Module-3

Quantum Computing

Syllabus:

Principles of Quantum Information & Quantum Computing: Introduction to Quantum Computing, Moore's law & its end. Classical & quantum information comparison. Differences between classical & quantum computing. Concept of qubit and its properties, representation of qubit by Bloch sphere, single and two qubits. Extension to N qubits.

Dirac representation and matrix operations: Matrix representation of 0 and 1 states, Identity Operator I, applying I to|0> and |1> states to show there is no change, Pauli Matrices and its operations on 0 and 1 states, Explanation of i) Conjugate of a matrix and ii) Transpose of a matrix, Unitary Matrix U, Examples : Row and Column Matrices and their multiplication (Inner Product), Probability and quantum superposition, normalisation rule, Orthogonality and orthonormality.

Quantum Gates: Single Qubit Gates: Quantum Not Gate , Pauli X-Gate, Y-Gate and Z Gates, Hadamard Gate , Phase Gate (or S Gate), T Gate

Multiple Qubit Gates: Controlled gate, CNOT Gate, (Discussion for 4 different input states). Representation of Swap gate, Controlled -Z gate, Toffoli gate.

Prerequisites: Matrices

Self learning: Moore's law

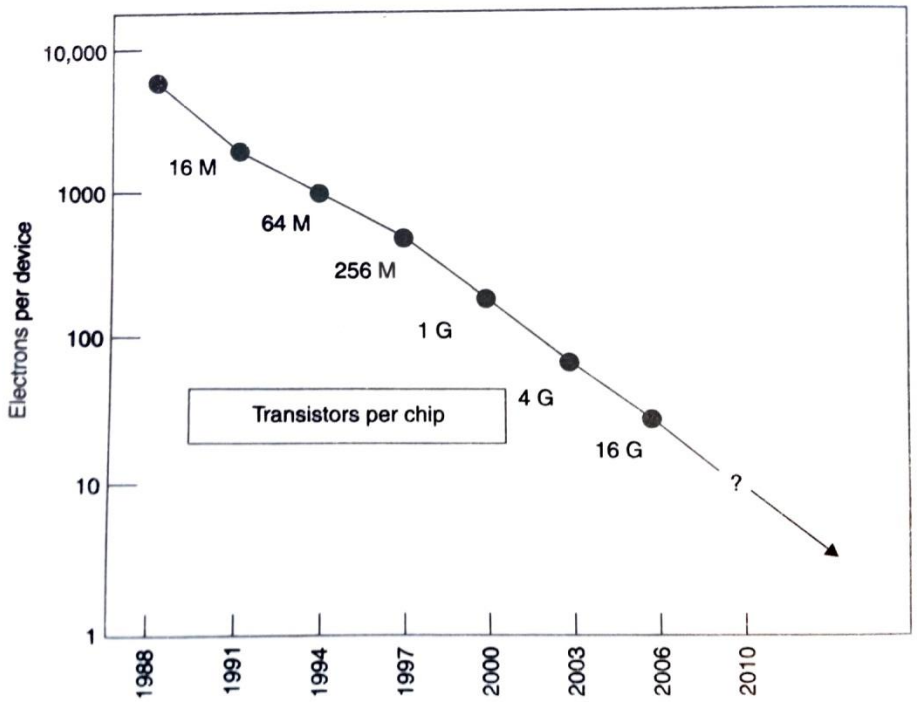
Principles of Quantum Information & Quantum Computing

Introduction to Quantum Computing

Modern computers operate according to programs that divide a task into elementary operations, which are then carried out serially, one operation at time. Even if we persuade two or more computers to work on different aspects of a problem at the same time, the computing process would be slow. This is because the logic built into microprocessors is inherently serial. Fortunately, a parallel computer that would be able to carry out many operations at once does exist. They are called quantum computers, which work according to the rules of quantum mechanics. The discovery that elementary particles such as protons, neutrons and electrons can exist in two or more states at a time has made it possible in principle to harness them as processing units in a machine that is more efficient than classical computers.

Quantum computers can perform computational tasks such as factorizing a number or carry out searches in database. Quantum computer networks can efficiently transmit and receive information in unusual ways. They find immense potential in the science of cryptography (science of maintaining secrecy and security in communication).

