

Introduction to Quantum Gates : Implementation of Single and Multiple Qubit Gates

Ropa Roy, Asoke Nath

Department of Computer Science, St. Xavier's College(Autonomous), Kolkata, West Bengal, India

ABSTRACT

Article Info

Volume 7, Issue 6

Page Number : 385-392

Publication Issue :

November-December-2021

Article History

Accepted : 15 Dec 2021

Published : 30 Dec 2021

A quantum gate or quantum logic gate is an elementary quantum circuit working on a small number of qubits. It means that quantum gates can grasp two primary feature of quantum mechanics that are entirely out of reach for classical gates : superposition and entanglement. In simpler words quantum gates are reversible. In classical computing sets of logic gates are connected to construct digital circuits. Similarly, quantum logic gates operates on input states that are generally in superposition states to compute the output. In this paper the authors will discuss in detail what is single and multiple qubit gates and scope and challenges in quantum gates.

Keywords: Spin angular moment, Bloch Sphere, qbit, Pauli , Hadamard, CNOT, Toffoli, Fredkin, CCNOT

I. INTRODUCTION

Currently, the computer industry widely uses circuit model of a computer as the most useful abstraction of the computing process in design and construction of practical computing hardware. Computer scientists regard any computation as being equivalent to the action of a circuit constructed of a handful of different boolean logic gates working on binary input in the circuit model. Any classical computation can be broken down into a series of logical gates acting on only a few classical bits at a time, similarly, in quantum computation circuits can be broken down into a sequence of quantum logic gates that act on a few qubits at a time. The most significant difference is that classical logic gates work on classical bits, 0 or

1, whereas quantum gates can manipulate superposition and entanglement of arbitrary multi-partite quantum states. Thus, it can be stated that quantum logic gates are more diverse than the classical logic gates.

Google quantum machine, in the recent times, performed a computation in 200 seconds, as per the calculations they determined that it would have taken the world's supercomputer roughly 10,000 years to perform the same computation.

Now atoms have fixed shells have and have electrons in different spin states (i.e. spin angular momentum $+1/2$ or $-1/2$).

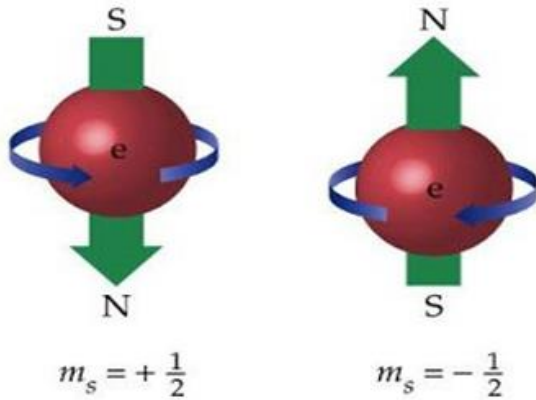


Figure 1. Spin angular momentum

So, denoting $+1/2$ as binary 1 and $-1/2$ as binary 0 in electron spin which acts as our qubit (which

For example- if there are 300 qubits in fully entangled state. So, the resultant will be 2 to the power 300 classical bits which are many particles are in our universe.

Classical computer does 'n' operations at one time using n-bits whereas quantum computer does 2^n operations in n-qubits in the same time. So, quantum computers can do more work and it increases exponentially in the same time.

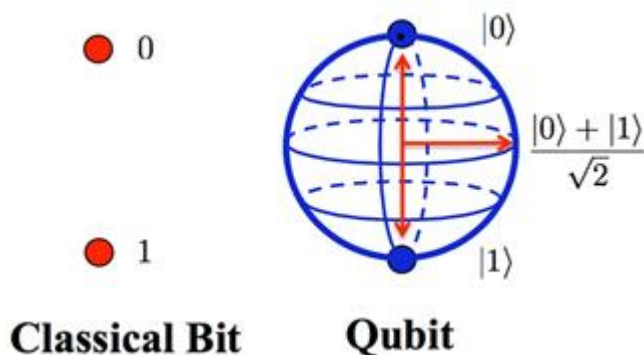


Figure 2. Classical bit and qbit

II. UNDERSTANDING QUANTUM GATES

To understand quantum logic gates more clearly there should be some knowledge about qubit, superposition and entanglement.

were simply bit in classical computers made up of whole atom instead of electron).

