Strengths and Weaknesses of Quantum Computing

Zahid Hussain

MS150200612, Virtual University of Pakistan

Zahidhussain334@gmail.com

Asma Talib

ms150401131

studentvu6@gmail.com

Abstract— Computers have evolved very much from last half century. The modern day computers are very small, fast, powerful and energy efficient. But this growth has a limit. Now scientists are working on a completely new kind of computer based on the Quantum physics rules. These computers are called quantum computers. The Quantum computers can solve many problems which are not solvable by the current classical computer systems. The large scale production of the Quantum computers will start soon, which will totally change the computers and this, will affect every field.

Keywords— **Quantum Computers, Qubit, Strengths and Weaknesses, Computation,**

I. INTRODUCTION

Quantum computational complexity is an exciting new area that touches upon the foundations of both theoretical computer science and quantum physics. The computational power of quantum Turing machines (QTMs) has been explored by several researchers and many researchers and companies are working on it currently. Early work done by Deutsch and Jozsa showed how to utilize some inherently quantum mechanical features of QTMs. Their results and the later research results by Berthiaume and Brassard established the existence of oracles under which there exists some computational problems that QTMs can solve in polynomial time with certainty, whereas if we require a classical probabilistic Turing machine to produce the correct answer with certainty, then it must take exponential time on some inputs.

Quantum computer works differently from the traditional computers. The traditional computers can work on and compute only one transaction at a time. On the other hand the quantum computers can work on and perform multiple transactions at the same time which increase their speed more than traditional computers.

The fund amental building block of a quantum computer is Qubit as shown in the diagram.

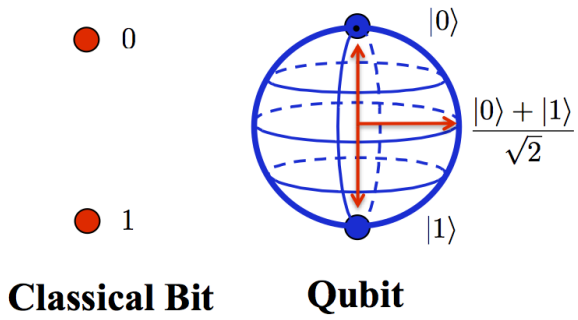

Figure: 1 Classical Bit Vs Qubit.

An ordinary bit can compute or store 0 or 1 but a Qubit can work and operate in between the values of 0 and 1.

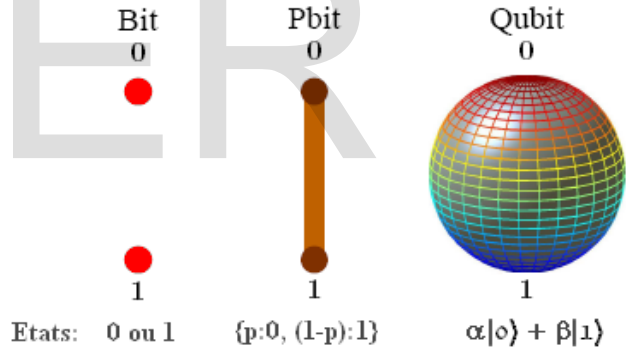

Figure: 2 Shows Difference between digital bit and Qubit

Qubits are made up of two things first is the controlled particles and second one is the means of control.

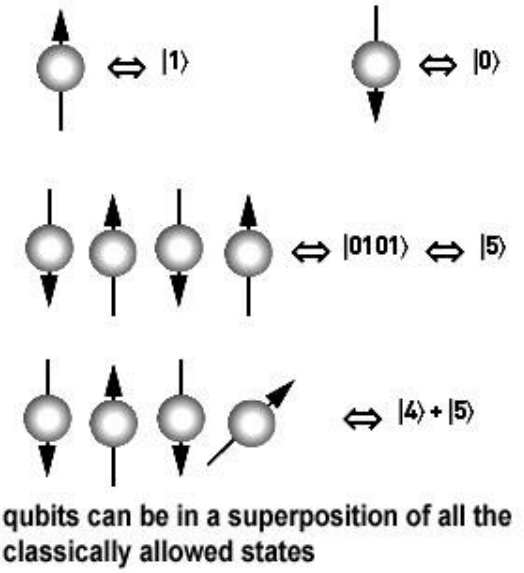

Figure: 3 Qubit. [21]

The following table will show the comparison between the classical computing and quantum computing.

