International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-2 Issue-2, December 2012

Can Quantum Computers Replace the Classical Computer?

Nikhil Talele, Ajinkya Shukla, Sumant Bhat

Abstract*—The first computer originated as an ordinary calculator in 19th century. Subsequently, the rapid evolution of computers began. The massive amount of processing power generated by computer manufacturers has always failed to quench the thirst for speed and computing capacity. If, as Moore's Law states, the number of transistors on a microprocessor continues to double every 18 months, then soon we will find the circuits on a microprocessor being measured on an atomic scale. Today's advanced lithographic techniques can squeeze fraction of micron wide logic gates and wires onto the surface of silicon chips. Thus it can be seen that very soon we will be facing the need to create quantum computers which can harness the power of atoms and molecules to perform memory and processing tasks. Quantum computers have the potential to perform calculations a billion times faster than any silicon-based computer. Also, theories suggest that every physical object, even the universe, is in some sense a quantum computer. If this is the case, then according to Turing's work which says that all computers are functionally equivalent; computers should be able to model every physical process. Scientists have already built basic quantum computers that can perform certain calculations; but a practical quantum computer is still years away. In this paper, we will be discussing about the history, development and the future scope of quantum computing. The pros and cons of this future technology have also been compared and our analysis has been put forth.

***Index Terms*— Quantum Computing, history, current trends, advantages, disadvantages, applications, future scope.**

I. INTRODUCTION

Although computers have become more compact and considerably faster in performing their task, the task remains the same: to manipulate and interpret an encoding of binary bits into a useful computational result. The key difference between a classical computer and a quantum computer is that 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[10]. 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. Shor's algorithm harnesses the power of quantum superposition to rapidly factor very large numbers (on the order ~10200 digits and greater) in a matter of seconds[10]. The premier application of a quantum computer capable of implementing this algorithm lies in the field of encryption, where one common (and best) encryption code, known as RSA, relies heavily on the difficulty of factoring very large composite numbers into their primes. Feynman asserted that a quantum computer could function as a kind of simulator for quantum physics, potentially opening the doors to many discoveries in the field. Currently the power and capability of a quantum computer is primarily theoretical speculation; the advent of the first fully functional quantum computer will undoubtedly bring many new and exciting applications.

Manuscript published on 30 December 2012.
***** Correspondence Author (s)
Nikhil Talele, Department of Information Technology, Fr. C.R.I.T, Vashi, India.
Sumant Bhat, Department of Information Technology, Fr. C.R.I.T, Vashi, India.
Ajinkya Shukla, Department of Information Technology, Fr. C.R.I.T, Vashi, India, +918976165714, (e-mail: ajinkyashukla02@gmail.com).

II. HISTORY OF QUANTUM COMPUTING

In 1965, Nobel prize-winning physicist Richard Feynman proposed significant theories of quantum electrodynamics, a realm concerned with the way in which electrons interact with one another through the electromagnetic force propagated through the photon[1]. He created simple visual depictions of the possible interactions between an electron and photon and other atomic interactions. Then in 1980, Feynman, among others, began investigating about the generalization of conventional information science concepts to quantum physical processes, considering the representation of binary numbers in relation to the quantum states of two-state quantum systems. David Deutsch, of Oxford, in 1985, published a theoretical paper describing a universal quantum computer, proving that if two-state system could be made to evolve by means of a set of simple operations, any such evolution could be produced, and made to simulate any physical system; these operations come to be called quantum 'gates', as they function similarly to binary logic gates in classical computers.1994 saw the making of Shor's Algorithm. Peter Shor proposed a method using entanglement of qubits and superposition to find the prime factors of an integer, a rather valuable process as many encryption systems exploit the difficulty in finding factors of large numbers[3]. The National Institute of Standards and Technology and the California Institute of Technology in 1995 jointly contemplated the problem of shielding a quantum system from environmental influences and began experiments with magnetic fields, which allow particles (ions) to be trapped and cooled to a quantum state. And in 1996, a team composed of University of California at Berkeley, MIT, Harvard University, and IBM researchers pursued a somewhat similar technique, but using nuclear magnetic resonance (NMR), a technology which manipulates quantum information in liquids[12]. The team then went on and developed a 2-bit quantum computer made from a thimble of chloroform; input consisted of radio frequency pulses into the liquid containing, in essence, the compiled program to be executed and thus began the age of Quantum Computing.