Moore's law & its end:



In 1965, Gordon Moore observed that the number of transistors on a microchip doubles every two years. This is known as Moore's law. The computer industry has followed his prediction throughout for 45 years. Because of this, conventional computers have increased the speed and miniaturisation at an exponential rate. So, we might reach a stage where a number of electrons to be small as 10 per device. Clearly there is an upper limit for the miniaturisation. A physical device of such microscopic dimensions may not behave the same way as a device of bigger dimensions. The present day research in the field of nanotechnology suggests that materials behave differently at such small scales. Also, miniaturisation will have direct impact on the progress of computing power. What this means specifically, is that transistors in integrated circuits have become faster. The faster the integrated circuit conducts electricity, the faster the computer operates. This means that computers are projected to reach their limits because transistors will be unable to operate within smaller circuits at increasingly higher temperatures. This is due to the fact that cooling the transistors will require more energy than the energy that passes through the transistor itself. So, Moore's law should come to an end soon. All these observations have encouraged the development of new computing system.

Classical & quantum information comparison

The units of information processing system in classical system are bits. A bit has just two possible states (namely, '0' and '1'). In quantum information system the units used for information processing are qubits. A qubit has two basic states represented by $|0\rangle$ and $|1\rangle$. But it can also exist in a superposition state, which is a state other than $|0\rangle$ or $|1\rangle$. A single qubit can thus encode an infinite number of classical bits. In classical information processing the joint states of bits are changed and manipulated by means of classical logic gates.

Quantum information processing is also achieved by the operation of gates. As in the classical case, the states of qubits making up a quantum register can be changed step by step by the action of a number of quantum gates that constitute a universal set, where there can be more than one possible set of universal gates.

Differences between classical & quantum computing

Classical computing	Quantum computing
Classical computers use binary codes i.e. bits 0 or 1 to represent information	Quantum computers use Qubits i.e. 0, 1 and both of them simultaneously to run machines faster
Information storage is bit based on voltage or charge etc.	Information storage is Quantum bit based on direction of an electron spin
Information processing is carried out by logic gates e.g. NOT, AND, OR etc.	Information processing is carried out by Quantum logic gates
Circuit behaviour is governed by classical physics	Circuit behaviour is governed by quantum mechanics
Operations are defined by Boolean Algebra	Operations are defined by linear algebra and can be represented by unitary matrices with complex elements
It is large scale integrated multi-purpose computer	It is high speed parallel computer based on quantum mechanics
No restrictions exist on copying or measuring signals	Severe restrictions exist on copying and measuring signals

Concept of qubit and its properties

This basic unit of information in quantum computing is called the qubit, which is short for quantum bit. There is a fundamental difference between a classical bit and a qubit. Like a bit, a qubit can also be in one of two states. We label these two states by $|0\rangle$ and $|1\rangle$. But it can also exist in a superposition state, which is a state other than $|0\rangle$ or $|1\rangle$. In other words, the state of a qubit is a vector in a two-dimensional complex vector space. The special states $|0\rangle$ and $|1\rangle$ are known as computational basis states. For example if white and black colours correspond to state $|0\rangle$ and $|1\rangle$ then a qubit is imagined to be to have any shade of grey.

The superposition state is a linear combination of the states $|0\rangle$ and $|1\rangle$. If we label this state $|\psi\rangle$, a superposition state is written as

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ ----------(1)

Here α, β are complex numbers. That is, the numbers of the form z = x + iy, where i = $\sqrt{-1}$

The laws of quantum mechanics tell us that the modulus squared of α, β in the above equation gives us the probability of finding the qubit in state $|0\rangle$ or $|1\rangle$. In other words,

$|\alpha|^2$: Tells us the probability of finding $|\psi\rangle$ in state $|0\rangle$

$|\beta|^2$: Tells us the probability of finding $|\psi\rangle$ in state $|1\rangle$

Therefore, when we measure a qubit we get either the result 0, with probability $|\alpha|^2$, or the result 1, with probability $|\beta|^2$. Also, the total probability $|\alpha|^2 + |\beta|^2 = 1$, according to theory of probability. Thus, we cannot examine a qubit to determine its quantum state, that is, the values of α and β. Instead, quantum mechanics tells us that we can only acquire much more restricted information about the quantum state. It is because a qubit can exist in a continuum of states between $|0\rangle$ and $|1\rangle$ until it is observed. So, we have to keep in mind that when a qubit is measured, it only gives '0' or '1' as the measurement result – probabilistically.

