Volume 3, Issue 10, October 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Introduction to Basic Logic Gates for Quantum Computer

Shaktikanta Nayak, Sitakanta Nayak, J.P.Singh
Department of Management Studies
Indian Institute of Technology
Roorkee, India

***Abstract*— Circuit model of computer is widely accepted as a better abstraction of computational process across the world. The building block of a circuit is the logic gates which are the main information processing units. The gates transform the input bits to the output bits in some deterministic fashion according to the definition of the logic gate. These gates are main information processing units not only for classical computers but also for quantum computers. In this paper the fundamental quantum gates have been studied. Also a comparison between classical and quantum logic gates is outlined.**

***Keywords*— Quantum logic gates, Quantum computing, Logic gate, Quantum computer**

I. INTRODUCTION

There exists some kind of well defined logic for every computation. The classical computation is being performed using Boolean logic which uses variables 0 and 1[1].The physical interpretation of 0 and 1 is the voltage On/Off. But in case of quantum computation, quantum mechanics provides a new set of rules that go beyond this classical paradigm. The basic variable in quantum computing [2, 3, 4] is a quantum bit which is represented as a vector in a two dimensional complex Hilbert space. The logic that can be implemented with such qubits is quite distinct from classical Boolean logic and this is what has made Quantum computing exciting by opening new possibilities. In recent years quantum computing becomes a forefront research in the field of algorithms, cryptography and artificial intelligence [5,6].We can describe qubits as mathematical objects with certain specific properties. The beauty of treating qubits as mathematical objects is that it gives us the freedom to construct a general theory of quantum computation, which does not depend upon a specific system for its realization. The task of information processing can be performed using quantum mechanical principles. And when quantum principles are applied on information processing it gives the concept of quantum computing. In quantum mechanics the state of a physical system is represented by its wave function which contains all information to describe the state of the system completely. Contrary to classical computing we carry out computations using quantum states which follow properties of Quantum mechanics. Changes occurring to a quantum state can be explained using the language of quantum computation. As classical computer is built from an electrical circuit containing wires and logic gates, a quantum computer is built from a quantum circuit containing wires and elementary quantum gates to carry out and manipulate the quantum information. This paper addresses the basic properties of classical and quantum gates and a comparison is made between them with emphasising the shortcomings of classical gates

II. LOGIC GATES IN CLASSICAL COMPUTER

Classical computation theory became prominent after Church and Turing made their investigation into the characteristics of computability in the year 1936 [7]. Logic gates and logic circuits took part major role in the theory of computation. In the course of time the implementation, sophistication and optimal structure of classical logic circuits have been developed [8].

A. IRREVERSIBLE CLAASICAL LOGIC GATES

A gate is said to be logically reversible if we can uniquely determine the input values from the output values otherwise the gate is said to be logically irreversible. We will begin our study of classical logic gates by introducing the notion of Boolean functions.

AND-GATE

It is defined as a Boolean Function $f(x,y) = \begin{cases} 1, if\ x = y = 1 \\ 0, otherwise \end{cases}$

The result can be written as $f(x,y) = xy$ (Meaning: product of *x and y*)

OR –GATE

It is defined as a Boolean Function $f(x,y) = \begin{cases} 0, if\ x = y = 0 \\ 1, otherwise \end{cases}$

The result can be written as $f(x,y) = x + y$ (Meaning: plus of *x and y*)

XOR –GATE

XOR (Exclusive-OR) is a variant of OR function.

It is defined as a Boolean Function $f(x,y) = \begin{cases} 0, if\ x = y = 0\ or\ x = y = 1 \\ 1, otherwise \end{cases}$

The result can be written as $f(x,y) = x \oplus y$

B. UNIVERSAL IRREVERSIBLE LOGIC GATES

NAND-GATE

NAND (NOT-AND) is a universal gate from which any Boolean function can be derived. Let $f(x)$ be a NOT function and $g(x,y)$ be a AND function. The NAND function can be defined as $h = fog = \overline{xy}$.