At a particular instant qubit can have either 0 or 1 or both at the same time. In quantum mechanics we cannot determine exact spin of electron, we can only determine its probability of having $+1/2$ or $-1/2$ at a particular instant. So, particles have to spin at the same time also termed as *Entanglement*.

Now 1 qubit is equivalent to 2 classical bits and 2 qubits are equivalent to 4 classical bits. And, N qubits are equivalent to 2^n classical bits. It rises exponentially.

A. Qubit

A Qubit by definition is a quantum bit. A qubit can hold both 1 and 0 simultaneously and is named a superposition state. A bit on the other hand can hold either 0 or 1 at the same time. So, in theory it can be said that a qubit can simultaneously participate in numerous processes. Thus, quantum computers are super fast.

Example:

There is a maze with only one way out and a million other ways leading to dead ends.

Now, imagine you are at the center of the maze.

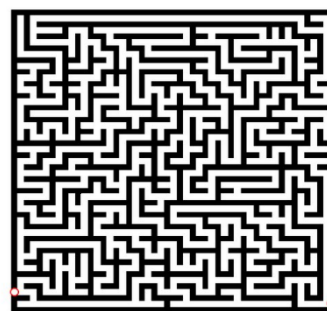


Figure 3. Maze

Case-1 _____:

The one way out is unknown to us. So, the correct

approach is the trial and error technique that might take years to find the way out. (Modern computer works this way)

Case-2 :

If we have millions of clones of one person, then that person and his clones will start finding the way out simultaneously and thus, one of the clone will find the way out in the first go itself. Thus, one can find the way out in the first try.

These clones working simultaneously to explore and find out the correct way out at once are the superposition states same as qubits.

Theoretically, the more complicated the problem the faster the solution attained with the help of quantum computer.

B. Superposition and Entanglement

A qubit can be denoted in an exceedingly linear combination of states :

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

The numbers α and β are complex numbers. The property of having the ability to exist in multiple states is termed *superposition*. Quantum mechanics does not allow the view of amplitudes, ie. α and β , of the two base vectors are. Instead, when we measure a qubit, we get the state $|0\rangle$ with probability $|\alpha|^2$ and the state $|1\rangle$ with probability $|\beta|^2$. The addition of these probabilities must be up to 1. If a quantum operation is performed on a qubit in multiple states, then the operation is performed on all states at the same time. Once the qubit ascertained, it will collapse back into a single state stochastically, according to the squares of the probabilities.

The famous physicist R. Feynmann advised that a qubit $\alpha|0\rangle + \beta|1\rangle$ occupies *all the states* between 0 and 1 *at the same time*, however collapses into 0 or 1 once ascertained physically. Therefore an infinite amount of information can be encoded in a qubit, but as it can never be observed most of the information is useless. This raises various fascinating philosophical questions about what information actually is. As

expressed previously, when observed, a qubit collapses into one of it's basis states. Nobody is aware why this happens, it is one of the essential tenets of quantum mechanics. The reason that a quantum state collapses upon physical observation is understood because of the Kobenhavn Interpretation, and is that the standard (though not the only) means of explaining the collapse upon measurement.

Superposition is one of the properties that enables the Quantum Computing paradigm to supersede classical computing and the other is Entanglement. A two qubit system has four computational basis states, which are $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$. The two qubit system may be in any superposition of these states. There are four very fascinating states that such a system can be prepared in. These states are referred to as the Bell States or EPR states. An example of Bell State :

$$|\phi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{(2)}}$$

When one measures the first qubit in this state, there are two possible results; 0 with probability $1/2$ leaving the other qubit in the state $|00\rangle$, and $|11\rangle$ with probability $1/2$, leaving the other qubit in the state $|11\rangle$. This suggests that once the second qubit is measured it will forever be in the same state as the first qubit! This correlation between the qubits is understood as entanglement. The measurement correlations between the two qubits are stronger than could ever exist between classical systems is proved by Bell. For example, entanglement between two qubits can persist even though they are spatially separated.

The properties of entanglement and superposition mean that certain speedups can be employed in quantum algorithms that will never be attainable on classical computers. The two most famed quantum algorithms are Shor's algorithm, which can find out the factor a number which is the product of two large

primes in exponential time, and Grover's algorithm which searches a random database in quadratic time.

