Annals of R.S.C.B., ISSN:1583-6258, Vol. 23, Issue 2, 2019, Pages. 175 - 181
Received 15 October 2019; Accepted 22 December 2019.

Information in Quantum Computers – The Qubit

Shenbagam,Assistant Professor, Dhanalakshmi Srinivasan College of Engineering and Technology

Nandhini Devi, Assistant Professor, Department of Information Technology, Dhanalakshmi Srinivasan College of Engineering and Technology

Abstract

Today's computers work on bits that exist as either 0 or 1. Quantum computers aren't limited to two states; they encode information as quantum bits, or qubits, which can exist in superposition. Qubits represent atoms, ions, photons or electrons and their respective control devices that are working together to act as computer memory and a processor. Because a quantum computer can contain these multiple states simultaneously, it has the potential to be millions of times more powerful than today's most powerful supercomputers. A processor that can use registers of qubits will be able to perform calculations using all the possible values of the input registers simultaneously. This superposition causes a phenomenon called quantum parallelism, and is the motivating force behind the research being carried out in quantum computing. Due to technical obstacles, till date, a quantum computer has not yet been realized. But the concepts and ideas of quantum computing has been demonstrated using various methods like NMR, Ion Trap, Quantum Dot, Optical Methods, etc. A quantum computer manipulates qubits by executing a series of quantum gates, each a unitary transformation acting on a single qubit or pair of qubits. In applying these gates in succession, a quantum computer can perform a complicated unitary transformation to a set of qubits in some initial state. The qubits can then be measured, with this measurement serving as the final computational result. Research must devise a way to maintain decoherence and other potential sources of error at an acceptable level. Probably the most important idea in this field is the application of error correction in phase coherence as a means to extract information and reduce error in a quantum system without actually measuring that system. Thereby, quantum computers will emerge as the superior computational devices and perhaps one day make today's modern computer obsolete.

Keywords – Qubits, superposition, parallelism, coherence, entanglement, quantum gates, decoherence, NMR, quantum dots.

Received 15 October 2019; Accepted 22 December 2019.

INTRODUCTION

Gershenfeld says that if making transistors smaller and smaller is continued with the same rate as in the past years, then by the year of 2020, the width of a wire in a computer chip will be no more than a size of a single atom. These are sizes for which rules of classical physics no longer apply. If the transistors become much smaller, the strange effects of quantum mechanics will begin to hinder their performance. In 1982, the Nobel prize-winning physicist Richard Feynman thought up the idea of a 'quantum computer', a computer that uses the effects of quantum mechanics to its advantage. For some time, the notion of a quantum computer was primarily of theoretical interest only, but recent developments have bought the idea to everybody's attention. One such development was the invention of an algorithm to factor large numbers on a

quantum computer, by Peter Shor (Bell Laboratories). By using this algorithm, a quantum computer would be able to crack codes much more quickly than any ordinary (or classical) computer could. In fact, a quantum computer capable of performing Shor's algorithm would be able to break current cryptography techniques in a matter of seconds. With the motivation provided by this algorithm, the topic of quantum computing has gathered momentum and researchers around the world are racing to be the first to create a practical quantum computer. According to Chuang a supercomputer needs about a month to find a phone number from the database consisting of world's phone books, where a quantum computer is able to solve this task in 27 minutes.

Massachusetts Institute of Technology, Oxford University, IBM and Los Alamos National Laboratory are the most successful in development of quantum computer.

