Seminar Report

On

QUANTUM COMPUTER

Submitted By

OMKAR VILAS BHOITE (11)

Guided By

Ms. N S Nagdeo

Third Year Instrumentation Engineering

SAVITRIBAI PHULE PUNE UNIVERSITY

ALL INDIA SHRI SHIVAJI MEMORIAL SOCIETY'S

INSTITUTE OF INFORMATION TECHNOLOGY, PUNE

ACADEMIC YEAR 2017-2018

ACKNOWLEDGEMENT

Inspiration and guidance are invaluable in every aspect of the life, especially in the field of the academics, which I have received from my respected seminar guide **Ms. N S Nagdeo** and my respected H.O.D **Mr. H. P. Chaudhari**. I would like to thank as he was responsible for the complete project and also for his endless contributions of time, efforts, valuable guidance and encouragement he has given to me. I would also like to thank principal. **Dr. P.B. Mane** without whom we would not have opportunity to reach up to this level. I would also thank my colleagues and friends for their inspiration and motivation and those who helped me directly or in directly for my project work.

ABSTRACT

Quantum computers is computation systems that make direct use of quantum-mechanical phenomena, such as superposition and entanglement, to perform operations on data. Quantum computers are different from binary digital electronic computers based on transistors. Quantum computation poses challenging engineering and basic physics issues for the control of nanoscale systems. Quantum computers have acutely illustrated how quantum circuits require extremely precise control instrumentation for pulsed excitation.

This seminar provides a brief description of the quantum computer and how it differs from the normal binary digital computers made up of transistor. It also includes overview of the cooling system requires for the quantum computer and real-life application of the quantum computer.

.

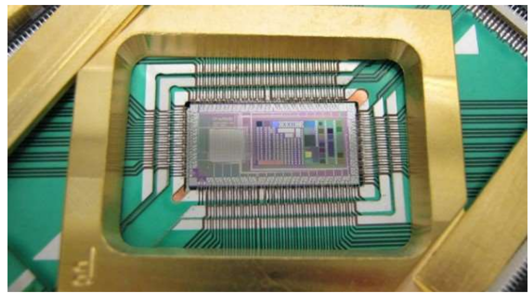
INDEX

Introduction

Quantum computing studies computation systems (**quantum computers**) that make direct use of quantum-mechanical phenomena, such as superposition and entanglement, to perform operations on data. Quantum computers are different from binary digital electronic computers based on transistors. Whereas common digital computing requires that the data be encoded into binary digits (bits), each of which is always in one of two definite states (0 or 1), quantum computation uses quantum bits, which can be in superpositions of states. A quantum Turing machine is a theoretical model of such a computer, and is also known as the universal quantum computer. The field of quantum computing was initiated by the work of Paul Benioff and Yuri Manin in 1980,] Richard Feynman in 1982, and David Deutsch in 1985. A quantum computer with spins as quantum bits was also formulated for use as a quantum spacetime in 1968.

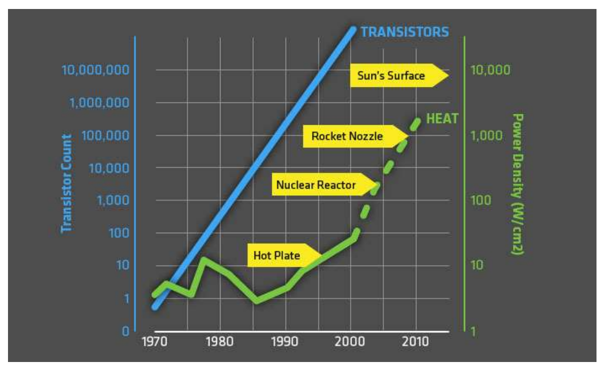
As of 2017, the development of actual quantum computers is still in its infancy, but experiments have been carried out in which quantum computational operations were executed on a very small number of quantum bits. Both practical and theoretical research continues, and many national governments and military agencies are funding quantum computing research in additional effort to develop quantum computers for civilian, business, trade, environmental and national security purposes, such as cryptanalysis. A small 5-qubit quantum computer exists and is available for hobbyists to experiment with via the IBM quantum experience project.

