EasyChair Preprint

№ 4958

The Future of Quantum Computer

Vikas Tiwari and Sonia Dubey

February 3, 2021

Volume 1, Issue 4 (2021)
Article No. X
PP XX-XX

VIVA Institute of Technology
9th National Conference on Role of Engineers in Nation Building – 2021 (NCRENB-2021)

VIVA-TECH IJRI
ANNUAL RESEARCH JOURNAL

VIVA-TECH INTERNATIONAL JOURNAL FOR RESEARCH AND INNOVATION
ANNUAL RESEARCH JOURNAL
ISSN(ONLINE): 2581-7280

THE FUTURE OF QUANTUM COMPUTER

Vikas Rajendradeo Tiwari[1], Prof. Sonia Dubey[2]
[1](*Department of Computer Application, Viva School of MCA, University of Mumbai,India)*
[2](*Department of Computer Application, Viva School of MCA, University of Mumbai,India)*

Abstract : *Quantum Computer is a machine that is used for Quantum Computation with the help of using Quantum Physics properties. Where classical computers encode information in binary "bits" that can either 0s or 1s but quantum computer use Qubits. Like the classical computer, the Quantum computer also uses 0 and 1, but qubits have a third state that allows them to represent one or zero at the same time and it's called "Superposition". This research paper has presented the Basics of Quantum Computer and The Future of Quantum Computer. So why Quantum Computer can be Future Computer, Because Quantum Computer is faster than any other computer, as an example, IBM's Computer Deep Blue examined 200 million possible chess moves each second. Quantum Computer would be able to examine 1 trillion possible chess moves per second. It can be 100 million times faster than a classical computer. The computer makes human life easier and also focuses on increasing performance to make technology better. One such way is to reduce the size of the transistor and another way is to use Quantum Computer. The main purpose of this paper is to know that how Quantum Computers can become the future computer.*

Keywords - *Computation, Superposition, Entanglement, Quantum Bits, Transistor*

1. INTRODUCTION

Why we need Computers because computers reduce human effort and make human life easier. However, there are challenges that today's systems will never be able to solve therefore we need Quantum Computer. To be able to solve some of these problems, we need a new kind of computing. Quantum computers leverage the quantum mechanical phenomena of superposition and entanglement to create states that scale exponentially with the number of qubits. Quantum computers can spur the development of new scientific advances, life-saving drugs, rapid diagnostic techniques, high-performance equipment and materials, retirement financial strategies, and quick-tracking algorithms for resources such as ambulances.

With the development of Science and Technology, they were focused on Quantum Physics Properties to make technology more advance. Quantum Computer is a machine that is used for Quantum Computation with the help of using Quantum Physics properties. The possibility of quantum computing was first proposed by physicist Richard Feynman in 1982. Quantum physics has challenged logic since the atom was first studied in the early 20th century. It turns out atoms don't follow the conventional rules of physics. Quantum particles can move forward or backward in time, exist in two places simultaneously, and even "teleport." It's these strange behaviors that quantum computers aim to use to their advantage.

In 1994, mathematician Peter Shaw demonstrated how quantum computing could be used to crack the common encryption standards that existed at the time, which could find the prime factors of large numbers efficiently, which could detect prime factors of large numbers efficiently. Here, "efficiently" means at the time of practical value, which is beyond the capability of state-of-the-art classical algorithms. While this may seem an oddity, it is impossible to convey the significance of Shor's understanding. The security of almost every online transaction today depends on the RSA cryptosystem system that hinges on the intractability of the factoring problem to classical algorithms.

2. QUANTUM CIRCUIT

2.1 Definition

The prevailing model of quantum computation represents the computation in terms of a network of quantum logic gates. This model could be thought of as an abstract linear-algebraic generalization of a classical circuit. Since this circuit model performs quantum mechanics, a quantum computer able to efficiently controlling these circuits is believed to be physically realizable.

