Study of Quantum Computing

Alka Chandan[1], Ankit Naik[2], Purushottam Patel[3]
Student,CSE, Kirodimal Institute of Technology, Raigarh,India[1]
Lecturer CSE, Kirodimal Institute of Technology, Raigarh,India[2]
HOD CSE, Kirodimal Institute of Technology, Raigarh,India[3]

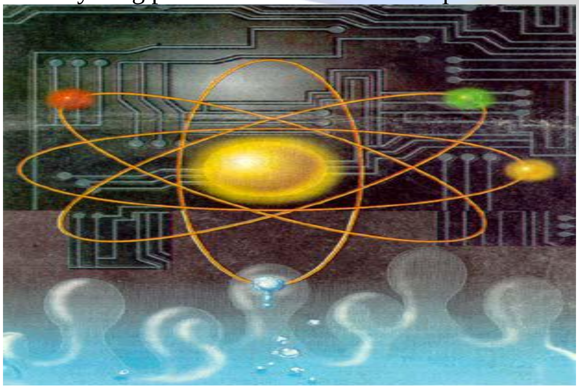
Abstract: Quantum computing is an emerging technology. The clock frequency of current computer processor systems may reach about 40 GHz within the next 10 years. By then, one atom may represent one bit. For the last fifty years computers have grown faster, smaller, and more powerful —transforming and benefiting our society in ways too numerous to count. But like any exponential explosion of resources, this growth — known as Moore's law — must soon come to an end. Research has already begun on what comes after our current computing revolution. This research paper gives an overview of quantum computers – description of their operation, differences between quantum and silicon computers.

Keywords:- Classical computers, quantum computers, quantum computer systems, Bits vs qubits , History of Quantum Computers, Languages and Quantum Computation , Moore's Law for Quantum Computers ,Future Benefits of Quantum Computers .

I. Introduction

A technology of quantum computers is also very different. For operation, quantum computer uses quantum bits (qubits). Qubit has a quaternary nature. Quantum mechanic’s laws are completely different from the laws of a classical physics. A qubit can exist not only in the states corresponding to the logical values 0 or 1 as in the case of a classical bit, but also in a superposition state.

A qubit is a bit of information that can be both zero and one simultaneously (Superposition state). Thus, a computer working on a qubit rather than a standard bit can make calculations using both values simultaneously. A qubyte, is made up of eight qubits and can have all values from zero to 255 simultaneously. “Multi-qubyte systems have a power beyond anything possible with classical computers.”



Quantum computing is essentially harnessing and exploiting the amazing laws of quantum mechanics to process information. A traditional computer uses long strings of “bits,” which encode either a zero or a one. A quantum computer, on the other hand, uses quantum bits, or qubits. What's the difference? Well a qubit is a quantum system that encodes the zero and the one into two distinguishable quantum states. But, because qubits behave quantumly, we can capitalize on the phenomena of "superposition" and "entanglement."

A quantum computer is a computation system that makes direct use of quantum-mechanical phenomena, such as superposition and entanglement, to perform operations on data.

Quantum computers are different from digital computers based on transistors. Whereas digital computers require data to be encoded into binary digits (bits), each of which is always in one of two definite states (0 or 1), quantum computation uses qubits (quantum bits), which can be in superpositions of states. A theoretical model is the quantum Turing machine, also known as the universal quantum computer.

II. Quantum Computer Systems

Superposition State:

In classical computers, electrical signals such as voltages represent the 0 and 1 states as one-bit information. Two bits indicate four states 00, 01, 10, and 11, and n bits can represent 2n states. In the quantum computer, a quantum bit called “qubit,” which is a two-state system, represents the one-bit information. For instance, instead of an electrical signal in classical computers, an electron can be used as a qubit. The spin-up and spin-down of an electron represent two states: 0 and 1, respectively. A photon can also be used as a qubit, and the horizontal and vertical polarization of a photon can be used to represent both states. Using qubits, quantum computers can perform arithmetic and logical operations as does a classical computer. The important difference, however, is that one qubit can also represent the superposition of 0 and 1 states.

Bits versus qubits: A quantum computer with a given number of qubits is fundamentally different from a classical computer composed of the same number of classical bits. For example, to represent the state of an n-qubit system on a classical computer would require the storage of 2n complex coefficients. Although this fact may seem to indicate that qubits can hold exponentially more information than their classical counterparts, care must be taken not to overlook the fact that the qubits are only in a probabilistic superposition of all of their states. This means that when the final state of the qubits is measured, they will only be found in one of the possible configurations they were in before measurement. Moreover, it is incorrect to think of the qubits as only being in one particular state before measurement since the fact that they were in a superposition of states before the measurement was made directly affects the possible outcomes of the computation. Qubits are made up of controlled particles and the means of control (e.g. devices that trap particles and switch them from one state to another).

