Concept of Quantum Computing and Complexity: A New Dimension in Computational Science

Krishna Pratap Singh
Gyan Vihar University, Mahal Jagatpura, Jaipur-302017
Rajasthan, India

ABSTRACT

Since the inception of the development of Quantum theory, its weiredness has been startling physicists as well as it's researchers throughout its strange behaviour at quantum level. In the past century, there have been many drastical changes made for physical realization of this information, i.e., coding of information into physical system.

Our modern classical computer system is, thus, a practical result of this information theory. But, when it comes to do certain complex factorizing operations, the conventional computer processors fails to compromise with the time and memory resources. This is where, the term "Quantum Computing" comes in, which is a combination of quantum physics, computer science and information theory and defines a new set of computational terminologies with respect to their quantum aspects. It would outrun classical information processing theory with a modified quantum version.

In order to explain their relationship, this research paper tells about the quantum architecture of a quantum computer that begins with an introduction to classical information theory including basic building blocks of quantum information processing: quantum bits and quantum gates. It discusses about exploitation of the quantum properties of information which could perform certain types of calculations far more efficiently than any classical computer.

In the later sections of paper, it provides a deep insight over various notions of complexity, and specified quantum algorithms to perform operations within a quantum system. Quantum circuits, quantum teleportation and measurements, quantum teleportation and error-correcting coding are well described down after the topics. A special emphasis has been given to provide a model for a fault-tolerant computational system which avoids interaction of quantum processors with its surrounding that leads to information leakage, also known as 'decoherence' for a reliable quantum computer. It'll also talk about latest experimental status and progress related to the field of quantum technology which would help us in developing a practical quantum computer that well suits our requirements.

Keywords: Quantum bits, Quantum gates and registers, Quantum teleportation, Quantum algorithms and factorization, Quantum cryptography, Error-correcting codes, Fault-tolerant system and quantum architecture.

1. INTRODUCTION: CLASSICAL INFORMATION THEORY TO QUANTUM THEORY

In the past 20th century, two major theories that prevailed over all of the most influential and innovative ideas were: Quantum theory and information theory. Both of these theories reflects a vast scope in the eyes of the researchers' since their origin. The practical implementation of information theory is all before us in the form of modern computers which are based on the classical mechanical approximations applicable to a physical system and now scientists and researchers are looking forth to modify this classical information theory by exploiting the quantum principles into classical system. In present scenario, lithographic technique has made us capable to draw a micro silicon chip with advanced features by differing only a fraction of micron width. If it goes further like this, the day isn't far when we would reach a point where logical gates for processing data would happened to be operated on the atomic level, i.e, at a level where we'll need to finally approach the quantum world and it's strange theory as our all classical approximations do not hold true anymore at quantum level.

Moreover, the conventional way of computational system fails to meet the standard accuracy and computing speed when performing certain complex factorizing calculations which can be overcome by the introduction of a new technology known as *'Quantum Computing'*.

The basic principle of quantum computation is that the quantum properties can be used to represent and structure data, and that quantum mechanisms can be devised and built to perform operations with this data. For computing and processing of information, a single information to be processed is encoded into a physical system by utilizing the physical properties of that known system, following which we can compute and process any data element by encoding into a physical way. In conventional computing case, a bit is used as a physical system which can be prepared in one of the two different states representing two logical values --- no or yes, false or true, or simply 0 or 1. For example, in digital computers, the voltage between the plates in a capacitor represents a bit of information: a charged capacitor denotes bit value 1 and an uncharged capacitor bit value 0.One bit of information can be also encoded using two different polarisations of light or two different electronic states of an atom[1]. However, if we choose an atom as a physical bit then quantum mechanics tells us that apart from the two distinct electronic states the atom can be also prepared in a coherent superposition of the two states. This means that the atom is both in state 0 and state 1.

Thus likewise a classical (or conventional) computer where information is stored as bits, in a quantum computer, it is stored as *qubits* (quantum bits)[1,2].

A *qubit* is a simplest quantum system in which elementary particles are used for storing and processing of data elements, persists in superposed states of many other particular quantum states and behaves like wave nature instead of a particle at a particular moment.

For computing these informations stored in the physical system, we need a physically realizable device, i.e, a computer in common word, which works on various well designed logical gates and algorithms. So, a "*quantum computer*" is a device for computation that makes direct use of distinctively quantum mechanical phenomena, such as superposition and entanglement, to perform operations on data. Researches are still going on to make a real practical quantum computers which works on quantum platform and could give desired results. Even a real quantum computer is still have to wait for many years to be in reality as current technology is not capable to harness quantum properties through a classical computer, this paper is an attempt to shower some light on the potential quantum architecture.