III. PRINCIPLE

A quantum computer is a machine that performs calculations based on the behavior of particles at the sub-atomic level. Such a computer will be capable of executing far more millions of instructions per second (MIPS) than any previous computer. Such an exponential advance in processing capability would be due to the fact that the data units in a quantum computer, unlike those in a binary computer, can exist in more than one state at a time.

Engineers have coined the term 'qubit' to denote the fundamental data unit in a quantum computer. A qubit is essentially a bit (binary digit) that can take on several, or many, values simultaneously. One way to think of how a qubit can exist in multiple states is to imagine it as having two or more aspects or dimensions, each of which can be high (logic 1) or low (logic 0). Thus if a qubit has two aspects, it can have four simultaneous, independent states (00, 01, 10, and 11); if it has three aspects, there are eight possible states, binary 000 through 111, and so on.

IV. PRESENT DEVELOPMENT SITUATION

A Hitachi-Cambridge team has successfully demonstrated qubit operation of a silicon circuit, made using standard fabrication techniques and which is the first step towards making a silicon quantum computer [11].

Now the team is involved in the development of devices for quantum information processing, nano-spintronics and organic devices [11].

Many other organizations are working globally on the development of quantum computing technologies.

Quantum Computing has made it possible to factorize large numbers into 300 digit prime factors. This is computationally infeasible for traditional computers.

Current Research areas include:

(1) Robust solid-state qubits and related technologies.
(2) Short-to-medium-range quantum information transfer in solid-state systems.
(3) Ideas & methods for the verification of quantum computing components.
(4) Procedures for validating quantum computing components.

Current Algorithms implemented:
Shor's Algorithm[3]
Grover's Algorithm

V. APPLICATION AND CURRENT TRENDS

With the global forces of computer competition, encryption technology for national security, new applications, and the thermodynamics of computer systems changing as they are, there is a rush toward the new quantum technology to produce the first viable quantum computer. The world is moving toward a place that no classical computer has gone before, nor can go.

Quantum Computation has a wide range of applications like :

1. Quantum Communication:

Quantum communication is the art of transferring a quantum state from one location to another. It allows a sender and receiver to agree on a code without ever having to meet in person. From an application point of view the major interest is Quantum Key Distribution (QKD), as this offers for the first time a provably secure way to establish a confidential key between distant partners. This key is then first tested and, if the test succeeds, used in standard cryptographic applications. The uncertainty principle, an inescapable property of the quantum world, ensures that if an eavesdropper tries to monitor the signal in transit it will be disturbed in such a way that the sender and receiver are alerted. The expected capabilities of quantum computation promise great improvements in the world of cryptography.

2. Quantum Cryptography:

Quantum cryptography was discovered independently in US and Europe[14]. The American approach, pioneered by Steven Wiesner, was based on coding in non-commuting observables, whereas the European approach was based on correlations due to quantum entanglement. This has the potential to solve a long-standing and central security issue in our information based society. Ironically the same technology also poses current cryptography techniques a world of problems. The implications of Shor's factoring algorithm on the world of cryptography are staggering. The ability to break the RSA coding system will render almost all current channels of communication insecure.

3. Artificial Intelligence:

The theories of quantum computation have some interesting implications in the world of artificial intelligence. The debate about whether a computer will ever be able to be truly artificially intelligent has been going on for years and has been largely based on philosophical arguments. Those against the notion suggest that the human mind does things that aren't, even in principle, possible to perform on a Turing machine. The theory of quantum computation allows us to look at the question of consciousness from a slightly different perspective. The first thing to note is that every physical object, from a rock to the universe as a whole, can be regarded as a quantum computer and that any detectable physical process can be considered a computation. Under these criteria, the brain can be regarded as a computer and consciousness as a computation. The next stage of the argument is based in the Church-Turing principle and states that since every computer is functionally equivalent and that any given computer can simulate any other, therefore, it must be possible to simulate conscious rational thought using a quantum computer. Ultimately this suggests that computers will be capable of simulating conscious rational thought. These theories provoke a minefield of philosophical debate, but maybe the quantum computer will be the key to achieving true artificial intelligence.

