Available at: www.researchpublications.org

Quantum Computer : An Overview

Amit V. Pandhare[#1] , Prof. Ms. V. M. Deshmukh[#2]
"Department of Computer Science and Engineering"
"Prof. Ram Meghe Institute of Technology and Research Badnera"
amitvpandhare@gmail.com[#1]
msvmdeshmukh@rediffmail.com[#2]

Abstract:

Combining physics, mathematics and computer science, quantum computing has developed in the past two decades from a visionary idea to one of the most fascinating areas of quantum mechanics[4]. If the bits of computer are scaled down to the size of individual atom, then it can change the nature of computation itself. In that case the function of such a quantum computer may consist of a superposition of many computations carried out simultaneously. This can solve many computational problem such as factoring of large integers , tractable. This research paper gives an overview of quantum computer, description of qubit, difference between quantum and silicon computer.

Keyword: Quantum computer, Qubit, Bloch Sphere, Quantum Gates, Moore law.

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 digital computers. Digital computer are based on transistors and it require data to be encoded into binary digits(bits), whereas in quantum computation we use quantum properties to represent data and perform operations on these data. Around 2025 computers might not have any transistors and chips. Think of a computer that is much faster than a common classical silicon computer. This might be a quantum computer. Theoretically it can run without energy consumption and billion times faster than today's PIII computers. Scientists already think about a quantum computer, as a next generation of classical computers[9].

A technology of quantum computers is also very different. For operation, quantum computer uses quantum bits (qubits)[9][12]. Qubit has a quaternary nature. Quantum mechanic's laws[9][14] 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. Forty qubits could have the same power as modern supercomputers. 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.

Civilisation has advanced as people discovered new ways of exploiting various physical resources such as materials, forces and energies. In the twentieth century information was added to the list when the invention of computers allowed complex information processing to be performed outside human brains. The history of computer technology has involved a sequence of changes from one type of physical realisation to another — from gears to relays to valves to transistors to integrated circuits and so on. Today's advanced lithographic techniques can squeeze fraction of micron wide logic gates and wires onto the surface of silicon chips. Soon they will yield even smaller parts and inevitably reach a point where logic gates are so small that they are made out of only a handful of atoms. On the atomic scale matter obeys the rules of quantum mechanics, which are quite different from the classical rules that determine the properties of conventional logic gates. So if computers are to become smaller in the future, new, quantum technology must replace or supplement what we have now. The point is, however, that quantum technology can offer much more than cramming more and more bits to silicon and multiplying the clock-speed of microprocessors. It can support entirely new kind of computation with qualitatively new algorithms based on quantum principles!

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. A quantum register composed of three qubits can store in a given moment of time all eight numbers in a quantum superposition (Fig. 2)[7][9]. This is quite remarkable that all eight numbers are physically present in the register but it should be no more surprising than a qubit being both in state 0 and 1 at the same time. If we keep adding qubits to the register we increase its storage capacity exponentially i.e. three qubits can store 8 different numbers at once, four qubits can store 16 different numbers at once, and so on; in general L qubits can store 2L numbers at once. Once the 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 superpositions of encoded numbers into different superpositions[13]. 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 superpositions 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.

Literature Review :

Alan Turing invented the programmable computer in 1936 as a thought experiment to show that certain mathematical problems were not computable. Implicit in his argument was the idea that a computer, armed with sufficient resources, is capable of realizing any reasonable algorithm. Since that time, the computer industry has not only managed to build programmable computing machines, they've also outdone themselves by doubling the capabilities every eighteen months or so. Despite these frenetic advances in computer technology, modern computers are still unable to make significant dents in hard problems. Problems that require exponential resources (compared to the size of the problem itself), remain as intractable today as they were in 1936[4].