Large-scale quantum computers would theoretically be able to solve certain problems much more quickly than any classical computers that use even the best currently known algorithms, like integer factorization using Shor's algorithm or the simulation of quantum many-body systems. There exist quantum algorithms, such as Simon's algorithm, that run faster than any possible probabilistic classical algorithm. A classical computer could in principle (with exponential resources) simulate a quantum algorithm, as quantum computation does not violate the Church–Turing thesis. On the other hand, quantum computers may be able to efficiently solve problems which are not practically feasible on classical computers.



Moore's Law:

- **Moore's Law** states, the number of transistors on a microprocessor continues to double every 18 months.



Classical computer:

- Classical computers encode information in bits. Each bit can take the value of 1 or 0. These 1s and 0s act as on/off switches that ultimately drive computer functions. Quantum computers, on the other hand, are based on qubits, which operate according to two key principles of quantum physics: superposition and entanglement.

Superposition & Entanglement:

Superposition means that each qubit can represent both a 1 and a 0 at the same time. Entanglement means that qubits in a superposition can be correlated with each other that is, the state of one (whether it is a 1 or a 0) can depend on the state of another. Qubits act as more sophisticated switches, enabling quantum computers to function in ways that allow them to solve difficult problems that are intractable using today's computers.

Difference between Classical and Quantum Computers.

Basic Properties of elements /material used in fabrication of Quantum Computer.

Gold Basic Properties

Property	Value	Property	Value
Atomic Number	79	Melting Point	1064 deg C
Atomic Group	Transition Elements	Boiling Temp	2808 deg C
Atomic Weight	196.97	Specific Gravity	19.3

Silver Basic Properties

Property	Value	Property	Value
Atomic Number	47	Melting Point	962 deg C
Atomic Group	Transition Elements	Boiling Temp	2212 deg C
Atomic Weight	107.868	Specific Gravity	10.5

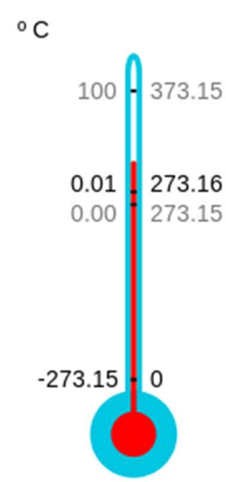
Absolute Zero Temperature

Absolute zero is the lower limit of the thermodynamic temperature scale, a state at which the enthalpy and entropy of a cooled ideal gas reaches its minimum value, taken as 0. The theoretical temperature is determined by extrapolating the ideal gas law; by international agreement, absolute zero is taken as −273.15° on the Celsius scale and −459.67° on the Fahrenheit scale.

It is commonly thought of as the lowest temperature possible, but it is not the lowest *enthalpy* state possible, because all real substances begin to depart from the ideal gas when cooled as they approach the change of state to liquid, and then to solid; and the sum of the enthalpy of vaporization (gas to liquid) and enthalpy of fusion (liquid to solid) exceeds the ideal gas's change in enthalpy to absolute zero. In the quantum-mechanical description, matter (solid) at absolute zero is in its ground state, the point of lowest internal energy.

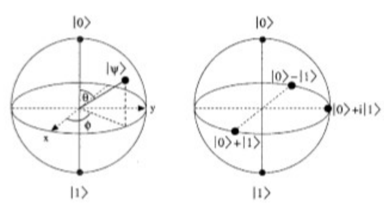
The laws of thermodynamics indicate that absolute zero cannot be reached using only thermodynamic means, because the temperature of the substance being cooled approaches the temperature of the cooling agent asymptotically, and a system at absolute zero still possesses quantum mechanical zero-point energy, the energy of its ground state at absolute zero. The kinetic energy of the ground state cannot be removed.

Scientists and technologists routinely achieve temperatures close to absolute zero, where matter exhibits quantum effects such as superconductivity and superfluidity.



