Classical and Quantum Computing

[1]Tamanna Punia, [2]Attar Singh
[1]Arya College of Education Hisar, CRS Univ. Jind (Haryana) India
[2]Assoc. Prof. HOD Physics, CRM PG College, Hisar (Haryana) India
Email: tamanna.1131@gmail.com

Abstract: *Integrating physics, computer science and mathematics quantum computing has evolved in the last two decades from an imaginative idea to one of the most interesting field of quantum mechanics. Altering the model underlying information and computation from a classical mechanical to a quantum mechanical gives faster algorithms. Quantum algorithm can execute a selective set of tasks widely more effectively than any classical algorithm, but for many tasks, it has proven that quantum algorithms give no actual benefit. The scope of quantum computing applications is still being examined. This research paper gives an overview of quantum computer, explanation of qubit and discusses about the various applications of quantum mechanics to verify the existence of quantum computers.*

Keywords: *Quantum computer, Qubit, Quantum gates, entanglement, algorithms.*

I. Introduction

A quantum computer makes straight use of quantum mechanical phenomena such as superposition and entanglement, (it is the ability for pairs particles to interact over any distance) for carrying out operations on data. Both quantum and digital computers vary from each other. The basic idea behind digital computers is the use of transistors in them which needs data to be encoded in form of binary digits (bits) while in quantum computation to represent data and to perform operations on such data quantum properties are used. It is expected that in the coming 8 years that is in around 2025, transistors and chips will be no longer present in computers. When we think of computers first thing that comes to our mind is the common classical silicon computer (digital computer) . Every one of us thinks that these are the fastest. But, quantum computes are faster than classical ones. Quantum computers are a next general of classical computers according to scientists.

The technology used in quantum computers is very much different from classical ones. Quantum computer uses bits of quantum (qubits) for operation. The nature of Qubit is quaternary. The laws of quantum mechanics are totally different from classical mechanics. The main difference between bit and qubit is that qubit can not only exist in 0 or 1 logical values, but also in linear combination of 0 and 1 state due to the phenomenon of principle of superposition of quantum mechanics. The superposition state is one in which a qubit can be both 0 and 1 simultaneously. Eight qubits are combined to form a qubyte which is similar to a byte of a classical computer but qubyte can have all values from 0 to 255 simultaneously unlike a byte which can’t take all values simultaneously due to the lack of presence of superposition principle.

The computer technology has evolved from gears to relays to valves to transistors to integrated circuits and so on. Due to the presence of advanced lithographic techniques, one can compress fraction of large micron login gates and wires onto the surface of silicon chips which results into even smaller parts and assured to reach a stage where logic gates are so little that are made out of only handful of atoms. The rules of quantum mechanics are obeyed by the matter at atomic scale and such rule varies from the classical rules which determine the various properties of ordinary logic gates. So, new quantum technology must supplement present technology in order to have smaller computers in the future. Based on quantum principles, quantum computers can support completely new type of computation with qualitatively new algorithms.

Let us reflect on a register made up of three physical bits. According to classical computer, its register in a particular time can store only one out on eight different values i.e. there are total eight possible values. Like 000, 001, 010, ……….. 111 and the register can be in anyone of the above configurations at a particular instant of time. While if I talk about quantum register which is also made up of three qubits, at a particular time it can store all 8 configurations due to the quantum superposition principle. The physical presence of all 8 configurations in the register is a striking feature, which is only possible due to the principles of quantum mechanics. To represent the state of an L-qubit system on a classical computer requires the storage of 2^L complex coefficient whereas to characterize the state of n-bit classical system it is sufficient to give the values of L-bits, i.e., only L numbers. Hence, the storage capacity of register when qubits are added increases exponentially i.e. there are total eight possible configurations when three qubits are present. Similarly, four qubits can store sixteen different configuration at a time, so, the general formula depicts that L qubits can store $(2)^L$ configurations or numbers at a time. All operations can be performed once the register is prepared in a superposition of different configurations. A large amount of gain in time and memory is offered by quantum computer due to huge parallel computation in one piece of quantum hardware i.e. only 1 computation step carryout the same mathematical operations on $(2)^L$ different input configurations compressed in coherent superposition of L qubits. While classical computer has to repeat the same computation $(2)^L$ times in order to complete the same task. So, qubits can hold exponentially more information than their classical counterparts. Therefore, one can say, qubits can be in a superposition of all the classically allowed states.