III. SINGLE QUBIT GATES

Introduction to BOSCH SPHERE :

We'll begin by considering the action of a quantum gate on a single quantum bit. A single classical bit (cbit) is relatively boring; either it's in a zero state, or a one state.[4] In contrast a quantum bit is a much richer object that can exist in a quantum superposition of zero and one. This state can be conveniently visualized as a point on the surface of a 3-dimensional ball, generally called the Bloch sphere [2, 0]. The sphere is rotated around some axis due to the the action of a 1-qubit gate.

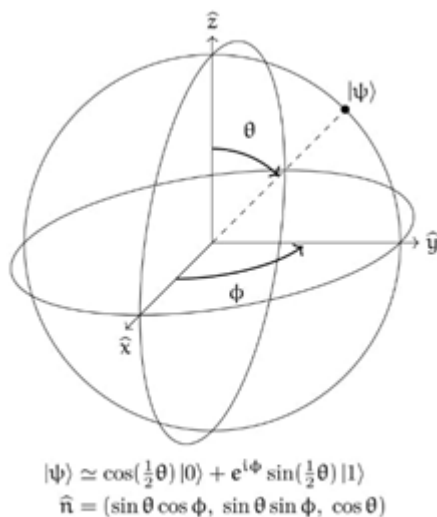


Figure 4. Bloch sphere representation of single qubit states.

A. Pauli Gates :

Classically, there are only 2 1-bit reversible logic gates, identity and NOT (And 2 irreversible gates, reset to 0 and reset to 1). But in quantum mechanics the zero and one states can be placed into superposition, so there are many other interesting possibilities.

The simplest 1-qubit gates are the 4 gates represented by the Pauli operators, I, X, Y, and Z. These operators are also sometimes notated as $\sigma_x, \sigma_y, \sigma_z$, or with an index σ_i , so that $\sigma_0 = I, \sigma_1 = X, \sigma_2 = Y, \sigma_3 = Z$.

Note that the Pauli gates are all Hermitian, $\sigma_i^\dagger = \sigma_i$, square to the identity $\sigma_i^2 = I$, and that the X, Y, and Z gates anti-commute with each other. [4]

$$XY = -YZ = iZ$$

$$YZ = -ZY = iX$$

$$ZX = -XZ = iY$$

$$XYZ = iI$$

A.1. Pauli-I gate (identity):

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



The trivial no-operation gate on 1-qubit, represented by the identity matrix. Acting on any arbitrary state, the gate leave the state unchanged.

$$I = |0\rangle\langle 0| + |1\rangle\langle 1|$$

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

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

A.2. Pauli-X gate (X gate, bit flip)

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



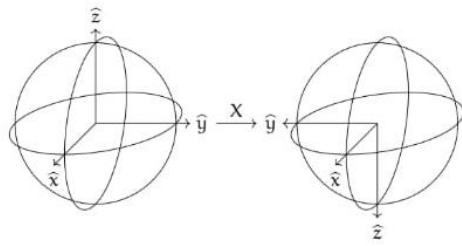


Figure 5. The X-gate bring about a half-turn in the Bloch sphere about the x axis.

With relation to the computational basis, the X gate is similar to a classical NOT operation, or logical negation. The computation basis states are interchanged, so that $|0\rangle$ becomes $|1\rangle$ and $|1\rangle$ becomes $|0\rangle$.

$$X = |10\rangle + |01\rangle$$

$$X |0\rangle = |1\rangle$$

$$X |1\rangle = |0\rangle$$

However, the X-gate is not a real quantum NOT gate, since it solely logically negates the state in the computational basis. A real quantum logical negation would need mapping every point on the Bloch sphere to its antipodal point. However, that would need an inversion of the sphere which can not be generated by rotations alone. There is no quantum NOT operation that will negate an arbitrary qubit state.

A.3. Pauli-Y gate (Y-gate):

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



A useful mnemonic for remembering where to place the minus sign in the matrix of the Y gate is “Minus eye high” [0]. In some older literature the Y-gate is defined as $iY = [0 \ 1 \ -1 \ 0]$, which is the same gate up to a phase.

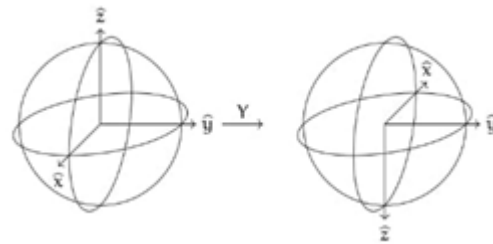


Figure 6. The Pauli-Y gate generates a half-turn in the Bloch sphere about the \hat{y} axis.