A memory consisting of n bits of data has 2^n possible states. A vector representing all memory states thus has 2^n entries (one for each state). This vector is observed as a probability vector and describes the fact that the memory is to be found in a particular state.

In a classical way, one entry would have a value of 1 (i.e. a 100% probability of being in this state), and all other entries will be zero. In quantum mechanics, probability vectors are generalized to frequency operators. This is the technically accurate mathematical foundation for quantum logic gates, but the intermediate quantum state vector formalism is usually introduced first because it is conceptually simpler. This paper focuses on the quantum state vector formalism for purity.

We begin by examining a simple memory consisting of only one bit. This memory may be discovered in one of two states: the zero state or the one state. We may describe the state of this memory using Dirac notation so that

$$|0\rangle := \binom{1}{0}; \qquad |1\rangle := \binom{0}{1}$$

A quantum memory may then be found in any quantum superposition $|\psi\rangle$ of the two classical states $|0\rangle$ and $|1\rangle$:

$$|\Psi\rangle := \alpha|0\rangle + \beta|1\rangle = \binom{\alpha}{\beta}; \quad |\alpha|^2 + |\beta|^2 = 1$$

2.2 Quantum algorithms

Progress in finding quantum algorithms usually focuses on this quantum circuit model, even if something similar to the existing quantum adiabatic algorithm. Quantum algorithms can be categorized almost by the type of speed achieved above the corresponding classical algorithms. Quantum algorithms offer more than a polynomial speedup over a well-known classic algorithm including the Shor algorithm for generating algorithms and quantum algorithms related to using unambiguous logarithms, solving Pell's equation, and problem-solving of the hidden group problem of abelian finite groups. These algorithms are based on the classics of the Fourier quantum modification. No statistical evidence has been found to indicate that the fast classical algorithm cannot be detected, although this is considered impractical. Certain oracle problems such as Simon's problem and Bernstein's problem - Vazirani offers unstructured speed, even though this is a quantum query model, which is a restricted model where lower limits are much easier to prove, and does not mean translating into speedups to work problems.

Other problems, including the imitation of quantum physical processes from chemical and solid-state physics, the limitations of certain Jones polynomials, and the quantum algorithm of the corresponding systems of equations have quantum algorithms that appear to provide super-polynomial speedups and finished with BQP. Because these problems are complete with BQP, a fast classical algorithm for them would mean that there is no quantum algorithm that offers high polynomial speeds, which they believe is impossible.

Other quantum algorithms, such as the Grover algorithm and amplitude amplification, offer polynomial speeds over similar classical algorithms. Although these algorithms offer the same quadratic speed, they are very effective and thus provide speedups for a variety of problems. Many examples of quantum speedups for questioning problems are related to Grover's algorithm, including Brassard, Høyer's algorithm, and Tapp for two to one collision, using Grover's algorithm, and Farhi, Goldstone, and Gutmann's NAND test algorithm trees, different from the search problem.

VIVA Institute of Technology
9th National Conference on Role of Engineers in Nation Building – 2021 (NCRENB-2021)

3. FUNDAMENTALS OF QUANTUM COMPUTING

All computing systems depend on a fundamental ability to store and manipulate information. Current computers use individual bits, which is store information as binary 0 and 1 states. Quantum computers leverage quantum mechanical phenomena to use information. To do this, they rely on quantum bits (qubits).

3.1 Quantum Properties

There are three quantum mechanical properties that is superposition, entanglement, and interference are used in quantum computing to manipulate the state of a qubit.

3.1.1. Superposition

Superposition refers to the quantum phenomenon where a quantum system can represent multiple states simultaneously.

