Preston Hales

Marianne Madsen

Writing 3014

29 November 2021

Quantum Computers: Past, Present, and Future

Abstract

Computers have completely transformed society from the advent of their invention. However, with the progress of computers slowing down due to physical limitations, many look to quantum computers as the next major step in computer development. Development of quantum computing throughout the last decades as well as current developments in quantum computing seem very promising. This research review seeks to look at these developments in relation to important topics in the field of quantum computers such as their functionality, their limitations, and the differences between quantum advantage and quantum supremacy in order to gain a better understanding of what quantum computers are and what they are capable of. Certain applications of quantum computers are also discussed, especially as they relate to cryptography and machine learning. Finally, the future of quantum computing is also considered.

Introduction

Today, computers are one of the most advanced forms of technology that humans have created. They have transformed almost all aspects of society since their invention, and continue to change how various world problems are solved as computer technology continues to advance. This has been seen especially recently with the Covid-19 pandemic as many parts of human life including employment and education were shifted to being done remotely via computers and the internet, and while some things have transitioned back to how they were pre-pandemic, it is

likely that many changes from the pandemic will continue far into the future, including the greater reliance that people have upon computers. This makes continued development of computers a huge priority as our world becomes more geared to computer use. However, computer development as it relates to hardware has reached a critical point in its history. From about 1965 until now, computers have developed and gotten more powerful according to Moore's law, which essentially states that about every 1.5 to 2 years the number of transistors inside a computer would double, ultimately making it so that computers would become about twice as powerful as they were before.[1] More transistors means transistors had to get smaller by a factor of about one half about every 2 years, which has mostly held true until recently. Today, transistors can be as small as 5 nanometers; however, this is so small that quantum mechanics starts to become a serious problem, especially once they hit the threshold of about 0.3 nanometers.[1] Due to the crazy and uncertain nature of quantum mechanics, transistors of this size would no longer work as intended, meaning that we are likely witnessing the end of Moore's law. So, is this the limit of computing power? Or is there any way to continue to push computers past their limits, so as to harness the power contained within the nature of quantum mechanics that seems to prevent us from going any further? For many, it seems that the answer to these questions lies in the relatively recent development of quantum computers, computers that not only have the potential to be faster than what we have now, but that also utilize the laws of quantum mechanics.

The concept of a quantum computer is nothing new. The famous physicist Richard Feynman theorized back in 1981 and 1982 about the possibility of simulating the laws of quantum mechanics using a device that itself obeys those same laws.[1, 2] Three years later the physicist David Deutsch came up with a computational model that was the quantum equivalent

of a Universal Turing Machine (the computing model that forms the basis for modern computers today).[1] What makes the idea of a quantum computer so fascinating to many people back then and even now is that quantum computers have the potential of performing certain tasks much faster than any classical computer could ever accomplish, or even possibly accomplish tasks that a classical computer wouldn't be able to accomplish at all. This would prove to be very valuable in certain fields of computer science, including cryptography and machine learning. They also have the ability to simulate real world natural phenomena at a quantum level, meaning that they would be extremely valuable for many science disciplines including physics, biology, and medicine. The purpose of this research review is to observe and analyze the progress that has been and is currently being made towards developing quantum computers, especially in the contexts of these fields, and where this research could potentially lead to in the future.

What is Quantum Computing?

To begin, a basic understanding of what a quantum computer is and how it works is crucial. Essentially, quantum computers utilize certain principles of quantum mechanical laws in order to solve problems. One of these principles is the concept of superposition. Computers today perform calculations and store data using bits with two states of 0 or 1 depending upon whether or not a current of electrons is passing through the bit. In contrast, quantum computers use qubits ("quantum bits"), where a qubit represents a superposition of two states (like 0 and 1). Superposition "exists when the state of a particle (an electron, for example) is suspended between two physical states" as described by J. Atik and V. Jeutner.[3] This allows for a qubit to essentially exist in multiple states at the same time until its value is measured, at which point it is reduced to only one of two states. Ultimately, this enables qubits to store and process two states simultaneously, unlike a classical computer which only can store and process only one state at

