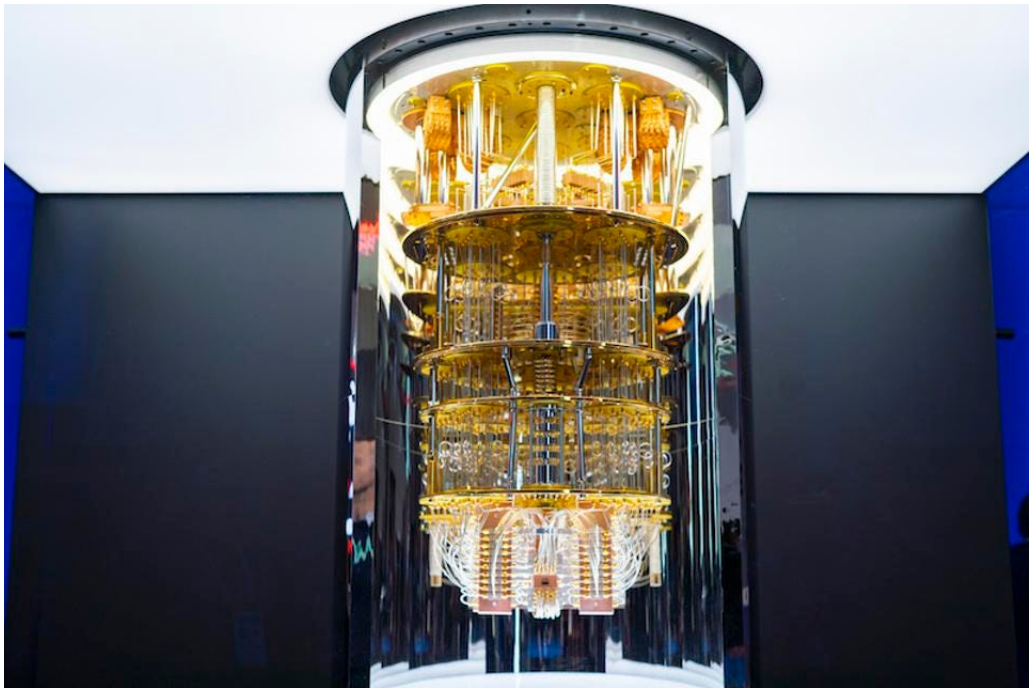
Quantum Computing SoS Endterm report

Josyula Venkata Aditya - 210050075
Mentor: Anagha Bhangare

July 2022



Contents

1 Introduction

Before starting anything, let us informally define what a Turing Machine is:

It is an abstract computing machine that can determine a result from the input through some **predefined** rules.

Quantum Computing, in a nutshell, is the way of achieving computation through quantum mechanical systems. Analogous to the classical bits(0 and 1), here are qubits, whose basis comprises of the vectors $|0\rangle$ and $|1\rangle$

Key motivation - study of single quantum systems(eg. electrons)

Quantum Cryptography allows us to transfer secret messages at long distances.

Quantum Computers are believed to be much faster than classical computers.

As a note, $|x\rangle$ represents a column vector and $\langle x|$ represents a row vector. A vector, by default, will refer to a column vector in the following discussion. The default inner product of two vectors, $|x\rangle$ and $|y\rangle$ is represented as $\langle y|x\rangle$, $\langle y| = |y\rangle^\dagger$. The default outer product of two vectors, $|x\rangle$ and $|y\rangle$ is represented as $|x\rangle\langle y|$.

At any place in this report, $|x\rangle|y\rangle$ corresponds to $|x\rangle \otimes |y\rangle$, where $\otimes$ denotes the tensor product of two column vectors.

2 Birth of Quantum Computation

The Turing machine model had a major setback when the Solovay-Strassen test for prime numbers was proposed. It used randomized calculation which was more efficient than the systematic computation as stated in the Turing thesis.

Quantum Computation solved two major problems efficiently, those which do not have an efficient solution using a classical computer.

1. Finding prime factors of a number
2. Discrete logarithm problem

Grover's algorithm of unstructured search is another example of a quauntum algorithm being more efficient than a classical algorithm.

3 Quantum Bits

A single quantum bit can be expressed as

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

where α and β are complex. A qubit is a unit vector.

The basis states $|0\rangle$ and $|1\rangle$ can be realized practically. But to develop the theory, it suffices to consider them to be abstract mathematical quantities.

Multiple qubits can also be represented as unit vectors. Eg: 2 qubit systems

are represented by

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

N-qubit systems have 2^N basis vectors. One of the most important states in quantum computation is the Bell state or the EPR pair and is given by

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

The two qubits in this state are correlated(entangled) with each other.

4 Prerequisites of Quantum Computation

Just like the classical circuits, which are made by wires and logic gates, quantum circuits are made by wires and **quantum gates**.

A quantum gate obeys the principle of linearity, and hence it can be represented by a matrix.

A quantum gate is valid if and only if it can be represented as a **Unitary matrix**, i.e. $U^\dagger U = I$. Some quantum gates:

X(Quantum NOT) = $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

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

H(Hadamard) = $\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ Hadamard gate can be considered analogous to the classical coin gate. In fact, any single bit quantum gate can be represented as

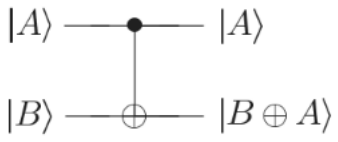
$$U = e^{i\alpha}\begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix}\begin{bmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{bmatrix}$$

.

4.1 Multiple Qubit Gates

NAND gate(along with ancilla bits) can function as a universal classical gate. This means that any classical gate can be made using NAND gates alone.

In the same way, CNOT(Controlled-NOT) gates(along with ancilla bits) are universal for quantum computation. The CNOT gate is described below:



$$U_{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Observe that all quantum gates are unitary, i.e all quantum gates are **invertible**. This is also called **reversibililty**. So, there is no loss of information in a quantum circuit.

For instance, assume that there are 2 bits in a classical circuit and these are passed into an XOR gate. Let's say that the output value is 1. Now, we have no clue whether the initial 2 bits were 0, 0 or 1, 1. Hence, we have lost some information regarding the bits in the circuit. This is not possible in a quantum circuit because every quantum gate is reversible.

4.2 Measurements along non conventional bases

Measurements need not only be done along the usual basis, but can be done along any orthonormal basis. One useful non conventional basis would be $|+\rangle$, $|-\rangle$.

5 Quantum Circuits

A quantum circuit is made of "wires" and quantum gates. Recollect that any unitary matrix represents a quantum gate and any quantum gate has to be a unitary matrix. This forbids us from the following, which classical circuits can achieve quite easily:

1. Joining of wires is not allowed, since this would lead to a 2-in 1-out gate, and this is a forbidden gate.

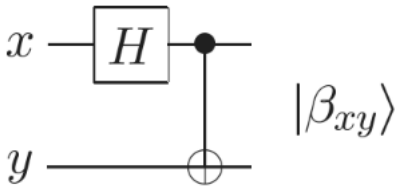
2. Branching out a wire is not permitted.(qubits can't be copied!)

3. There are no loops in quantum circuits. Wires in a quantum circuit need not essentially be wires. For instance, it could just be the path that a qubit follows.

The result that qubits cannot be copied, also known as the **No-Cloning Theorem**, is one of the major differences between quantum computation and classical computation.

Let us look at some circuits:

5.1 EPR pairs or Bell states



Let's say we pass $|00\rangle$ as the two bits into this gate, then after the H gate, the state of the system would be

$$\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)|0\rangle$$

. Now, after passing through the CNOT gate, the state of these bits would be

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

The above state is symbolically represented as β_{00}. In the same way, we can construct β_{01}, β_{10}, β_{11}. These 4 states are called EPR pairs or Bell states. (EPR = Einstien, Podolsky and Rosen).