NOR-GATE

Similarly NOR gate is another universal gate from which any Boolean function can be derived. It can be defined as a function $f(x+y) = \overline{x+y}$.

C. LIMITATION OF IRREVERSIBLE LOGIC GATES

The AND and OR gates are example of irreversible logical gates. The physical meaning of logical irreversibility can be interpreted as the erase of bits during information processing. The work done to erase a bit can be represented as the heat dissipation. According to conservation of energy this loss of energy can be interpreted as physical irreversibility which leads to logical irreversibility in case of irreversible logic gates. This amount of energy loss can be expressed in terms of $KTln_2$ per bit (Where K = Boltzman's constant and T = Absolute temperature) [9]. One way to overcome this problem is to modify chip design and use only reversible logic gates. In case of reversible gates there will be no erase of information and hence no loss of energy. NOT gate is an example of reversible logic gate. From the output of a NOT gate we can find the input just inverting the output bit value. Classically we can design reversible logic gates [10,11] but in the next section we will see quantum gates are reversible by nature.

III. LOGIC GATES IN QUANTUM COMPUTER

In quantum mechanics the state of a physical system is represented by its wave function which contains all information to describe the system completely. A quantum bit or qubit is the smallest unit of information used for quantum information processing. Just as classical bit has two possible states 0 and 1, the qubit has two possible states ket $|0\rangle$ and ket $|1\rangle$ .These two states are also known as computational basis states. In general a qubit is a vector in the two dimensional complex vector space. The main difference between a classical bit and quantum bit is that, a qubit can stay in the superposition of basis states. The superposition is the linear combination of the two basis states $|0\rangle$ and $|1\rangle$ to form the state $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are two complex scalar numbers called amplitudes. The amplitudes can be thought of as the quantum probabilities. The classical probability amplitudes are represented by real numbers, where as the quantum probability amplitudes are represented by complex numbers. The probabilities of a classical system must sum to 1 to form a complete probability distribution. Similarly the squares of the absolute values of the amplitudes of states in a quantum system must add up to 1.The logic that can be implemented with qubits is quite distinct from Boolean logic, and that is why quantum computing is exciting by opening new possibilities.

Mathematically quantum logic gates are represented by transformation matrices or linear operators. The quantum logic gate in the form of transformation matrix interacts with the quantum register through tensor operations. All linear operators that correspond to the quantum logic gates must be unitary i.e. the inverse of that matrix must be equal to its complex conjugate transpose. Unitary operators preserve the inner product of the two vectors. Geometrically the lengths of vectors and the angle between them are preserved i.e. $\langle u|U^{\dagger}U|v\rangle = \langle u|I|v\rangle = \langle u|v\rangle$. The unitary transformation on single qubit may be visualized as rotation and reflection about the x, y and z axes of the Bloch sphere. If U and V are two unitary operators then the composition is also unitary:

$$(UV)^{\dagger} = V^{\dagger}U^{\dagger} = V^{-1}U^{-1} = (UV)^{-1}$$

Classical gates like NAND and XOR are irreversible but the quantum gates, represented in the form of unitary matrices, are always reversible. The matrix representation of single as well as multiple qubit gates is a convenient mathematical way of expressing their input output relationship. If the i^{th} truth-table combinations of a gate are denoted as $|input_i\rangle$ and $|output_i\rangle$, then the matrix representation of the gate can be computed as $\sum_i |input_i\rangle\langle output_i|$

A. SINGLE QUBIT GATES

As NOT gate is a single bit gate in classical computer, in the similar way there exists single qubit quantum gate in quantum computer. Hence single qubit gates are those that act on only a single quantum bit.

