Sally Devitry
A01980316
CS 5000 Term Paper
December 2020

An Overview of Quantum Computing

A quantum computer harnesses the power of quantum mechanics to perform computations that offer exceptionally more advanced processing power than a conventional computer. The impacts of the development of quantum computers could prove groundbreaking in various fields. Many believe that the field of quantum computing will be booming by the year 2030. Others think a useful quantum computer will never be built. This paper gives an overview of quantum computing, discussing its history, basic concepts, motivation, and challenges.

History of Quantum Computing

Quantum computing materialized as a theoretical possibility in the early 1980s when Paul Benioff, an American physicist, proposed a Turing machine operating under the laws of quantum mechanics. His model was based on the reversible Turing machine of Charles Bennett. Benioff was a pioneer in the field of quantum computing and his work is still being expanded on today.[3]

Richard Feynman, an American theoretical physicist, was another pioneer of quantum computing. Feynman was regarded as a brilliant researcher and served as a touch-source for many other great scientists because "he could argue with them." [1] Feynman built on Benioff's quantum computing ideas, putting quantum computers on a solid theoretical foundation. Feynman produced a universal quantum simulator, a quantum computer that avoids slowdown when simulating quantum phenomena. Feynman was a talented communicator, with the following quote perfectly depicting his vigor for quantum mechanics/computing: "Nature isn't classical… and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly, it's a wonderful problem, because it doesn't look so easy." [2]

Benioff and Feynman were joined by other physicists and mathematicians in researching the possibilities for quantum computers. Yoshihisa Yamamoto proposed the first physical realization of a quantum computer in 1988, using qubits and atoms to perform two-qubit operations. Several computational problems were discovered that cannot be computed by classical computers but could be by quantum computers. Peter Shor made an important stride in quantum computing in 1994 when he discovered an algorithm that can factor large integers extremely quickly, a very useful operation in cryptography. Shor's algorithm (described in detail in the *Motivation* section of this paper) sparked great interest in quantum computing [3].

In the late 1990s, companies and governments began investing in quantum computing research. The United States Department of Defense held its first workshop on quantum computing/cryptography in 1995, and companies like IBM, Google, and NIST were forming research groups dedicated to developing a useful quantum computer [3]. In 1998, the first 2-qubit quantum computer was created and demonstrated by Jonathan A. Jones and Michele Mosca at Oxford University. The system only ran for a few nanoseconds and computed nothing meaningful, but it was the first quantum computer that could be loaded with data and output a solution [4]. It demonstrated that the principles of quantum computing were physically possible.

In the 21st century, research and development in quantum computing have accelerated greatly. In 2012, John Preskill, coined the term "quantum supremacy" to describe the point where quantum computers could perform tasks that classical computers could not (ignoring whether the tasks are useful). Since then, Google has announced that they have achieved quantum supremacy after their 'Sycamore' quantum computer was able to solve a complex problem that would otherwise be impossible for a classical computer to solve in its lifetime. Google's 'Sycamore' quantum computer solved the problem in just three minutes and 20 seconds, compared to the estimated 10,000 years it would take the world's most advanced classical computer. It is argued that Google's achievement did not demonstrate quantum supremacy because the problem their machine solved was carefully chosen just for the purpose of demonstrating the quantum computer's superiority. The term "quantum advantage" is now more commonly used and is touted by quantum computing research groups often.

Tremendous strides have been made toward the creation of a feasible quantum computer that can perform meaningful computations, but there are great barriers to overcome in the field of quantum computing. [3]. The development of quantum computers became somewhat secretive as companies race to be the first to produce a useful/affordable quantum computer. Now, in 2020, many companies claim to have quantum computers, but they are still largely inaccessible [13].