For example, a qubit can be in the state

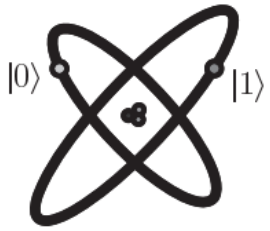
$\frac{1}{\sqrt{2}}\ |0\rangle + \frac{1}{\sqrt{2}}\ |1\rangle$

By comparing with equation (1) we get $\alpha = \frac{1}{\sqrt{2}}$ and $\beta = \frac{1}{\sqrt{2}}$

Which means $|\alpha|^2 = |\beta|^2 = \frac{1}{2}$, Therefore, the measurement gives 0 fifty percent of the time and 1 another fifty percent of the time. Hence we often return the state represented by $|+\rangle$.

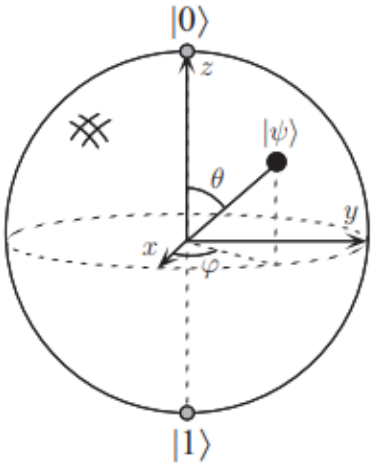
Examples for physical systems used to realize qubits:

1. Two states of an electron orbiting a single atom are as shown in Figure. In the atom model, the electron can exist in either the 'ground' or 'excited' states, which we call $|0\rangle$ and $|1\rangle$, respectively. By shining light on the atom, with appropriate energy and for an appropriate length of time, it is possible to move the electron from the $|0\rangle$ to $|1\rangle$ and vice versa. But, by reducing the time we shine the light, an electron initially in the state $|0\rangle$ can be moved 'halfway' between $|0\rangle$ and $|1\rangle$, into the $|+\rangle$ state.
2. Two different polarisations of a photon.
3. Alignment of a nuclear spin in a uniform magnetic field.



If we consider a system of n qubits, the quantum state of such a system is specified by 2^n amplitudes. For n = 500 this number is larger than the estimated number of atoms in the Universe. Storing all these complex numbers would not be possible on any conceivable classical computer. But it is possible in quantum computers.

Representation of a qubit by Bloch Sphere



Bloch Sphere representation of a qubit

To represent qubits geometrically, we use a three dimensional sphere of unit radius called Bloch sphere. It provides a useful means of visualising the state of a single qubit.

A complex number $Z = x + iy$ can be expressed in polar form as

$$x = rcos\theta$$

$$y = rsin\theta$$

$$Z = r(cos\theta + isin\theta) = re^{i\theta}$$

We know that a superposed state is represented by the equation $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Since $|\alpha|^2 + |\beta|^2 = 1$, we can rewrite the superposed state as

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

Where θ and $\emptyset$ define a point on the Bloch sphere as shown in figure.

For $\emptyset = 0^o$ and $\theta = 0$, the state $|\psi\rangle$ corresponds to $|0\rangle$ and is along +Z- axis.

For $\emptyset = 0^o$ and $\theta = 180^o$, the state $|\psi\rangle$ corresponds to $|1\rangle$ and is along -Z- axis.

When $\theta = 90^o$, the vector is in the x-y plane

For $\emptyset = 90^o$, $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$, is a superposition state along + y axis.

For $\emptyset = -90^o$, $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$, is a superposition state along - y axis.

For $\emptyset = 0^o$, $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, is a superposition state along + x axis.

For $\emptyset = 180^o$, $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, is a superposition state along - x axis.

