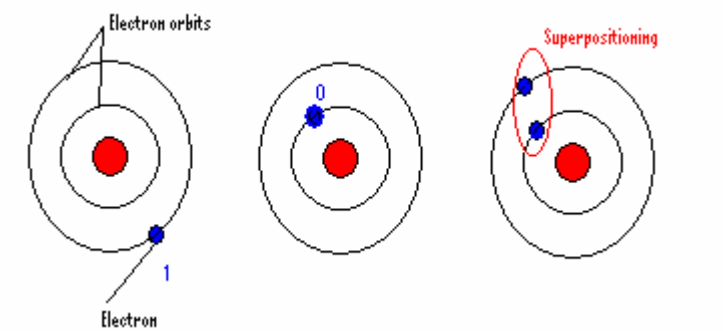
# Quantum Computing

Quantum computing is a surprising older field than most would expect. In Fact, in 1982 Richard Feynman, who originally thought up the idea of "Quantum Computers," won the Nobel Prize for his research on the subject. Back then quantum computing was mostly theoretical. It has not been until recently that the most modern information has come to light.

If you ask someone who has a decent knowledge of computers: what are the basic elements of how the computer functions? They'll say that binary digits arranged in a series of combinations of 1's and 0's are the fundamental elements. But in the quantum world these 1's and 0's are not the only element that hold true. Instead there is one more characteristic, which allows for a '1' and a '0' to exist at the same time. This phenomenon is called "superposition" and it only holds true in the quantum mechanical world.

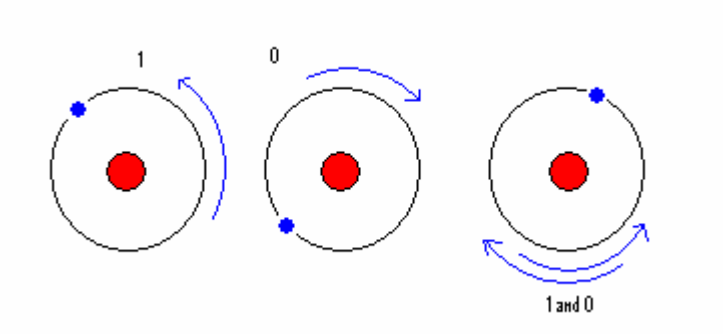
## An Introduction To Qubits:

A *qubit* is the basic data form in a quantum computer much like the bit is the basic unit of data in a classical computer. Below is a method in which *qubits* are stored on an atom. The classical possibility comprised of 2 bits was basically 00,10,01, and 11, but now with the principle of "super-positioning" in a qubit we can have 00,10,01, and 11 in 2 qubits simultaneously.

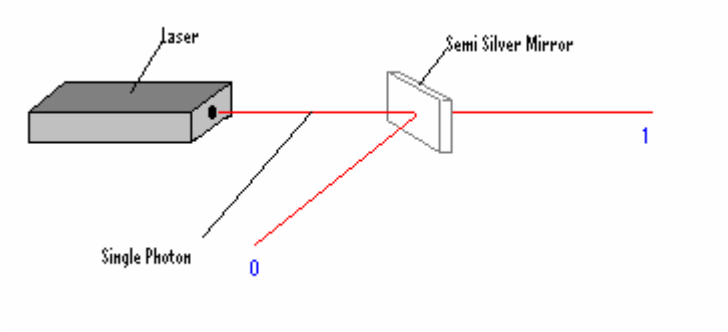



Another way to represent qubits is through the use of quantum 'spin states' that exist in every atom. For example, you could represent the upward of an electron as a 1 and the downward spin as a 0. But even with this type of storage you can also utilize the superposition principle. In essence, the atom would be spinning in both the upward and downward direction simultaneously, almost like the wave affect in the double slit experiment.

With the idea of superposition comes the ability to perform computations simultaneously, which is also known as “quantum parallelism”.




