

# Quantum Computing

---

## Introduction

During the 1930's key figures such as Alan Turing developed the classical theories of computing. These theories describe the limitations of machine-executable algorithms and are still in use today. It is interesting to note that most of these theories predate the modern computer which only came into existence as we know it during the 1950's. The modern computer has developed rapidly since then, from valve technology through to VLSI integrated circuits. We have already reached the stage where the design features of modern processors are so small that they are being affected by the strange rules of quantum mechanics.

Whilst these effects represent a limit to the size reduction that has been one of the key methods of increasing processor performance, a school of thought has developed believing that maybe these effects can be used to our advantage in some kind of new computer, a quantum computer.

Richard Feynman led the way by producing an abstract model of how, in principle, a quantum system could be used to perform computations. Then, in 1985, David Deutsch published a ground breaking theoretical paper describing how any physical process could be modeled perfectly (in theory) using a quantum computing system. Such a computer, he argued, would be able to perform tasks like true random number generation that no classical computer can achieve. The most powerful feature of a quantum computer would be its ability to use the phenomenon of 'quantum parallelism' to perform certain types of calculations in a fraction of the time taken by a classical computer.

In a quantum computer, the fundamental unit of information (called a quantum bit or qubit), is not binary but rather more quaternary in nature. This qubit property arises as a direct consequence of its adherence to the laws of quantum mechanics which differ radically from the laws of classical physics. A qubit can exist not only in a state corresponding to the logical state 0 or 1 as in a classical bit, but also in states corresponding to a blend or superposition of these classical states. In other words, a qubit can exist as a zero, a one, or simultaneously as both 0 and 1, with a numerical coefficient representing the probability for each state. This may seem counterintuitive because everyday phenomenon are governed by classical physics, not quantum mechanics -- which takes over at the atomic level.

Let's consider a register of three classical bits: it would be possible to use this register to represent any one of the numbers from 0 to 7 at any one time. If we then consider a register of three qubits, we can see that if each bit is in the superposition or coherent state, the register can represent all the numbers from 0 to 7 simultaneously!

A processor that can use registers of qubits will in effect be able to perform calculations using all the possible values of the input registers simultaneously. This phenomenon is called quantum parallelism, and is the motivating force behind the research being carried out in quantum computing.

This superposition of qubits is what gives quantum computers their inherent parallelism. According to physicist David Deutsch, this parallelism allows a quantum computer to work on a million computations at once, while your desktop PC works on one. A 30-qubit quantum computer would equal the processing power of a conventional computer that could run at 10 teraflops (trillions of floating-point operations per second). The fastest supercomputers have achieved speeds of about 2 teraops (trillions of fixed-point operations per second).

Quantum computers also utilize another aspect of quantum mechanics known as entanglement. One problem with the idea of quantum computers is that if you try to look at the subatomic particles, you could bump them, and thereby change their value. But in quantum physics, if you apply an outside force to two atoms, it can cause them to become entangled, and the second atom can take on the properties of the first atom. So if left alone, an atom will spin in all directions; but the instant it is disturbed it chooses one spin, or one value; and at the same time, the second entangled atom will choose an opposite spin, or value. This allows scientists to know the value of the qubits without actually looking at them, which would collapse them back into 1's or 0's.

Researchers at IBM have built quantum computers by using nuclear magnetic resonance (NMR) techniques to measure and manipulate the spin of individual atoms. Radio-frequency energy bursts can begin the "computing" process by changing the energy level of an atom, which might then interact with other atoms in a controlled manner, to establish the patterns of quantum computing that correspond to answers that might be gathered through normal computers.

The quantum computer uses nuclear magnetic resonance to manipulate particles in the atomic nuclei of molecules of trans-crotonic acid, a simple fluid consisting of molecules made up of six hydrogen and four carbon atoms. The particles are like tiny bar magnets spinning in a magnetic field that can be "lined up" by applying an electromagnetic pulse from the nuclear magnetic resonance device. This lining up of spinning particles in positions either parallel or counter to the magnetic field allows the quantum computer to mimic the information encoding of bits -- zeros and ones -- in classic digital computers.

Quantum computer scientists believe they may someday be able to use nuclear magnetic resonance pulses of just the right frequency to manipulate or flip the quantum states of particles with sufficient reliability to create a functional quantum computer.

Los Alamos has been a leader in experimental quantum computation since quantum computers were first proposed in the early 1990s as a way to factor large numbers. The first three-qubit quantum computer was achieved at Los Alamos in 1998 using nuclear magnetic resonance and a trichloroethylene molecule.

## Conclusion

Although the future of quantum computing looks promising, we have only just taken our first steps to actually realising a quantum computer. There are many hurdles which need to be overcome before we can begin to appreciate the benefits they may deliver. Researchers around the world are racing to be the first to achieve a practical system, a task which some scientists think is futile. David Deutsch - one of the ground breaking scientists in the world of quantum computing - said himself that perhaps 'their most profound effect may prove to be theoretical'.

Another important aspect to look at is that probably, the quantum computer would not be suitable to run conventional desktop applications like word processors, spreadsheets etc. This may in turn affect the economics of pushing quantum technology ahead as the target market would be limited, limited to Governments, Secret Service Agencies and similar organizations as quantum computing best suits cryptography and modeling / indexing huge databases.

In comparison the progress in quantum communications has been somewhat more fruitful. Companies like BT have actually achieved working systems that are able to use quantum effects to detect eavesdropping on a channel. Whether or not such systems will prove practical remains to be seen.

Can we really build a useful quantum computer?

Who knows; in a quantum world, anything is possible!