NEED OF QUANTUM COMPUTER

Quantum computer with 500 qubits gives2^{500}superposition states. Each state would be classically equivalent toa single list of 500 1's and 0's. Such computer could operate on 2^{500}states simultaneously. Eventually, observingthe system would cause it to collapse into a single quantum state corresponding to a single answer, a single listof 500 1's and 0's, as dictated by the measurement axiom of quantum mechanics. This kind of computer isequivalent to a classical computer withapproximately10^{150}processors. Integer factorization is believed to be computationally infeasible with an ordinary computer for large integers if they are the product of few prime numbers (e.g., products of two 300-digit primes). By comparison, a quantum computer could efficiently solve this problem using Shor's algorithm to find its factors. This ability would allow a quantum computer to decrypt many of the cryptographic systems in use today. In particular, most of the popular public key ciphers are based on the difficulty of factoring integers. These are used to protect secure Web pages, encrypted email, and many other types of data. Breaking these would have significant ramifications for electronic privacy and security. An example of this is a password cracker that attempts to guess the password for an encrypted file (assuming that the password has a maximum possible length).

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.

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.

These are the most important applications currently known:

- Cryptography: Perfectly secure communication.
- Searching, especially algorithmic searching (Grover's algorithm).
- Factorizing large numbers very rapidly (Shor's algorithm).
- Simulating quantum-mechanical systems efficiently.

QUANTUM COMPUTER BASICS

In the classical model of a computer, the most fundamental building block, the bit, can only exist in one of two distinct states, a 0 or a 1. In a quantum computer the rules are changed. Not only can a 'quantum bit', usually referred to as a 'qubit', exist in the classical 0 and 1 states, it can also be in a coherent superposition of both. When a qubit is in this state it can be thought of as existing in two universes, as a 0 in one universe and as a 1 in the other. An operation on such a qubit effectively acts on both values at the same time. The significant point being that by performing the single operation on the qubit, we have performed the operation on two different values. Likewise, a two-qubit system would perform the operation on 4 values, and a three-qubit system on eight. Increasing the number of qubits therefore exponentially increases the 'quantum parallelism' we can obtain with the system. With the correct type of algorithm, it is possible to use this parallelism to solve certain problems in a fraction of the time taken by a classical computer. The characteristic feature of quantum computing is quantum parallelism. A quantum system is in general not in one "classical state", but in a "quantum state" consisting (crudely speaking) of a superposition of many classical or classical-like states. Superposition does not mean we could drop all but one of the classicallike states (after deducing retrospectively which one was "the right one") and still get the time evolution right. But actually, we need the whole superposition to get the time evolution right. The system really is in some sense in all the classical-like states at once! If the superposition can be protected from unwanted entanglement with its environment (known as decoherence), a quantum computer can output results dependent on details of all its classical-like states. This is quantum parallelism - parallelism on a serial machine. But unlike classical bits, qubits can exist simultaneously as o and 1, with the probability for each state given by a numerical coefficient; describing a two-qubit quantum computer thus requires four coefficients. In general, n qubits demand2^nnumbers, which rapidly becomes a sizable set for larger values of n. For example, if n equals 50, about2^{15}numbers are required to describe all the probabilities for all the possible states of a quantum machine – a number that exceeds the capacity of the largest conventional computer, a quantum computer promises to be immensely powerful because it can be in multiple states at once-a phenomenon called superposition—and because it can act on all its possible states simultaneously. Thus, a quantum computer could naturally perform myriad operations in parallel, using a single processing unit. A quantum computer operates by setting the qubits in a controlled initial state that represents the problem at hand and by manipulating those qubits with a fixed sequence of quantum logic gates. The sequence of gates to be applied is called a quantum algorithm. The calculation ends with measurement of all the states, collapsing each qubit into one of the two pure states, so the outcome can be at most classical bits of information.

In order to do this, we use certain Quantum Mechanical concepts like:

1) Superposition

2) Entanglement

3) Parallelism

In any quantum mechanical system, a particular state of the system is represented by a mathematical function called as the wave function of that state. A wave function is a complex exponential which includes all possible phases of existence of that particular state. Considering any quantum mechanical system, let ψ1 and ψ2 be two wave functions that represent any two independent states ofthe system. Then quantum mechanics tells us that there exists a state of the same system that can be represented by the wave function c1ψ1 + c2ψ2. This state is called as a superposition of the two states represented by ψ1 and ψ2. It means that the system would be in both the states of ψ1 and ψ2 simultaneously. All superposition of two quantum states of a system are not stable. If the superposition is to be stable, then there should be some sort of coherence between the two states that are being super positioned. Such a superposition is called as a coherent superposition. There can be more than one coherent superposition for a pair of states of a quantum mechanical system.