For a classical computer the states the two logical states 0 and 1 are represented by poles of the sphere. In contrast, the state of a qubit can be represented by any point on the sphere. Since there are infinite points on the sphere, a qubit has capacity to store more information compared to classical bit.

Single and two qubits, extension to N qubits

Two qubits:

In case we have two classical bits the possible configurations are 00, 01, 10 and 11. Suppose we have two qubits, they can be in one of the four computational basis states denoted by $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$. Similarly a pair of qubits can also exist in superposition of these four states, so that

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

These four states define various possibilities. Thus a two qubit system can store all four numbers simultaneously. An interesting feature with two qubit system is the occurrence of entangled states. They are known as Bell states or EPR (Einstein-Podolsky-Rosen) states. These states enormously enhance the power of computation and communication. The Bell state is represented by

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

If we measure the first qubit, then with 50% probability we obtain the result 0. The resulting post-measurement state will be $|00\rangle$ so measuring the second qubit will also give a result of 0.

On the other hand, if we measure the first qubit as 1 with 50% probability, then the resulting post-measurement state will be $|11\rangle$, so measuring the second qubit will now give a result of 1. In general for *n*-qubit states, there will be superposition involving 2^n terms and can be represented by

$|\psi\rangle = \sum_{x=0}^{2^n-1} a_x|x\rangle$

Where x within the symbol $|\ \rangle$ (this symbol is called ket) is written in the binary notation. Thus in general a system of L qubits can store up to 2^L numbers at the same time in superposition.

Dirac representation and matrix operations:

Matrix representation of 0 and 1 states:

In quantum mechanics 0 and 1 states are represented by kets $|0\rangle$ and $|1\rangle$. They are given by the column matrices

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

Identity Operator I:

The Identity Operator I is given by $I = \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$

It is the simplest operator, and does nothing to any ket on application, ie. $I|u\rangle = |u\rangle$

On applying I to $|0\rangle$ and $|1\rangle$, no change occurs as shown below

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

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

Pauli Matrices and its operations on 0 and 1 states:

Pauli matrices:

These are 2 by 2 matrices, which go by a variety of notations. The matrices, and their corresponding notations, are shown below. The Pauli matrices are very useful in the study of quantum computation and quantum information.

$$\sigma_0 = I = \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$$

$$\sigma_1 = \sigma_X = X = \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$$

$$\sigma_2 = \sigma_Y = Y = \begin{bmatrix}0 & -i\\i & 0\end{bmatrix}$$

$$\sigma_3 = \sigma_z = Z = \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}$$

Operation of Pauli matrices on $|0\rangle$ and $|1\rangle$ basis states

We know that the basis states are given by

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

For X, we find that

$$X|0\rangle = \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix} \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}0*1 & + & 1*0\\1*1 & + & 0*0\end{bmatrix} = \begin{bmatrix}0\\1\end{bmatrix} = |1\rangle$$

$$X|1\rangle = \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix} \begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0*0 & + & 1*1\\1*0 & + & 0*1\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix} = |0\rangle$$

As noted above, since X transforms one basis state into the other, it is sometimes called the NOT operator.

$$Y|0\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0*1 & - & i*0 \\ i*1 & + & 0*0 \end{bmatrix} = \begin{bmatrix} 0 \\ i \end{bmatrix} = i|1\rangle$$

$$Y|1\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0*0 & - & i*1 \\ i*0 & + & 0*1 \end{bmatrix} = \begin{bmatrix} -i \\ 0 \end{bmatrix} = -i|0\rangle$$

And for Z, we have

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

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

Conjugate of a matrix:

If a matrix A consists of a complex number as elements, then the matrix obtained by the corresponding conjugate complex elements is called the conjugate of A and is denoted by A^*

If $A = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$ then $A^* = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}$

If $A = \begin{bmatrix} i & 0 \\ i & 0 \end{bmatrix}$ then $A^* = \begin{bmatrix} -i & 0 \\ -i & 0 \end{bmatrix}$

If $A = \begin{bmatrix} 1 & i \\ 1 & i \end{bmatrix}$ then $A^* = \begin{bmatrix} 1 & -i \\ 1 & -i \end{bmatrix}$

If $A = \begin{bmatrix} 1+3i & 1+i \\ 2i & 1-4i \end{bmatrix}$ then $A^* = \begin{bmatrix} 1-3i & 1-i \\ -2i & 1+4i \end{bmatrix}$

Transpose of a matrix:

If A is a matrix of order $m \times n$, then a matrix of order $n \times m$ obtained by interchanging the rows and columns of matrix A is called the transpose of A and is denoted by A^T.

