Quantum Computing: A Brief Overview

Chase Mortensen

History of Quantum Computing

Although the technology to realize quantum computing has only been present for a few years and still has much room to advance, the foundational principles of quantum computing have been present for many years.

In 1927, German physicist Werner Heisenberg claimed that the more a person knows about a particle's position, the less that person is able to know about the particle's momentum [1]. This is known as the uncertainty principle and is sometimes confused with the observer effect, which states that the observation of a system affects the measurement of that system [2]. Instead, the uncertainty principle is an inherent property and not simply a result of imperfect measurement technology [3].

Another important advancement in quantum computing is the paper "Quantum Information Theory" by Roman Stanisław Ingarden which established, as the name suggests, a quantum information theory based on an abstracted version of Shannon information theory [4]. Quantum information theory differs from classical computing by using qubits instead of bits - more to come on that distinction in the following section.

At a conference in 1981, "Richard Feynman [challenged] a group of computer scientists to develop a new breed of computers based on quantum physics" and outlined a model for a quantum computer [1]. Feynman himself pioneered developments in quantum electrodynamics and quantum gravity. Around the time of his challenge, he worked towards quantum computing at Thinking Machines Corporation [5].

Peter Shor, in 1994, built on Dan Simon's algorithm from the previous year and introduced an integer factorization algorithm which theoretically performs significantly faster on a quantum computer than on a classical computer [6]. Shor's algorithm was finally executed for the first time in 2001 when IBM and Stanford factored the number 15 using a 7-qubit quantum computer [1].

In 2017, scientists simulated the Beryllium hydride molecule - the largest molecule simulated on a quantum computer at that date [1,7]. However, current classical computers are also able to simulate the molecule, so the experiment isn't a demonstration of *quantum supremacy*. Quantum supremacy is one goal of quantum computers and is to demonstrate that a quantum computer is capable of solving problems that aren't possible to solve on classical computers [8]. Simulating the Beryllium hydride molecule may actually be an example of *quantum speedup* - which essentially means that a quantum computer could perform a problem significantly faster than on traditional computers [9].

There are many companies attempting to build their own versions of quantum computers. Because different companies use different technologies, it's often difficult to compare systems and know which quantum computer is most advanced. For instance, Canadian company D-Wave uses quantum annealing, while others, such as Google and IBM use gate-based models [10]. D-Wave's latest system, the D-Wave 2000Q, has 2000 qubits [11] while Google's newest iteration ran with 53 qubits (one less than planned due to malfunction) [12] and IBM has launched its own 53-qubit system as well [13].

Each company also has its own specific goals and preferred metrics that aim to cast its quantum computing technology as the frontrunner. D-Wave's CEO claims that it aims to "put [their system] to meaningful use" [10] and is less focused on some of the more academic ventures that other companies emphasize. For example, D-Wave has used its technology to optimize bus routes in Lisbon [10]. On the other hand, Google and IBM seem to be much more focused on the academic aspect of quantum computing. In 2019, Google claimed to have achieved quantum supremacy with its 53-qubit machine [14]. The computation, it claimed "performed the target computation in 200 seconds," while the fastest

classical computer would have taken over 10,000 years to run [14]. However, IBM responded to Google's claims by casting doubt on the validity of the experiment [15]. IBM claimed:

> [...] an ideal simulation of the same task can be performed on a classical system in 2.5 days and with far greater fidelity. This is [...] a conservative, worst-case estimate, and we expect that with additional refinements the classical cost of the simulation can be further reduced [15].

D-Wave experienced a similar response when computer scientists were able to optimize algorithms for classical computers which minimized the quantum advantage [12]. Google admitted that optimizations will happen for classical algorithms and stated that they fund researchers for this purpose. However, by adding more and more qubits to their machine, Google seems to believe that the quantum breakthroughs will far surpass any classical computing optimizations [12].

So, it seems that the companies have demonstrated quantum advantage, but have yet to definitively proven quantum supremacy. As further advances are made in the field (qubits added and error decreased), it seems inevitable that quantum computers will become more and more powerful and ubiquitous.

