Original Research Paper

Quantum Computers

Daniel Cordova[1,*], Osman Guzide[2,*]

[1]Department of Computer Sciences, Mathematics, and Engineering, Shepherd University, Shepherdstown, United States of America;
[2]Department of Computer Sciences, Mathematics, and Engineering, Shepherd University, Shepherdstown, United States of America.

Article history
Received: 20 June 2017
Revised: 23 September 2017
Accepted: 3 November 2017

**Corresponding Author*: Daniel Cordova, Shepherd University, Shepherdstown, United States of America;
Email: dcordo01@rams.shepherd.edu

Abstract: Quantum Computers once only existed in dreams and science fiction. Now, they are very much a reality. With Quantum Computers entering the market, questions are being asked. What is a Quantum Computer? What does it do? What are some of its features? And what is the future of Quantum Computers? This paper presents an analysis of Quantum Computers' purpose, functionality, future uses, and limitations.

Keywords: Quantum, Computers, New, Technology, Hardware, Physics.

Introduction

This report presents an analysis of Quantum Computers. Quantum Computers operate differently from normal computers and with good reason. The reason Quantum Computers operate differently than normal computers is because Quantum Computers were built to overcome the limitations of normal computers. As a result Quantum Computers function much differently. Furthermore, as Quantum Computers function differently, they have different possible uses and limitations. In order to accurately understand Quantum Computers, it is necessary to analyze their purpose, functionality, future uses and limitations.

Purpose of Quantum Computers

In order to accurately understand Quantum Computers, it is necessary to analyze their purpose. Quantum Computers were made in response to a physical limitation of computer hardware. As computers have advanced over the years, pieces of computer hardware have gotten more microscopic and more computationally efficient than ever before. However, as pieces of computer hardware approach the size of a couple of atoms, normal physics stops working and quantum physics takes effect. This is a problem, because in quantum physics electricity (or the flow of electrons) cannot be stopped. This is because in quantum physics an electron can pass through an obstruction (like a switch) by a process called quantum tunneling (Mastin 2009). This would cause computers to cease function as computers have transistors, a type of switch. These transistors are nearing the size of a couple of atoms and have a typical size of 14nm (Gartenberg 2016) in width, to put that in perspective, an atom's diameter can be .255nm (Mastin 2009). In short, Quantum Computers were invented to surpass the physical limitations of the hardware by creating a computer whose components are, not only smaller than an atom, but also more computationally efficient than ever before through the use of quantum physics. This is how Quantum Computers got their name, as they use quantum physics to function rather than normal physics.

Functionality of Quantum Computers

In order to accurately understand Quantum Computers, it is necessary to analyze their functionality. While normal computers have bits representing the flow of electricity as a one or no flow of electricity as a zero, Quantum Computers use qubits (quantum bits) which have a probability of being zero or one at any given time which is a concept called superposition (Annenberg Learner 2017). In order to achieve qubits, makers of Quantum Computers use two level quantum systems

as seen in Figure 1. Figure 1 shows an example of a two level quantum system in which there is a counter clockwise flow of current (spin up defined as zero) or clockwise flow of current (spin down defined as one) in the wire. Defining of the spins as one or zero is arbitrary. Types of these systems include electrons with a positive or negative spin in a magnetic field or a photon with a vertical or horizontal polarization. In quantum physics as soon as one of these subatomic particles in a two level quantum systems is measured, the measurement collapses into one of two possible states either zero or one. Qubits are also computationally more efficient. In a normal computer, x normal bits can be in two to the power of x possible states, but only one can be used. However, in a Quantum Computer, x qubits can occupy all two to the power of x possibilities simultaneously. Another advantage of qubits is entanglement which is when a qubit will react to another qubit instantaneously no matter the distance between them (Annenberg Learner 2017). The advantage of this is that only one qubit needs to be measured to determent the other entangled qubits. Qubit manipulation is another essential part of Quantum Computers. While normal computers have logic gates that manipulate inputs and produce an output, Quantum Computers have quantum gates that manipulate probabilities of input superpositions and produce an output superposition. In summary, a Quantum Computer uses qubits, applies quantum gates to superpositions, entangles qubits, outputs a superposition, and measures the qubit collapsing the superposition into one of its possible states of zeros and ones. Because of this system, all possibilities possible with a Quantum Computer's setup are done at the same time. Due to the nature of this probabilistic system, rechecking the output and repeating the process may have to occur. However, this system in Quantum Computers has proven itself to be exponentially more computationally efficient than normal computers.

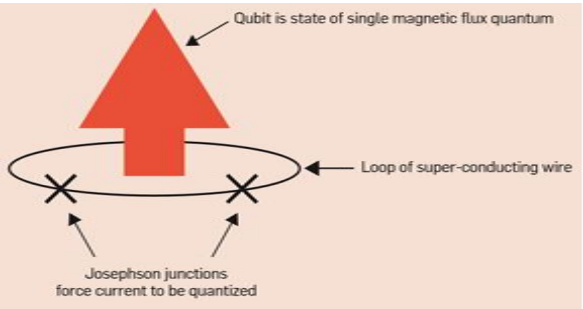

Figure 1. (Van Meter and Horsman 2013).

