Journal of Information and Operations Management
ISSN: 0976–7754 & E-ISSN: 0976–7762 , Volume 3, Issue 1, 2012, pp-236-240
Available online at http://www.bioinfo.in/contents.php?id=55

QUANTUM COMPUTERS: A NEW BOON IN COMPUTATION

AMIT CHAUHAN[1*], VISHAL BHATNAGAR[2], VINEET CHAUHAN[1] AND GAGANDEEP SINGH[2]

[1]Department of Computer Science, Phonics School of Engineering, Roorkee, Uttrakhand, India.
[2]Department of ECE, Phonics School of Engineering, Roorkee, Uttrakhand, India.
*Corresponding Author: Email- go.chauhan@gmail.com.

Received: December 12, 2011; Accepted: January 15, 2012

Abstract- The paper describe, the model underlying information and computation from a conventional mechanical to a quantum mechanical one way faster algorithms, original cryptographic mechanisms, and another methods of communication. Quantum algorithms can perform a select set of tasks very much more efficiently than any traditional algorithm, but for many tasks it has been established that quantum algorithms provide benefit for the technology.

Keywords- Quantum Computer, Qubit, Decoherence, Cryptography

Citation: Amit Chauhan, Vishal Bhatnagar, Vineet Chauhan And Gagandeep Singh (2012) Quantum Computers: A New Boon in Computation. Journal of Information and Operations Management ISSN: 0976–7754 & E-ISSN: 0976–7762, Volume 3, Issue 1, pp-236-240.

Introduction

A quantum computer is a device for computation that makes direct use of quantum mechanical phenomena, such as superposition and entanglement, to perform operations on data. Quantum computers are different from traditional computers based on transistors. The basic principle behind quantum computation is that quantum properties can be used to represent data and perform operations on these data.

Quantum computers share theoretical similarities with non-deterministic and probabilistic computers, like the ability to be in more than one state simultaneously. The field of quantum computing was first introduced by RICHARD FEYNMAN in 1982.

Changing the model underlying information and computation from a classical mechanical to a quantum mechanical one provide a way faster algorithms, novel cryptographic mechanisms, and alternative methods of communication. Quantum algorithms can perform a select set of tasks vastly more efficiently than any classical algorithm, but for many tasks it has been proven that quantum algorithms provide no advantage. The breadth of quantum computing applications is still being explored. Major application areas include security and the many fields that would benefit from efficient quantum simulation. The quantum information processing viewpoint provides insight into classical algorithmic issues as well as a deeper understanding of mess and other non-classical aspects of quantum physics. Quantum computation explores how efficiently nature allows us to compute.

The standard model of computation is grounded in classical mechanics; the Turing machine is described in classical mechanical terms. In the last two decades of the twentieth century, researchers recognized that the standard model of computation placed redundant limits on computation. Our world is inherently quantum mechanical. By placing computation on a quantum mechanical foundation faster algorithms, novel cryptographic mechanisms, and alternative methods of communication have been found. Quantum information processing, a field that includes quantum computing, quantum cryptography, quantum communication, and quantum games, examines the implications of using a quantum mechanical model for information and its processing. Quantum information processing changes not only the physical processes used for computation and communication, but the very notions of information and computation themselves.

What is Quantum Computing - In quantum computers we exploit quantum effects to compute in ways that are faster or more efficient than, or even impossible, on conventional computers.

Quantum computers use a specific physical implementation to gain a computational advantage over conventional computers. Properties called superposition and entanglement may, in some cases, allow an exponential amount of parallelism. Also, special purpose machines like quantum cryptographic devices use entanglement and other peculiarities like quantum uncertainty.

Quantum computing combines quantum mechanics, information theory, and aspects of computer science. The field is a relatively new one that promises secure data transfer, dramatic computing speed increases, and may take component miniaturization to its fundamental limit. The above texts explain some of the introductory aspects of quantum computing.

We will examine some basic quantum mechanics, elementary quantum computing topics like qubits, quantum algorithms, physical realizations of those algorithms, basic concepts from computer science (like complexity theory, Turing machines, and linear algebra), information theory, and more.

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. . In general a quantum computer with *n* qubits can be in an arbitrary superposition of up to 2^n different states simultaneously (this compares to a normal computer that can only be in *one* of these 2^n states at any one time). A quantum computer operates by manipulating those qubits with a fixed sequence of quantum logic gates.. The sequence of gates to be applied is called a quantum algorithm. 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

Bits Vs Quantum Bits Or Qubits

Quantum computers perform operations on qubits which are analogous to conventional bits but they have an additional property in that they can be in a superposition. The amount of information stored during the "computational phase" is essentially Infinite - it's just that we can't get at it. The inaccessibility of the information is related to quantum measurement: When we attempt to readout a superposition state holding many values the state collapses and we get only one value (the rest get lost).

