# Quantum Computers: past, present, and future

Alejandro Gutierrez Munoz
Department of Computer Science and Engineering
University of South Florida
agutier2@cse.usf.edu

***Abstract*—For more than over half a century the transistor has dominated the scene of microprocessors, and the primary goal, the reduction of its size, has become paramount in the computer electronics arena. We are approaching the atomic size barrier. The size of the current transistors is shrinking to the point that within the next few years, quantum effects between the atoms will become unavoidable. As the size of the transistors is shrunk, the power consumption and heat generation have become problems that are reaching critical levels. New technologies that explore the real limits of what a computing machine can be, and the understanding of the quantum mechanics properties of subatomic particles in order to exploit the inherent parallelism hidden in their nature, is an exciting field of research. Quantum computing emerges as a new radically different approach to the problem of increasing the actual computing power. The heart of quantum computers lies in the incredible properties of the subatomic world dictated by quantum mechanics; properties like superposition, and entanglement allow the design of new computer architectures.**

***Index Terms*—Quantum computers, quantum computation, quantum technologies.**

## I. Introduction

THE idea behind quantum computers has been around since 1982, when Nobel Prize winning physicist Richard Feynman was investigating the possibility of simulating quantum systems in a conventional computer. After realizing that the storage requirements grew exponentially to the number of particles in the system due to the nature of the quantum interactions between them, Feynman proposed the idea of building a computer using subatomic particles and using the quantum properties of the particles as the base for its computational calculations [1].

A conventional computer is based in what we call a Universal Probabilistic Turing Machine. Alan Turing and Alonzo Church showed that *any algorithmic process can be simulated efficiently using a probabilistic Turing machine*, this assertion is known as the Church-Turing thesis. The physical incarnation of a conventional computer came into fruition after Turing's paper, by the hand of John Von Neumann in what is called a "Von Neumann architecture". After Richard Feynman realized that the requirements needed to simulate a quantum system in a conventional computer in an efficient way were too high, and for small systems they will be overwhelming, and most likely impossible to simulate in a real scenario, scientists started looking for new ways to implement the physical representation of a computer, a new idea that would replace the Von Neumann architecture.

One of the most fundamental physical theories is quantum mechanics, the properties of the matter exposed at a subatomic level were highly attractive to scientists as a possible path in order to represent what a computational machine can achieve using physical elements. The integration of quantum mechanics with the abstraction of a computing machine led to the creation of the quantum computing field. The study of the information processing tasks that can be accomplished using quantum mechanical devices is known as quantum computation and quantum information [2]. Due to the nature of quantum mechanics, the inherent parallelism that can be achieved using the quantum properties of the particles used to build the quantum computer, the advantages over a classical Von Neumann computer are gargantuan.

During 1982 and 1986 Richard Feynman considered the possibility of a quantum system, which could simulate the physical behavior of any other. Since any computer must be a physical system, such simulator would be a universal computer too. Feynman wanted to prove that such simulation system could be used to compute certain problems more efficiently than any classical computer. Feynman simulator was not detailed enough to be considered the first blueprint for a quantum computer.

In 1985, David Deutsch proposed what it can be considered the first representation of a quantum computer. Deutsch's idea was not only specific and simple enough to allow real machines to be contemplated, but also versatile enough to be a universal quantum simulator. Deutsch's system consisted of a line of two-state systems, and it resembled more a register machine than a Turing machine. Deutsch proved that any unitary

evolution could be produced based on an initial set of basic operations, and therefore the evolution of the system would allow to simulate any physical system. He also showed that using a two-state system a Turing-like behavior could be reproduced. These basic operations described by Deutsch are now called quantum gates, since they are the quantum computers counterparts of binary logic gates in classical computers [3].

In the early 1990s computer scientists were interested in finding computational tasks that for a classical computer to solve would take it a very long time but that a quantum computer will be able to solve in a significant less amount of time. During the first years of the 1990s only small differences in performance were found were a probabilistic classical computer could find an answer only with extremely high probability, and a quantum computer was able to find the answer with certainty, restricted by the quantum mechanics properties of the system. The algorithms that were proposed required the quantum system to be noise-free, which for large systems this constrain will become an almost impossible to overcome obstacle. In 1994 Daniel R. Simon made an important advance, he described an efficient quantum algorithm for an abstract problem for which no efficient solution was possible by classical methods, even probabilistic methods. Simon's work inspired Peter Shor, who proposed and amazing quantum algorithm that addressed one of the most important problems is computer science, the factorizing of large integers. Shor's algorithm was not only efficient, but also opened the door for new and innovating solutions to other problems.

Based on Deutsch design and a more formal specification of what quantum information really is, an effort to establish the essential nature of quantum information was underway. The question "how much information can a two-state quantum system store?" was of the utmost importance for computer scientists. Richard Jozsa and Benjamin Schumacher provided the answer in 1994. They showed that the quantum information content of a system can be measured as the minimum number of two-state systems that would be needed to store or transmit the systems state with high accuracy. This concept is now called a quantum bit, or *qubit*. The qubit plays a similar role in quantum information theory to that of the bit in classical information theory [4].

Quantum computing is one of the main research areas of computer science and physics. Researchers are working in several areas. Areas that range from developing new materials and ways to build the building blocks of quantum computers, such as quantum dots and ion traps, to computer scientists working on the complexity of the algorithms trying to discover the real power behind a quantum computer. Quantum computing techniques can be applied in a plethora of computational problems, such as cryptography, communication, and some problems that would fit better in the realm of science fiction novels than in a computational problem such as quantum teleportation.

## II. The Quantum Realm

During the last decade of the 19th century and the first half of the 20th century the science of physics went through a phase of big changes that ultimately led to the creation of a new branch of physics known as quantum mechanics. Quantum mechanics is considered one of the most fundamental and accurate physical theories. Other theories like the Newtonian model and the Electromagnetism theory fail to explain the behavior of the particles at a subatomic level. Quantum mechanics can be considered as a mathematical framework to explain the interactions between subatomic particles. One of the most important aspects of quantum mechanics is the redefinition of what an entity of nature is, in classical physics an entity is either a particle or a wave, in quantum mechanics an entity can behave as a particle and as a wave. Several experiments demonstrated the dual nature of light as a particle and as a wave, this property is known as the *Principle of Wave-Particle Duality*. As proposed by Louis de Broglie in 1923 not only photons exposed this quality, other particles of nature expose the Wave-Particle duality, the electron is an example as demonstrated by Davisson and Germer in 1927 [5].

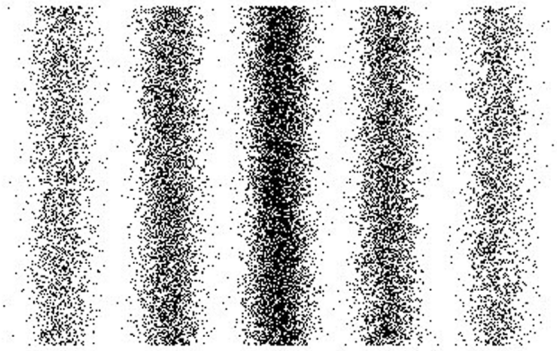

**Figure 1.** Illustration of Wave-Particle Duality exposed by the electron diffraction pattern in a double slit experiment. Courtesy of Boston University Physics Department

The duality exposed by a particle at a subatomic level led physicists to explore new ways to represent the state of a particle in a given system. In 1926 Erwin Schrödinger published a paper that contained an equation known as the *wavefunction*. The wavefunction represents

all of the possible states of a physical system and the *potential* of a particle to be found in certain state. This differential equation is basically the principle of conservation of energy, translated to the new probability-wave formalism of quantum mechanics. A particle can be found in any of the states described by the wavefunction as well as in what is known as a ***superposition*** of states (this term will be key later on this paper in order to understand the inherent parallelism of quantum computing systems) this means the particle can be in more than one state at the same time. Once a measurement has been done to determine the position of the particle, the wavefunction collapses. This means that the probability associated with the states where the particle was not found goes to 0 and the probability of the state (or the sum of the states that were involved in the superposition state) goes to 1. The key point here is that before the measurement the particle was not in a definite state [6].

