**I. INTRODUCTION**

Quantum computers use atoms to perform calculations. Here, computation depends on principle of quantum theory. In the quantum scenario, the fundamental unit of memory is called a qubit.

Civilization has advanced as people discovered new ways of exploiting various physical resources such as materials, forcesand energies. In the twentieth century informationwas added to the list when the invention of computers allowed complex information processing to be performed outside human brains. The history of computer technology has involved a sequence of changes from one type of physical realization to another --- from gears to relays to valves to transistors to integrated circuits and so on.

Today’s computers are classical, a fact which is actually not entirely obvious. A basis of modern computers rests on semiconductor technology. Transistors, which are the “neurons” of all computers, work by exploiting properties of semiconductors. Classical computers are in a certain, restricted, sense quantum mechanical, because, as far as we understand today, everything is quantum mechanical. No, classical computers, although based on quantum physics, are not fully quantum, because they do not use “quantumness” of matter at the information-theoretical level, where it really matters.

Gordon Moore proposed Moore’s law in 1965, which originally stated that processor power and speed would double in size every eighteen months (this was later revised to two years). This law still holds but is starting to falter, and components are getting smaller. Soon they will be so small, being made up of a few atoms that quantum effects will become unavoidable, possibly ending Moore’s law. There are ways in which we can use quantum effects to our advantage in a classical sense, but by fully utilizing those effects we can achieve much more. This approach is the basis for quantum computing.

**II. HISTORY**

1982-Feynman proposed the idea of creating machines based on the laws of quantum mechanics instead of laws of classical physics.1994-Peter shor came up with a quantum algorithm to factor very large numbers in polynomial time.

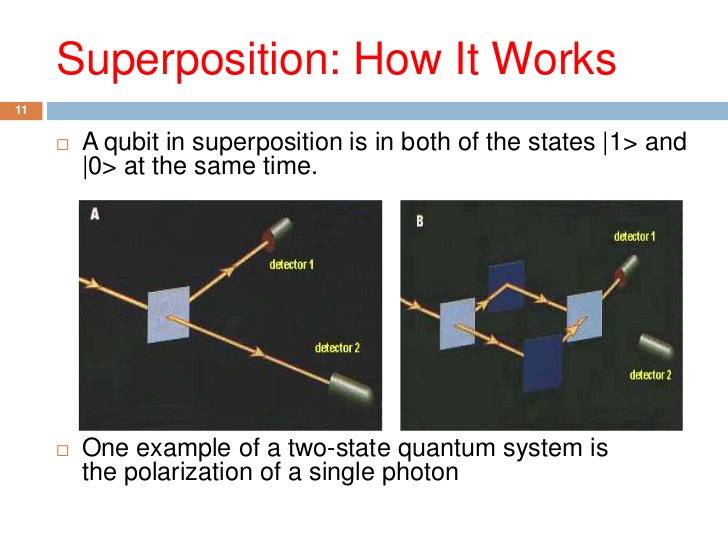
The fled of quantum computation is largely a body of theoretical promises for some impressively fast algorithms which could be executed on quantum computers. However, since the first significant algorithm was proposed in 1994 experimental progress has been rapid with several schemes yielding two and three quantum-bit manipulations.

Quantum computers were first discussed by Paul Benioff in the context of simulating classical Turing machines (very elementary conventional computers) with quantum unitary evolution. Feynman considered the converse question of how well classical computers can simulate quantum systems. He concluded that classical computers invariably super from an exponential slow-down in trying to simulate quantum systems, but that quantum systems could, in principle, simulate each other without this slowdown. It was Deutsch, however, who first suggested that quantum superposition might allow quantum evolution to perform many classical computations in parallel.

**III. QUANTUM MECHANICS**

The Quantum mechanics is generally about the novel behavior of very small things. At this scale matter become squantaised, this means that it can’t be subdivided no more. Quantum mechanics has never been wrong, it explains why the stars shine, how matter is structured, the periodic table, and countless other phenomena. The following are main parts of quantum mechanics that are important for quantum computing:

* Superposition and interference
* Uncertainty
* Entanglement
* Linear algebra
* Dirac notation
* Representing information

