k^* b_k$$

Where,

$$|\phi\rangle = \sum_k b_k |k\rangle .$$

and,

$$\langle \psi | \phi \rangle = \langle \phi | \psi \rangle^* \in \mathbb{C}$$

3.2 The Measurement principle:

This principle describes the extraction of the information from the superimposed world of an electron or any particle displaying superposition. A measurement of this k-state superimposed system yields one of the k possible outcomes with the probability of that outcome to be the square of the magnitude of complex coefficient, but it also alters the state of the system, such that the new state is exactly the outcome of the measurement, that means that if the outcome of the measurement is j, then after the measurement the qubit is in state |j>.

Hence, you can't collect any additional information following about the amplitudes following the measurement. Therefore, measurement is a probabilistic rule for projecting the state vector on the one of the vectors of the orthonormal basis [3] [2] [1].

3.3 Qubits

Qubits are the quantum bits, quantum analog of the classical bits, and they form the basic building blocks having all fundamental quantum phenomenon. Qubits are basically, 2 state quantum systems. For instance, taking the aforementioned hydrogen atom and considering only two of its states.

$$|\psi\rangle = \alpha||0\rangle + \beta\,|1\rangle \qquad \text{with} \quad \alpha, \beta \in \mathbb{C} \quad \text{and} \quad |\alpha|^2 + |\beta|^2 = 1.$$

The simplest measurement is in the standard basis, and measuring |ψ> in this {|0>, |1>} basis yields 0 with probability |α|2, and 1 with probability |β|2 and this measurement alters the state of the system. Examples of Qubits could be atomic orbitals, photon polarization, and spin of the electrons.

4 Two Qubits and Entanglement

Let us consider a two-state quantum system consisting of two qubits, which is described by two hydrogen atoms, such that considering the system to be comprising of two electrons from these two atoms, wherein the electrons can either be in ground state for both atoms or excited state for both atoms or excited for first atom and in ground state for the second or vice versa. So basically, these four states are possible.

By superposition principle, quantum state of the aforementioned system can be represented by the following state vector and thus the system can be in any linear combination of these four classical states :

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \quad [2]$$

The measurement of this 2-qubit system reveals only two bits of information with the probability as the square of the coefficients of that particular state. For example, say we measure the above system, the probability that we'll find both the qubits in the state 0($|00\rangle$) is $|\alpha_{00}|^2$. Then the system will fall into a state where both electrons will be in the ground state as per the measurement principle. [1] [2]

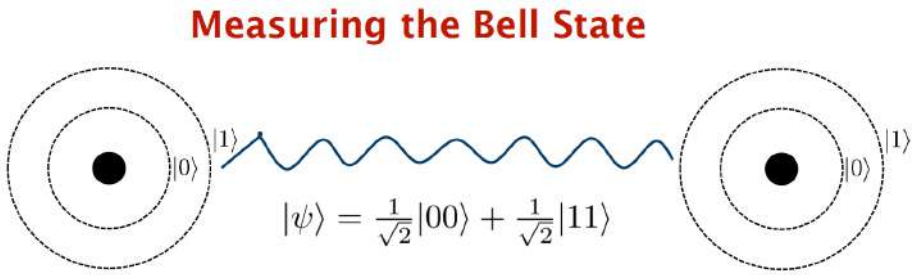
But what if we just measure the first qubit to be in 0 and not the second one? What would be the probability outcome for that?

Pr {1st bit = 0} = Pr{00} + Pr {01} = $|\alpha_{00}|^2 + |\alpha_{01}|^2$. Therefore, the probability outcome is exactly the same as it would have been had we measured both the qubits. [2]

Therefore, in a general sense we can say that given the state of first qubit to be $\alpha_0|0\rangle + \alpha_1|1\rangle$ and the state of the second qubit to be $\beta_0|0\rangle + \beta_1|1\rangle$, then the combined state of the two qubit system is given by $\alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle$.

But can every state of two qubits be decomposed in this way? We have found some states in nature which cannot be. They are of the form $|\Phi^+\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$. Such states are called the Entangled states, giving rise to the phenomenon of Entanglement.

When we have two entangled qubits, we cannot determine the state of each qubit independently. For instance, say, if the first and respectively, the second qubit of $|\Phi^+\rangle$ is measured then the outcome is 0 with probability 1/2 and 1 with probability 1/2. However, if the outcome is 0, then a measurement of the second qubit results in 0 with certainty. This is irrespective of the spatial separation between the two particles.



[2] [1]

5 EPR Paradox

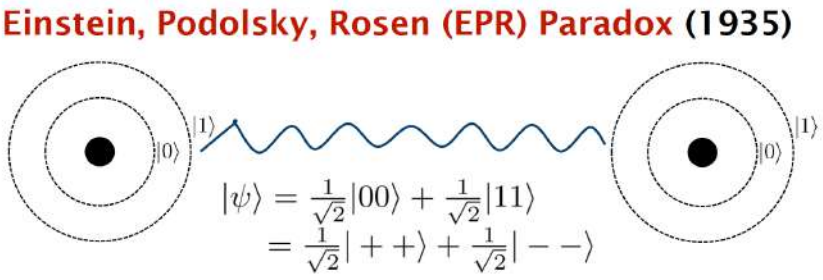
Albert Einstein considered Quantum mechanics to be an incomplete theory and believed that randomness of quantum measurements reflected our lack of knowledge about additional degrees of freedom, or "Hidden variables", of the quantum system.

Einstein, along with Podolsky and Rosen worked on this line of reasoning in a paper they wrote in 1935, introducing the famous Bell states ($|\Phi^+\rangle = 1/\sqrt{2}\ (|00\rangle + |11\rangle)$). For the Bell states, if we measure the first qubit in the bit basis, the other qubit is determined in the bit bases, no matter how far they are apart. [2]

Lets assume that the qubits are very far apart, say one light second, and we measure the qubit 1 in the standard basis and half a second later we measure qubit 2 in the same basis; the two measurements must agree. But qubit 2 could not possibly know which basis was qubit 1 measured in until a complete second after we measure it because light itself takes one second to reach from qubit 1 to qubit 2. Both qubits couldn't have communicated any information in that time.

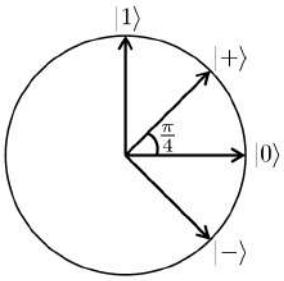
From the above findings, Einstein, Podolsky, and Rosen formulated the result that because qubit 2 cannot have any information about which basis qubit 1 was measured in, its state in both bit and sign bases is simultaneously determined, which is something that quantum mechanics does not allow.

Hence, they suggested that quantum mechanics is an incomplete theory, and there is a more complete theory where "God does not throw dice." or a " local hidden variable theory" which describes the predictions of quantum mechanics, but without resorting to probabilistic outcomes.