Basic Concepts

The power of a quantum computer lies in its ability to generate and manipulate quantum bits, qubits. A qubit in quantum computing is equivalent to a binary bit in classical computing. Qubits are the basic unit of quantum information. A qubit system can be represented by several different physical phenomena, but simply put, a qubit can be in two states (1 or 0) simultaneously, whereas a traditional bit can be a 0 or 1, but never both simultaneously. Qubits can be represented mathematically as unit vectors in two-dimensional space as follows in Equation 1. [6]:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

where $|1\rangle$ and $|0\rangle$ are the excited state and the ground state of an electron orbiting a nucleus.

Equation 1. Mathematical representation of a qubit.

The ability of qubits to exist as a 1 or 0 at the same time is a fundamental principle of quantum computing called superposition. Simply put, superposition is when a system is defined by two different states, but the system can exist in both at the same time. A simple physical example is an electron, which has two potential quantum states: spin up and spin down. When an electron is in superposition, the spin is a complex combination of both up and down at once, and the electron is in superposition until it is measured when it adopts one state or the other. A quantum state in superposition creates a new valid quantum state and allows for complex and powerful algorithms.

Superposition is shown in a simple experiment called the double-slit experiment, performed by Urbasi Sinha. The double-slit experiment shows that photons act both as waves and as particles simultaneously. In the experiment, a light is shined through two closely spaced slits. Classical views would suggest that the light photons travel through one slit or the other, displaying two separate parallel lines of light on the other side. Instead, the light displays in alternating lines of light and dark. This experiment suggests that a single photon passes through both slits at the same time. In other words, the photon displays the concept

of superposition [5]. This experiment was a large breakthrough in quantum mechanics and an advanced understanding of superposition. A diagram of the double-slit experiment is shown below in Figure 1.

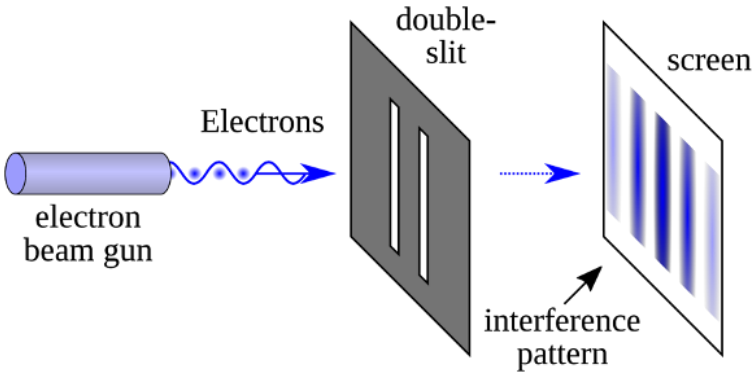

Figure 1. A diagram of the Double-slit experiment.

Entanglement, another fundamental principle of quantum computing, is when pairs of qubits are 'entangled', and the two qubits exist in a single quantum state. A change of state in one qubit will immediately result in a change of state in the other qubit. Entangled qubits are predictably dependent on one another even when separated by long distances (i.e., opposite ends of the universe!). The mystical qualities of this phenomenon inspired Albert Einstein to describe entanglement as, "spooky action at a distance." You can see a visual representation of two entangled qubits in Figure 2 below.

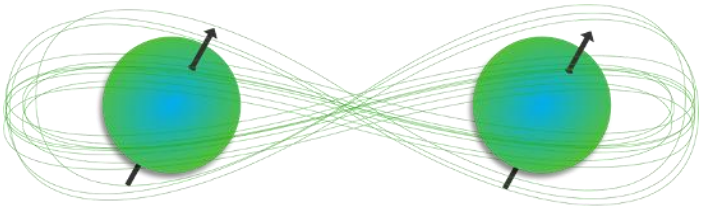

Figure 2. Two qubits displaying entanglement

Superposition and entanglement provide quantum computers with exponential speedup compared to classical computers. A classical computer deals with bits of ones and zeros, a quantum computer has the advantage of using ones, zeros, and various superpositions and entanglements of ones and zeros. The ability of a qubit to be in multiple states at once allows for large amounts of parallel processing. For example, when solving a maze, a classical computer can generally explore one path at a time, trying a new one when a dead-end is reached. Because of superposition and entanglement, a quantum computer could simultaneously explore all paths in the maze, solving this problem, and others similar to it, exponentially faster than a classical computer.