If $A = \begin{bmatrix} 1 & i \\ 1 & i \end{bmatrix}$ then $A^T = \begin{bmatrix} 1 & 1 \\ i & i \end{bmatrix}$

If $A = \begin{bmatrix} 0 & 1 \\ i & 0 \end{bmatrix}$ then $A^T = \begin{bmatrix} 0 & i \\ 1 & 0 \end{bmatrix}$

If $A = \begin{bmatrix} 1+3i & 2i \\ 1+i & 1-4i \end{bmatrix}$ then $A^T = \begin{bmatrix} 1+3i & 1+i \\ 2i & 1-4i \end{bmatrix}$

Unitary Matrix U:

A Unitary matrix is represented as *U*. Conjugate transpose of *U* is $U^\dagger$ (called U-dagger).

The property of Unitary matrix is $UU^\dagger$= I

where I is a unit matrix (a square matrix having unit elements in the principal diagonal or leading diagonal and zero element everywhere else). Unitary operators are important because they describe the time evolution of a quantum state.

Row and Column Matrices and their multiplication (Inner Product):

All bra vectors are row matrices

ie $\langle\beta|$ = $(\beta_1 \ \beta_2)$

and all ket vectors are column matrices

ie $|\psi\rangle = \begin{pmatrix}\alpha_1\\ \alpha_2\end{pmatrix}$ which also means $\langle\psi| = (\alpha_1^* \ \alpha_2^*)$

Now, the inner product is $\langle\beta|\psi\rangle = (\beta_1 \ \beta_2)\begin{pmatrix}\alpha_1\\ \alpha_2\end{pmatrix} = \alpha_1\beta_1 + \alpha_2\beta_2$

For example: Wave function $\vec{\psi} = a\hat{\imath} + ib\hat{\jmath}$

$\hat{\imath} = \binom{1}{0} \quad \hat{\jmath} = \binom{0}{1}$

Therefore $\vec{\psi} = a\binom{1}{0} + ib\binom{0}{1} = \binom{a}{0} + \binom{0}{ib}$

$|\psi\rangle = \begin{pmatrix}a\\ ib\end{pmatrix}$ $|\psi^\dagger\rangle = (a \ -ib)$

$|\psi^\dagger\rangle|\psi\rangle = (a \ -ib)\binom{a}{ib} = a^2 + b^2$ -------gives probability

$|\psi^\dagger\rangle|\psi\rangle = \langle\psi|\psi\rangle$ is the inner product

Orthogonality:

Condition for orthogonality:

Inner product is $\langle\psi|\emptyset\rangle = 0$

For example: $\langle 0|$ = (1 0) and $|1\rangle = \begin{pmatrix}0\\ 1\end{pmatrix}$

Therefore $\langle 0|1\rangle$ = (1 0) $\begin{pmatrix}0\\ 1\end{pmatrix}$ = 0 + 0= 0

Orthonormality:

If $\langle a|a\rangle = 1$, then the vector is normalised.

If each element of a set of vectors is normalized and the elements are orthogonal with respect to each other, we say the set is orthonormal.

For example: Consider the set $\{\langle 0|, |1\rangle\}$

$\langle 0|0\rangle = (1\ 0)\begin{pmatrix}1\\0\end{pmatrix} = 1\times 1 + 0\times 0 = 1$ (normalized)

$\langle 0|1\rangle = (1\ 0)\begin{pmatrix}0\\1\end{pmatrix} = 1\times 0 + 0\times 1 = 0$ (orthogonal)

$\langle 1|0\rangle = (0\ 1)\begin{pmatrix}1\\0\end{pmatrix} = 0\times 1 + 1\times 0 = 0$ (orthogonal)

