International Journal of Scientific Engineering and Research (IJSER)
ISSN (Online): 2347-3878
Impact Factor (2020): 6.733

Quantum Computing as Emerging Computing for Future

Dr. R. Saravana Moorthy

Associate Professor (SF), Department of Computer Science, Kongunadu College of Arts and Science, Coimbatore, India

Abstract: ***Quantum computing is an emerging new field of science which uses quantum phenomena to perform operations on data. The goal of quantum computing is to find algorithms that are considerably faster than classical algorithms solving the same problem. In this paper we will talk about need of quantum computation and the advantages they offer us in compare with the classical computers. We will discuss what the elements of Quantum computing are. Along with this we will talk about the challenges to Quantum computing.***

Keywords: Quantum computing, phenomena, classical computers

1. Introduction

As of 2016, actual quantum computers are yet to be developed, but using small number of bits several experiments are carried out. Research in the field of Quantum Computing is being funded by many military agencies and national governments to develop Quantum Computers. Theoretical and practical research is on for Quantum Computing.

Problems solved by classical computers with best possible algorithms available can be solved by using Large-scale quantum computers much more quickly. Any possible probabilistic classical algorithm runs slower than Quantum algorithms like Simon's algorithm.. Any classical computer can make use of quantum algorithm as quantum computation does not violate the Church– Turingthesis.

2. Quantum Computing

In Quantum computing operations on data are performed using principle of superposition which is one of kind of quantum mechanical phenomenon. While classical or digital computers are based on transistors, Quantum computers are different from them which uses the theoretical computer science. Quantum computer makes use of qubits where classical computer works on binary digits which are either 1 or 0. The qubit can be in superposition's of states i.e. it can take any value between 0 and 1. A quantum Turing machine is called as the universal quantum computer which is a theoretical model of such computers. Quantum computers share theoretical similarities with non-deterministic and probabilistic algorithms.

3. Elements of Quantum Computing

A classical computer has worst performance than quantum computer only in few thing so it makes sense to do the bulk of the processing on the classical machine. In general we'll modify a classical computer to design a quantum computer which will have some kind of quantum circuit attached to it and some kind of interface between conventional and quantum logic.

3.1 Bits and Qubits

These are the building blocks of quantum computing. It gives the description of qubits, gates, and circuits. Quantum computers perform operations on qubits which can be in superposition of state which is an additional property and are same as bits used by classical or digital computer.

In comparison with classical computer a quantum register with 2 qubits can store 4 numbers in superposition simultaneously where classical register with 2 bits stores only 2 numbers and 300 qubit register holds more numbers than the total number of atoms in the universe. This leads to storage of infinite information at the time of computation but we can't get at it. The problem occurs at the time of reading out an output in a superposition state holding so many different values.

Superposition state collapses and we get only one value. This tantalizes us but sometimes it can work as computational advantage forus.

3.2 The Ket |>

Part of Dirac's notation is the ket (|>). The ket is just a notation for a vector. The state of a single qubit is a unit vector in C2.So,

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

is a vector, and is written as:

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

With

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

And

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

3.3 Entangled States

Subatomic particles are in entangled state which means that regardless of distance between them they are connected to each other. They show instantaneous effect on measurement with each other. This effect is useful for computational purposes.

Consider the following state (which is not entangled):

$$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$$

it can be expanded to:

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|01\rangle + 0|10\rangle + 0|11\rangle$$

Upon measuring the first qubit (a partial measurement) we get 0100% of the time and the state of the second qubit becomes:

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

giving us equal probability for a 0 or a 1.

3.4 Quantum Gates

Single Qubit Gates
Just as a single qubit can be represented by a column vector, gate acting on the qubit can be represented by a 2 x 2 matrix. The quantum equivalent of a NOT gate, for example, has the following form:

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

The only constraint these gates have to satisfy (as required by quantum mechanics) is that they have to be unitary, where a unitary matrix is one that satisfies the condition underneath. This allows for a lot of potential gates.

$$U^{\dagger}U = I.$$

Multi Qubit Gates
A true quantum gate must be reversible, this requires that multi qubit gates use a control line, where the control line is unaffected by the unitary transformation. In the case of the CNOT gate, the classical XOR with the input on the b line and the control line a. Because it is a two qubit gate it is represented by a 4 x 4 matrix:

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

3.5 Quantum Circuits

Quantum circuit is a quantum state which represents one or more qubits on which unitary operators i.e. quantum gates are applied is sequence. We now take a register and let gates act on qubits, in analogy to a conventional Circuit

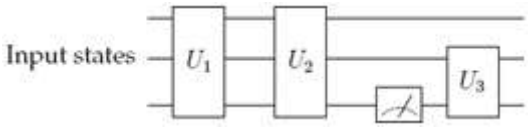

Figure 1: Generalized Quantum Circuit

This gives us a simple form of quantum circuit (above) which is a series of operations and measurements on the State of n-qubits. Each operation is unitary and can be described by a 2^n X 2^n matrix. Each of the lines is an abstract wire, the boxes containing unitary quantum logic gates or it can be a series of gates. Meter symbol is a measurement. Quantum algorithms implementation is all together this gates, wires, input, and output mechanisms.

It is always possible to rearrange quantum circuits so that all the measurements are done at the end of the circuit. Quantum circuits are one way circuits that just run once from left to right, whereas traditional classical circuits contains loops.