Quantum bits

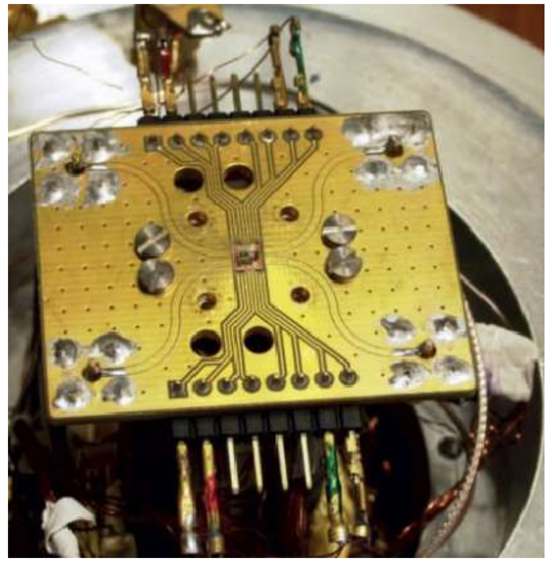
The indivisible unit of classical information is the bit, which takes on one of two possible values: logical 0, or logical 1. The corresponding unit of quantum information is known as the "quantum bit" or qubit. In contrast to classical bits, a qubit can exist in a superposition of states 0 or 1, otherwise denoted by the quantum states:10) and 11). The most general normalized state for a single qubit can be expressed mathematically as 14) = a lO) + b1l), (2.10) where a and b are complex numbers that satisfy Ia12 + b12 = 1. The overall phase of the qubit is physically irrelevant and cannot be revealed by any measurement. We can also write |0) as4') = cos () 10) + exp (iq) sin (0) 1). (2.11) The state of a qubit can be visualized as a vector in a sphere, called the Bloch sphere. In this representation, the qubit has two degrees of freedom, 6 and #. If the state of the qubit is along the i-axis, then 1') = 10) or 11). When the vector lies along the 2 - Q plane, the qubit is in a superposition of 10) and 11).

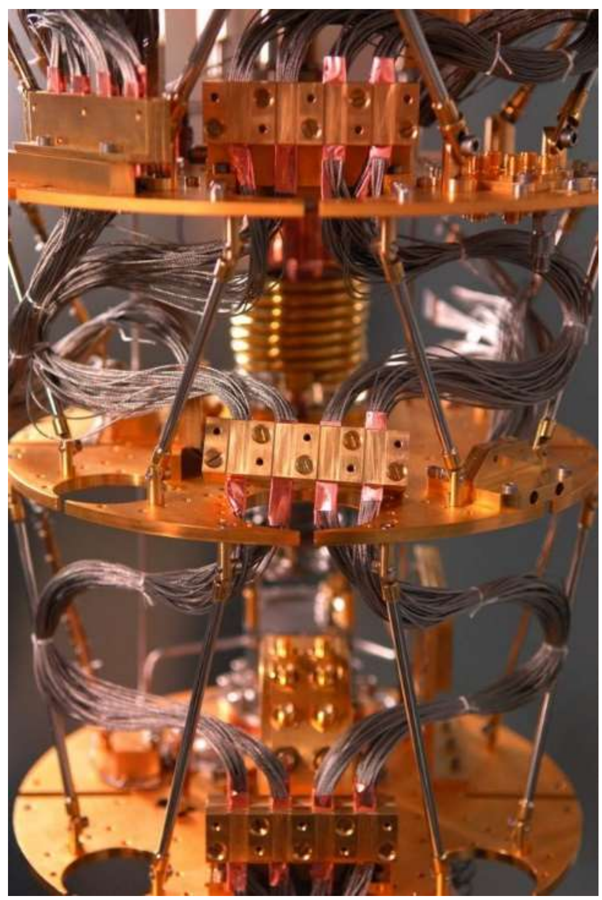


Bloch Sphere Representation.

Superconducting qubits

This is the granddaddy of all quantum computer tech. Back in 1962, Cambridge physicist Brian Josephson showed that putting a small gap into a strip of superconductor – a material that has zero resistance to the flow of electricity at low temperatures – has a surprising effect. For example, superconducting loops incorporating such a "Josephson junction" let current flow clockwise and anticlockwise simultaneously. That's a superposition of states – just what you need for a qubit.





Quantum Gate

In quantum computing and specifically the quantum circuit model of computation, a **quantum gate** (or **quantum logic gate**) is a basic quantum circuit operating on a small number of qubits. They are the building blocks of quantum circuits, like classical logic gates are for conventional digital circuits.

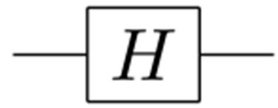
Unlike many classical logic gates, quantum logic gates are reversible. However, it is possible to perform classical computing using only reversible gates. For example, the reversible Toffoli gate can implement all Boolean functions, often at the cost of having to use ancillary bits. The Toffoli gate has a direct quantum equivalent, showing that quantum circuits can perform all operations performed by classical circuits.

