Module-4

Quantum Computing

Introduction

Quantum computing is a rapidly-emerging field focused on the development of computer technologies centered on the principles of Quantum Physics. Quantum Physics explains the nature and behaviour of energy and matter on the quantum (atomic and subatomic) scale. Elementary particles such as protons, neutrons and electrons can exist in two or more states at a time. This fundamental behaviour is utilized in designing the quantum computation processing units and in fact it is more efficient than classical computation

Quantum computing uses a combination of bits to perform specific computational tasks with greater efficiency than their classical counterparts. Even though quantum computers are not going to replace classical computers, quantum technology is significantly changing the way the world operates. The quantum computer gains much of its processing power through the ability for bits to be in multiple states simultaneously. They can perform tasks using a combination of 1's, 0's and both 1 and 0 at a time

Brief History

In 1981, Paul Benioff at Argonne National Labs came up with the idea of a computer that operates with quantum mechanical principles. In 1984, David Deutsch of Oxford University provided the critical idea behind quantum computing research and the possibility of designing a computer that is based exclusively on quantum rules.

The Essential Elements of Quantum Theory

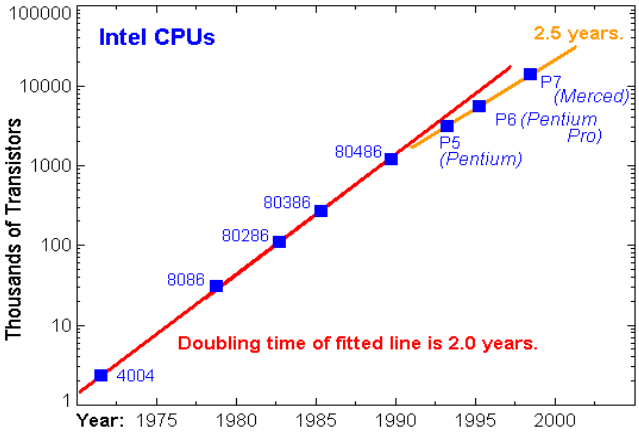
- Energy values are discrete units.
- Elementary particles may behave like particles or waves.
- The movement of elementary particles is inherently random and, thus, unpredictable.
- The simultaneous measurement of two complementary values - such as the position and momentum of a particle - is imperfect. The more precisely one value is measured, the more flawed the measurement of the other value will be.

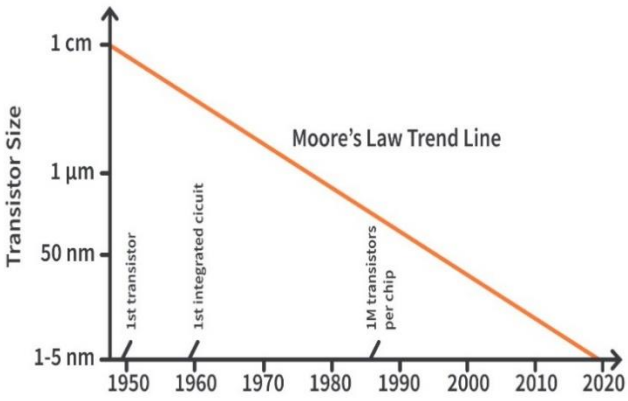
Moore's law & its end

In 1965, Gordon E. Moore—co-founder of Intel—postulated that *"the number of transistors that can be packed into a given unit of space will double about every eighteen months"*. This is also known as Moore's Law

Gordon Moore did not call his observation as "Moore's Law," nor did he set out to create a "law". Moore made this statement based on noticing emerging trends in chip manufacturing at the semiconductor industry. Eventually, Moore's insight became a prediction, which in turn became the golden rule known as Moore's Law.

Moore's Law implies that computers, machines that run on computers, and computing power all become smaller, faster, and cheaper with time, as transistors on integrated circuits become more efficient.
Here is a graphic representation for microprocessors





Impact of Moore's Law on Computing

Moore's Law has had a direct impact on the progress of computing power. What this means specifically, is that transistors in integrated circuits have become faster. Transistors conduct electricity, which contain carbon and silicon molecules that can make the electricity run faster across the circuit. The faster the integrated circuit conducts electricity, the faster the computer operates.

Is Moore's Law Coming to an End?

The electronic industry for computers grows hand-in-hand with the decrease in size of the integrated circuits. This miniaturization is necessary to increase computational power, that is, the number of floating-point operations per second (FLOPS) a computer can perform. In 1950's, electronic computers were capable of performing approximately 10^3 FLOPS while present supercomputers have a power greater than 10^{13} FLOPS. According to Moore's law, the number of transistors that may be placed on a single integrated circuit chip doubles approximately every 18 – 24 months. The present limit is approximately **10^8 transistors** per chip and the typical size of circuit components is of the order of 100 nano meters. That means, we have reached the atomic size for storing a single bit of information and quantum effects have become unavoidably dominant.

Taking all these factors into consideration, it is necessary to look for alternative ways of computing outside of the electrons and silicon transistors. One such alternative is quantum computing.

Quantum computers are based on quantum bits (qubits) and use quantum effects like *superposition* and *entanglement* to their benefit, hence overcoming the miniaturization problems of classical computing.

Comparison of Classical and Quantum Computing

Classical computing relies on principles of Boolean algebra. Data must be processed in an exclusive binary state at any point in time; either 0 (off / false) or 1 (on / true). The millions of transistors and capacitors at the heart of computers can only be in one state at any point. In addition, there is still a limit as to how quickly these devices can be made to switch states. As we progress to smaller and faster circuits, we begin to reach the physical limits of materials and the limitations for classical laws of physics to apply

The quantum computer operates with a two-mode logic gate. In a quantum computer, a number of elemental particles such as electrons or photons can be used. Each particle is given a charge or polarization, acting as a representation of 0 and/or 1. Each particle is called a *quantum bit*, or *qubit*. The nature and behaviour of these particles form the basis of quantum computing. The two most relevant aspects of quantum physics are the principles of superposition and entanglement.

Differences between classical and quantum computing

Comparison key	Classical computer	Quantum computer
Basis of computing	Large scale multipurpose computer based on classical physics	High speed computer based on quantum mechanics
Information storage	Bit-based information storage using voltage/charge	Quantum bit-based information storage using electron spin or polarization
Bit values	Bits having a value of either 0 or 1 can have a single value at any instant	Qubits have a value of 0, 1 or sometimes linear combination of both, (a property known as superposition)
Number of possible states	The number of possible states is 2 which is either 0 or 1	The number of possible states is infinite since it can hold combinations of 0 or 1 along with some complex information
Output	Deterministic (repetition of computation on the same input gives the same output)	Probabilistic (repetition of computation on superposed states gives probabilistic answer)
Gates used for processing	Logic gates (AND, OR, NOT, etc.)	Quantum gates (X, Y, Z, H, CNOT etc.)
Operations	Operations use Boolean Algebra	Operations use linear algebra and are represented with unitary matrices
Circuit implementation	Circuit implemented in macroscopic technologies (e.g. CMOS) that are fast and scalable	Circuits implemented in microscopic technologies (e.g. nuclear magnetic resonance) that are slow and delicate

Concept of qubit and its properties

From bits to qubit

Bit: A digital computer stores and processes information using bits, which can be either 0 or 1. Physically, a bit can be anything that has two distinct configurations: one represented by "0", and the other represented by "1". It could be a light bulb that is on or off, a coin that is heads or tails, or any other system with two distinct and distinguishable possibilities. In modern computing and communications, bits are represented by the absence or presence of an electrical signal, encoding "0" and "1" respectively