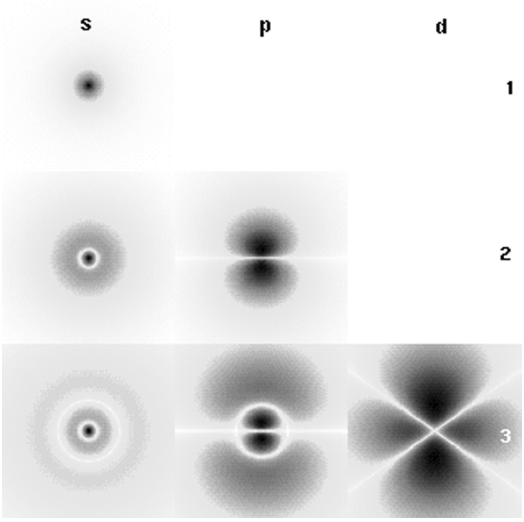


**Figure 2.** The electron probability density. these orbits form an orthonormal basis for the wavefunction of the electron. Courtesy of Wikimedia Commons.

Quantum mechanics dictates that during a given measurement only one property of the system can be known at a time, for example, if we try to measure the position of a particle and the momentum of the same particle only one of these properties will be revealed by the measurement. This problem is known as the *Heisenberg Uncertainty Principle*. The Uncertainty Principle tells us that once we measure either the position or the momentum of a particle the other property will be pushed to a superposition state, making impossible to known for certain the correct location and speed of a particle at any given time. Another phenomena that was product of Heisenberg and Schrödinger theories was the ***quantum entanglement*** (this is also a key concept in order to understand the use of quantum properties during the quantum encryption techniques).

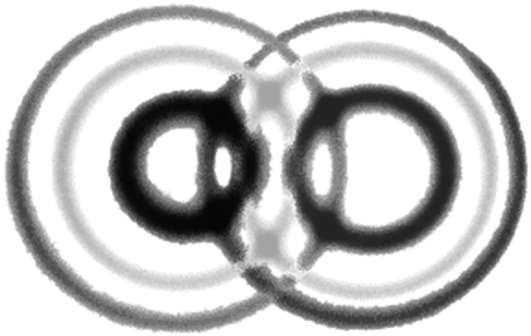

**Figure 3.** Entanglement picture. Courtesy of Anton Zeilinger, Inst. University of Vienna.

This phenomena known as "quantum weirdness" explains the correlation between two different particles at any given distance. This phenomena troubled one of the most important physicists of our time, Albert Einstein. Einstein was not at ease with the idea that one particle can be in "communication" with another particle regardless the distance between them and have immediate effects in the state of the the other particle. This was known as the non-locality property or how Einstein called it "Spooky action at distance." He thought that it was more than a measurement problem rather than a real physical problem. Einstein, together with Podolsky and Rosen proposed what is called the EPR paradox. In an attempt to prove that quantum mechanics as was proposed by the Copenhagen interpretation was incomplete Einstein and his colleagues created this thought experiment that based on conventional properties of physics as the principle of locality showed that quantum mechanics was incomplete. The experiment instead of proving the incompleteness of quantum mechanics refutes the principle of locality and further experiments based on the EPR paradox showed that there exists this correlation between to entangled particles and that any change in one of the particles will affect the other regardless of the distance between them.

The most important work based on the EPR paradox was carried by John Bell. Bell transformed the idea of Einstein, Podolsky, and Rosen from a philosophical speculation into a measurable experiment that could be carried by concrete methods. Bell proposed that if instead of only two properties being affected by the uncertainty principle, there were more properties affected, the question of whether the impossibility of knowing the

position and velocity of a particle at a given moment, was, as proposed by the EPR paradox, imposed by the limitations of physically carrying the experiment, and a particle does have a definite position and velocity; or as proposed by quantum mechanics, a particle does not have a definite state until a measurement is made. This extra property sought by Bell, turned out to be the spin of a particle. Once the spin of a particle was identified to be affected by the uncertainty principle, several experiments were carried over using a statistical framework that proved wrong the assumptions made by Einstein, and his colleagues. Quantum uncertainty applied to spin, shows that the spin of a particle about a given axis cannot be determined simultaneously with the spin about another axis. As shown by physicist David Bohm, the EPR paradox can be extended to the spin problem, and rather than asking about definite position and velocity of a particle, one can ask about define spin values about any and all chosen axis. Quantum mechanics correctly stated that the state of a particle cannot be known with certainty at a given moment, and that a particle can be in multiple states at the same time (this statement is crucial in quantum information theory) [5], [7].

Bell proposed his idea in 1964, and at this time, the technology to carry out the required experiments did not exist. During the first half of the 1970s, the technology became available. Physicists like Stuart Freedman and John Clauser at Berkley, Edward Fry and Randall Thompson at Texas A&M, and during the 1980s the work of Alain Aspect, contributed incredible amounts of experimental data that confirmed Bell's theory. Using Bell's idea, Aspect showed the data from multiple runs of the experiment did not agree more than 50 percent of the time, and if the EPR idea were correct, this percentage would have to be more than 50. Aspect proved experimentally that the EPR statement was flawed, and quantum mechanics was correct in the assumption that there exists a correlation between entangled particles, regardless of the distance between them. And this sort of "communication" between the particles occurs immediately. We could be wondering, how it is possible for two particles to "communicate" themselves immediately regardless of the distances between them? This will imply that information between the particles travels faster than light! This will imply that Einstein's special theory of relativity was wrong! Well, it happens that no information can be transmitted faster than light, and although the two particles separated by great distances can behave accordingly to the behavior of the its partner, since their behavior is random, no data can be recovered from their current state. Remember that if we try to read the state of a particle, its quantum state will be disturbed and the reading will have no relation with the previous state of the system.

After Aspect's experiments the properties of entangled particles abandon the field of science fiction and became a reality, and the "spooky action at distance", as Einstein called it, was confirmed to be happening in the real world. Once a couple of particles have been entangled they shared a connection between them, and this connection is shared across any distance as long as the system is not perturbed from outside. As we said before, no data can be transmitted faster than light, but we can be wondering, what if instead of disturbing the original pair of entangled particles to make a reading, we copy the state of one of the particles, and then we perform a reading in the copy rather than the original; this way the original system will no be affected, and we will be able to transmit data faster than light [5], [6]. Well, for more exciting that this idea might look, it is not possible to copy the state of another particle without disturbing the original system and therefore obtaining a non-related reading of the original state. This is known as the ***no-cloning theorem*** [2].