QUANTUM NOT-GATE

The quantum NOT gate for qubits can be defined as a process that takes $|0\rangle$ and produces $|1\rangle$ and vice-versa. However in case of superposition, the NOT gate acts linearly in the state $\alpha|0\rangle + \beta|1\rangle$ to $\alpha|1\rangle + \beta|0\rangle$

The matrix representation of quantum NOT gat is $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

The matrix representation of $\alpha|0\rangle + \beta|1\rangle$ is $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$

$$\left(\because \quad \alpha|0\rangle + \beta|1\rangle \; = \; \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \right)$$

If we apply quantum NOT gate to the state $\alpha|0\rangle + \beta|1\rangle$ then

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

TRUTH TABLE AND GRAPHICAL REPRESENTATION OF QUANTUM NOT GATE

INPUT	OUTPUT
$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$
$\alpha\|0\rangle+\beta\|1\rangle$	$\alpha\|1\rangle + \beta\|0\rangle$

Table-1

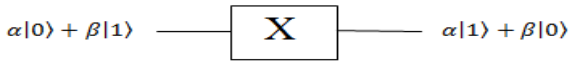

Fig-1

Derivation of Matrix Representation of Quantum NOT Gate:

The matrix representation of $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

The matrix representation of NOT gate $X = \sum_i |input_i\rangle\langle output_i|$

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

Unitary Constraint on Quantum Gate

As shown above, a single quantum bit gate can be represented by 2×2 matrices. The normalization condition requirement for any α and β in the form $\alpha|0\rangle + \beta|1\rangle$ is $|\alpha|^2 + |\beta|^2 = 1$, due to the requirement of the conservation of probability to be 1. Hence in general it can be said that if a single quantum bit gate is defined by a unitary matrix U, then $adj(U).U = I$.

Verification of Unitary Constraint of Quantum NOT Gate:

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

Then $adj(X) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $adj(X).X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} . \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = I$

Hence we can conclude from above discussion that there exists a single non-trivial single qubit bit gate i.e. NOT gate. But in case of single qubit NOT gates, several possible cases are possible as long as the unitary constraint is satisfied. Some of these are Hadamard gates and Z gates.

Z-Gate

The Matrix Representation of Z-Gate is defined as: $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

It inverts sign of $|1\rangle$ to give $-|1\rangle$ and leaves $|0\rangle$ unaltered.

For $|0\rangle$ the output is $|0\rangle$: $Z|0\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$

For $|1\rangle$ the output is $-|1\rangle$: $Z|1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ -1 \end{bmatrix} = -|1\rangle$

For the state $\alpha|0\rangle + \beta|1\rangle$: $Z(\alpha|0\rangle + \beta|1\rangle) = \alpha Z|0\rangle + \beta Z|1\rangle = \alpha|0\rangle - \beta|1\rangle$

TRUTH TABLE AND GRAPHICAL REPRESENTATION OF QUANTUM Z-GATE

INPUT	OUTPUT
$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$-\|1\rangle$
$\alpha\|0\rangle+\beta\|1\rangle$	$\alpha\|0\rangle - \beta\|1\rangle$

Table-2

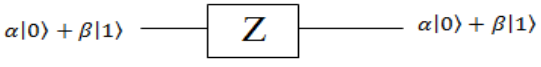

Fig-2

Derivation of Matrix Representation of Quantum Z- Gate:

The matrix representation of $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$ and $|1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$.

The matrix representation of Z- gate $Z = \sum_i |input_i\rangle\langle output_i|$

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

Verification of Unitary Constraint for Z-Gate:

We have to show: $adj(Z).Z = I$

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

HADAMARD GATE

The Matrix Representation of Hadamard gate *is defined as*: $H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$

For $|0\rangle$ the output is $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$:

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

Similarly, for $|1\rangle$ the output is $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$:

$$H|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix} = \frac{1}{\sqrt{2}}\left[\begin{bmatrix}1\\0\end{bmatrix} - \begin{bmatrix}0\\1\end{bmatrix}\right] = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Hence, the Hadamard gate is also known as "square- root" of a NOT gate as it transforms $|0\rangle$ into $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|1\rangle$ in to $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, which may be considered as the mid way between $|0\rangle$ and $|1\rangle$.