any given time. Due to the fact that a qubit can represent two states, the addition of more qubits allows for exponential increase in the number of possible states that the computer can represent simultaneously (i.e. n qubits = 2^n possible states), and thus allows for great increase in computability power.[4, 5] R. Horodecki describes this feature as "quantum parallelism," which he claims "underlies the superiority of quantum computing over classical [computing]."[4] These qubits then form the basis of quantum gates, which perform logical unitary operations, which gates then make up quantum circuits in a quantum computer.

Examples and Limitations of Quantum Computing

Many have proposed various possible designs for creating quantum computers, many of which are currently being researched. For example, in the year 2000, IBM and Stanford University created the first 7 qubit quantum computer utilizing NMR (nuclear magnetic resonance).[4] Recent examples include Google's programmable 53 qubit quantum computer named Sycamore, created in 2019, and a 76 qubit quantum computer named Jiuzhang from the University of Science and Technology of China in Hefei, created in 2020, which is interferometer (or photon) based unlike Google's quantum computer, but is also not programmable like Google's quantum computer is.[4, 6] It is important to realize however that these computers are limited in the sense that they are not considered universal quantum computers, where a universal quantum computer is one that physically implements universal quantum computation. This means that universal quantum computers would be able to perform general computations among other things, and these examples mentioned above were not designed for general computations, but rather very specific computations.[6] There are in fact five criteria known as the Divincenzo criteria, offered by the physicist David DiVincenzo in the year 2000, that must be met in order to achieve universal quantum computation. While all these criteria are

very important, only the last of the five criteria will be covered here in detail in order to illustrate just how difficult it is to successfully achieve these criteria. However, the first four, quoted directly from Horodecki's paper titled "Quantum Information," are:

1. A scalable physical system with well characterized qubits.
2. The ability to initialize the state of the qubits to a simple fiducial state.
3. A "universal" set of quantum gates.
4. A qubit-specific measurement capability.[4]

The fifth of DiVincenzo's criteria, and arguably the most important of the five, has to deal with what is known as decoherence times. Many quantum computers today including Google's Sycamore computer utilize superconducting circuits maintained at very cold temperatures (practically absolute zero).[4] This cold temperature allows for longer decoherence times, meaning the states of the qubits within the computer remain independent from the environment around them for a longer time before becoming entangled with said environment (or "decoherent").[5] The issue is that these decoherence times are very short, even near absolute zero, and when the states become decoherent it can cause errors in any calculations being performed. To help counteract short decoherence times, error correction techniques have and are being researched. A relatively simple one proposed by scientist Peter Shor resembles the error correction used in classical computers which involves utilizing multiple qubits to represent a single logical qubit of information, that way if one or multiple of those qubits becomes corrupted through decoherence, then the other coherent qubits can override the decoherent ones by a majority rule.[5] Many other devised error correction techniques also use similar logic to achieve the desired result, and, according to Don Monroe in his article on quantum error correction, some of these techniques "guarantee perfect accuracy, as long as the physical error rate is below some threshold."[5]

However, in order to drop below a specified error rate threshold for these kinds of techniques, it is necessary for many qubits to be utilized to represent just one logical qubit of information. Don Monroe further paraphrases professor John Preskill of California Institute of Technology when he explains that "with current experimental error rates in multi-qubit devices somewhat below 1%, large calculations like those needed for quantum chemistry might require 1,000 physical qubits per logical qubit."[5] This means that quantum computers with a lot of qubits would be necessary for ideal error correction (this idea actually ties back to the first of DiVincenzo's criteria listed above). As demonstrated by the recent quantum computers Sycamore and Jiuzhang which utilize 53 and 76 qubits respectively, and also due to the fact that the error correction process is not completely error prone, this may be more than just a (qu)bit of a ways off into the future.