Qubit is the physical carrier of quantum information. It is the quantum version of a bit, and its quantum state can be written in terms of two levels, labelled $|0\rangle$ and $|1\rangle$. $|\ \rangle$ this notation is known as 'ket' notation and $\langle\ |$ is known as 'brac' notation. Both are together called as **Dirac notations** 'Ket' is analogous to a column vector.
They are also called basis vectors and represented by two-dimensional column vectors as follows

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

The qubit can be in any one of the two states as well as in the superposed state simultaneously

In quantum computation two distinguishable states of a system are needed to represent a bit of data. For example, two states of an electron orbiting a single atom is shown in the following figure. Spin up is taken as $|1\rangle$ and spin down is taken as $|0\rangle$. Similarly ground state energy level is $|0\rangle$ and excited state level is $|1\rangle$

Qubit represented by two electronic levels in an atom

This is the abstract notion of a qubit. The quantum computers actually use a physical type of qubit called a *superconducting qubit* is made from superconducting materials (of course, there are other approaches also to build the qubits)

NOTE:
In quantum computing the vectors are members of complex vector space[#]. Each member of this space is represented as column vector of n dimensions with single 1 at the location corresponding to a particular basis vector.
It is as follows

$$|0\rangle = \begin{bmatrix}1\\0\\0\\\cdot\\\cdot\\0\end{bmatrix} \quad |1\rangle = \begin{bmatrix}0\\1\\0\\\cdot\\\cdot\\0\end{bmatrix} \quad |2\rangle = \begin{bmatrix}0\\0\\1\\\cdot\\\cdot\\0\end{bmatrix} \ldots\ldots \quad |N-1\rangle = \begin{bmatrix}0\\0\\0\\\cdot\\\cdot\\1\end{bmatrix}$$

[#] Complex vector space is a vector space which contains complex numbers

Here we use only two dimensions (or only two sets). Hence we write as

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

Superposition of two states

The difference between qubits and classical bits is that a qubit can be in a linear combination (superposition) of the two states $|0\rangle$ and $|1\rangle$. For ex, if $\propto$ and β are the probability amplitudes of electron in ground state (ie, in $|0\rangle$ state) and in excited state (ie, in $|1\rangle$ state) then the linear combination of two states is

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

The numbers α and β are complex but due to normalization conditions

$$|\propto|^2 + |\beta|^2 = 1.$$

Here $|\propto|^2$is the probability of finding $|\psi\rangle$ in state $|0\rangle$ and $|\beta|^2$is the probability of finding $|\psi\rangle$ in state $|1\rangle$. So, we have to keep in mind that when a qubit is measured, it only gives either '0' or '1' as the measurement result – probabilistically

Consider the following example of qubit representation

$$|\Psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$
$$\therefore \propto = \frac{1}{\sqrt{2}} \; and \;\; \beta = \frac{1}{\sqrt{2}}$$
$$|\propto|^2 = |\beta|^2 = \frac{1}{2}$$

This means that with 50% probability the qubit will be found in $|0\rangle$ state as well as in $|1\rangle$ state. The superposed states are also called as **space states** where as $|0\rangle$ and $|1\rangle$ are called **basis states**.

Properties of qubits

1. Qubits make use of discrete energy state particles such as electrons and photons
2. Qubits exists in two quantum state $|0\rangle$ and $|1\rangle$ or in a linear combination of both states. This is known as superposition. This property allows for *exponentially many logical states* at once (and no classical computer can achieve it)
3. Unlike classical bits, qubit can work with the overlap of both 0 & 1 states. For ex, a 4-bit register[1] can store one number from 0 to 15 (because of $2^n = 2^4$=16), but 4-qubit register can store all 16 numbers
4. When the qubit is measured, it collapses to one of the two basis states $|0\rangle$ or $|1\rangle$
5. Quantum entanglement and quantum tunnelling are two exclusive properties of qubit
6. State of the qubits is represented using Bloch sphere

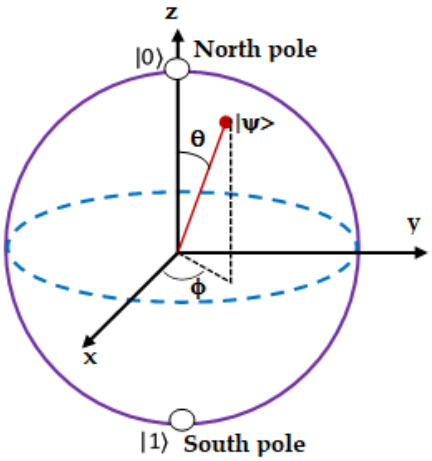
[1] Register – is a group of flip-flops. Its basic function is to hold information within a digital system so as to make it available to the logic units during the computing process. However, a register may also have additional capabilities associated with it.

After studying the physics of qubits it is now time to look at the mathematics of qubits. Let us start with the representation of qubit using Bloch sphere in a vector space. Later on we proceed towards single qubit, multi qubit, tensor operation, operators and matrix representation

NOTE: Vector space is a set of elements (or vectors) which are added together or multiplied by real numbers. Addition of two vectors or multiplication of a vector by a scalar is satisfied here. It should not be confused with vector field

Bloch sphere

Bloch sphere is an imaginary sphere which is used to represent pure single-qubit states as a point on its surface. It has unit radius. Its North Pole and South Pole are selected to represent the basis states namely $|0\rangle$ and $|1\rangle$. North Pole represents $|0\rangle$ (say spin up↑) and South Pole represents $|1\rangle$ (say spin down ↓). All other points on the sphere represent superposed states (ie, state space). Bloch sphere allows the state of a qubit to be represented in spherical coordinates (ie, r, θ and ϕ). It is as follows



The state qubit $|\psi\rangle$ on the Bloch sphere makes an angle θ with z-axis and its projection (azimuth) makes angle ϕ with x-axis as shown. It is clear from the fig that $0 < \theta < \pi$ and $0 < \phi < 2\pi$. $|\psi\rangle$ is represented as

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

It can be proved that

$$|\Psi\rangle = cos\frac{\theta}{2}|0\rangle + e^{i\phi}sin\frac{\theta}{2}|1\rangle - - - (1)$$

Using this equation we can represent $|\psi\rangle$ for different θ and ϕ as follows

Case-1: let $\theta = 0$ and $\phi = 0$, then eq (1) becomes

$$|\Psi\rangle = cos\ 0|0\rangle + e^{i0}sin0|1\rangle = |0\rangle + 0$$
$$\therefore |\Psi\rangle = |0\rangle$$

Case-2: let $\theta = \pi$ and $\phi = 0$, then eq (1) becomes

$$|\Psi\rangle = cos\ \frac{\pi}{2}|0\rangle + e^{i0}sin\frac{\pi}{2}|1\rangle = 0 + |1\rangle$$

$$\therefore |\Psi\rangle = |1\rangle$$

Case-3: let θ = π/2 and ϕ = 0, then eq (1) becomes

$$|\Psi\rangle = cos\ \frac{\pi}{4}|0\rangle + e^{i0} sin\frac{\pi}{4}|1\rangle$$

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

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

Case-4: let θ = π/2 and ϕ = π, then eq (1) becomes

$$|\Psi\rangle = cos\ \frac{\pi}{4}|0\rangle + e^{i\pi} sin\frac{\pi}{4}|1\rangle$$

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

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

In the above discussion we have represented only single qubit state. Bloch sphere is a nice visualization of single qubit states.

Multiple Qubits

Single qubits are interesting, but individually they offer no computational advantage. We will now look at how to represent multiple qubits, and how these qubits can interact with each other.