Classical computers use two discrete states (e.g. states of charging of a capacitor) to represent a unit of information, this state is called a binary digit (or bitfor short). A bit has the following two values:

0 and 1.

There is no intermediate state between them, i.e. the value of the bit cannot be in a superposition.

Quantum bits, or *qubits*, can on the other hand be in a state "between" 0 and 1, but only during the computational phase of a quantum operation. When

measured, a qubit can become either$|0\rangle$or $|1\rangle$ i.e. we readout 0 or 1. This is the same as saying a spin particle can be in a superposition state but, when measured, it shows only one value. In terms of the above it essentially means the same thing as 0 and 1, just like a classical bit. Generally, a qubit's state during the computational phase is represented by a linear combination of states otherwise called a superposition state.$\alpha|0\rangle+ \beta|1\rangle$.Here α and β are the probability amplitudes. They can be used to calculate the probabilities of the system jumping into $|0\rangle$or $|1\rangle$following a measurement or readout operation. There may be, say a 25% chance a 0 is measured and a 75% chance a 1 is measured. The percentages must add to 100%. In terms of theirrepresentation qubits must satisfy:$|\alpha|2 + |\beta|2 = 1$.

This the same thing as saying the probabilities adds to 100%.Once the qubit is measured it will remain in that state if the same measurement is repeated provided the system remains closed between measurements. The probability that the qubit's state, when in a superposition, will collapse to states $|0\rangle$or $|1\rangle$is

$|\alpha|2$ for $|0\rangle$and$|\beta|2$ for $|1\rangle$.

$|0\rangle$and $|1\rangle$are actually vectors, they are called the computational basis states that form an orthonormal basis for the vector space C2.

The Quantum Gates

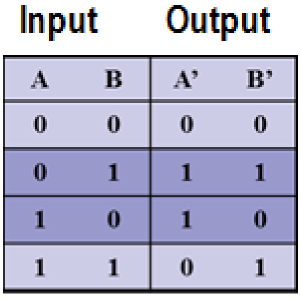
Due to the nature of quantum physics, the destruction of information in a gate will cause heat to be evolved which can destroy the superposition of qubits so the normal AND, OR & NOT GATES cannot be used here. Hence we need a gate with some REVERSIBLE LOGIC so that the previous information must not be destroyed and kept intact.

This means that a deterministic computation can be performed on a quantum computer only if it is reversible.

Listed below are some of the common reversible gates and their truth tables.

Controlled Not

Like a NOT gate (on *b*) but with a control line, *a*. *b'* can also be expressed as *a* XOR *b*.

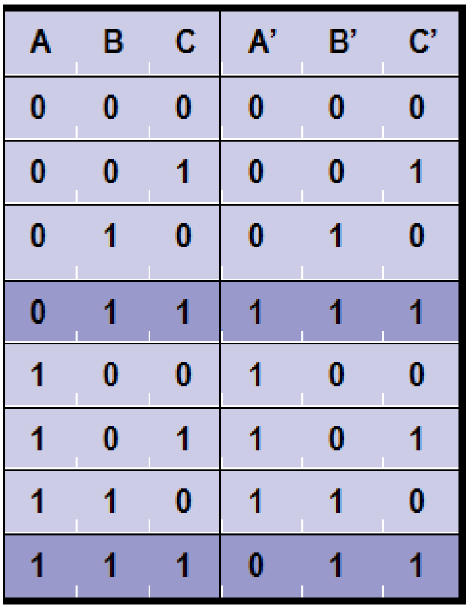


Input		Output	
A	B	A’	B’
0	0	0	0
0	1	1	1
1	0	1	0
1	1	0	1

Table1- Truth table

Properties of the CNOT gate, CNOT(*a, b*):CNOT(*x*, 0) : *b'* = *a'* = *a* = FANOUT

Table2- Truth table



A	B	C	A’	B’	C’
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	1	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	0
1	1	1	0	1	1

Toffoli Gate

If the two control lines are set it flips the third bit (i.e. applies NOT). The Toffoli gate is also called a controlled-controlled NOT.

Properties of the Toffoli Gate, *TF* (*a, b, c*):
TF (*a, b, c*) = (*a, b, c* XOR(*a* AND *b*)).
TF (1, 1, *x*) : *c'* = NOT *x.*
TF (*x, y*, 1) : *c'* = *x* NAND *y.*
TF (*x, y*, 0) : *c'* = *x* AND *y.*
TF (*x*, 1, 0) : *c'* = *a* = *a'* = FANOUT.

