A Study of Quantum Computing

D. G. Vyawahare
Asst. Professor,
Department of Computer Science and Engineering
Anuradha Engineering College, Chikhli Distt. Buldana, M.S. India

K. H. Walse
Associate Professor,
Department of Computer Science and Egineering
Anuradha Engineering College, Chikhli Distt. Buldana, M.S. India

Nitin V. Sali
Final Year, Computer Science & Engineering
Anuradha Engineering College, Chikhli

ABSTRACT

Quantum computation is an exciting new field, which touches on the foundations of both computer science and quantum mechanics. It provides a new model of computation that is both physically reasonable and more powerful than classical computing. In a classical computer, a bit is a fundamental unit of information, classically represented as a 0 or 1. In a quantum computer, the fundamental unit of information, called a quantum bit or qubit, is not binary but rather more quaternary in nature.

Keywords

Quantum, qubit, Computation..

1. INTRODUCTION

Quantum computer is the future of computing world. With the help of quantum computers, it would be possible to search databases containing millions of records for a particular record in a matter of seconds-even if the database is unordered. Using quantum computations, it would also be possible to communicate sensitive data between two terminals without absolutely any chance of a third party eavesdropping.

Further since quantum computers, as the name suggest, would be working on the principles of quantum mechanics, they would be ideal machines to simulate quantum mechanical systems.

The Story of quantum computation started as early as 1982, However unusual power of quantum computation was not really anticipated until 1985, when David Deutch of the University of OXFORD published crucial theoretical paper.

2. NEED FOR QUANTUM MECHANICS

2.1 What is quantum mechanics?

The deepest theory of physics; the framework within which all other current theories, except the general theory of relativity, are formulated. Some of its features are:

2.2 Quantization

(which means that observable quantities do not vary continuously but come in discrete chunks or 'quanta'). This is the one that makes computation, classical or quantum, possible at all.

2.3 Interference

(which means that the outcome of a quantum process in general depends on all the possible histories of that process). This is the one that makes quantum computers qualitatively more powerful than classical ones.

2.4 Entanglement

(Two spatially separated and non-interacting quantum systems that have interacted in the past may still have some locally inaccessible information in common - information which cannot be accessed in any experiment performed on either of them alone.) This is the one that makes quantum cryptography possible.

3. LIMITATIONS OF CLASSICAL COMPUTING

In 20th century, "Information" was added to the list when the invention of computers allowed complex information processing to be performed outside human brains. Evolution of computer technology has undergone steps as shown:

Gears->Relays->valves->transistors->ICs

The computer power has grown at an amazing rate due to the continual miniaturization of the computer's most elementary component, a transistor.

As transistors became smaller and smaller, More could be integrated into a single microchip, increasing the computational power.

3.1 limitations:

The miniaturization process, mentioned above, is now reaching a limit. Sometime in next 10 to 20 years, component technology will reach various strict physical limits. One of the biggest problems with the program of miniaturizing conventional computers is the difficulty of dissipated heat.

Another limitation of classical computers is the lack of potential for solving some "hard" problems. If the best algorithm known for a particular problem has execution time as a non-polynomials function of input size ,it is a "hard problem".

The difficulty with these classical computers is that they are not only slow but also inherently inefficient. Modern computers operate still serially, one operation at a time. Progress in the parallel computing has been slow and fitful.

4. QUANTUM COMPUTING

Quantum computing is the idea of storing information in the quantum states of individual atoms. Thus an atom in its ground state can be viewed as being in state '0' (denoted |0> for quantum bits), and an atom in an excited state would be in state '1' (denoted |1> for quantum bits). Each one of these bits of information is known as a quantum bit or "qubit." There is an important difference between quantum bits and classical bits. Whereas classical bits are either a |1> or a |0>, qubits can also store the coherent superposition of both states, due to the weird rules of subatomic particles. In other words a qubit can be in both states at once!

The structure of a typical qubit is shown in the figures below

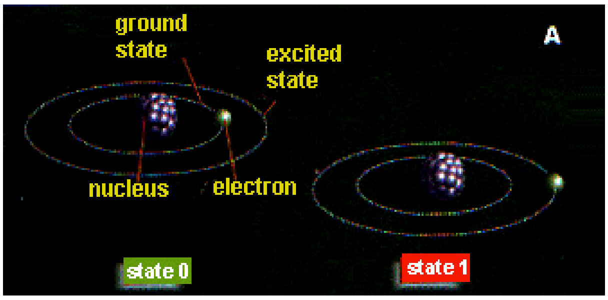


Fig 1 Shows a typical qubit. State |0> is represented by the atom in its ground state, and state |1> is represented by the atom with its electrons in their excited state.

