International Journal of Scientific Research in Physics and Applied Sciences
Vol.6, Issue.4, pp.82-87, August (2018)

Research Paper

**E-ISSN:** 2348-3423

# Contribution of Quantum Computing in Advance Computing with Practical Challenges

**Yogesh Pant**

CIS Department, HSET, Srhu, Dehraun, India

**Available online at: www.isroset.org**

Accepted: 26/Jul/2018, Online: 31/Aug/2018

***Abstract*—** Quantum computation is a nanotechnology that is getting quite a buzz in the field of technology over past few years because of in polynomial time its ability to solve exponentially hard problems. Alternatively, an important feature is having an ultra-low power dissipation and high frequency. CMOS technologies have some drawbacks in Nano-scales. There are 7 billion transistors in NVidia graphics chip so it is simply understood that it is about to achieve subatomic level. This paper explains the concept of quantum computing and quantum universal gates are also discussed in order to provide a good foundation for this emerging technology. This paper also covers the review of the current experimental status of quantum computers and various challenges faced by this technology are also discussed**.**

***Keywords*—** Boolean function; Circuit; Encoding; Quantum logic gates; Matrix transformation; D-Wave.

## I. INTRODUCTION

Ever since, the Quantum mechanics is discovered, scientists have now found an alternative mechanics to develop computer system. Quantum mechanical phenomena behave differently than the classical physics. In 1982, beginning of the story of quantum computing the physicist Richard Feynman considered simulation of quantum-mechanical objects by other quantum systems. Though the unusual strength of quantum computation was not really measured until the 1985 when David Deutsch of the University of Oxford published a critical theoretical paper in which he described a universal quantum computer. After the Deutsch paper, the search was to find something interesting for quantum computers to do. Richard Feynman was the first one to ask what effect this has on computation [1]. In traditional computer it is possible to implement each operation by logic gates. For example universal gate is operationally complete by itself. In classical computing NAND gate is used by combining and recombining such set of operations, it is possible to implement each operation functionally complete. Quantum gate acts on the n-qubit as $2^n$ x $2^n$ unitary matrix. When the input is fetched through gate, the vector of the system state is multiplied by the matrix of the gate and producing new vector of the state. Quantum gate operations are reversible because the gate is unitary matrix and one to one mapping between inputs and outputs. In this formal review, the basic quantum gates will be explained and why they possess universal property. In 1994 Peter Shor from AT&T's Bell Laboratories in New Jersey proposed the first quantum algorithm. This algorithm can perform efficient factorization. This was known as a `killer application' at that time and it was something that only a quantum computer can perform. Difficulty of factorization is used in security of many widespread methods of encryption; for example RSA. Quantum computing implementation faces problems related to de-coherence, error correction, and implement ability of gates.

## II. RELATED WORK

### A. QUANTUM COMPUTING OVER CLASSICAL COMPUTING

Classical computation theory became prominent after Church and Turing made their study into the characteristics of computability in the year 1936 [2]. Logic gates and logic circuits took an important part in the theory of computation. In the passage of time the execution, sophistication and optimal structure of classical logic circuits have been developed [3]. The classical world-view works fine at the everyday level and much of modern engineering relies on this but there are things at the macroscopic level that cannot be comprehend. Using classical physics, these include the color of a heated object, the existence of solid objects. So where does classical physics come unstuck?

The classical computation was implemented using variables 0 and 1 Boolean logic [4].The physical analysis of 0 and 1 is the voltage On/Off. But when it comes to quantum computation, quantum mechanics provides a new protocol that works beyond than the classical paradigm of Boolean logic [5-6]. The basic variable in quantum computing is a

 

quantum bit or qubit which is represented as a vector in a two dimensional complex Hilbert space. The logic that uses such qubit is quite different from classical Boolean logic and this is what has made Quantum computing exciting with new possibilities. Non-classical behavior is mainly observed for microscopic systems like atoms and molecules, but is in fact present at all scales. These kinds of behavior exhibited by microscopic systems that are indicators of a collapse of classical physics are Intrinsic Randomness, Interference phenomena (e.g. particles behaves like waves) and Entanglement. Finding and multiplying of large prime numbers. There is no efficient classical algorithm for the factorization of large number. The best known (or at least published) classical algorithm (the *quadratic sieve*) needs operations for factoring a binary number of N bits i.e. scale exponentially with the input size.

