Quantum Computers & Networks: An Overview

Saif Taher, STEM High School for Boys – 6th of October

Abstract

Today's classical computers are headed to a plateau regarding performance/power increases and size decreases. Many companies are investing in quantum computers as the next generation of computers due to their vast potential. Said potential stems from their ability to exploit bizarre quantum phenomena, such as superposition and entanglement. However, the road is still long to achieve quantum computers capable of doing anything that today's supercomputers cannot. The road is riddled with design challenges that heavily limit the extent of problems quantum computers can solve. Those challenges include error correction, increasing the number of qubits, and finding more efficient ways to create the super-cooled ultra-vacuum environments necessary for the operation of supercomputers.

I. Introduction

The integrated circuit present in most of today's modern computers was first introduced in 1959. Since then, computers have been following a trend termed "Moore's Law": In 1965, computer engineer Gordon Moore observed that the number of components on integrated circuits had been roughly doubling every 1-2 years since circuits were invented. This allowed circuits to run at higher speeds and efficiencies per unit area for the same amount of power. Consequently, computers have both been shrinking in size and growing in computing power over the decades. However, the end to Moore's law is looming on the horizon as the size of components on circuits is approaching the atomic scale, which means that further increases in classical computers' power are going to be quite difficult. It's time to start developing entirely new technology that will succeed today's computers as our tool for moving forward, and quantum computers seem to be the perfect candidate [4].

Quantum computers have the potential to revolutionize science, medicine, commerce, space exploration, and countless other industries and markets. That potential lies in their ability to easily solve problems that even the most powerful of today's supercomputers struggle to tackle, such as chemical/biological simulations, machine learning, financial modeling, cybersecurity, and optimizing manufacturing and supply chains [1].

In fact, many companies are starting to heavily invest in R&D efforts towards quantum computers: Google and IBM built and tested two quantum processors in 2017 and 2018, the European Commission devoted 1 €-billion to quantum technology research and a team in China under the lead of Professor Pan Jianwei successfully established a 1200-km-long quantum connection between ground stations and satellite Micius. Furthermore, Volkswagen and Daimler are using quantum computers for simulations of the electrochemical processes in their cars' batteries in an attempt to improve their performance. Pharmaceutical companies are also using quantum computers to accelerate the development of novel drugs. Finally, airbus calculated the most fuel-efficient ascent/descent flight paths with the help of quantum computers. These were just a few examples of how quantum computers are being used today and why so many industries are interested in them. Let's take a look at the scientific principles behind the workings of these machines [1] [5].

II. How Quantum Computers Work

All “classical” computers and devices rely on the concept of 0’s and 1’s to represent data: The state of 0 means “off” and the state of 1 means “on”. Bits can only be 0 or 1 at a time, and the number of combinations that can be produced by a string of bits of length n is equal to 2^n. On the other hand, quantum computers utilize the phenomenon of superposition to massively outclass classical bits: Superposition is the ability of particles to be in two states simultaneously. Quantum computers use Qubits instead of bits to represent data. Unlike bits which can only represent one out of the 2^n possible combinations, qubits can be in a superposition of all of them. In other words, a qubit of length n represents all of the 2^n combinations at the same time, which enables solving certain classes of problems, such as optimization and search problems, at exponentially faster rates than normal computers can achieve [1] [6].

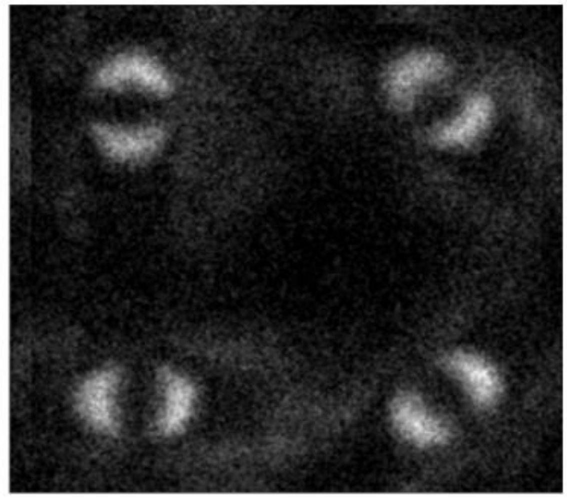

Figure #2: Photo of the first case of successful quantum entanglement between photons of light. The photo was captured in the University of Glasgow, 2019. [2]

Quantum computers make use of another phenomenon known as quantum entanglement, shown in figure #2. A pair of entangled qubits is known as an EPR pair, and they exhibit some very interesting properties. Once one of them is measured the other one collapses to the opposite quantum state of the first one, no matter how long the distance between the two qubits is (i.e., if the first qubit collapses to 0 the other one will collapse to 1, and vice versa). This non-classical behavior could be used as the first building block of a quantum internet; a network of interconnected quantum computers. Qubits could be transferred across these networks using technologies such as Quantum Key Distribution (QKD) and SuperDense Coding.