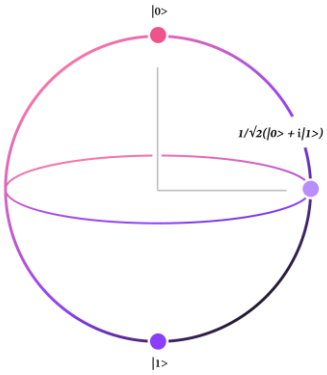


Fig 1. Superposition

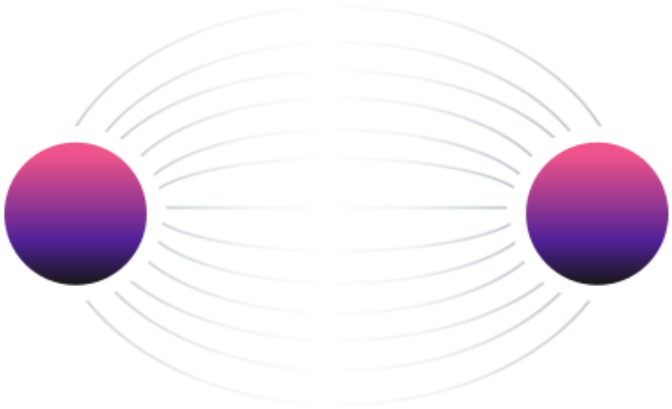


Fig 2. Entanglement

3.1.2. Entanglement

Quantum entanglement is a quantum mechanical phenomenon in which is the quantum states of two or more objects have to be specified with relating to each other, even though the individual objects may be spatially separated.

3.1.3. Interference

Quantum states can undergo interference due to a phenomenon known as a phase. Quantum interference can understand like to wave interference; when two waves are in phase, their amplitudes add, and when they are out of phase, their amplitudes will be cancelled.

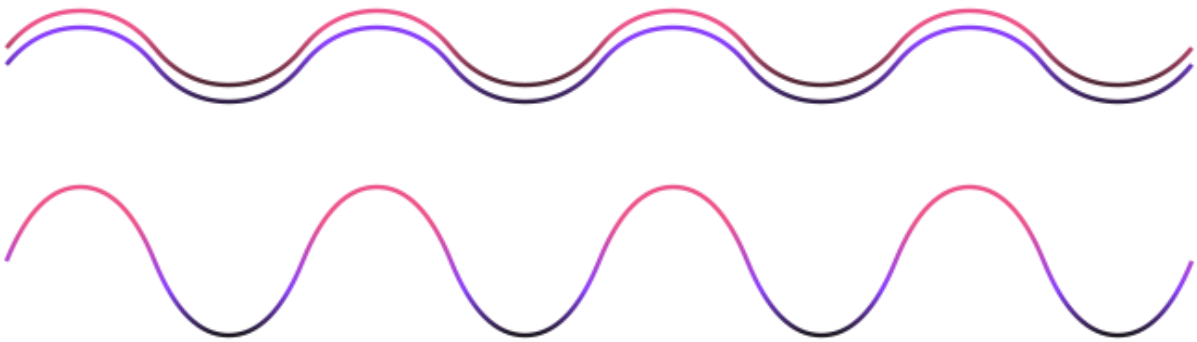
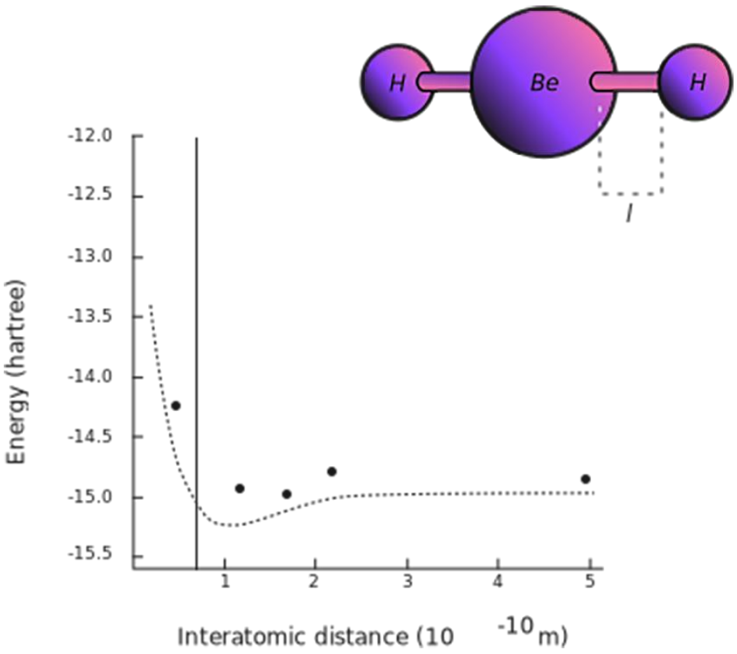