$$O(\exp((\frac{64}{9})^{1/3} N^{1/3} (\ln N)^{2/3}))$$

Table1. Some characteristic comparison of classical Vs quantum logic gates:

| **Characteristics** | **Classical Gates** | **Quantum Gates** |
|---|---|---|
| Basic unit of information | Binary bits {0,1} | Quantum bits {\|0>,\|1>} in the form of superposition |
| Error possibilities | Over communication channel | Storage and retrieval |
| Couse of error | Noise | Decoherence |
| Measurements | Never influence the system | Influence the system |
| Dynamics | Deterministic | Probabilistic |
| Reversibility | Not always | Always |
| Feedback loop | Cyclic | Acyclic |

## B. QUANTUM COMPUTATION-UNITARY OPERATIONS

Quantum computation is a reversible process, logically and physically. All reversible Boolean functions are some particular cases of unitary transformations. For example, if a two-bit function mapped |01⟩to |11⟩, the inverse would map |11⟩back to |01⟩, which is what we would get if we took the transpose of the corresponding unitary matrix. Therefore, loosely speaking, any problem that can be simulated classically can also be simulated quantum mechanically. However, the new features of the quantum computer – superposition, interference between qubits, entanglement, and measurement – allow quantum computers to solve some certain problems, like the factoring and database search problems, exponentially faster than can be done on any classical computer. According to the axioms of quantum mechanics, the evolution of a closed quantum system is described by a unitary transformation. If a system is in state |Ψ| at time $t_1$ is related with its state |Ψ'| at time $t_2$ by a unitary operator U.

$$|\Psi'\rangle = U|\Psi\rangle$$

In the study of quantum computation and quantum information, Pauli matrices are four extremely useful unitary matrices. The matrices, and their notations, are shown in Figure 1[7]

$$\sigma_0 \equiv I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad \sigma_1 \equiv \sigma_X \equiv X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$
$$\sigma_2 \equiv \sigma_Y \equiv Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \qquad \sigma_3 \equiv \sigma_Z \equiv Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Figure1. Pauli matrices

Matrix representation of Quantum bit (qubit):

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

Quantum gate follows the unitary constraint. Single quantum gate can be represented by 2 X 2 matrices. The superposition of qubit follows the condition:

$$\alpha|0\rangle + \beta|1\rangle \text{ where } |\alpha|^2 + |\beta|^2 = 1$$

Single quantum bit gate is defined by a unitary matrix U, then adj(U).U=I. Verification of Unitary Constraint of Quantum NOT Gate:

$$Let\ X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ then adj}(X) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$
$$\text{adj}(X).X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} . \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = I$$

## C. LOGIC GATES

Logic gates and logic circuits took vital place in the theory of computation. Logic gates are the fundamental circuit which performs computing.

### *a) Clasical Logic Gates*

Classical logic gates are irreversible except NOT gate. If we can distinctively determine the input values from the output

 

values than gate is said to be logically reversible otherwise logically irreversible. Classical logic gates are defined as follows by introducing the notion of Boolean functions.

- AND-GATE: The Boolean function of AND gate can defined as:

$$f(x,y)=\begin{cases}1 \text{ if } x=y=1\\ 0 \text{ otherwise}\end{cases}$$

- OR-GATE: The Boolean function of OR gate can defined as:

$$f(x,y)=\begin{cases}0 \text{ if } x=y=0\\ 1 \text{ otherwise}\end{cases}$$

- NAND-GATE: NAND (NOT-AND) is a universal gate which can derive any Boolean function. Let f(x) be a NOT function and g(x, y) be a AND function. The NAND function can be defined as.

$$R = fog = \overline{xy}$$

b) *Quantum* Logic Gates

Quantum gates possess a particular property which makes it special than the classical logic gate. That is reversibility of output to input. The initial concerns about the reversibility of computation appeared in the 1970s. Quantum gate provides classical output with extra information and the extra information is used for regenerate the input state. If a system has reversible gates then we can perform reversible computation in a system. Reversible circuits do not lose information, and there is a one-to-one mapping between the input and the output vectors so it can generate unique output vector from each input vector and *vice versa* [8**].** Landauer has shown that for irreversible logic computations, each bit of information lost heat energy is equivalent to $KT\ln_2$ joule, where *k* is Boltzmann's constant and *T* the absolute temperature at which the computation is performed **[9-10**].