Two qubits

Consider two qubits. They can be in any one of four possible states represented as |00⟩, |01⟩, |10⟩ and |11⟩. The interaction among these qubits is described by creating a new vector space[2] using a special kind of operation called *tensor product* or *Kronecker product*. It is as follows

Let U and V are two 2-d vectors given as

$$U = \begin{bmatrix} x_1 \\ y_1 \end{bmatrix}, V = \begin{bmatrix} x_2 \\ y_2 \end{bmatrix}$$

Their tensor product is

$$U \otimes V = \begin{bmatrix} x_1 \begin{bmatrix} x_2 \\ y_2 \end{bmatrix} \\ y_1 \begin{bmatrix} x_2 \\ y_2 \end{bmatrix} \end{bmatrix}$$

[2] Vector space is a set of elements (or vectors) which are added together or multiplied by real numbers or scalars. Addition of two vectors or multiplication of a vector by a scalar is satisfied here. It should not be confused with vector field

$$U \otimes V = \begin{bmatrix} x_1x_2 \\ x_1y_2 \\ y_1x_2 \\ y_1y_2 \end{bmatrix}$$

Based on this we can write |00⟩ as follows

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

Sometimes we avoid the symbol ⊗ and write directly as

$$|00\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}$$

Similarly

$$|01\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix} \quad |10\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix} \text{ and } |11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

The state qubit is (ie, linear combination of these four)

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

For 2 qubit system we have 4 complex amplitudes namely α_{00}, α_{01}, α_{10} and α_{11}. According to normalization condition

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

Similarly if there are 3 qubits there will be 8 complex amplitudes and in general for *n* qubits we will have 2^n complex amplitudes. This means that a basis state is represented by a number 0 to 2^{n-1}. The superposition state is represented as

$$|\Psi\rangle = \sum_{x=0}^{2^{n-1}} \propto_x |x\rangle$$

Qubit has two quantum states similar to the classical binary states. The qubit can be in any one of the two states as well as in the superposed state simultaneously.

Dirac representation and Matrix operations

Matrix representation of 0 and 1 states

In Quantum mechanics, Brac-Ket notation is a standard notation for describing quantum states. The notation | ⟩ is known as 'ket' notation and ⟨ | is known as 'brac' notation. Both are together called as **Dirac notations.**

The ‘ket’ vector typically represented as a column vector and ‘brac’ vector typically represented as a row vector as follows

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \qquad |1\rangle = \begin{bmatrix}0\\1\end{bmatrix} - - - - - - \text{ket notations}$$

$$\langle 0| = [1 \quad 0] \qquad \langle 1| = [0 \quad 1] - - - - - \text{ brac notations}$$

Hence, any arbitrary state can be represented as

$$|\psi> = \begin{bmatrix}\alpha\\\beta\end{bmatrix} \quad or \quad |\psi\rangle \; = \; \alpha\,|0\rangle \; + \beta\,|1\rangle$$

Some of the properties of these notations are

i. Addition of two kets gives another ket (commutative)

$$|\mathrm{A}\rangle + |B\rangle = |C\rangle = |B\rangle + |A\rangle$$

ii. Addition of kets obeys associative property

$$|\mathrm{A}\rangle + (|B\rangle + |C\rangle) = (|A\rangle + |B\rangle) + |C\rangle$$

iii. If c_1 and c_2 are scalars or a complex numbers and |A ⟩ is a ket then

$$(c_1 + c_2)|A\rangle = c_1|A\rangle + c_2|A\rangle$$

iv. In a complex vector space for every ket there is unique brac. Brac is the Hermitian[#] conjugate of the ket.

$$\text{If } |A\rangle = \begin{bmatrix}A_1\\A_2\end{bmatrix} \text{ then } \langle A| = [A_1^* \quad A_2^*]$$

v. Bracs are useful in calculating probability amplitudes.
For ex, the probability amplitude of |1⟩ is β which can be calculated as follows

$$\langle 1||\Psi\rangle = \langle 1|\alpha\,|0\rangle \; + \langle 1|\beta\,|1\rangle$$
$$\langle 1||\Psi\rangle = \alpha\langle 1|\,|0\rangle \; + \beta\,\langle 1||1\rangle$$
$$\langle 1||\Psi\rangle = \alpha[0 \quad 1]\begin{bmatrix}1\\0\end{bmatrix} + \beta[0 \quad 1]\begin{bmatrix}0\\1\end{bmatrix}$$
$$\langle 1|\Psi\rangle = \alpha \times 0 + \beta \times 1$$
$$\langle 1|\Psi\rangle = \beta$$

Similarly

$$\langle 0|\Psi\rangle = \alpha$$

vi. If ⟨U| and ⟨V| are two bracs then

[#] Will be discussed later

$$\langle U| + \langle V| = \langle U + V|$$

Operators and matrices

An operator is a mathematical rule that transform a given function into another function.
Ex:

i. $\sqrt{4} = 2$. Here $\sqrt{}$ is a square root operator. It transforms 4 to 2
ii. $D = \frac{d}{dx}$ is a differentiate operator. It transforms $2x^3$ to $6x^2$

Similar to this we have the following example. In this case operator 'A' transforms the vector $|a\rangle$ to another vector $|b\rangle$

$$\hat{A}\ |a\rangle\ =\ |b\rangle$$

There are different types of operators like Linear operator, Identity operator, Null operator, Inverse operator, Singular & non-singular operator etc.

Identity operator 'I'

The identity operator is an operator which, operating on a function, leaves the function unchanged i.e.

$$I\ |a\rangle\ =\ |a\rangle$$

It is given in matrix form by

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

This is also called as identity matrix. There will be no change when I operates on either $|0\rangle$ state or $|1\rangle$ state. It is explained as follows

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

$$\therefore I\ |0\rangle\ =\ |0\rangle$$

Similarly

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

$$\therefore I\ |1\rangle\ =\ |1\rangle$$

Identity matrix acts as number 1. It is always a square matrix.

Conjugate matrices

If the elements in a matrix A are complex numbers, then the matrix obtained by the corresponding conjugate complex elements is called the **conjugate** of A and is denoted by A^*. For ex

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

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

$$\text{If } A = \begin{bmatrix} 1 & 2i \\ 4i+1 & 0 \end{bmatrix} \text{ then } A^* = \begin{bmatrix} 1 & -2i \\ -4i+1 & 0 \end{bmatrix}$$

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

Transpose matrices

If columns and rows of a matrix A are interchanged then the resultant matrix is **transpose** of A and represented as A^T. For ex,

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

$$\text{If } A = \begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix} \text{ then } A^T = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}$$

$$\text{If } A = \begin{bmatrix} 1 & 2i \\ 4i+1 & 0 \end{bmatrix} \text{ then } A^T = \begin{bmatrix} 1 & 4i+1 \\ 2i & 0 \end{bmatrix}$$

Hermitian matrices

The transpose of complex conjugate of a matrix is known as Hermitian operator (also called as adjoint operator) and the resultant matrix is known as **Hermitian matrix.** It is represented by $A^\dagger$

Let A be a matrix, A^* be its complex conjugate and A^{*T} is its transpose then its **Hermitian** matrix is

$$A^\dagger = A^{*T}$$

Ex:

$$\text{If } A = \begin{bmatrix} 1 & 2i \\ 4i+1 & 0 \end{bmatrix} \text{ then } A^* = \begin{bmatrix} 1 & -2i \\ -4i+1 & 0 \end{bmatrix}$$

$$A^\dagger = \begin{bmatrix} 1 & -4i+1 \\ -2i & 0 \end{bmatrix}$$

Unitary matrices

Matrix A is said to be unitary if it produces an identity matrix *I* when multiplied by its conjugate transpose

$$AA^\dagger = I$$

In other words, A is a unitary matrix if its conjugate transpose is equal to its reciprocal, ie

$$A^\dagger = \frac{I}{A} = \frac{1}{A} = A^{-1}$$

we can show that $A = \frac{1}{2}\begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix}$ is a unitary matrix