6 Bit And Sign Bases

As discussed, we have a orthonormal basis represented by quantum analog of classical bits 0 and 1 as |0> and |1>, which is called the Bit Bases, but these are not only the possible bases which can be used to represent any states. We can have infinitely many orthonormal bases, which can be used to represent a quantum state. Another important and most frequently basis is the Sign basis which are obtained by rotating the Bit basis by an angle of 45 degrees on the geometric plane and represented by |+> and |->. [3] [1] [2]



[2]

7 Uncertainty Principle

Uncertainty principle given by Werner Heisenberg states that “One can never know with perfect accuracy both of those two important factors which determine the movement of one of the smallest particles- its position and its velocity.”

Quantum analog of this principle deploys the Bit and Sign basis, where the Bit basis corresponds to position and Sign basis corresponds to velocity/ momentum. So the principle boils down to the question of if we can know both bit and sign of a qubit simultaneously? Bit of a qubit can be |0> or |1>, and the Sign of the qubit can be |+> or |->.

To quantify this, we define an entity Spread of a quantum state. Consider a quantum state being represented in Bit and Sign basis as follows: [2] [1] [3]

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle = \beta_0|+\rangle + \beta_1|-\rangle$$

Correspondingly, we define the spread in standard and sign basis, respectively as:

$$S(|\psi\rangle) = |\alpha_0| + |\alpha_1|$$

and,

$$\hat{S}(|\psi\rangle) = |\beta_0| + |\beta_1|$$

Therefore, the spread for |0> and |+>, in both Bit and Sign basis respectively could be calculated as follows :

$$S(|0\rangle) = 1 + 0 = 1 \qquad \hat{S}(|0\rangle) = \tfrac{1}{\sqrt{2}} + \tfrac{1}{\sqrt{2}} = \sqrt{2}$$

$$S(|+\rangle) = \tfrac{1}{\sqrt{2}} + \tfrac{1}{\sqrt{2}} = \sqrt{2} \qquad \hat{S}(|+\rangle) = 1 + 0 = 1$$

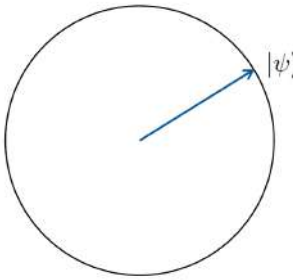
We have defined the spread this way because of the following reasoning. As per the aforementioned calculations, if we know the bit value perfectly, |0> or |1>, the spread is 1, in either case. But in the case that we don't know the bit value, say in case of |+>, that is we have the state plus, then alpha 0 and alpha 1 are both 1 over square root 2 and therefore, the spread is square root 2. Hence, the only way the spread can be small implying it to be 1, is if you know the bit perfectly. And the farther from 1 it is, the more uncertain, the less certain you are about the bit value. Same is the scenario for |+> and |-> basis. [3] [1] [2]

Thus, Uncertainty principle for bit and sign states is that if you look at the spread in the standard basis and multiply by the spread in the sign basis or any qubit, then this product is at least square root 2. Which means that both values cannot simultaneously be 1, at least one of them has to be square root of square root of 2. So in that sense it states that you must be uncertain about either one or the other.

Uncertainty principle for bit and sign: $S(|\psi\rangle)\hat{S}(|\psi\rangle) \geq \sqrt{2}$ for any $|\psi\rangle$.

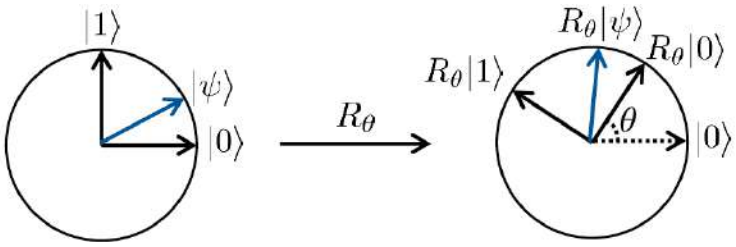
8 Unitary Evolution

Principle of Unitary evolution defines how a system evolve in time, by the rotation of the Hilbert space.



$$|\psi\rangle = \alpha_0|0\rangle + \cdots + \alpha_{k-1}|k-1\rangle = \begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_{k-1} \end{pmatrix} \in \mathbb{C}^k$$

The angles between the vectors are preserved while rotating, thereby its analogous to the rigid body rotation. This rotation is a linear transformation represented by the matrix. [2] [1]



$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

---

9 Quantum Gates

We discussed the Unitary evolution, which, geometrically is the rigid body rotation of the Hilbert space, thus resulting in the transformation of the quantum state vector such that the length of that vector remains constant during the transformation. We specify a Unitary transformation of the given vector in the Hilbert space by mapping the basis states |0> and |1> to orthonormal states $|v_0\rangle = a|0\rangle + b|1\rangle$ and $|v_1\rangle = c|0\rangle + d|1\rangle$, a linear transformation on C^2(The complex vector space). [3]

$$U = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \qquad U^\dagger = \begin{pmatrix} a^* & b^* \\ c^* & d^* \end{pmatrix}$$

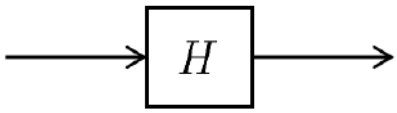
Where U and U perpendicular represent the transformation matrix and transpose of the transformation matrix respectively, and they satisfy the following relation:

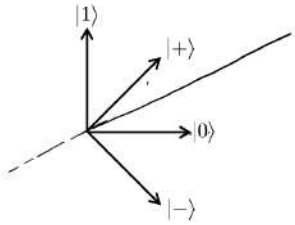
$$UU^\dagger = U^\dagger U = I.$$

Quantum gates are basically these unitary transformations on the qubits. Some of the prominent One qubit quantum gates are : [1] [2]

- Hadamard gate

Hadamard gate is the unitary transformation which is reflection around Pi/8 axis in the real plane.





$$H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

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

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

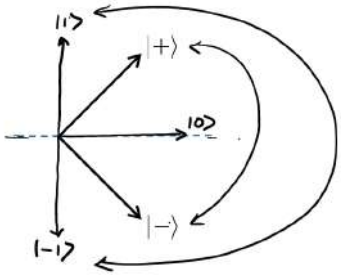
- Rotation gate

Rotation gate transforms the state by rotating the plane by an angle theta.

$$U = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

- Phase flip gate

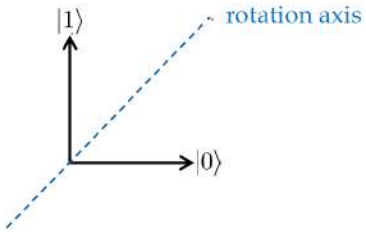
$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$



$$\alpha_0|0\rangle + \alpha_1|1\rangle \longrightarrow \boxed{Z} \longrightarrow \alpha_0|0\rangle - \alpha_1|1\rangle$$

- Bit flip/ NOT gate

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$



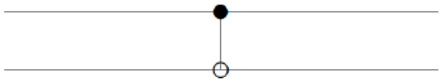
$$\alpha_0|0\rangle + \alpha_1|1\rangle \longrightarrow \boxed{X} \longrightarrow \alpha_1|0\rangle + \alpha_0|1\rangle$$

Basically, Phase flip gate is NOT gate acting in the |+> = 1/√2(|0> + |1>) and |−> = 1/√2(|0> − |1>) basis. Hence, Z |+> = |−> and Z |−> = |+>.