The Y-gate can be considered a combination of X and Z gates, $Y = -iZX$. With respect to the computational basis, we interchange the zero and one states and apply a relative phase flip.

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

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

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

A.4. Pauli-Z gate (Z-gate, phase flip)

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

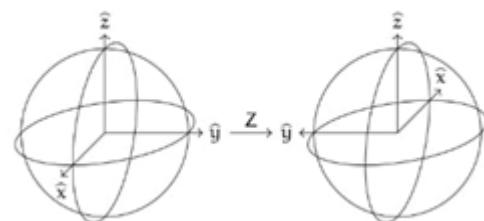


Figure 7. The Pauli-Z gate generates a half-turn in the Bloch sphere about the \hat{z} axis.

With respect to the computational basis, the Z gate flips the phase of the $|1\rangle$ state relative to the $|0\rangle$ state.

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1|$$

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

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

B. Hadamard Gate

The Hadamard gate is one of the most fascinating and useful among the common gates. Its effect is a half turn or a π rotation in the Bloch sphere about the axis $(1/\sqrt{2})(\hat{x} + \hat{z})$. [4]

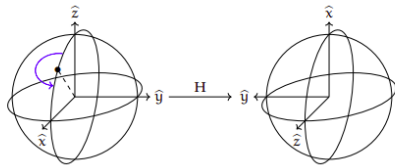


Figure 11. The Hadamard Gate generates half turn or a π rotation in the Bloch sphere about the axis $(1/\sqrt{2})(\hat{x} + \hat{z})$

IV. MULTIPLE QUBIT GATES

A. CNOT Gate

The CNOT gate operates on a quantum register that consists of 2 qubits. The CNOT gate flips the second qubit (the target qubit) if and only if the first qubit (the control qubit) is $|1\rangle$.

Before		After	
Control	Target	Control	Target
$ 1\rangle$	$ 0\rangle$	$ 0\rangle$	$ 1\rangle$
$ 0\rangle$	$ 1\rangle$	$ 0\rangle$	$ 0\rangle$
$ 0\rangle$	$ 0\rangle$	$ 0\rangle$	$ 1\rangle$
$ 0\rangle$	$ 0\rangle$	$ 1\rangle$	$ 0\rangle$

If $\{|0\rangle, |1\rangle\}$ are the allowed input values for both the qubits, then the final output of the CNOT gate corresponds to the result of a classical XOR gate. By changing CONTROL as $|1\rangle$, the final output given by the CNOT gate generates the result of a classical NOT gate.

In other words, the inputs are allowed to be a linear superposition of $\{|0\rangle, |1\rangle\}$. The CNOT gate changes the quantum state:

$$a|00\rangle + b|01\rangle + c|11\rangle + d|10\rangle$$

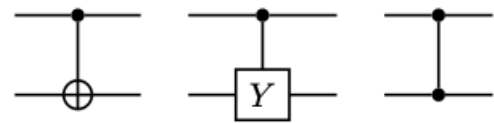
into:

$$a|00\rangle + b|01\rangle + c|11\rangle + d|10\rangle$$

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

The modifications made by the CNOT gate can be represented by the matrix (permutation matrix form)

Circuit representation of CNOT gates:

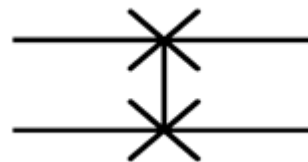


B. SWAP Gate

Two bits are swapped by using SWAP gate. With respect to the basis $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ and it can be represented by the matrix:

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

Circuit representation of SWAP gate :



C. Toffoli Gate (CCNOT)

The Toffoli gate, named after Tommaso Toffoli; additionally known as CCNOT gate (Controlled CNOT Gate), is a 3-bit gate. It is outlined for 3 qubits. If we tend to limit ourselves to solely acceptable input qubits that are $|0\rangle$ and $|0\rangle$, then if the primary two bits are in the state $|1\rangle$ it applies a Pauli-X (or NOT) on the third bit, else it does nothing. It is an example of a controlled gate. Since it is the quantum analog of a classical gate, it is complete given by its truth table.