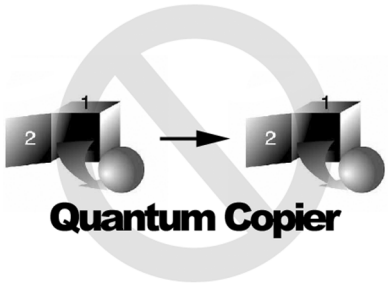


**Figure 4.** Quantum information cannot be copied perfectly.

The measurement of quantum systems presents a puzzle to physicists, the collapse of the wavefunction, and where and when it happens, it is still undetermined. Several ideas throughout the years had tried to explain why, when a measurement to the system is made, the quantum system takes a definite value, and the wavefunction collapses to a spike-like shape. Some of the ideas that involved non-locality models of reality have tried to explain the collapse of the wavefunction. Ideas like the *Many Worlds interpretation*, also called multiverse, and *superdeterminism* models of reality, where everything that happens in reality has been already predetermined, so the illusion of superluminal communication is only a consequence of the initial conditions.

Even though the quantum measurement problem is still unsolved, a possible solution based on a new ap-

proach called ***quantum decoherence*** has presented as a viable solution to the problem. Quantum decoherence explains the collapse of the wavefunction by eliminating the fuzzy barrier between the classical world and the quantum world. The results predicted by quantum mechanics, and our real life experience are described in a radically different way by the decoherence effect. In our real life experience, if we were to analyze a probabilistic event, like the toss of a coin, we would come up with an outcome of a 50/50 probability for the coin to lands heads or tails. This result is not associated with a single instance of the experiment, but with all of the tosses of the coin. Also, we would say that the first toss was not correlated with the last one, or any other for this matter. All of our results and assumptions will be correct, as predicted and showed by our normal experience. Now, in a quantum mechanic framework, we cannot say that each toss is not related to the others, moreover, any toss will be the result of how the different instances, or paths that the result can take, interact with each other.

Experiments had showed that under specific laboratory conditions, where a quantum system is not disturbed by any other element in the environment, the different outcomes of the experiment are closely related to each other. So, if the subatomic world behaves in a different manner than the macroscopic world, why we do not see these effects in our everyday experience? Well, it turns out that the experiments that are carried out in the laboratory are being made under special conditions that are not common throughout the Universe. These special conditions are due to the coherence between the particles not being disturbed, and the collapse of the wavefunction occurs only when a measurement is made, this is, when an external entity interacts with the system, disturbing it. Under normal conditions, every single particle interacts with other particles, even the background microwave radiation remaining from the Big-Bang, that permeates the entire Universe, interacts with any system. Although this interaction between particles sometimes is not enough to cause a system to be disturbed, and hence, collapsing to a definite value, every little interaction "nudges" the system, forcing it to acquire a definite state. If we use Schrödinger's cat as an example, the state where the cat is dead and alive at the same time is not possible, since the system would have been forced to take a definite value before the observer would have opened the door to confirm the state of the cat. Quantum decoherence solves the measurement problem by proposing that a quantum system is forced to acquire a definite state due to small interactions with the environment [5], [8].

Quantum decoherence plays a pivotal role in quantum information processing. Quantum decoherence eliminates the superposition states that are crucial to the exploitation of the real power of a quantum computer. Without the property of superposition, a quantum computer will behave at best as a classical computer. Although quantum decoherence provides a solution to the measurement problem, it creates another one to the isolated quantum systems required for quantum computations. The application of quantum physics to information processing has been limited by great obstacles due to the fragility of the systems needed to do the necessary computations. Decoherence plays two roles in quantum information processing. First, it is a thread to the quantumness of a system, since it destroys the superposition properties of the particles essential to the quantum computation techniques. Second, decoherence is necessary in quantum information processing at the moment of obtaining the results produced by the system, after all, the purpose of every quantum information processing algorithm is to obtain a result, which at the end, it is a measurement. A measurement is made to convert quantum states, and quantum correlations, into classical, definite outcomes [8].

Quantum mechanics provides us with a perfect framework for a new model of computation based on the exciting properties of the matter exposed at a subatomic level. Properties like superposition, entanglement, and decoherence, will serve as the foundation for a radical different approach to process information.

## III. Quantum Computing

Classical physics sets a limit to what normal computers can do, the representation of the most elementary block of information, the bit, is either a 1 or a 0. The conventional approach in order to represent any piece of information is to assign a definite value at any given time to a group of bits. Conventional computers use silicon-based chips, and high and low voltages to represent the possible values of a bit. A quantum computer exploits the properties of the quantum properties of the subatomic particles.

David Deutsch, motivated by the question: is there any model of computation that can solve problems more efficiently than computational models based on the Turing's model? And not only if such model exists, but also if there is a model that can efficiently simulate any other model of computation, Deutsch proposed a model for a quantum computer. Deutsch's model of a quantum computer allowed to challenge the strong form of the Church-Turing thesis. Deutsch tried to define a computational model that would be able to simulate efficiently any arbitrary computational model, and based on the premise that a computer machine ultimately will have to be a

physical entity, thus limited by the laws of physics, he was led to consider a quantum mechanic framework for his computational model. Deutsch constructed a simple example that showed that indeed, quantum computers would be able to solve some problems more efficiently than a classical computer, even a probabilistic Turing machine.

Following Deutsch's footsteps, other scientists proposed innovated ideas for new quantum computing techniques, one of these great algorithms was proposed by Peter Shor in 1994. Shor demonstrated that two of the most important problems in mathematics, the factoring of large integers, and the discrete logarithm problem, could be solved using a quantum computer in a more efficient way than the one possible in classical computers. These two problems are still in the center of debate since it has not been proved yet that there is no an efficient solution using a classical computer. Another important algorithm worth mentioning is the one proposed by Lov Grover in 1995. Grover proposed a novel solution to the search problem in a unstructured search space.

As the concept of quantum computation and quantum computer was being shaped, the concept of quantum information was also under development. In 1995, Ben Schumacher developed a theorem that defined the building block of quantum information, the quantum bit, or qubit. Schumacher based his research work on the previous work by Claude Shannon, who developed back in 1948 a mathematical definition of what information is, the resources needed to communicate information across channels, and the amount of information that can be communicated through these channels. Shannon's seminal work in communication addressed those issues with two theorems. *The noiseless channel coding theorem*, and *the noisy channel coding theorem*. Shannon's theorems show that in order to achieve reliable communication between two channels, error-correction techniques can be applied in order to overcome the noise problem. Shannon's presented the idea of error-correction techniques, but did not specify the set of techniques that will allow a system to reach the limit proposed by his theorems.

Several researchers used Shannon's ideas in order to define a more precise set of error-correction techniques, in order to achieve the limit proposed by the theory. Today, there are a great variety of techniques that are used in several industries, like, computer modems, compact disc players, and satellite communications. These techniques rely on the prevention and recovery of corrupt information transmitted through the communication channels. A similar set of techniques that allow the correct treatment and capturing of information using quantum computers has been developed, and error-correction techniques have become increasingly important in developing new quantum computing algorithms [2].

Quantum computing base its inherent parallelism in the concept of quantum superposition. In order to clearly differentiate between a "classical" bit and a quantum bit, or "qubit", let us show the following example. A classical 3-bit register can represent any value between 0 and 7 (000,001,010,011,100,101,110,111). So, if we assign the value of 101 to a 3-bit register we can say that its value is 5. Now, let us use a 3-qubit register. A single qubit can take a value of 1 or 0 or a superposition of both values 0|1 at the same time. For a 3-qubit register, the register can take any of the 8 values or the a superposition of those values, so a single 3-qubit register can have 8 different values at the same time!