Inner product

Introduction

Let $U = x_1 i + y_1 j + z_1 k$ and $V = x_2 i + y_2 j + z_2 k$ be the two vectors in real space then their dot product is

$$U.V = x_1 x_2 + y_1 y_2 + z_1 z_2$$

If U = V then

$$U.U = |U|^2 = x_1^2 + x_2^2 + x_3^2$$

The length of the resultant vector is $|U| = \sqrt{U.U} = \sqrt{x_1^2 + y_1^2 + z_1^2}$

In matrix form U and V are written as

$$U = \begin{bmatrix} x_1 \\ y_1 \\ z_1 \end{bmatrix} \text{ and V} = \begin{bmatrix} x_2 \\ y_2 \\ z_2 \end{bmatrix}$$

And the dot product is written as

$$U.V = [x_1 y_1 z_1] \begin{bmatrix} x_2 \\ y_2 \\ z_2 \end{bmatrix} = U^T V$$

This dot product is also called as *inner product.* In real space inner product is same as dot product of two vectors and it finally gives a scalar quantity.

In quantum computing the vectors are the members of *complex space* and the *inner product* gives a complex number

Definition of inner product

The inner product of two vectors U and V in the complex space is a function that takes U and V as inputs and produces a complex number as output

In terms of Dirac notation, the inner product is given as

$$\langle U|V\rangle = c$$

Let $|U\rangle = \begin{bmatrix} x_1 \\ y_1 \end{bmatrix}$ and $|V\rangle = \begin{bmatrix} x_2 \\ y_2 \end{bmatrix}$ be the two vectors. Their inner product is written as $\langle U|V\rangle$

But $\langle U|$ is equal to conjugate transpose of $|U\rangle$

$$ie, \langle U| = |U^*\rangle^{-1} = |U\rangle^{\dagger} = [x_1^* \quad y_1^*]$$

$$\therefore \langle U|V\rangle = [x_1^* \quad y_1^*] \begin{bmatrix} x_2 \\ y_2 \end{bmatrix} = x_1^* x_2 + y_1^* y_2$$

The square root of the inner product of a vector with itself is also called as ***norm*** **o**r the *length* of the vector. It is given by

$$|U| = \sqrt{\langle U|U\rangle}$$

Ex: Find the inner product of $|\boldsymbol{U}\rangle = \begin{bmatrix} \boldsymbol{3+i} \\ \boldsymbol{4-i} \end{bmatrix}$ **and** $|\boldsymbol{V}\rangle = \begin{bmatrix} \boldsymbol{3i} \\ \boldsymbol{4} \end{bmatrix}$

First we shall find the conjugate transpose of $|U\rangle$

$$|U^*\rangle = \begin{bmatrix} 3-i \\ 4+i \end{bmatrix}$$

$$|U\rangle^\dagger = [3-i \quad 4+i]$$

$$\therefore \langle U| = |U\rangle^\dagger = [3-i \quad 4+i]$$

$$\langle U|V\rangle = [3-i \quad 4+i]\begin{bmatrix} 3i \\ 4 \end{bmatrix}$$

$$\langle U|V\rangle = (3-i)\times 3i + (4+i)\times 4$$

$$\langle U|V\rangle = 9i + 3 + 16 + 4i$$

$$\langle U|V\rangle = 13i + 19$$

Ex: Find the inner product of $|\boldsymbol{A}\rangle = \begin{bmatrix} \boldsymbol{a} \\ \boldsymbol{ib} \end{bmatrix}$ ***with itself***

First we shall find the conjugate transpose of |A⟩

$$|A^*\rangle = \begin{bmatrix} a \\ -ib \end{bmatrix}$$

$$|U\rangle^\dagger = [a \quad -ib]$$

$$\therefore \langle A| = [a \quad -ib]$$

$$\langle A|A\rangle = [a \quad -ib]\begin{bmatrix} a \\ ib \end{bmatrix}$$

$$\langle A|A\rangle = a^2 + (-ib)(ib)$$

$$\langle A|A\rangle = a^2 + b^2$$

Ex: find the norm of $|\boldsymbol{U}\rangle = \begin{bmatrix} \boldsymbol{1-i} \\ \boldsymbol{2} \end{bmatrix}$

$$|U| = \sqrt{\langle U|U\rangle}$$

$$|U| = \sqrt{[1+i \quad 2]\begin{bmatrix} 1-i \\ 2 \end{bmatrix}}$$

$$|U| = \sqrt{(1+i)(1-i) + 2\times 2} = \sqrt{1+1+4} = \sqrt{6}$$

Orthogonality

If the inner product of two vectors is equal to 0 then they are said to be ***orthogonal*** *(or perpendicular)* to each other

If $\langle U|V\rangle = 0$ then $|U\rangle$ and $|V\rangle$ are perpendicular.

Consider,

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

Then

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

Hence $|0\rangle$ is perpendicular to $|1\rangle$

The most important property of the inner product of a vector with itself is equal to one

$$\text{ie, } \langle\psi|\psi\rangle = 1$$

This is known as normalization condition. The physical significance of normalization is that the "probability amplitude" of the quantum system is1

Orthonormality

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*** (ortho + normalization = orthonormalization)

Consider the set

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

$\langle 0|0\rangle = \begin{bmatrix}1 & 0\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = 1 + 0 = 1$ normalized

$\langle 0|1\rangle = \begin{bmatrix}1 & 0\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = 0 + 0 = 0$ orthogonal

$\langle 1|1\rangle = \begin{bmatrix}0 & 1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = 0 + 1 = 1$ normalized

$\langle 1|0\rangle = \begin{bmatrix}0 & 1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = 0 + 0 = 0$ orthogonal

Hence set of $|0\rangle$ and $|1\rangle$ is orthonormal

Pauli Matrices

These are the 2 × 2 complex matrices introduced by Pauli in order to account for the interaction of the spin with an external electromagnetic field. They are given by

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

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

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

NOTE: X, Y and Z are also called as X – gate, Y- gate and Z- gate

Properties of Pauli matrices

The most important property of Pauli matrices is that square of all the three matrices gives an identity matrix I. For ex,

$$\sigma_1^2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\therefore \sigma_1^2 = I$$

In general

$$\sigma\sigma^\dagger = 1$$

$$\sigma^\dagger = \frac{1}{\sigma} = \sigma^{-1}$$

So, they are unitary

Another property of Pauli matrices is that they are Hermitian. Let A be a matrix, A^* be its complex conjugate and $A^\dagger$ [3] is its transpose. If A = $A^\dagger$then the matrix is Hermitian. For ex,

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

$${\sigma_2}^* = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}$$

$${\sigma_2}^\dagger = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$\therefore {\sigma_2}^\dagger = \sigma_2$$

Operation of Pauli Matrices on 0 and 1 states

Three Pauli matrices X, Y and Z act on basis states $|0\rangle$ and $|1\rangle$ as follows

i. X operating on $|0\rangle$ and $|1\rangle$

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

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

Since X inverts each input (ie, $|0\rangle$ becomes $|1\rangle$ and $|1\rangle$ becomes$|0\rangle$) it is also called as *bit-flip* gate
If a superposed qubit goes through X gate, the result will be