3.6 Quantum Computer

A quantum computer looks like this, taking n input qubits, the register V, and producing n output qubits, the register W:

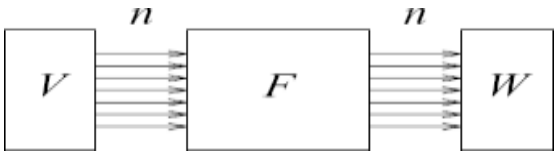

Figure 2: Basic Structure of Quantum Computer

The input register can be prepared as a superposition of states, e.g. superposition of all integers from 0 to 2can be stored in input register. The computer then calculates in parallel the function applied to all 2 integers simultaneously. From QMP (Quantum Measurement Postulate), when we measure W, according to resulting wave of qubits which is in entangled state a Boolean value for every bit from the output register is chosen. To maximize the probability that the answer we want and output we measure is same we have to design F.

4. Challenges

The challenges to build a quantum computer are enormous and can be separated in physics and engineering challenges.

The physics challenges are mainly- coherence time of output bit in super position state and qubits in entangled state and on defining ways to increase the exactness of the qubit and to compensate for the errors that occur during the quantum operations. The engineering challenge can be summarized by the word ‘scalability’. Several articles emphasis that due

to the above mentioned physical challenges, we will need a very large number of qubits in order to perform any meaningful quantum operation. For instance, in order to apply the famous factorization algorithm developed by Shor, it is expected that for the factorization of 2000bit number in sufficiently lesser time we require around 5 billion physical qubits. But we know that on today's date we can create and control maximum of 10 physical qubits, it immediately becomes clear that several breakthroughs are needed to achieve the goal of building a quantum computer. This is further illustrated by the speed at which qubit technology needs to evolve to reach the goal of billions of qubits in 30 years from now.

The engineering challenges are thus focused on the scalability by preservation of exponential computing power of qubits which means qubits are needed to be corrected and controlled. Sometimes we need to manipulate the qubit.

The quantum state of the qubit is very fragile because a qubit is in entangled. Any small interaction with the environment causes a superposition state to decohere lead by phase shift error. In addition, the superposition state gets destroyed while measuring the quantum state. This destructive reading as well as the duration and breaking of the superposition state i.e. de coherence time are the vulnerabilities of quantum computing. This qubit behavior disturbs the correct operation which is a main challenge for any quantum computer.

4 Conclusion

Quantum computation promises the ability to compute solutions to problems that, for all practical purposes, are insoluble by classical computers. However, the quantum promise is still a long way from achieving practical realization. The some properties of quantum mechanics that enable quantum computers superior performance also make the design of quantum algorithms and the construction of functional hardware extremely difficult.

We need to imply some solutions to improve the quality of qubit technology by increasing the coherence time of qubits and the speed of quantum operations. We also need to correct the state of the qubit for quantum error correction.

References

[1] Quantum Computing: A Short Course from Theory to Experiment, by Joachim Stolze, Dieter Suter, Wiley publications
[2] Bertels, K., "Quantum computing: How far away is it?," in High Performance Computing & Simulation (HPCS), 2015 International Conference on, vol., no., pp.557-558, 20-24 July2015
[3] Paler, A.; Devitt, S.J., "An introduction into fault-tolerant quantum computing," in Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE, vol., no., pp.1-6, 8-12 June2015
[4] Wu, C.H., "Qubits or Symbolic Substitutions for General-Purpose Quantum Computing?," in Information Technology - New Generations (ITNG), 2015 12th International Conference on , vol., no., pp.698-702, 13-15 April2015
[5] Barila, A., "From classical computing to quantum computing," in Development and Application Systems (DAS), 2014 International Conference on, vol., no., pp.198-203, 15-17 May2014
[6] Hahanov, V.I.; Hyduke, S.M.; Gharibi, W.; Litvinova, E.I.; Chumachenko, S.V.; Hahanova, I.V., "Quantum Models and Method for Analysis and Testing
[7] Computing Systems," in Information Technology: New Generations (ITNG), 2014 11th International Conferenceon,vol.,no.,pp.430-434,7-9April2014
[8] Kaizer Vizzotto, J., "Quantum Computing: State-of-Art and Challenges," in Theoretical Computer Science (WEIT), 2013 2nd Workshop-School on , vol., no., pp.9-13, 15-17 Oct.2013
[9] Morimae, T., "Basics and applications of measurement-based quantum computing," in Information Theory and its Applications (ISITA), 2014InternationalSymposiumon,vol.,no.,pp.327- 330, 26-29 Oct.2014
[10] Grodzinsky, F.S.; Wolf, M.J.; Miller, K.W., "Quantum computing and cloud computing: humans trusting humans via machines," in Technology and Society (ISTAS), 2011 IEEE International Symposium on , vol., no., pp.1-5, 23-25 May 2011 doi: 10.1109/ISTAS.2011.7160598
[11] Jun Hu; Chun Guan, "Granular Computing Model Based on Quantum Computing Theory," in Computational Intelligence and Security (CIS), 2014 Tenth International Conference on , vol., no., pp.157-160, 15-16 Nov. 2014. doi: 10.1109/CIS.2014.55
[12] Singh, H.; Sachdev, A., "The Quantum way of Cloud Computing," in Optimization, Reliability, and Information Technology (ICROIT), 2014. International Conference on, vol., no., pp. 397-400, 6-8 Feb. 2014. doi: 10.1109/ ICROIT.2014.6798362
[13] Ying, M.; Yuan Feng, "An Algebraic Language for Distributed Quantum Computing," in Computers, IEEE Transactions on , vol.58, no.6, pp.728-743, June 2009 doi:10.1109/TC.2009.13

Author Profile

Dr. R. Saravana Moorthy, Associate Professor (SF), Department of Computer Science. Kongunadu College of Arts and Science, Coimbatore. rsaravanamoorthy_cs@kongunaducollege.ac.in