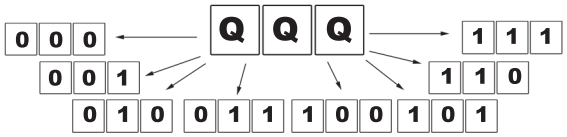


**Figure 5.** Graphic representation of a 3-qubit register.

If we try to define all of the different values that can be represented by a small set of qubits, we can see that even for small arrangements of qubits the number of possibilities is quite big. For example, for a 10-qubit register there will be nearly 1000 different values that can be represented at the same time. For a 20-qubit register the number increases to almost 1,000,000. For a 30-qubit the number is close to 1,000,000,000. As we can see the number of possible values grows exponentially to the number of qubits. For a "small" arrangement of qubits, let us say 300, the number will be so big that not even the number of atoms in the whole Universe will be enough to be compared to that number.

As we can see, quantum computers offer a potential solution to problems that will take a non realistic amount of time to solve in classical computers. As mentioned before, Peter Shor's algorithm for factoring large integers is a perfect example of what can be achieved by using quantum computing techniques. Let us take as an example a really big number:

```
180708208868740480595165 61
644059055662781025167694 01
349170127021450056662540 24  = ? x ?
404838734112759081230337 17
818879665631820132148805 57
```

**Figure 6.** 130-digit number.

The 130-digit number expressed in the figure above can be expressed as a product of two 65-digit prime factors. In order to find those two prime factors using the actual computer power today, it will require several months, and the user of a large network of computers working to accomplish this goal. But what about if instead of a 130-digit number we were interested in a 500-digit number? The number of computer power and time needed will grew exponentially as well with the number of digits, making near impossible to solve with classical computers, not even the age of the Universe will suffice to calculate the prime factors of a 500-digit number using classical computers.

But what about using a quantum computing approach? We have seen that as the number of qubits increases, the number of states that can be represented grows exponentially as well [9]. As we can see, and as Peter Shor did, quantum computers will be ideal candidates to solve this kind of problems. But why trying to find prime factors is so hard? And how exactly can a quantum computer improve the time in calculating these factors in less time? In order to answer those questions, let us express first the factoring problem using an example. Finding a prime factor is like finding the combination of a safe by trial an error. If one code does not work, we would try the next one, and so on and so for, for every single possible combination, until we find the correct code to open the safe. But if instead of combinations, the safe had also a key per each possible combination, and we could test a key at a time. If we could try more than one key at the same time, we could save a lot of time trying to find the right key. That is precisely what a quantum computer does for us; it allows us to try multiple keys at the same time. The bigger the number of qubits in the system, the bigger the number of keys that we can try at the same time. With a quantum computer of some hundreds of qubits a problem like the factoring problem could be solved in some few years, at least it is a realistic amount of time if we compare it with the age of the Universe!

The question of whether a quantum computer is more powerful than a classical computer remains unanswered. In order to analyze the real power of a quantum computer scientists had turned to the theory of computational complexity. In the theory of computational complexity, there is a concept called a complexity class. A complexity class is a set of problems that share the same characteristics needed in resources, this is, space and time, to solve a problem. Two of the most common complexity classes are **P** and **NP**. The class P is the class of computational problems that can be solved in polynomial time by a classical computer. By polynomial we mean in an efficient way. NP in the other hand is the class that contains problems that have a solution that can be checked in polynomial time, or as it is known, a certificate, can be verified in polynomial time, but there is no known algorithm that can yield the solution in polynomial time. The question whether P=NP it is still subject of debate in the scientific community, and it remains as one of the more important questions to be solved in computer theory.

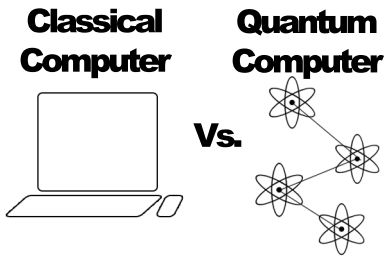


**Figure 7.** Classical Computer Vs. Quantum Computer.

Most scientists believe that NP it is not equal to P, and this is due to a special class of problems that belong to the NP class known as NP-complete problems. If a problem is a NP-complete problem, any other problem in the NP class is as hard as any NP-complete problem. Due to this characteristic of the NP-complete problems, if one efficient algorithm is found to solve an NP-complete problem, it will mean that any other problem in the NP class could be solve in an efficient way as well. There are some other complexity classes described by the theory of computational complexity, one of these classes is the class **PSPACE**. PSPACE consists of all of the problems that can be solved using a small amount of resources in terms of space, this is, the computer required to solve the problem does not require huge amount of memory to solve it, but it requires a huge amount of resources in terms of the time needed to solve the algorithm. PSPACE is believed to be bigger than P and NP, but this remains unproven. Also, there is a complexity class called **BPP**. This class describes the problems that can be solved in polynomial time by a randomized algorithm if a bounded probability of error is allowed in the solution. BPP is said to be more or so as P.

So far, we have talked about the complexity classes of classical computers, but what about the kind of problems that can be solved using quantum computers? There is a complexity class known as **BQP**. This class describes the problems that can be solved efficiently in a quantum computer, where there is a bounded probability of error allowed in the solution, similar to the one in the BPP class. The size of BQP in terms of P, NP, and PSPACE, is still unknown, but it is believed to be somewhere between P and PSPACE. This implies that a quantum computer can solve any problem in P efficiently, but there is no problem outside of PSPACE that can be solved efficiently by a quantum computer. If researchers find that a quantum computer is in fact more powerful than a classical computer, this will imply that P is not equal to PSPACE. This last statement has been the center of discussion by many computer scientists, and it remains unsolved, this shows that the question whether a quantum computer is more powerful than classical computer is non-trivial, and it might take some time to be answered, if ever [2].

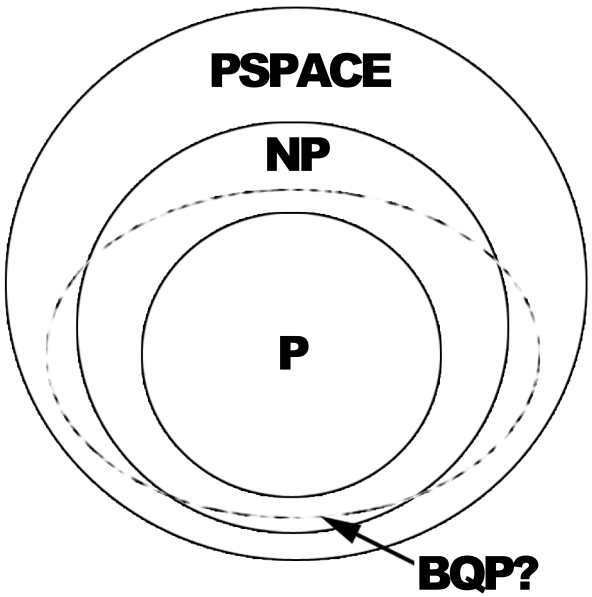


**Figure 8.** Complexity Classes.

There are different models of quantum computation. Models like the quantum Turing machine (QTM), and the quantum circuit model (QCM). Quantum Turing machines are the analogue of the classical Turing machine model of computation, but just as real computers are not build based in the classical Turing machine, since is not practical, quantum computers does not seem to be practical if built as Turing machines. The quantum Turing machine is not practical either when it comes to the construction of quantum algorithms. The model is difficult to work with since when it comes to analyze the state of the system, superposed values of the data in the tape, the position of the memory pointer (the head), and the internal configuration are also in a superposition state. This leave us with difficult questions to answer when it comes to analyze the state of the machine, as different branches of the computation may take different numbers of steps to complete, making hard to determine when the machine actually finished the computation.