**3.1 SUPERPOSITION:**

**Fig 3.1**: Superposition

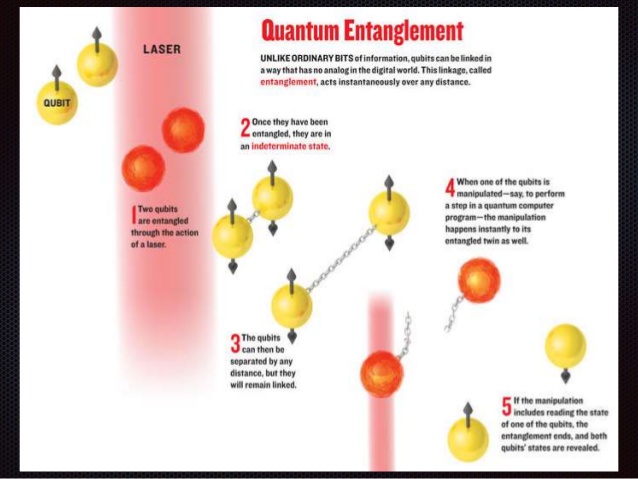
Superposition means a system can be in two or more of its states simultaneously. For example a single particle can be traveling along two different paths at once. This implies that the particle has wave-like properties, which can mean that the waves from the different paths can interfere with each other. Interference can cause the particle to act in ways that are impossible to explain without these wave-like properties. The ability for the particle to be in a superposition is where we get the parallel nature of quantum computing.

If each of the states corresponds to a different value then, if we have a superposition of such states and act on the system, we effectively act on all the states simultaneously

**3.2 UNCERTAINTY:**

The quantum world is irreducibly small so it’s impossible to measure a quantum system without having an effect on that system as our measurement device is also quantum mechanical. As a result there is no way of accurately predicting all of the properties of a particle. There is a trade off - the properties occur in complementary pairs (like position and momentum, or vertical spin and horizontal spin) and if we know one property with a high degree of certainty then we must know almost nothing about the other property. That unknown property’s behavior is essentially random. An example of this is a particle’s position and velocity: if we know exactly where it is then we know nothing about how fast it is going. This indeterminacy is exploited in quantum cryptography. It has been postulated (and currently accepted) that particles in fact DO NOT have defined values for unknown properties until they are measured. This is like saying that something does not exist until it is look.

**3.3 ENTANGLEMENT:**

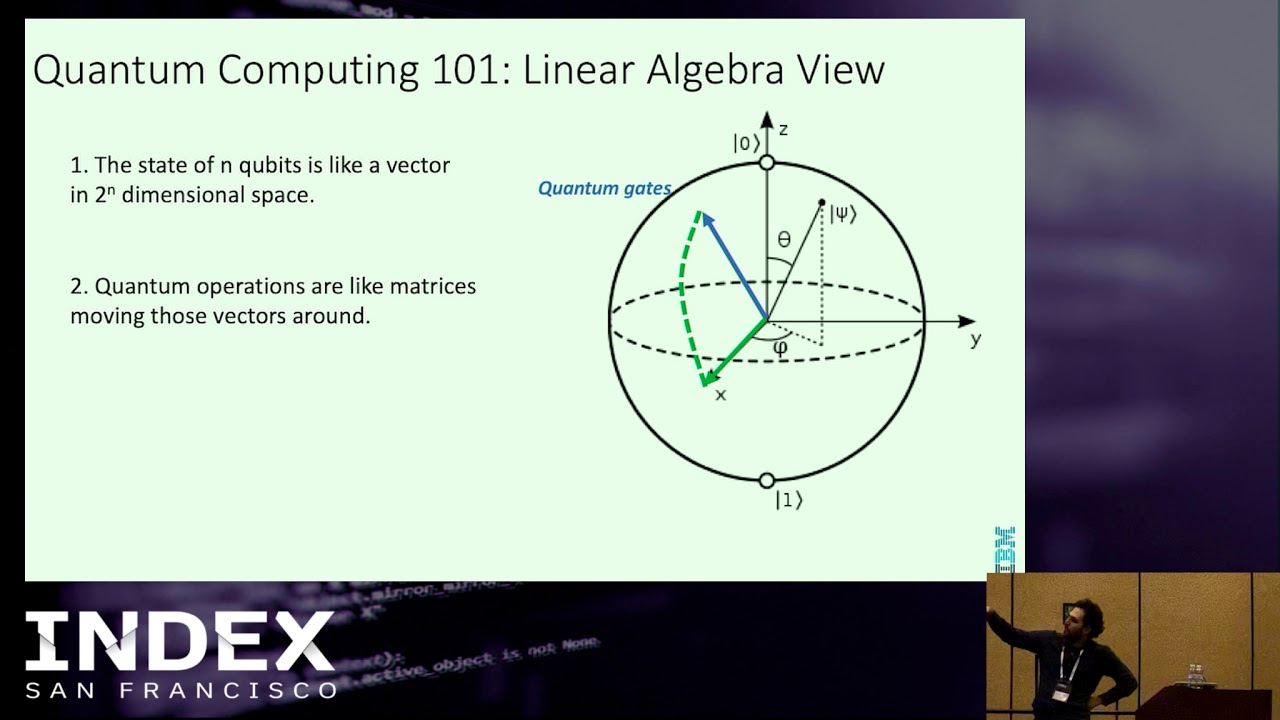
In 1935 Einstein (along with colleagues Podolski and Rosen) demonstrated a paradox (named *EPR* after them) in an attempt to refute the undefined nature of quantum systems. The results of their experiment seemed to show that quantum systems were defined, having *local state* BEFORE measurement. Although the original hypothesis was later proven wrong (i.e. it was proven that quantum systems do not have local state before measurement). The effect the demonstrated was still important, and later became known as entanglement. Entanglement is the .