- Single Qubit Gates

In classical computer NOT gate acts on a single bit, in the similar way in quantum computer have single qubit quantum gate. Single qubit gates are those that act on only a single quantum bit.

Table2. Characteristic comparison of single qubit logic gates:

| **Characteristics** | **Quantum Not Gate** | **Z Gate** | **Hadamard Gate** |
|---|---|---|---|
| Input/ Output | $\|0\rangle / \|1\rangle$<br>$\|1\rangle / \|0\rangle$ | $\|0\rangle / \|0\rangle$<br>$\|1\rangle / -\|1\rangle$ | $\|0\rangle / \frac{1}{\sqrt{2}}(\|0\rangle+\|1\rangle)$<br>$\|1\rangle / \frac{1}{\sqrt{2}}(\|0\rangle-\|1\rangle)$ |
| Metrics Representation | $X=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$ | $Z=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$ | $H=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$ |
| Characteristic of Superposition | $\alpha\|0\rangle+\beta\|1\rangle$<br>$\rightarrow \boxed{X} \rightarrow$<br>$\alpha\|1\rangle+\beta\|0\rangle$ | $\alpha\|0\rangle+\beta\|1\rangle$<br>$\rightarrow \boxed{Z} \rightarrow$<br>$\alpha\|0\rangle-\beta\|1\rangle$ | $\alpha\|0\rangle+\beta\|1\rangle$<br>$\rightarrow \boxed{H} \rightarrow$<br>$\alpha(\frac{1}{\sqrt{2}}(\|0\rangle+\|1\rangle))$<br>$-\beta(\frac{1}{\sqrt{2}}(\|0\rangle-\|1\rangle))$ |

- Multiple Qubit Gates

In classical computer there are number of multiple input gates except NOT gate. These are AND, OR, NAND, NOR etc. There we have also multiple input gates in Quantum computer. In 1955, a number of researchers declared that the two-qubit gates are basic gates [11-12]

In CNOT Gate we have two input qubit as Control qubit and Target qubit.


Figure. 2

Controlled NOT-Gate (CNOT)

 

In CNOT Gate if control qubit is set to 0 then target qubit remains unchanged. The target qubit is inverted only if the control qubit is set to 1.

$$f(x,y) = \begin{cases} x \oplus y, y & \text{if } y=1 \\ x, y & \text{otherwise} \end{cases}$$

*where* x=target bit

y=control bit

D. UNIVERSAL GATE

In classical computer NAND and NOR gates are universal gate. Using these universal gates we can derive any other logic gate. Similarly we can derive classical NAND gate using Quantum gate with reversible property.

Controlled-Controlled Not-Gate (CCNOT) As Classical NAND Gate-

In CCNOT-GATE there are two control bits and a target bit. When both the control bits input is $|1\rangle$ then the target bit is inverted.


Figure. 3

Table 3-TRUTH TABLE OF CCNOT-GATE

| *input* | *output* |
|---|---|
| $\|000\rangle$ | $\|000\rangle$ |
| $\|001\rangle$ | $\|001\rangle$ |
| $\|010\rangle$ | $\|010\rangle$ |
| $\|011\rangle$ | $\|011\rangle$ |
| $\|1\bar{0}\bar{0}\rangle$ | $\|1\bar{0}\bar{0}\rangle$ |
| $\|1\bar{0}\bar{1}\rangle$ | $\|1\bar{0}\bar{1}\rangle$ |
| $\|1\bar{1}\bar{0}\rangle$ | $\|1\bar{1}\bar{1}\rangle$ |
| $\|1\bar{1}\bar{1}\rangle$ | $\|1\bar{1}\bar{0}\rangle$ |

Above truth table have the input as $|ABC\rangle$ where input A and B is the control bits and input C is the target bit. The input bits B and C from Row 5-8 and there corresponding output bit C have the similar bits as the NAND in classical computer and the other bits provide reversibility.