Motivation

The main motivation for developing a quantum computer is achieving tasks much faster than a classical computer. A well-known computer science principle, Moore's law, states that the number of transistors on a chip will double every two years. This prediction is becoming less accurate in the modern world of computing as transistors are becoming so small that simple physics begins to block the necessary

processes [10]. Classical computing has hit somewhat of a roadblock regarding the speed of the computers. Quantum computing, however, introduces a completely new approach that could offer superior computing speed.

Google has announced in recent years that they have a quantum computer that is 100 million times faster than a classical computer [8]. It is important to note that this speedup is only offered when performing specific computations/algorithms, but down the road, it will likely be expanded. The fast, parallel processing powers that quantum computers possess are likely to impact various fields. Fields improved by quantum computing include healthcare, energy, finance, security, and entertainment.

Recently, it has been discovered that quantum computers will be able to solve problems that are completely impossible for classical computers to solve. Computer scientists Ran Raz and Avishay Tal discovered one such problem only solvable by a quantum computer. The problem is this: two random number generators both produce a sequence of digits. The computer is tasked with deciding whether the two sequences are completely independent of each other, or are they related where one is the "Fourier transform" of the other. Raz and Tal proved that quantum computers could solve this problem, but classical computers would never reach a conclusion. This discovery introduces the powerful idea that quantum computing could solve problems that classical computers, even at their most advanced level, could not [7].

Other problems, called NP-hard problems in computer science, can technically be solved by classical computers, but they would take so long that the computation is almost useless. If quantum computing is fully realized, many NP-hard problems may be efficiently solvable. A few of these problems include:

- Traveling Salesman
- RSA encryption
- Grover's Algorithm
- Shor's Algorithm

The Traveling Salesman problem is, given a set of *n* nodes that must be included in the path, find the shortest path. To understand the difficulty of this problem, consider the following. Given *n* number of nodes, the number of possible paths that must be enumerated is (n-1)! / 2. A traditional computer takes about a microsecond to compute one path. For 20 nodes, a traditional computer would take about 2,000 years to find the most efficient path. Traditional computers can make approximations for the best path in much less time, but to find the shortest path with 0% error is effectively impossible with a traditional computer. A fully realized quantum computer, however, could offer a timely solution to the traveling salesman problem while making no approximations [9].

RSA encryption is another important problem that could be greatly affected by quantum computing. RSA encryption is practically unbreakable on the basis that a traditional computer would take a huge amount of time to decrypt the encryption. With the exponential speedup offered by quantum computers, breaking RSA encryption would be possible within a reasonable amount of time. Additionally, Shor's Algorithm is a quantum computer algorithm that can efficiently find the prime factors of a given integer, the essence of RSA decryption. This suggests a worrisome future as many current infrastructures use RSA encryption. Current estimates still give 10+ years before a quantum computer could perform this kind of computation [10].

Grover's Algorithm is an unstructured search algorithm. Unstructured means that the data being searched has no particular order. Unstructured search is often formulated concerning databases where we want to find an item that meets some criteria [11]. With classical computing, a linear number of queries must be performed but using quantum computation, the unstructured search problem can be solved in $O(\sqrt{N})$

queries. One caveat is that the quantum computation of Grover's algorithm has a small error margin. This can be combated by running the algorithm multiple times and minimizing the error to be close to nothing. This algorithm has many practical applications, and its use would prove meaningful in many fields [11].

Quantum computers cannot yet solve the above described problems or many meaningful problems at all. However, many say that it is only a matter of time until quantum computers are able to solve these problems that would prove very impactful in various fields.

Challenges

Building a quantum computer physically is very difficult. The principles of quantum mechanics mean that many components of a quantum computer are extremely small, and the quantum systems are fragile. Additionally, the conditions for a quantum computer to work are very specific as qubits only function at extremely low temperatures. Several physical platforms have been explored for building a quantum computer including superconducting systems, trapped atomic ions, and semiconductors, each of which has large flaws.