In this paper, we will discuss the properties that distinguish quantum information from classical information. And we will see how these properties can be exploited in the designing of quantum algorithms that solve certain problems faster than classical algorithms can.

Thus, we will talk about quantum error-correcting codes that can be exploited to protect quantum information from *decoherence* and other potential sources of error. And we will see how coding can enable a quantum computer to perform reliably despite the inevitable effects of noise.

2. QUBITS: STANDARD BUILDING BLICKS FOR COMPUTATION

Quantum bits are the fundamental units of information in quantum information processing in much the same way that bits are the fundamental units of information for classical processing.

Just as there are many ways to realize classical bits physically (two voltage levels, lights on or off in an array, positions of toggle switches), there are many ways to realize quantum bits physically.[3]

2.1 Elementary Quantum Notation (Dirac Bra-Ket Notation):

A simple quantum system is the two-level spin- ½ particle. Its basis states, spin-down and spin-up, may be relabelled to represent binary zero and one, i.e., and, respectively. The state of a single such

particle is described by the wave-function $\psi = \alpha|0\rangle + \beta|1\rangle$. The squares of the complex coefficients and represent the probabilities for finding the particle in the corresponding states[2,3].

Therefore, for a certain superposed quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are the probability amplitudes for quantum states o and 1 respectively and square of these amplitudes gives the specific probability of element in corresponding state, i.e., $|\alpha|^2$ = Probability of element in 0 state in a quantum system or in a qubit and, $|\beta|^2$ = Probability of element in 1 state in a quantum system or in a qubit.

Similarly,
$P(0) + P(1) = 1$
Or, $|\alpha|^2 + |\beta|^2 = 1$ (1)

2.2 Qubits Implementation and Measurements

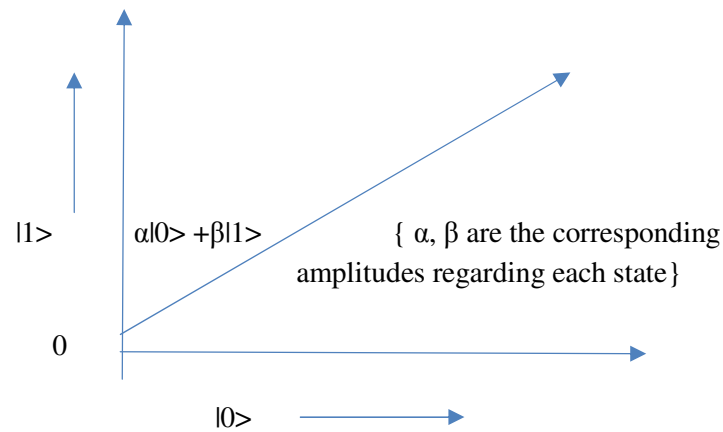

Fig 1: Graphical representation of a quantum state in a qubit

It is impossible to state exact quantum state of any particle in a quantum system in accordance with *Heisenberg's Uncertainity principle*, but we can draw partial information through calculating probability of each superposed state by squaring their amplitudes.

3. QUANTUM CIRCUITS

3.1Quantum Gates

Quantum gates provide a way for manipulating quantum information stored in the form of multiple quantum system within a single qubit. These quantum gates are analogues to their classical

counterparts but with a slight difference, i.e., it has an additional superposed state. Following are the some simplest quantum gates represented for the understanding point of view:

(a) Quantum NOT gate:

Likewise the NOT gate in classical computation, it just reverts the states with their opposites.

Fig.2: NOT gate

Input X : Output X'
If we denote NOT gate with *X* sign, then

$X(|0\rangle) = |1\rangle$ (2)

$X(|1\rangle) = |0\rangle$ and $X(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle$ (3)

(b) Hadamard gate:

This quantum gate has been devised to expand the quantum states for complex processing. If we denote *H* for showing the gate operation on a quantum state,following are the operations performed by this gate:

$H(|0\rangle) = (|0\rangle + |1\rangle)/\sqrt{2}$ (4)

$H(|1\rangle) = (|0\rangle - |1\rangle)/\sqrt{2}$ (5)

$H(\alpha|0\rangle + \beta|1\rangle) = [\ \{\alpha(|0\rangle + |1\rangle)/\sqrt{2}\} + \{\beta(|0\rangle - |1\rangle)/\sqrt{2}\}\ ]/\sqrt{2}$

$=\{(\alpha+\beta)/\sqrt{2}\}(|0\rangle) + \{(\alpha-\beta)/\sqrt{2}\}(|1\rangle)$ [4,5,7] (6)