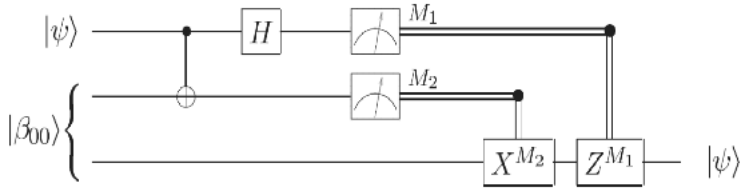
Notice that these states cannot be written in a **product form**, i.e. they cannot be written in the form $|\psi_1\rangle|\psi_2\rangle$. Hence, these states are called **entangled states**. Such states show many interesting properties because the 2 qubits are essentially "entangled" with each other. The next section talks in a greater detail about the EPR pairs.

5.2 Quantum Teleportation

In a nutshell, it is possible to **teleport** a quantum state from one location to another even in the absence of a quantum communication channel. This is achieved through EPR pairs. So, the story goes like this -

Alice is supposed to send a qubit to bob who stays sufficiently far away(another universe, say!) and the tricky part is, she doesn't know what the qubit is. She is allowed to perform "classical" communication with Bob.

Even unbeknownst of the qubit, Alice can send the qubit to Bob using EPR pairs. Let's say that Alice and Bob constructed an EPR pair long ago and each of them had taken one of the 2 qubits in the pair.



Alice uses her EPR bit and the qubit to be transported($\psi = \alpha|0\rangle + \beta|1\rangle$) in a quantum circuit shown above. Initial state of the circuit is:

$$(\alpha|0\rangle + \beta|1\rangle)\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)$$

After the CNOT gate is applied, the state becomes:

$$\frac{1}{\sqrt{2}}(\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle))$$

Now, after the Hadamard Gate is applied, the final state becomes,

$$\frac{1}{2}(\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle))$$

Rearranging the terms, we get:

$$\frac{1}{2}(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\beta|0\rangle + \alpha|1\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(-\beta|0\rangle + \alpha|1\rangle))$$

Now the strategy that Alice and Bob have discussed and agreed upon while making their EPR bits will come into play. Depending on Alice's bits after the measurement, an appropriate gate can be used by Bob on his EPR bit to convert it into the state ψ. Say, Alice measured $|11\rangle$. In that case, Bob would need a gate U that would do the following:

$$U|0\rangle = -|1\rangle$$

$$U|1\rangle = |0\rangle$$

This way, the qubit ψ has actually been teleported!

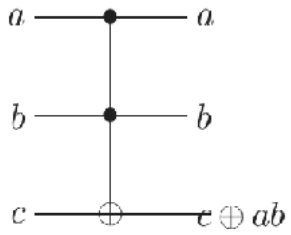
At the first sight, all this would seem quite overwhelming; one would feel that information is being teleported faster than light. Indeed, the qubit has been teleported to Bob instantaneously but there's a catch here! Alice has to convey the state of her measured qubit to Bob so that he could apply the appropriate gate on his qubit to recover the state ψ. And conveying this information can atmost happen at the speed of light. So, The Special Theory of Relativity is not violated here.

6 Quantum Algorithms

6.1 Classical circuits as Quantum Circuits

It is believed that every classical phenomenon can be explained by the Quantum Mechanical Theory and hence, all the classical circuits can also be converted to quantum circuits. The only hassle is that we can't replace all the gates directly since every gate in a quantum circuit has to be **reversible**

Now we introduce a new gate called the Toffoli Gate(CCNOT gate):



This gate is a reversible as it can be represented by the following unitary matrix:

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

Setting the bit c to 1, this now functions as a NAND gate. Hence, the Toffoli gate is a universal gate for both classical and quantum circuits. Also, Toffoli gates can be used to perform a FANOUT operation(since the bit in a classical circuit is either 0 or 1, FANOUT is possible).

Through FANOUT operations and NAND gates, we can construct any classical circuit. Hence, all classical circuits can be converted to equivalent quantum circuits using Toffoli gates.

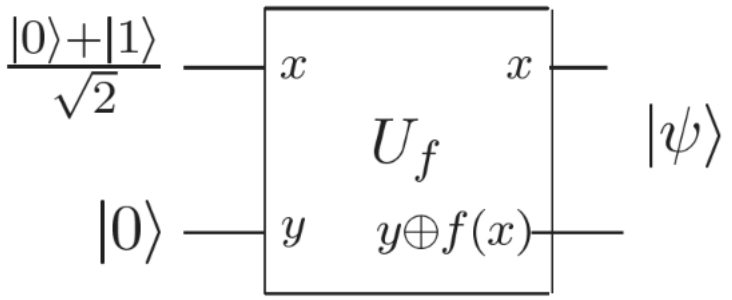
If COIN gates are used in the classical circuits, then Hadamard gates can be used in the quantum circuits to generate random bits.

6.2 Quantum Parallelism

Let us say that there is a function $f : \{0,1\} \longrightarrow \{0,1\}$. To get for the values of a function simultaneously through classical circuits, we would need multiple of them.(One to calculate $f(0)$ and the other to calculate $f(1)$. Now, look at the following quantum circuit that consists of a gate U such that

$$U : |x\rangle \otimes |y\rangle \longrightarrow |x\rangle \otimes |y \oplus f(x)\rangle$$

.



The 2^{nd} bit is the bit of interest for us. In this case, it would be

$$\psi = |0\rangle \oplus f(x) = f(x) = \frac{|0\rangle \otimes |f(0)\rangle + |1\rangle \otimes |f(1)\rangle}{\sqrt{2}}$$

So, it appears as if we have retrieved the values $f(0)$ and $f(1)$ in a single circuit. This is what we refer to as Quantum Parallelism. Whereas in the classical case, one would require 2 circuits to retrieve the values of $f(0)$ and $f(1)$. However, there is a subtlety here. It is not directly possible to measure the value of both $f(0)$ and $f(1)$, since after a measurement is made, the qubit becomes deterministic. So, we need a way to harness the power of Quantum Parallelism since Parallelism alone, provides no significant advantage to quantum computer over classical computers.

Let us digress a bit here and introduce the **Hadamard Transform**. For n bits, the Hadamard transform is represented by $H^{\otimes n}$. Let us say that the initial state of the system was $\psi = |x_1\rangle \otimes |x_2\rangle \otimes \cdots |x_n\rangle$, where $|x_1\rangle$, $|x_2\rangle \cdots$ represent the individual qubits. The Hadamard transform is defined as

$$|y_i\rangle = H|x_i\rangle,\ H^{\otimes n}\psi = |y_1\rangle \otimes |y_2\rangle \otimes \cdots |y_n\rangle$$

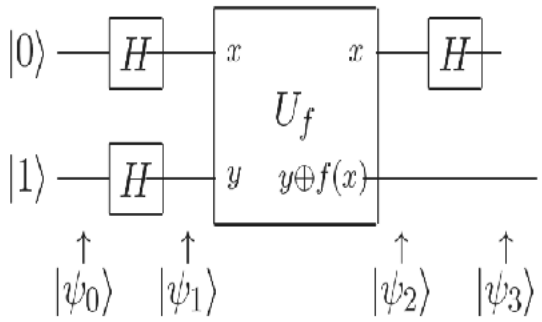
So, if we apply $H^{\otimes n}$ to $\psi = |000\cdots\rangle$, then we would get the following state:

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle$$

where the summation is over all the basis vectors of n qubits. This is quite an achievement; we have produced a superposition of 2^n qubits using only n Hadamard gates. Now, if our function f is such that it takes n bits as input, then we could use the above method to generate the basis of n qubits.

6.3 Deutsch's algorithm

Let us say that there is a function $f : \{0, 1\} \longrightarrow \{0, 1\}$. Through this algorithm, we can harness Quantum Parallelism to measure a property of a function ($f(0) \oplus f(1)$ in this case) using a single circuit. Whereas, a classical computer would require at least 2 circuits to accomplish this. This time, the second qubit would be $y = H|1\rangle = |-\rangle$ instead of $|0\rangle$.