**Fig 3.3:** Entanglement

ability for pairs of particles to interactover any distance instantaneously. Particles don’t exactly communicate, but there is a statistical correlationbetween results of measurements on each particle that is hard to understand using classical physics.

To become entangled, two particles are allowed to interact; they then separate and, on measuring say, the velocity of one of them (regardless of the distance between them), we can be sure of the value of velocity of the other one (before it is measured). The reason we say that they communicate instantaneously is because they store no local state and only have well defined state once they are measured. Because of this limitation particles can’t be used to transmit classical messages faster than the speed of light as we only know the states upon measurement. Entanglement has applications in a wide variety of quantum algorithms and machinery.

**3.4 LINEAR ALGEBRA:**

Quantum mechanics leans heavily on linear algebra. Some of the concepts of quantum mechanics come from the mathematical formalism, not thought experiments, that’s what can give rise to counter intuitive conclusions.

**Fig 3.4**: Linear Algebra

**3.5 DIRAC NOTATION:**

Dirac notation is used for quantum computing. We can represent the states of a quantum system as kets. For example, an electron’s spin can be represented as *|*0> spin up and *|*1>as spin down. The electron can be thought of as a little magnet, the effect of a charged particle spinning on its axis. When we pass a horizontally traveling electron through an inhomogeneous magnetic field, in say, the vertical direction, the electron either goes up or down. If we then repeat this with the up electron it goes up, with the down electron it goes down. We say the up electron after the first measurement is in the state |0*>*and the down electron is in state *|*1>. But, if we take the up electron and pass it through a horizontal field it comes out on one side 50% of the time and on the other side 50% of the time. If we represent these two states as | + > and | - > we can say that the up spin electron was in a superposition of the two states |+> and | - > : such that, when we make a measurement with the field horizontal we project the electron into one or the other of the two states, with equal probabilities ½.

**3.6 REPRESENTATION INFORMATION:**

Quantum mechanical information can be physically realized in many ways. To have something analogous to a classical bit we need a quantum mechanical System with two states only, when measured. Methods for representing binary information in a way that is capable of exhibiting quantum effects (e.g. entanglement and superposition) are: electron spin, photon direction, polarization of photons and nuclear spins.

**IV. ELEMENTS OF QUANTUM COMPUTING**

The basic element of quantum computing includes the qubits, the quantum gates, quantum circuits and quantum algorithms*.*

**4.1THE QUBIT:**

The qubit is the quantum analogue of the bit, the classical fundamental unit of information. It is a mathematical object with specific properties that can be realized physically in many different ways as an actual physical system. Just as the classical bit has a state (either 0 or 1), a qubit also has a state. Yet contrary to the classical bit, 0 and 1 are but two possible states of the qubit, and any linear combination (superposition) thereof is also physically possible. In general, thus, the physical state of a qubit is the superposition

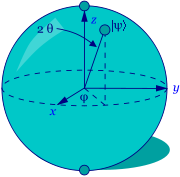
ψ = α0 + β1

(Where α and β are complex numbers). The state of a qubit can be described as a vector in a two-dimensional Hilbert space, a complex vector space. The special states 0 and 1 are known as the computational basis states, and form an orthonormal basis for this vector space. According to quantum theory, when we try to measure the qubit in this basis in order to determine its state, we get either 0 with probability α² or 1 with probability β². Since α² + β² = 1 (i.e., the qubit is a unitvector in the aforementioned two-dimensional Hilbert state), we may (ignoring the overall phase factor) effectively write its state as ψ = cos(θ)0 + eiφsin(θ)1, where the numbers θ and φ define a point on the unit three-dimensional sphere, as shown here. This sphere is often called the Bloch sphere, and it provides a useful means to visualize the state of a single qubit.

Theoretically, a single qubit can store an infinite amount of information, yet when measured it yields only the classical result (0 or 1) with certain probabilities that are specified by the quantum state. In other words, the measurement changesthe state of the qubit, “collapsing” it from the superposition to one of its terms.

The crucial point is that unless the qubit is measured, the amount of “hidden” information it stores is conserved under the dynamic evolution (namely, Schrödinger's equation). This feature of quantum mechanics allows one to manipulate the information stored in unmeasured qubit with quantum gates, and is one of the sources for the putative power of quantum computer.