Basic Concepts

The previous section frequently mentions *qubits* - one of the building blocks of a quantum computer. Qubits are quantum bits. Classical computers use bits (each bit is a binary 1 or 0) to represent data and perform computations. Quantum computers use qubits, which are similar to bits but behave differently. Qubits, like bits, can represent the binary 1 or 0 but also contain another state, called *superposition*. Superposition is a state where the qubit is in a proportion of the other two states [16]. A particle in a superposition state is both 0 and 1 at the same time - until you measure it. Once measured,

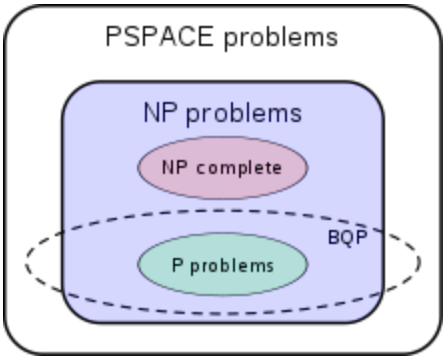
the particle collapses into one of the original states. Superposition is an important concept for quantum computers and, theoretically allows for much more powerful computation [16].

Qubits can also be *entangled;* entanglement is a property of two qubits. It is "a close connection that makes each of the qubits react to a change in the other's state instantaneously, no matter how far they are apart." So, one can infer information about a separate qubit based on the measurement of another [16].

Motivation

Quantum computing has the potential to greatly improve computing capabilities. It could allow faster computation and also enable computation of problems that were previously not computable. As mentioned above, Google claimed to have demonstrated quantum supremacy (and quantum advantage) when it performed a computation in 200 seconds that, according to Google, would have taken 10,000 years for the best classical computer to run [14]. IBM disputed this and claimed it would take a supercomputer only 2.5 days to run [15]. Even if IBM is correct, a speedup from 2.5 days to 200 seconds is enormously significant and could have a huge impact on computing.

Also mentioned above is D-Wave's bus routing algorithm. This is a practical application of the traveling salesman problem, which can run much faster on a quantum computer than on a traditional computer. However, it is unclear whether or not quantum computers will be able to solve problems currently unsolvable on traditional computers. Current classical computers can solve BPP ("bounded error, probabilistic, polynomial time") problems while quantum computers are or will be capable of solving BQP (bounded error, quantum, polynomial time") problems. While uncertain, experts theorize that BQP problems relate to P and NP problems as shown in the figure above [17]. Quantum computers



can solve problems like integer factorization and discrete log, which are not NP-complete problems. Some believe that quantum computers will be capable of solving NP-complete problems, but experts believe that to be untrue [17,18].

Even though NP-complete problems may be out of the question, quantum computers could still allow interesting and useful problems to be solved. Some examples include traveling salesman, RSA, Grover's Algorithm, and Shor's Algorithm. The traveling salesman problem has important implications in everyday life. The example above demonstrates its utility for buses, but it will be increasingly useful as self-driving cars become common. Quantum computers, combined with other technologies (such as 5G) will allow for self-driving cars to find optimal routes to avoid traffic. RSA (Rivest–Shamir–Adleman) is related to Shor's algorithm. Because quantum computers will perform these calculations (factoring the product of two large prime numbers [19] more efficiently than traditional computers, current encryption technology based on these algorithms will be easily deciphered with quantum computers. There are also other algorithms that won't grant huge advantages to quantum computers [17]. However, quantum computers will be able to encrypt data more securely than classical computers [20]. Grover's algorithm is essentially a database lookup that is optimized for quantum computation and provides significant speedup compared to classical computation [21a].

Another area of interest for quantum computing is artificial intelligence (AI). Because AI relies heavily on probabilities, quantum computers are well suited for the problem since they are probabilistic in nature rather than deterministic [21b].

Challenges and Technical Hurdles

Advancements in computing and cryptography, as described, are dependent on quantum computing technologies. Some of these challenges have been briefly mentioned in the *History of Quantum Computing* section of this paper. It goes without saying that quantum computers are much more

complex and challenging to build than classical computers. The lowest level - bits versus qubits - illustrates the increase in complexity as well as the reliance on quantum mechanics. David P. DiVincenzo outlined several important characteristics (and therefore, challenges) necessary of quantum computers:

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. Long relevant decoherence times, much longer than the gate operation time
4. A “universal” set of quantum gates
5. A qubit-specific measurement capability
6. The ability to interconvert stationary and flying qubits
7. The ability faithfully to transmit flying qubits between specified locations

As a note, 1-5 above were regarded as essential for computation while 6 and 7 regard communication for quantum computers [22].