Evolution of a two qubit system is given on C^4 Hilbert space, given by 4 * 4 matrix and the four columns of U specify the four orthonormal vectors $|v_{00}\rangle$, $|v_{01}\rangle$, $|v_{10}\rangle$ and $|v_{11}\rangle$ that the basis states |00>, |01>, |10> and |11> are mapped to by U.

A basic two qubit gate is given by CNOT (controlled-not gate):

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



First bit of the CNOT gate, represented by the upper bit in the diagram on the right side, is the control bit which controls the second bit, the target bit. The target bit flips only if the control bit is 1, if the control bit is 0 then target bit remains the same. [2] [1]

10 Quantum Circuit

Any Unitary transformation on a quantum state can represented by a sequence of CNOT gate and single qubit gates. An important point to consider is the application of single qubit quantum gate to the first qubit in a two qubit system and checking the behavior of the second qubit.

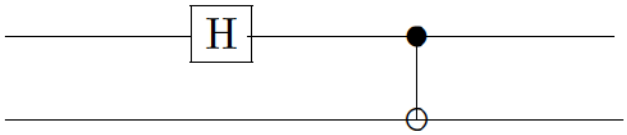
For instance we apply Hadamard transformation to the state :
$|\psi\rangle = 1/2\ |00\rangle - i/\sqrt{2}\ |01\rangle + 1/\sqrt{2}\ |11\rangle$.

The first qubit has been applied this unitary transformation and therefore, it yields the following result (The state of first qubit after the transformation):
$|0\rangle \rightarrow 1/\sqrt{2}\ |0\rangle + 1/\sqrt{2}\ |1\rangle$ and $|1\rangle \rightarrow 1/\sqrt{2}\ |0\rangle - 1/\sqrt{2}\ |1\rangle$.

Hence the two qubit system is affected as :
$|\psi\rangle \rightarrow 1/2\sqrt{2}\ |00\rangle + 1/2\sqrt{2}\ |01\rangle - i/2\ |00\rangle + i/2\ |01\rangle + 1/2\ |10\rangle - 1/2\ |11\rangle$ resulting from the above three equations.

Therefore, $|\psi\rangle \rightarrow (1/2\sqrt{2} - i/2)\ |00\rangle + (1/2\sqrt{2} + i/2)\ |01\rangle + 1/2\ |10\rangle - 1/2\ |11\rangle$.

Now this can be used to design a very important quantum circuit, which can generate the Bell states ($|\Phi^+\rangle = 1/\sqrt{2}\ (|00\rangle + |11\rangle)$), the one responsible for entanglement. This quantum circuit consists of a Hadamard gate followed by a CNOT gate, and can be represented as follows:



First qubit is transformed using the Hadamard unitary transformation as did in the example above, then this transformed qubit is entangled with the other qubit using CNOT gate.

Consider the input to be |0> and |0> , wherein the first qubit is subjected to Hadamard transformation and is changed to the state $\mathbf{1/\sqrt{2}\ (|0> + |1>) \otimes\ |0> = 1/\sqrt{2}\ |00> + 1/\sqrt{2}\ |10>}$.

This state $\mathbf{1/\sqrt{2}\ |00> + 1/\sqrt{2}\ |10>}$ is then subjected to the CNOT gate which flips the second bit of the second qubit, as it's control bit is 1. Hence the state becomes $\mathbf{1/\sqrt{2}\ |00> + 1/\sqrt{2}\ |11>}$, which is a Bell state. [3] [1] [4] [2]

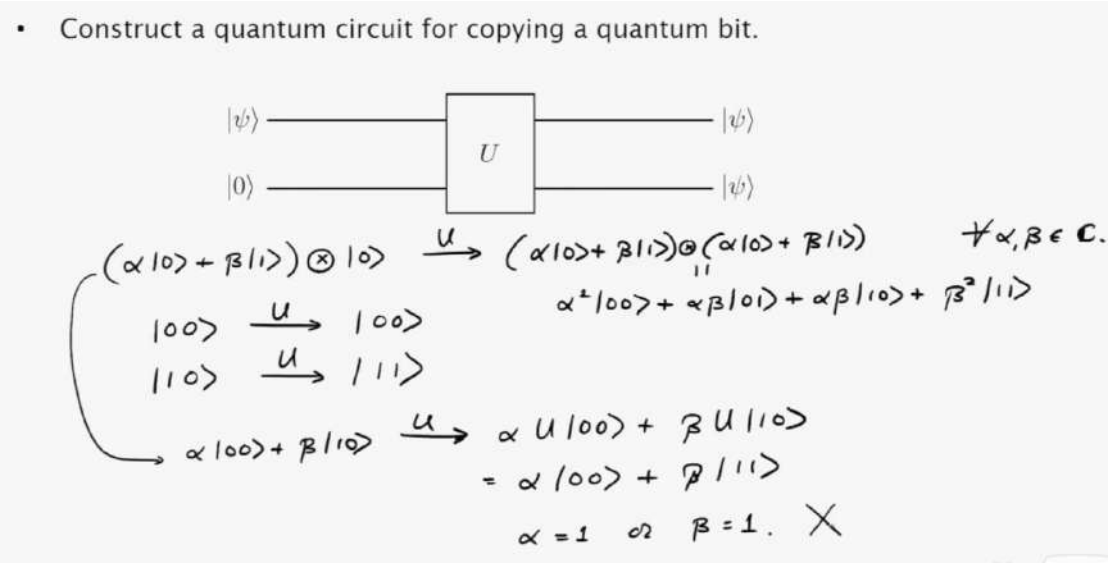
11 No Cloning Theorem

Our next aim to be able to transfer the quantum information from one place to another. No cloning theorem delves into this realm of quantum computation. It caters to the very important question of if it is feasible to make a copy of any given quantum state $|\varphi> = \alpha_0 |0> + \alpha_1 |1>$, that is create a state such that : $|\varphi> \otimes |\varphi> = (\alpha_0 |0> + \alpha_1 |1>) \otimes (\alpha_0 |0> + \alpha_1 |1>)$.

Another way of asking this question is if it is possible to start with two qubits in state $|\varphi> \otimes |0>$ and transform them to the state $|\varphi> \otimes |\varphi>$?

By the third postulate of the Quantum mechanics, for this to happen we should have a unitary transformation such that $U\ |\varphi> \otimes\ |0> = |\varphi> \otimes\ |\varphi>$. But this theorem proves that no such unitary transformation is possible, hence this operation is forbidden. Proof given in the appendix. [2] [1]

- Construct a quantum circuit for copying a quantum bit.