The initial state of the system is:

$$\psi = |+\rangle \otimes |-\rangle$$

After the U_f gate is applied, realize that the $|-\rangle \oplus f(x) = (-1)^{f(x)}|-\rangle$. Hence, the state after U_f gate is applied can be written as:

$$\psi = \frac{1}{\sqrt{2}} \sum_i (-1)^{f(x_i)} |x_i\rangle \otimes |-\rangle$$

Applying H on the first qubit, and after some brainstorming, the final state can be written as:

$$\psi = |f(0) \oplus f(1)\rangle \otimes |-\rangle$$

This is, once again, quite an achievement. We have computed the value of $f(0) \oplus f(1)$ in a single quantum circuit, where at least 2 circuits would be required in the classical way. This algorithm is one of the examples which combines Quantum Parallelism and Interference. The next one is another algorithm which is more general, but relies on the same idea.

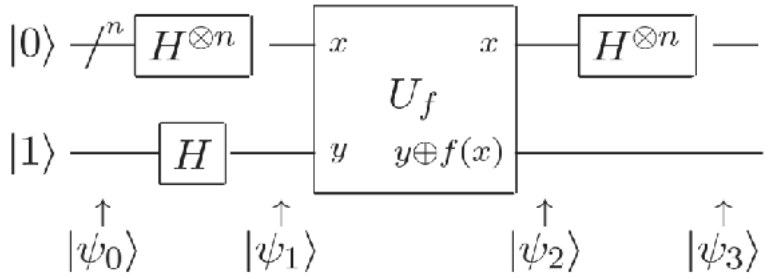
6.4 The Deutsch-Jozsa Algorithm

This can be considered to be an extension to the Deutsch's algorithm. Consider the following scenario:

Bob has a function $f : \{0,1\}^n \longrightarrow \{0,1\}$. Bob only can compute the values of the function but doesn't know about the nature of the function. He though knows that the function is either a constant function or it is a balanced function. Alice can communicate with Bob to find more about the function f. The question is, what is the procedure Alice should follow so that she can determine, with certainty, the nature of f, with minimum number of correspondences with Bob. The answer is that, this can be done with only a **single** evaluation of the function f.

Before looking at the quantum algorithm, let us look at the most efficient classical non-randomized algorithm. In the worst case, Alice would need to exchange $2^{n-1}+1$ bits with Bob(since exchanging anything less then $2^{n-1}+1$ bits would not determine with certainty if the function is constant or balanced). The $2^{n-1}+1^{th}$ bit would tell Alice if the function is constant or balanced; for if it was a constant, then the values of function for the first 2^{n-1} bits would be the same as the last bit. And if it was a balanced function, the last bit would be different from the first 2^{n-1} bits(in the worst case).

Now, let us consider the quantum algorithm for this problem.



Let us go through the algorithm step by step. Initially, the state of the circuit is:

$$\psi = |0\rangle^{\otimes n}|1\rangle$$

After the Hadamard transform is applied, the state becomes:

$$\psi = \frac{1}{\sqrt{2^n}}(\sum_x |x\rangle) \otimes |-\rangle$$

.

After applying U_f, the state becomes:

$$\psi = \frac{1}{\sqrt{2^n}}(\sum_x (-1)^{f(x)}|x\rangle) \otimes |-\rangle$$

Now, let us generalize the effect of a Hadamard transform on an n-bit register. Consider $|x\rangle = |x_1\rangle \otimes |x_2\rangle \cdots \otimes |x_n\rangle$, where $|x_i\rangle$'s are single qubit registers. Now,

$$H|x_i\rangle = \frac{1}{\sqrt{2}} \sum_z (-1)^{x_i z} |z\rangle$$

$H^{\otimes n}|x\rangle = H|x_1\rangle \otimes H|x_2\rangle \cdots \otimes H|x_n\rangle$. Substituting the above result, we get $H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{z_1, z_2, \cdots z_n} (-1)^{x_1 z_1 + x_2 z_2 + \cdots x_n z_n} |z_1\rangle \otimes |z_2\rangle \cdots \otimes |z_n\rangle$. This can be re-written as

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_z (-1)^{x.z} |z\rangle$$

, where $x.z$ denotes the bitwise product of the registers x and z.

Now let us come back to the process of applying gates. After applying the Hadamard transform on the first n qubits, the final state becomes:

$$\psi = \frac{1}{\sqrt{2^n}} (\sum_x (-1)^{f(x)} H^{\otimes n}|x\rangle) \otimes |-\rangle = \frac{1}{2^n} (\sum_x \sum_z (-1)^{f(x)+x.z} |z\rangle) \otimes |-\rangle$$

After all the mathematical jugglery, it is now time to make a measurement on the n bit register. Consider the amplitude of the bit $|00...0\rangle$. It would be equal to $\frac{1}{2^n} \sum_x (-1)^{f(x)}$. If f was a constant function, then the amplitude would be equal to 1. We also know that the sum of squares of amplitudes of all the vectors should be 1. This means that whenever f is constant, the state of the n bit register is $|00...0\rangle$.

Now, if f was a balanced function, then the amplitude of $|00...0\rangle$ would be 0!. So, we can come to a conclusion that: If Alice measures $|00...0\rangle$, then the function is a constant; else it is balanced.

We have only used a single evaluation to find if f is a constant or not, whereas we would take $2^{n-1} + 1$ evaluations to find the same on a classical computer(in the worst case). This is again quite an achievement! Though this algorithm has no real consequences, nor is it very helpful to think of sophisticated quantum algorithms for this problem(since the randomized classical algorithm is not bad either!), yet this algorithm plants seeds for the more impressive quantum algorithms.

7 Linear Algebra

A complete discussion of linear algebra is not possible here, but a few important things are highlighted.

- A matrix is diagonalizable if and only if it has a set of eigenvectors which form a basis of $\mathbb{C}^n$
- **Normal Matrix**: A matrix that satisfies $AA^\dagger = A^\dagger A$ is called a normal matrix.
- **Spectral theorem**: Any normal matrix can be diagonalized and there exists a set of eigenvectors of that matrix which form an orthonormal basis of $\mathbb{C}^n$. In other words, there exists a unitary matrix U such that $U^\dagger AU = D$, D is a diagonal matrix(the diagonal entries are the eigenvalues of A). A normal matrix A has the following spectral decomposition:

  $$A = \sum_a \lambda_a |a\rangle \langle a|$$

  where $|a\rangle$ represent the orthonormal eigenvectors and λ_a correspond to the eigenvalue of $|a\rangle$
- A Unitary matrix/operation preserves inner products. That is,

  $$(U|v\rangle, U|w\rangle) = \langle v|U^\dagger U|w\rangle = \langle v|w\rangle$$

- **All the Quantum Gates are Unitary**. Let us say that the state of the state of the system before U was applied is ψ. Since ψ is a quantum state, we know that $\langle\psi|\psi\rangle = 1$. After applying the gate U, the state becomes $U|\psi\rangle$. This also has to be a quantum state. The means, $(U|\psi\rangle, U|\psi\rangle) = 1 \implies \langle\psi|U^\dagger U|\psi\rangle = 1 \implies U$ satisfies $U^\dagger U = I$. Also, observe that $U^\dagger U = I \implies UU^\dagger = I \implies U^\dagger U = UU^\dagger$. This means that U is normal. Hence, it has a spectral decomposition.
- For the discussions in Quantum Computing, it suffices to consider the term **Hilbert space** to just mean a finite dimensional vector space equipped with an inner product. We don't consider infinite dimension vector spaces.
- **Change of basis**: Through (4), we conclude that two orthogonal vectors will remain orthogonal after any unitary operation. This means that a Unitary operation maps an orthonormal basis to another orthonormal basis with the same dimension. Let us say that $U|v_i\rangle = |w_i\rangle \ \forall i$ for some unitary matrix U, where $|v_i\rangle$'s are orthonormal. Now, the matrix U can be expressed as

  $$U = \sum_i |w_i\rangle\langle v_i|$$

7.1 Projection Matrices

Let us consider a vector space V of dimension d and a subspace W of V having dimension k. Using the Gram-Schmidt process, we can generate an orthonormal basis $|v_1\rangle, |v_2\rangle \cdots |v_d\rangle$ of V such that $|v_1\rangle, |v_2\rangle \cdots |v_k\rangle$ is an orthonormal basis for W. Define the matrix P

$$P = \sum_{i=1}^{k} |v_i\rangle \langle v_i|$$

This matrix is called the **projector** onto the subspace W. Observe that

$$v \in W \implies Pv = v$$

Projection matrices:

- are Hermitian i.e $P^\dagger = P$
- satisfy $P^2 = P$

At this juncture, let us look at an interesting property of the projection matrix P. Using the same notation, let $v \in W$. This implies that v is an eigenvector of P. Consider the matrix $Q = I - P$; it is a hermitian matrix and also an idempotent matrix. Hence, Q is a projection matrix. Q has a rather interesting property. $Pv = v \implies Qv = 0$. This means that the projection of any vector on the subspace 'Q' is 0. So, the subspace W and the subspace defined by the projector Q are orthogonal. In other words,

$$Q = \sum_{i=k+1}^{d} |v_i\rangle \langle v_i|$$

7.2 Tensor Product

The tensor product of two Hilbert spaces V of dimension m and W of dimension n is a vector space denoted by $V \otimes W$, has dimension mn, and has the following properties:

- $c(|v\rangle \otimes |w\rangle) = c|v\rangle \otimes |w\rangle = |v\rangle \otimes c|w\rangle$
- $(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle$
- $|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_1\rangle$

If A is a linear operator on V and B is a linear operator on W, then we would want to find a matrix/operator C such that

$$C(|v\rangle \otimes |w\rangle) = A|v\rangle \otimes B|w\rangle$$

where $|v\rangle \in V$ and $|w\rangle \in W$. The operator C, indeed turns out to be $A \otimes B$. The matrix tensor product is defined as follows:

Let A be an m x n matrix and B be a p x q matrix. Let $A = a_{ij}$.

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & & & \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{bmatrix}$$

It is quite straightforward to observe that the tensor product isn't commutative. $A \otimes B$ is an mp x nq matrix. The inner product for the tensor product is given by:

$$\left(\sum_i a_i |v_i\rangle \otimes |w_i\rangle, \sum_j b_j |v'_j\rangle \otimes |w'_j\rangle) \right) = \sum_{i,j} a_i^* b_j \langle v_i | v'_j \rangle \langle w_i | w'_j \rangle$$

.

7.3 Operator Functions

Let A be a normal matrix. Then we can write a spectral decomposition for it as follows:

$$A = \sum_a \lambda_a |a\rangle \langle a|$$

Then, we can define

$$f(A) = \sum_a f(\lambda_a) |a\rangle \langle a|$$

8 Quantum Measurement

8.1 Quantum Evolution

Postulate 1 *For a closed system, the state ψ_1 of the system at a time t_1 and the state of the system ψ_2 at a later time t_2 are related by*

$$\psi_2 = U_{12}\psi_1$$

*where U_{12} is a **unitary** matrix and depends only on t_1 and t_2.*

The above postulate tells us about the discrete time evolution. The following postulate tells us about the continuous time evolution of a closed system.

Postulate 2 *The continuous time evolution of a closed quantum system is described by the Schrodinger equation.*

$$\iota\hbar\frac{\partial\psi}{\partial t} = H\psi$$

This equation can be viewed as a matrix equation and its solution can be written as

$$|\psi_2\rangle = \exp\left(-\frac{\iota H(t_2 - t_1)}{\hbar}\right)|\psi_1\rangle$$

Note that a matrix exponential is present in this equation. Let us try to relate this with Postulate 1. Consider a unitary matrix U. We know that all the eigenvalues of a unitary matrix have unit modulus. Hence all the eigenvalues can be written in the form $e^{\iota\lambda}$ where λ are **real** numbers. A unitary matrix is a normal matrix, so it has a spectral decomposition. Consider a function $f(x) = -\iota \log x$. We, can now say that the matrix $f(U)$ is hermitian since the eigenvalues are real and the spectral decomposition takes care of the fact that it is hermitian. Similarly, we can also prove that if H is a hermitian matrix, then $e^{\iota H}$ is unitary.

Now, we observe that Postulate 2 is in compliance with Postulate 1 since $\exp\left(-\frac{\iota H(t_2-t_1)}{\hbar}\right)$ can be written as a unitary matrix which depends only on t_1 and t_2.

H is a fixed hermitian operator. Hence, we can write a spectral decomposition as follows:

$$H = \sum_E \lambda_E |E\rangle\langle E|$$

where $|E\rangle$ are the energy eigenstates with corresponding eigenvalues λ_E. These eigenstates evolve according to the Schrodinger equation as:

$$|E\rangle \longrightarrow e^{-\frac{\iota\lambda_E t}{\hbar}}|E\rangle$$

Quite often, the system of interest is not actually "closed". For example, a quantum circuit is not a closed system w.r.t the system of qubits. But it has been observed that such systems evolve according to the Schrodinger equation to a good extent. Hence, we can describe the evolution of a quantum system using unitary operators, to a good approximation.

8.2 Measurement

Measurements are performed using measurement operators $\{M_m\}$.

Postulate 3 *The probability of a particular state m being observed after the measurement is*

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

The state of the system after the measurement is

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

The measurement operators satisfy the completeness relation, i.e.

$$\sum_m M_m^\dagger M_m = 1$$

8.2.1 Projective Measurement

These are the most common types of measurements encountered in Quantum Computing. These deal with the measurement of an observable i.e., a Hermitian operator. An observable, M is a hermitian operator on the system. It has a spectral decomposition:

$$M = \sum_m m P_m$$

where P_m are the **projectors** onto the eigenspace of M with eigenvalue m. After measurement, the probability of the state being m is

$$p(m) = \langle\psi| P_m |\psi\rangle$$

and the state after measurement is

$$|\psi\rangle' = \frac{P_m |\psi\rangle}{\sqrt{p(m)}}$$

9 Circuit Model of computation

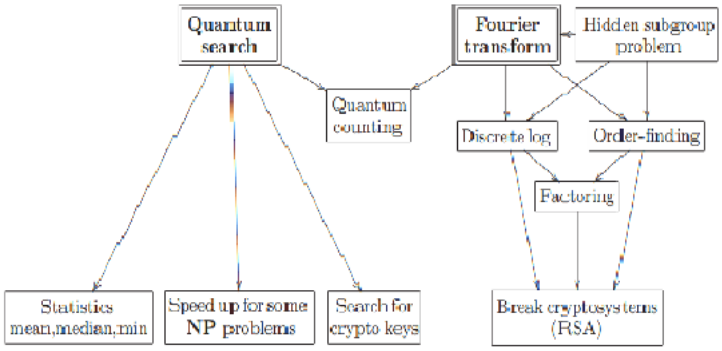
This model is more often used than the Turing Model to understand quantum computation. A cicuit consists of wires and gates which transfer information from one place to the other. We also impose a condition that the circuits in the circuit model are acyclic, since cyclic circuits can bring instabilities.

10 Quantum Circuit model

There are mainly two types of quantum algorithms:

- Those based on Shor's Quantum Fourier transform. These are used for fast factoring of numbers.
- Those based on Grover's search algorithm.

A summary of the quantum algorithms is described in the following figure.