For the state $\alpha|0\rangle + \beta|1\rangle$: $H(\alpha|0\rangle + \beta|1\rangle)\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\begin{bmatrix}\alpha\\\beta\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}\alpha+\beta\\\alpha-\beta\end{bmatrix}$

Or $H(\alpha|0\rangle + \beta|1\rangle) = \alpha H|0\rangle + \beta H|1\rangle = \alpha\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) + \beta\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) = \frac{\alpha+\beta}{2}|0\rangle + \frac{\alpha-\beta}{2}|1\rangle$

If we apply $\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)$ to H: $\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right).\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\begin{bmatrix}1\\1\end{bmatrix}\frac{1}{2}\begin{bmatrix}2\\0\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix} = |0\rangle$

Similarly, if we apply $\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$ to H: we will get $|1\rangle$.

TRUTH TABLE AND GRAPHICAL REPRESENTATION OF HADAMARD-GATE

INPUT	OUTPUT
$\|0\rangle$	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$
$\|1\rangle$	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$
$\alpha\|0\rangle+\beta\|1\rangle$	$\alpha\left(\frac{\|0\rangle+\|1\rangle}{\sqrt{2}}\right) + \beta\left(\frac{\|0\rangle-\|1\rangle}{\sqrt{2}}\right)$ $= \frac{\alpha+\beta}{2}\|0\rangle + \frac{\alpha-\beta}{2}\|1\rangle$

Table-3

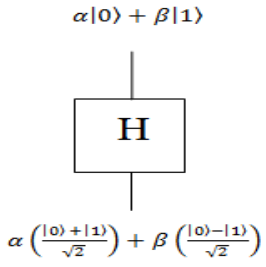

Fig-3

Derivation of Matrix Representation of Hadamard- Gate:

The matrix representation of $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$ and $|1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$.

The matrix representation of H- gate $H = \sum_i |input_i\rangle\langle output_i|$

$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$$H = \sum_i |input_i\rangle\langle output_i| = |0\rangle\frac{1}{\sqrt{2}}(\langle 0| + \langle 1|) + |1\rangle\frac{1}{\sqrt{2}}(\langle 0| - \langle 1|)$$
$$= \frac{1}{\sqrt{2}}[|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|]$$

$$= \frac{1}{\sqrt{2}}\left[\begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}1 & 0\end{bmatrix} + \begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}0 & 1\end{bmatrix} + \begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}1 & 0\end{bmatrix} - \begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}0 & 1\end{bmatrix}\right]$$

$$= \frac{1}{\sqrt{2}}\left[\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix} + \begin{bmatrix}0 & 1\\0 & 0\end{bmatrix} + \begin{bmatrix}0 & 0\\1 & 0\end{bmatrix} - \begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}\right] = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$$

Verification of Unitary Constraint for Hadamard-Gate:

We have to show: $adj(H).H = I$

$$\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix} = \frac{1}{2}\begin{bmatrix}2 & 0\\0 & 2\end{bmatrix} = \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} = I$$

PHASE GATE (S-GATE)

The S-Gate is defined as: $S = \begin{bmatrix}1 & 0\\0 & i\end{bmatrix}$

For $|0\rangle$ the output is $\begin{bmatrix}1 & 0\\0 & i\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix} = |0\rangle$

For $|1\rangle$ the output is $\begin{bmatrix}1 & 0\\0 & i\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0\\i\end{bmatrix} = i|1\rangle$

For $\alpha|0\rangle + \beta|1\rangle$ the output is $\begin{bmatrix}1 & 0\\0 & i\end{bmatrix}\begin{bmatrix}\alpha\\\beta\end{bmatrix} = \begin{bmatrix}\alpha\\i\beta\end{bmatrix} = \alpha|0\rangle + i\beta|1\rangle$

Graphical representation:

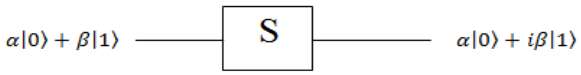

Fig-4

It can be verified that S gate satisfies unitary constraint.