TABLE I
COMPARISON OF TRADITIONAL AND QUANTUM COMPUTING

S.No	Description	Classical Computing	Quantum Computing
1	Information storage and representation	0 or 1	Qubit
2	Delivery of information	Information can be copied without distributing.	Information cannot be copied distributing
3	Behaviour of information	Unidirectional	Multidirectional
4	Security	Hacker can break into communication	Hacker cannot break into communication.
5	Noise Tolerance	Noisy channel can be used to deliver the information.	Noiseless channel is required.
6	Computation Cost.	Directly proportional to the computation	Not Directly proportional to the computation

II. REVIEW AND RELATED WORK

A Large 3-Dimensional cluster lattice is used as resource for quantum computer to process information and it is also used in mainframe computers. This is the idea which can lead to a construction of 7.5 billion photonic chips Quantum Computer.

The computer models which are motivated by physics relate to both of the systems. These have both physical as well as computational interpretation. Quantum mechanics represent most of our understanding which is related to microscopic physical phenomena and the operations of a computer should also be in form of quantum mechanics.

Quantum computing is still at evolving stage and no one yet knows when its requirements will be met, weather some tradeoffs will be made or research on entirely new path will begun. It is proposed that how explicit microscopically models of quantum computer register can be made and sphere models bonded with the first and second kind can be used to represent quantum register.

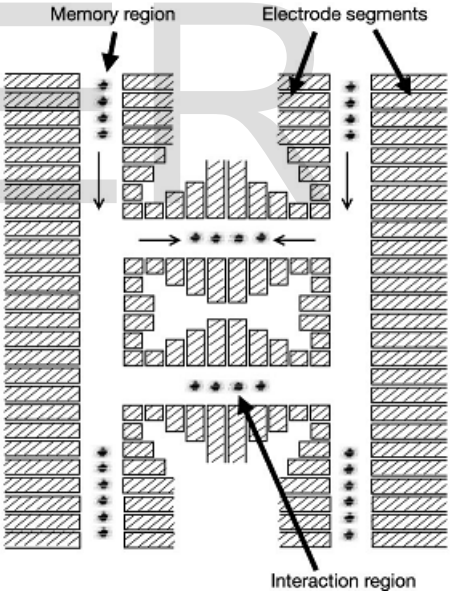

Figure: 4 Quantum Charged Coupled Device (QCCD) [1]

Ion traps can be used as the building block of quantum computers.

So what is an ion? An ion is an atom that has lost one or more of its electrons. An ion trap is a system which consists of electric and magnetic fields, which can capture ions and keep them at locations. Using an ion trap, one can arrange several ions in a line, at regular intervals

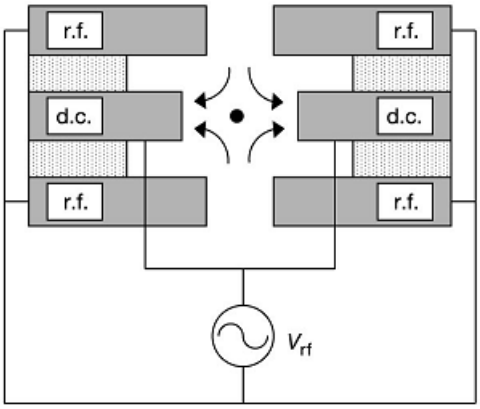

Figure: 5 Configuration of static and radio frequencies for QCCD. [2]

III. HISTORY OF QUANTUM COMPUTING

In 1982, the Nobel Prize winner physics scientist Richard Feynman thought up the idea of a quantum computer. He thought it as a computer that can use the effects of quantum mechanics to its advantage [23]. A quantum computer would be able to crack the codes more speedily than any ordinary classical computer.