In the other hand, quantum circuit is the most popular model, and it has been the most thoroughly worked out. Quantum circuits present a closer picture of the actual implementation of physical devices. Instead of bits, qubits are transmitted in the wires. Quantum gates, represented by unitary operations replace the classical logical gates. In the quantum circuit model, the state of the system is represented by the superposition of the qubits, this is, the data only, not by the superposition of the other components of the system as in the quantum Turing machines. The actual wiring and the number of gates applied to the data are treated the same way as in classical computers. The model is formulated in terms of unitary computation matrices, that given arbitrary n-qubit input vectors, produce the desired n -qubit output vectors. The task of constructing new quantum algorithms is reduced to the construction of such matrices out of simpler matrices. These primitive matrices act over a selected group of qubits at a time. Finding methods for efficient algorithm construction, and finding a universal set of building blocks, something like programming primitives, has become paramount for quantum computing researchers. As in classical circuit model, the quantum circuit model is not a complete computational model. In classical computing, a logic circuit model computes a fixed function based on a given range of input, let us say *n*bits, if the output generated requires a larger number of bits that the one allowed by the circuit, the circuit must be extended to $m > n$ input bits. This is called a uniform circuit family, where an algorithm is needed in order to generate the required data beyond the range of the circuit. The task of assembly the uniform circuit family $\{C_n\}_{n=1}^{\infty}$, cannot be performed by another circuit, therefore a more refined definition of what constructing an algorithm is in the quantum circuit model is required. Each wire in the circuit will carry a two-state qubit (the qubit will be in its superposition state), an *n*-qubit circuit $C_n$ has the ability to perform unitary operations that are represented by a $2^n x 2^n$unitary matrix $U_{C_n}$. Since all of the wires in the circuit carry data, the circuit will perform the same algorithm on the data every time. This would like if the circuit was designed for one and only one purposed, thus it will

not constitute a general purpose computer. In order to avoid this constrain the inputs can be used to provide a program, or rather an instruction that will be carried out on the rest of the input. Quantum gates and wires are the backbone of a quantum circuit. The data in form of qubits is being carried through the wires between the gates, from outputs to inputs. The real processing takes place in the gates. There are no feedback wires, so the number of output and input wires is to be the same for individual gates as well for the complete circuit [10].

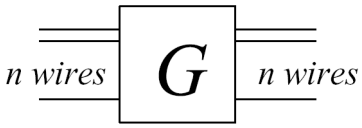


**Figure 9.** A Generic Quantum Gate.

A universal quantum gate, this is, the equivalent of the classical universal gate, can replicate the action of any other gate by repeated use and combination of several universal quantum gates. But what is the set of all possible quantum gates? The answer is found in the principle of quantum mechanics, moreover, Schrödinger's equation. Since all quantum evolution operations are unitary, by generating all unitary transformations of the *n*-qubits in the computer will be enough to reproduce the action of any other quantum gate. As shown by David Deutsch in 1985, a universal quantum gate is rather simple. It can be shown that any $nxn$ unitary matrix can be represented by the composition of 2-qubit XOR gates and single qubit rotations. These two operations are universal for quantum computation. The XOR and rotation operations can be combined to make a controlled rotation which is a single universal gate [4].

Quantum decoherence presents a problem to any quantum computer. The fragility of the system due to environmental factors is really high, and the most minimum interaction with external factors will cause the system to loose coherence. A crucial component of any quantum algorithm, are the error-correction techniques. One of the main concerns of researchers is that quantum computers will be more susceptible to making errors than conventional computers. In conventional computers there are several techniques that can be used to prevent the corruption of the data. For example, redundancy of the data is a pretty straight forward error-correction technique, where instead of having only one copy of the data, multiple copies of the data are stored, and in case that any of the copies gets corrupted by external factors, the corrupted data is restored based on the information contained in the other instances of the data. But how we can protect quantum bits from data corruption using redundancy? We have seen that by the no-cloning theorem a quantum bit cannot be copied since it will disturb the original data. There is a technique that involves five copies of the data (instead of two or three needed in conventional computers). The idea is that instead of storing quantum information in only one qubit, the data is encoded in correlations of several qubits. That way there is not any information present in any of the boxes, and the information that we have protected by the encoding technique cannot be damage by modifying the data of one of the qubits. Furthermore, if one of the qubits is disturbed, the encoding technique is able to determine what was the value before the error and restores the value to its original state. Redundancy can be use to protect the accuracy of the information, but instead of creating multiple copies of the data, the date is shared across multiple units that allow the recovery of the information in case of a disturbance of any of its components [9].

Despite the number of obstacles that quantum computing techniques need to overcome, the potential showed so far by some of the quantum algorithms proposed to day is very encouraging. In some cases the improvement over some classical computer algorithms is exponential, like in Shor's factoring algorithm, and in most of the cases, the improvement over their classical counterparts is at least polynomial. One of the areas that has attracted most of the attention is the area of cryptographic methods. Quantum key distribution (QKD) is a technology based on single photon communications that aims to provide secure communication protocols with a higher level of security compared to the current encryption techniques. Nowadays, the majority of encryption techniques rely in the distribution of public keys, which the sender uses to encrypt the message, and later, the recipient uses its private key to decrypt the original message. These technologies usually support their security in the fact that it will take a really long time for an intruder to decrypt the message. With today's computer power, it might take years for an intruder to decode a message based on the current computational techniques. QKD is unconditionally secure, regardless of what present or future technology an intruder might possess; QKD bases its security in the laws of Nature. Because a photon is an indivisible elementary particle, and intruder will have to use a more sophisticated method than "listening" to the transmission, this is because Heisenberg's Uncertainty Principle ensures that any active attack will disturb the message, and it will prevent the attacker to read the key of the transmission [11].

Quantum computing is an exiting field of research, its applications range from small to large size imple-

mentations. Quantum computing techniques exploit the inherent parallelism provided by the superposition property of quantum systems, and tasks that look daunting and most likely impossible for current computers, could be one day achieved using quantum computers.

## IV. Quantum Hardware

The idea of having a computer so powerful that with a small number of qubits we can accomplish tasks that will require incredible amounts of resources in a classical computer is really encouraging, but the reality is that the process of building a quantum computer so far has proven very difficult. The main reason behind this difficulty is that trying to isolate single atoms and manipulate them in order to perform the quantum computations is really complicated. During the last two decades, several techniques like ion traps and quantum dots have dominated the scene, but new techniques and error correction algorithms have bolstered the improvement of the methods to isolate and work with an array of atoms. So far the biggest quantum computer in the world uses an array of seven qubits. Not only the qubits but also the quantum gates must be built in order to produce a real quantum computer. There are several requirements that any quantum hardware component must meet. These requirements are known as the "DiVincenzo checklist": [12], [13].

- Clearly identifiable qubits (an enumerable Hilbert space) and the ability to scale up in number.
- "Cold" starting states (e.g. the ability to prepare the thermal ground state of whole system).
- Low decoherence (so that error correction techniques may be used in a fault-tolerant manner).
- Quantum gates (the ability to realise a universal set of gates through control of the system Hamiltonian).
- Measurement (the ability to perform quantum measurements on the qubits to obtain the result of the computation).

The most important technologies nowadays are [14], [15]:

- Ion traps: the qubit is stored using different levels of energy of an ion.
- Quantum dots: it is based in the control of the spin of a trapped electron in a semiconductor nanocrystal.
- Superconductors: the qubits can be encoded using two superconductors separated by an insulator and applying an electrical charge.
- Cluster state quantum computers: this methodology exploits the entanglements between qubits. Creating the entanglement beforehand much of the hurdles of the other methods can be overcome.

Ion traps store qubits using different energy levels of an ion. Manipulation of the vibrations sensed through electromagnetic fields is needed in order for ions to transfer information to each other. At the moment researches have been able to create and entangle several qubits at a time, but working with thousands of ions in one trap have proven very difficult.