In classical computers, calculations are performed significantly in the same way as by hand. Consequently, the class of problems that can be solved efficiently is the same as the class that can be solved efficiently by hand. Here "efficiently", refers to the idea that the evaluation time doesn't grow too quickly with the size of the input. While in quantum computers, calculations are done by unitary transformations on the state of quantum bits. Combines with the principle of superposition, this creates possibilities that are not available for hand calculations. This translates into more efficient algorithms for a.o. factoring, searching and simulation of quantum mechanical systems. First 16- bit quantum computers were build by IBM Q industry . Along with the IBM computer a company known as D-Wave has also been developing their own version of a quantum computer which is based on a process called annealing.

Qubit (Quantum Bit):

In a quantum computer, information carried in the smallest unit is quantum bit. A. quantum bit exists in the superposition of two states i.e. 0 and 1 unlike classical bits which are present in only two forms i.e. 0 and 1. Bit is the fundamental unit of information of a classical computer. A quantum bit is also called as qubit. Both bit and qubit are analogous to each other. Only difference between them is that qubit has some quantum phenomena associated with it. Although, these bits and qubits are mathematical objects with certain properties yet they can be perceived physically in various ways as an actual physical system. Both bit and qubit are represented by states, bit has either a state 0 or 1 while qubit in addition to these 0 and 1 states can have any linear combination (superposition) as a physical state so, any physical state of a qubit can be described by:

$\Psi = \alpha/0> + \beta / 1>$, where α and β take only complex values.

The 2-dimenssional Hilbert space which is an abstract space for complex vectors can also describe the state of a qubit. States 0 and 1 form an orthonormal basis for this vector space. We get 0 with probability α^2 and 1 with probability β^2 when qubit is measured in orthonormal basis to determine its state according to theory of quantum mechanics. One can successfully write the state of qubit as $\Psi = \cos\theta /0> + e^{i\phi} \mathrm{Sin}\theta /1>$ (Eq. 1)

Where, all phases factors are ignored and θ and ϕ define a point on the Bloch sphere. Also, $\alpha^2 + \beta^2 =1$ due to property of Hilbert space as qubit is a unit vector of previously mentioned 2-dimensional Hilbert space.

State which is mentioned in (Eq. 1) can be represented by 3-dimensional sphere called Bloch sphere. With help of this sphere, one can a single qubit can be visualized. Traditionally, the bits 0 and 1 are represented by bra-ket notation.

Geometrical Representation of Qubit:

The basis states (or basis vectors) in which qubit may be measured are normally written as /0> or /1> and (pronounced as "ket 0" and "ket 1").

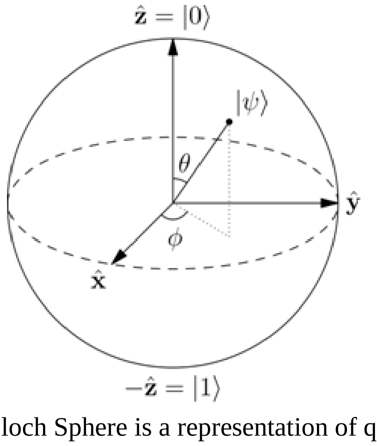

Fig. 1 Bloch Sphere is a representation of qubit

An infinite amount of information can be stored in single qubit theoretically, but when measured we get (0 or 1) i.e. classical results having specific probability which are specified by the quantum state. One of the most important features of quantum mechanics is that "hidden" information is conserved under the dynamic progression (namely, Schrodinger equation) the same happen when qubit measured. So, it is allowed to change the information stored in unmeasured qubits with quantum gates. With the help of this feature and the allocation to manipulate the information is one of the sources for reputed power of quantum computers.

II. Matrices as Quantum Gates:

Logic gates that are used for the classical computers are based upon Boolean algebra. These Boolean logic gates do manipulations of the information that is stored in bits while in quantum computers, these gates are represented by matrices. When rotations of quantum state on the Bloch sphere takes place then quantum gates (matrices) can be visualized. Under such visualization, it has been observed that quantum gates are unitary operators i.e. the norm of quantum sate remains conserved (Let U is a matrix which describes a single qubit gate, then according to the property of unitary operators, $U^{+}U = 1$, where U^{+} is the adjoint of U which is basically first doing transpose and then complex conjugate of U). As we have a NAND gate which is a universal gate of classical computing, we have a C NOT gate which is also a universal gate of quantum computing. In quantum computing, any multiple qubit logic gate may be made up from a quantum C NOT gate. C NOT gate involves an operation similar to that of classical XOR gate. Another distinguishing feature of quantum gates from classical gates is that they are reversible; if we perform inverse operation on the unitary matrix, then we get again get unitary matrix and therefore inversion is possible in quantum gates. One gate can invert another gate.