**4.2 BLOCH SPHERE:**



**Fig 4.2:** The Bloch Sphere

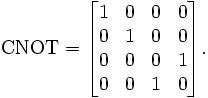
To see why, let us suppose we have two qubits with us. If these were classical bits, then they could be in four possible states (00, 01, 10, and 11). Correspondingly, a pair of qubits has four computational basis states (00, 01, 10 and 11). But while a single classical two-bit register can store these numbers only one at a time, a pair of qubits can also exist in a superposition of these four basis states, each of which

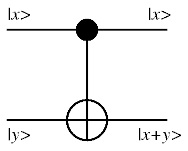
With its own complex coefficient (whose mod square, being interpreted as probability, is normalized). As long as the quantum system evolves unitarily and is unmeasured, all four possible states are simultaneously “stored” in a single two-qubit quantum register. More generally, the amount of information that can be stored in a system of n unmeasured qubits grows exponentially in n. The difficult task, however, is to retrieve this information efficiently.

**4.3 QUANTUM GATES:**

Classical computational gates are Boolean logic gates that perform manipulations of the information stored in the bits. In quantum computing these gates are represented by matrices, and can be visualized as rotations of the quantum state on the Bloch sphere. This visualization represents the fact that quantum gates are unitary operators, i.e., they preserve the norm of the quantum state (if U is a matrix describing a single qubit gate, then U†U=I, where U† is the ad joint of U, obtained by transposing and then complex-conjugation.

As in the case of classical computing, where there exists a universal gate (the combinations of which can be used to compute any computable function), namely, the NAND gate which results from performing an AND gate and then a NOT gate, in quantum computing it was shown that any multiple qubit logic gate may be composed from a quantum CNOT gate (which operates on a multiple qubit by flipping or preserving the target bit given the state of the control bit, an operation analogous to the classical XOR, i.e., the exclusive OR gate) and single qubit gates. One feature of quantum gates that distinguishes it from classical gates is that they are reversible: the inverse of a unitary matrix is also a unitary matrix, and thus a quantum gate can always be inverted by another quantum gate.





**Fig 4.3:** The CNOT Gate

Unitary gates manipulate the information stored in the quantum register, and in this sense ordinary (unitary) quantum evolution can be regarded as computation (showed how a small set of single-quits gates and a two-qubit gate is universal, in the sense that a circuit combined from this set can approximate to arbitrary accuracy any unitary transformation of n qubits). In order to read the result of this computation, however, the quantum register must be measured.

The measurement gate is a non-unitary gate that “collapses” the quantum superposition in the register onto one of its terms with the corresponding probability. Usually this measurement is done in the computational basis, but since quantum mechanics allows one to express an arbitrary state as a linear combination of basis states, provided that the states are orthonormal (a condition that ensures normalization) one can in principle measure the register in any arbitrary orthonormal basis. This, however, doesn't mean that measurements in different bases are efficiently equivalent. Indeed, one of the difficulties in constructing efficient quantum algorithms stems exactly from the fact that measurement collapses the state, and some measurements are much more complicated than others.

**4.4 QUANTUM CIRCUITS:**

Quantum circuits are similar to classical computer circuits in that they consist of wires and logical gates. The wires are used to carry the information, while the gates manipulate it (note that the wires do not correspond to physical wires; they may correspond to a physical particle, a photon, moving from one location to another in space, or even to time-evolution). Conventionally, the input of the quantum circuit is assumed to be a computational basis state, usually the state consisting of all 0. The output state of the circuit is then measured in the computational basis, or in any other arbitrary orthonormal basis. The first quantum algorithms were constructed in this paradigm [2, 3, and 20]. Additional paradigms for quantum computing exist today that differ from the quantum circuit model in many interesting ways. So far, however, they all have been demonstrated to be computationally equivalent to the circuit model (see below), in the sense that any computational problem that can be solved by the circuit model can be solved by these new models with only a polynomial overhead in computational resources

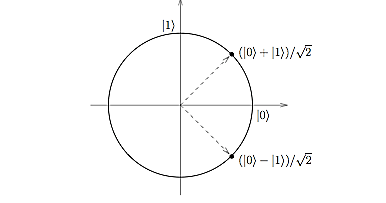
**V.IMPORTANT PROPERTIES OF QUANTUM CIRCUITS**

Quantum circuit diagrams have the following constraints which make them different from classical diagrams. They are acyclic (no loops). No FANIN, as FANIN implies that the circuit is NOT reversible, and therefore not unitary. No FANOUT, as we can’t copy a qubits state during the computational phase because of the no-cloning theorem.