Another way of representing a qubit is with a photon setup as seen below. The idea is to have a semi-silver mirror setup at a 45° angle to the linear axis of a photon gun, also known as a laser. When the photon is shot on the semi-silver surface it can either go straight through, resulting in a 1 or reflect, resulting in a 0. Again, a third possibility can occur in which the photon would split and cause the superpositioning as mentioned earlier.

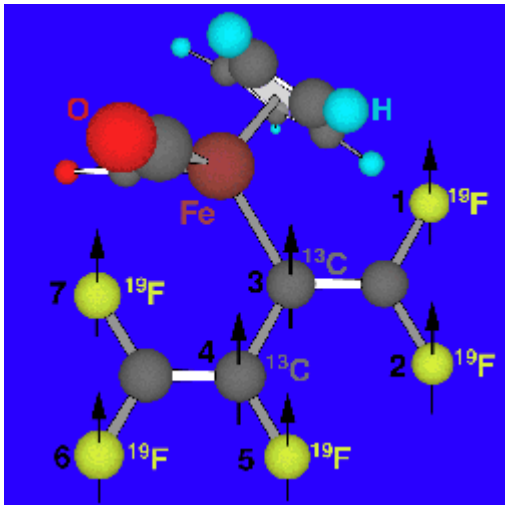



## Putting It All Together:

Quantum computing is very strongly related to the Turing machine, which is essentially some kind of tape with unlimited length and which is divided into small squares. In quantum mechanics these holes can be of the nature of an atom or a photon as a form of storage.

The world’s most advanced quantum processor was first made by IBM. It contains 5 fluorine and 2 carbon atoms each acting as a Qubit. They can interact with each other or be isolated. They can be programmed by radio frequency pulses and detected by nuclear magnetic resonance. By changing the spin on the atom, it helps to relate the processor to more modern methods with which we can process information. Energy bursts can begin the computing process by changing the energy level of an atom, which then interacts with other atoms in a controlled manner to establish the patterns of quantum computing that correspond to classical computing.

The two ways in which quantum computing is achieved is through either Nuclear Magnetic Resonance(NMR) or Cavity Quantum Electrodynamics(CQE).




Nuclear Magnetic Resonance(NMR) has come to be one of the most popular methods, as IBM and several other companies researching qubits have gone this direction with much success. The entire process is essentially based on the use of magnetic fields. The qubits are spun-1/2 atomic nuclei and are manipulated via radio frequencies. However, this is usually only carried out in the single qubit case. When dealing with multiple qubits, spin coupling interaction naturally occurs which happens with the more complex gates. But there has been problems with large groups of qubits because of the spin affect that occurs with the neighboring qubit. (when one qubit hits another it will cause an inverse spin.)

On the other hand, Cavity Quantum Electrodynamics (CQE) computing is still in its developing stages. In this setup, ions are placed inside a type of optical resonator with each atom acting independent and as a qubit. Computing occurs when a photon is shot into the intracavity field, which then causes one or two bit interaction between atoms. The only problem with this design is that the light beam of photons needs to be more precise than current standards allows. But there have been successful trials with 2 bit gates.

The basic problem that exists with quantum computing is controlling the spin interaction of a Qubit, because an atom's electrons are free flowing through the atom in erratic directions. But right when an atom comes in contact with another atom it assumes a standard spin, one of which is opposite to the other. This can be deduced through a pattern that occurs with the other atom with different energy states.

## Quantum Computing Algorithm:

In the case of quantum computing, an algorithm is an essential formula for solving problems. And when you think about it, classical computer programs are nothing but elaborate algorithms, each solving simple parts of the whole.

When you consider a processor, even a quantum one, nothing is more important than coming up with a way to use it. The answer is almost always through an algorithmic way for the computing to be done with the utmost efficiency. Below is a list of quantum algorithms.