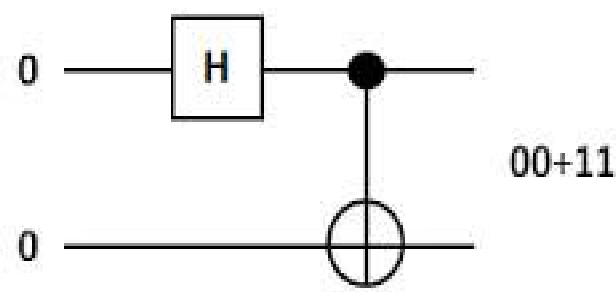

Fig. 3: Hadamard gate with two input states

(c) Rotation Gate: This rotates the plane by an angle Θ.

$$U = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

(d) Phase Flip:

Phase Flip.

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

The phase flip is a NOT gate acting in the $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ basis. Indeed, $Z|+\rangle = |-\rangle$ and $Z|-\rangle = |+\rangle$.

Fig. 5: Diagram for designing a phase flip.

3.1 Quantum Registers

Consider a register composed of three physical bits. Any classical register of that type can store in a given moment of time only one out of eight different numbers, i.e., the register can be in only one out of eight possible configurations such as 000, 001, 010, ... 111. A quantum register composed of three qubits can store in a given moment of time all eight numbers in a quantum superposition (Fig.4). This is quite remarkable that all eight numbers are physically present in the register but it should be no more surprising than a qubit being both in state 0 and 1 at the same time. If we keep adding qubits to the register we increase its storage capacity exponentially i.e. three qubits can store 8 different numbers at once, four qubits can store 16 different numbers at once, and so on; in general L qubits can store 2 numbers at once. Once the register is prepared in a superposition of different numbers we can perform operations on all of them.

For example, if qubits are atoms then suitably tuned laser pulses affect, atomic electronic states and evolve initial superpositions of encoded numbers into different superpositions. During such evolution each number in the superposition is affected and as the result we generate a massive parallel computation albeit in one piece of quantum hardware. This means that a quantum computer can in *only one* computational step perform the same mathematical operation on 2 different input numbers encoded in coherent superpositions of L qubits. In order to accomplish the same task any classical computer has to repeat the same computation 2 times or one has to use 2 different processors working in parallel. In other words a quantum registers utilizing a quantum environment to store data outruns the time and memory capacity.[7,9]

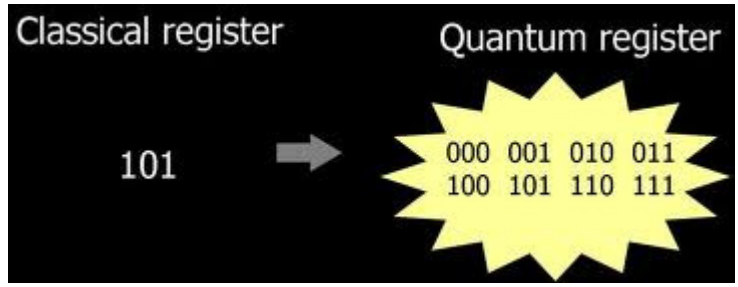

Fig 4: A pictorial representation of quantum register.

3.2 Quantum Algorithms:

In order to solve a particular problem computers follow a precise set of instructions that can be mechanically applied to yield the solution to any given instance of the problem. A specification of this set of instructions is called an algorithm.

Many quantum algorithms use quantum analogs of classical computation as at least part of their computation. Quantum algorithms often start by creating a quantum superposition and then feeding it into a quantum version *Uf* of a classical circuit that computes a function f . This setup, called *quantum parallelism*, accomplishes nothing by itself—any algorithm that stopped at this point would have no advantage over a classical algorithm—but this construction leaves the system in a state that quantum algorithm designers have found a useful starting point. Both Shor's algorithm and Grover's algorithm begin with the quantum parallelism setup.[10]

Shor's algorithm also known as Quantum fourier transform is a major initiative step for designing a quantum algorithm for factorizing a quite large string of numbers which is literally an impossible task for a normal classical computer.[14]

On the other hand, Grover's algorithm tells us about a ordered approach for searching an unsorted database with N entries in O(N1/2) time and using O(log N) storage space much faster and accurate than its classical counterpart. One can go for the references for detailed study of these algorithms provided in the last of paper as these mostly consists of mathematical concepts and calculation. [15]

4. QUANTUM TELEPORTATION

This is another aspect for quantum processing. Teleportation simply means to move any object from one place to another. In quantum analogy, this would mean movement of elementary particles from one superposing states to another.