12 Superdense Coding and Quantum Teleportation

Consider Alice and Bob, connected by a communication channel which is capable of transferring the qubits. So in transferring quantum information from one place to another, another important aspect is to establish how many classical bits can Alice transmit to the Bob, in a message consisting of single qubit.

It is observed that if Alice and Bob share the quantum state which is entangled, and is a Bell state then, Alice can send 2 classical bits by transmitting just one qubit over the channel. [1] [2]

Let's consider the Proof.

Say, they both share the state $|\Phi^+\rangle = 1/\sqrt{2}\ (|00\rangle + |11\rangle)$, and that By applying suitable gate to her qubit, Alice can transform this shared state to any of the four Bell basis states $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, $|\Psi^-\rangle$.

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B)$$

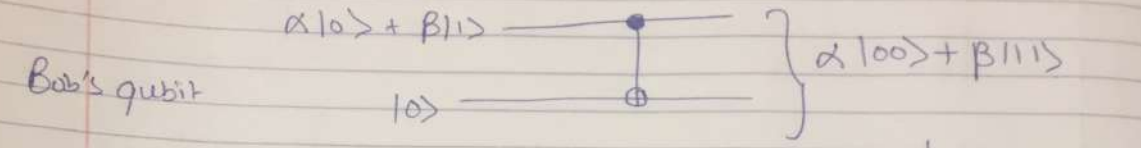
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B).$$

Now having got the Bell basis state, which is possible using two cases, first one being in case you have a CNOT gate between Alice and Bob as shown in the Notes image 1. When when she measures in the standard basis, she gets either 0 or 1, which if she conveys to Bob as a message, he won't be able to get the required quantum state. Hence, what she does is measure in the Sign basis states, wherein as per the calculations, she either gets |+> or |->. If she gets a |+> state, then she conveys that to bob using say a bit 0, which means Bob has already received the required quantum state and need not do anything. In case her measurement result is |->, then she conveys the bit 1, which means Bob needs to apply the phase flip gate in order to receive the required quantum state.

Quantum Teleportation

Alice's qubit.



Bob's qubit

$\alpha|00\rangle + \beta|10\rangle$

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

Alice.

Measure her qubit 0 $|00\rangle$ — Bob: $|0\rangle$ X

1 $|11\rangle$ — Bob: $|1\rangle$

Measure in +/− basis

$$\alpha|00\rangle + \beta|11\rangle = \alpha\left(\tfrac{1}{\sqrt{2}}|+\rangle + \tfrac{1}{\sqrt{2}}|-\rangle\right) \otimes |0\rangle + \beta\left(\tfrac{1}{\sqrt{2}}|+\rangle - \tfrac{1}{\sqrt{2}}|-\rangle\right)|1\rangle$$

$$= \tfrac{1}{\sqrt{2}}|+\rangle[\alpha|0\rangle + \beta|1\rangle] + \tfrac{1}{\sqrt{2}}|-\rangle[\alpha|0\rangle - \beta|1\rangle]$$

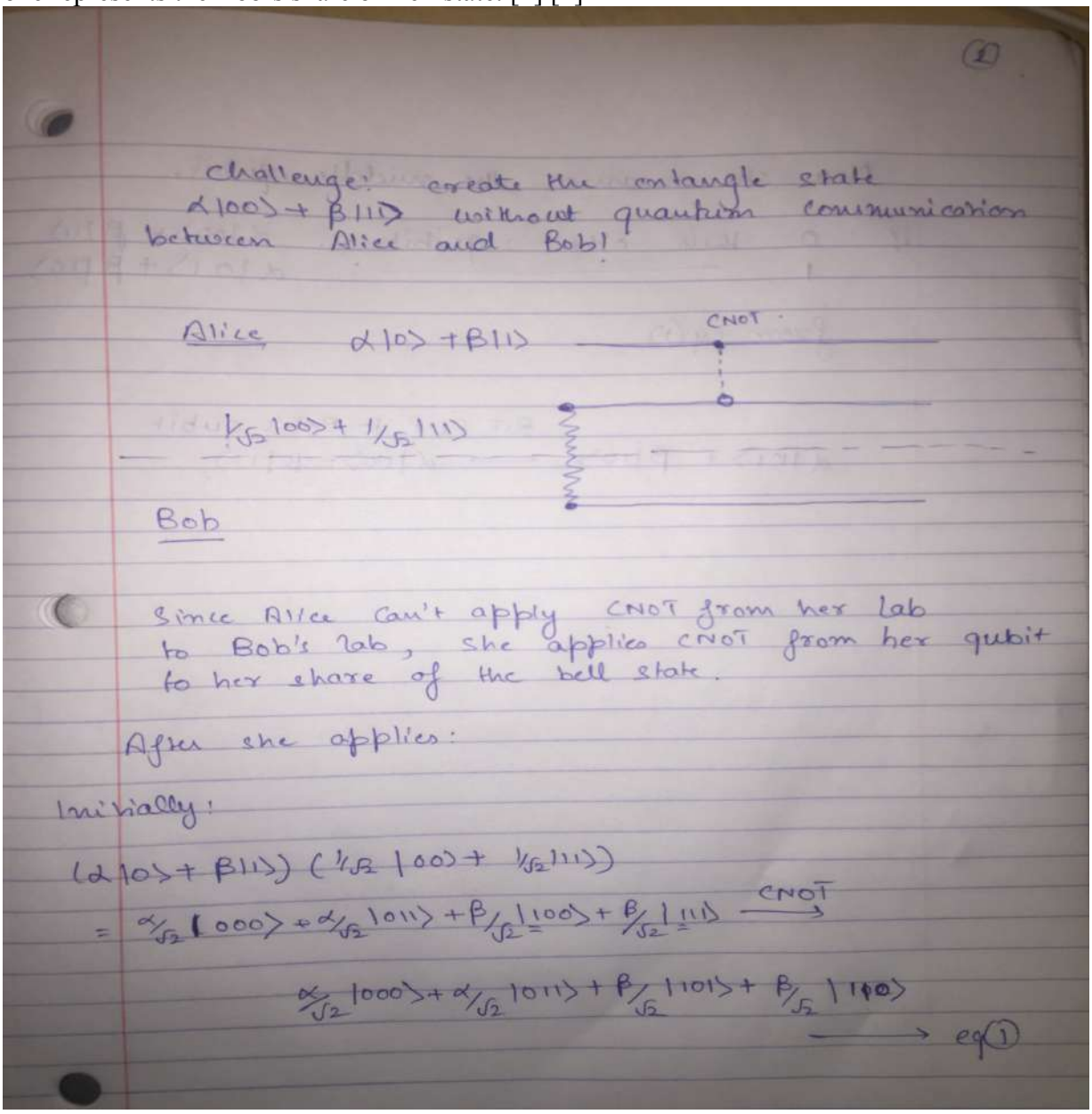
+ : New state $= |+\rangle[\alpha|0\rangle + \beta|1\rangle] \Rightarrow |\psi\rangle$