Lov K Grover is a technical staff member at Bell Labs. He is the creator of what has been proven to be the best search algorithm that can run on a quantum computing device. Peter Shore of Bell Labs essentially got people going on quantum computing reality with his algorithm designed to factor down huge numbers.

Classical Fastest Factor algorithm: $O(e^{c(\log n)^{1/3}*(\log\log n)^{2/3}})$

Shor's Algorithm: $O((\log n)^2 * \log\log n)$

*Steps for both equations are attached…*

One Quantum Computer can handle much, much greater processing loads. For example, in 1994 a 129-digit number was factored by 16 powerful computers and took 8 months to complete. While with a quantum computer this would be down to a matter of hours.

## Quantum Computing Final Thoughts:

When you think about quantum computers you think there ridiculously powerful, but when thinking this is so much of an understatement. Here is an example now if we take 400protons ex( 0 & 1)….(0 & 1 )^400 in simultaneously stored its 2^400 total. Now this is just about 10^120 numbers stored simultaneously. Now are known universe is about 14billion lights years wide horizontal => 4/3PiR^3 which is about 8.87x10^83cm^3. Now if we take Hubbles constant which is 3H^2/8PiG which is about 1.0x10^-29 grams/cm^3 which in turn is around 5.0x10^-6 atoms of hydrogen per a cm^3. Now if we figure that only about 4.3% of the universe density is of the form of typical atoms so we take the (5.0x10^-6 atoms of hydrogen per a cm^3)x(.04)=2.1x10^-7 atoms/cm^3 of hydrogen times this by the volume of the known universe which comes to around 1.08x10^77 which compared to the 10^120 numbers show how considerably powerful quantum computing can be.

# ***The Pro's & Con's of Quantum computing***

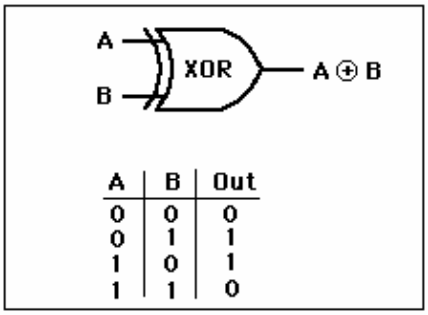
## *Comparison of classical and quantum computing*

Quantum computer's are still in their initial stages of development. This class of computing currently proposes to be the fastest form of computation ever witnessed. The growth of this technology seems to follow a pattern, similar to that of Moore's Law. Moore's Law states that "the concentration of transistors on integrated circuits and the calculating speed of the traditional computer, both double every 18 months."


Gordon Moore
e Robert Noyce

The birth of the three-qubit quantum computer came roughly 18 months ago at Los Alamos. Therefore, a hypothetical 30-qubit quantum computer would be comparable to a usual computer running at 10 teraops (trillion operations per second). So far, the fastest known supercomputers in the world have achieved peak speeds of a mere three teraops. Comparing quantum and classical computers, we observe that classical computing primarily relies on principles expressed by Boolean algebra, operating usually with a 7-mode logic gate principle. Data must be processed in an exclusive binary state at any point in time - that is, either 0 (off / false) or 1 (on / true). These values are binary digits,

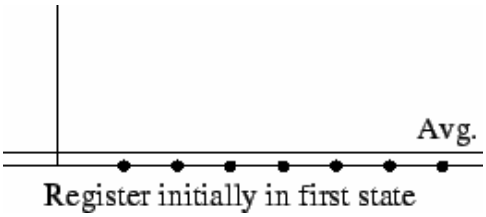
or bits. The millions of transistors and capacitors and various miniscule parts of microchips at the heart of computers can only be in one state at any point in time. Even though the time that each transistor or capacitor needs to be either in 0 or 1 state before switching states is now measurable in billionths of a second, there is still a limit as to how quickly these devices can be made to switch state. Progress is being made and smaller and faster circuits are being developed but we begin to reach the physical limits of materials and the threshold for classical laws of physics to apply. Beyond this, the quantum world takes over. It has a vast amount of latent potential that has been dormant all these years.