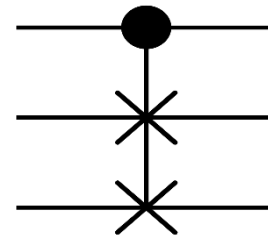
Truth table

m					
INPUT			OUTPUT		
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

Matrix for

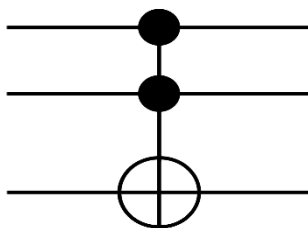
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Circuit representation of Fredkin gate :



The Toffoli gate is closely related to the classical **AND**(\wedge) and **XOR**(\oplus) operations as it performs the mapping $|a, b, c\rangle \rightarrow |a, b, c \oplus (a \wedge b)\rangle$ on states in the computational basis.

Circuit representation of Toffoli gate :



D. Fredkin Gate(CSWAP)

The Fredkin gate (also CSWAP or CS gate), named after Edward Fredkin, is a 3-bit gate that performs a controlled swap.

Truth Table **Matrix form**

INPUT			OUTPUT		
C	\mathcal{I}	\mathcal{J}	C	\mathcal{O}_1	\mathcal{O}_2
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	0
1	1	1	1	1	1

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

V. LIMITATIONS OF QUANTUM COMPUTING

The research for this problem is still continuing the effort applied to identify a solution for this problem that has no positive progress.

1. Qubits are not digital bits of the day thus they cannot use as conventional error correction.
2. The main disadvantage of Quantum computing is the technology required to implement a quantum computer is not available at present days.
3. The minimum energy requirement for quantum logical operations is five times that of classical computers.
4. Quantum CPU will have efficiency and heating problems of its own.
5. When a measurement of any type is made to a quantum system, decoherence is totally broken down and the wave function collapses into a single state.

VI. REFERENCES

[1]. Wikipedia the free encyclopedia, Quantum Gates. online]. Available: https://en.wikipedia.org/wiki/Quantum_logic_gate

[2]. Jason Roell, “Demystifying Quantum Gates-One Qubit at a time”, 2018. online]. Available: <https://towardsdatascience.com/demystifying->

quantum-gates-one-qubit-at-a-time-54404ed80640

- [3]. Pradosh K. Roy, "Quantum Logic Gates", 2020. online]. Available: https://www.researchgate.net/publication/343833536_Quantum_Logic_Gates
- [4]. Gavin E. Crooks, "Gates, States, and Circuits", 2021. online]. Available: https://threeplusone.com/pubs/on_gates.pdf
- [5]. Colm O hEigeartaigh, "Qubits- Superposition and Entanglement", 2003. online]. Available: <https://hego.redbrick.dcu.ie/technicalmanual/node34.html>
- [6]. Nielsen, M. A. & Chuang, I. L. "Quantum Computation and Quantum Information" (Cambridge Univ. Press, Cambridge, 2000) Available: <https://zbmath.org/1049.81015>
- [7]. Yamamoto, T., Pashkin, A., Astafiev, O., Nakamura, Y. & Tsai, J. S., "Demonstration of conditional gate operation using superconducting charge qubits." Available: <https://www.nature.com/articles/nature02015>
- 8Steffen, M. et al., "Measurement of the entanglement of two superconducting qubits via state tomography." Available: <https://doi.org/10.1126%2Fscience.1130886>
- [8]. Nakamura, Y., Pashkin, A. & Tsai, J. S., "Coherent control of macroscopic quantum states in a single-Cooper-pair box." Available: <https://www.nature.com/articles/19718>

Cite this article as :

Ropa Roy, Asoke Nath, "Introduction to Quantum Gates : Implementation of Single and Multiple Qubit Gates", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 6, pp. 385-392, November-December 2021. Available at
doi : <https://doi.org/10.32628/CSEIT217697>
Journal URL : <https://ijsrcseit.com/CSEIT217697>

AUTHOR PROFILE



Dr. Asoke Nath is working as Associate Professor in the Department of Computer Science, St. Xavier's College (Autonomous), Kolkata. He is engaged in research work in the field of Cryptography and Network Security, Steganography, Green Computing, Big data analytics, Li-Fi Technology, Mathematical modelling of Social Area Networks, MOOCs, Quantum Computing etc. He has published more than 257 research articles in different Journals and conference proceedings.



Ms. Ropa Roy is a student of St. Xavier's College, currently pursuing M.Sc. in Computer Science. Her interests lie in the field of Quantum Computing, Machine Learning, Coding, AI and real-world project implementation of these fields.