Quantum logic gates are represented by unitary matrices. The most common quantum gates operate on spaces of one or two qubits, just like the common classical logic gates operate on one or two bits. As matrices, quantum gates can be described by sized unitary matrices, where is the number of qubits. The variables that the gates act upon, the quantum states, are vectors in complex dimensions, where again is the number of qubits of the variable: The base vectors are the possible outcomes if measured, and a quantum state is a linear combination of these outcomes.

E.g. Of Quantum Gates

Hadamard gate

The Hadamard gate acts on a single qubit. It maps the basis state means that a measurement will have equal probabilities to become 1 or 0 (i.e. creates a superposition)

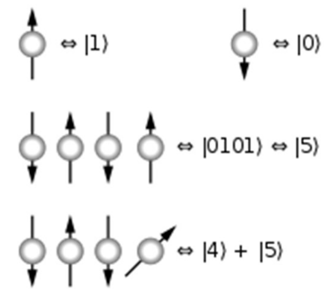


Pauli-Y gate

The Pauli-X gate acts on a single qubit. It is the quantum equivalent of the NOT gate for classical computers

Principle of operation of Quantum Computer

A quantum computer with a given number of qubits is fundamentally different from a classical computer composed of the same number of classical bits. For example, representing the state of an n-qubit system on a classical computer requires the storage of 2^n complex coefficients, while to characterize the state of a classical n-bit system it is sufficient to provide the values of the n bits, that is, only n numbers. Although this fact may seem to indicate that qubits can hold exponentially more information than their classical counterparts, care must be taken not to overlook the fact that the qubits are only in a probabilistic superposition of all of their states. This means that when the final state of the qubits is measured, they will only be found in one of the possible configurations they were in before the measurement. It is generally incorrect to think of a system of qubits as being in one particular state before the measurement, since the fact that they were in a superposition of states before the measurement was made directly affects the possible outcomes of the computation.



qubits can be in a superposition of all the clasically allowed states

Operation of Quantum computer

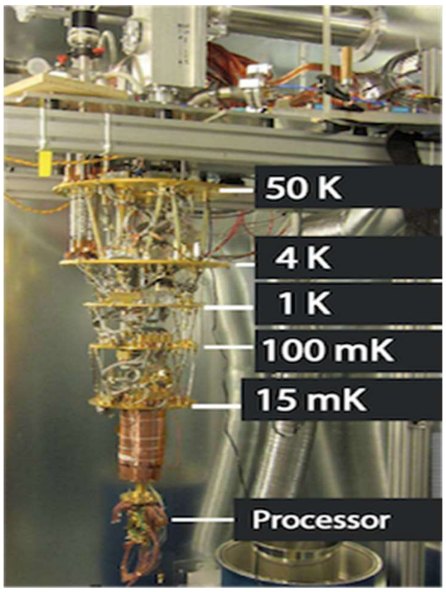
While a classical 3-bit state and a quantum 3-qubit state are each eight-dimensional vectors, they are manipulated quite differently for classical or quantum computation. For computing in either case, the system must be initialized, for example into the all-zeros string, , corresponding to the vector (1,0,0,0,0,0,0,0). In classical randomized computation, the system evolves according to the application of stochastic matrices, which preserve that the probabilities add up to one (i.e., preserve the L1 norm). In quantum computation, on the other hand, allowed operations are unitary matrices, which are effectively rotations (they preserve that the sum of the squares add up to one, the Euclidean or L2 norm). (Exactly what unitarizes can be applied depend on the physics of the quantum device.) Consequently, since rotations can be undone by rotating backward, quantum computations are reversible. (Technically, quantum operations can be probabilistic combinations of unitarizes, so quantum computation really does generalize classical computation. See quantum circuit for a more precise formulation.)

