Quantum Computers

And its prospects

Abstract

M Krishna Kumar  
EN18IITH02029

Conventional computers have two tricks that they do well: store numbers and process stored numbers with simple operations. Both of these are accomplished using transistors. **A transistor can either be on or off**.

One problem is that the basic switching and memory units of computers, known as transistors, are now approaching the point where they'll soon be as small as individual atoms. If we want computers that are smaller and more powerful than today's, we’ll need to do our computing in a radically different way.

Quantum computing takes advantage of the ability of subatomic particles to exist in more than one state at any time.

The idea of quantum computer takes inspiration from two statements

• **Church–Turing–Deutsch principle**

Universal computing device can simulate every physical process.

• A simple class of 'universal simulator' can mimic the behaviour of any finite physical object, by **Richard Feynman**.

A **quantum bit**, or a 'qubit', exist in the classical 0 and 1 states, it can also be a coherent superposition of both. When a qubit is in this state it can be thought of as existing in **two universes, as a 0 in one universe and as a 1 in the other**. The significant point being that by performing the single operation on the qubit, there is operation on two different values. Just as a quantum computer can store multiple numbers at once, so it can process them simultaneously. Instead of working in serial, doing a series of things one at a time in a sequence, it can work in **parallel**. Only when an attempt is made to find out what state it's actually in at any given moment, in other words does it "collapse" into one of its possible states.(**analogous to superposition of two waves**).  
  
In practice, there are many ways to change the state of atoms. One method is to make qubits using **quantum dots**, which are tiny particles of semiconductors inside which individual charge carriers, electrons and holes can be controlled.

Doing complex calculations using a quantum can be a difficult process due to the complexity involved in affecting particles at the atomic scale.

There are a few promising prospects- **Shor's algorithm** (for integer factorisation), and a search method called Grover's algorithm. Another feature is that these machines are able to do immediate **pattern recognition**. What could this mean for the development of **Artificial Intelligence**? Quantum computers can act an **infinite random generator** whose output is verified statistically. Discovering how diseases develop and creating more **effective drugs** to battle them.

Given the high speed of quantum computers and its extraordinary computation abilities to crack any kind of code, there are some serious threats that might arise –in the field of cyber cryptography and security.

Will the future of quantum computers be in light or will it become a dangerous threat? The answer very much depends on the way we use it, as it has always been the case.