In 1982 Richard Feynman[1][4] suggested that the venerable Turing machine might not be as powerful as people thought. Feynman was trying to simulate the interaction of N particles with quantum mechanics. Try as he might, he was unable to find a general solution without using exponential resources. Quantum computing can be understood by learning the quantum laws of physics by which so much of processing power is achieved and the capacity will be developed to several states and these will together helps in executing the tasks in terms of parallel attainable combinations. Generally quantum computing depends on quantum laws of physics because there are many advantages from the quantum physics atoms and nuclei properties which are definite, as the quantum physics laws and quantum computing are permitted by these properties to work mutually as quantum bits or simply as qubits, to be the processor or memory of a computer. The advantage of qubits[9][12] is particular calculation are made faster exponentially when compared to the usual computers.

Yet somehow, nature is able to simulate this mathematical problem using only N particles. The conclusion was inescapable: nature is capable of building a fundamentally superior computing device, and that suggests that the Turing machine had not been the all-purpose computer people had thought[4].

Quantum bit :

The smallest unit of information in a quantum computer. Unlike bits in classical systems, which are in one of two possible states labelled 1 and 0, a quantum bit exists in a superposition of these two states, settling on one or the other only when a measurement of the state is made. Also called qubit[9][12]. The qubit is the quantum analogue of the bit, the classical fundamental unit of information. It is a mathematical object with specific properties that can be realized physically in many different ways as an actual physical system. Just as the classical bit has a state (either 0 or 1), a qubit also has a state. Yet contrary to the classical bit, 0 and 1 are but two possible states of the qubit, and any linear combination (superposition) thereof is also physically possible. In general, thus, the physical state of a qubit is the superposition $\psi = \alpha 0 + \beta 1$ (where α and β are complex numbers)[9][12][14]. The state of a qubit can be described as a vector in a two-dimensional Hilbert space, a complex vector space (see the entry on quantum mechanics). The special states 0 and 1 are known as the computational basis states, and form an orthonormal basis for this vector space. According to quantum theory, when we try to measure the qubit in this basis in order to determine its state, we get either 0 with probability α^2 or 1 with probability β^2. Since $\alpha^2 + \beta^2 = 1$ (i.e., the qubit is a unit vector in the aforementioned two-dimensional Hilbert state), we may (ignoring the overall phase factor) effectively write its state as $\psi = \cos(\theta)0 + e^{i\varphi}\sin(\theta)1$, where the numbers θ and φ define a point on the unit three-dimensional sphere, as shown here. This sphere is often called the Bloch sphere, and it provides a useful means to visualize the state of a single qubit.

Representation of Qubit :

The two states in which a qubit may be measured are known as basis states (or basis vectors). As is the tradition with any sort of quantum states, Dirac, or bra-ket notation, is used to represent them. This means that the two computational basis states are conventionally written as and (pronounced "ket 0" and "ket 1").

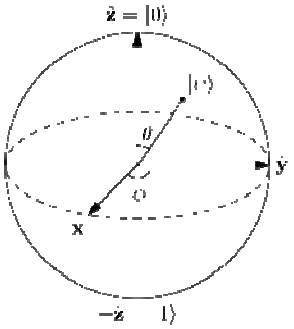

Fig 1: The Bloch Sphere

Theoretically, a single qubit can store an infinite amount of information, yet when measured it yields only the classical result (0 or 1) with certain probabilities that are specified by the quantum state. In other words, the measurement changes the state of the qubit, “collapsing” it from the superposition to one of its terms. The crucial point is that unless the qubit is measured, the amount of “hidden” information it stores is conserved under the dynamic evolution (namely, Schrödinger's equation). This feature of quantum mechanics allows one to manipulate the information stored in unmeasured qubits with quantum gates, and is one of the sources for the putative power of quantum computers. To see why, let us suppose we have two qubits at our disposal. If these were classical bits, then they could be in four possible states (00, 01, 10, 11). Correspondingly, a pair of qubits has four computational basis states (00 , 01 , 10 , 11). But while a single classical two-bit register can store these numbers only one at a time, a pair of qubits can also exist in a superposition of these four basis states, each of which with its own complex coefficient (whose mod square, being interpreted as probability, is normalized). As long as the quantum system evolves unitarily and is unmeasured, all four possible states are simultaneously “stored” in a single two-qubit quantum register. More generally, the amount of information that can be stored in a system of n unmeasured qubits grows exponentially in n. The difficult task, however, is to retrieve this information efficiently.