10.1 Single Qubit operations

10.1.1 Bloch Sphere

We know that a qubit can be represented as $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$. Also, $\langle\psi\rangle\,\psi = 1$. Keeping these in mind, we can represent a qubit as

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

The absolute phase of a qubit is not important, only the relative phase is. Hence, we can dissolve the $e^{\iota\gamma}$ term and represent a qubit in terms of θ and ϕ. This representation is called the Bloch Sphere representation; the vector

$$(\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\phi)$$

is the Bloch vector corresponding to (θ, ϕ). Observe that the orthogonal basis vectors are antipodal to each other.

10.1.2 Pauli matrices

Three of the most important single qubit operators are the Pauli Matrices. They are defined as follows:

- X = $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
- Y = $\begin{bmatrix} 0 & -\iota \\ \iota & 0 \end{bmatrix}$
- Z = $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

Other important operators include

- H(hadamard) = $\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
- S(phase gate) = $\begin{bmatrix} 1 & 0 \\ 0 & \iota \end{bmatrix}$
- T($\pi/8$ gate) = $\begin{bmatrix} 1 & 0 \\ 0 & \exp\frac{\iota\pi}{4} \end{bmatrix}$

The Pauli matrices satisfy $A = A^\dagger$ and $A^2 = I$. Hence, we can construct a matrix

$$R_x = e^{-\iota\theta X/2} = \cos\frac{\theta}{2}I - \iota\sin\frac{\theta}{2}X$$

Similarly, we can also define R_y and R_z, all of which are unitary matrices(since the Pauli matrices are hermitian) and these matrices represent the rotation about x, y and z axes respectively.
A rotation about an arbitrary axis represented by $\hat{n}$ is described by

$$R_n = e^{-\iota\theta(\hat{n}.\bar{\sigma})/2} = \cos\frac{\theta}{2}I - \iota\sin\frac{\theta}{2}(\hat{n}.\bar{\sigma})$$

where $\bar{\sigma}$ is the vector (X, Y, Z). These matrices are called rotation matrices because, when applied on a qubit, their Bloch sphere representation gets rotated by that angle with respect to that axis.

Theorem 1 *If U is a unitary matrix, then there exist real numbers α, β, γ and δ such that*

$$U = e^{\iota\alpha}R_z(\beta)R_y(\gamma)R_z(\delta)$$

Corollary 1 *For a unitary matrix U and linearly independent unit vectors $\hat{n}$ and $\hat{m}$, there exist real numbers α, β, γ and δ such that*

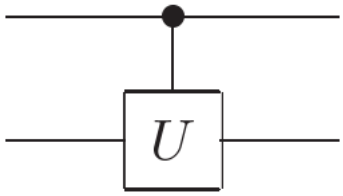
$$U = e^{\iota\alpha}R_{\hat{n}}(\beta)R_{\hat{m}}(\gamma)R_{\hat{n}}(\delta)$$

Some identities: $HZH = X, HXH = Z, HYH = -Y$

10.2 Controlled gates

10.2.1 2 qubit system

A controlled U gate is a 2 qubit gate such that $|c\rangle |t\rangle \longrightarrow |c\rangle U^c |t\rangle$, i.e. teh gate U is applied to $|t\rangle$ if the bit $|c\rangle$ is 1, otherwise it is not. It is represented as follows:



For a 2 qubit system, say that gate U_1 acts on the first qubit and the gate U_2 acts on the second qubit, then the gate which acts on both the qubits combinedly and produces the same effect is $U_1 \otimes U_2$. Let us now look at an example. It is known that $HZH = X$. A question is posed which asks us to construct a CNOT gate from a CZ gate and 2 H gates. Realize that CNOT is the same as a CX gate. And indeed,

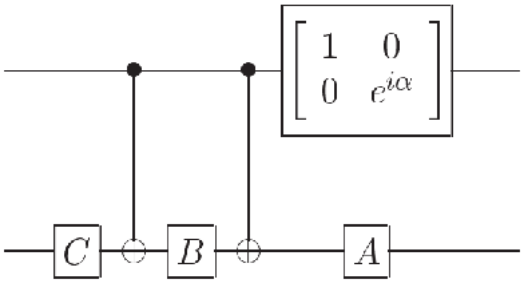
$$CX = (I \otimes H)CZ(I \otimes H)$$

this is true because $H^2 = I$.

Next, we look at how to implement an arbitrary Controlled-U gate. Observe that for a unitary matrix U, there exist matrices A, B and C satisfying $ABC = I$ and a real number α such that

$$U = e^{\iota\alpha} AXBXC$$

Now, this information is almost sufficient to conclude our answer. Consider the following circuit:



Let us go through the circuit; if the control bit is $|0\rangle$, then the CNOT gates won't get activated. Hence the penultimate state would be

$$|x_1\rangle |x_2\rangle \longrightarrow |x_1\rangle ABC |x_2\rangle = |x_1\rangle |x_2\rangle$$

If the control bit is $|1\rangle$, the CNOT gate is activated and the penultimate state becomes

$$|x_1\rangle |x_2\rangle \longrightarrow |x_1\rangle AXBXC |x_2\rangle$$

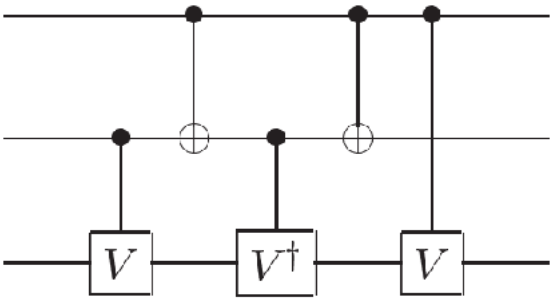
A final treatment is done to the "penultimate" state by applying the gate which adds a phase factor of $e^{\iota\alpha}$ to the state if the control bit is $|1\rangle$. After this treatment, we get the required behaviour from this circuit i.e. Controlled-U gate.

10.2.2 $n + k$ qubit system

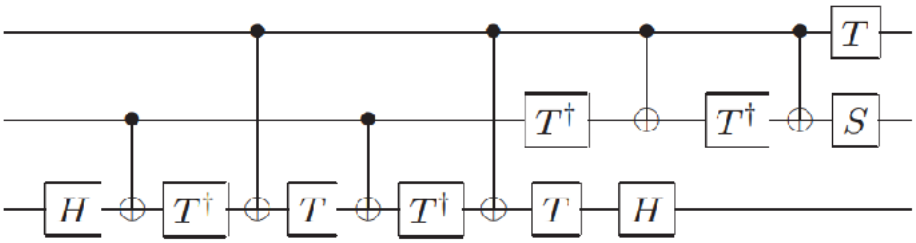
Now, we want the control bits to be the first n bits and the target bits to be the last k bits. We use the following notation:

$$C^n(U) |x_1 x_2 \cdots x_n\rangle |\psi\rangle = |x_1 x_2 \cdots x_n\rangle U^{x_1 x_2 \cdots x_n} |\psi\rangle$$

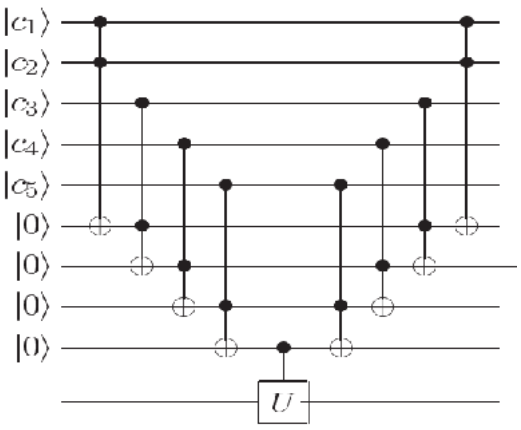
Given below is the general circuit diagram of $C^2(U)$ gate where U is a single qubit gate. Let V be a unitary operator such that $V^2 = U$, then the following circuit, built of only 1 and 2 qubit gates is equivalent to the $C^2(U)$ gate.