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

So,

$$X|\Psi\rangle = \alpha|1\rangle + \beta|0\rangle$$

[3] Transpose means convert rows into column and columns into row

ii. Y operating on $|0\rangle$ and $|1\rangle$

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

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

So,

$$Y|0\rangle = i|1\rangle$$

Similarly

$$Y|1\rangle = -i|0\rangle$$

If a superposed qubit goes through Y gate, the result will be

$$Y|\Psi\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} 0\times\alpha + (-i)\times\beta \\ i\times\alpha + 0\times\beta \end{bmatrix} = \begin{bmatrix} -i\beta \\ i\alpha \end{bmatrix} = -i\beta|0\rangle + i\alpha|1\rangle$$

So,

$$Y|\Psi\rangle = i\alpha|1\rangle - i\beta|0\rangle$$

iii. Z operating on $|0\rangle$ and $|1\rangle$

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

$$Z|1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1\times 0 + 0\times 1 \\ 0\times 0 + (-1)\times 1 \end{bmatrix} = \begin{bmatrix} 0+0 \\ 0-0 \end{bmatrix} = \begin{bmatrix} 0 \\ -1 \end{bmatrix} = -\begin{bmatrix} 0 \\ 11 \end{bmatrix} = -|1\rangle$$

So,

$$Z|0\rangle = |0\rangle$$

$$Z|1\rangle = -|1\rangle$$

If a superposed qubit goes through Z gate, the result will be

$$Z|\Psi\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} 1\times\alpha + 0\times\beta \\ 0\times\alpha + (-1)\times\beta \end{bmatrix} = \begin{bmatrix} \alpha \\ -\beta \end{bmatrix} = \alpha|0\rangle - \beta|1\rangle$$

So,

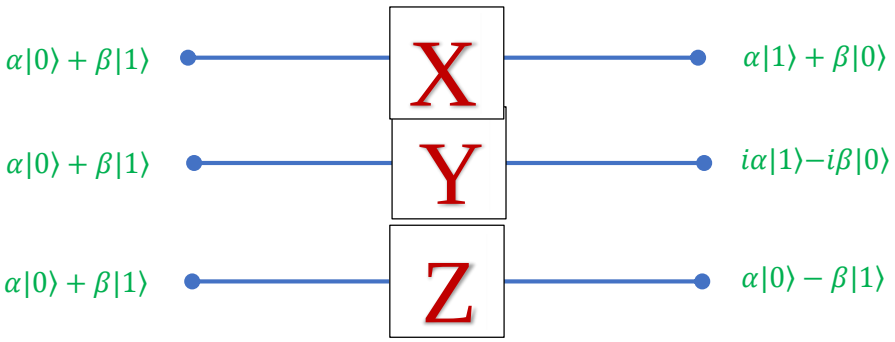
$$Z|\Psi\rangle = \alpha|0\rangle - \beta|1\rangle$$

This is also called *phase-flip* gate

The truth tables for X, Y and Z gates are as follows

X- gate		**Y-gate**		**Z-gate**	
Input	**Output**	**Input**	**Output**	**Input**	**Output**
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$i\|1\rangle$	$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$-i\|0\rangle$	$\|1\rangle$	$-\|1\rangle$
$\alpha\|0\rangle + \beta\|1\rangle$	$\alpha\|1\rangle + \beta\|0\rangle$	$\alpha\|0\rangle + \beta\|1\rangle$	$i\alpha\|1\rangle - i\beta\|0\rangle$	$\alpha\|0\rangle + \beta\|1\rangle$	$\alpha\|0\rangle - \beta\|1\rangle$

Symbolically these gates are represented as follows



Limitation of Pauli matrices or Pauli gates

Using only the Pauli-gates it is impossible to move our initialized qubit to any state other than $|0\rangle$ or $|1\rangle$, i.e. we cannot achieve superposition. This means we can see no behaviour different to that of a classical bit. To create more interesting states we need more gates

Quantum Gates

In classical computers gates are a small set of circuit elements that are used to implement the combination of binary variables 0's and 1's. Most commonly known gates are AND gate, OR gate and NOT gate.

A ***quantum gate***, a counterpart of classical gate, is a very simple computing device that performs quantum operation on qubits. Quantum gates are one of the essential parts of a quantum computer and are the building blocks of all quantum algorithms.

Quantum gates are mathematically represented as transformation matrices that are *unitary* and the operations performed by these gates are *reversible*. Each unitary transformation U has inverse transformation $U^\dagger$ so that

$$UU^\dagger = I$$
$$U^\dagger = \frac{I}{U} = \frac{1}{U} = U^{-1}$$

Now, the basic question is that *why quantum gates shall be unitary in nature*? It can be explained as follows
A fundamental property of qubits is that they are restricted by the normalization condition, i.e. sum of amplitudes square is equal 1.

$$ie, |\propto|^2 + |\beta|^2 = 1$$

Quantum gates operate on set of qubits and transform them to another quantum state. These operations must preserve the normalization throughout the whole process. The only possible operation for this purpose is unitary matrices. Hence the quantum gates are inevitably *unitary*

Another important feature of quantum gate is that they are *always reversible*. The outputs can be calculated from inputs and inputs can be retrieved from outputs. This is because all unitary matrices are reversible as explained earlier

Note:

1. If the product of a number and its reciprocal is equal to 1, then the number is reversible. For ex

$$2 \times \frac{1}{2} = 1$$

There are different types of quantum gates. *Single-qubit gates* can flip a qubit from 0 to 1 as well as allowing superposition states to be created. *Two-qubit gates* allow the qubits to interact with each other and can be used to create **quantum entanglement** (a strange phenomenon that can't be explained by classical physics).

Some of the important single qubit gates are discussed here. They all are represented by 2 × 2 matrix. (Note that X, Y and Z gates are already discussed earlier under the heading Pauli's matrices. So, it is a sort of repetition)

Single qubit gates

1. X – Gate

This is also called as Pauli X – gate. It is given by

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

When X operates on $|0\rangle$ and $|1\rangle$ the output will be inverted (ie, $|0\rangle$ becomes $|1\rangle$ and $|1\rangle$ becomes$|0\rangle$)

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

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

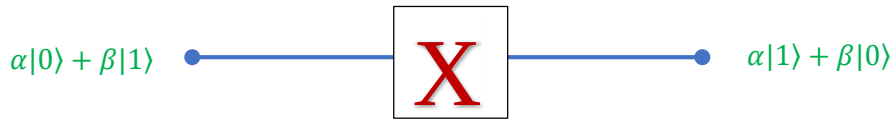
Since X inverts each input it is also called as *bit-flip* gate. If a superposed qubit goes through X gate, the result will be

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

So,

$$X|\Psi\rangle = \alpha|1\rangle + \beta|0\rangle$$

Symbolically these gates are represented as follows



2. Y – Gate

This is also called as Pauli Y – gate. It is given by

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

When Y operates on $|0\rangle$ and $|1\rangle$

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

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

So,

$$Y|0\rangle = i|1\rangle \text{ and } \qquad Y|1\rangle = -i|0\rangle$$

If a superposed qubit goes through Y gate, the result will be

$$Y|\Psi\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} 0\times \alpha + (-i)\times \beta \\ i\times \alpha + 0\times \beta \end{bmatrix} = \begin{bmatrix} -i\beta \\ i\alpha \end{bmatrix} = -i\beta|0\rangle + i\alpha|1\rangle$$

So,

$$Y|\Psi\rangle = i\alpha|1\rangle - i\beta|0\rangle$$

Symbolically these gates are represented as follows

3. Z – Gate

This is also called as Pauli Z – gate. It is given by

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

When Z operates on $|0\rangle$ and $|1\rangle$ the phase will change. Hence this is also called as *phase-flip* gate