**5.1 QUANTUM ALGORITMS:**

Algorithm design is a highly complicated task, and in quantum computing it becomes even more complicated due to the attempts to harness quantum mechanical features to reduce the complexity of computational problems and to “speed-up” computation. Before attacking this problem, we should first convince ourselves that quantum computers can be harnessed to perform standard, classical, computation without any “speed-up”. In some sense this is obvious, given the belief in the universal character of quantum mechanics, and the observation that any quantum computation that is diagonal in the computational basis, i.e., involves no interference between the qubits, is effectively classical. Yet the demonstration that quantum circuits can be used to simulate classical circuits is not straightforward (recall that the former are reversible while the latter use gates which are inherently irreversible). Indeed, quantum circuits cannot be used directly to simulate classical computation, but the latter can still be simulated on a quantum computer using an intermediate gate, namely the Toffoli *g*ate.

This gate has three input bits and three output bits, two of which are control bits, unaffected by the action of the gate. The third bit is a target bit that is flipped if both control bits are set to 1, and otherwise is left alone. This gate is reversible (its inverse is itself), and can be used to simulate all the elements of the classical irreversible circuit with a reversible one. Consequently, using the quantum version of the Toffoli gate one can simulate, although rather tediously, irreversible classical logic gates with quantum reversible ones. Quantum computers are thus capable of performing any computation which a classical deterministic computer can do What about non-deterministic computation? Not surprisingly, a quantum computer can simulate also this type of computation by using another famous quantum gate, namely the Hadamard gate, which receives as an input the state 0 and produces the state (0 + 1)/√2. Measuring this output state yields 0 or 1 with 50/50 probability, which can be used to simulate a fair coin toss.





**Fig 5.1:** The Hadamard Gate

**5.2 QUANTUM COMPUTERS:**

A quantum computer looks like this, taking *n* input qubits, the register *V*, and producing *n* output qubits, the register *W*:

**Fig 5.2**: Quantum computers

The input register can be prepared as a superposition of states, e.g. an equal superposition of *all* integers from 0 to 2*n*:



The computer then calculates in parallel the function applied to all 2*n* integers simultaneously. From QMP (Quantum Measurement Postulate)*,* when we measure W, it will choose a Boolean for each bit of the output register according to the resulting entangled wave function of the output qubits. Design *F* so that it maximizes the probability that the output we measure is the answer we want. Measuring the output collapses the wave function: get Boolean values for all the qubits in *W*. The result is one of the possible outputs.

Imagine that *F* is (integer) square root *W* =√*V.* Prepare *V* as the superposition of all integers from 0 to 2*n*, run the computer, then measure *W*. Result will square root of *some* number between 0 and 2*n*. The square root of any such number, with equal probability. *F* calculates the square roots of all the integers in parallel, but QMP says we can only find out about one. For real problems, arrange *F* so the probability amplitudes of the output state strongly favor the desired output from *F*. A quantum computer is *probabilistic*: we may need to run it multiple times before we get the answer we want.

**5.3 WHAT QUANTUM COMPUTERS DO?**

The biggest success so far -- and the event which ignited the current explosive growth of the field of quantum computing -- was Peter Shor's 1994 discovery of an efficient quantum algorithm for finding the prime factors (factoring) of large integers.

By making clever use of superposition’s, interference, quantum parallelism, and some classical number theory, Shor's algorithm finds a factor of a number N in time roughly the square of the length of the input (which is log N bits). In contrast, every known classical algorithm requires exponential time to factor. Since factoring is one of the most elementary aspects of number theory, the oldest mathematical discipline, and centuries of efforts by the greatest mathematicians have not yielded better methods, it is widely believed that such better methods either do not exist or are prohibitively difficult to find.

In fact, this belief underlies most of current public-key cryptography, notably the RSA system, ubiquitously used on the Internet and in the financial world. Such crypto-systems can be broken if one can factor large numbers fast. Accordingly, the advent of quantum computing compromises all such systems: if a quantum computer can be built, then most of current cryptography becomes totally insecure, and, for example, electronic money can be forged.

What quantum computing takes away with one hand (classical public-key crypto), it gives back in another form with the other (quantum secret-key crypto).In 1984, Bennett and Brassard found a scheme which allowed two distant parties to obtain a shared secret key via quantum mechanical communication. Their scheme was always believed to be fully secure against any type of spy or eavesdropper, and recently this has indeed been formally proven. On the other hand, some other parts of electronic transactions, like unforgivable signatures, appear to be beyond the power of quantum methods.

A third application is Grover's 1996 algorithm for searching databases. Consider finding some specific record in a large unordered database of N items. Classically, there is no smarter method than just to go through all records sequentially, which will requires expected N / 2 time steps for a record in general position. Grover's algorithm, however, uses quantum superposition’s to examine all records ``at the same time'', and finds the desired record in roughly √N steps.