The $C^2(X)$ gate is also called the Toffoli Gate(introduced earlier as well).
Any Unitary operation can be described to an arbitrary precision by using only the Hadamard, phase, CX and $\pi/8$ gates. Following is an implementation of the Toffoli gate using the above mentioned gates:



Now, for an arbitrary unitary operator U, let us make a circuit that implements $C^n(U)$. The following cicuit does the job.



This cicuit is for $n = 5$. There are n control bits, 4 work bits(w_i, initialized to $|0\rangle$) and 1 target bit. First, we AND all the control bits using the work bits.(i.e $c_1.c_2$ and store it in w_1, $w_1.c_3$ and store it in w_2 and so on). Then apply CU on w_{n-1}. This bit would've stored the AND of c_i's till then. Finally perform C^2X operations again and since $(C^2X)^2 = I$, the work bits will revert to their original state.

10.3 Measurement

We use projective measurements unless otherwise specified.

Principle of deferred measurement: Measurements can always be moved from an intermediate stage of a quantum circuit to the end of the circuit; if the measurement results are used at any stage of the circuit then the classically controlled operations can be replaced by conditional quantum operations

Principle of implicit measurement: Without loss of generality, any unterminated quantum wires (qubits which are not measured) at the end of a quantum circuit may be assumed to be measured.

Measurement in quantum circuits is like an interface between the quantum and classical worlds. In most of the cases, measurements are irreversible, destroying quantum information and replacing them with classical information. This might look contradictory as quantum teleportation seems to preserve quantum information after measurement. However, this is not the information about the quantum state being measured.

There is a stronger theorem which says that in order for a measurement to be reversible, it must reveal no information about the state being measured.

11 Quantum Fourier Transform

11.1 The Quantum Discrete Fourier Transform

11.1.1 Introduction

The prime factorization of an n bit number is thought to require $\exp(\Theta(n^{\frac{1}{3}} \log^{\frac{2}{3}} n))$ operations using the best classical algorithm called the *number field sieve*. Quantum Computers are thought to compute the factorization in only $O(n^2 \log n \log\log n)$.

11.1.2 The Discrete Fourier Transform

Now we'll look at the Quantum Fourier Transform which is an efficient algorithm for performing a Fourier Transform of Quantum Mechanical Amplitudes. Note that it does NOT speed up a classical Fourier Transform of classical data. QFT enables us to perform *phase estimation* i.e. approximation of eigen values of a unitary operator.

A key step in the discovery of fast quantum algorithms is the discovery of transforms that can be performed much faster on a quantum computer than a classical computer. One such transform is the *discrete fourier transform*. In the classical notation, this transform takes an input vector $(x_0, x_1 \cdots x_{N-1})$ and outputs the transform $(y_0, y_1, \cdots, y_{N-1})$ using the following algorithm:

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

The quantum discrete fourier transfom does exactly the same thing, just that ir requires a bit more formalization. It acts on an orthogonal basis $|0\rangle, |1\rangle \cdots |N-1\rangle$ and transforms them a follows:

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

This is equivalent to writing

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

Observe that the above transformation is unitary. Now we introduce a different and much more convenient to use notation for the quantum fourier transform. Before that. let's make a few more observations. Hereon, we are interested in the computational basis for n qubits i.e. $N = 2^n$. $|j\rangle = |j_1 j_2 \cdots j_n\rangle$ and $j = \sum_{i=1}^{n} 2^{n-i} j_i$. Also, we introduce the notation

$$0.j_l j_{l+1} \cdots j_m = \sum_{i=1}^{m-l+1} 2^{-i} j_{l+i-1}$$

. Now, let us write an alternative form of the QFT. For a qubit $|j\rangle$, teh QFT transforms it into:

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

$$\implies |j\rangle \longrightarrow \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{\iota(2\pi j \sum_{l=1}^{n} 2^{-l} k_l)} |k_1 k_2 \cdots k_n\rangle$$

$$\implies |j\rangle \longrightarrow \frac{1}{2^{n/2}} \sum_{k_1=\{0,1\}} \sum_{k_2=\{0,1\}} \cdots \sum_{k_n=\{0,1\}} e^{\iota(2\pi j \sum_{l=1}^{n} 2^{-l} k_l)} |k_1 k_2 \cdots k_n\rangle$$

$$\implies |j\rangle \longrightarrow \frac{1}{2^{n/2}} \sum_{k_1=\{0,1\}} \sum_{k_2=\{0,1\}} \cdots \sum_{k_n=\{0,1\}} e^{\iota(2\pi j \sum_{l=1}^{n} 2^{-l} k_l)} \bigotimes_{l=1}^{n} |k_l\rangle$$

$$\implies |j\rangle \longrightarrow \frac{1}{2^{n/2}} \sum_{k_1=\{0,1\}} \sum_{k_2=\{0,1\}} \cdots \sum_{k_n=\{0,1\}} \bigotimes_{l=1}^{n} e^{\iota(2\pi j(2^{-l} k_l))} |k_l\rangle$$

$$\implies |j\rangle \longrightarrow \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \sum_{k_l=\{0,1\}} e^{\iota(2\pi j(2^{-l} k_l))} |k_l\rangle$$

$$\implies |j\rangle \longrightarrow \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left(|0\rangle + e^{\iota(2\pi j(2^{-l}))} |1\rangle\right)$$

Using the fact that $e^{\iota(2\pi p)} = 1$ where p is an integer, we can further simplify the above expression as:

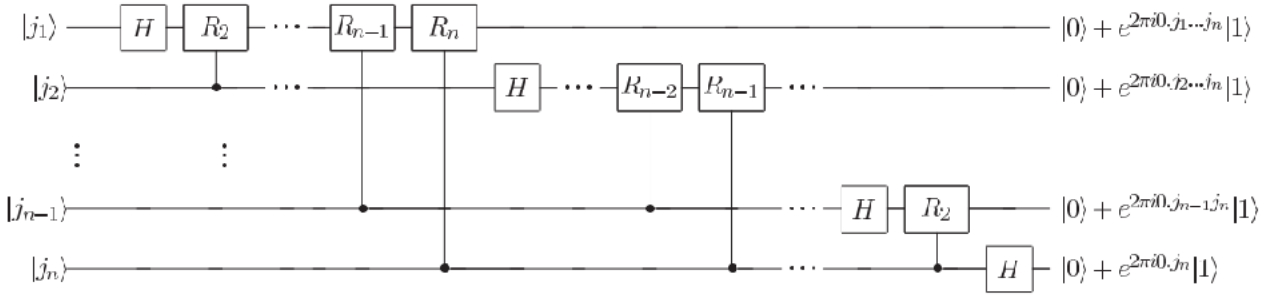
$$\implies |j\rangle \longrightarrow \frac{\left(|0\rangle + e^{\iota(2\pi(0.j_n))} |1\rangle\right) \otimes \left(|0\rangle + e^{\iota(2\pi(0.j_{n-1}n))} |1\rangle\right) \cdots \left(|0\rangle + e^{\iota(2\pi(0.j_1 j_2 \cdots j_n))} |1\rangle\right)}{2^{n/2}}$$

Now, this representation of the QFT is easier to implement. Let us define a gate

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{\iota(2\pi/2^k)} \end{bmatrix}$$

11.2 QFT circuit

Consider the following circuit. This circuit applies QFT on the computational basis $|j_1 j_2 \cdots j_n\rangle$.