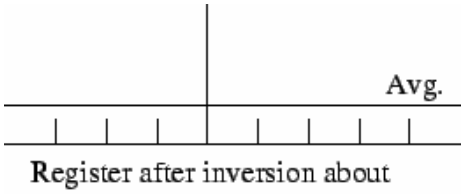

| A | B | Out |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

The Quantum computer, by contrast, can work with a two-mode logic gate: **XOR** and a mode we'll call QO1 (the ability to change 0 into a superposition of 0 and 1, a logic gate which cannot exist in classical computing). In a quantum computer, a number of elemental particles such as electrons or photons can be used with either their charge or polarization acting as a representation of 0 and/or 1. Each of these particles is known as a quantum bit, or **qubit**, the nature and behavior of these particles form the basis of quantum computing. The two most relevant aspects of quantum physics are the principles of superposition and entanglement and are the main reasons why quantum computers would be phenomenally fast compared to their classical counterparts.

This technology will also have a profound effect in the field of cryptography. We mentioned the use of **Shor's algorithm** which could be used to factorize a number with exceptionally large number of digits. Multiplying 65875 by 96354 is still easier to work out than calculating the factors of 6347319750. The complexity of factorizing a numeral increases with addition of more & more digits. "It took 8 months and 1600 Internet users to crack RSA 129 (a number with 129 digits). Cryptographers thought that more digits could be added to the key to combat increasing performance in computers (it would take longer than the age of the universe to calculate RSA 140). However, using a quantum computer, which is running Shor's algorithm, the number of digits in the key has little effect on the difficulty of the problem. Cracking RSA 140 would take a matter of seconds." (see *Shor's algorithm*).



Register initially in first state



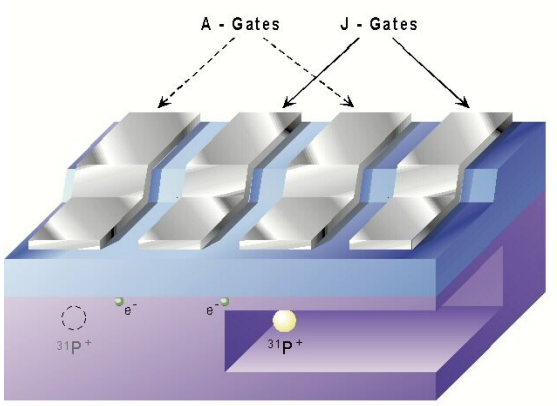
Register after inversion about average.

Another similar algorithm has been written specifically for quantum computers. **Grover's algorithm** aims at saving time while searching through a database. Normally it would take N/2 number of searches to find a specific entry in a database with N entries. Grover's algorithm makes it possible to perform the same search in root N searches. (see *Grover's algorithm*).

One, however has to be very careful while developing this technology & algorithms written specifically for it. The problem lies mainly with the implementation of such algorithms. These programs are capable enough to crack any security passwords over the

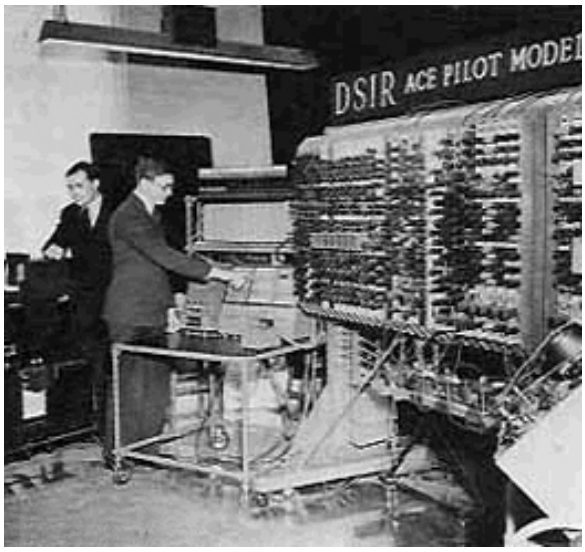
internet, data encryption standards (used for secure financial transactions between banks) etc. A more secure form of cryptography will have to be developed in order to maintain the secrecy of lots of confidential information.