## III. IMPLIMENTATON OF QUANTUM COMPUTER

The implementation of quantum hardware is remarkable, obtained from atomic physics, quantum optics and electron magnetic resonance spectroscopy, in superconducting device physics, in electron physics, and in microscopic and quantum dot research.

- Ions Implanted in Silicon

The Kane [13] experiment of phosphorus in silicon builds upon modern semiconductor fabrication, design upon known physical properties. The nuclear spin of a phosphorus atom integrated with an electron embedded in silicon under a high magnetic field and low temperature is used to design Quantum bit [14].

- Solid-State Devices

The design of solid-state devices involves subjecting a substrate to a sequence of physiochemical process. Solid-state device are electronic device in which electricity flows through solid semiconductor crystals (silicon, gallium arsenide, and germanium. Solid-state technology offers an appealing option for manufacturing thousands of qubits as small objects.

## IV. D-WAVE QUANTUM COMPUTING HARDWARE FOR THE NEXT GENERATION

D-Wave One (128 bits) is the first-generation version of quantum computer. That world's first commercial quantum computer-Wave successively shape the hardware design of D-Wave Two (512 bits), a second-generation machine that has already been leased by customers such as Google, NASA. The technologies for hardware design used by D-Wave's quantum computing architecture explore the future approach for the researcher to build more powerful quantum computers.

A. Hardware in D-Wave's quantum computer

D-Wave's quantum computing hardware based on metal loops of niobium that have tiny electrical currents running through them.

B. D-Wave's Quantum Machine

In metal loops of niobium current creates a tiny magnetic field pointing up and down by running counterclockwise and clockwise through the loop. The niobium loops become

 

superconductors when chilled to frigid temperatures of 20 mill kelvin (-273 degrees C). Magnetic field pointing up and down property is used as qubit state 0 and 1. The low temperature makes this possible the currents and magnetic fields can enter the strange quantum state known as "superposition" that allows them to represent both 1 and 0 states simultaneously. That allows D-Wave to use these "superconducting qubits" as the building blocks for making a quantum computing machine.

C. Information Processing Quantum Annealing

Each metal loops of niobium also contains a number of Josephson junction's two layers of superconductor which is separated by a thin insulating layer that act as a mechanism of switches for routing magnetic pulses to the correct locations. D-Wave has worked on a specialized technique known as "quantum annealing" a method of tackling optimization problems instead of building quantum computers using the traditional logic-gate model of computing. D-Wave starts a group of qubits in their lowest energy state and then moderately turns on interactions between the qubits, which encodes a quantum algorithm. When the qubits settle back down in their new lowest-energy state, D-Wave can read out the qubits to get the results .the result is used for solving optimization problems means finding the lowest minimum.

## V. CHELLENGES IN IMPLEMENTATION OF QUANTUM COMPUTER

Quantum computing faces problems related to decoherence, state preparation, error correction, and implement ability of gates. The requirements for physical implementation of a quantum computer include long decoherence time, a stable memory, feasible state preparation for the initial state, a universal set of gate operations and capability for single quantum measurements [15].

A. Decoherence

Quantum computers are extremely sensitive to interaction with the surroundings since any measurement leads to a collapse of the state function an unwanted interaction of quantum information with extraneous entities, is a hazard of quantum computing in that it destroys the information the system is processing. This phenomenon is called decoherence. It is really difficult to separate a quantum system, especially an engineered one for a computation, without it getting entangled with the environment [16]. It is harder to maintain the coherence with larger number of qubits. Decoherence cannot be reversed by redundancy coding [17] even it raise the quantum computer's vulnerability against decoherence by adding extra physical quantum bits to achieve redundancy.