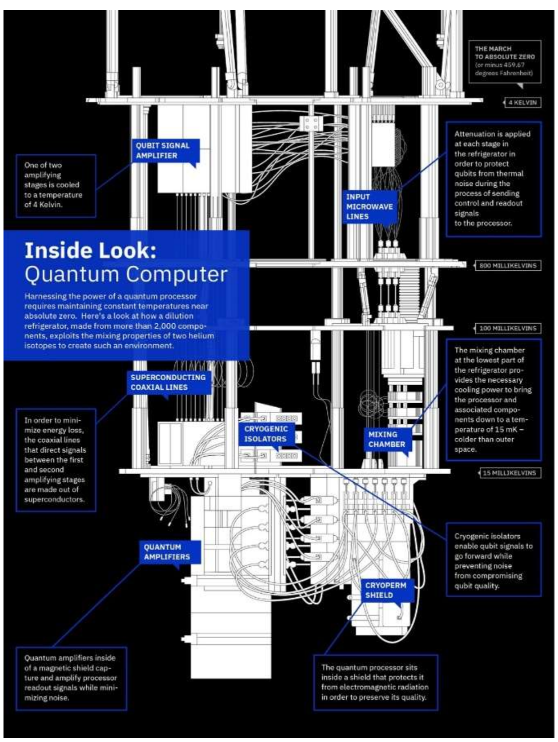
Finally, upon termination of the algorithm, the result needs to be read off. In the case of a classical computer, we sample from the probability distribution on the three-bit register to obtain one definite three-bit string, say 000. Quantum mechanically, one measures the three-qubit state, which is equivalent to collapsing the quantum state down to a classical distribution (with the coefficients in the classical state being the squared magnitudes of the coefficients for the quantum state, as described above), followed by sampling from that distribution. This destroys the original quantum state. Many algorithms will only give the correct answer with a certain probability. However, by repeatedly initializing, running and measuring the quantum computer's results, the probability of getting the correct answer can be increased. In contrast, counterfactual quantum computation allows the correct answer to be inferred when the quantum computer is not actually running in a technical sense, though earlier initialization and frequent measurements are part of the counterfactual computation protocol.

Quantum Computer cooling

- ✓ Reduction of the temperature of the computing environment below approximately 80mK is required for the processor to function, and generally performance increases as temperature is lowered - the lower the temperature, the better. The QPU and parts of the input/output (I/O) system, comprising roughly 10kg of material, is cooled to this temperature, which is approximately 180 times colder than interstellar space! Most of the physical volume of the current system is due to the large size of the refrigeration system. The refrigeration system used to cool the processors is known as a dilution refrigerator.
- ✓ To reach the near-absolute zero temperatures at which the system operates, the refrigerators use liquid helium as a coolant. This means that all the liquid helium resides inside a closed cycle system, where it is recycled and re-condensed using a pulse-tube technology.

"The Fridge" is a closed cycle dilution refrigerator. The superconducting processor generates no heat. Cooled to 180x colder than interstellar space (0.015 Kelvin).





Superconducting coaxial lines:
They minimize the energy loss, and direct the signals between the first and second amplifying stages and these lines are made out of superconductor.

Quantum Amplifier:
Quantum Amplifier inside of a magnetic shield capture and amplify processors readout signals and minimize the noise.

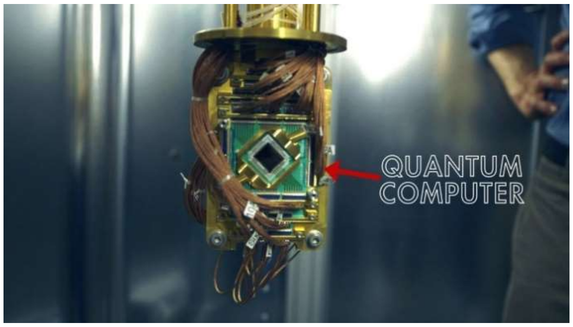
Cryoperm Shield:
The quantum processor sits inside the shield and protect it from the external electromagnetic radiation in order to preserve its quality.

Cryogenic Isolators:
Cryogenic isolator enables qubit signals to go forward while preventing the noise from compromising the quality of qubit.

Mixing Chamber:
Mixing chamber at the lowest part of the refrigerator provides the necessary cooling to bring the processor and the necessary components to the temperature of 15mK.

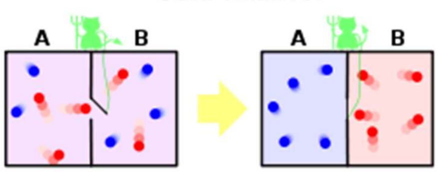
Input Microwave Line:

Attenuation is applied to each stage of the refrigerator in order to
protect the qubits from the thermal noise during the process of sending the control and readout signals to the processor.