Entanglement of Quantum Systems

According to quantum mechanics an outside force acting on two particles of the quantum system can cause them to become entangled. The quantum state of this system can contain all positions of spins (internal magnetic moments) of each particle. The total spin of the system can only be equal to certain discrete values with different probabilities. Measurements of total spin of certain quantum systems showed that positions of spins of some particle are not independent from others. For such systems, when an orientation of a spin of one particle changed by some reason, an orientation of a spin of another particle changes automatically and instantly. The laws that that have been developed so far about the speed of light are disobeyed in this case, because the change in an orientation of a spin happens immediately. At least there is hypothesizing to use these phenomena for quantum computing. It is well known that a speed of communication is limited by a speed of light as nothing can travel faster than the speed of light. The question is how particles of the quantum system communicate when they change their spin orientation and consequently their vector states. Famous scientists spent a lot of time discussing this issue. Einstein’s idea that some unknown “hidden parameters” of quantum system were contributing to this effect has been rejected theoretically and experimentally. This is one of the example showing the difference between classical and quantum realities. This effect of the quantum system explains a lot of aspects of the nature (f.e. chemical characteristics of atoms and molecules) and is proved by the experiments.

“In fact, theories about entanglement have led scientists to believe there could be a way to speed up computing. Even today's computers are nearing a point at which their speed is being limited by how fast an electron can move through a wire - the speed of light. Whether in a quantum or traditional computer, entanglement could blow past that limit.”

The Major Between Quantum And Classical Computerst

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.

Future Benefits Of Quantum Computers

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.

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.

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.

Shor’s Algorithm

Shor’s algorithm shows (in principle,) that a quantum computer is capable of factoring very large numbers in polynomial time. The algorithm is dependent on:

- Modular Arithmetic
- Quantum Parallelism
- Quantum Fourier Transform

Shor’s Algorithm - In Depth Analysis

This is an algorithm invented by Peter Shor in 1995 that can be used to quickly factorize large numbers. If it is ever implemented it will have a profound effect on cryptography, as it would compromise the security provided by public key encryption (such as RSA).

Shor's algorithm - An example

The purpose of this section is to illustrate the basic steps involved in Shor's Algorithm. In order to keep the example relatively easy to follow we will consider the problem of finding the prime factors of the number 15. Since the Algorithm consists of three key steps, this explanation will be presented in 3 stages.

Stage 1

The first stage of the algorithm is to place a memory register into a coherent superposition of all its possible states. The letter 'Q' will be used denote a qubit that is in the coherent state.

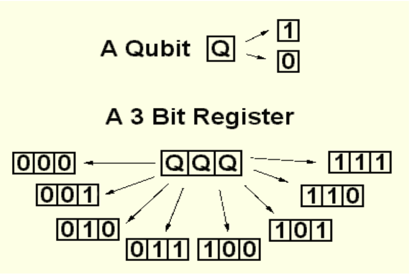


Fig.1- A three-qubit register can represent 8 classical states simultaneously.

When a qubit is in the coherent state, it can be thought of as existing in two different universes. In one universe it exists as a '1' and in the other it exists as a '0' (See Figure 1). Extending this idea to the 3 bit register we can imagine that the register exists in 8 different universes, one for each of the classical states it could represent (i.e. 000, 001, 010, 011, 100, 101, 110, 111). In order to hold the number 15, a four bit register is required (capable of representing the numbers 0 to 15 simultaneously in the coherent state). A calculation performed on the register can be thought of as a whole group of calculations performed in parallel, one in each universe. In effect, a calculation performed on the register is a calculation performed on every possible value that register can represent.

Stage 2

The second stage of the algorithm performs a calculation using the register. The details of which are as follows:

- The number *N* is the number we wish to factories, *N* = 15.
- A random number *X* is chosen, where 1 <*X*<*N*-1
- *X* is raised to the power contained in the register (register A) and then divided by *N.*
- The remainder from this operation is placed in a second 4 bit register.

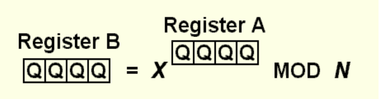


Fig.2- Operation performed in stage 2.

After this operation has been performed, register B contains the superposition of each universes results. This is best illustrated with an example, if we choose *X* to be 2, then the contents of register B, for every possible value in register A are as follows.