After the Hadamard gate is applied on the first bit, the state becomes

$$\psi = \frac{1}{\sqrt{2}} \left(|0\rangle + e^{\iota 2\pi (0.j_1)} |1\rangle \right) |j_2 j_3 \cdots j_n\rangle$$

Next, apply a $C - R_2$ gate with the second bit as the control bit and the first bit as the target bit. The state then becomes

$$\psi = \frac{1}{\sqrt{2}} \left(|0\rangle + e^{\iota 2\pi (0.j_1 j_2)} |1\rangle \right) |j_2 j_3 \cdots j_n\rangle$$

In a similar way, apply $C - R_3, C - R_4 \cdots C - R_n$ and then the state becomes

$$\psi = \frac{1}{\sqrt{2}} \left(|0\rangle + e^{\iota 2\pi (0.j_1 j_2 \cdots j_n)} |1\rangle \right) |j_2 j_3 \cdots j_n\rangle$$

Now perform similar operations on the second bit, and then on the third bit and so on so that the final state becomes

$$\psi = \frac{\left(|0\rangle + e^{\iota (2\pi (0.j_1 j_2 \cdots j_n))} |1\rangle \right) \otimes \left(|0\rangle + e^{\iota (2\pi (0.j_2 j_3 \cdots j_n))} |1\rangle \right) \cdots \left(|0\rangle + e^{\iota (2\pi (0.j_n))} |1\rangle \right)}{2^{n/2}}$$

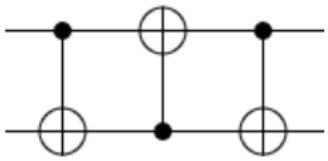
Now apply swap operations on the qubits to reorder them as:

$$\psi = \frac{\left(|0\rangle + e^{\iota (2\pi (0.j_n))} |1\rangle \right) \otimes \left(|0\rangle + e^{\iota (2\pi (0.j_{n-1} n))} |1\rangle \right) \cdots \left(|0\rangle + e^{\iota (2\pi (0.j_1 j_2 \cdots j_n))} |1\rangle \right)}{2^{n/2}}$$

Since we haven't introduced the SWAP gate before, let's take a moment to look at it. SWAP gate is represented by the following unitary matrix:

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

We can implement this gate using 3 CX gates as follows:



Coming to the QFT circuit, we would need approximately n^2 gates so the time complexity of the circuit is $\Theta(n^2)$ In lame terms, n bits are equivalent to 2^n elements in the classical world. The complexity of the fastest classical algorithm for FT, which is the *Fast Fourier Transform*, is $\Theta(n2^n)$. But as we already know, this huge speed up in the algorithm is not quite accessible to us because there is no way to find the amplitudes without performing a measurement; and when a measurement is performed, information is lost. Moreover, there is no efficient way to input into the QFT circuit. Hence, the QFT is not of any direct use. We now look at an application of the QFT called *Phase Estimation*.

11.3 Phase Estimation

11.3.1 Introduction

We know that all the eigen values of a Unitary matrix have modulus unity. Here is a quick proof:
Let v be an eigenvector of a unitary matrix U and let λ be the corresponding eigenvalue.

$$\implies Uv = \lambda v$$

Multiplying by $U^\dagger$ on both sides, we get

$$v = \lambda U^\dagger v \implies U^\dagger v = v/\lambda$$

Now, multiply the first equation on both sides by $v^\dagger$, we get

$$v^\dagger U v = \lambda v^\dagger v$$

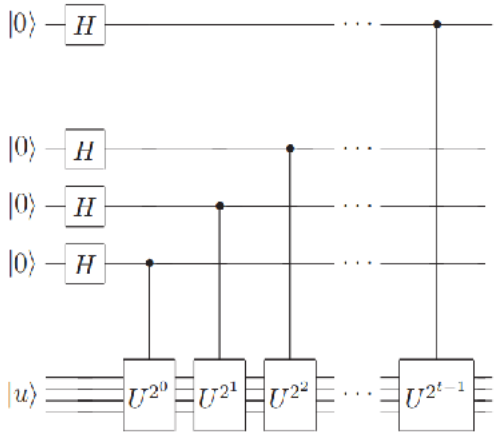
Taking adjoint on both sides, we get

$$v^\dagger U^\dagger v = \overline{\lambda} v^\dagger v \implies v^\dagger v/\lambda = \overline{\lambda} v^\dagger v$$

Cancelling $v^\dagger v$ on both sides, we get $|\lambda| = 1$. This means that λ can be written in the form $e^{\iota(2\pi\phi)}$, $\phi \in [0, 1]$. The goal of the *phase estimation* algorithm is to estimate ϕ. Now we assume that we have **black boxes** that prepare the initial state and compute $C - U^{2^j}$ for suitable j. Note that this assumption makes the phase estimation process just a module and not a complete algorithm.

11.3.2 The Algorithm

This procedure uses 2 registers. The first register contains t qubits in the state $|0\rangle$. t reflects the precision in estimating the phase and also the probability with which the procedure would be successful. The second register begins with the state $|u\rangle$, where $|u\rangle$ is the eigenvector corresponding to the phase factor ϕ. Consider the following circuit.



Observe that $U^i |u\rangle = \lambda^i |u\rangle$. After the application of this circuit, the final state of the circuit becomes:

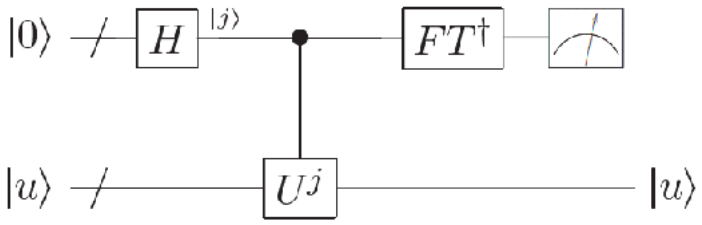
$$\psi = \frac{1}{2^{t/2}} \left(|0\rangle + e^{\iota(2\pi\phi 2^{t-1})} |1\rangle\right) \otimes \left(|0\rangle + e^{\iota(2\pi\phi 2^{t-2})} |1\rangle\right) \cdots \left(|0\rangle + e^{\iota(2\pi\phi 2^{0})} |1\rangle\right) \otimes |u\rangle$$

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

Now, apply an *inverse QFT* on the first register by reversing the QFT circuit(assume that the circuit of QFT is the unitary matrix X, then apply $X^\dagger$ for the inverse QFT). Let us assume that $\phi = 0.\phi_1\phi_2\cdots\phi_t$ to a precision of t digits. Now, we can rewrite the first state result of the first register as

$$\psi = \frac{\left(|0\rangle + e^{\iota(2\pi(0.\phi_t))} |1\rangle\right) \otimes \left(|0\rangle + e^{\iota(2\pi(0.\phi_{t-1}t))} |1\rangle\right) \cdots \left(|0\rangle + e^{\iota(2\pi(0.\phi_1\phi_2\cdots j_t))} |1\rangle\right)}{2^{t/2}}$$

Observe that this is the QFT of the state $|\phi_1\phi_2\cdots\phi_t\rangle$, Hence on applying inverse QFT to the above state, the first register becomes $|\phi_1\phi_2\cdots\phi_t\rangle$. Given below is a schematic of both the stages combined:



11.4 Applications of QFT: Order finding and Factoring

11.4.1 Order

Order: For coprime positive integers x and N with $x < N$, the order of x modulo N is defined as the least positive integer r such that

$$x^r \equiv 1 \bmod N$$

We now prove that $r \leq N$.
Proof: Consider the set of numbers

$$\{x^0, x^1 \cdots x^N\}$$

This set has length N; if we take the modulo of all the numbers in this set with N, then we would have $N+1$ numbers. But the set of remainders modulo N has size N. So there have to be 2 indices m and $n, m > n$ such that

$$x^m \equiv x^n \bmod N$$

Now, we use the fact that x and N are coprime and write

$$x^{m-n} \equiv 1 \bmod N$$

So, we have proved that there exits a non-zero index $m-n$ for which the modulo is 1. $m - n < N$ and this completes the proof.