$\langle 1|1\rangle = (0\ 1)\begin{pmatrix}0\\1\end{pmatrix} = 0\times 0 + 1\times 1 = 1$ (normalized)

Hence the set $\{\langle 0|, |1\rangle\}$ is orthonormal

Quantum Gates

Single Qubit Gates

Quantum Not Gate: A quantum NOT gate for a qubit is a process that takes the state $|0\rangle$ to the state $|1\rangle$ and vice-versa. It is the quantum analogue for the NOT gate. In case of superposition, the quantum NOT gate acting linearly in the state $\alpha|0\rangle + \beta|1\rangle$ is taken to the state $\alpha|1\rangle + \beta|0\rangle$.

A quantum NOT gate is represented in matrix form by matrix X as shown below.

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

If the quantum state $\alpha|0\rangle + \beta|1\rangle$ is written in vector notations as $\begin{bmatrix}\alpha\\\beta\end{bmatrix}$

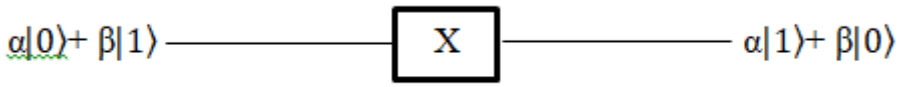
Then output from the quantum NOT gate is

$$X\begin{bmatrix}\alpha\\\beta\end{bmatrix} = \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}\begin{bmatrix}\alpha\\\beta\end{bmatrix} = \begin{bmatrix}\beta\\\alpha\end{bmatrix}$$ or $\alpha|1\rangle + \beta|0\rangle$

Similarly, if the input to the quantum NOT gate is $\alpha|1\rangle + \beta|0\rangle$

Then the output becomes $X\begin{bmatrix}\beta\\\alpha\end{bmatrix} = \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}\begin{bmatrix}\beta\\\alpha\end{bmatrix} = \begin{bmatrix}\alpha\\\beta\end{bmatrix}$ or $\alpha|0\rangle + \beta|1\rangle$

Following are the figure and truth table for quantum NOT gate



Input	Output
$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$
$\alpha\|0\rangle+ \beta\|1\rangle$	$\alpha\|1\rangle+ \beta\|0\rangle$

Pauli Z gate:

Pauli Z gate is defined as

$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ (Recall Pauli matrices)

If it operates on $|0\rangle$, we get

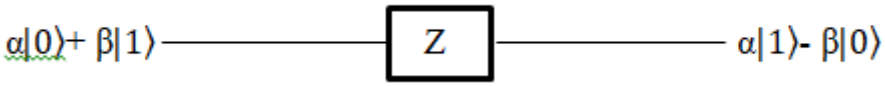
$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ ie $Z|0\rangle = |0\rangle$

If it operates on $|1\rangle$, we get

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

Thus the state $\alpha|0\rangle+ \beta|1\rangle$ is transformed to $\alpha|0\rangle- \beta|1\rangle$

Following are the figure and truth table for Pauli Z gate



Input	Output
$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$-\|1\rangle$
$\alpha\|0\rangle+ \beta\|1\rangle$	$\alpha\|0\rangle- \beta\|1\rangle$

Similarly for Pauli X and Y Gates

$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ (Recall Pauli matrices)

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

and similar kind of operation can be carried out on $|0\rangle$ and $|1\rangle$ as shown in the truth table below:

Truth table for Pauli X Gate	
Input	**Output**
$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$
$\alpha\|0\rangle+ \beta\|1\rangle$	$\alpha\|1\rangle+ \beta\|0\rangle$
Truth table for Pauli Y Gate	
Input	**Output**
$\|0\rangle$	$i\|1\rangle$
$\|1\rangle$	$-i\|0\rangle$
$\alpha\|0\rangle+ \beta\|1\rangle$	$-i\ \beta\|0\rangle + i\alpha\|1\rangle$

Hadamard Gate:

Hadamard Gate is defined as

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

If the quantum state $\alpha|0\rangle+ \beta|1\rangle$ is written in vector notations as $\begin{bmatrix}\alpha\\ \beta\end{bmatrix}$