Fig 3. Interference

3.2 Quantum Computation

There are some different ways quantum systems use quantum properties to compute. Let's examine one type of algorithm designed for present quantum hardware, which uses quantum computing to find the "best" solution among various possible solutions.

This algorithm can be used to affect a molecule by determining the lowest energy state between several molecular bond lengths. For each available bond length, parts of the energy state are described on a quantum processor. Then, features of the quantum state are measured and related back to energy in the molecule, to the provided electronic configuration.
Repeating this process for different inter-atomic spacing's ultimately leads to the bond length with the lowest energy state, which describes the equilibrium molecular configuration.



In addition to algorithms for near-term quantum computing systems, researchers have created algorithms for future quantum systems, usually related to fault-tolerant quantum computers. These systems will need to implement many sequential quantum operations and run for long periods of time.

Fig 4. Experimental results (circles) and the exact energy values (dotted line) for several interatomic distances of BeH2

4. QUANTUM COMPUTER : FUTURE COMPUTER

4.1. Quantum Computer vs Classical Computer

Quantum computers can solve problems that are impossible or would take billions of years for classical computers to solve.

Quantum computers would change the landscape of data security. Even though quantum computers will be able to crack many of today's encryption techniques.

Classical computers are good at some tasks than quantum computers (email, spreadsheets, and more). The purpose of quantum computers is to be a different tool to solve various problems, not to replace classical computers.

Quantum computers are great than Classical Computer for solving optimization problems. Google claims that it has a quantum computer that is 100 million times faster than any classical computer.

Every day, we produce 2.5 Exabytes of data. That number is similar to the content on 5 million laptops. Quantum computers can make it possible to process the amount of data we're creating in the time of big data.

4.2. Why Quantum Computer?

According to the report, a Quantum Computer is 100 million times faster than a Classical Computer. For example, once IBM's computer Deep Blue defeated chess champion, Garry Kasparov in 1997. It was able to gain a competitive advantage because it calculates 200 million possible moves each second. A Quantum Computer will be able to examine 1 trillion moves per second!

Rather than using more electricity, quantum computers would reduce power consumption anywhere from 100 to 1000 times because quantum computers use quantum tunnelling. There are various algorithms already developed for quantum computers including Grover's for searching an unstructured database and Shor's for factoring large numbers. Once a stable quantum computer gets developed, expect that machine learning will exponentially stimulate even reducing the time to solve a problem from hundreds of thousands of years to seconds.

The aim of developing a quantum computer sophisticated enough to execute Shor's algorithm for large numbers has been a primary motivator for advancing the field of quantum computation. To develop a broader view of quantum computers, however, it is necessary to understand that they will likely deliver tremendous speed-ups for only specific types of problems. Researchers are researching to both understand which problems are suited for quantum speed-ups and develop algorithms to prove them. As usual, it is believed that quantum computers would help immensely with problems related to optimization, which play important roles in everything from protect to financial trading.

Many additional applications for quantum bit systems that are not related to computing also exist and are active areas of research, but they are beyond the scope of this overview. Two of the most prominent areas are first is quantum sensing and metrology, which leverage the extreme sensitivity of qubits to the environment to realize sensing beyond the classical shot-noise limit, and second is quantum networks and communications, which may lead to revolutionary ways to share information.