Another problem seems to be the efficiency of the system. Results produced by quantum computers, as it turns out, are inconsistent after repeated usage. In the 1960s and 1970s, Rolf Landauer and Charles H. Bennett at the IBM Thomas J. Watson Research Center did research that investigated the basic physics of computing, which laid the groundwork for quantum computing. Although quantum computing has lots of potential, there are still many problems yet to be solved. According to Landauer, there's the formidable issue of maintaining a coherent quantum system. "A quantum computer has to operate under two conditions that are hard to reconcile," he explains. "The qubits must interact strongly with one another to perform the computations. Yet they must do so without interacting with the environment itself. That's very difficult to do, especially if you're trying to perform computations over any length of time. For example, the thermal vibrations of the frame that holds the bits in their proper positions will cause the quantum logic to lose its coherence. One of the major obstacles of quantum computing is the problem of decoherence, which causes the unitary character (and more specifically, the invertibility) of quantum computational steps to be violated. Decoherence times for candidate systems, in particular the transverse relaxation time T2




*A schematic of a silicon based quantum computer showing phosphorus qubits embedded in silicon*

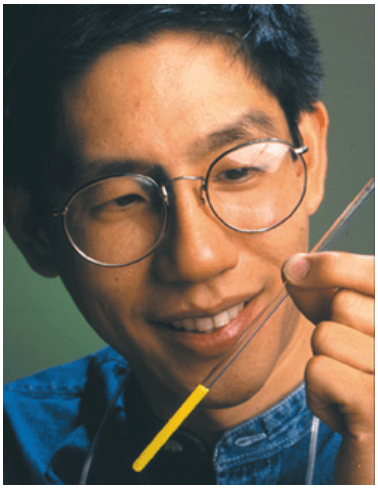
(terminology used in NMR and MRI technology), typically range between nanoseconds and seconds at low temperature. Error rates are typically proportional to the ratio of operating time to decoherence time, hence any operation must be completed much quicker than the decoherence time. If the error rate is small enough, it is possible to use quantum error correction, which corrects errors due to decoherence thereby allowing total calculation times longer than the decoherence time. This implies that each gate must be able to perform its task 10,000 times faster than the decoherence time of the system. Another problem is that flaws in the equipment cause errors to build up--unlike with digital computation, where at every stage the system is pushed back to a level of 0 or 1." (see *Tom Thompson*)




**The very first created by Charles Babbage.**

A major advantage of quantum computers is its size. Currently, the worlds most advanced quantum computer is actually smaller in diameter as compared to a regular test-tube. The size of the computer has kept reducing since the first computer was created.

*Ranges from 10 – 17 inches*



*IBM's Isaac Chuang with the most advanced quantum computer to date*

Quantum computers might therefore prove especially useful in the following applications:

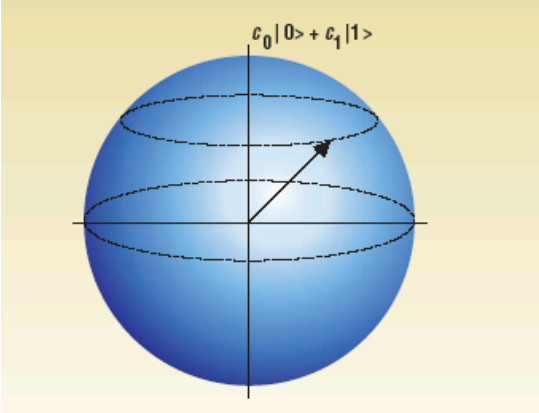
- Breaking ciphers
- Statistical analysis
- Factoring large numbers
- Solving problems in theoretical physics
- Solving optimization problems in many variables

The **main difficulty** that the research-and-development engineers have encountered is the fact that it is **extremely difficult to get particles to behave in the proper way for a significant length of time.** The slightest disturbance will cause the machine to cease working in quantum fashion and revert to "single-thought" mode like a conventional computer. Stray electromagnetic fields, physical movement, or a tiny electrical discharge can disrupt the process.