Maxwell Demon Method for cooling the Quantum Computer

Maxwell's demon is a experiment created by the physicist James Clerk Maxwell in which he suggested how the second law of thermodynamics might hypothetically be violated. In the experiment, a demon controls a small door between two chambers. As individual molecules approach the door, the demon quickly opens and shuts the door so that fast molecules pass into the other chamber, while slow molecules remain in the first chamber. Because faster molecules are hotter, the demon's behavior causes one chamber to warm up as the other cools, thus decreasing entropy and violating the second law of thermodynamics.



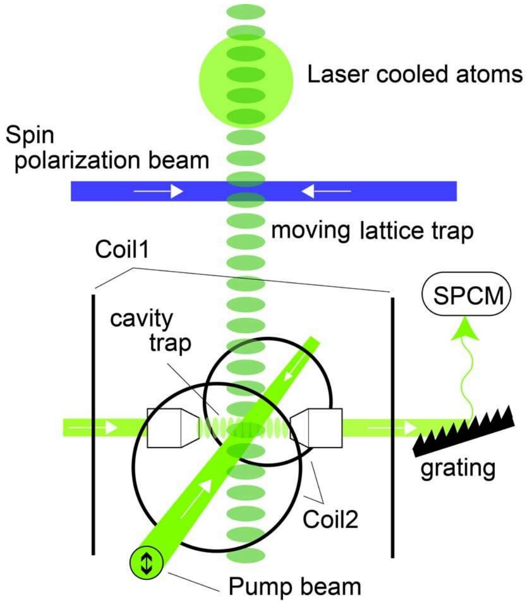
Energy Exchange Method for cooling the Quantum Computer

The particles that make up a liquid or a gas have different energies. The distribution of these energies depends on the temperature. The hotter the gas, the higher the number of particles with high energies. Therefore, a simple trick can be used to cool down cold gases: with the help of electromagnetic fields, the particles with the highest energy are removed from the gas. The remaining ones interact, redistribute the energy, and the gas relaxes again to a typical energy distribution -- but at a slightly lower temperature than before.

The experiments in Schmiedmayer's research group. "The particles with the highest energy manage to leave the liquid and are blown away. The remaining quickly reaches an equilibrium state at a slightly lower temperature."

However, there are cases, in which reaching such a thermal equilibrium is not possible. A Newton's cradle for example is a device that has several spheres hanging from strings, arranged in a straight line. When one of the spheres is set in motion and hits the others, the last sphere in line is kicked away, while the others do not move. "In this case, the spheres can only exchange energies between each other. Researchers studied a similar system: a one-dimensional gas of atoms, kept in a straight line by an electromagnetic trap. The atoms can just exchange their energies, just like the spheres in Newton's cradle. Therefore, one would expect the cooling mechanism of removing the most energetic particles to fail in this case. When the fastest particles are gone, no other particles in the gas will ever have the same speed again. According to this simple model, an energy that is missing will be gone forever.

Astonishingly, this is not true for the one-dimensional gas. It can be cooled down by continuously removing particles -- to much lower energies than one would expect, according, to the simplified picture of fast and slow particles.



Sensor use to detect the electron spin:

Use of nitrogen-vacancy (NV) defects in diamonds. These defects in which one carbon atom in a diamond is replaced with a nitrogen atom and a neighbouring atom is removed can be used to detect minute magnetic fields.

Tiny rods of diamond containing NV centres are fabricated and are placed nanometres above the chip (Quantum processing unit). As the spin waves move through the material, they generate a magnetic field, which is picked up by the NV centre. Based on NV-centre measurements, we can figure out the spin.

Grover's Algorithm /Operator

Grover's algorithm is a quantum algorithm that finds with high probability the unique input to a black box function that produces a particular output value, using just evaluations of the function, where *N* is the size of the function's domain. It was devised by Lov Grover in 1996.

The analogous problem in classical computation cannot be solved in fewer than evaluations (because, in the worst case, the *N*-th member of the domain might be the correct member). At roughly the same time that Grover published his algorithm, Bennett, Bernstein, Brassard, and Vazirani proved that no quantum solution to the problem can evaluate the function fewer than times, so Grover's algorithm is asymptotically optimal.