Examining a 1012 records with unit microsecond probes, this is the difference between about two months of computing and one second of computing! His algorithm also allows to solve the widespread and notoriously hard NP-complete problems (such as the traveling salesman problem) quadratic ally faster than known classical methods--reducing say exponential time with exponent N to exponential time with exponent N / 2.

A fourth application was initially conceived and primarily developed in collaboration with the CWI (Centrum voor Wiskunde en Informatics, University of Amsterdam) group. It deals with the setting where two separated parties, Alice and Bob, want to compute some function f(x,y) depending on x (only known to Alice) and y (only known to Bob).

A simple scheme would be for Alice to send her x to Bob and then let Bob do all the work by himself, but this may take a lot of bits of communication and often there are much more clever schemes requiring less communication. The field of communication complexityexamines the optimal number of bits that have to be communicated in order to compute the function at hand. What happens if we generalize this setting to the quantum world and allow Alice and Bob the use of quantum computers and qubit-communication?

It turns out that some tasks can be solved with significantly less communication if we allow such quantization. We have obtained similar advantages by sticking to classical communication, but allowing Alice and Bob the use of pre-established ``entangled'' qubits. Both approaches beat the limits provable for just classical communication.

The above developments suggested the vision that *all* computation can be enormously speeded up by quantum computers. But not so! CWI's researchers obtained strong and general limitationsof quantum computers as well. Grover's algorithm is quadratically faster than classical search algorithms. It was already known that such a quadratic speed-up is the best quantum computers can achieve for searching a database, so exponential speed-ups cannot be obtained for this problem.

CWI-researchers recently showed that the same holds for *all* problems in the database-setting of Grover's algorithm: for all such problems, quantum computers can be at most polynomially faster than classical computers.

Limiting results like the above, of course, do not preclude exponential speed-ups in different settings, like Shor's, or a clever future setting as yet unknown. Exploring this potential of quantum computation remains an exciting and important task for computer scientists and physicists alike.

.

**5.4 HOW QUANTUM COMPUTERS DO IT?**

The above results are very promising, but so far mostly theory. How about actually building quantum computers which can run the fast algorithms like Shor's, Grover's, or CWI's? To date only very small quantum algorithms (and slightly bigger quantum crypto devices) have been implemented, but the physical realization of quantum computers is still in its infancy.

The main problem is that quantum superpositions are extremely vulnerable and any interactions with its environment will quickly cause errors, which degrade the performance of the computer. Quantum versions of error-correcting codes have been developed recently which to a large extent solve this problem in theory, but not yet in the brittle practice of the physical lab (let alone the brittle practice of our desktops).

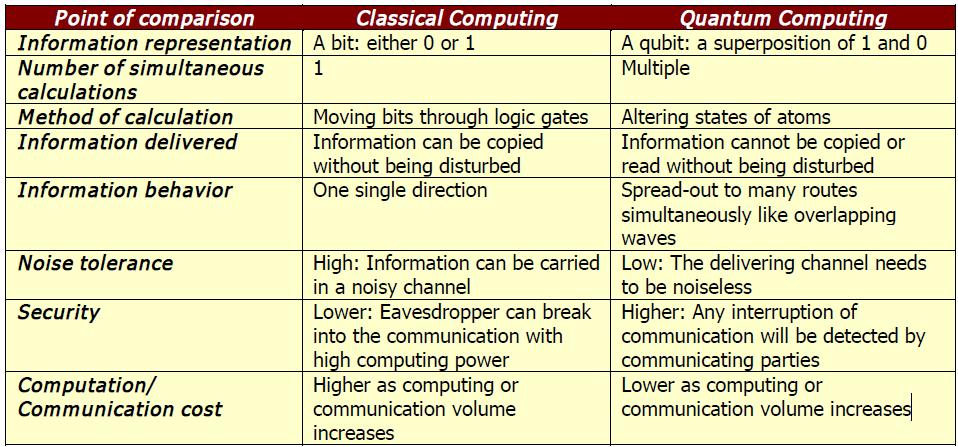
This is related to development of Quantum Information Theory--the quantum extension of classical information theory. CWI's group has contributed to this research, and to related notions of the information in individual quantum states: Quantum Kolmogorov Complexity.

Building large quantum computers presents formidable problems to experimental physicists reminiscent of the initial barriers to classical computing: unreliable components, physically large components, memory, organization, communication, and programming. The theory of quantum mechanics is currently extended, partially by CWI research, in particular with respect to the algebraic analysis of ``quantum entanglement''--a vital notion in many quantum algorithms, apparently not yet thoroughly investigated in quantum theory.