T-GATE

The T-Gate is defined as follows: $T = \begin{bmatrix}1 & 0\\0 & exp\left(\frac{i\pi}{4}\right)\end{bmatrix}$

This is also known as $\frac{\pi}{8}$ gate since it can also be expressed as:

$$T = exp\left(\frac{i\pi}{4}\right)\begin{bmatrix}exp\left(-\frac{i\pi}{8}\right) & 0\\0 & exp\left(\frac{i\pi}{8}\right)\end{bmatrix}$$

For $|0\rangle$ the output is $\begin{bmatrix}1 & 0\\0 & exp\left(\frac{i\pi}{4}\right)\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix} = |0\rangle$

For $|1\rangle$ the output is $\begin{bmatrix}1 & 0\\0 & exp\left(\frac{i\pi}{4}\right)\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0\\exp\left(\frac{i\pi}{4}\right)\end{bmatrix} = exp\left(\frac{i\pi}{4}\right)|1\rangle$

For $\alpha|0\rangle + \beta|1\rangle$ the output is $\begin{bmatrix}1 & 0\\0 & exp\left(\frac{i\pi}{4}\right)\end{bmatrix}\begin{bmatrix}\alpha\\\beta\end{bmatrix} = \begin{bmatrix}\alpha\\\beta exp\left(\frac{i\pi}{4}\right)\end{bmatrix} = \alpha|0\rangle + \beta exp\left(\frac{i\pi}{4}\right)|1\rangle$

Graphical representation of T gate:

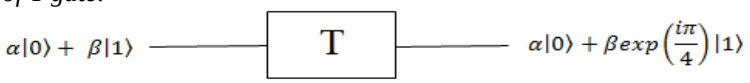

Fig-5

Relation between S and T Gates:

The algebraic relation between S and T is as follows:

$S = T^2$ as

$$T^2 = \begin{bmatrix}1 & 0\\0 & exp\left(\frac{i\pi}{4}\right)\end{bmatrix}\begin{bmatrix}1 & 0\\0 & exp\left(\frac{i\pi}{4}\right)\end{bmatrix} = \begin{bmatrix}1 & 0\\0 & i\end{bmatrix} = S$$

B. MULTIPLE QUBIT GATES

In 1995, a number of researchers declared that the two-qubit gates are basic gates [12-14] and higher qubit gates can be constructed using them in compared to classical reversible logic gates which require three-bit gates for universality.

Classical multiple input gates are AND, OR, XOR, NAND, NOR etc. Similarly we can have multiple qubit gates in case of quantum computation.

The operation of *controlled gate* is described as "If A is true, then do B" .Where A is the *control qubit* and B is the *target qubit*. If control qubit is set to 0 then target qubit is not altered. If control qubit is set to 1 then target qubit is inverted.

CONTROLLED NOT-GATE (CNOT-GATE)

The CNOT gate is the prototype of multi qubit quantum gate. The circuit of CNOT is given below:

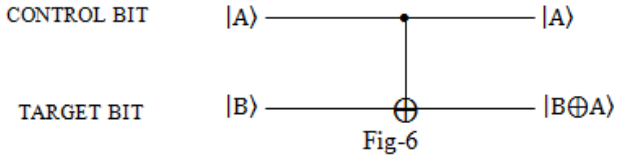

Fig-6

The CNOT Gate has two input qubits:

(I) Control Qubit: Here in the above figure control bit is represented by $|A\rangle$.

(II) Target Qubit: The garget bit is represented by $|B\rangle$.

The CNOT gate works in the following way: If the control qubit is set to 0 then target qubit remains unaltered. If the control qubit is set to 1 then the target qubit is inverted. Now we will examine the functionality of CNOT gate with all possible configurations of bits.

