Quantum Computing: The Next Technological Revolution?

Computers have come a long way since their first realization in 1945 in the form of ENIAC, a mammoth machine weighing more than 30 tons and consisting of over 17,000 vacuum tubes, 10,000 capacitors and more than 1500 relays. Shrinking in size has been accompanied with an increase in capabilities and a concurrent decrease in prices. In fact, over the last 50 years, computers have roughly shrunk to half their size every two years or so. Microprocessors, the heart of today's computers have also followed what is termed as Moore's law (after Gordon Moore, one of the co-founders of Intel) which states that the number of transistors on a chip double every 18 months.

Impressive as this growth might be, there are some fundamental hurdles which limit the growth in speed and performance. Some of these hurdles are technological like the limit of current lithographic techniques which restrict the etching of the circuits on silicon while others are more basic and have to do with the quantum mechanical behavior of electrons. The technological bottlenecks will undoubtedly be cleared with the development of new techniques like x-ray lithography but the inherent limitations have proven to be a dead end for most researchers. It is now widely accepted that to achieve real revolutionary progress in the development of computers, a new paradigm is needed which will replace the existing computer design at both the hardware and programming level.

One such idea which is causing a lot of excitement in the field is that of quantum computation. On the face of it, the disciplines of computer science and quantum mechanics seem to have little to do with each other. But, as has happened often in the history of science, fruitful results have emerged from combining two hitherto unrelated fields. The idea that quantum mechanics has something to do with computers emerged in the early eighties when Paul Benioff in 1980 described how one could conceive of computers made with quantum components. Then in 1982, the famous physicist, Richard Feynman formulated a model which allowed, in principle a quantum system to be used for doing computations. He also proposed a "universal quantum simulator" which could simulate a quantum system and carry out experiments on it.

The big breakthrough came in 1985 when David Deutsch of Oxford University wrote two seminal papers which laid down the fundamentals of quantum computing. He showed that it was not only a quantum system which can be modeled by a quantum computer but ANY physical process can be perfectly modeled with this hypothetical machine, the "universal quantum computer". In doing this, he extended the work of the famous mathematician Alan Turing who had proposed a universal Turing machine to carry out calculations. Not only was this machine capable of doing everything a traditional computer can do, but there were problems which a quantum computer can tackle which are beyond the scope of traditional machines.

The essential ingredient in quantum computing is the use of the principle of superposition of quantum mechanics. This principle, which is responsible for most of the "ghost-like spooky" properties of quantum systems states that until a quantum system is measured, it exists in a superposition of all possible states at the same time. While a classical computer will store information as ordinary bits, i.e. either as a 0 or a 1 but not both, quantum mechanical computers use quantum bits or "qubits". These objects use states which are superposition of 0 and 1simultaneously. Thus n qubits can represent 2^n numbers simultaneously. The key word here is simultaneously since this means that the quantum machine can perform computations on all of these at once. This is in contrast with the ordinary computers which only process data in a serial fashion. This effect , called quantum parallelism is fundamentally different from the parallel architecture which is being used in some supercomputers. While in the machines with parallel architecture the

tasks are shared between processors, in a quantum computer, it is inherent in the laws of evolution of quantum systems.

This also means that while a set of 10 processors working in parallel can only give one 10 times the speed for a given problem, a quantum computer can be faster by an arbritary large amount, this being governed by the system under consideration. The phenomenon of quantum parallelism could in principle be used to handle complex problems which were beyond the scope of traditional computers. These problems, like the realistic modeling of fluid behavior or that of finding the shortest path which touches some points (" the traveling salesman problem) are so complex that ordinary computers would take a long time to solve them. For instance, the traveling salesman problem with 25 cities has so many possibilities that it would take a machine evaluating a million possibilities a second, close to 10 billion years to go through all of them ! A quantum computer could use parallelism to search through al these possibilities simultaneously.

Since they use inherently different logic than the ordinary two-valued logic used by traditional computers, quantum computers also require new types of logical gates. Two valued logic operates with logic gates like the AND, NOT and OR gates. These form the heart of the machine and allow operations on variables. Quantum logic, because of the superposition principle extends the domain and introduces new kinds of gates like the "square root of NOT" which is something which when applied twice gives us the NOT gate.

The same laws of quantum mechanics which give the quantum computer its power also impose a fundamental restriction on it. The quantum computer must be forever isolated from the environment during the entire process of computation. The superposition principle states that as long as a system is isolated (or more precisely, there is no measurement) it exists as a superposition of all possible states. The interaction with the environment in the process of performing a measurement forces the system to choose one of the possible states. Which state the system collapses to is an essentially probabilistic process and there is no way to definitely predict the outcome of any one measurement. Though this poses a problem for practical realization of these computers, there are interpretations of quantum mechanics, like the many worlds interpretation which can be used to understand the process.

While these developments were very exciting for theoretical computer scientists it was not at all clear as to what use all this was. Though in principle there are many things that only a quantum computer can do, there was no clearly defined procedure which could be used to test whether this spooky quantum parallelism was worth anything at all. All this changed in 1994. In 1994, history of sorts was created in the field of computation when a 129 digit number was factorised. The task took more than eight months and was carried out by 1600 computers, hooked up via the Internet. It is a measure of the enormity of the problem that though proposed in 1977, this humungous number withstood factorization for almost two decades.