# APPLICATIONS OF THE QUANTUM COMPUTER

### *NASA's Interest in Quantum Computing*

NASA has begun investing in quantum computing for several reasons. Quantum computers have the ability to store information within incredibly small physical structures, even in the orientation of nuclear spin for example. The advantage that NASA sees in this is that these structures have enormously smaller cross-sectional areas than those of classical circuitry. As a result, the affect of incoming radiation would be much less on a quantum computer than a classical computer. And though that may seem irrelevant to the electronics we deal with everyday, circuits that are orbiting in space have to take into account the impact that different radiations can have.



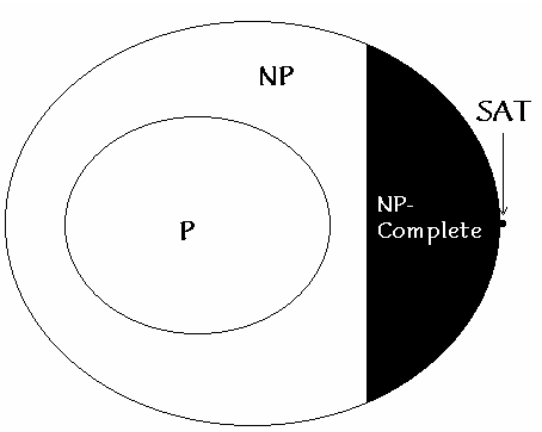

In addition, one of the principles at the core of quantum computers is that they could potentially have the ability to recover any energy which was expended during a computation. In other words, they would be reversible, only dissipating energy in the event that information was erased.

Finally, since it has been shown that quantum computers have the unique ability to perform computations at a much faster rate than classical computers, NASA is interested in their ability to solve "spur of the moment complications." For example, it would be useful to have an algorithm that could quickly make a decision or change a previous plan if a spaceship suddenly realized that it was about to collide with something in space. Currently no such algorithm exists, but the possibility seems to be much more promising in the realm of quantum computation.

### *Attempting To Solve "Non-Classical" Problems*

A common misconception is that the quantum computer will be able to outperform the classical computer in every sense. But that is not true. For example, the simple action of multiplication will not be any faster with the quantum computer. The most valuable tool

of the quantum computer would be its ability to factor incredibly large numbers, and do it in a very short period of time.




This problem is not unique to the factoring of large numbers. In fact, an entire class of problems such as this exist and are called NP Problems (non-deterministic polynomial time). Essentially a particular complication is called NP, or NP-Hard, if the number of steps it takes to solve it is not bounded by a polynomial function. The concept is based on the principles of a simple Turing machine.

Interestingly, with the perfection of quantum computing, just about every standard of encryption we know today would be rendered useless.

### *Artificial Intelligence*

Several experts have taken a philosophical approach towards quantum computing and questioned the possibility of it leading to a form of artificial intelligence. The theory is very broad, as it basically forces you to concede that any physical object can be thought of as a computer, and therefore any action as a computation. This logic is then supposed to lead you to believe that the human mind is therefore a computer, and general consciousness is a computation. Using this argument, along with the Church-Turing principle, several theorists believe that the quantum computer could be the answer to artificial intelligence.

Obviously this theory has many critics who claim that the concept is not even strong enough to merit any consideration. But some seriously attack the theory, hoping to shed some light on the idea. Roger Penrose of Oxford University believes that the principle problem lies in the fact that human consciousness may very well operate on the fundamentals of some exotic, unknown set of physics.