Other challenges facing those pursuing advances in quantum computing technologies are noise and decoherence [23,24]. Google has addressed some of the errors inherent in quantum computing by creating redundant qubits that act as a single logical qubit [12] and quantum error-correcting codes [24, 25]. Some claim that the threshold theorem, which argues “that a noisy quantum computer can use quantum error-correcting codes” [24] will allow for quantum computers to advance to the level of being truly useful. Others point out that when taking error-correcting into account, the number of physical qubits necessary to represent one logical qubit could be between 1,000 and 100,000, which means that a 1,000 qubit quantum computer would require at least a million physical qubits and that it is futile to try to really tackle the error-correcting necessary for a true quantum computer [26].

Quantum decoherence is another challenge. It generally requires the qubits to be placed in vacuums, kept at temperatures near absolute zero, and the removal of nearly all magnetic fields in order to

avoid interference [17]. These challenges add significant complexity to advances to physical realizations of quantum computers.

Regardless of challenges and obstacles, companies continue to build larger and more powerful quantum computers each passing year. The current trajectory certainly indicates that quantum computing will play a significant part in computing's future and could impact everyday life, cryptography, algorithm design, and much more in the years to come.

References

[1] Research.ibm.com. What is quantum computing? - IBM Q – US [online] Available at: https://www.research.ibm.com/ibm-q/learn/what-is-quantum-computing/.

[2] Violation of Heisenberg's Measurement-Disturbance Relationship by Weak Measurements https://arxiv.org/abs/1208.0034v2

[3] Introduction to Quantum Physics; Heisenberg's uncertainty principle https://www.youtube.com/watch?v=TcmGYe39XG0

[4] Quantum Information Theory. Reports on Mathematical Physics, vol. 10, 43–72, 1976.

[5] Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer (1982) https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.45.9310

[6] Algorithms for quantum computation: discrete logarithms and factoring https://ieeexplore.ieee.org/document/365700

[7] How to measure a molecule's energy using a quantum computer https://www.ibm.com/blogs/research/2017/09/quantum-molecule/

[8] Quantum computing and the entanglement frontier https://arxiv.org/abs/1203.5813

[9] Measures of quantum computing speedup https://arxiv.org/abs/1307.7488

[10] Forget quantum supremacy: This quantum-computing milestone could be just as important https://www.zdnet.com/article/never-mind-quantum-supremacy-this-quantum-computing-milestone-could-be-just-as-important/

[11] D-Wave Announces D-Wave 2000Q Quantum Computer and First System Order https://www.dwavesys.com/press-releases/d-wave%C2%A0announces%C2%A0d-wave-2000q-quantum-computer-and-first-system-order

[12] Here's what the people who claimed Google's quantum supremacy have to say about it https://arstechnica.com/science/2019/10/inside-googles-quantum-computing-efforts/

[13] IBM will soon launch a 53-qubit quantum computer https://techcrunch.com/2019/09/18/ibm-will-soon-launch-a-53-qubit-quantum-computer/

[14] Quantum Supremacy Using a Programmable Superconducting Processor https://ai.googleblog.com/2019/10/quantum-supremacy-using-programmable.html

[15] On "Quantum Supremacy" https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/

[16] Kurzgesagt – In a Nutshell. "Quantum Computers Explained – Limits of Human Technology." https://www.youtube.com/watch?v=JhHMJCUmq28.

[17] Quantum computing https://en.wikipedia.org/wiki/Quantum_computing

[18] Quantum complexity theory (1993) https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.144.7852

[19] RSA (cryptosystem) https://en.wikipedia.org/wiki/RSA_(cryptosystem)

[20] What are quantum computers and how do they work? WIRED explains https://www.wired.co.uk/article/quantum-computing-explained

[21a] A fast quantum mechanical algorithm for database search https://arxiv.org/abs/quant-ph/9605043

[21b] Principles of Quantum Artificial Intelligence https://www.worldscientific.com/worldscibooks/10.1142/8980

[22] The Physical Implementation of Quantum Computation https://arxiv.org/abs/quant-ph/0002077

[23] How Quantum Computers Fail: Quantum Codes, Correlations in Physical Systems, and Noise Accumulation https://arxiv.org/abs/1106.0485

[24] Quantum supremacy https://en.wikipedia.org/wiki/Quantum_supremacy

[25] Error-Correcting Codes in Quantum Theory https://ui.adsabs.harvard.edu/abs/1996PhRvL..77..793S/abstract

[26] The Case Against Quantum Computing
https://spectrum.ieee.org/computing/hardware/the-case-against-quantum-computing