But according to "*No Cloning Theorem*"[3], it is quite impossible to copy quantum states as well as their information. To make it possible without really violating the above said theorem, an especial quantum protocol should be generated such that it creates no any disturbance to the quantum systems under consideration during the process as it may lead even more difficult situations such as information leakage or even worse.

Most experiments have only teleported a single spin. In principle, if we can teleport one spin, then we can teleport many spins simply by repeating the experiment in series many times.

5. QUANTUM ARCHITECTURE FOR A RELIABLE QUANTUM COMPUTER

Till date, many working architectures regarding a real quantum computer have been proposed but no such reliable structure has been confirmed for a practical implementation. However, recent experiments have sparked a new hope in this direction."*Quantum-walk model*" is the latest such model which is said to be as much promising one. In this new model, a desired quantum algorithm can be implemented by letting the qubits "quantum walk" on an appropriately chosen graph, without having to control the qubits. The process is analogous to a billiard-ball computer where classical logic gates are performed using collisions.[19]

5.1 Fault-tolerant Computation Model

The discovery of quantum error correction has greatly improved the long-term prospects for quantum computing technology. Encoded quantum information can be protected from errors that arise due to uncontrolled interactions with the environment, or due to imperfect implementations of quantum logical operations. Recovery from errors can work effectively even if occasional mistakes occur during the recovery procedure. Furthermore, encoded quantum information can be processed without serious propagation of errors. In principle, an arbitrarily long quantum computation can be performed reliably, provided that the average probability of error per quantum gate is less than a certain critical value, the *accuracy threshold*[17].

Adequate use of quantum error correction and fault tolerance theoretically should enable much better scaling, but the sheer complexity of the techniques involved limits what is achievable today. The feasibility of quantum computation will increasingly depend on software tools, especially compilers, that translate quantum algorithms into low-level, technology-specific instructions and circuits with added fault tolerance and sufficient parallelism.

6. CONCLUSION AND KEY INSIGHTS FOR FUTHER RESEARCH

The idea of 'Quantum Computing' has fired many imaginations simply because the words themselves suggest something strange but powerful, as if the physicists have come up with a

second revolution in information processing to herald the next millennium. Following is, thus, a concise summary and discussion about our quantum project which needs to be furnished very clearly:

(i) In order to properly exploit the quantum features, suitable lab made molecules should be developed so that to have a greater extent of control over quantum mechanical phenomena such as, ultracold molecules below their critical temperature [18].

(ii) Though the exact quantum states of any quantum system can't be determined, atleast we would have to develop an artificial interacting model where we can keep more than only partial information about quantum information.

(iii) From a fundamental standpoint, however, it does not matter how useful quantum computation turns out to be, nor does it matter whether we build the first quantum computer tomorrow, next year or centuries from now. The quantum theory of computation must in any case be an integral part of the world view of anyone who seeks a fundamental understanding of the quantum theory and the processing of information

REFERENCES FOR FURTHER RESEARCH

[1] K. Kraus, States, Effects, and Operations: Fundamental Notions of Quantum Theory. Lecture Notes in Physics, vol. 190, Berlin: Springer-Verlag, 1983

[2] Thomas Cover and Joy Thomas: *Elements of Information Theory* .

[3] Rieffel E.G., Polak W.H.: Quantum Computing.. A Gentle Introduction (MIT, 2011)

[4] Riley T. Perry: The Temple of Quantum Computing,Version 1*:*1 - April 29, 2006

[5] Andrew Steane: Quantum Computing, july 1997.

[6] John Preskill, Quantum Computing: Pro and Con.

[7] Michael Nielsen and Isaac Chuang, *Quantum Computation and Quantum Information*.

[8] Michael Garey and David Johnson, *Computers and Intractability*.

[9] Zdzilaw Meglicki: Quantum Computing without magic devices, MIT PRESS.

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

[11] 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).

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

[13] R. Cleve, A. Ekert, C. Macchiavello and M. Mosca:Quantum Algorithms Revisited

[14] Peter W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing, 26(5):1484–1509, 1997.

[15] Grover L K. A fast quantum mechanical algorithm for database search. In: Proceedings of the 28th Annual ACM Symposium on the Theory of Computation. New York: ACM Press, 1996. 212–219

[16] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A, 53, 2046 (1996).

[17] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, Quantum Error Correction and Orthogonal Geometry, July 2, 1996.

[18] A. M. Childs, D. Gosset, Z. Webb. Universal Computation by Multiparticle Quantum Walk. Science, 2013

[19] Stefanie Barz, Joseph F. Fitzsimons, Elham Kashefi, Philip Walther. Experimental verification of quantum computation. Nature, 2013