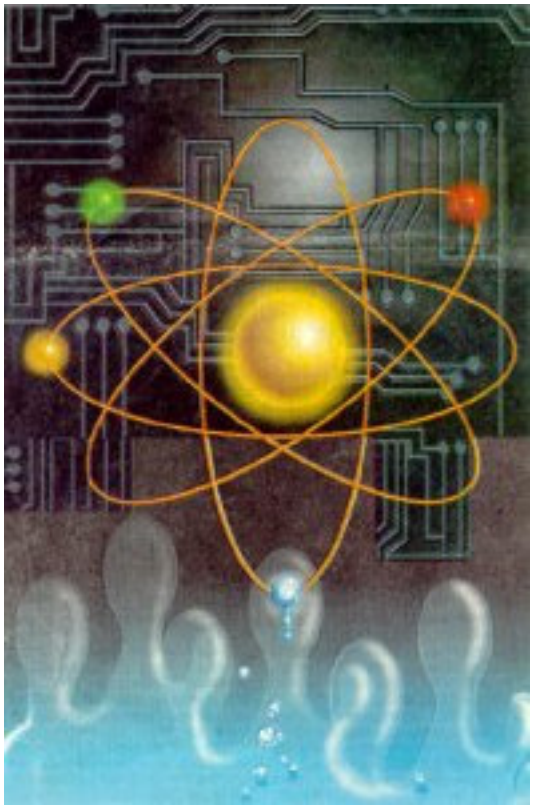
The Final Frontier of Computing: Quantum Computers

Muhammad Aurangzeb Ahmad

Ever since the first computer was constructed more than fifty years ago the general trend has been towards smaller and smaller computers. The trend is in line with Moore's Law that states that the number of transistors on a semiconductor doubles roughly every 18 months with a 50 percent reduction in area. Within the next twenty years a truly amazing milestone would have been reached, transistors would have become the size of a few aggregates of atoms. Going smaller requires manipulating rules of Quantum Mechanics where the laws of Classical Physics and even common sense breaks down. Quantum mechanics describes the world of sub-atomic particles that has many counter-intuitive laws, like a particle can exist in two places at the same time! Not only do the laws of Quantum Mechanics allow us to build smaller computer but they also let us increase the computational power exponentially. Such a computer based on Quantum Mechanics is known as the Quantum Computer. In a Quantum computer there would be no wires, no plugs and no transistors.



The field of Quantum Computing is relatively new, owing its birth to a lecture by Richard Feynman in 1982. Later in 1985 David Deutsch of the University of Oxford published the first paper on a universal Quantum Computer. Not much progress was made over the decade until Peter Shor published his, now Classical, paper on factorization by Quantum Computing. Since then a large number of Quantum algorithms have been discovered and the field of Quantum Cryptology is also budding. At present applications are minimal but

the future is promising. Then there are secure Quantum communication Channels that are also theoretically impossible to hack. In this type of communication information is sent through polarized beams of light. The sender and the receiver then cross check to see the amount of error in the channels. If an eavesdropper has intercepted the transmission then there would be more errors than expected, thus rendering the process fool-proof. There is even a proposal to build a Quantum Neural Network. Neural Networks are based on the same principle as a human mind. A sizable Quantum Neural Network, if built, would behave just like the human mind but exponentially faster.

-- Converted from Word to PDF for free by Fast PDF -- www.fastpdf.com --

The ‘Classical computers’ that we use today store information in the form of 0’s and 1’s, called Bits. In Classical Physics a particle can exist only at a single point in space at a particular instant in time, keeping in line with common sense and everyday life but in Quantum Mechanics such restrictions are not present. A Quantum Computer on the other hand stores information in the form of Qubits (Quantum Bits). Whereas a bit is *either* a 1 or a 0, a Qubit is 1 *and* 0 at the same time! Hence two Qubits can store four bits, three Qubits can store eight bits of information and a collection of N bits can store 2^N bits of information. It would be sufficient to say that a Quantum Computer the size of today’s desktop computer will have more computational power than the combined computational power of all the human beings that have ever lived on Earth. Also it would take a Classical computer 10 million billion billion years to factor a 1000 digit number, where as a quantum computer would take around 20 minutes. Another field that can greatly benefit from Quantum computing is that of Cryptology that deals with the encryption of information. Theoretically it is impossible for a Classical computer to break the encryption if it is transmitted by manipulating the principles of Quantum Computing. Such a promise has even led the American Government to research into the subject.

The problem of factorization would help elucidate the working of a Quantum Computer. Classical Computers and human beings compute the factors of a given number by diving it with the lowest Prime number *i.e.,* 2 and then with the next Prime number (A Prime number is a number that can only be divided by itself or one) and then with the next until it divides completely. A Quantum Computer on the other hand divides the number with all the numbers less than it at the same time! There are however serious pitfalls in constructing a Quantum Computer. Since all the Qubits in a Quantum computer exist in a superimposed state the mere act of measuring *i.e.,* finding out the answer of a computation, forces the Qubits to a Classical state. This process is called de-coherence. The output from a Quantum Computer would then have to be calculated by the constructive interference among the parallel computations taking place inside it. The ‘trick’ lies in finding out the answer without forcing the system into de-coherence.

Last but not least is the idea of Quantum Networking. Two photons can be entangled in a Quantum state and one is transmitted along a line. If a change is brought in the state of one proton the other immediately changes irrespective of the distance involved. It is as if there is no distance involved. The principle of Quantum Entanglement can form the basis for high-speed networking in the future. Progress in Quantum Computing is being made at a frantic pace. Scientists at IBM have been able to construct a Quantum Computer with 10 Qubits. Going beyond this threshold is a big task since de-coherence becomes a greater and greater problem. Currently research is being done in a number of Universities in the United States, Canada, Europe and Japan. A conference on Quantum Computing is held every year and the current will be held at Massachusetts Institute of Technology in the United States later this month. Predictions of construction of a working Quantum Computer range from a few decades to a few centuries, whatever the outcome is, Quantum Computing is surely going to revolutionize our understanding of Computation. Physicist Raymond Laflamme best summarizes the outlook of many scientists, "On my optimistic days I think we will have quantum computers in 20, 30, 40 years maybe; on my pessimistic days, I think quantum computing is crazy."

-- Converted from Word to PDF for free by Fast PDF -- www.fastpdf.com --