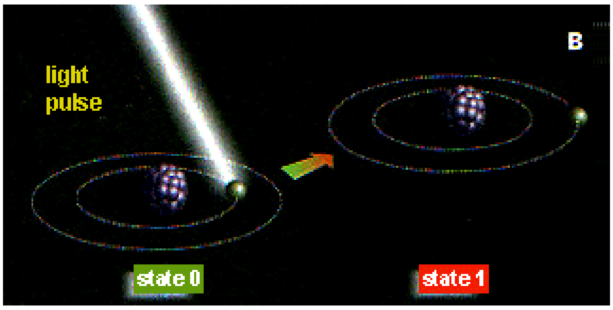


Fig 2 Illustration of how a qubit can be implemented

The method for changing between states is shown in Figure 2. If a light pulse of the correct intensity is aimed at an atom in its ground state, its electrons will bump up to the next excited state, state |1>. While the reverse is not shown, it is also true. If an atom in an excited state is hit with a laser of the same intensity, the excited electrons will be knocked out of their high energy state back to the ground state.

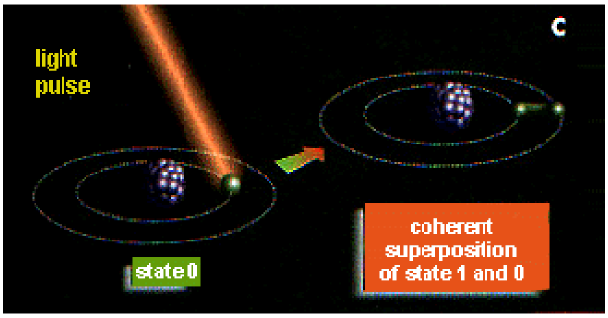
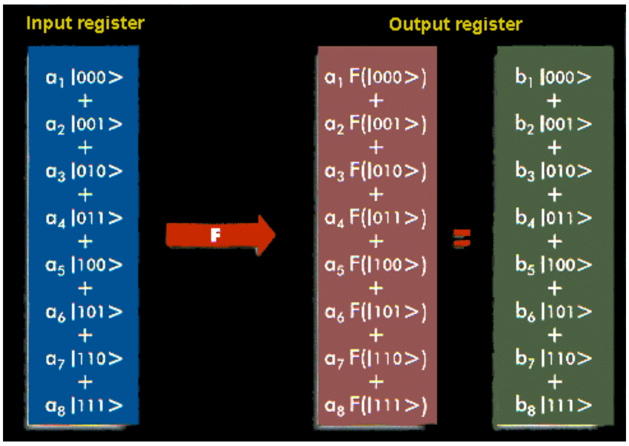


Fig 3 An atom in coherent superposition state

Figure 3 shows the state of quantum superposition. If an atom in its ground state is hit with a laser lacking the intensity to bump it up to the next energy state, the atom will reach its state of superposition. Note that the laser was not of sufficient energy to complete the excitation, but it added enough energy to the system that the atom is no longer completely in the ground state either. The atom is now in both states at once. Another half-pulse would knock the atom into its excited state (state |1>). The idea of a qubit being in the superposition of two states is difficult to understand, but it is fundamental too much of the functionality of a quantum computer. One qubit, using this superposition of states, can store two classical bits of information at once. Two qubits together can represent any one of four states (|00>, |01>, |10>, or |11>), or if both bits are in quantum superposition, they can represent all four states simultaneously (bit A can be both |0> and |1>, and bit B can be both |0> and |1>, so the combination AB can represent |00> and |01> and |10> and |11> at the same time). So N qubits can represent 2N different numbers at once.

The importance of this can be seen when we try to do an operation on these qubits. If, for example, we have a three bit register (register a) with all three bits set to their superposition states, eight numbers are represented. If we then perform a computational operation (function F(a)) on this register and put the output in a second register (register b), the operation is performed on all eight numbers simultaneously (see figure)



Input register		Output register		
$a_1\,|000>$		$a_1\,F(|000>)$		$b_1\,|000>$
+		+		+
$a_2\,|001>$		$a_2\,F(|001>)$		$b_2\,|001>$
+		+		+
$a_3\,|010>$		$a_3\,F(|010>)$		$b_3\,|010>$
+		+		+
$a_4\,|011>$	F	$a_4\,F(|011>)$	=	$b_4\,|011>$
+		+		+
$a_5\,|100>$		$a_5\,F(|100>)$		$b_5\,|100>$
+		+		+
$a_6\,|101>$		$a_6\,F(|101>)$		$b_6\,|101>$
+		+		+
$a_7\,|110>$		$a_7\,F(|110>)$		$b_7\,|110>$
+		+		+
$a_8\,|111>$		$a_8\,F(|111>)$		$b_8\,|111>$

Fig 4 This figure shows an example of quantum parallelism on a three qubit register.