Also, the latest applications include :

1. Encryption Technology:

The speed of quantum computers also jeopardizes the encryption schemes that rely on impracticably-long times to decrypt by brute force methods. Encryption schemes that may take millions of years to guess and check are now vulnerable to quantum computers that may reach a solution within one year. Many governments, included ours, use such encryption schemes for national security. They are very interested in any technology that puts that at risk. As a result, the Office of Naval Research, the CIA, and DARPA, are sinking huge funds into quantum computer research.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

DARPA is funding $5 million for a Quantum Information and Computing Institute, and the CIA is funding an unknown amount for factoring of large integers, a fundamental part of encryption technology.

2. *Ultra-secure and Super-dense Communications:*

It is possible to transmit information without a signal path by using a newly-discovered quantum principle, quantum teleportation. There is no way to intercept the path and extract information. Ultra-secure communication is also possible by super-dense information coding, which is a new technology in its own right. Quantum bits can be used to allow more information to be communicated per bit than the same number of classical bits.

3. *Improved Error Correction and Error Detection:*

Through similar processes that support ultra-secure and super-dense communications, the existing bit streams can be made more robust and secure by improvements in error correction and detection. Recovering informational from a noisy transmission path will also be a lucrative and useful practice.

4. *Molecular Simulations:*

Richard Feynman showed in 1982 that classical computers cannot simulate quantum effects without slowing down exponentially; a quantum computer can simulate physical processes of quantum effects in real time[1]. Molecular simulations of chemical interactions will allow chemists and pharmacists to learn more about how their products interaction with each other, and with biological processes such as how a drug may interact with a person's metabolism or disease. Pharmaceutical research offers a big market to such applications.

5. *True Randomness:*

Classical computers do not have the ability to generate true random numbers. The random number generators on today's computers are pseudo-random generators—there is always a cycle or a trend, however subtle. Pseudo-random generators cannot simulate natural random processes accurately for some applications, and cannot reproduce certain random effects. Quantum computers can generate true randomness, thus give more veracity to programs that need true randomness in their processing. Randomness plays a significant part of applications with a heavy reliance on statistical approaches, for simulations, for code making, randomized algorithms for problems solving, and for stock market predictions, to name a few.

VI. ADVANTAGES

1. First, atoms change energy states very quickly -- much more quickly than even the fastest computer processors. Next, given the right type of problem, each qubit can take the place of an entire processor -- meaning that 1,000 ions of say, barium, could take the place of a 1,000-processor computer. The key is finding the sort of problem a quantum computer is able to solve.
2. If functional quantum computers can be built, they will be valuable in factoring large numbers, and therefore extremely useful for decoding and encoding secret information. If one were to be built today, no information on the Internet would be safe. Our current methods of encryption are simple compared to the complicated methods possible in quantum computers.
3. Quantum computers could also be used to search large databases in a fraction of the time that it would take a conventional computer.

VII. DISADVANTAGES

1. The technology needed to build a quantum computer is currently beyond our reach. This is due to the fact that the coherent state, fundamental to a quantum computers operation, is destroyed as soon as it is measurably affected by its environment.
2. Classical algorithms cannot be applied to quantum computers.
3. In-depth knowledge of quantum mechanics is needed for implementation.

VIII. CASE STUDY

I.B.M. Researchers Inch toward Quantum Computer:

I.B.M is jumping into an area of computing that has, until now, been primarily the province of academia: the quest to build a quantum computer[13]. "In the past, people have said, maybe it's 50 years away, it's a dream, maybe it'll happen sometime," said Mark B. Ketchen, manager of the physics of information group at I.B.M.'s Thomas J. Watson Research Center in Yorktown Heights, N.Y. "I used to think it was 50. Now I'm thinking like it's 15 or a little more. It's within reach. It's within our lifetime. It's going to happen." Many university researchers have done good work solving the basic science problems, Dr. Ketchen said, but "it's going take an I.B.M. in the end to put it together." It's still too early for I.B.M. to have a commercial product in mind, but computer scientists are encouraged that the company is paying attention. Scott Aaronson, a professor of electrical engineering and computer science at the Massachusetts Institute of Technology, called I.B.M.'s work "a cause for cautious optimism" in the development of quantum computers. "It looks very interesting," Dr. Aaronson said of the I.B.M. research. "Basically, it's another step in continuing progress." While a working quantum computer is still quite a few years away, there have been a number of advances over the last couple of years, and the I.B.M. one is just among the most recent. These days, the pathto the future now looks more like a series of very hard engineering problems rather than an uphill fight against physics. The I.B.M. researchers are building quantum computer components out of electronic circuits containing superconductors, materials that carry electricity without electrical resistance. When cooled to a hundredth of a degree above absolute zero, the circuits act as qubits.