Quantum Advantage versus Quantum Supremacy

An important part of what makes quantum computers special is their potential to demonstrate what is known as quantum advantage and quantum supremacy. Arguably the one thing that makes quantum computers so attractive to many scientists and engineers is the fact that they have the potential of solving certain problems that normally would have taken an absurd amount of time on a traditional computer in only a very short time on a quantum computer; this is called quantum advantage.[3, 6] It is even possible that certain problems may only be possible to solve on a quantum computer as opposed to a traditional computer; this is called quantum supremacy.[3, 6]

One of the first instances of quantum advantage being theorized was in 1992 where the physicist David Deutsch along with Richard Jozsa showed in their paper titled "Rapid solution of problems by quantum computation" that a certain class of problems could be solved "with

certainty in exponentially less time than any classical deterministic computation" via quantum computation.[7] Since then many quantum algorithms have been proposed that can solve certain problems exponentially faster than a regular computer could solve them, including the famous Shor's algorithm discovered by Peter Shor in 1994.[10] This is huge as there is a whole field in computer science that deals solely with how long it takes to solve specific problems using classical computers known as computational complexity theory, and these problems are categorized depending on how long it takes to solve them. Assuming a problem isn't solvable in constant time, as the number of factors increases in a problem, the time it takes to solve said problem increases, and if the time increases proportional to the rate at which a polynomial increases or smaller, the problem is classified under the category known as P (the P stands for polynomial).[3] Problems that increase in time faster than a P problem are placed in another category known as NP, where the N means "non-deterministic" which means that there is no known, efficient algorithm to solve said problem (unlike the P category of problems).[3] The solution of NP problems can be confirmed correct in P time, but finding the solution to these problems takes NP time. There are even other categories of problems that take even more time such as EXP (problems where time complexity increases exponentially) and NP-Complete (essentially the hardest type of NP problems). While these hard problems may take a long time to solve on a regular computer, some of these problems have been shown to be solvable within polynomial time on quantum computers. For example, Google's quantum computer Sycamore was designed to solve a specific problem related to boson sampling, a problem that is estimated to have taken modern algorithms and supercomputers to solve in about 10,000 years, but only took Sycamore 200 seconds to solve.[4, 6, 8, 9] As impressive as that sounds, this is nothing in comparison to Jiuzhang, as this quantum computer developed about a year later in China was

also designed to solve another, likely more complicated variation of the boson sampling problem, a problem they claimed would take about 2.5 billion years to perform on a modern supercomputer, but took Jiuzhang only about 200 seconds to solve.[4, 6] To put this into perspective, the quantum computer Jiuzhang was able to solve this problem, in P time, roughly 10^14 times faster than a supercomputer, and this is a problem whose time complexity is at least as complex as NP, if not more complex. These examples of quantum advantage easily demonstrate the sheer amount of power and potential that quantum computers can have.

Despite these examples clearly showing quantum advantage at play, many seem to think that these examples actually demonstrate quantum supremacy in addition to quantum advantage. For example, at the time when Google demonstrated that their quantum computer Sycamore could solve the boson sampling problem, they themselves claimed that they had achieved quantum supremacy for the very first time.[4, 6, 8, 9] However, IBM criticized their use of the word "supremacy" according to Aaron Dalton,[8] and IBM further "countered that Google hadn't done anything special" according to Emily Conover.[9] While this seems like the usual competitive interplay between two tech giants (as Emily also points out in her article), IBM may actually have had a valid point. For one, the definition paraphrased above for quantum supremacy as given by Jeffery Atik and Valentin Jeutner in their paper and also Katarzyna Nalecz-Charkiewicz, et. al. in their paper states that quantum supremacy is defined when a quantum computer can solve a task that isn't possible to solve by a classical computer.[3, 6] However, the computations done Google's quantum computer Sycamore, and possibly by extension China's quantum computer Jiuzhang, can still be done on a regular computer. Granted it would still take supercomputers many years to finish solving them, but this doesn't necessarily warrant that these situations are examples of quantum supremacy because they are problems that