In 2000 March, Scientists from Los Alamos National Laboratory announced that they have succeeded to develop a 7-qubit quantum computer with a single drop of liquid.

In 2001 IBM and Stanford University scientists successfully experienced Shor's Algorithm on a quantum computer. The Shor's Algorithm is used to find the prime factors of numbers. These scientists used a 7-qubit computer to calculate the factors of number 15. The computer correctly calculated that the prime factors were 3 and 5.

In 2006 Scientists in Waterloo and Massachusetts establish ways to control a 12-qubit system. They found that Quantum computation related control becomes more and more complex as we increase the number of Qubits.

In 2007 Canadian base quantum computer manufacturing company D-Wave created a 16- qubit quantum computer. This quantum computer solved many pattern matching problems.

IV. QUANTUM LANGUAGES

QCL (Quantum Computer Language) is the most advanced implemented quantum programming language. Its syntax is similar to the syntax of the C programming language and classical data types are similar to data types in C.

Quantum Computation involves some new concepts which are related to the movement of the particles like entanglement. So the Quantum programming language should be able to deal with these concepts.

Conventionally the quantum languages are defined at the low level and which discourages the normal programming practices so a new high language is described which has proper properties of a language. [4]

The Quantum Languages are continuously evolving and new dimensions are being added resulting in more structures and high level languages but still there is lot to do.

V. HIGH PERFORMANCE QUANTUM COMPUTING

Various problems which need huge computational power and are unsolvable now days with classical computers will be solved by high performance Quantum computing. The High performance computing will be possible and this will result in huge operations $1x10^{15}$ floating point operations per second. [5] Those super computers which will be having powers of petascale during the processing of some applications can reach to one quadrillion FLOPS. [5]

An algorithm built for this purpose works very well. This algorithm uses 1 to 2 QBIT gates works very well with IBM p690 having 1024 processors and 3TB of memory. [6]

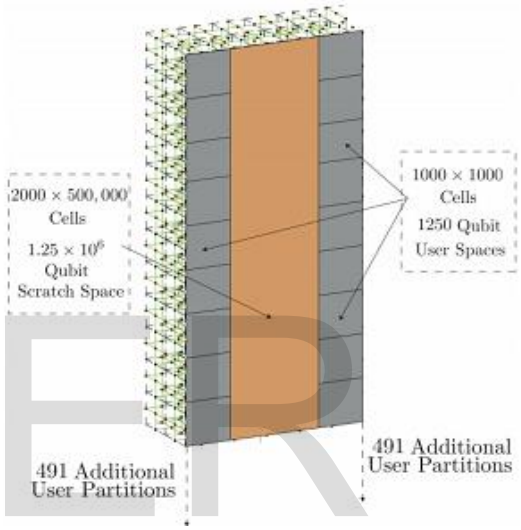

Fig: 6 Partitioning of 3d Global lattice for a HPQC mainframe. [7]

The global lattice shown above measures 4000 x 500,000 unit cells and it is prepared using approximately 7.5 x 109 photonic chips. [7]

The lattice have initiated the idea of a High Performance Quantum Computer, the quantum computer uses a 3 dimensional cluster lattice for processing multiple user related information.

VI. CAPABILITIES AND LIMITATIONS

Quantum computers are much powerful than classical computers. The Quantum computer can solve problems with no time which a classical computer can take years to solve. Quantum computers can perform multiple transactions at one time as compared to the classical computers. This increases their power very much.

The making of quantum computers will be revolutionary for whole mankind. It will reduce workload and solve problems with no time which now we can solve in days or weeks.

On the other hand the quantum computers are still a dream and they are not as much scalable yet. We should not be too optimistic regarding quantum computers because they might let us down. Because this is too early to guess what will they do. Noise distortion can lead to information corruption. Different implementations of Quantum Computers have been developed but they are of limited use and are made only for certain type of demonstration.
Here are few computer science fields in which quantum computers can be used.