- Input state $|00\rangle$: *Control qubit = 0 and Target qubit = 0*

  As control qubit is 0 the target qubit remains unaltered. Hence the output state is the same as the input state.

  $$|00\rangle \rightarrow |00\rangle$$

- Input state $|01\rangle$: *Control qubit = 0 and Target qubit = 1*

  As control qubit is 0 the target qubit remains unaltered. Hence the output state is the same as the input state.

  $$|01\rangle \rightarrow |01\rangle$$

- Input state $|10\rangle$: *Control qubit = 1 and Target qubit = 0*

  As control qubit is 1, the target qubit is inverted to 1. Hence the output state has both the qubits 1.

  $$|10\rangle \rightarrow |11\rangle$$

- Input state $|11\rangle$: *Control qubit = 1 and Target qubit = 1*

  As control qubit is 1, the target qubit is inverted to 0. Hence the output state becomes

  $$|11\rangle \rightarrow |10\rangle$$

Truth Table of CNOT-Gate:

INPUT	OUTPUT
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$

Table-4

Matrix Representation of CNOT-Gate:

$$|00\rangle = |0\rangle\oplus|0\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix} \quad , |01\rangle = |0\rangle\oplus|1\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}$$

$$|10\rangle = |1\rangle\oplus|0\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix} \quad , |11\rangle = |1\rangle\oplus|1\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

$$CNOT = \sum_i |input_i\rangle\langle output_i|$$

$$= |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|$$

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

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

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

CNOT gate can be considered as a generalized XOR gate since the action of the gate can be considered as: $|A, B\rangle \rightarrow |A, B \oplus A\rangle$ where $\oplus$ stands for modulo-2 addition.

Verification of Unitary Constraint for CNOT-Gate: $\text{adj}(\text{CNOT}).\text{CNOT} = I$

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

CNOT-Gate is Reversible:

Unitary quantum gates are always invertible since inverse of unitary matrix is also a unitary matrix.

Universality of CNOT Gate:

Any multiple qubit logic gates may be composed from CNOT and single qubit gates. This is the quantum parallel of the universality of the NAND gate.

SWAP-GATE

Swap gate is defined as: $U_{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

Graphical Representation of Swap Gate:

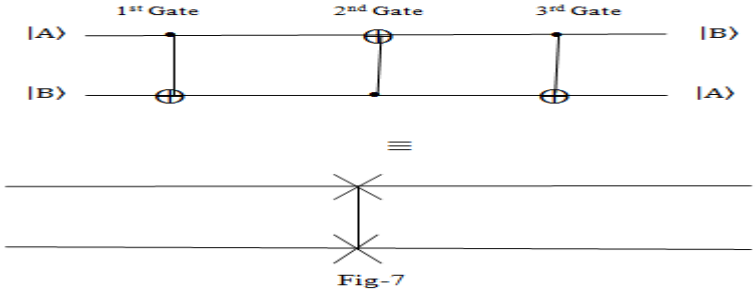

Fig-7

The swap gate is prepared using three CNOT gets. The circuit is read from left to right and each line represents a quantum passage, maybe of time, perhaps a physical particle such as a photon or a light to move from one location to another space.

The inputs are $|A, B\rangle$.The output of first CNOT gate is $|A, B \oplus A\rangle$ .This is fed to the second CNOT gate, the output is $|A \oplus (B \oplus A), A \oplus B\rangle = |B, A \oplus B\rangle$ .This is now fed to the third CNOT gate, the final output becomes $|B, (A \oplus B) \oplus B\rangle = |B, A\rangle$. Hence the overall effect is that the two qubits have been swapped.

Truth Table of Swap gate:

INPUT	OUTPUT
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|10\rangle$
$\|10\rangle$	$\|01\rangle$
$\|11\rangle$	$\|11\rangle$

Table-5

Matrix Representation of Swap-Gate:

$$|00\rangle = |0\rangle \oplus |0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, |01\rangle = |0\rangle \oplus |1\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$|10\rangle = |1\rangle \oplus |0\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, |11\rangle = |1\rangle \oplus |1\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

$$U_{SWAP} = \sum_i |input_i\rangle\langle output_i|$$
$$= |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|$$
$$= \begin{bmatrix}1\\0\\0\\0\end{bmatrix}[1\ 0\ 0\ 0] + \begin{bmatrix}0\\1\\0\\0\end{bmatrix}[0\ 0\ 1\ 0] + \begin{bmatrix}0\\0\\1\\0\end{bmatrix}[0\ 1\ 0\ 0] + \begin{bmatrix}0\\0\\0\\1\end{bmatrix}[0\ 0\ 0\ 1]$$
$$= \begin{bmatrix}1&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{bmatrix} + \begin{bmatrix}0&0&0&0\\0&0&1&0\\0&0&0&0\\0&0&0&0\end{bmatrix} + \begin{bmatrix}0&0&0&0\\0&0&0&0\\0&1&0&0\\0&0&0&0\end{bmatrix} + \begin{bmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&1\end{bmatrix}$$
$$= \begin{bmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&1&1\end{bmatrix}$$