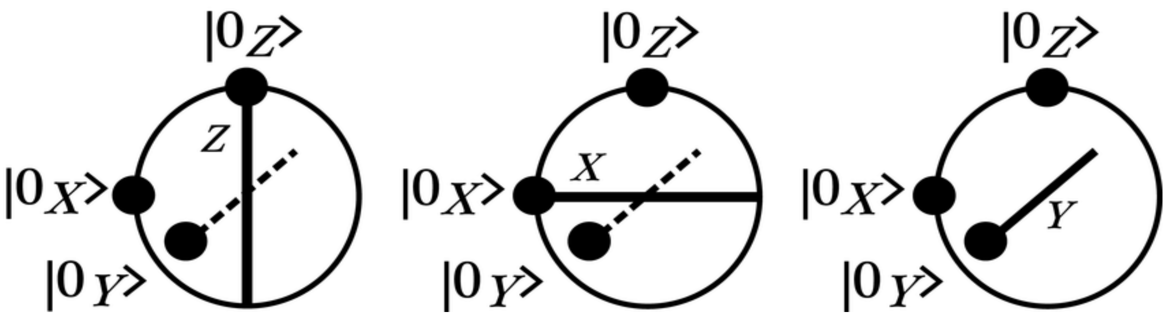

Figure #3: Three vectors representing three qubits corresponding to 0, 1, and a vector at 45° with equal amounts of both, respectively. [8]

After performing all calculations, measuring qubits will yield a probabilistic result of either 0 or 1 depending on “how much” they had of each component. In other words, 0 and 1 could be represented as two orthogonal vectors, and a qubit could be anything between them. For example, a vector at 45° represents a qubit with an equal amount of 0 and 1, as shown in figure #1. Therefore, upon measuring there is a 50/50 probability that the outcome will be 0/1. It is also worth noting that a qubit’s quantum state collapses after measuring it and that every subsequent measurement will result in the same outcome regardless of how much 0 and 1 the qubit initially had. [1]

These technologies enable exchanging secret encryption keys via photons. This allows for ultra-secure connections that are impossible to hack due to something known as decoherence (discussed in the next section). In a nutshell, quantum connections cannot be hacked because any attempt by a third party to access the qubits will alter their delicate quantum state which causes them to lose their data. [1] [3] [7]

While quantum computers may seem like a revolutionary breakthrough in informatics, the road is still very long for them to actually achieve any tangible results due to the numerous challenges facing them. We discuss some of those challenges in the next section.

III. Challenges Facing Quantum Computers

There are two main obstacles in the road to achieving quantum supremacy; that is, successfully designing and implementing a quantum computer superior to any classical supercomputer. Namely, those obstacles are noise and errors.

The quantum state of qubits is extremely fragile, which inhibits quantum computers from operating in normal environments or communicating cubits at long distances due to something known as noise. Even the slightest of changes in environmental conditions, such as temperature or pressure, is considered as noise, and interaction with noise causes errors/decoherence; i.e., qubits tend to lose their special quantum state and subsequently lose the data they carry. Therefore, although the size of quantum chips and circuits is not too large compared with their classical counterparts, it is the equipment required for preserving the qubits that take up large space and funds. This equipment includes super-cooled fridges and ultra-vacuum chambers, and it ensures qubits retain their superposition to achieve their purpose. [1]

The number of calculations that can be performed using classical bits scales linearly with the number of bits. On the other hand, the computing power of quantum computers increases exponentially with the number of qubits, which gives quantum computers their vast potential. However, at the moment it takes hundreds of thousands or millions of qubits to solve even a fundamental chemistry problem to correct all the errors arising from noise. To help with this, error-correction techniques and algorithms have been developed. However, further research is required to improve them. Not to mention that creating qubits is already quite a challenging engineering task. [1] [6]

IV. Conclusion

Quantum computers are the most promising tools at our hands if we are to explore the next frontiers of science and technology. Nevertheless, they are still very early in development, and we have barely scratched the surface of their power. More work is needed to decrease the size and costs of the equipment needed to shield qubits from noise and to find efficient ways of achieving superposition and entanglement. Current quantum computers haven't exceeded double digits in terms of qubits, and there's still a long way to go before we can accomplish anything useful with them.

V. References

[1] A. S. Cacciapuoti, M. Caleffi, F. Tafuri, F. S. Cataliotti, S. Gherardini, and G. Bianchi, "Quantum Internet: Networking Challenges in Distributed Quantum Computing," IEEE Network, vol. 34, no. 1, pp. 137–143, 2020.

[2] D. Mosher, "A 'spooky' effect of physics that Einstein couldn't believe has been photographed for the first time," Business Insider, 13-Jul-2019. [Online]. Available: https://www.businessinsider.com/quantum-entanglement-einstein-first-picture-2019-7?utm_source=quora&utm_medium=referral. [Accessed: 26-Apr-2021].

[3] J. Aron, "Quantum internet goes the distance," New Scientist, vol. 238, no. 3177, p. 13, 2018.

[4] J. M. Shalf and R. Leland, "Computing beyond Moore's Law," Computer, vol. 48, no. 12, pp. 14–23, 2015.

[5] M. Giles, "Explainer: What is a quantum computer?," MIT Technology Review, 02-Apr-2020. [Online]. Available: https://www.technologyreview.com/2019/01/29/66141/what-is-quantum-computing/. [Accessed26-Apr-2021].

[6] S. Lloyd, J. H. Shapiro, F. N. Wong, P. Kumar, S. M. Shahriar, and H. P. Yuen, "Infrastructure for the quantum

internet," ACM SIGCOMM Computer Communication Review, vol. 34, no. 5, pp. 9–20, 2004.

[7] S. Wehner, "Introduction to the Quantum Internet," RIPE Labs. [Online]. Available: https://labs.ripe.net/author/becha/introduction-to-the-quantum-internet/. [Accessed: 26-Apr-2021].

[8] L. Lizama-Pérez, J. López, E. De Carlos-López, and S. Venegas-Andraca, "Quantum Flows for Secret Key Distribution in the Presence of the Photon Number Splitting Attack," Entropy, vol. 16, no. 6, pp. 3121–3135, 2014.