Quantum Gates:

Classical computational gates are Boolean logic gates that perform manipulations of the information stored in the bits. In quantum computing these gates are represented by matrices, and can be visualized as rotations of the quantum state on the Bloch sphere. This visualization represents the fact that quantum gates are unitary operators, i.e., they preserve the norm of the quantum state (if U is a matrix describing a single qubit gate, then U†U=I, where U† is the adjoint of U, obtained by transposing and then complex-conjugating U). As in the case of classical computing, where there exists a universal gate (the combinations of which can be used to compute any computable function), namely, the NAND gate[14] which results from performing an AND gate and then a NOT gate, in quantum computing it was shown [9] that any multiple qubit logic gate may be composed from a quantum CNOT gate[9] (which operates on a multiple qubit by flipping or preserving the target bit given the state of the control bit, an operation analogous to the classical XOR, i.e., the exclusive OR gate) and single qubit gates. One feature of quantum gates that distinguishes them from classical gates is that they are reversible: the inverse of a unitary matrix is also a unitary matrix, and thus a quantum gate can always be inverted by another quantum gate.

$$\mathrm{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

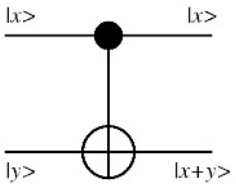

Fig 2:The CNOT Gate

Moore's Law:

Moore's Law[9][14][16] is a computing term which originated around 1970; the simplified version of this law states that processor speeds, or overall processing power for computers will double every two years. A quick check among technicians in different computer companies shows that the term is not very popular but the rule is still accepted.

To break down the law even further, it specifically stated that the number of transistors on an affordable CPU would double every two years (which is essentially the same thing that was stated before) but 'more transistors' is more accurate.

If you were to look at processor speeds from the 1970's to 2009 and then again in 2010, one may think that the law has reached its limit or is nearing the limit. In the 1970's processor speeds ranged from 740 KHz to 8MHz; notice that the 740 is KHz, which is Kilo Hertz – while the 8 is MHz, which is Mega Hertz[16].

From 2000 – 2009 there has not really been much of a speed difference as the speeds range from 1.3 GHz to 2.8 GHz, which suggests that the speeds have barely doubled within a 10 year span. This is because we are looking at the speeds and not the number of transistors; in 2000 the number of transistors in the CPU numbered 37.5 million, while in 2009 the number went up to an outstanding 904 million; this is why it is more accurate to apply the law to transistors than to speed. With all this talk of transistors the average technician or computer user may not understand what the figures mean; a simpler way to explain is that the earlier CPUs on the market had a single speed or frequency rating while the newer models have a rating which refers to more than one CPU. If you've purchased a computer recently you might have an idea of what this means as salespersons may have sold you on the wonders of multi-core CPUs. In the example given above, the speeds over a large number of years went between 1.3 and 2.8, which is barely double but what needs to be kept in mind is that the 2.8 is a QUAD CORE while the 1.3 is a single CORE. This means that the actual power of the 2.8 would be found if you multiply by four – which would give you a whopping 11.2 which is a far cry from 1.3. Due to the rapid rate that technology has grown in the past few years, most computer technicians you speak with – whether they have heard of Moore's Law or not will tell you that CPU speeds double each year. Though Moore's Law had said every two years, this rapid increase in technological production has lessened the period in the minds of technicians and users alike. The limitation which exists is that once transistors can be created as small as atomic particles, then there will be no more room for growth in the CPU market where speeds are concerned[9][16].