**5.5 COMPARISON OF CLASSICAL AND QUANTUM COMPUTER:**

Classical computing relies, at its ultimate level, on principles expressed by Boolean algebra, operating with a (usually) 7-mode logic gate principle, though it is possible to exist with only three modes (which are AND, NOT, and COPY). 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 at the heart of computers can only be in one state at any point. While the time that the each transistor or capacitor need be either in 0 or 1 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. As we progress to smaller and faster circuits, we begin to reach the physical limits of materials and the threshold for classical laws of physics to apply.

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 (in practice, success has also been achieved with ions), 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.



**Table 5.5:** Summary of Comparison between classical and quantum Computing

**5.6 THE MAJOR DIFFERENCE BETWEEN QUANTUM AND CLASSICAL COMPUTERS:**

The memory of a classical computer is a string of 0s and 1s, and it can perform calculations on only one set of numbers simultaneously. The memory of a quantum computer is a quantum state that can be a superposition of different numbers. A quantum computer can do an arbitrary reversible classical computation on all the numbers simultaneously. Performing a computation on many different numbers at the same time and then interfering all the results to get a single answer, makes a quantum computer much powerful than a classical one. (West, 2000).

**5.6.1 THE POTENTIAL AND POWER OF QUANTUM COMPUTING:**

Quantum computer with 500 qubits gives 2500 superposition states. Each state would be classically equivalent to a single list of 500 1's and 0's. Such computer could operate on 2500 states simultaneously. Eventually, observing the system would cause it to collapse into a single quantum state corresponding to a single answer, a single list of 500 1's and 0's, as dictated by the measurement axiom of quantum mechanics. This kind of computer is equivalent to a classical computer with approximately 10150 processors. (West, 2000, p. 3).

**5.7 MOORE’S LAW OF QUANTUM COMPUTERS:**

According to Moore's Law, the number of transistors of a microprocessor continues to double in every 18 months. According to such evolution if there is a classical computer in year 2020, it will run at 40 GHz CPU speed with 160 GB RAM. If we use an analogue of Moor’s law for quantum computers, the number of quantum bits would be double in every 18 months. But adding just one qubit is already enough to double a speed. So, the speed of quantum computer will increase more than just doubling it. (Quantum Computers & Moore's Law, §1).

**VI**. **PROJECTED BENEFITS OF QUANTUM COMPUTING**

Quantum computing offers many potential benefits to the organizations of tomorrow. This new conceptualization of computing power will result in three main benefits: increases in computing power, advances in security, and the ability for firms to use the sci-fi concept of teleportation. Each of these opportunities can overcome the limitations of the current computational paradigm.

**6.1 QUANTUM COMUTATION: INCREAING COMPUTING POWER:**

Utilizing quantum parallelism, a quantum computer can calculate or factor any huge number that is currently infeasible to be analyzed on a classical computer. For example, factoring a number with 400 digits will take the existing fastest supercomputers billions of years to accomplish. A quantum computer can obtain the answer within a year. Therefore, quantum computers well serve the purpose of searching information in unsorted databases or performing difficult mathematical calculations that are impossible using semiconductor computers.

**6.2 QUANTUM CRPTOLOGY: ADVANCES IN SECURITY:**

Linked with the first benefit (the increase in computing power) then comes the possibility for advancements in computing security. Quantum cryptography allows two parties to exchange public keys in a private channel and thus secure privacy in quantum communication. The technical aspect of quantum cryptography requires tremendous amount of physics knowledge; the basic idea is that quantum mechanics will not allow any eavesdropper to obtain the private key. Two legitimate parties will reveal a random subset of the key bits and check the error rate to test for eavesdropping. In so doing, even though eavesdropping will not be prevented, any attempt, regardless how subtle and complicated, to break into the communication channel will be detected.

**6.3 TELEPORTATION:**

Perhaps the most astounding of the claimed for benefits of quantum computing is teleportation, the favoured local transportation mechanism in Star Trek episodes. Teleportation is the capability to make an object or a person disintegrates in one place while a perfect replica appears in another. In physics, teleportation has never been taken seriously because of the uncertainty principle. According to the uncertainty principle, the duplicating process will disturb or destroy the original objects; the more an object is duplicated, the more it is destroyed. The detail information regarding how the duplication is made and how the original object is destroyed is unknown. Therefore, it will reach a point where one cannot extract enough information from the original to make a perfect replica.

**6.4 ARTIFICIAL INTELLIGENCE:**

It has been mentioned that quantum computers will be much faster and consequently will perform a large amount of operations in a very short period of time. On the other side, increasing the speed of operation will help computers to learn faster even using the one of the simplest methods - mistake bound model for learning.

**6.5 OTHER BENEFITS:**

High performance will allow us in development of complex compression algorithms, voice and image recognition, molecular simulations, true randomness and quantum communication. Randomness is important in simulations. Molecular simulations are important for developing simulation applications for chemistry and biology.