− : New state $= |-\rangle[\alpha|0\rangle - \beta|1\rangle]$

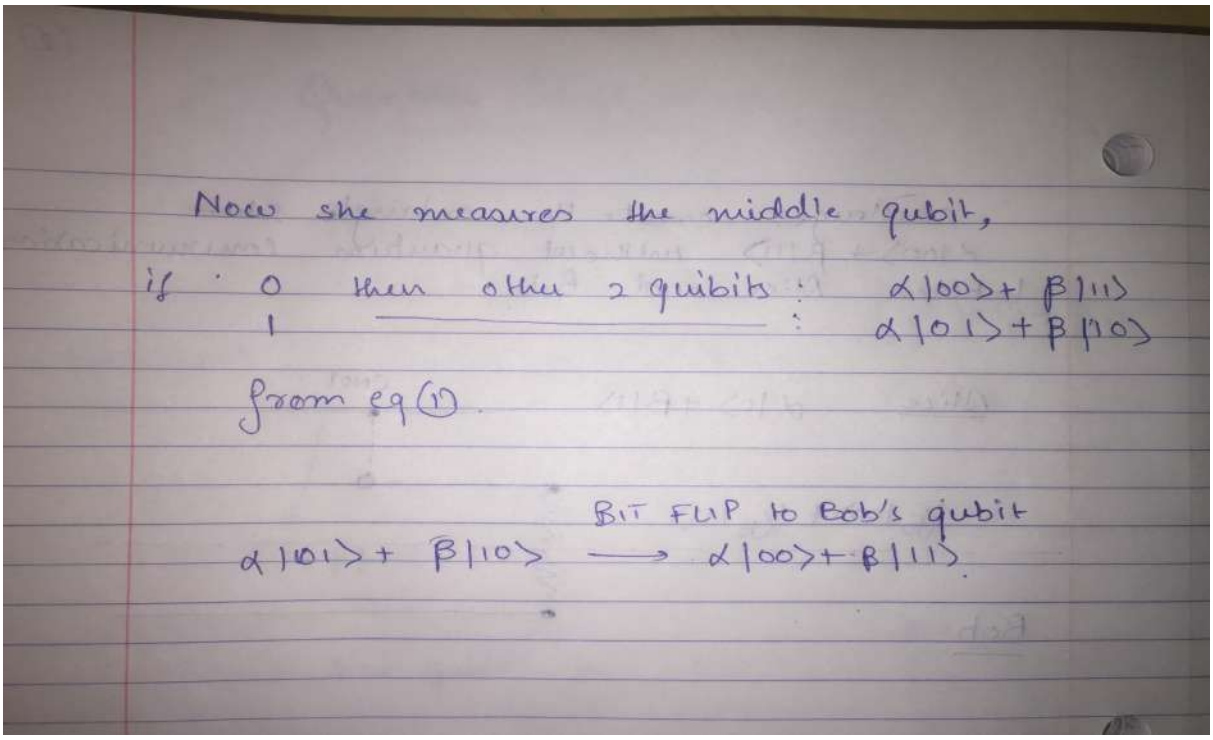
Phase flip $\longrightarrow Z[\alpha|0\rangle - \beta|1\rangle] = |\psi\rangle$.

NOTES IMAGE 1

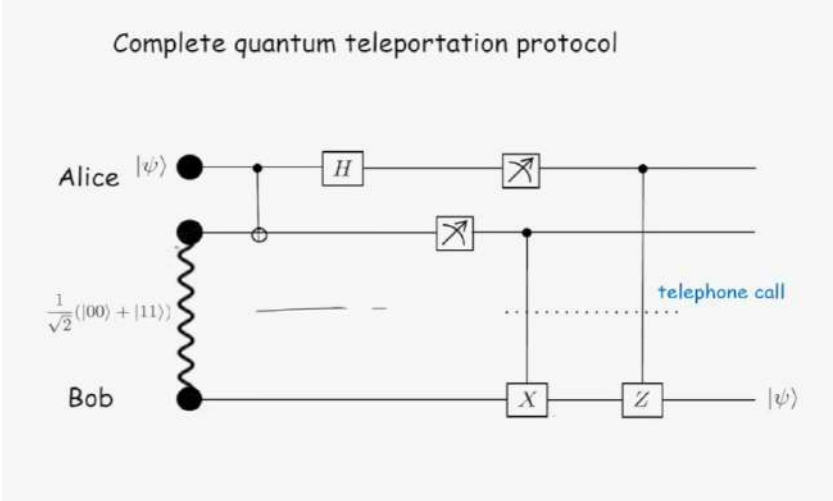
Actual challenge happens when Alice and Bob are very far apart and we can't have any shared CNOT gate between them. In such a case as shown in the Notes image 2, We consider 3 lines of communication being shared between Alice and Bob. First one is the one having Alice's qubit, middle one is shared and contains the shared Bell state for Alice, while third one represents the Bob's share of Bell state. [2] [1]



NOTES IMAGE 2



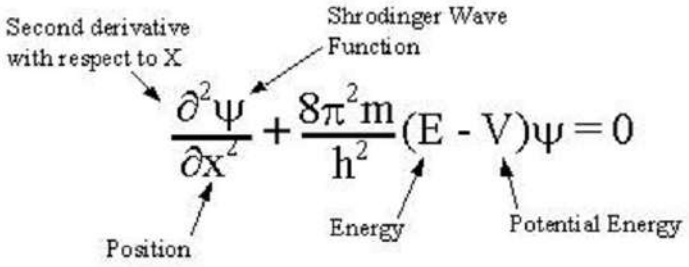
So Alice applies CNOT to her part of the lines and does the computation as shown in the notes. So, if she receives the qubit 0, she conveys 0 to Bob and Bob needs not do anything but has his required qubit. Whereas if she receives bit 1, then Bob needs to do a Bit flip for the required quantum state.
Hence the Quantum Teleportation.



Notice that measuring in the sign basis is same as applying the Hadamard transform and measuring it in the standard basis.

13 Observables, Hamiltonian and Schrodinger's equation

- "In quantum mechanics, the **expectation value** is the probabilistic expected value of the result (measurement) of an experiment. It is not the *most* probable value of a measurement; indeed the expectation value may have zero probability of occurring. It is a fundamental concept in all areas of quantum physics."
- "In quantum mechanics, the **Hamiltonian** is the operator corresponding to the total energy of the system in most of the cases. It is usually denoted by *H*, also $\check{H}$ or $\hat{H}$. Its spectrum is the set of possible outcomes when one measures the total energy of a system. Because of its close relation to the time-evolution of a system, it is of fundamental importance in most formulations of quantum theory."
- "In physics, an **observable** is a dynamic variable that can be measured. Examples include position and momentum. In systems governed by classical mechanics, it is a real-valued function on the set of all possible system states. In quantum physics, it is an operator, or gauge, where the property of the system state can be determined by some sequence of physical operations. For example, these operations might involve submitting the system to various electromagnetic fields and eventually reading a value."
- "In quantum physics, the relation between system state and the value of an observable requires some basic linear algebra for its description. In the mathematical formulation of quantum mechanics, states are given by non-zero vectors in a Hilbert space *V* (where two vectors are considered to specify the same state if, and only if, they are scalar multiples of each other) and observables are given by self-adjoint operators on *V*. " [5] [4]
- Schrodinger Equation :