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

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

So,

$$Z|0\rangle = |0\rangle \text{ and } Z|1\rangle = -|1\rangle$$

If a superposed qubit goes through Z gate, the result will be

$$Z|\Psi\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} 1\times \alpha + 0\times \beta \\ 0\times \alpha + (-1)\times \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ -\beta \end{bmatrix} = \alpha|0\rangle - \beta|1\rangle$$

So,

$$Z|\Psi\rangle = \alpha|0\rangle - \beta|1\rangle$$

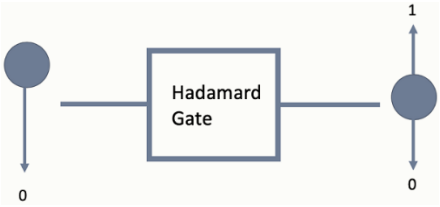
Symbolically these gates are represented as follows

The truth tables for X, Y and Z gates are as follows

X- gate		Y-gate		Z-gate	
Input	**Output**	**Input**	**Output**	**Input**	**Output**
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$i\|1\rangle$	$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$-i\|0\rangle$	$\|1\rangle$	$-\|1\rangle$
$\alpha\|0\rangle + \beta\|1\rangle$	$\alpha\|1\rangle + \beta\|0\rangle$	$\alpha\|0\rangle + \beta\|1\rangle$	$i\alpha\|1\rangle - i\beta\|0\rangle$	$\alpha\|0\rangle + \beta\|1\rangle$	$\alpha\|0\rangle - \beta\|1\rangle$

4. Hadamard Gate – The gate to superposition

The Hadamard Gate is a well-known gate that brings a qubit into a superposition state. Similar to the Pauli-X gate, the Hadamard Gate acts on a single qubit, and can be represented by a 2 x 2 matrix as follows



Hadamard gate brings a qubit in superposition

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

Let us find out what happens when Hadamard gate operates on a qubit that is in the $|0\rangle$ state.

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\times 1 + 1\times 0\\ 1\times 1 + -1\times 0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$$

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

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad ---(1)$$

Let us find out what happens when Hadamard gate operates on a qubit that is in the $|1\rangle$ state.

$$H|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{bmatrix}0\\1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\times 0 + 1\times 1\\ 1\times 0 + -1\times 1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$$

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

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

If a superposed qubit goes through H gate, the result will be

$$H|\psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{bmatrix}\alpha\\\beta\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\times\alpha + 1\times\beta\\ 1\times\alpha + -1\times\beta\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}\alpha+\beta\\\alpha-\beta\end{bmatrix}$$

$$H|\psi\rangle = \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle$$

$$H|\psi\rangle = \alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle-|1\rangle}{\sqrt{2}} - - - (3)$$

The above equations shows that, after applying the Hadamard gate to a qubit that are in $|0\rangle$ & $|1\rangle$ states enter a new superposed states. This is the major difference between X, Y, Z and H gates. In X, Y and Z gates we get only single state whereas in H gate we get superposed state.

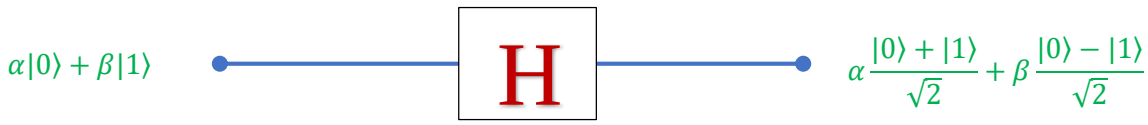
The probability of measuring 0 and 1 is

$$\left(\frac{1}{\sqrt{2}}\right)^2 + \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$$

The truth table is as follows

INPUT	OUTPUT
$\|0\rangle$	$\frac{\|0\rangle+\|1\rangle}{\sqrt{2}}$
$\|1\rangle$	$\frac{\|0\rangle-\|1\rangle}{\sqrt{2}}$
$\|\psi\rangle = \alpha\|0\rangle + \beta\|1\rangle$	$\alpha\frac{\|0\rangle+\|1\rangle}{\sqrt{2}} + \beta\frac{\|0\rangle-\|1\rangle}{\sqrt{2}}$

The circuit symbol is as follows



5. Phase Gate (S Gate)

The Phase gate or S gate is a gate that transfers $|0\rangle$ into $|0\rangle$ and $|1\rangle$ into $i|1\rangle$. It is represented as

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

If we apply S gate to a state $|0\rangle$ it will remain same

$$S|0\rangle = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1(1)+0(0) \\ 0(1)+i(0) \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$S|0\rangle = |0\rangle$$

If we apply S gate to a state $|1\rangle$ it will be transformed into $i|1\rangle$

$$S|1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1(0)+0(1) \\ 0(0)+i(1) \end{bmatrix} = \begin{bmatrix} 0 \\ i \end{bmatrix} = i\begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$S|1\rangle = i|1\rangle$$

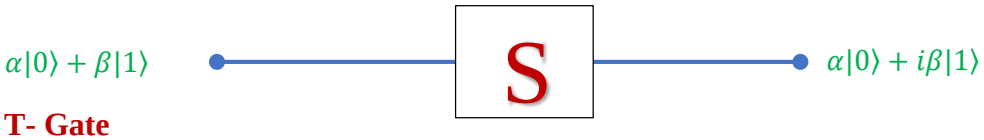
It transforms the state $\alpha|0\rangle + \beta|1\rangle$to the state $\alpha|0\rangle + i\beta|1\rangle$

$$S|\psi\rangle = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ i\beta \end{bmatrix}$$

The truth table is as follows

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

The symbol is as follows



6. T- Gate

The T-gate is a very commonly used gate and it is given by

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{bmatrix}$$

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

$$T|0\rangle = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$T|0\rangle = |0\rangle$$

If the input is $|1\rangle$ then the output state is $e^{\frac{i\pi}{4}}|1\rangle$

$$T|1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ e^{(\frac{i\pi}{4})} \end{bmatrix} = e^{\frac{i\pi}{4}} \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$T|1\rangle = e^{\frac{i\pi}{4}}|1\rangle$$

It transforms the state $\alpha|0\rangle + \beta|1\rangle$ to $\alpha|0\rangle + e^{i\pi/4}\beta|1\rangle$

$$T|\psi\rangle = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta e^{\frac{i\pi}{4}} \end{bmatrix}$$

The following figure shows quantum T- gate and the table gives the truth table.