So in a single step, we have performed what on a classical computer would have taken eight separate operations (one for each number represented). This procedure is called quantum parallelism because it has done all of these eight operations in parallel (at the same time). The ability to use quantum parallelism is the main advantage of using quantum computers. An N qubit quantum computer can do in one operation what would take 2N operations on a classical computer, an exponential improvement!

5. DIFFERENCE BETWEEN CLASSICAL COMPUTING AND QUANTUM COMPUTING

To explain what makes quantum computers so different from their classical counterparts, we begin by having a closer look at a basic part of information, namely a bit. From physical point of view a bit of information is represented by a physical system, which can exist in one of two different states representing two logical states representing two logical values-0 and 1.

One bit of information can also be encoded using two different polarizations of light or two different electronic states of an atom. However if we choose an atom as a physical bit then quantum mechanics tells us that apart from the two electronic states, the atom can exist in a coherent superposition of two states. This means atom is both in state 0 as well as in state 1.An atom can be prepared in a superposition of two different electronic stated, in general, a quantum two-state system, called a quantum bit or qubit, can be prepared in superposition of its two logic states 0 and 1.Thus one qubit can encode at a given moment of time both 0 and 1. Note that the application of quantum physical principles to the field of computing leads to the concept of quantum computer, in which data isn't stored as bits in conventional memory, but as the combined quantum state of many 2-state system of qubits.

6. QUANTUM COMPUTER

Where a classical computer obeys the well understood laws of classical physics, a quantum computer is a device that harnesses physical phenomenon unique to quantum mechanics (especially quantum interference) to realize a fundamentally new mode of information processing. In a quantum computer, the fundamental unit of information (called a quantum bit or qubit), is not binary but rather more quaternary in nature. This qubit property arises as a direct consequence of its adherence to the laws of quantum mechanics which differ radically from the laws of classical physics. A qubit can exist not only in a state corresponding to the logical state 0 or 1 as in a classical bit, but also in states corresponding to a blend or superposition of these classical states.

7. How a Quantum Computer Works?

A quantum particle, such as an electron or atomic nucleus, can exist in two states at the same time -- say, with its spin in the up and down states. This constitutes a quantum bit, or qubit. When the spin is up, the atom can be read as a 1, and the spin down can be read as a 0. This corresponds with the digital 1s and 0s that make up the language of traditional computers. The spin of an atom up or down is the same as turning a transistor on and off, both represent data in terms of 1s and 0s. Qubits differ from traditional digital computer bits, however, because an atom or nucleus can be in a state of "superposition," representing simultaneously both 0 and 1 and everything in between. Moreover, without interference from the external environment, the spins can be "entangled" in such a way that effectively wires together a quantum computer's qubits. Two entangled atoms act in concert with each other -- when one is in the up position, the other is guaranteed to be in the Down position.

The combination of superposition and entanglement permit a quantum computer to have enormous power, allowing it to perform calculations in a massively parallel, non-linear manner exponentially faster than a conventional computer. For certain types of calculations -- such as complex algorithms for cryptography or searching -- a quantum computer can perform billions of calculations in a single step.

8. APPLICATIONS OF QUANTUM COMPUTERS

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.

It is important to note that a quantum computer will not necessarily outperform a classical computer at all computational task. Multiplication for example, will not be performed any quicker on a quantum computer than it could be done on a similar classical computer. example, Shor's algorithm allows extremely quick factoring of large numbers, a classical computer can be estimated at taking 10 million billion years to factor a 1000 digit number, where as a quantum computer would take around 20 minutes.

8.1 Shor's algorithm

This is an algorithm invented by Peter Shor in 1995 that can be used to quickly factorize large numbers. For example, multiplying 1234 by 3433 is easy to work out, but calculating the factors of 4236322 is not so easy. The difficulty of factorizing a number grows rapidly with additional digits.

8.2 Grover's algorithm

Lov Grover has written an algorithm that uses quantum computers to search an unsorted database faster than a conventional computer. Normally it would take N/2 number of searches to find a specific entry in a database with N entries. Grover's algorithm makes it possible to perform the same search in root N searches. Grover's algorithm has a useful application in the field of cryptography.