It has been shown that a non-local hidden variable quantum computer could implement a search of an N-item database at most in steps. This is faster than the steps taken by Grover's algorithm. Neither search method will allow quantum computers to solve NP-Complete problems in polynomial time.

Unlike other quantum algorithms, which may provide exponential speedup over their classical counterparts, Grover's algorithm provides only a quadratic speedup. However, even quadratic speedup is considerable when is large. Grover's algorithm could brute-force a 128-bit symmetric cryptographic key in roughly 2^{64} iterations, or a 256-bit key in roughly 2^{128} iterations. As a result, it is sometimes suggested that symmetric key lengths be doubled to protect against future quantum attacks.

Like many quantum algorithms, Grover's algorithm is probabilistic in the sense that it gives the correct answer with a probability of less than 1. Though there is technically no upper bound on the number of repetitions that might be needed before the correct answer is obtained, the expected number of repetitions is a constant factor that does not grow with . Grover's original paper described the algorithm as a database search algorithm, and this description is still common. The database in this analogy is a table of all of the function's outputs, indexed by the corresponding input.

The algorithm requires an N-dimensional state space H, which can be supplied by $n = \log_2 N$ qubits. Consider the problem of determining the index of the database entry that satisfies some search criterion. Let f be the function that maps database entries to 0 or 1, where $f(x) = 1$ if and only if x satisfies the search criterion ($x = \omega$). We are provided with (quantum black box) access to a subroutine in the form of a unitary operator U_ω that acts as follows:

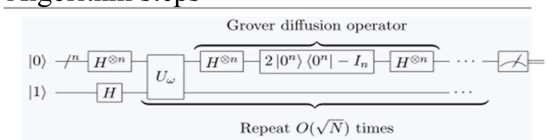
An alternative definition of U_ω may be encountered assuming the presence of an ancillary qubit system (like in the quantum circuit depicted below). The operation then represents a conditional inversion (*NOT* gate) conditioned by the value of $f(x)$ on the main system:

This is a natural way to realize a binary operation using the method of un-computation. Note that if the ancillary qubit is prepared in the state , the effective operation of this controlled *NOT* gate becomes equivalent to the original form, leaving the ancillary system disentangled from the main system:

In either setting, our goal is to identify the

index .

Algorithm steps



Quantum circuit representation of Grover's algorithm

The steps of Grover's algorithm are given as follows. Let denote the uniform superposition over all states

The algorithm:

1. Initialize the system to the state .
2. Perform the following "Grover iteration" $r(N)$ times. The function $r(N)$, which is asymptotically $O(N^{1/2})$, is described below.
3. Apply the operator .
4. Perform the measurement Ω. The measurement result will be eigenvalue λ_ω with probability approaching 1 for $N \gg 1$. From λ_ω, ω may be obtained.

Application

- Medicine and Materials: Untangling the complexity of molecular and chemical interaction leading to discovery of new material and medicine.
- Artificial Intelligence: Making machine learning powerful when the availability of data is extremely large.
- Financial Services: Finding of new ways to model financial data and isolating key global risk factor.
- Supply chain Logistics: Finding out most ultra-efficient logistics and global chain, for optimizing fleet operation.
- Military Operations.
- Image Processing.
- Data Acquisition
- Encryption and decryption of the data.

Artificial Intelligence

A primary application for quantum computing is artificial intelligence (AI). AI is based on the principle of learning from experience, becoming more accurate as feedback is given, until the computer program appears to exhibit "intelligence."

This feedback is based on calculating the probabilities for many possible choices, and so AI is an ideal candidate for quantum computation. It promises to disrupt every industry, from automotive to medicine, and it's been said AI will be to the twenty-first century what electricity was to the twentieth.

For example, Lockheed Martin plans to use its D-Wave quantum computer to test autopilot software that is currently too complex for classical computers, and Google is using a quantum computer to design software that can distinguish cars from landmarks. We have already reached the point where AI is creating more AI, and so its importance will rapidly escalate.

Molecular Modeling

Another example is precision modelling of molecular interactions, finding the optimum configurations for chemical reactions. Such "quantum chemistry" is so complex that only the simplest molecules can be analysed by today's digital computers.

Chemical reactions are quantum in nature as they form highly entangled quantum superposition states. But fully-developed quantum computers would not have any difficulty evaluating even the most complex processes.