Then it is transformed due to Hadamard Gate as

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}\alpha+\beta\\ \alpha-\beta\end{bmatrix} = \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle = \alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

Therefore

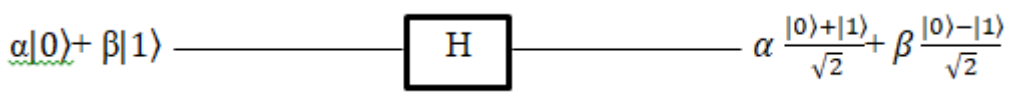
If Hadamard Gate operates on $|0\rangle$, we get

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} = 1\frac{|0\rangle+|1\rangle}{\sqrt{2}} + 0\frac{|0\rangle-|1\rangle}{\sqrt{2}} = \frac{(|0\rangle+|1\rangle)}{\sqrt{2}}$$

If Hadamard Gate operates on $|1\rangle$, we get

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix} = 0\frac{|0\rangle+|1\rangle}{\sqrt{2}} + 1\frac{|0\rangle-|1\rangle}{\sqrt{2}} = \frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$$

Following are the figure and truth table for Hadamard gate



Input	Output
$\|0\rangle$	$\frac{(\|0\rangle + \|1\rangle)}{\sqrt{2}}$
$\|1\rangle$	$\frac{\|0\rangle - \|1\rangle}{\sqrt{2}}$

Phase Gate (or S Gate):

The S or phase gate is defined as

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

The effect of phase gate on $|0\rangle$

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

Hence the output is $|0\rangle$

The effect of phase gate on $|1\rangle$

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

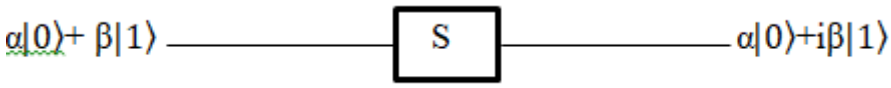
Hence the output is $i|1\rangle$

The S or phase gate transforms the state $\alpha|0\rangle + \beta|1\rangle$ as

$$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ i\beta \end{bmatrix}$$

To the state $\alpha|0\rangle + i\beta|1\rangle$

Following are the figure and truth table for S or phase gate



Input	Output
$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$i\|1\rangle$
$\alpha\|0\rangle + \beta\|1\rangle$	$\alpha\|0\rangle + i\ \beta\|1\rangle$

T Gate:

The T Gate is defined as

$$T = \begin{bmatrix} 1 & 0 \\ 0 & exp(\frac{i\pi}{4}) \end{bmatrix}$$

If the input is $|0\rangle$, then the output is

$$\begin{bmatrix} 1 & 0 \\ 0 & exp(\frac{i\pi}{4}) \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

i.e the state is $|0\rangle$,

If the input is $|1\rangle$, then the output is

$$\begin{bmatrix} 1 & 0 \\ 0 & exp(\frac{i\pi}{4}) \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ \exp(\frac{i\pi}{4}) \end{bmatrix}$$

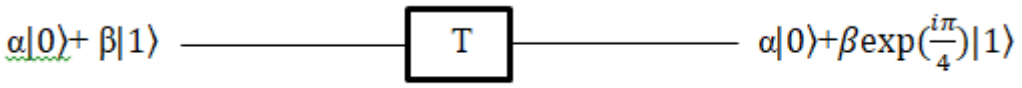
i.e the state is $exp(\frac{i\pi}{4})\ |1\rangle$,

It transforms the state $\alpha|0\rangle + \beta|1\rangle$ as

$$\begin{bmatrix} 1 & 0 \\ 0 & exp(\frac{i\pi}{4}) \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta\exp(\frac{i\pi}{4}) \end{bmatrix}$$

to $\alpha|0\rangle + \beta\exp(\frac{i\pi}{4})|1\rangle$

The following are the truth table and figure for a *T* Gate



Input	Output
$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$\exp(\frac{i\pi}{4})\|1\rangle$
$\alpha\|0\rangle + \beta\|1\rangle$	$\alpha\|0\rangle + \beta\exp(\frac{i\pi}{4})\|1\rangle$

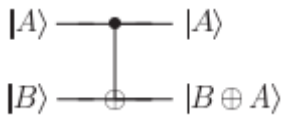
Multiple Qubit Gates:

Controlled gate:

A controlled gate is one in which the operation is of the kind "If *A* is true then *B* is also true". *A* is usually referred to as control qubit and *B* is the target qubit. If the control qubit is 0, then the target qubit is not altered. If the control qubit is 1, then the target qubit is transformed (inverted). However, the control qubit remains unaltered in both cases.