B. Errors And Their Correction

Computation invariably involves errors, which are internal or externally induced. The classical computers has the capability to perform well because the non-linearly of the computation process makes it possible to eliminate small errors by redundant error correction bit. In quantum error correcting algorithms [18] consider only bit flips, phase flips or both between the relative phases but these are not all the errors that might encounter in a quantum computation. Unlike the situation in classical computing, small errors cannot be eliminated in quantum computing [19] as it is a linear process, and it rules out operations comparable to clamping and hard-limiting. The no-cloning theorem prevents us from copying an unknown state and doing additional testing on it. In initialization phase of qubit have random unitary transformation errors can occur [20]. The characteristic of errors is also need to be considered they might be component proliferation, nonlocal effects and amplitude errors. We cannot group the errors in a systematic way because in quantum register the errors can be due to a variety of reasons. In quantum arena information error is nonlocal compared to the local in classical arena and hence the concept of controlling errors using higher dimensional code word space is not realistic.

## VI. CONCLUSION

Quantum computation is a nanotechnology that has a great future. New features of the quantum computer –superposition, entanglement, and measurement, allow quantum computers to solve certain problems, like the factoring and database search problems, exponentially faster than can be done on any classical computer. This paper provides the concept of quantum computing, quantum gates have been discussed with graphical and mathematical representation. This paper also provides quantum computer implementation techniques designed by D-Wave (first commercial Quantum computer) briefly. The challenges with decoherence and error correction in Quantum computer also discussed. Hence using quantum computer can overcome the irreversibility nature of classical computation and avoid information loss. This technology opened a number of great opportunities for researcher with some challenges to change the whole scenario of computation.

## REFERENCES

[1] R.Feynman, "*simulating physics with Computers*," International Journal of Theoretical Physics, Vol. 21, No. 6/7, pp.467-488(1982).

[2] A. Turing, "*On computable numbers with an application to the Entscheidungs-problem*," Proc. Lond. Math. Soc. Ser. 2, 42 (1936), 230-65.

[3] Church, "*An unsolvable problem of elementary number theory*," American J. of Math., 58 (1936), 345-63.

[4] F. E. Hohn, "*Applied Boolean Algebra – An Elementary Introduction*", theMacmillan Company, New York, (1966)

 

[5] M.Morris Mano, "*Digital Design Prentice Hall*", Third Edition, (2002)
[6] Mikio Nakahara and Tetsuo Ohmi*, "Quantum computing,"* CRC press, (2008)
[7] Nielsen, M.A. and Chuang, I.L., "*Quantum computation and quantum information*" UK: Cambridge University Press,(2000)
[8] [M. A. Nielsen and I. L. Chuang, "*Quantum Computation and Quantum Information*", Cambridge University Press , (2002)
[9] H.Thapliyal, and N.Ranganathan,"*Reversible Logic-Based Concurrently Testable Latches for Molecular QCA*" IEEE Transactions On Nanotechnology, Vol. 9, No. 1, January 2010
[10] R. Landauer, "*Irreversibility and heat generation in the computational process*," IBM J. Res. Dev., vol. 5, pp. 183–191, (1961)
[11] R. P. Feynman, "*Quantum mechanical computers*," Found. Phys., 16 (1986), 507
[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] Bruce Kane, "*A silicon-based nuclear spin quantum computer*", Nature **393**(1998), 133–137.
[15] N. Gershenfeld and I.L. Chuang, "*Quantum computing with molecules*",Scientific American (1998).
[16] M. A. Nielsen and I.L. Chuang, "*Quantum Computation and Quantum Information*" Cambridge University Press, (2000)
[17] W.H. Zurek, "*Decoherence and transition from quantum to classical*". Physics Today, October 1991.
[18] H.D. Zeh, "*The roots and fruits of decoherence*". arXiv: quant-ph/0512078.
[19] P.W. Shor, "*Fault-tolerant quantum computation*". arXiv: quant-ph/9605011
[20] S. Kak, "*General qubit errors cannot be corrected*". Inform. Sc. 152, 195-202, 2003; arXiv: quant-ph/0206144.
[21] S. Kak, "*The initialization problem in quantum computing*". Found. Phys., 29: 267- 279, 1999; arXiv: quant-ph/9805002.

**AUTHORS PROFILE**

Mr. Yogesh Pant pursed Diploma, B. Tech. and M.Tech, from GPD Dehradun, UTU and GBPEC respectively in 2010, 2013 & 2016. He is currently working as Assistant Professor in Department of Computer information and Sciences from HSET, SRHU since 2017. His main research work focuses on wireless sensor network, Artificial intelligence and quantum computing. He has 3 years of teaching experience.

 