A. Cryptography and Quantum Computing:

The cryptographic procedures and methodology are more secured utilizing Quantum cryptography as the routine framework needs one time key exchange for a protected information exchange which can be accomplished by the quantum communication channel.
The protocol is used for key exchange is BB84 and the method is divided in two stages. The communication between the two sites is done over a quantum and public channel respectively. The protocol detects probing if someone tried to hack the network with some very high precision. [8]
The quantum superposition rule has enabled new capabilities for information extraction and sharing which are far more than the conventional techniques.
The quantum systems are prone to inconsistency. Due to perturbations from the environment qubits can become corrupted which will result in the loss of data. The current procedures used in quantum communication lacks the devices which can regenerate the signals. Regeneration will reduce the chance of corrupted data. If proper devices will not be used then the original signal can be destroyed or completely changed, If somehow some procedure is developed to amplify the signal then the same procedure can be used for hacking the signal. [8]

B. Quantum Algorithms

The quantum computing is related with foundations of mathematics and physics. Grover's search uses different technique for speeding up traditional algorithms on quantum computers. [9]
The Grover's search algorithm is very important algorithm in quantum computing. Other than search this algorithm can also be applied to many other problems and it can increase the speed up to polynomial time . If we are searching
in a database a search speed up by square root can make the system very efficient like search engines website databases etc. [10]
Optimal quantum query algorithms for project scheduling is developed along with the improvement in salesman problem quadratic degree faster having maximal degrees of three, four or five. [11]
Some open problems like Boolean matrix product regarding tight time space tradeoffs and Boolean matrix vector and matrix product tradeoffs need to be researched for both classical and quantum computers. [12]
Exponential Congruences Solution in polynomial time is also given in quantum computing.

We are given a,b,c,f,g∈Fq. We must find x,y∈Fq such that afx+bgy=cafx+bgy=c.

Quantum computers can solve this problem in polynomial time. To solve same problem the best classical algorithm requires exponential time. The quantum algorithm of is based on the quantum algorithms for discrete logarithms and searching. [13]

Classical error correcting codes allow the detection and correction of bit-flips by storing data redundantly. Maximum possibility decoding for arbitrary linear codes is NP-complete in the worst case. But for structured codes or bounded error efficient decoding algorithms are known. Quantum algorithms have been formulated to speed up the decoding of convolutional codes and simplex codes [14].

C. Security and Quantum Computing

The best feature of quantum computers is their security. Theoretically speaking, it's impossible to hack the quantum computer system. Quantum computers use observer effect. In this if we try to measure one parameter of a micro-particle will alter another parameter. This phenomenon, should resolve the main issue of classical communications. Each attempt to spy on a communication will alter the transmitted message. There are three main reasons which make the Quantum cryptography much more secure than the classical computation.

Firstly the unknown quantum state cannot be copied and no one can take advantage of the unknown state. Secondly any attempt to calculate and measure the quantum state will make a disturbance in the system and any message which is intercepted by some eavesdropper will become infected. Infected message will be of no use for anyone including recipient. Thirdly if some quantum property is measured and changed it is not possible to reverse it to original state. These three properties gives power to the quantum computation and make it secure from any eavesdropper. [15]
High level research is required in order to standardize the quantum information to make related protocols for quantum computing to make it available for public use.
The hardware which will be required for quantum computation will be similar to QKD communication systems. QKD and quantum both require receivers and transmitters for weak signals.

D. Complexity and Quantum computation

The complexity class P is defined to be the set of problems solvable by a Turing machine in polynomial time. Similarly we can define a quantum complexity class using standard quantum computer or a quantum Turing machine. Thus, the complexity class BQP is defined to be the set of problems solvable by a quantum computer in polynomial time with bounded error.