Controlled NOT (CNOT Gate):

The circuit of CNOT Gate control qubit *A* and target qubit *B* is shown below



where $\oplus$ is modulo 2 addition (Modulo 2 addition/subtraction is performed using an XOR gate in classical computing. For ex: 0 ± 0 = 0; 0 ± 1 = 1; 1 ± 0 = 1; 1 ± 1 = 0)

This kind of Gate has two input qubits:

(a) Control qubit: It is shown by the top line in the figure
(b) Target qubit: It is shown by the bottom line in the figure

For input state $|00\rangle$ (control qubit = 0 and target qubit = 0): Both the bits remain unaltered and hence the output state becomes $|00\rangle$, which is same as input state.

For input state $|01\rangle$ (control qubit = 0 and target qubit = 1): Both the bits remain unaltered and hence the output state becomes $|01\rangle$, which is same as input state.

For input state $|10\rangle$ (control qubit = 1 and target qubit = 0): The target qubit is flipped to 1. Therefore the output state becomes $|11\rangle$

For input state $|11\rangle$ (control qubit = 1 and target qubit = 1): The target qubit is flipped to 0. Therefore the output state becomes $|10\rangle$.

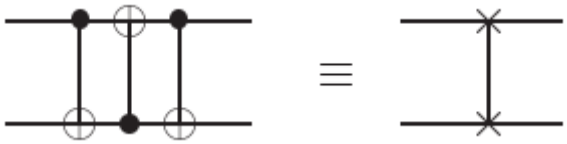
Truth table for CNOT Gate

Input	Output
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$

In general, $|A, B\rangle \longrightarrow \quad |A, B \oplus A\rangle$

Swap Gate:

A Swap Gate is a quantum circuit which contains three quantum Gates



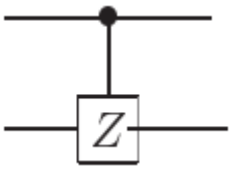
In a Swap Gate the output of the first CNOT Gate is fed as input to the second Gate and this result is fed to the third Gate. Therefore two qubits are swapped in the final output.

In general, $|A, B\rangle \longrightarrow |B, A\rangle$

Truth table for Swap Gate

Input	Output
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|10\rangle$
$\|10\rangle$	$\|01\rangle$
$\|11\rangle$	$\|11\rangle$

Controlled -Z gate:

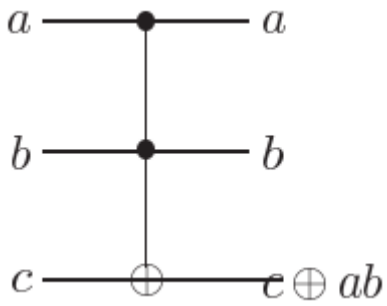


Truth table for Controlled -Z gate

Input	Output
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|10\rangle$
$\|11\rangle$	$-\|11\rangle$

Toffoli Gate:

It is a reversible Gate having three inputs (a, b, c) and three output bits (a', b' c'). The first two bits are control bits which remain unaffected by the action of Toffoli Gate. The third is the target bit which is inverted if both the control bits are 1; else it does not change. The quantum Taffolli Gate can be used to simulate irreversible classical logical Gates and ensures that they are capable of doing any computation.



Truth table for Toffoli Gate

Input			**Output**		
a	***b***	***c***	***a'***	***b'***	***c'***
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

NOTE:

While the basic unit of information in quantum computation is the qubit, the arena in which quantum computation takes place is a mathematical abstraction called a vector space. It turns out that quantum states behave mathematically in an analogous way to physical vectors—hence the term vector space. This type of space is one that shares most basic properties that vectors have with physical vectors— for example, a length.