Quantum Computer: A computing spaceship

Parth Parikh

November 14, 2017

"If quantum mechanics hasn't profoundly shocked you, you haven't understood it yet." - Niels Bohr

Let's say you have a girlfriend and God forbid she is fussy. Her birthday is about to come and you are obliged to give her a present. You first decide to check her Facebook page to observe her likings, but you are not satisfied. It is then that you decide to embark on a journey to know her true character. By performing this activity, you are optimizing the problem to a greater extent. If you do get an output in the end, chances are quite high that she will love it.

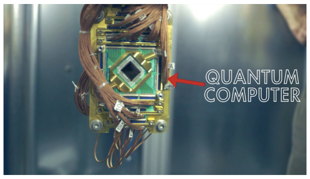
Quantum computers work in a similar fashion. Build on the bedrock of quantum mechanics, these computing hoplites exploit complexities which are otherwise hidden.

What forms the basis of Quantum Computing ?

In one word - 'Qubits'. Qubit is to quantum computer, what cell is to a human body. Anyone familiar with the working of a classical computer knows that a 'bit' is a fundamental unit of information. They are binary digits composed of two values, 0 (or OFF) and 1 (or ON). Unlike binary digits, qubits are quite different. Though the end result is usually 0 or 1, qubits can achieve a state which is a quantum superposition of both these states. The best example to explain quantum superposition is that of the interference peaks from an electron wave seen in Young's double-slit experiment. One has to understand that the moment we start considering light as particle, they would lose their quantum ability. This is just like Schrodinger's cat, wherein if you refrain from looking in the box, the cat maybe dead or alive at the same time. These fascinating units of quantum information have an even fascinating notation $|0\rangle$ (ket 0) and $|1\rangle$ (ket 1).

How revolutionary is Quantum Computing ?

Recently IBM simulated the molecular structure of beryllium hydride (BeH_2) using their $7-$qubit chip. Though it may sound easy but to determine a molecule's ground state one has to consider the quantum effects which occurs with the interaction of their structure's sub-atomic particles. Up until now we were approximating results to a certain extent, but this may soon change. It even gets better, with the company announcing their testing of a 50 qubit quantum computer. These projects can be the founding stone to the theory of quantum supremacy.



Quantum Computer

Another area where quantum computing can show great progress is in the field of cryptography. Public key ciphers such as RSA and Diffie-Hellman can be easily cracked using Shor's algorithm. Shor's algorithm is a quantum algorithm used to find the prime factors of an integer N. Working on the principle of integer factorization, these ciphers are used as digital signatures, used to protect satellite communication, secure web pages, and data. Hence quantum computing can change the look of electronic security in the coming years.

What are the major drawbacks ?

While discussing quantum superposition, we discussed the double-slit experiment. The interference peaks observed were due to the coherence of waves. Coherence in physics is the correlation between all the physical properties of waves or particles. In the double-slit experiment, it helps to explain the wave particle duality. The loss of this quantum coherence is called quantum decoherence. It is usually caused when the system is not completely isolated from it's environment. Quantum decoherence can be lowered significantly by reducing the temperature. Modern quantum computers are cooled to as low as 300 nanokelvins (10^{-9} K) to preserve the coherence.

How has the journey been so far ?

The journey of quantum computing began around the time Led Zeppelin released their fifth album. It was 1973, when Alexander Holevo published the paper "Bounds for the quantity of information transmitted by a quantum communication channel". This paper proved that though n qubits can carry a large amount of classical information (due to quantum superposition), the information retrieved can only be upto n classical bits. From here the journey has been quite steady. During 1980s Yuri Manin and Richard Feynman were among the first to propose the idea of quantum computing. But it was not until in 1994, the year when Peter Shor discovered a breakthrough algorithm, that quantum computing generated attention. This algorithm could factor large integers quickly using integer factorization. Today the world has truly evolved. With IBM Q, one can easily run experiments using IBM's quantum computer using their cloud service.

Will the future be ruled by quantum computers ?

Currently quantum computers are used to fill the holes left open by supercomputers. They are used mainly in molecular research and cryptography. There is no direct benefit of using it as an alternative to classical computers for daily use. However this may soon change with companies like D-Wave, Google and Microsoft heavily investing in this field. Will it give us a breakthrough in medical science or AI ? In an ever so volatile world, only time will solve this mystery.

D-Wave Facility