5. CONCLUSION

In this paper we have researched Quantum Computer and why it can become a future computer. The aim of this paper is to understand how quantum computers can overtake current classical computers in the future. This paper will help the reader to know about quantum computers. And we have also focus on quantum algorithms and fundamentals of quantum computers which included quantum computation, quantum properties - Superposition, Entanglement, and Interference.

In the future, there has a large demand for Quantum Computers and currently, multiple Companies and scientists are researching Quantum computers to launch them commercially. Because a quantum computer can do those things which are impossible or would take billions of years for any classical computers.

6. ACKNOWLEDGEMENT

I am thankful to my college for giving me this opportunity. I give my special thanks and sincere gratitude towards Prof. Sonia Dubey for encouraging me to complete this research paper, guiding me and helping me through all the obstacles in the research. Her self-less preaching influenced almost every aspect of my thought.

I also present my obligation towards all our past years teachers who have bestowed deep understanding and knowledge in us, over the past years. We are obliged to our parents and family members who always supported me greatly and encouraged me in each and every step.

7. REFERENCES

[1] Shohini Ghose "The Future of Quantum Computing, 2020". https://www.bosch.com/stories/future-of-quantum-computing/

[2] "What Are Quantum Computers And Why Are They Important?". https://ictreverse.com/what-are-quantum-computers-and-why-are-they-important/

[3] William Coffeen Holton "Quantum computer". https://www.britannica.com/technology/quantum-computer

[4] Chris Bernhardt "Quantum Computer for Everyone 2019, Massachusetts Institute of technology, 2003".

[5] Bernard Marr "15 Things Everyone Should Know About Quantum Computing, 2017". https://www.forbes.com/sites/bernardmarr/2017/10/10/15-things-everyone-should-know-about-quantum-computing/?sh=6e5092701f73

[6] Bernard Marr "20 Mind-Boggling Facts About Quantum Computing Everyone Should Read, 2018". https://www.forbes.com/sites/bernardmarr/2018/02/23/20-mind-boggling-facts-about-quantum-computing-everyone-should-read/?sh=1d5d0ba55edb

[7] ICTREVERSE "What Are Quantum Computers And Why Are They Important?". https://ictreverse.com/what-are-quantum-computers-and-why-are-they-important/

[8] William Coffeen Holton "Research Professor of Electrical and Computer Engineering, North Carolina State University, Raleigh." https://www.britannica.com/technology/quantum-computer

[9] David Hemmendinger "Professor Emeritus, Department of Computer Science, Union College, Schenectady, New York. Coeditor of Encyclopedia of Computer Science, 2000.

[10] IBM "What is quantum computing?". https://www.ibm.com/quantum-computing/learn/what-is-quantum-computing/

[11] JAKE FRANKENFIELD "Quantum Computing, 2020". https://www.investopedia.com/terms/q/quantum-computing.asp

[12] Donald Krambeck "Fundamentals Of Quantum Computing, 2015". https://www.allaboutcircuits.com/technical-articles/fundamentals-of-quantum-computing

[13] John Preskill (2018). "Quantum Computing in the NISQ era and beyond". *Quantum*. **2**: 79. arXiv:1801.00862. doi:10.22331/q-2018-08-06-79. S2CID 44098998

[14] *Nielsen, Michael A.; Chuang, Isaac L. (2000). Quantum Computation and Quantum Information. Cambridge University Press. ISBN 978-0-521-63503-5.*

[15] SARA GAMBLE "Quantum Computing: What It Is, Why We Want It, and How We're Trying to Get It". https://www.ncbi.nlm.nih.gov/books/NBK538701/

[16] Biham, Eli; Brassard, Gilles; Kenigsberg, Dan; Mor, Tal (2004), "Quantum computing without entanglement", *Theoretical Computer Science*, **320** (1): 15–33, arXiv:quant-ph/0306182, doi:10.1016/j.tcs.2004.03.041, MR 2060181