For example: Consider first a classical computer that operates on a three-bit register. The state of the computer at any time is a probability distribution over the different three-bit strings 000, 001, 010, 011, 100, 101, 110, 111. If it is a deterministic computer, then it is in exactly one of these states with probability 1. However, if it is a probabilistic computer, then there is a possibility of it being in any one of a number of different states. We can describe this probabilistic state by eight nonnegative numbers A,B,C,D,E,F,G,H (where A = probability computer is in state 000, B = probability computer is in state 001, etc.). There is a restriction that these probabilities sum to 1.

The state of a three-qubit quantum computer is similarly described by an eight-dimensional vector (a,b,c,d,e,f,g,h), called a ket. Here, however, the coefficients can have complex values, and it is the sum of the squares of the coefficients' magnitudes, , that must equal 1. These square magnitudes represent the probability amplitudes of given states. However, because a complex number encodes not just a magnitude but also a direction in the complex plane, the phase difference between any two coefficients (states) represents a meaningful parameter. This is a fundamental difference between quantum computing and probabilistic classical computing.

III. HISTORY OF QUANTUM COMPUTERS

In 1982 R.Feynman presented an interesting idea how the quantum system can be used for computation reasons. He also gave an explanation how effects of quantum physics could be simulated by such quantum computer. This was very interesting idea which can be used for future research of quantum effects. Every experiment investigating the effects and laws of quantum physics is complicated and expensive. Quantum computer would be a system performing such experiments permanently. Later in 1985, it was proved that a quantum computer would be much more powerful than a classical one.

IV. LANGUAGES AND QUANTUM COMPUTATION

The quantum computation model, has been through, and still exists in, many forms. Classical computation models such as the Turing machine, Lambda calculus,and circuit representation have all been extended to encompass quantuminformation. Currently, the most efficient forms of representation of quantum algorithms include the circuit model and the associated operator calculus. In this model, quantum bits are manipulated by abstracted operators which have a mathematical construction independent of implementation.

From this model, multiple quantum computing languages have been developed which attempt to provide a complete framework for simulating and verifying algorithms within the circuit-operator model. From experience in working with quantum computing languages as well as from a theoretical standpoint, computer scientists have constructed the following list of requirements which any useful quantum computing language must satisfy.

• Abstracted Quantum Model

Any language must provide a high level construction to allow programmers to develop modular, intuitive, and compact code. Thus, the language must have some automated mechanism for translation to a sequence of low level instructions for a quantum machine.

• Hardware Independence

Any quantum computing language must not make reference to the hardware of the quantum machine, only the operators which any quantum machine should be capable of. The automated translation to low level instructions may take responsibility for this independent of the programmer and his code.

• Quantum Registers

There are three basic operations that a quantum register (qureg) must be able to perform for the user.

• Allocation and Deallocation

This will likely only involve the addressing and scoping of a qureg.

• Quantum Operators

Operators may have a number of possible implementations. Properties of operators within languages which contributed to readable, efficient code are described below.Low Level

Operators Common operators which must form a complete set (redundancy is fine) should be quickly accessible. Operator Composition From these low level operators, higher level operators can be constructed through composition. Thus, a user may conjugate many operators into a single operator which may be used more than once. Operator Inversion Because all quantum operators must be unitary they must be reversible. Inverting an operator should be easy and accessible.

•Moore's Law for Quantum Computers

According to Moore's Law, the number of transistors of a microprocessor continues to double in every 18 months. According to such evolution if there is a classical computer in year 2020, it will run at 40 GHz CPU speed with 160 Gb RAM. If we use an analogue of Moor’s law for quantum computers, the number of quantum bits would be double in every 18 months. But adding just one qubit is already enough to double a speed. So, the speed of quantum computer will increase more than just doubling it.

V. The Major Difference between Quantum and Classical Computers

The memory of a classical computer is a string of 0s and 1s, and it can perform calculations on only one set of numbers simultaneously. The memory of a quantum computer is a quantum state that can be a superposition of different numbers. A quantum computer can do an arbitrary reversible classical computation on all the numbers simultaneously. Performing a computation on many different numbers at the same time and then interfering all the results to get a single answer, makes a quantum computer much powerful than a classical one.