The importance of coherent-super positioned storage can be understood from the following example. 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. Consider the case of a quantum register at that place. Since a qubit can store both the values of 0 & 1 simultaneously, a quantum register composed of three qubits can store in a given moment of time all the eight numbers in a quantum superposition. The catch is that the memory size grows exponentially when additional bits are added compared to the linear growth in classical computers. Also, once the register is prepared in such a superposition, operations can be performed on all the numbers simultaneously.

We have seen that once a 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 superposition of encoded numbers into different superposition. 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 2L different input numbers encoded in coherent superposition of L qubits. In order to accomplish the same task, any classical computer has to repeat the same computation 2L times or one has to use 2L different processors working in parallel. In other words, a quantum computer offers an enormous gain in the use of computational resources such as time and memory.

CONCEPT OF INFORMATION IN QUANTUM COMPUTERS – THE QUBIT

In quantum computers also, the basic unit of information is a bit. The concept of quantum computing first arose when the use of an atom as a bit was suggested. If we choose an atom as a physical bit then quantum mechanics tells us that apart from the two distinct electronic states (the excited state and the ground state), the atom can be also prepared in what is known as a coherent superposition of the two states. This means that the atom can be both in state 0 and state 1 simultaneously. It is at this point that the concept of a quantum bit or a qubit arises. This concept is the backbone of the idea of quantum computing. 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. 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).

POSTULATES OF QUANTUM COMPUTING

An important distinction needs to be made between quantum mechanics, quantum physics and quantum computing. Quantum mechanics is a mathematical language, much like calculus. Just as classical physics uses calculus to explain nature, quantum physics uses quantum mechanics to explain nature. As classical computers can be thought of in Boolean algebra terms, quantum computers are reasoned about with quantum mechanics. There are four postulates to quantum mechanics, which will form the basis of quantum computers:

Postulate 1: Definition of a quantum bit, or qubit.
Postulate 2: How qubit(s) transform (evolve).
Postulate 3: The effect of measurement. **Postulate 4:** How qubits combine together into systems of qubits.

CONCLUSION

The quantum computers power to perform calculations across a multitude of parallel universes gives it the ability to quickly perform tasks that classical computers will never be able to practically achieve. This power can only be unleashed with the correct type of algorithm, a type of algorithm that is extremely difficult to formulate. Some algorithms have already been invented; they are proving to have huge implications on the world of cryptography. This is because they enable the most commonly used cryptography techniques to be broken in a matter of seconds. Ironically, a spin-off of quantum computing, quantum communication allows information to be sent without eavesdroppers listening undetected. For now at least, the world of cryptography is safe because the quantum computer is proving to be very difficult to implement. The very thing that makes them powerful, their reliance on quantum mechanics, also makes them extremely fragile. The most successful experiments only being able to add one and one together. Nobody can tell if the problems being experienced by researchers can be overcome, some like Dr. Gershenfield are hopeful that they can whilst others believe that the quantum computer will always be too fragile to be practical. 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.

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. The Fabric of Reality. David Deutsch
2. Physics - A Textbook for Advanced Level Students. Tom Duncan A brief introduction to elementary quantum physics
3. Algorithmics - The Spirit of Computing. David Harel
4. A quantum revolution for computing. Julian Brown, New Scientist 24/9/94
5. The best computer in all possible worlds. Tim Folger, Discover 1/10/95
6. Cue the qubits: Quantum computing - How to make a quantum computer.
7. Quantum keys for keeping secrets. Artur Ekert, New Scientist Volume 137