Let $L = \lceil \log N \rceil$. Consider the unitary matrix U such that

$$U\,|y\rangle = |xy \bmod N\rangle$$

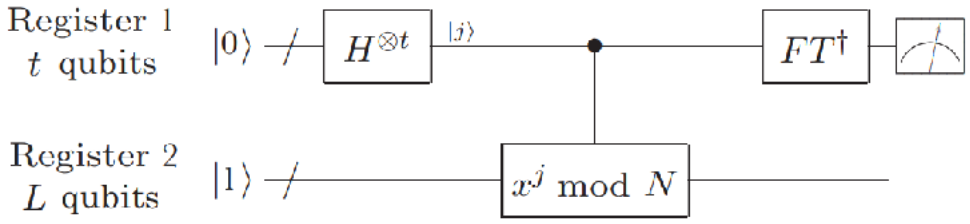
where $|y\rangle \in \{0,1\}^L$. Observe that the vectors

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\iota(2\pi sk/r)}\,|x^k \bmod N\rangle$$

are eigenvectors of U with eigenvalues $e^{\iota(2\pi s/r)}$ respectively. Now the problem reduces to applying the phase estimation procedure and finding the value of r. Here, the tricky problem is to prepare the state $|u_s\rangle$ because it appears as if it requires us to know r already. Observe that

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

Now, if we take $t = 2L + 1 + \left\lceil \log\left(2 + \frac{1}{2\epsilon}\right) \right\rceil$ and construct the second register in the state $|1\rangle$, we can estimate the phase s/r to a precision of $2L+1$ bits with a probability of atleast $(1-\epsilon)/r$



From the retrieved value of s/r upto $2L+1$ digits, we can estimate the value of r knowing that the decimal is a ratio of 2 integers using the **continued fractions theorem.**

Theorem 2 *Let s/r be a rational number such that*

$$\left|\frac{s}{r} - \phi\right| \leq \frac{1}{2r^2}$$

Then s/r is the convergent continued fraction for ϕ and can be computed in $O(L^3)$ time using the continued fractions algorithm.

11.4.2 Factoring

Theorem 3 *Suppose that N is an L bit composite number and x is a non trivial solution to $x^2 = 1 \mod N$ such that $x \in [1, N]$. Then, at least one of gcd($x-1$, N) or gcd($x+1$, N) is a non trivial factor of N that can be computed using $O(L^3)$ operations.*

Theorem 4 *Let $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be the prime factorization of an odd composite N. Let x be an integer chosen at random, subject to $x \in [1, N-1]$ and x is coprime to N. Let r be the order of x with respect to N. Then,*
P(r is even and $x^{r/2} \neq -1 \mod N$) $\geq 1 - \frac{1}{2^k}$

Procedure:

- If N is even, return 2.
- Determine if $N = a^b$. If yes, then return a.
- Choose x randomly from $[1, N]$. If gcd(x, N) $\neq 1$, then return gcd(x, N) $\neq 1$.
- Perform the order finding sub routine to find the order r of x modulo N.
- If r is even and $x^{r/2} \neq -1 \mod N$, then compute gcd($x^{r/2} - 1$, N) and gcd($x^{r/2} + 1$, N) to check if one of them is non trivial. If yes, then return that factor.
- Else, the algorithm fails.

12 Quantum Search

12.1 Grover's Algorithm

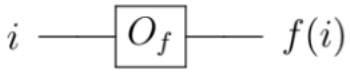
This algorithm solves the problem of unstructured search in $O(\sqrt{N})$ time. The problem is as follows
Given a set of N elements $X = \{x_1, x_2 \cdots x_N\}$ and a function $f : X \longrightarrow \{0, 1\}$, our goal is to find an $x^* \in X$ such that $f(x^*) = 1$

12.1.1 Classical Search

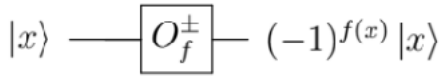
In the classical case, we make $\Theta(N)$ queries and a running time of $\Theta(N)$. This can't be made better by any means.

12.1.2 Quantum Search

We now assume that the element x^* is unique and that $N = 2^n$. In the classical scenario, the function is applied to the bits as follows:



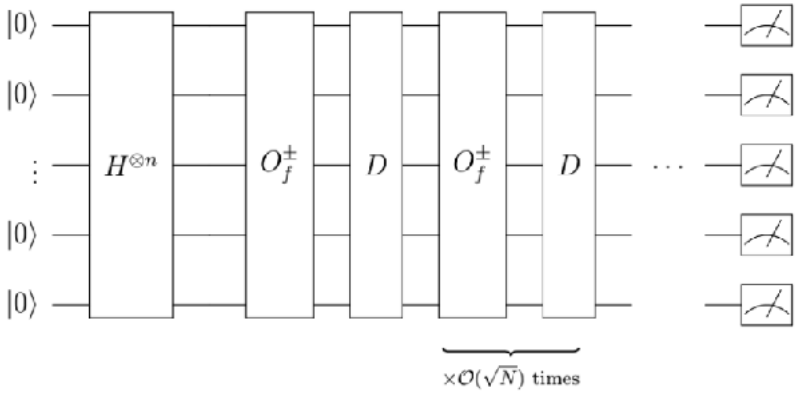
But this circuit is forbidden is the quantum world because it is not reversible. We can overcome this by the following circuit:



Let $\mu = \langle \alpha_i \rangle$ where α_i's are the amplitudes of $\{0, 1\}^n$. Let us define another gate called the *Grover's diffusion gate D* which does the following:

$$\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \longrightarrow \sum_{x \in \{0,1\}^n} (2\mu - \alpha_x) |x\rangle$$

Now, Consider the following circuit.



After applying the $H^{\otimes n}$ gate, we get the state

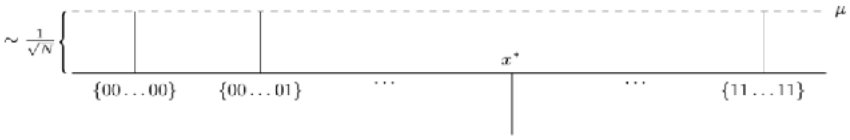
$$\frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle$$

The amplitudes of different components in the state is as follows:

After the $O_f^{\pm}$ gate, the state becomes

$$\frac{1}{\sqrt{N}} \left(-|x^*\rangle + \sum_{x \in \{0,1\}^n,\, x \neq x^*} |x\rangle \right)$$

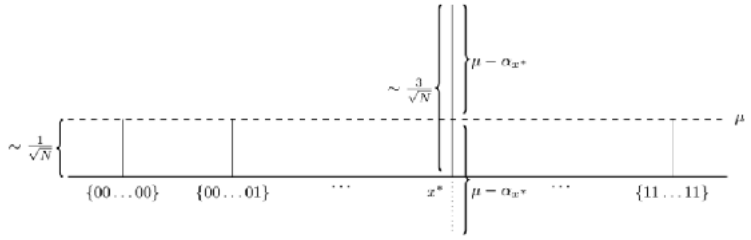
The amplitudes of different components is now:



Now we apply the diffusion gate, this is what lets us increase the amplitude of $|x^*\rangle$. The mean amplitude prior to the diffusion gate is

$$\mu = \frac{1}{N} \sum_{x \in \{0,1\}^n} \alpha_x = \frac{2^n - 2}{N\sqrt{N}} \sim \frac{1}{\sqrt{N}}$$

Hence, the amplitudes of the other components would roughly be the same, except the amplitude of $|x^*\rangle$ which would be roughly $3/\sqrt{N}$.



Now we repeat the same process to amplify $|x^*\rangle$ to an arbitrary amount(say, 0.1). It is easy to see that this can be achieved in $O(\sqrt{N})$ time.

References

1. Quantum Computing and Quantum Information, 10^{th} Anniversary Edition - Michael A. Nielsen Isaac L. Chuang
2. Quantum Computation Scribe Notes by Ryan O Donnell and John Wright