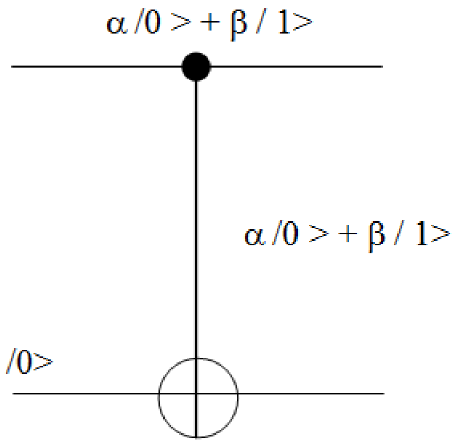

Fig. 2 C NOT Gate

$$\text{C NOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$\text{C NOT} \;\; \Psi = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \\ \delta \\ \gamma \end{pmatrix}$$

C NOT GATE

III. Applications of Quantum Computers:

1. **For conducting virtual experiments:** Feynman first observed the quantum computing. His observations depicted that quantum systems are hard to model on classical computers. To model quantum system, we need quantum computers (This is “quantum stimulation”). For example, if we want to model chemical reactions then we need quantum computers since interactions among atoms in a chemical process is a quantum process.
2. **Cryptography:** The first quantum algorithm was found by Peter Shor in 1974, which can perform an efficient factorization in principle. Only a quantum computer can do such a complex application.

Cryptography involves factoring as one of the most important problems. For example, the safety of electronic banking security system depends on factoring and is a big problem but due to useful feature of quantum computers, it takes only a few years to encrypt the data while it takes almost centuries on existing computers.

3. **Faster in speed:** As already mentioned, quantum computers will be much faster and as a result they perform a huge number of operations in a very short span of time.
4. **Reliability:** With quantum communication, both receiver and sender are alerted when an eavesdropper tries to capture the signal. More amount of information is communicated per bit in quantum computers as compared to classical computers. Also, quantum computers make communication more secure.

Quantum Computers have limitations also:

Decoherence is the process in which superposition of quantum state collapse into a classical state (Decohering is the process in which quantum coherence is lost). This happens due to some changes in parameters in a quantum state due to interaction process with environment. In production of quantum computers, this is the major obstacle. If one can solve this decoherence problem, them only quantum computers are better than classical computers.

To construct a quantum computer that will make calculations before decohering is quite impossible. Alongwith the above mentioned problems; another problem that prevails is hardware of quantum computers. Some of the experiments on NMR (Nuclear Magnetic Resonance) technology are successful in constructing a simple quantum computer. But, it has also certain limitations. Therefore, time consuming tasks may result some quantum algorithms inoperable because of keeping the state of qubits for a long time will corrupt the superposition eventually. Hence, it is not possible to predict about the hardware of quantum computers.

IV. Conclusion:

Experiments and Researches conducted till now gives an idea about the new type quantum computation with many advantages over classical computation. Such advantages are continuously being discovered and analysed and we trust that some of the discoveries will give technological fruit. IBM scientists have developed a new approach to stimulate molecules on a quantum computer that may one help revolutionize chemistry and material science. For the people who look for a basic understanding of for realizing quantum computers, new technologies are being proposed. For the people who look for a basic understanding of the quantum theory and processing of information, quantum theory of computations is an integral part for them.

References:

[1]. Barenco, D. Deutsch, A. Ekert and R. Jozsa, Phys. Rev. Lett. 74, 4083 (1995).

[2]. Kitaev and J. Watrous. Parallelization, ampli_cation, and exponential time simulation of quantum interactive proof systems. In Proceedings of the 32nd ACM Symposium on the Theory of Computing, pages 608{617. ACM, New York, 2000.

[3]. Kitaev. Quantum computations: Algorithms and error correction. Russian Mathematical Surveys, 52(6), 1997.