The complexity theory practitioners give a lot of importance to the Quantum computation, they are not only working on the computational complexity but also on quantum interactive proof systems and quantum related NP.
There are some arguments which say that Church Turing problem cannot be solved using quantum Turing machines or quantum computers. [16]
The graphs related quantum complexity is a new area of research. Quantum query and quantum time complexity is being studied as a part of quantum complexity measures. [17]
The query complexity of a graph algorithm refers to the number of queries adjacency list of the graph and quantum time complexity is related to the basic quantum operations. [17]

VII. PRACTICAL QUANTUM COMPUTERS

D-Wave Systems is a quantum computing company, based in Burnaby, British Columbia, Canada. The D-Wave One was built on early prototypes such as D-Wave's Orion Quantum Computer. The prototype was a 16-qubit quantum annealing processor, demonstrated on February 13, 2007 at the Computer History Museum in Mountain View, California. D-wave is first of its kind commercial quantum computing company which is founded in 1999. [18]

Figure: 7 A D-Wave Quantum Computer.
The D-Wave had worked for five years only gathering information to how to build a quantum computer.
They focused on how to design, manufacture and scale the quantum computer into realization. [18]
Along with the quantum computers different layers of the software are also designed in order to operate on the new hardware and the architecture. The work has also done for solving the industry scale related learning, classification and optimization problems. [18]
D-Wave has doubled the number of qubits each year, and in 2013 they shipped their 512-qubit D-Wave Two™ system. In 2015 they announced general availability of the 1000+ qubit D-Wave 2X™ system. The customers of D-Wave include Google, NASA and University Of Southern California. [18]

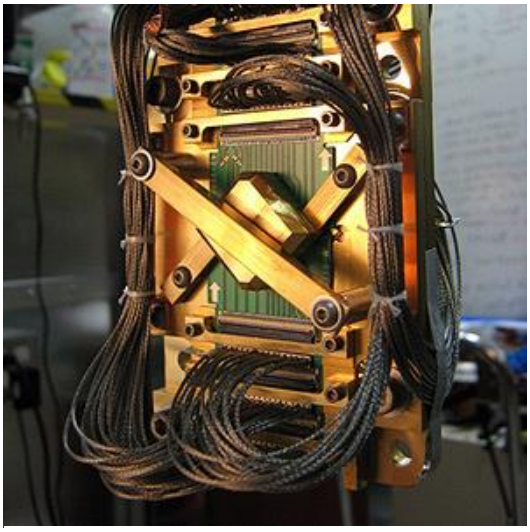

Figure: 8 Quantum leap chip, the heart of D-Wave's computers.

Since 2013, Google scientists have been testing a quantum computer purchased from D-Wave. The new study shows that the upgraded machine Google received earlier this year, the D-Wave 2X, uses quantum tricks to solve some problems 100 million times as fast as an Intel processor running a particular kind of algorithm. [19]
Extensive research is going on at University Of Waterloo regarding quantum error correction and fault tolerance , quantum complexity, quantum algorithms, quantum information theory, spin based quantum information, non electronics related quantum information processing, optical information processing related to quantum theory and quantum cryptography. [28]
The researchers at Waterloo University are working on the laws of nature related to quantum theory so that new powerful technologies can be developed which in result will help in developing future economies. [20]

VIII. HOW QUANTUM COMPUTING WILL CHANGE EVERYTHING

Furthermore quantum computers could herald radical changes for the following areas:
Safer airplanes: Jet software that is currently too complex for classical computers. Lockheed Martin plans to use its D-Wave quantum computer for this purpose.
Discover distant planets: Quantum computers will be able to analyse the vast amount of data which is collected by telescopes and spaceships. Quantum computer can search Earth-like planets from that data.
Boost GDP: By using personalized advertisement, based on quantum computation will encourage consumer spending which will boost GDP.
Detect cancer earlier: Quantum computational models will help determine how diseases develop. So doctors will be able to detect cancer at early stages.

Help automobiles drive themselves: Google is working on this project already that can distinguish cars from landmarks.
Reduce deaths from natural disasters: Precision forecasting will give people more time to take cover and this will reduce deaths from any disaster.
Develop more effective drugs: By analysing DNA-sequencing data, doctors will discover and design superior drug-based treatments.