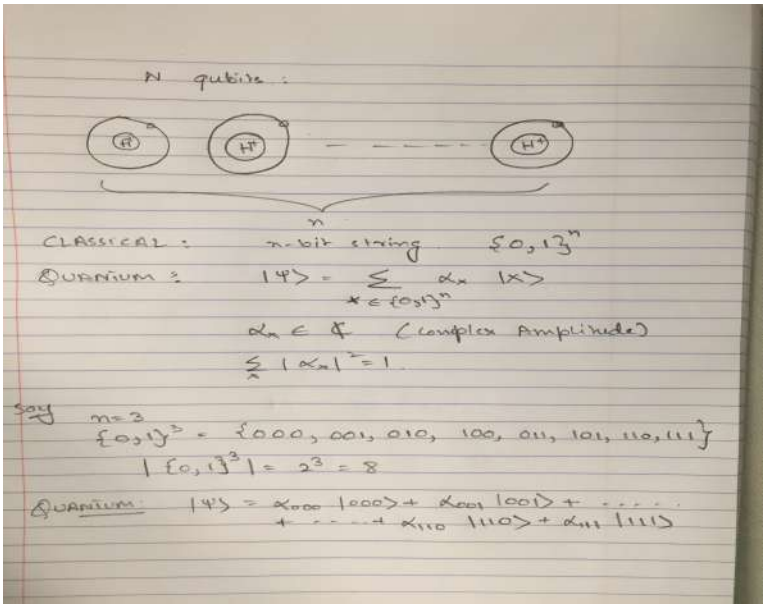
[4]

The Schrodinger equation is the name of the basic non-relativistic wave equation used in one version of quantum mechanics to describe the behaviour of a particle in a field of force. There is the time dependant equation used for describing progressive waves, applicable to the motion of free particles. And the time independent form of this equation used for describing standing waves. [4] [1]

14 Quantum Algorithms

14.1 n qubit system

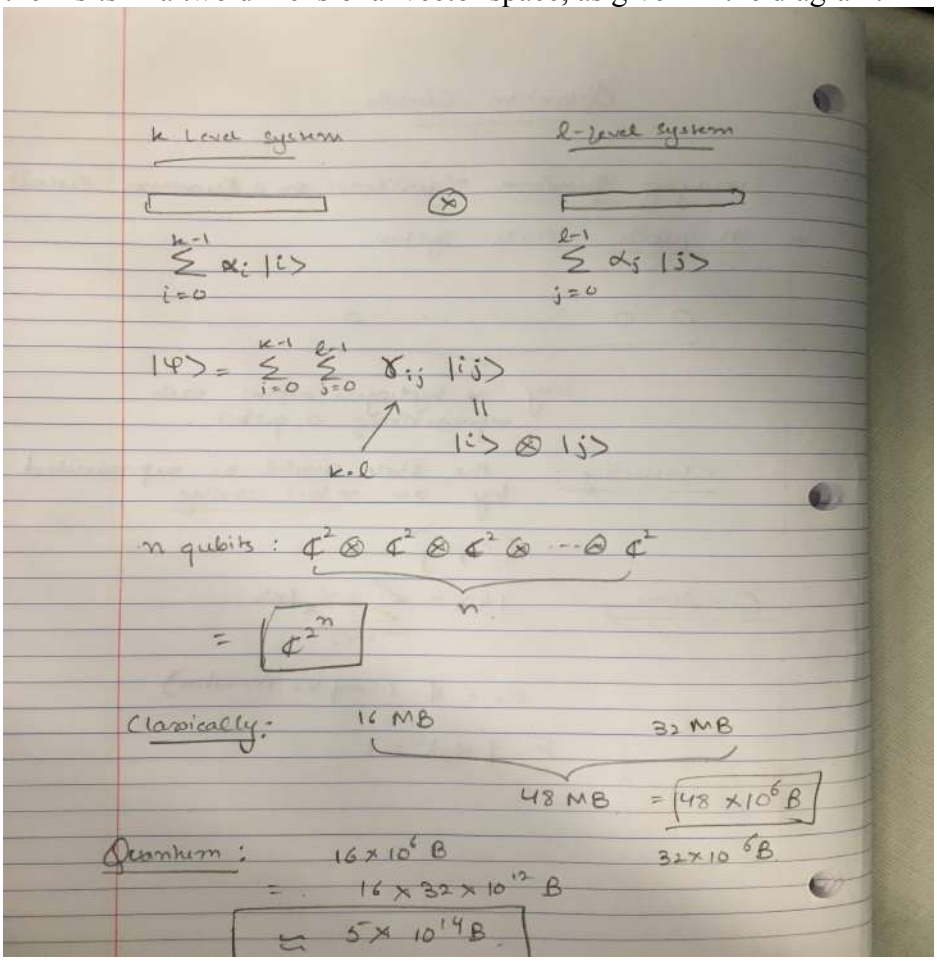
Now here, focus on how we specify a quantum algorithm in terms of a quantum circuit, considering that quantum circuit acts on a system of n qubits, what the state of an n qubit system looks like. Considering a qubit as the state of an electron in a hydrogen atom, say that we have many such hydrogen atoms such that they form a system of n qubits. In a classical paradigm, we represent this system using n bits, hence, the state of such a system is given by an n-bit string. In Quantum realm, by the superposition principle, the state is a superposition of all these classical possibilities, psi, is a superposition over all n-bit strings with probability amplitude alpha sub x, alpha sub x being a complex number. Consider the example given in the diagram.



We can see that exponential function grows extremely fast such that even for moderate values of n, say a few hundred, 2 to the power of n is already larger than the number of particles in the visible universe, or even the age of the universe in femtoseconds. Consider the following scenario to understand the exponential nature of the superposition, where we have two quantum systems, one a k level one and the other l level one.

These system states are written as a superposition of k different states (0 through k-1) and l different basis states respectively. Considering these two as a composite system. We get the state of this general system, which consists of this composite of these two different subsystems by taking tensor products as given in the diagram.

So we need k parameters, k complex numbers, to specify if we only had the first system and l parameters to specify only the state of the second system, but putting these systems together we need k*l parameters to specify the state of that system. Consider that we have a computer with 16 megabytes of memory and another one with 32 megabytes. Combining these two systems, classically, we have 48 MB memory but Quantum mechanically, we have 16 * 32 MB and that is what happens when we take a system of n qubits it is that the state of each of them sits in a two dimensional vector space, as given in the diagram.