The truth table is as follows

Input	Output
$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$e^{\frac{i\pi}{4}}\|1\rangle$
$\alpha\|0\rangle + \beta\|1\rangle$	$\alpha\|0\rangle + e^{i\pi/4}\beta\|1\rangle$

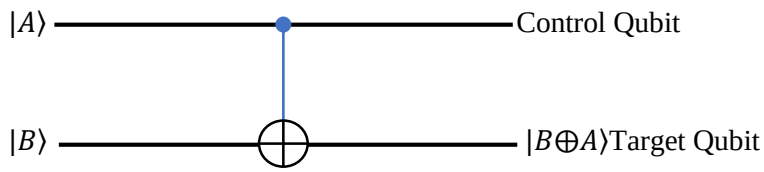
Multiple Qubit gates

As mentioned in the earlier section, Single qubits are interesting, but individually they offer less computational advantage. It is hence essential to look for multiple qubit system and the operation on them. Quantum gates operating on multiple qubits are called as *multiple qubit gates*. Some of them are as follows

1. Controlled Gate (CNOT)

The CNOT gate is a two-qubit operation, where the first qubit is referred as the ***control qubit*** (A) and the second qubit as the ***target qubit*** *(B)*. If the control qubit is $|1\rangle$ then it will flip the target qubit state from$|0\rangle$ to $|1\rangle$ or from $|1\rangle$ to $|0\rangle$. When the control qubit is in state $|0\rangle$ then the target qubit remains unchanged. In fact CNOT applies X on target whenever its control is in state $|1\rangle$

The symbolic representation is as follows. The upper line represents control qubit and bottom line represents target qubit



In the combined qubit, first term is control qubit and the second term is target qubit. For ex, in $|AB\rangle$, A is control qubit and B is target qubit

NOTE: In diagram the control qubit is represented by ● and target is represented by ⊕

Discussion for 4 different input states

1. Input state $|00\rangle$ (Control qubit = 0, Target qubit = 0): Both the bits remain unaltered. Hence, the output state is the same as the input state or $|00\rangle \rightarrow |00\rangle$
2. Input state $|01\rangle$ (Control qubit = 0, Target qubit = 1): Both the bits remain unaltered. Again, the output state is the same as the input state or $|01\rangle \rightarrow |01\rangle$
3. Input state $|10\rangle$ (Control qubit =1, Target qubit = 0): The target qubit is flipped to 1. Therefore, the output state has both qubits 1 or $|10\rangle \rightarrow |11\rangle$
4. Input state $|11\rangle$ (Control qubit =1, Target qubit = 1): The target qubit is flipped to 0. Therefore, the output state becomes $|10\rangle$ or $|11\rangle \rightarrow |10\rangle$.

The truth table of a CNOT gate is as follows

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

We know that two qubits can be in any one of four possible states represented as $|00\rangle$ $|01\rangle|10\rangle$ and $|11\rangle$. The matrix form of them are

$$|00\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix} \; |01\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix} \; |10\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix} \; |11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

The state qubit is $|\Psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$. When it is operated by CNOT we get CNOT($\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$) = $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|11\rangle + \alpha_{11}|10\rangle$

From this we can construct the matrix form of CNOT gate as follows (it is 4 ×4 matrix)

The $|00\rangle$remains same as $|00\rangle$. Hence the first column is $\begin{bmatrix}1\\0\\0\\0\end{bmatrix}$

The $|01\rangle$remains same as $|01\rangle$. Hence the second column is $\begin{bmatrix}0\\1\\0\\0\end{bmatrix}$

The $|10\rangle$changes to $|11\rangle$. Hence the third column changes from $\begin{bmatrix}0\\0\\1\\0\end{bmatrix}$ to $\begin{bmatrix}0\\0\\0\\1\end{bmatrix}$

The $|11\rangle$changes to $|10\rangle$. Hence the fourth column changes from $\begin{bmatrix}0\\0\\0\\1\end{bmatrix}$ to $\begin{bmatrix}0\\0\\1\\0\end{bmatrix}$

Hence the matrix form of CNOT gate is

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

Ex (1) S.T the $|00\rangle$remains same as $|00\rangle$ when operated by CNOT

$$\text{CNOT}|00\rangle = \begin{bmatrix}1 & 0 & 0 & 0\\0 & 1 & 0 & 0\\0 & 0 & 0 & 1\\0 & 0 & 1 & 0\end{bmatrix}\begin{bmatrix}1\\0\\0\\0\end{bmatrix}$$

$$\text{CNOT}|00\rangle = \begin{bmatrix}1+0+0+0\\0+0+0+0\\0+0+0+0\\0+0+0+0\end{bmatrix} = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}$$

$$\therefore \text{CNOT}|00\rangle = |00\rangle$$

Ex (2) S.T the $|01\rangle$remains same as $|01\rangle$ when operated by CNOT

$$\text{CNOT}|01\rangle = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}\begin{bmatrix}0\\1\\0\\0\end{bmatrix}$$

$$\text{CNOT}|01\rangle = \begin{bmatrix}1+0+0+0\\ 0+1+0+0\\ 0+0+0+0\\ 0+0+0+0\end{bmatrix} = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}$$

$$\therefore \text{CNOT}|01\rangle = |01\rangle$$

Ex (3) S.T the $|10\rangle$changes to $|11\rangle$ when operated by CNOT

$$\text{CNOT}|10\rangle = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}\begin{bmatrix}0\\0\\1\\0\end{bmatrix}$$

$$\text{CNOT}|10\rangle = \begin{bmatrix}0+0+0+0\\ 0+0+0+0\\ 0+0+0+0\\ 0+0+1+0\end{bmatrix} = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

$$\therefore \text{CNOT}|10\rangle = |11\rangle$$

Ex (4) S.T the $|11\rangle$changes to $|10\rangle$ when operated by CNOT

$$\text{CNOT}|11\rangle = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}\begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

$$\text{CNOT}|11\rangle = \begin{bmatrix}0+0+0+0\\ 0+0+0+0\\ 0+0+0+1\\ 0+0+0+0\end{bmatrix} = \begin{bmatrix}0\\0\\1\\0\end{bmatrix}$$

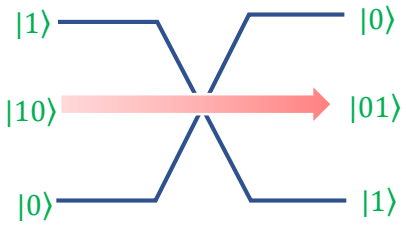
$$\therefore \text{CNOT}|11\rangle = |10\rangle$$

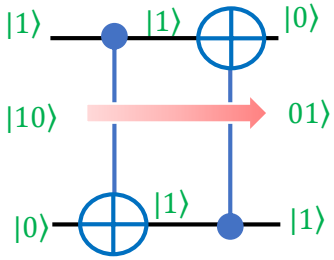
2. Swap Gate

In quantum computation sometimes we need to move state between two qubits, ie from control to target and vice versa. This is nothing but ***swapping*** of the states and the gate used for this purpose is known as SWAP gate.

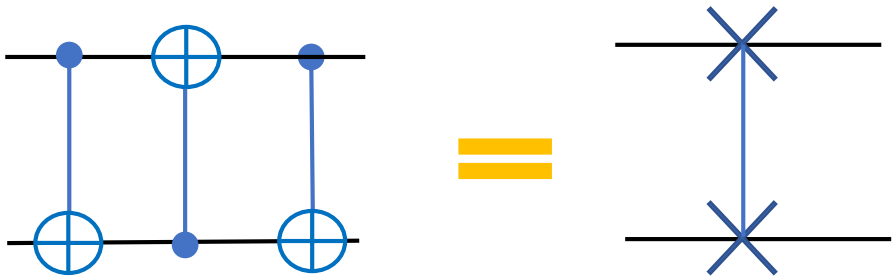
SWAP gate is a two qubit operation gate and swaps the state of the two qubits involved in the operation. It contains 3 CNOT gates.