VI. Future Benefits of Quantum Computers

1. Cryptography and Peter Shor’s Algorithm

In 1994 Peter Shor (Bell Laboratories) found out the first quantum algorithm that, in principle, can perform an efficient factorization. This became a complex application that only a quantum computer could do. Factoring is one of the most important problems in cryptography. For instance, the security of RSA (electronic banking security system) - public key cryptography - depends on factoring and it is a big problem. Because of many useful features of quantum computer, scientists put more efforts to build it. However, breaking any kind of current encryption that takes almost centuries on existing computers, may just take a few years on quantum computer.

2. Artificial Intelligence

It has been mentioned that quantum computers will be much faster and consequently will perform a large amount of operations in a very short period of time. On the other side, increasing the speed of operation will help computers to learn faster even using the one of the simplest methods - mistake bound model for learning.

3. Other Benefits

High performance will allow us in development of complex compression algorithms, voice and image recognition, molecular simulations, true randomness and quantum communication. Randomness is important in simulations. Molecular simulations are important for developing simulation applications for chemistry and biology. With the help of quantum communication both receiver and sender are alerted when an eavesdropper tries to catch the signal. Quantum bits also allow more information to be communicated per bit. Quantum computers make communication more secure.

VII. Limitations of Quantum Computing

Beals et al. proved that, for a broad class of problems, quantum computation cannot provide any speed-up. Their methods were used by othersto provide lower bounds for other types of problems. Ambainis found another powerful method for establishing lower bounds. In 2002, Aaronson showed that quantum approaches could not be used to efficiently solve collision problems. This result means there is no generic quantum attack oncryptographic hash functions. Shor’s algorithms break some cryptographic hash functions, and quantum attacks on others may still be discovered, but Aaronson’s result says that any attack must use specific properties of the hash function under consideration.

VIII. The Potential and Power of Quantum Computing

Quantum computer with 500 qubits gives 2500 superposition states. Each state would be classically equivalent to a single list of 500 1's and 0's. Such computer could operate on 2500 states simultaneously. Eventually, observing the system would cause it to collapse into a single quantum state corresponding to a single answer, a single list of 500 1's and 0's, as dictated by the measurement axiom of quantum mechanics. This kind of computer is equivalent to a classical computer with approximately 10150 processors.

IX. CONCLUSION

It is important that making a practical quantum computing is still far in the future. Programming style for a quantum computer will also be quite different. Development of quantum computer needs a lot of money. Even the best scientists can’t answer a lot of questions about quantum physics. Quantum computer is based on theoretical physics and some experiments are already made. Building a practical quantum computer is just a matter of time. Quantum computers easily solve applications that can’t be done with help of today’s computers. This will be one of the biggest steps in science and will undoubtedly revolutionize the practical computing world.

REFERENCES

[1]. Y. Kanamori,! S.-M. Yoo,! W.D. Pan,! and F.T. Sheldon!! ’’ A SHORT SURVEY ON QUANTUM COMPUTERS’’ International Journal of Computers and Applications, Vol. 28, No. 3, 2006

[2]. C.P. Williams & S.H. Clearwater, Exploration in quantum computing (New York: Springer-Verlag, 1997).

[3]. P.W. Shor, Algorithm for quantum computation: Discrete logarithm and factoring, Proc. 35th IEEE Annual Symp. On Foundations of Computer Science, Santa Fe, NM, November 1994, 24–134.

[4]. M. Oskin, F.T. Chong, & I. Chuang, A practical architecture for reliable quantum computers, IEEE Computer, January 2002, 79–87.

[5]. Quantum Computers & Moore's Law. Retrieved on December 1st, 2002 from: http://www.qubyte.com

[6]. Daniel, G. (1999). Quantum Error-Correcting Code Retrieved on November 31st, 2002 from:http://qso.lanl.gov/~gottesma/QECC.html

[7]. Manay, K. (1998). Quantum computers could be a billion times faster than Pentium III. USA Today. Retrieved on December 1st, 2002 from: http://www.amd1.com/quantum_computers.html

[8]. Scott Aaronson ‚Dave Bacon’’ Quantum Computing and the Ultimate Limits of Computation: The Case for a National Investment’’ Version 6: December 12, 20081

[9]. Cris Cecka, “Review of Quantum Computing Research” Summer 2005

[10]. M. Nielson, I. Chuang, Quantum Computation and Quantum Information (Cambridge Univ. Press, Cambridge, 2000)

[11]. D’Hondt, Ellie and Prakash Panangaden. Quantum weakest preconditions. Proc. QPL 2004, pp. 75-90

[12]. Quantum Computing by Eleanor Rieffel

[13]. http://en.wikipedia.org/wiki/Quantum_computer

[14]. https://uwaterloo.ca/institute-for-quantum-computing/quantum-computing-101