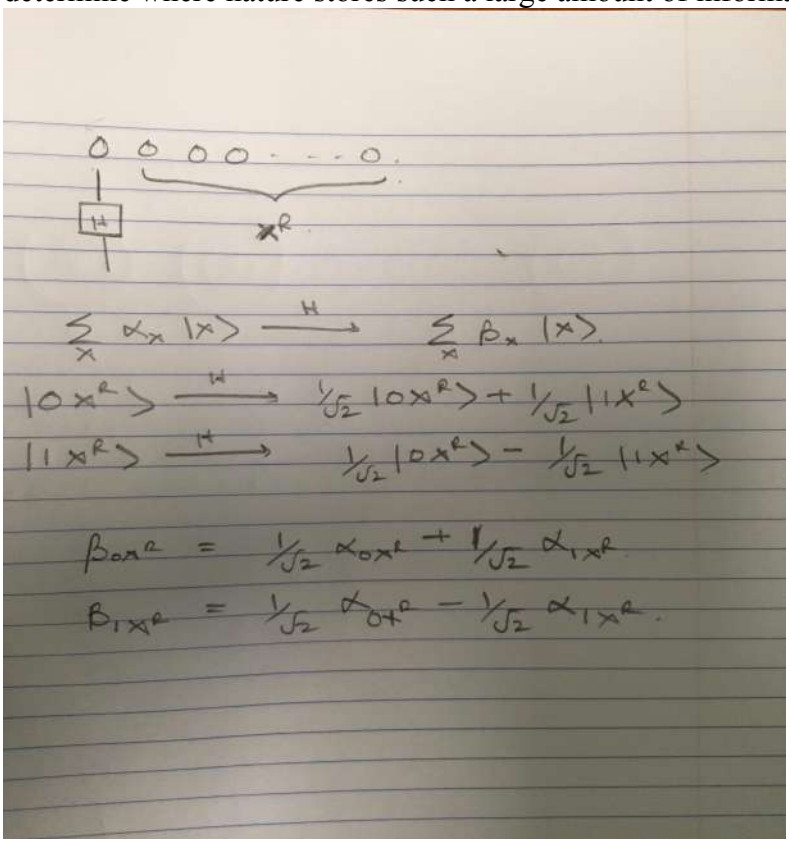


Now to implement a quantum computer, we need to effectively manipulate this exponentially large vector space and corresponding complex numbers. The question we next address is if we can manipulate all these exponentially many amplitudes efficiently and measure the results because this is what the potential for quantum algorithms is going to rely on.

14.2 Manipulating n qubits

To manipulate the aforementioned amount of data, we need to perform some kind of a quantum gate on atleast one a pair or on one of these qubits and we see that by doing that, all the exponentially many amplitudes get updated simultaneously. For example, as given in the diagram, we have our n qubits here. We perform the Hadamard transformation on the first qubit, leave the remaining qubits as such. We are interested in knowing the state of the system after the transformation. Denoting the remaining qubits by X^R.

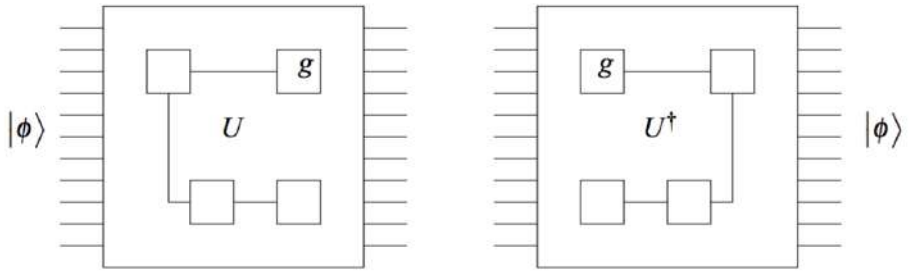
Hadamard gate transforms a |0> to $1/2^{1/2}$ |0> and $1/2^{1/2}$ |1>, correspondingly |1>. Now the superimposed amplitudes after the transformation given by Beta, are changed as in the diagram. Logically, we had an exponential superposition to start with, and even if n was as small as a few hundred or a thousand, 2 to the n is
much larger than the number of particles in the visible universe. An intriguing fact is to determine where nature stores such a large amount of information.



With such large amount of data present, if we do just a slight change, the underneath computation that takes part to change the amplitudes of the resulting superposition represents enormous computation that nature is carrying out, and quantum computation is trying to delve

into that. But then finally, when we measure, we only get very limited access to this information and Hence, quantum algorithms is the art of making use of these resources that quantum mechanics gives us extravagant resources with some degree of control, but very limited access,
and to use those to solve a difficult computational problem.

15.0 Reversible Computation



A quantum circuit acting on n qubits is described by an $2^n * 2^n$ unitary operator U. Since U is unitary, $UU^\dagger = U^\dagger U = I$. This implies that each quantum circuit has an inverse circuit which is the mirror image of the original circuit and which carries out the inverse operator $U^\dagger$.

Quantum Computation and Quantum Algorithms : Project Synopsis

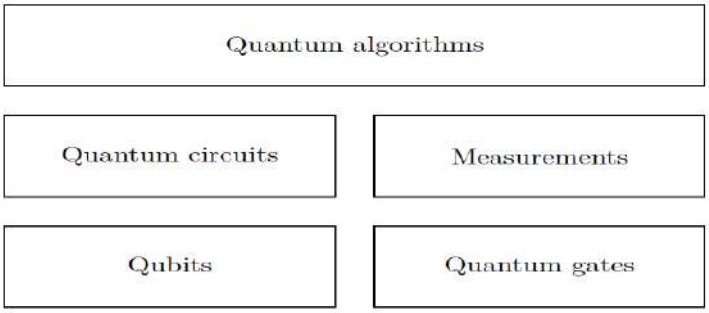
Introduction

In this project we'll start with the simulation of a simple quantum circuit model, which would implement a basic qubit behavior and simple single qubit and two qubit gates. We'll create a GUI for testing the each of the Quantum circuit model, Shor's algorithm, Grover's Algorithm and Duetsch - Josza Algorithm.

Generally, there are four steps involved in quantum algorithms. Input qubits are initialised into some classical start state; the system is put into some superposition state; the superposition state is acted upon via unitary operations; some measurement of the system is taken, providing a classical output state.

A brief description of these algorithms are given below.

Quantum Circuit model



A bit can represents two states, termed 0 and 1thereby, allowing us to store one piece of information: a yes or no (a Boolean value). Whereas a quantum bit can be described in terms of classical bit as in the figure.

We'll use jQuantum set of library functions to describe and mimic the behavior of quantum bits and define functions to implement the corresponding gates.

The end user would be able to create his own circuit by setting the value of the qubits and applying the corresponding gate transformations to it.

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad \text{or} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Shor's Algorithm

"The problem of distinguishing prime numbers from composites, and of resolving composite numbers into their prime factors, is one of the most important and useful in all of arithmetic... The dignity of science seems to demand that every aid to the solution of such an elegant and celebrated problem be zealously cultivated" — Carl Gauss

A great deal of effort has been spent trying to find classical algorithms to factor numbers. Indeed, probably more than we will ever know has been spent on this problem: the National Security Agency is supposedly the largest employer of mathematicians in the world and it would be reasonable to assume that they have spent a considerable amount of attention attempting to break the cryptosystems whose hardness is related to the hardness of factoring. Thus it was quite remarkable when, in 1994, Peter Shor showed that quantum computers could efficiently factor numbers.