Some ideas have been proposed to manipulate several ion traps instead of one, and allowing certain ions to transfer information between distant groups of traps. It is currently possible to carry out experiments that require 2 or three qubits, but for a realistic quantum computer to be feasible, thousand of qubits will be needed. Clearly, ion traps represent a good start in order to represent quantum bits, but still has a long way to go before practical uses can be exploited based on this technique [14], [9].

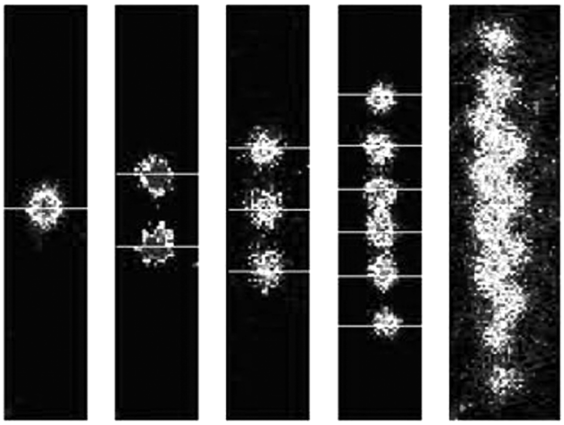

**Figure 10.** Images of 1, 2, 3, 6, and 12 magnesium ions loaded into NIST's new planar ion trap. Courtesy of National Institute of Standards and Technology

During the last decade, significant progress has been made in designing quantum computer hardware. Early work during the 1990s in ion traps, nuclear magnetic resonance, and cavity quantum electrodynamics, has served as a strong foundation in designing quantum computer hardware in solid-state quantum electronics. Current techniques in microprocessor fabrication provide an excellent framework and bring to the table years of experience in solid-state technologies design.

Different schemes in order to represent the information are used in current technologies, from electric charge, nuclear spin, magnetic flux, superconducting phase, or electron spin. Each scheme presents some advantages and disadvantages over the others, but the main idea of harnessing quantized charge is particularly

appealing since current techniques being used to fabricate superconducting circuitry, like e-beam lithography equipment can be used in the construction of qubits.

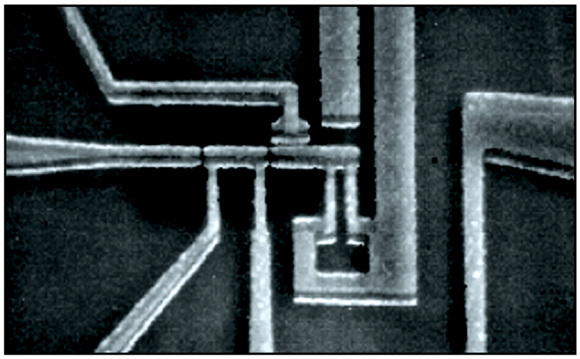

**Figure 11.** A single qubit, implemented as a quantized charge device fabricated in aluminum using e-beam lithography in a superconductor, electrons pair up as Cooper pairs. Courtesy of IEEE Intelligent Systems

Also, crucial quantum properties, like quantum coherence, and entanglement, have been demonstrated experimentally. Having a physical system that can maintain these two properties make solid-state technologies a strong contender for the basic element in the construction of quantum bits [11]. Quantum dots are one of the most hopeful candidates for solid-state. Manipulating the electron's spin or by exciting the electron to make it leave its regular spot in the crystal, researchers control the state of an electron trapped in a semiconductor nanocrystal, or quantum dot, in order to store the information. Researchers make use of lasers or sending electric charges to the dots to accomplish this manipulation of the spin[14].

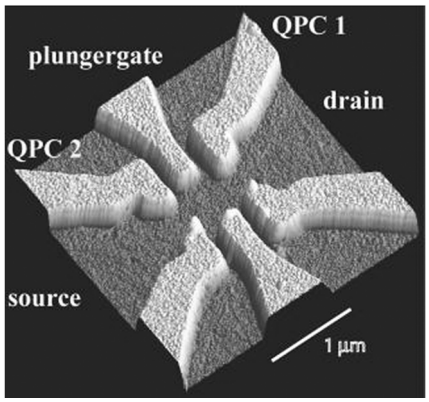


**Figure 12.** Quantum dots on parabolic quantum wells. Courtesy of the Swiss Nanoscience Institute

Another technology to store information in quantum bits is related to superconductive materials. Qubits based on quantum properties of superconducting materials, which exhibit no electrical resistance at very low temperatures. Using an electric charge, the direction of the current flow, and a quantum property called phase are encoded using two superconductors separated by an insulator. The flux qubit has two fundamental quantum states that have current circulating in clockwise and counterclockwise directions. The measurement of the state is performed by a superconductor quantum interferometer, or DC-SQUID. The DC-SQUID is aligned close to the qubit. The DC-SQUID can detect the magnetic flux generated by qubit circulating current. This approach uses established technologies, and it presents a promising idea in the development of further quantum registers [12], [14].

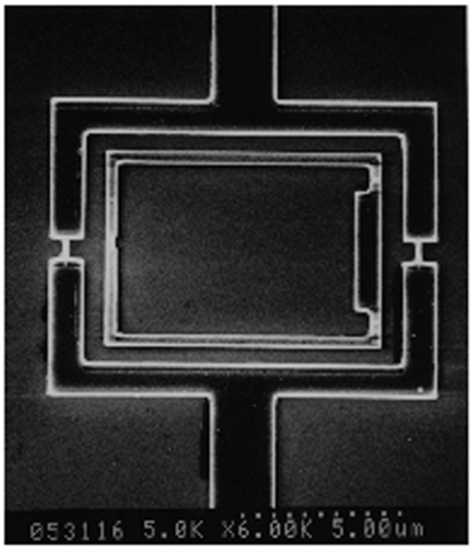


**Figure 13.** Picture of the qubit and DC-SQUID. Courtesy of the Tokyo Institute of Technology

In the summer of 2005, theorist Simon Benjamin, a University of Oxford physicist, told David Deutsch about cluster states, a new idea that could solve the major problems that quantum computers have encounter in order to become a reality. The idea is based in a new approach of how a quantum computer processes the information, and instead of dealing with the hardest and trickiest parts of the calculation on the fly; it deals with the possible problems that may arise from the beginning of the setup of the system. The new idea also will allow bigger systems to be developed, since its scalability is far greater than the one displayed for its predecessors. Deutsch, the original designer of the first blueprint of what a quantum computer should be, thinks that a quantum computer is within 10 years.

Early versions of quantum computers, like energy levels of ions trapped in electric fields, qubits stored as polarization of photons, nuclear spin and electron spins

within nanocrystals, also known as quantum dots, have all presented problems while maintaining the entanglement properties of the system. Also, these techniques presented the problem that for large systems the technical problems were really difficult to overcome. In all of these models of quantum bits, quantum computations were being performed by manipulation of the qubits being held close together. Normally a laser pulse was used to manipulate the qubits, and to create the entanglements between them. As the qubits get closer together is was hard to manipulate one particular qubit without disturbing their neighbors. This disturbance, or quantum decoherence, forced the qubit to take a definite state, in order words, to become a value of 1, or 0, and halting the whole quantum computation. Any measurement within the system was forced to be done only at the very end of the calculation. Due to these limitations and constrains, researches had managed to control about 10 qubits simultaneously. The progress in the quantum computing field was growing at a very slow rate.