[4]. Archil Avaliani (2002)" Quantum Computers" International University.

[5]. Biham, E., et al. (2004), 'Quantum computing without entanglement', Theoretical Computer Science, 320: 15–33.

[6]. Bub, J. (2005), 'Quantum mechanics is about quantum information', Foundations of Physics, 34: 541–560.

[7]. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. Strengths and weaknesses of quantum computing. SIAM Journal on Computing, 26(5):1510{1523, 1997.

[8]. Bennett, G. Brassard, and A. Ekert. Quantum cryptography. Scienti_c American, pages 50{57, October 1992.

[9]. Bennett. Logical reversibility of computation. IBM Journal of Research and Development, 17(6):525{532, November 1973.

[10]. Monroe, D.M. Meekhof, B.E. King, W.M. Itano and D.J. Wineland, Phys. Rev. Lett. 75, 4714 (1995).

[11]. Cirac, J.I. and Zoller, P. (1995), 'Quantum computations with cold trapped ions', Phys. Rev. Lett., 74: 4091–4094.

[12]. Boneh and R. Lipton. Quantum cryptanalysis of hidden linear functions. In Proceedings of the 15th CRYPTO Conference, volume 963 of Lecture Notes in Computer Science, pages 424{437. Springer, Berlin, 1995.

[13]. Deutsch, Proc. R. Soc. London A 400, 97 (1985).

[14]. Meyer. Quantum games and quantum algorithms. In Quantum Computation and Quantum Information Science, Contemporary Mathematics Series. American Mathematical Society, 2001. To appear.

[15]. Davis, M. (2003), 'The myth of hypercomputation', in C. Teuscher (ed.), Alan Turing, Life and Legacy of a Great Thinker, New York: Springer, pp. 195–212.

[16]. Bernstein and U. Vazirani. Quantum complexity theory. SIAM Journal on Computing, 26(5):1411{1473, 1999

[17]. http://www.ibm.com/developerworks/library/quant/index.html.

[18]. J. Balc_azar, J. D__az, and J. Gabarr_o. Structural Complexity I, volume 11 of EATCS Monographs on Theoretical Computer Science. Springer, 1988.

[19]. L. Adleman, J. DeMarrais, and M. Huang. Quantum computability. SIAM Journal on Computing, 26(5):1524{1540, 1997.

[20]. L. Fortnow. The role of relativization in complexity theory. Bulletin of the European Association for Theoretical Computer Science, 52:229{244, February 1994.

[21]. L. Li. On the counting functions. PhD thesis, University of Chicago, 1993. Department of Computer Science TR 93-12.

[22]. M. Nielsen and I. Chuang. Quantum Computation and Quantum Information. Cambridge University Press, Cambridge, United Kingdom, 2000.

[23]. P. Domokos, J.M. Raymond, M. Brune and S. Haroche, Phys. Rev. A 52, 3554 (1995).

[24]. P.W. Shor, in Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, edited by S. Goldwasser (IEEE Computer Society Press, Los Alamitos, CA), p. 124 (1994).

[25]. R. Aleliunas, R. Karp, R. Lipton, L. Lov_asz, and C. Racko_. Random walks, universal traversal sequences, and the complexity of maze problems. In Proceedings of the 20th IEEE Symposium on Foundations of Computer Science, pages 218{223. IEEE, New York, 1979.

[26]. R. Feynman, Int. J. Theor. Phys. 21, 467 (1982).

[27]. R. Landauer, Trans. R. Soc. London, Ser. A 353, 367 (1995).

[28]. S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy. Proof veri_cation and the hardness of approximation problems. Journal of the ACM, 45(3):501{555, May 1998.

[29]. S. Fenner, F. Green, S. Homer, and R. Pruim. Determining acceptance possibility for a quantum computation is hard for PH. Technical Report 98-008, Computer Science Department, Boston University, 1998.

[30]. S. Fenner, L. Fortnow, S. Kurtz, and L. Li. An oracle builder's toolkit. In Proceedings of the 8th IEEE Structure in Complexity Theory Conference, pages 120{131. IEEE, New York, 1993.

[31]. Shor, P. (1994) 'Algorithms for quantum computation: Discrete logarithms and factoring', *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*, pp. 124–134.

[32]. www.qubit.org/qubit.html.