CONTROLLED Z-GATE

The controlled-Z gate is defined as: $U_Z = \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&-1\end{bmatrix}$

The action of Controlled Z- Gate: If A is true, then do B

Truth table:

INPUT	OUTPUT
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|10\rangle$
$\|11\rangle$	$-\|11\rangle$

Table-6

IV. COMPARISON OF CLASSICAL VS QUANTUM LOGIC GATES

CHARACTARISTICS	CLASSICAL GATES	QUANTUM GATES
Basic unit of information	Binary bits:{0,1}	Quantum bits: $\{\|0\rangle, \|1\rangle\}$ in the form of superposition $\alpha\|0\rangle + \beta\|1\rangle$
Dynamics	Deterministic	Probabilistic
Measurements	Never influence the system	Influence the system
Feedback loop	Cyclic	Acyclic
Role of Fan-In and Fan-Out when more than one gate combine	Possible	Not possible
Reversibility	Not always	Always

Table-7

V. CONCLUSION

In this paper the quantum gates have been discussed with graphical and mathematical representation. The reversible nature of quantum gates have been proved mathematically. Hence using quantum computer we can overcome the irreversibility nature of classical computation and avoid information loss. Finally a comparison is made between the classical and quantum logic gates.

REFERENCE

[1] M.Morris Mano, Digital Design Prentice Hall, Third Edition, (2002)
[2] Mikio Nakahara and Tetsuo Ohmi, Quantum computing, CRC press, (2008)
[3] Nielsen, M.A. and Chuang, I.L., Quantum computation and quantum information. UK: Cambridge University Press,(2000)
[4] Sahni, V., Quantum computing. New Delhi: Tata McGraw Hill, (2007)

[5] Sitakanta Nayak, Shaktikanta Nayak, J.P Singh, **"**Quantum Concepts in Neural Computation", Proceedings of the International Conference on Soft Computing for problem Solving, 2011, Advances in Intelligent and Soft Computing ,Vol. 130, pp. 395–400 , Springer India

[6] Sitakanta Nayak, Shaktikanta Nayak "A Study on Quantum inspired Hybrid Neural Networks Model", International Journal of Advanced Research in Computer science and Software Engineering.Vol-3, No-06, June-2013

[7] A. Turing, "On computable numbers with an application to the Entscheidungs-problem," Proc. Lond. Math. Soc. Ser. 2, 42 (1936), 230-65. Also see A. Church, "An unsolvable problem of elementary number theory," American J. of Math., 58 (1936), 345-63.

[8] F. E. Hohn, Applied Boolean Algebra – An Elementary Introduction, The Macmillan Company, New York, 1966.

[9] R. P. Feynman, "Quantum mechanical computers," Found. Phys., 16 (1986), 507.

[10] C. H. Bennett, "Logical Reversibility of Computation," IBM Journal of Research and Development, 17 (1973), 525-32.

[11] T. Toffoli, "Reversible Computing," Tech. Memo MIT/LCS/TM-151, MIT Lab. for Com. Sci. (1980).

[12] D. P. DiVincenzo, "Two-bit gates are universal for quantum computation," Phys. Rev. A, 51 (1995), 1015-18.

[13] T. Sleator, H. Weinfurter, "Realizable Universal Quantum Logic Gates," Phys. Rev. Lett., 74 (1995), 4087-90.

[14] A. Barenco, "A universal two-bit gate for quantum computation," Proc. R. Soc. Lond. A, 449 (1995), 679-83.