The idea of cluster states, originality presented in 2001 by Robert Raussendorf and Hans Briegel of the Ludwig Maximilian University in Munich, Germany, provides a novel architecture for quantum computers. Instead of dealing with the entanglements during the calculations, all of the necessary relationships between the qubits are laid out at the start up of the calculation. This approach is also known as one-way computing. The idea came from a similar set-up known as optical lattice, in which a grid of lasers traps uncharged atoms at their intersection points.

In order to create multiple entanglements of qubits, lasers are used to move rows of qubits close together. One limitation here is that in entire rows of qubits need to be moved in order to create the required entanglements, since the manipulation of individual qubits will cause possible disturbance to the system and increasing the decoherence factor within the calculation. In a cluster state, operations are performed over a particular set of qubits at each step, instead of performing multiple operations over time on a given set of qubits.

In a cluster state computer, a set of qubits aligned in a row represent each step of the calculation. In a past system, if the algorithm performs five operations in order to yield a result, these calculations would have been made using the same set of qubits. In a cluster state computer, each operation uses only one set of qubits. Entanglements within a column represent operations between multiple qubits, while entanglements within a row represent the time steps of the calculation. Once the grid of entangled qubits is created, the computation is carried out one column at a time. Based on the results of the first column, physical adjustments are made to the next column. The same procedure applies to all of the columns in the grid. The final result of the calculation is the result of the last column. It might seem that cluster states is only a workaround to how the calculations are being made, and also, that an unnecessary numbers of extra qubits are required to performed the calculations, but in order to see the full potential of this technique we must keep in mind, that at each step of the calculation a different set of qubits is being used, making easier to entangled the qubits, and making easier to perform a measurement to the system, which is exactly the hardest part in the other models [14], [15].

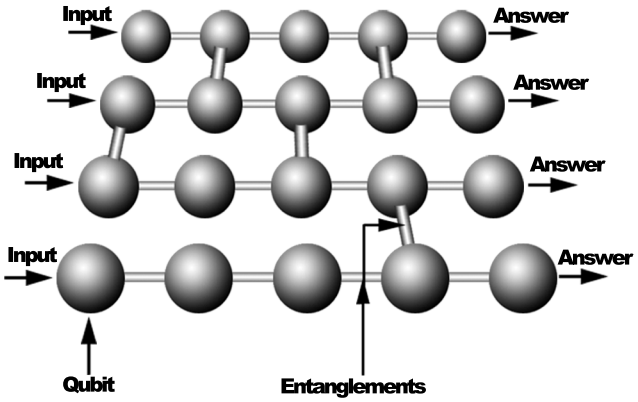


**Figure 14.** A cluster state quantum computer.

## V. Quantum Algorithms

Back in 1981 when Richard Feynman asked the question if a quantum system could be simulated in a computer and after realizing that it could be in theory simulated but it will take too long for a simulation to run, it was then when he proposed the idea of creating a computer that was based on the quantum properties of the subatomic particles. Quantum computers and its inherent parallelism allow to solve in a faster manner computational problems that otherwise will take thousands of years to solve using the actual computer techniques. We would be tempted to ask if a quantum computer can do something that a classical computer cannot, and the answer is no. Using a Universal probabilistic Turing machine, in what is known as the Church-Turing thesis [2], any algorithmic problem can be simulated using a Turing machine. The key point here is that using quantum computers we can solve problems that are consider “hard” in a timely manner. Quantum computers do not solve any problems that in theory cannot be solved using a classical computer, but it introduces a new set of computational complexity and the possibility of solving problems that would otherwise

be near impossible to solve. A great example of the huge difference in computing time that can be achieved using a quantum computer versus a classical Von Neumann computer is the Peter Shor's algorithm which computes the factorial of very large numbers [4]. Another good example is the Lov Grover's search algorithm. Grover's algorithm reduces significantly the amount of comparisons required in order to find an element in an unsorted array [11].

A quantum algorithm consists of a series of operation over a group of quantum registers. A quantum register is a set of qubits whose value can be represented in a vector-like form: $state: a|0\rangle + b|1\rangle$ where $a^2 + b^2 = 1$. The operations that are applied to the vectors are called transformations. Now, you might be wondering how we can apply a transformation without disturbing the state of superposition. Remember that the superposition state collapses once a measurement occurs. The answer is quite simple, no measurement is necessary in order to apply the transformations. The transformations are independent of the measurements. In fact, the transformations take advantage of the interactions between the qubits to produce destructive interference patterns that will decrease the potential of the wrong solution to appear, leaving at the end only the correct solution as the one with the higher potential [16].

During the last two decades, a variety of quantum algorithms have been created trying to address basic computational problems, and also trying to demonstrate the potential of quantum computing techniques. Some of these algorithms present an exponential improvement over their classical counterparts; some others display only polynomial improvements over implementation of the same algorithms in classical computers. A good example of a computational problem that can be solved faster in a quantum computer is what is called quantum search. Although the improvement over traditional computing techniques is in the polynomial order, the versatility offered by quantum computing approaches exposes speedup in certain scenarios in the exponential order.

Quantum search attacks the problem known as the unstructured search problem. This problem can be described as if we were given the value that we want to find in a dataset, we would have to search every possible position in the dataset in order to find the position of the value in the dataset. Important real life applications, like searching for cryptographic keys, fall into this category of problems. In a conventional computer trying to find the correct key will involved searching the correct one in a set of almost $2^{56}$ possible keys. If we could process 100 million keys per second, this problem will take 23 years to solve using todays computer power. A quantum computer running at the same rate could use a quantum search algorithm to find the correct key in about four years. A conventional computer will need $O(n)$operations in the worst case in order to find the correct key, and it will take $O(\frac{n}{2})$ operations in average.

Can we do better? Can quantum computing techniques give us a significant improvement over these values? Quantum computers are not bounded by the same limits as classical computers, and exhaustive searches does not have to limit to check one entry in each step. Using quantum parallelism several candidates can be checked at once. But there is a price to pay, the same rules that allows quantum searches to be perform in parallel prohibit the result to be checked before the search has finished, this is due to possible disturbance of the system, and the introduction of quantum decoherence at the moment of measurement. Fortunately, despite this inconvenient, quantum search techniques offer a significant improvement compared to their classical versions.

Lov Grover, a computer scientist at Lucent Technologies Bell Labs, discovered the quantum search algorithm in 1996. The algorithm solves the quantum search problem under the assumption that exists an oracle that can decide if a possible solution is the real one or not. The oracle is constructed as a black box, and the key point in Grover's algorithm is to consult the oracle as fewer times as possible. Grover's algorithms results in a worst case of $O(\frac{\pi}{4}\sqrt{n})$.

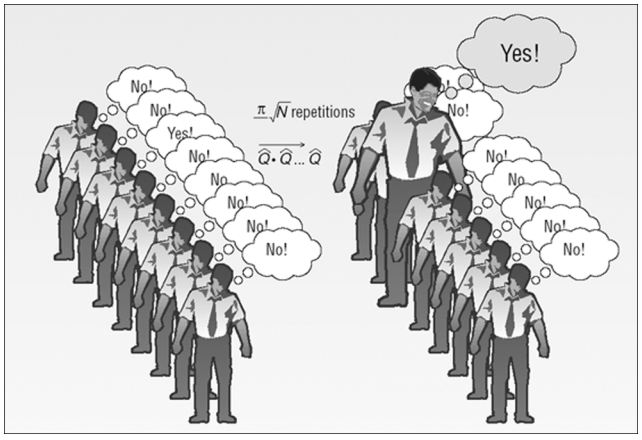


**Figure 15.** Quantum Computer Oracle
Courtesy of IEEE Intelligent Systems

As we can see the improvement is only in polynomial time, but for large entries of n, the time the difference between the classical and the quantum algorithm is very significant. Quantum search has been proven to be very versatile. One of the most efficient classical algorithms to solve hard computational problems such as constrain

optimization is the so-called randomized algorithm. Randomized algorithms work either by converging to a desire solution after a certain number of steps, or they try with no result to find the result to the problem in a region of the solution space, and after an specific time they decide that the solution was not found and run the whole algorithm using a different random number generator. Quantum search can improve the time given by randomized algorithms; every pseudo-random number generator requires a seed that will serve as the input value to the generator. The idea is to use a superposition of seeds; this will create a superposition of final states that more likely will contain the correct answer to the problem.