9. ADVANTAGES

Quantum computers have many advantages over classical computers. Quantum computers would store information in a much smaller physical space than that needed for classical computers. The smaller size of quantum registers corresponds to faster operation. Both of these advantages are minor when compared to the applications of quantum parallelism, as described earlier. Classical computers can solve many large and complex mathematical problems much faster than a person can do on his own, but there are problems even too difficult for conventional computers to solve.

123 X 25 = ?

If the problem was made bigger by adding digits to either number (a large problem of low complexity), a human could probably still solve it easily, though perhaps it would be a tedious process. If a person were asked to solve a factorization problem such as finding all of the prime constituents of the number 35 (a small problem of substantial complexity), it probably would still not that be that difficult. But if we add digits to that problem, it increases in complexity exponentially!

10. CURRENT PROGRESS

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.

Fig 5 Operating IBM's quantum computer

Drs. Isaac Chuang (left) and Costantino Yannoni operate IBM's quantum computer, which uses the interactions of nuclear spins within a specially designed molecule to perform calculations in a manner that is exponentially more powerful than conventional computers. The spins are programmed by a series of radiofrequency pulses and the answer is revealed by a nuclear magnetic resonance spectrum

Fig 6 Loading IBM's 7-qubit quantum computer

Dr. Isaac Chuang loads the vial containing the 7-qubit quantum computer molecules into the top of the nuclear magnetic resonance apparatus. Within the tank, the molecule's spins will be aligned by very powerful magnetic fields and manipulated by a program of radiofrequency pulses designed to direct the molecules to execute Shor's quantum factoring algorithm.

11. FUTURE SCOPE

11.1 NASA:

As NASA spacecraft explore deeper into the cosmos, speed-of-light-limited signal delays make it increasingly impractical to command missions from Earth. Future spacecraft will need greater onboard computing capacity to mimic human-level intelligence and autonomy. Unfortunately, computer manufacturers will have difficulty providing the vastly increased computing power the space-exploration community will need. The solution might well come from quantum computers, which offer properties of size, power, and robustness that are ideally suited to the space environment. The potential of quantum technologies goes far beyond enhanced computing capacity. Future space missions will involve direct participation of non-NASA scientists. This will necessitate allowing more open access to spacecraft systems via free-space communication links. Quantum cryptography would allow such channels to be made absolutely secure and invulnerable to attack by malevolent hackers. To explore these possibilities, this article describes the progress to date in understanding how quantum computers and related quantum information-processing devices might advance space exploration.

12. CONCLUSION

With classical computers gradually approaching their limit, the quantum computer promises to deliver a new level of computational power. With them comes a whole new theory of computation that incorporates the strange effects of quantum mechanics and considers every physical object to be some kind of quantum computer. 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. 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.

13. ACKNOWLEDGMENT

The author would like to thank Dr. S. V. Agarkar, Principal of the AECC and Dr. Naik, R& D Dean for their help and support in making this work possible.

14. REFERENCES

[1] An Introduction to Quantum Computation and Quantum Communication by Rob Pike, Bell Labs Lucent Technologies June 23, 2000.

[2] Quantum Computation & Quantum Computing Wikipedia – The Free Encyclopedia.

[3] Jozef Gruska, Quantum Computing, Shoppenhangers Road Maidenhead Berkshire SL6 2QL UK, april 1999.

[4] An Introduction to Quantum Computation and Quantum Communication by Rob Pike, Bell Labs Lucent Technologies June 23, 2000.

[5] Quantum Computing and the Ultimate Limits of Computation by Scott Aaronson (MIT), Dave Bacon (University of Washington) December 12, 2008.

[6] Quantum Computing - Lecture Notes of Mark Oskin Department of Computer Science and Engineering University of Washington

[7] www.ibm.research.com

[8] Nielsen M., Quantum Computing (unpublished notes) (1999).

[9] J. Preskill, Quantum Computing: Pro and Conquant-V3, 26 Aug 1997.

[10] A Brief History of Quantum Computing Simon Bone and Matias Castro

[11] A Short Introduction to Quantum Computation A.Barenco, A.Ekert, A.Sanpera and C.Machiavello

[12] Centre for Quantum Computation: www.qubit.org

[13] Quantum Computing with Molecules Neil Gershenfeld and Isaac L. Chuang

[14] How Quantum Computers will Work www.HowStuffWorks.com

[15] Wikipedia – The Free Encyclopedia Quantum Computation