The importance of the endeavor lies in the most widely used encryption method known as the RSA, after its inventors, Ronald Rivest, Adi Shamir and Leonard Adelman of the Massachusetts Institute of Technology. This method --- which is almost universally used in encrypting sensitive data, from credit card details to high security defense communications --- relies on the fact that while it is easy to multiply two large prime numbers to obtain a composite number, it is extremely difficult to factorise the composite number. Moreover, the complexity of factorization increases tremendously with increasing number of digits. The 129 digit number, known as RSA-129 was proposed by the inventors in 1977 who challenged anyone to factorise it. Ironically, given the amount of effort involved, the factorization proved the power of the encryption algorithm.

In 1996, a path breaking paper by a computer scientist Peter Shor at the AT&T Bell Labs took the entire community by storm. Shor laid out certain well defined mathematical operations which could only be carried out by a quantum computer and then used them to develop an unambiguous method to factorise large numbers. What was amazing was that this algorithm, using the parallelism inherent in quantum computers, could factorise numbers in a fraction of the time taken by traditional computers. This was a revolutionary discovery because it now meant that all the transactions used by financial institutions, the military and others, which depended on RSA were no longer as safe as they were thought to be. Furthermore, Shor showed that given a quantum computer which works as fast as our present day PC, one could crack the RSA-129 in a few seconds!

Shor's work renewed the computer community's interest in quantum computers and the hunt was on to realize these machines practically. The challenge in building a quantum computer is to have a quantum system which can be controlled (i.e. input and output can be measured) from the outside and yet does not undergo a collapse because of this measurement process. The reconciling of these two, seemingly contradictory demands have posed formidable technical problems for the experimentalists. Nevertheless, there have been several attempts at realizing a quantum computer using a variety of systems. Some groups like David Wineland and Chris Monroe at the National Institute of Standards and Technology have used a trapped beryllium ion to create a quantum gate while others like Hitachi have been using quantum dots to simulate the logic gates. But the enormous amount of effort required to create these systems and the exotic conditions needed to isolate and manipulate the small numbers of qubits which these systems typically possess. has discouraged researchers from looking at these systems for anything practically useful.

In late 1996, there was another startling development which has the potential of changing the paradigm of quantum computing altogether. Two groups of researchers working independently have proposed ways of using liquids as quantum computers with 15-20 quantum bits. This effort is significant because on the one hand, the previous systems could only work with two qubits, thus being incapable of doing anything reasonably complex and interesting. But more importantly, for the first time, a system which is macroscopic is being used as a quantum computer. This is a radical step because quantum systems have been associated typically with microscopic dimensions.

Isaac Chuang of the University of California, Santa Barbara together with Neil Gershenfeld of MIT and Tim Havel, Amr Fahmy of Harvard in collaboration with David Cory of MIT have proposed using nuclear magnetic resonance to develop a tabletop quantum computer. Nuclear Magnetic Resonance (NMR) is a well studied and used technique in chemical analysis and lately medical imaging. NMR involves a strong magnetic field in which the molecules are introduced and "hit" by pulses of radio waves The molecules have atoms whose nuclei behave like tiny magnets (because of their spins) which are acted upon by the magnetic field. Like any other system, the molecules come into equilibrium with a majority of the spins aligned in the magnetic field. Now when the radio pulse of precisely the correct frequency (depending upon the composition of the material) hits the nuclei, they flip their orientation. When the pulse ends, the spins are left precessing and in the process generate a tiny electromagnetic signal which can be detected. This signal gives us the information about the composition of the sample.

The advantage of using NMR systems is that the nuclear spins can remain in any one configuration for unusually long times. This is because they are shielded by the orbiting electrons of the atoms. Typically, while other quantum systems decohere, i.e. . lose their quantum characteristics because of interaction with the environment, in milliseconds, the time scales in NMR systems are of the order of thousands of seconds. This provides a unique system for studying the quantum properties.

Though the problem of decoherence can be solved in NMR systems, there is another problem related to the preparation of the initial state of the sample. Quantum computing requires that the initial sate of the system is a pure state, i.e. in this case there should be perfect knowledge of the direction the spins point towards. In typical systems, at room temperature or even at low temperatures this is not possible because the molecules are moving around at random because of the thermal energy. The researchers then used some ingenious techniques to circumvent this problem and to get the correct answer from the sample. In a brilliant experiment, they have used carbon molecules in alanine to act as qubits and used them to perform simple calculations like adding of two single digit numbers.

All these recent developments might give an impression that a practical quantum computer which can perform miracles like crack high security databases or model accurately the way a typhoon progresses is around the corner. This is not the case. For tackling anything which is reasonably interesting in computation we would need systems with at least a 100 qubits. This is clearly much beyond the scope of the present day experimental techniques. What is required are either radically different technologies or even novel algorithms. But what is clear is that there is a lot of excitement in the field of quantum computing, not so much because of what has been achieved but because of the promise the subject holds for tackling complex problems and opening up new vistas in exploring nature.