Future Uses of Quantum Computers

In order to accurately understand Quantum Computers, it is necessary to analyze their future uses. While Quantum Computers may not replace all computers any time soon, they are ideal for some applications. One of these applications is database querying. A query in a database implemented with normal computers today has to look at every single entry resulting in a worse case run time proportional to the number of entries. However, a query in a database implemented with Quantum Computers results in a worse case run time proportional to the square root of the number of entries (Arikan 2002). Table 1 shows a run time comparison of Grover's algorithm for Quantum Computers and a basic search algorithm for a normal computer using big O notation. Search Algorithm written by Daniel Cordova and Grover's Algorithm written by Derek Dang (2016) were run in Java to obtain data. Another application of Quantum Computers is factoring large prime numbers. This could be a significant problem in the coming years, because of commonly used Rivest–Shamir–Adleman (R.S.A.) encryption. In R.S.A. encryption, data is kept secure by two large prime numbers: a public key and private key. The public key is used to encrypt data that only can be decoded with the private key. The problem with this R.S.A. encryption method is that the public key can be used to calculate the private key. Up until now, this method has worked because the computational time required for calculating the private key on any normal computer would take years. However, this is not true for Quantum Computer. Since Quantum Computers are exponentially more computationally efficient than normal computers, the computational time required to calculate the private key is far less than a normal computer. In an effort to make data more secure than ever before companies like "… MagiQ and id Quantique are marketing the first generalization quantum key distribution devices, paving the way to full commercialization" (Bacon and Leung 2007). Thus, Quantum Computers can both hurt and help information security. Another application for Quantum Computers is simulations. Quantum Computers are ideal at simulating complex events such as quantum physics, molecular biology, climate change, traffic patterns, etc. While currently Quantum Computers are seen as just another specialized tool, as more people come to use and

understand Quantum Computers their future uses will continue to grow. As is the case with technology, it is only as limitless as the human imagination.

Table 1. Run Time Comparison

Array Size (n)	Array Search O(n)	Grover's Algorithm $O(\sqrt{n})$
2^{10}	1024	32
2^{12}	4096	64
2^{14}	16384	128
2^{16}	65536	256
2^{18}	262144	512
2^{20}	1048576	1024

Limitations of Quantum Computers

In order to accurately understand Quantum Computers, it is necessary to analyze their limitations. While Quantum Computers are full of potential future uses, they have limitations of cost and time. A brand new Quantum Computer can cost fifteen million dollars (Gartenberg 2017). This poses a definite limitation on Quantum Computers as not everyone can afford one. Another limitation of Quantum Computers is the time of implementation, maintenance, and education of operators. An additional limitation of Quantum Computers is the expertise needed in their development. Quantum Physics experts and Quantum Computer programmers are needed in the building, maintenance, and algorithms writing necessary in a Quantum Computer's operation. As there is a shortage of these experts, Quantum Computers will be limited by the number of people capable of running them. With these challenges in mind, it is uncertain if Quantum Computers will remain a specialized tool or the next computer revolution. However, it is certain that Quantum Computers are another attempt by mankind to overcome physical limitations.

Conclusion

It is necessary to analyze a Quantum Computer's purpose, functionality, future uses, and limitations, in order to accurately understand them. The purpose for the invention of Quantum Computers is to surpass physical limitations of the hardware in normal computers by creating a computer whose components are, not only smaller than an atom, but also more computationally efficient than ever before through the use of quantum physics. Quantum Computers function by using qubits, applying quantum gates to superpositions, entangling qubits, outputting a superposition, and measuring the qubit collapsing the superposition into one of its possible states of zeros and ones. Because of the way a Quantum Computer functions, all possibilities possible with a Quantum Computer's setup are done at the same time making Quantum Computers exponentially more computationally efficient than normal computers. Future uses for Quantum Computers include quick database searching, quick calculation of Rivest–Shamir–Adleman (R.S.A.) private keys, and advanced simulations. While Quantum Computers are full of potential future uses they are not without there challenges in development including: cost of implementation, time of implementation, lack of Quantum Physics experts, and lack of Quantum Computer programmers. With these challenges in mind, it is uncertain if Quantum Computers will remain a specialized tool or the next computer revolution. However, it is certain that Quantum Computers are another attempt by mankind to overcome physical limitations.

Literature Cited

Annenberg Learner. (2017). "Glossary." Retrieved September 23, 2017, from Annenberg Learner website: https://www.learner.org/courses/physics/glossary/glossary_alpha.html

Arikan, E. (2002, October 11). "An Information-theoretic Analysis of Grover's Algorithm." Retrieved February 20, 2017, from https://arxiv.org/abs/quant-ph/0210068

Bacon, D., & Leung, D. (2007). "Toward a World with Quantum Computers." Communications of the A.C.M., 50(9), 55-59. doi:10.1145/1284621.1284648

Dang, Derek (2016). GroversAlgorithm [Computer software]. Retrieved April 4, 2017, from https://github.com/dqdang/Grover-Algorithm

Mastin, L. (2009). "Glossary of Terms." Retrieved February 20, 2017, from http://www.physicsoftheuniverse.com/glossary.html

Gartenberg, C. (2016, October 6). "The World's Smallest Transistor is 1nm Long, Physics be Damned." Retrieved February 20, 2017, from http://www.theverge.com/circuitbreaker/2016/10/6/13187820/one-nanometer-transistor-berkeley-lab-moores-law

Gartenberg, C. (2017, January 25). "D-Wave is now shipping its new $15 million, 10-foot tall quantum computer" Retrieved

September 23, 2017, from https://www.theverge.com/circuitbreaker/2017/1/25/14390182/d-wave-q2000-quantum-computer-price-release-date

Van Meter, R. & Horsman, C. (2013). "A Blueprint for Building a Quantum Computer." Communications of the A.C.M., 56(10), 84-93. doi:10.1145/2494568.