CONCLUSION

The quantum computers are the future of computing.
Quantum computing is a great prospect and it will solve many problems which cannot be solved by classical computing. It will also decrease the time of problem solving for the problems which are now solvable by classical computing.
The hardware and programs related to Quantum computing are not yet built completely. These are evolving but soon it will become a reality and will change the technology worldwide.
Many technology giants like Google, IBM, Microsoft and the giant of processors intel is also working on quantum computing and they are spending millions of dollars on research.
They are researching on building hardware and algorithms for the quantum computers. The work is also being done in relation to the security and complexity of the quantum computation in order to get secure and reliable quantum systems.
When they will succeed in building Quantum computers, quantum computers will change the entire concept of computing. The speed, the power the time everything will be changed amazingly.
The hardware, programming languages and algorithms will also change.
The measures for security, complexity and cryptography will also change. There will be more secure systems with less hacking chances. Although it is a bad news for hackers.
It will create lot of new opportunities and jobs to computer scientists.
It will also provide benefit to the businesses because quantum computer can predict the financial market more accurately than classical computers. It will generate more money for business persons.
The problems which seem not solvable through traditional computing stand a very good chance to give results using quantum computing.
Every field of life including research, education, engineering, aero-space, medical, technology, media, nuclear technology, space travel, armed forces and sports, in fact every field of life will be affected by the quantum computers.

ACKNOWLEDGMENT

I acknowledge my respected teacher who is supervising this project and will guide me to improve this research paper.

REFERENCES

[1] Figure 1: Diagram of the quantum charge-coupled device (QCCD).Ions are... - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/11308739_fig1_Figure-1-Diagram-of-the-quantum-charge-coupled-device-QCCDIons-are-stored-in-the.
[2] Figure 2: Configuration of radio-frequency (r.f.) and static (d.c.)... - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/11308739_fig2_Figure-2-Configuration-of-radio-frequency-rf-and-static-dc-electrodes-for-the
[3] Quantum computation. David Deutsch, Physics World, 1/6/92*A comprehensive and inspiring guide to quantum computing*
[4] Peter Selinger ,Towards a quantum programming language, ACM Digital Library Volume 14 Issue 4, August 2004
Pages 527 – 586
[5] Sergey Edward Lyshevski, High Performance Computing and Quantum Processing. 2012.
[6] Guido Arnold, Marcus Richter, and Thomas Lippert, High Performance Simulation of Ideal Quantum Computers, NIC Series, Vol. 32 ISBN 3-00-017351-X, pp. 349-356, 2006.
[7] Simon J. Devit, William J. Munro, and Kae Nemoto , High Performance Quantum Computing, Progress in Informatics, No. 8, pp. 1-7, (2011)
[8] Hidayath Ansari, Aditya Parameswaran, Lakulish Antani,Bhaskara Aditya,Ankur Taly and Luv Kumar, Quantum Cryptography and Quantum Computation.
[9] Peter W Shor, Introduction to quantum Algorithms, arXiv.org , Version2, July 6,2001.
[10] Peter W. Shor, Introduction to Quantum Algorithms. Version 2, July 6 2001.
[11] Sebastian Dorn, Quantum Algorithms for Graph Traversals and Related Problems.2009.
[12] Robert Spalek, Quantum Algorithms , Lower Bounds and Time-Space Tradeoffs. arXiv.org Version 2, May 9, 2006.
[13] Wim van Dam and Igor Shparlinski
Classical and quantum algorithms for exponential congruences.
Proceedings of TQC 2008, pg. 1-10.
[14] Alexander Barg and Shiyu Zhou
A quantum decoding algorithm of the simplex code
Proceedings of the 36th Annual Allerton Conference, 1998
[15] Bruce R. Aubum, Quantum Encryption – A Means to Perfect Security , SANS Institute 2003.
[16] Umesh V. Vazirani, A Survey of Quantum Complexity Theory, Proceedings of Symposia in Applied Mathematics, 2002.
[17] Sebastian Dorn, Quantum Complexity Bounds for independent set Problems, arXiv.org, Version 3, February 28, 2007.
[18] http://www.dwavesys.com/our-company/meet-d-wave
[19] https://www.sciencenews.org/blog/science-ticker/google%E2%80%99s-quantum-computer-speeds-practical-use-unclear
[20] https://uwaterloo.ca/institute-for-quantum-computing/
[21] http://en.wikipedia.org/wiki/Qubit