Applications of Quantum computer :

1**. Cryptography and Peter Shor's Algorithm**

In 1994 Peter Shor[3][8] (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. (Maney, 1998)

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[10], 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.

Limitations of Quantum computer :

Any kind of measurement of quantum state parameters considers interaction process with environment (with other particles - particle of light for example), which causes a change of some parameters of this quantum state. Measurement of superposition quantum state will collapse it into a classical state. This is called decoherence. This is the major obstacle in a process of producing of a quantum computer. If decoherence problem cannot be solved, a quantum computer will be no better than a silicon one.

In order to make quantum computers powerful, many operations must be performed before quantum coherence is lost. It can be impossible to construct a quantum computer that will make calculations before decohering. But if one makes a quantum computer, where the number of errors is low enough, than it is possible to use an error-correcting code for preventing data looses even when qubits in the computer decohere. There are a lot of error-correcting codes. One of the simplest classical error-correcting codes is called repetition code. 0 is encoded as 000 and 1 as 111. Then if only one bit is flipped, one gets a state for example 011 that can be corrected to its original state 111. The signs of states in a quantum superposition are also important, but sign errors can also be corrected. There exists even a theory about quantum error-correcting codes.

Another problem is hardware for quantum computers. Nuclear Magnetic Resonance (NMR) technology[11] is the most popular today, because of some successful experiments. MIT and Los Alamos National Laboratory have constructed a simple quantum computer using NMR technology. Some other designs are based on ion trap and quantum electrodynamics (QED). All of these methods have significant limitations. Nobody knows what the architecture of future quantum computers hardware will be.

Conclusion :

Experimental and theoretical research in quantum computation is accelerating world-wide. New technologies for realising quantum computers are being proposed, and new types of quantum computation with various advantages over classical computation are continually being discovered and analysed, and we believe some of them will bear technological fruit. From a fundamental standpoint, however, it does not matter how useful quantum computation turns out to be, nor does it matter whether we build the first quantum computer tomorrow, next year or centuries from now. The quantum theory of computation must in any case be an integral part of the world view of anyone who seeks a fundamental understanding of the quantum theory and the processing of information.

References :

[1] R. Feynman, Int. J. Theor. Phys. 21, 467 (1982).
[2] D. Deutsch, Proc. R. Soc. London A 400, 97 (1985).
[3] P.W. Shor, in Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, edited by S. Goldwasser (IEEE Computer Society Press, Los Alamitos, CA), p. 124 (1994).
[4]http://www.ibm.com/developerworks/library/quant/index.html.
[5] R. Landauer, Trans. R. Soc. London, Ser. A 353, 367 (1995).
[6] P. Domokos, J.M. Raymond, M. Brune and S. Haroche, Phys. Rev. A 52, 3554 (1995).
[7] C. Monroe, D.M. Meekhof, B.E. King, W.M. Itano and D.J. Wineland, Phys. Rev. Lett. 75, 4714 (1995).
[8]Shor, P. (1994) 'Algorithms for quantum computation: Discrete logarithms and factoring', *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*, pp. 124–134.
[9] Archil Avaliani (2002)" Quantum Computers" International University.
[10]Bub, J. (2005), 'Quantum mechanics is about quantum information', Foundations of Physics, 34: 541–560.
[11]Cirac, J.I. and Zoller, P. (1995), 'Quantum computations with cold trapped ions', Phys. Rev. Lett., 74: 4091–4094.
[12] A. Barenco, D. Deutsch, A. Ekert and R. Jozsa, Phys. Rev. Lett. 74, 4083 (1995).
[13] Davis, M. (2003), 'The myth of hypercomputation', in C. Teuscher (ed.), Alan Turing, Life and Legacy of a Great Thinker, New York: Springer, pp. 195–212.
[14] www.qubit.org/qubit.html.
[15] Biham, E., et al. (2004), 'Quantum computing without entanglement', Theoretical Computer Science, 320: 15–33.
[16] http://www.mooreslaw.org.