Quantum search techniques can be used to find statistical data related to the solution space, like means, medians, maxima, and minima. All of these calculations can be achieved in the squared root of the number of steps required in a classical computer. Another application for quantum search is as subroutines inside another quantum algorithms. A good approach to use this technique is to use the quantum Fourier transform, developed in Shor's algorithm, in conjunction with the quantum search amplitude capabilities. A problem where this approach can be use is we are trying to find the number of possible solutions in a problem. We could effectively count how many solutions the problem admits even though we do not know what those solutions are.

One more application where the quantum search technique can be applied is in the domain of experimental physics to prepare selected superposition states. The use of oracles that decide whether or not a state correspond to the desired superposition state can be used to systematically manufacture the desire states, this way quantum search algorithms could have several applications in experimental physics. [17].

One of the most important applications of quantum computing techniques is that of simulating some other quantum system. Quantum systems are very difficult to simulate in conventional computers, as pointed out by Feynman in 1981. In order to simulate a $2^n$ dimensional state vector in a Hilbert space, it is necessary to manipulate vectors containing of the order of $2^n$complex numbers. A quantum computer will require only *n* qubits. Both classical and quantum computers need to manipulate matrices that grows exponentially to the number of elements in the system, so there is guaranteed that a quantum computer can simulate efficiently any physical system, but the order needed for a classical computer to manipulate the vectors will involved matrices of the order of $2^{2^n}$ elements, while quantum computers will require $2^n$ unitary operations to handle the evolution of the system in a Hilbert space. Regardless of this exponential factor, it can be shown that quantum computers can simulate efficiently certain systems that are not known to have an efficient simulation in classical computers; systems like the many-body systems with local interactions [4].

There are many other important quantum algorithms, like the Period Finding algorithm, that works based on the quantum Fourier transform. Another good example is Peter Shor's algorithm for factoring integer numbers. The process of factoring large numbers is so limited in classical computers, that most of the securities codes used today base their security on the difficulty to calculate the correct prime factors of a large number. After Shor developed his algorithm, which provides an exponential improvement over its classical counterpart, several security entities were interested in the emerging field of quantum computation, the National Security Agency must guarantee their security codes to be safe for at least 30 years, since based on Shor's algorithm their codes could be in jeopardy, the NSA is an active collaborator in the discovery of new encryption techniques that rely on quantum computing techniques to safeguard their security codes [16].

## VI. Conclusion

Quantum computers represent a very promising idea of what it could be the future of computation. Although their real power is still undetermined, and many technical and physical hurdles pave the way for its development. Quantum computing techniques and its early results encourage the scientific community to continue in the quest to exploit its full potential. Technological advances, and new discoveries in the realm of physics, aid the development of quantum computers. New techniques like cluster state computers, photonic devices, and superconductors, are still in their infancy, and as these technologies evolve, new uses in the quantum computer arena can be applied.

The theory of computational complexity has not yet determine the potential of a quantum computer, and although this could take some time, when it finally reaches the answer of whether there are problems that can be solved efficiently in a quantum computer that cannot be solved efficiently in a classical computer, the real potential of quantum computers will be unleashed.

Ideas and theories from other areas of science, such as physics, statistics, and computer science, serve as a foundation to the development of new techniques in quantum computing. Combination of different computing techniques, such as randomized algorithms with quantum

computing algorithms yield very promising results. The future of quantum computers is still uncertain, but everyday more and more members of the scientific community are realizing the potential of this technology. Several government entities are founding research projects in the area of quantum computation, and several important physics problems could be solved more efficiently once a quantum computer became a reality.

The importance of a good background in quantum mechanics makes the involvement of computer scientists a little bit more difficult than other research areas. Nevertheless, the impact of quantum physics is permeating every aspect of several scientific areas, and as every day passes, more and more knowledge of this area of physics is needed in order to develop the full potential of what computers can achieve. The inclusion of quantum mechanics courses and a proper interaction with other areas of the scientific community will became of great importance for the development of this exciting area of research.

## REFERENCES


[1] G. J. Beach, C. Lomont, and C. J. Cohen, "Quantum image processing (quip)." in *AIPR*, 2003.

[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, October 2000.

[3] D. Deutsch, "Quantum theory, the church-turing principle and the universal quantum computer," *Proc. R. Soc. Lond. A*, vol. 400, pp. 97–117, 1985.

[4] A. M. Steane, "Quantum computing," *REPT.PROG.PHYS.*, vol. 61, p. 117, 1998. [Online]. Available: http://arxiv.org/pdf/quant-ph/9708022

[5] B. Greene, *The Fabric of the Cosmos: Space, Time, and the Texture of Reality*. Knopf, February 2004.

[6] G. Zukav, *The Dancing Wu Li Masters: An Overview of the New Physics*. Harper Perennial Modern Classics, July 2001.

[7] D. Deutsch, *The Fabric of Reality*. Penguin, 1997.

[8] W. Zurek, "Decoherence and the transition from quantum to classical," *Phys. Today*, vol. 44, pp. 36–44, 1991.

[9] J. Preskill, "Making weirdness work: Quantum information and computation," *Quantum Information Lecture Notes*, 1998. [Online]. Available: http://www.theory.caltech.edu/people/preskill/talks/ieee.pdf

[10] A. K. H. Bengtsson, "Quantum computation: A computer science perspective," Nov 2005. [Online]. Available: http://arxiv.org/abs/quant-ph/0511274

[11] R. J. Hughes and C. P. Williams, "Quantum computing: The final frontier?" *IEEE Intelligent Systems*, vol. 15, no. 5, pp. 10–18, 2000.

[12] J. Tejada, E. M. Chudnovsky, E. del Barco, J. M. Hernandez, and T. P. Spiller, "Magnetic qubits as hardware for quantum computers," 2000. [Online]. Available: http://lanl.arxiv.org/ftp/cond-mat/papers/0009/0009432.pdf

[13] D. D. Thaker, T. S. Metodi, A. W. Cross, I. L. Chuang, and F. T. Chong, "Quantum memory hierarchies: Efficient designs to match available parallelism in quantum computing," in *ISCA '06: Proceedings of the 33rd annual international symposium on Computer Architecture*. Washington, DC, USA: IEEE Computer Society, 2006, pp. 378–390.

[14] D. Cho, "Quantum computers: March of the qubits," *New Scientist magazine*, vol. 165, no. 2544, p. 42, 2006.

[15] P. Blythe and B. Varcoe, "Quantum Computing Using Crossed Atomic Beams," *ArXiv Quantum Physics e-prints*, May 2006.

[16] P. K. Amiri, "Quantum computers," *IEEE Potentials*, vol. 21, no. 5, pp. 6–9, 2002.

[17] C. P. Williams, "Quantum search algorithms in science and engineering," *IEEE MultiMedia*, vol. 3, no. 2, pp. 44–51, 1996.