With the help of quantum communication both receiver and sender are alerted when an eavesdropper tries to catch the signal. Quantum bits also allow more information to be communicated per bit. Quantum computers make communication more secure.

**VII. STRANGE THINGS ABOUT QUANTUM COMPUTERS**

“On the theory side, quantum mechanics delves deep into areas that are nearly unthinkable. For instance, it's possible that a quantum computer holds an infinite number of right answers for an infinite number of parallel universes. It just happens to give you the right answer for the universe you happen to be in at the time. "It takes a great deal of courage to accept these things," says Charles Bennett of IBM, one of the best known quantum computing scientists. "If you do, you have to believe in a lot of other strange things."

**7.1 DANCING CHLOROFORM ATOMS:**

A few years ago, Gershenfeld and Chuang made the first quantum computer. It was based on nuclear magnetic resonance technology. The program was performing a simple search using Grover’s algorithm. In comparison to classical computers it took one item out of four in just one step, instead of making two or three steps as classical computes. The price for making the first 2-qubit computer was approximately $1 million.

**7.2 ENTANGLEMENT OF QUANTUM SYSTEMS:**

According to quantum mechanics an outside force acting on two particles of the quantum system can cause them to become entangled. The quantum state of this system can contain all positions of spins (internal magnetic moments) of each particle. The total spin of the system can only be equal to certain discrete values with different probabilities. Measurements of total spin of certain quantum systems showed that positions of spins of some particle are not independent from others. For such systems, when an orientation of a spin of one particle changed by some reason, an orientation of a spin of another particle changes automatically and instantly. The laws that that have been developed so far about the speed of light are disobeyed in this case, because the change in an orientation of a spin happens immediately. At least there is hypothesize to use this phenomena for quantum computing.

It is well known that a speed of communication is limited by a speed of light as nothing can travel faster than the speed of light. The question is how particles of the quantum system communicate when they change their spin orientation and consequently their vector states. Famous scientists spent a lot of time discussing this issue. Einstein’s idea that some unknown “hidden parameters” of quantum system were contributing to this effect has been rejected theoretically and experimentally.

This is one of the example showing the difference between classical and quantum realities.

This effect of the quantum system explains a lot of aspects of the nature (f.e. chemical characteristics of atoms and molecules) and is proved by the experiments.

“In fact, theories about entanglement have led scientists to believe there could be a way to speed up computing. Even today's computers are nearing a point at which their speed is being limited by how fast an electron can move through a wire - the speed of light. Whether in a quantum or traditional computer, entanglement could blow past that limit.”

**7.3 WHEN WILL BE QUANTUM COMPUTERS BE AVAILABLE?**

It has been more than three decades since IBM Fellow, Rolf Landauer, first put forward the theory of quantum information. A decade later, David Deutsch and other research fellows proposed the concept of a quantum computer. Since then progress in the technical development of quantum computing has moved slowly.

Currently, IBM has a three-bit quantum computer while Alamos National Laboratory announced a seven-bit NMR (Nuclear Magnetic Resonance) computer not long ago. Even though IBM research fellows promise that a ten-bit computer will emerge soon, a useful quantum computer will require at least hundreds and perhaps thousands of qubits. Unfortunately, it appears almost impossible to develop more than 10 qubits. This is because room temperature and other conditions will be changed exponentially as the qubits are added resulting in disturbing the atom’s quantum behavior. As IBM Research Fellow Isaac Chuang, a leading scientist in quantum computing research, said “Quantum mechanics goes away when you look at it. So you have to make sure that the computer is extremely well isolated from the rest of the world.” In other words, the commercial development of quantum computing is still limited. The real life use of quantum computers therefore will not affect our everyday life in the near future. However, Chuang is very optimistic about it: “Quantum computing begins where Moore’s law ends—about the year 2020, when circuit features are predicted to be the size of atoms and molecules”. Other scientists estimate the birth of commercial quantum computers will be in at least another three decades.

**VIII. CONCLUSION**

It is important that making a practical quantum computing is still far in the future. Programming style for a quantum computer will also be quite different. Development of quantum computer needs a lot of money. Even the best scientist can’t answer a lot of questions about quantum physics. Quantum computer is based on theoretical physics and some experiments are already made. Building a practical quantum computer is just a matter of time. Quantum computers easily solve applications that can’t be done with help of today’s computers. This will be one of the biggest steps in science and will undoubtedly revolutionize the practical computing world.

**BIBLIOGRAPHY**

**WEBSITES:**

1. [http://www.qubit.org](http://www.qubit.org/)

2. <https://en.wikipedia.org/wiki/Quantum_computing>

3. [www.studymafia.org](http://www.studymafia.org/)