Stage 3

The final stage is perhaps the most difficult to follow. The frequency of repetition, *f*, can be found using a quantum computer. This is done by performing a complex operation on register B and then looking at its contents which causes the results from every universe to interfere with each other. The resulting value for f is then used in the following equation to calculate a (possible) factor.

$$\text{Factor P} = X^{\frac{f}{2}} - 1$$

Fig. 3 -Equation used to calculate factor.

In our example the value *f* = 4 does give a correct answer of 3.The fact that the answer cannot be guaranteed to be correct is of little consequence as it can be easily checked with multiplication. If the answer is incorrect, there is a very strong chance that repeating the calculation a few times with different values of *X* will produce the right answer.

The resulting number cannot be guaranteed to be a prime factor, but there is a good chance that it is one. The interference that produces the value for *f* tends to favour the correct answer as incorrect answers cancel each other out.

Quantum Decoherence

One of the greatest challenges is controlling or removing quantum decoherence. This usually means isolating the system from its environment as the slightest interaction with the external world would cause the system to decohere. This effect is irreversible, as it is non-unitary, and is usually something that should be highly controlled, if not avoided. Decoherence times for candidate systems, in particular the transverse relaxation time T_2 typically range between nanoseconds and seconds at low temperature.

These issues are more difficult for optical approaches as the timescales are orders of magnitude shorter and an often-cited approach to overcoming them is optical pulse shaping. Error rates are typically proportional to the ratio of operating time to decoherence time, hence any operation must be completed much more quickly than the decoherence time.

If the error rate is small enough, it is thought to be possible to use quantum error correction, which corrects errors due to decoherence, thereby allowing the total calculation time to be longer than the decoherence time. An often cited figure for required error rate in each gate is 10^{-4}. This implies that each gate must be able to perform its task in one 10,000th of the decoherence time of the system.

Meeting this scalability condition is possible for a wide range of systems. However, the use of error correction brings with it the cost of a greatly increased number of required qubits. The number required to factor integers using Shor's algorithm is still polynomial, and thought to be between L and L^2, where L is the number of bits in the number to be factored; error correction algorithms would inflate this figure by an additional factor of L. For a 1000-bit number, this implies a need for about 10^4 qubits without error correction. With error correction, the figure would rise to about 10^7 qubits. Note that computation time is about L^2 or about 10^7 steps and on 1 mhz , about 10 seconds.

Surrent Progress & Future Prospects

The recent work on the computing liquid technique pioneered by Dr. Gershenfield and Dr. Chuang (Los Alamos National Laboratory, New Mexico) has given quantum computing a promising future. In fact, Dr. Gershenfield believes that a quantum co-processor could be a reality within 10 years if the current pace of advancement continues. Other techniques, such as quantum dots, may also yield similar results as our technology advances. The optimist will point out that the problems being experienced by researchers appear to be technical rather than fundamental.

On the other side of the argument, is the topic of decoherence. This problem has not been resolved and many people, including Rolf Landauer of IBM's Thomas Watson Research Centre, believe that the quantum computer is unlikely to progress beyond the 10-qubit system (described above), as decoherence makes them too fragile to be practical.

Researchers in quantum communication have enjoyed a greater level of success. The partial quantum computers involved have enabled secure communication over distances as far as 10km. Depending on how costly these lines are to develop and the demand that exists for them; there could be a strong future for quantum communications.

Conclusion

It is important that construction a quantum computing is still extreme in the future. The algorithm of the quantum computer will also be quite differing. The development of quantum computer needs a lot of money. Even the best scientists cannot counter a lot of difficulty about quantum physics. Quantum computer is based on theoretical physics. Construction of a quantum computer is just a matter of time. Quantum computers easily solve applications that cannot be done with help of today's computers. This is useful for the nowadays technologies.

References

[1] Manay K. (1998)*Quantum computers could be a billion times faster than Pentium III. USA Today*.

[2] www.ewh.ieee.org(2002) *Quantum Computers*.

[3] www.qubyte.com (2002) *Quantum Computers & Moore's Law*.

[4] www.carolla.com (2002) *Quantum Computers: What are They and What Do They Mean to Us*?

[5] Deutsch D. *Royal Society of London A*, 97–117.

[6] Nanopoulos D.V. (1995)

[7] Nielsen M.A., Chaung I.L. (2000) *Cambridge, England: Cambridge*.

[8] Aaronson S. (2008) *Scientific American*, 298(3):62 – 69.

[9] Collins G.P. (2006) *Scientific American*, 294(4):56– 63.

[10] Hirvensalo M. (2001) *Springer - Verlag*.

[11] Nielsen M., Chuang. I.L. (2001) *Cambridge Press, Cambridge*.