Current quantum computers have high error rates, too high for meaningful, accurate computations. Error correction requires significant redundancy in each qubit. Quantum computers are so prone to errors because of limitations caused by quantum decoherence. A quantum program must complete execution before the quantum state begins to encounter errors. For existing quantum computers, this has never exceeded one second. Error correction will be a vital piece of developing quantum computers.

The algorithms used in quantum computation will be a large hurdle in developing a usable quantum computer. It is not as simple as slightly rethinking classical algorithms because quantum computing is vastly different from classical computing. There is no supporting software or literature on coding for quantum computers. No programming constructs (integers, floats, looping, branching, etc.) exist for quantum computers, and all of these constructs will have to be developed in a space with a very high learning curve.

The high cost of quantum computers is also a large challenge in their development. The tools and conditions needed to simulate quantum systems are expensive. Last year, a single qubit cost about $10,000. At that price, a useful quantum computer would likely cost billions of dollars. There are significant hardware optimizations to be made before a usable quantum computer is feasible [12].

This paper gave an overview of the history, basic concepts, motivation, and challenges of quantum computing. It is clear that general purpose, usable quantum computers are unlikely to exist anytime soon. Researchers are consistently making meaningful strides in quantum computing, but the challenges and barriers they are faced with are daunting. The race to quantum supremacy continues; if or when it is reached, society will surely change forever.

References

[1] Selwood, Dick, and Eejournalguy says: “Richard Feynman and Quantum Computing.” *EEJournal*, 24 May 2018, www.eejournal.com/article/richard-feynman-and-quantum-computing/.

[2] Feynman, Richard P. “Simulating Physics with Computers.” *International Journal of Theoretical Physics*, vol. 21, no. 6-7, 1982, pp. 467–488., doi:10.1007/bf02650179.

[3] “Timeline of Quantum Computing and Communication.” *Wikipedia*, Wikimedia Foundation, 13 Dec. 2020, en.wikipedia.org/wiki/Timeline_of_quantum_computing_and_communication.

[4] “Quantum History in a Nutshell.” *Wrelks*, wrelks.com/quantum-computing-history.

[5] Ananthaswamy, Anil. “Classic Quantum Experiment Could Conceal Theory of Everything.” *New Scientist*, 2 Nov. 2016, www.newscientist.com/article/mg23230983-200-classic-quantum-experiment-could-conceal-theory-of-everything/.

[6] Wright, John. “Lecture 22: Quantum Computing.” *Cs.cmu.edu*, Nov. 2014, www.cs.cmu.edu/~odonnell/toolkit13/lecture22.pdf.

[7] Michael Goderbauer, Stefan George. “TR18-107.” *ECCC*, eccc.weizmann.ac.il/report/2018/107/.

[8] Griffin, Matthew, et al. “Google's New Quantum Computer Is 100 Million Times Faster than Your PC.” *311 Institute*, 25 Sept. 2018, www.311institute.com/googles-new-quantum-computer-is-100-million-times-faster-than-your-pc/.

[9] Siegel, Ethan. “This 90 Year Old Math Problem Shows Why We Need Quantum Computers.” *Forbes*, Forbes Magazine, 28 May 2020, www.forbes.com/sites/startswithabang/2020/05/28/this-90-year-old-math-problem-shows-why-we-need-quantum-computers/?sh=23c7435f1c5d.

[10] arXiv, Emerging Technology from the. “How a Quantum Computer Could Break 2048-Bit RSA Encryption in 8 Hours.” *MIT Technology Review*, MIT Technology Review, 2 Apr. 2020, www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/.

[11] “Grover's Algorithm.” *Wikipedia*, Wikimedia Foundation, 7 Dec. 2020, en.wikipedia.org/wiki/Grover's_algorithm.

[12] “Quantum Supremacy Is Coming. It Won't Change the World.” *The Guardian*, Guardian News and Media, 2 Aug. 2019, www.theguardian.com/technology/2019/aug/02/quantum-supremacy-computers.