IX. FUTURE OF QUANTUM COMPUTING

1) Nano-particle Quantum Computing.
2) End to the problem of overheating.
3) Computing power of laptops increased to a trillion times.
4) New Generation radio, television and Internet.

Entanglement:

Einstein once proposed that two subatomic particles become entangled in quantum mechanics, i.e. they move in lockstep, even at a distance. This phenomenon is supposed to improve networking beyond horizons.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

X. CONCLUSION

The term Quantum Computing (QC) has been in the lingo of science for some years now, but it is just making its way into the public consciousness[15]. Quantum computers will not make regular computers obsolete, just as lasers haven't made light bulbs outmoded. The excitement about them pertains to what tasks they will do which have previously only been imagined: break a very large number, say one with 400 digits, into its component parts (factoring), a task critical for encryption of communication data. Currently, it would take a supercomputer billions of years to do this kind of factoring, more time than the age of the Universe. Yet quantum physicists believe that a quantum computer will do the same computation in only a few minutes. While quantum computing may revolutionize computing giving vastly new powers, it also exemplifies how highly theoretical physics can suddenly and shockingly have immense practical use. Angels on the head of a pin? Now they're on an atom -- and we're making them work for us [15]. Considering the difficulties, QC is not something which can be manufactured by anybody, anywhere, it requires controlled conditions .As the development of quantum physics continues it will pave the way for QC, but however it cannot be expected in near future. It is something which will open the vistas of future, revolutionalize the living, change the way we live and thus unreveal the mystery of nature, space and life!

REFERENCES

[1] D. Deutsch, Proc. Roy. Soc. London, Ser. A 400, 97 (1985).2. R. P. Feynman, Int. J. Theor. Phys. 21, 467 (1982).
[2] J. Preskill, "Battling Decoherence: The Fault-Tolerant Quantum Computer," Physics Today, June (1999).
[3] Shor, P. W., Algorithms for quantum computation: Discrete logarithms and factoring, in Proceedings of the 35th Annual Symposium on Foundations of Computer Science, IEEE Computer Society Press (1994).
[4] Nielsen, M., "Quantum Computing," (unpublished notes) (1999).
[5] QUIC on-line, "Decoherence and Error Correction," (1997).
[6] D.G. Cory et al., Physical Review Letters, 7 Sept 1998.
[7] J. Preskill, "Quantum Computing: Pro and Con," quant-ph/9705032 v3, 26 Aug 1997.
[8] Chuang, I. L., Laflamme, R., Yamamoto, Y., "Decoherence and a Simple Quantum Computer," (1995).
[9] D. Deutsch, A. Ekert, "Quantum Computation," Physics World, March (1998).
[10] “The Quantum Computer An Introduction” by Jacob West, April, 28, 2000.
[11] “Breakthrough in development of quantum computers - A Hitachi-Cambridge team develops a new silicon qubit”, (News releases), August 19, 2005.
[12] International journal of scientific & technology research volume 1,”Revealing New Concepts In Cpytography & Clouds””, issue 7, August 2012.
[13] “I.B.M. Researchers Inch Toward Quantum Computer”, Kenneth Chang, February 28, 2012.
[14] “Quantum Cryptography”, Artur Ekert.
[15] “Will Computers Take A Quantum Leap?”, Seth Lloyd.

Nikhil Talele : Currently Pursuing BE in Information Technology from Mumbai University. Member of Computer Society of India (CSI). Worked as intern with Aditya Birla Group for a period of 6 months. Attended workshops on Android Application Development. Won many coding, quiz, project and web designing competitions.

Ajinkya Shukla : Currently Pursuing BE in Information Technology from Mumbai University. Member of Computer Society of India (CSI)

Sumant Bhat: Currently Pursuing BE in Information Technology from Mumbai University. Member of Computer Society of India (CSI)

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)