The action of SWAP gate is explained by taking two CNOT gates as follows where $|10\rangle$ is swapped to $|01\rangle$

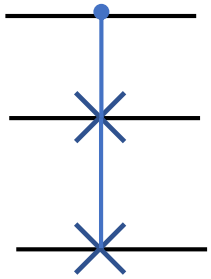




But for effective swapping of the states there must be minimum of 3 CNOT gates. The SWAP circuit is as given below



It is also represented as

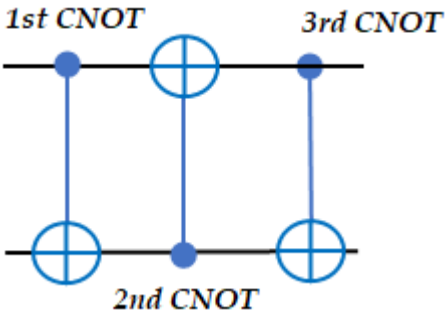


The matrix form of SWAP gate is given by

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

Ex (1) S.T the state $|00\rangle$ remains undisturbed by the SWAP gate operation

Consider the SWAP circuit diagram



We know that in CNOT gate if the control qubit is in $|1\rangle$ state then it will flip the target qubit from $|0\rangle$ to $|1\rangle$ and vice versa (otherwise no). So, when $|00\rangle$ is given, the 1st CNOT is **not** satisfied. We stay in the state $|00\rangle$.The 2nd CNOT's control is **not** satisfied. We stay in the state $|00\rangle$.The 3rd CNOT' is also **not** satisfied. We finally stay in the state $|00\rangle$. The same can be verified using matrix analysis as follows

$$SWAP|00\rangle = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}\begin{bmatrix}1\\0\\0\\0\end{bmatrix} = \begin{bmatrix}1+0+0+0\\0+0+0+0\\0+0+0+0\\0+0+0+0\end{bmatrix} = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}$$

$$\therefore SWAP|00\rangle = |00\rangle$$

Ex (2) S.T the state $|10\rangle$ is swapped to $|01\rangle$ by SWAP gate operation

$$SWAP|10\rangle = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}\begin{bmatrix}0\\0\\1\\0\end{bmatrix} = \begin{bmatrix}0+0+0+0\\0+0+1+0\\0+0+0+0\\0+0+0+0\end{bmatrix} = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}$$

$$\therefore SWAP|10\rangle = |01\rangle$$

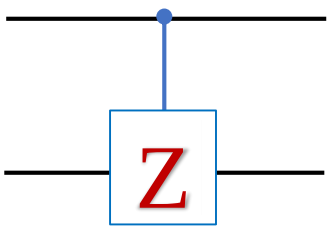
Truth table of swap gate is as follows

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

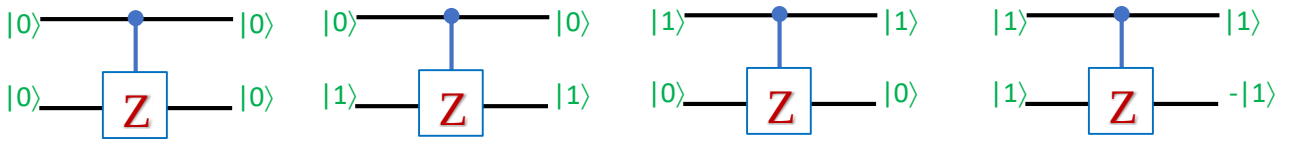
3. Controlled-Z Gate

CNOT gate can be extended in a way that it can work on two qubits based upon a single control qubit. C-Z gate is one such gate. In this gate there is one control qubit and Z unitary matrix as target qubit. If the control qubit is in state $|1\rangle$ then it acts on target Z and will flip the state (ie, there is 180^0 phase change)

The circuit is represented as follows.



Some of the examples are given below



No change because control bit is |0⟩ | *No change because control bit is |0⟩* | *Control bit acts on target but there is no flip of |0⟩* | *Control bit acts on target and flip |1⟩ to -|1⟩*

The truth table of a controlled-Z gate:

Input	Output
|00⟩	|00⟩
|01⟩	|01⟩
|10⟩	|10⟩
|11⟩	-|11⟩

The action of a controlled-Z gate is specified as follows

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

Ex (1): S.T the state |10⟩ remains un affected when operated by C-Z gate

$$U_Z|10\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0+0+0+0 \\ 0+0+0+0 \\ 0+0+1+0 \\ 0+0+0+0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

$$\therefore U_Z|10\rangle = |10\rangle$$

Ex (2): S.T the state |11⟩ flips to - |11⟩ when operated by C-Z gate

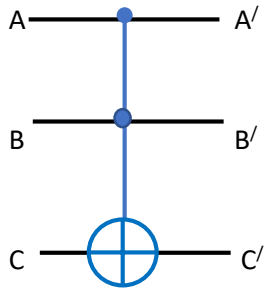
$$U_Z|11\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0+0+0+0 \\ 0+0+0+0 \\ 0+0+0+0 \\ 0+0+0-1 \end{bmatrix} = -\begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

$$\therefore U_Z|11\rangle = -|11\rangle$$

4. Toffoli Gate

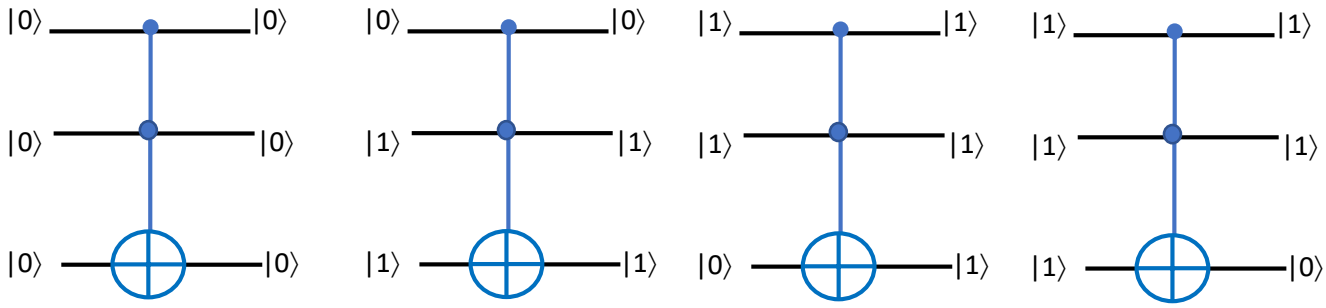
The **Toffoli gate** or **controlled-controlled-NOT (CCNOT)** gate is a logic gate having three input qubits. The first two bits are control bits which remain unaffected by the action of Toffoli Gate. The third is the target bit which is inverted (ie, changes from 0 to 1 or 1 to 0) if both the control bits are 1; else it does not change.

The circuit and the truth table are as follows



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

Some examples are given here



The Toffoli gate can be expressed as an 8 by 8 matrix as follows

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

.

NOTE:

- This is a *reversible* (no information is lost) and *universal* (all reversible logic circuits can be built using Toffoli gates).
- It can be verified that this matrix is unitary and thus the Toffoli gate is a legitimate quantum gate. The quantum Toffoli gate can be used to simulate irreversible classical logic gates and ensures that the quantum gates are capable of performing any computation that a classical computer can do

Limitations of quantum computing

As of now there are some technical difficulties and limitations in building quantum computers. Some of them are

- As the number of quantum gates in a network increases, more interacting qubits are involved, and it is very difficult to monitor their interactions

- The surrounding environment will affect the interactions of qubits (both superposition and entanglement). As a result the quantum information will spread outside the quantum computer and be lost into the environment, thus spoiling the computation. This process is called ***de-coherence.*** How long quantum information will survive before it is spread out is known as ***de-coherency time***
- The number of operations that can be performed before the information is lost due to de-coherency is therefore limited.
- Quantum chips must be kept at very low temperature to create super positions and entanglement of qubits
- The final output of the quantum computers is in the form of a probability. When the question is repeated, the answer changes. Hence repeated operations are required to get correct answer.

Some physicists are pessimistic about the prospects of substantial further progress in quantum computer technology. Some optimistic researchers believe that practical quantum computers will appear in a matter of years rather than decades. We tend towards the optimistic end because

Optimism makes things happen!!!