In this project we implement this algorithm, wherein it solves the following problem: given an integer N, find its prime factors.

If a quantum computer with a sufficient number of qubits could operate without succumbing to noise and other quantum decoherence phenomena, Shor's algorithm could be used to break public-key cryptography schemes such as the widely used RSA scheme. RSA is based on the assumption that factoring large numbers is computationally intractable. So far as is known, this assumption is valid for classical (non-quantum) computers; no classical algorithm is known that can factor in polynomial time. However, Shor's algorithm shows that factoring is efficient on an ideal quantum computer, so it may be feasible to defeat RSA by constructing a large quantum computer.

When finding order using the period finding algorithm, it is important to use enough qubits. A sensible rule is that you need to use m qubits so that 2m) N2, where N is the number we are trying to factor, because the order of a random number might be as large as N. We now have all the necessary tools to carry out Shor's algorithm. Start by picking a random number, then use the period finding algorithm to compute its order. If the order is even, we can use it to find a nontrivial square root of unity. If the order is odd or xs/2 = −1, throw it out and start with a new number. Because we know that the order of x will be even and xs/2 will be a nontrivial square root with probability at least 1/2, we can be confident that we will be able to factor N in just a few runs of the algorithm. Because the time it takes to find the period grows as a polynomial in the number of bits, and the number of bits grows like 2 log N(by the above requirement), we expect the time it takes to factor N to grow as a polynomial in log N. Here is the circuit for Shor's Algorithm. It relies heavily on period finding, and so the circuit looks a lot like the circuit for period finding. The key difference is that we are finding the period of f(i) = xi , and the number of bits we need to input is very large.

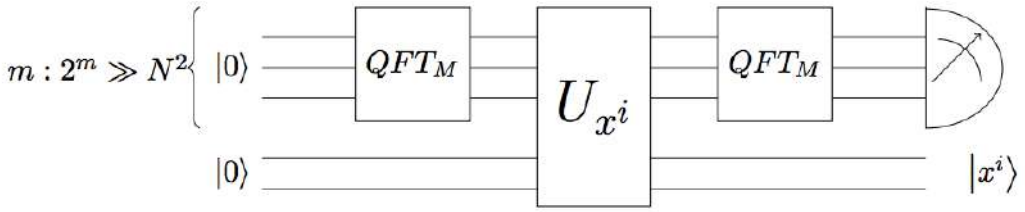
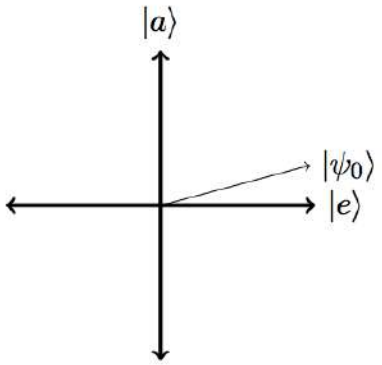


Figure 6.2: Circuit for factoring

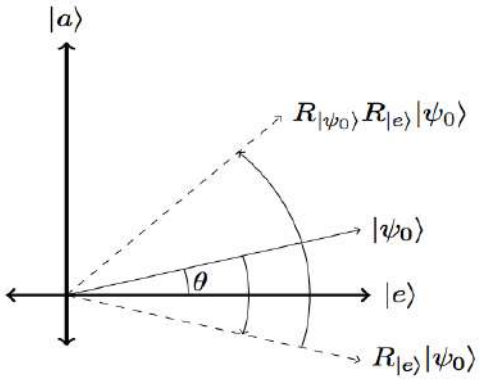
Grover's Algorithm

Searching an item in an unsorted table or array of size N costs a classical computer O(N) running time. If N is large, this is like searching for a needle in a haystack. Can a quantum computer search for a needle in a haystack more efficiently than its classical counterpart? Grover, in 1995, affirmatively answered this question by proposing a search algorithm that consults the table only O(√ N) times. In contrast to algorithms like quantum factoring which provide exponential speedups, the search algorithm only provides a quadratic improvement. However, the algorithm is quite important because it has broad applications, and because the same technique can be used to speedup algorithms for NP-complete problems.

The Grover search algorithm strives to solve this exact problem: We are given a boolean function f : {1,...,N} → {0, 1}, and are promised that for exactly one a ∈ {1,...,N}, f(a) = 1. Of course, a is the item we are searching for. The basic idea of the Grover search algorithm is best described geometrically. Because our black box function has only two outcomes, we can identify two important states: |a>, the state we are looking for; and everything else, call it |e> = ! x!=a √ 1 N−1 |x>. These two vectors span a two dimensional subspace, which contains the uniform superposition |ψ0> = ! x √ 1 N |x>. Furthermore, |a> and |e> are orthogonal. We can represent this two dimensional subspace geometrically. Because |ψ0> is N − 1 parts |e> and only one part |a>, it lies very close to |e>. Grover's algorithm works by starting with the state |ψ0> and successively increasing the angle between it and |e>, to eventually get closer and closer to |a>. It does this by a sequence of reflections: first by reflecting about |e>, and then by reflecting about |ψ0>. The net effect of these two reflections, as we will see, is to increase the angle between the state and |e>. Repeating this pair of reflections moves the state farther and farther from |e>, and therefore closer and closer to |a>. Once it is close enough, measuring the state results in outcome a with good probability.



Two dimensional space spanned by $|a\rangle$ and $|e\rangle$, and the uniform superposition $|\psi_0\rangle$.



First reflect about $|e\rangle$, then reflect about $|\psi_0\rangle$.

Deutsch-Jozsa Algorithm

One of the first examples of a quantum algorithm that is exponentially faster than any possible deterministic classical algorithm. It is also a deterministic algorithm, meaning that it always produces an answer, and that answer is always correct.

In the Deutsch-Jozsa problem, we are given a black box quantum computer known as an oracle that implements some function . In layman's terms, it takes n-digit binary values as input and produces either a 0 or a 1 as output for each such value. We are promised that the function is either constant (0 on all inputs or 1 on all inputs) or balanced[3] (returns 1 for half of the input domain and 0 for the other half); the task then is to determine if is constant or balanced by using the oracle.

Bibliography

[1] U. Vazirani, "https://people.eecs.berkeley.edu/~vazirani/f16quantum.html," [Online]. Available: https://people.eecs.berkeley.edu/~vazirani/f16quantum.html.

[2] N. a. Chuang, Quantum Computation and Quantum Information.

[3] S. Bhambri, "Quantum Clouds : A future perspective," *Arxiv.org,* 2014.

[4] "Wiki," [Online]. Available: https://en.wikipedia.org/wiki/Expectation_value_(quantum_mechanics).

[5] jcresser. [Online]. Available: http://physics.mq.edu.au/~jcresser/Phys301/Chapters/Chapter13.pdf.

[6] Z. Goodwin. [Online]. Available: http://www.physlink.com/education/askexperts/ae329.cfm.