Google has already made forays in this field by simulating the energy of hydrogen molecules. The implication of this is more efficient products, from solar cells to pharmaceutical drugs, and especially fertilizer production; since fertilizer accounts for 2 percent of global energy usage, the consequences for energy and the environment would be profound.

Cryptography

Most online security currently depends on the difficulty of factoring large numbers into primes. While this can presently be accomplished by using digital computers to search through every possible factor, the immense time required makes "cracking the code" expensive and impractical.

Quantum computers can perform such factoring exponentially more efficiently than digital computers, meaning such security methods will soon become obsolete. New cryptography methods are being developed, though it may take time: in August 2015 the NSA began introducing a list of quantum-resistant cryptography methods that would resist quantum computers, and in April 2016 the National Institute of Standards and Technology began a public evaluation process lasting four to six years.

There are also promising quantum encryption methods being developed using the one-way nature of quantum entanglement. City-wide networks have already been demonstrated in several countries, and Chinese scientists recently announced they successfully sent entangled photons from an orbiting "quantum" satellite to three separate base stations back on Earth.

Financial Modeling

Modern markets are some of the most complicated systems in existence. While we have developed increasingly scientific and mathematical tools to address this, it still suffers from one major difference between other scientific fields: there's no controlled setting in which to run experiments.

To solve this, investors and analysts have turned to quantum computing. One immediate advantage is that the randomness inherent to quantum computers is congruent to the stochastic nature of financial markets. Investors often wish to evaluate the distribution of outcomes under an extremely large number of scenarios generated at random.

Another advantage quantum offer is that financial operations such as arbitrage may require many path-dependent steps, the number of possibilities quickly outpacing the capacity of a digital computer.

Weather Forecasting

NOAA Chief Economist Rodney F. Weiher claims (PowerPoint file) that nearly 30 percent of the US GDP ($6 trillion) is directly or indirectly affected by weather, impacting food production, transportation, and retail trade, among others. The ability to better predict the weather would have enormous benefit to many fields, not to mention more time to take cover from disasters.

While this has long been a goal of scientists, the equations governing such processes contain many, many variables, making classical simulation lengthy. As quantum researcher Seth Lloyd pointed out, "Using a classical computer to perform such analysis might take longer than it takes the actual weather to evolve!". Director of engineering at Google Hartmut Neven also noted that quantum computers could help build better climate models that could give us more insight into how humans are influencing the environment. These models are what we build our estimates of future warming on, and help us determine what steps need to be taken now to prevent disasters.

The United Kingdom's national weather service Met Office has already begun investing in such innovation to meet the power and scalability demands they'll be facing in the 2020-plus timeframe, and released a report on its own requirements for exascale computing.

Particle Physics

Coming full circle, a final application of this exciting new physics might be… studying exciting new physics. Models of particle physics are often extraordinarily complex, confounding pen-and-paper solutions and requiring vast amounts of computing time for numerical simulation. This makes them ideal for quantum computation, and researchers have already been taking advantage of this.

Researchers at the University of Innsbruck and the Institute for Quantum Optics and Quantum Information (IQOQI) recently used a programmable quantum system to perform such a simulation. Published in Nature, the team used a simple version of quantum computer in which ions performed logical operations, the basic steps in any computer calculation. This simulation showed excellent agreement compared to actual experiments of the physics described.

"These two approaches complement one another perfectly," says theoretical physicist Peter Zoller. "We cannot replace the experiments that are done with particle colliders. However, by developing quantum simulators, we may be able to understand these experiments better one day."

Investors are now scrambling to insert themselves into the quantum computing ecosystem, and it's not just the computer industry: banks, aerospace companies, and cybersecurity firms are among those taking advantage of the computational revolution.

While quantum computing is already impacting the fields listed above, the list is by no means exhaustive, and that's the most exciting part. As with all new technology, presently unimaginable applications will be developed as the hardware continues to evolve and create new opportunities.

Summary

Thus, we have studied the difference between classical and quantum computer. The working of the quantum computer and the quantum mechanics ruling/governing the quantum computer. How fast the quantum computer performs and their speed of computing compared to classical and super computer, and their widespread application.

References

- http://www.research.ibm.com
- https://www.dwavesys.com/d-wave-two-system
- Massachusetts Institute of Technology Research Paper by Wei Han Huang