Quantum Computing: The Future of Computation

Luke Keely

Trinity College Dublin,
keelyl@tcd.ie

Abstract. This report covers a high-level examination of the realm of quantum computing. Beginning with a brief overview of quantum mechanical principles, then moving on to an outline of how a quantum computer functions and how this differs from a classical computer. It then looks at the history, current status, and potential future applications of quantum computing. By identifying key players in the current generation of quantum computers, we can gather insight into where this technology is heading and where it may be adopted in the early stages of its life.

Table of Contents

1 Introduction

Diving into quantum computing is like stepping into a different universe; it has its own rules that are completely different from what we are used to in classical computing. Instead of bits, we have these things called qubits. Unlike bits, which represent either a 0 or a 1, qubits may be many things at once due to the principles of quantum mechanics that they follow.

The underlying principles of quantum mechanics allow particles like electrons and photons to behave in ways that go against the conventional laws of physics. It is these underlying properties, like superposition and entanglement, that allow quantum computers to process information much better than classical computers; it is estimated that in some scenarios, problems may be solved over 100 million times faster.

In this report, we look at the basics of quantum mechanics, then a breakdown of the history of quantum computers, its current state, and potential future improvements. Many fields may be impacted as this technology advances. Cyber security and cryptography may completely change, drug discovery could be accelerated, and complex computational problems currently intractable for classical computers could be solved. This project aims to provide a brief overview of the theory of quantum computers and its real-life applications.

2 Basics of Quantum Mechanics

Quantum Mechanics is a fundamental theory in physics that governs the behavior of the smallest particles in the universe, such as atoms and subatomic particles, different from classical physics, which applies to objects on the macroscopic scale.
Below are key principles of quantum mechanics to better understand the rest of the report:

2.1 Superposition

The principle of superposition states that a quantum system can exist in multiple states at once. Mathematically, if $|A\rangle$ and $|B\rangle$ are two states of a quantum system, then a superposition is given by:

$$\alpha|A\rangle + \beta|B\rangle$$

where α and β are complex numbers. For example, an electron can spin-up and spin-down simultaneously until observed.

2.2 Entanglement

Quantum entanglement is a strange connection between particles where the state of one instantaneously influences the state of the others, regardless of distance. The state of an entangled pair is given by:

$$|\Psi\rangle = a|00\rangle + b|11\rangle$$

where a and b are complex coefficients. For example, two entangled coins; flipping one instantly dictates the outcome of the other.

2.3 Uncertainty Principle

Heisenberg's Uncertainty Principle states that you cannot simultaneously know the exact position (x) and momentum (p) of a particle. Mathematically, it's expressed as:

$$\Delta x \cdot \Delta p \geq \frac{\hbar}{2}$$

where $\hbar$ is the reduced Planck's constant.

2.4 Probability

Quantum outcomes are probabilistic, governed by the wave function Ψ, where $|\Psi|^2$ gives the probability density. It is like predicting rain likelihood but not the exact positions of the droplets.

2.5 Wave-Particle Duality

Particles exhibit wave-like and particle-like behavior based on the observational context. Shown in the double-slit experiment, where electrons show interference patterns like waves yet strike as particles.

3 How Quantum Computers Work

Quantum computers operate on the principles of quantum mechanics, which allows their algorithms to outperform classical computers. Unlike classical bits, which are either 0 or 1, the principle of superposition allows qubits to exist in both 0 and 1 states simultaneously.

Entanglement allows a connection between qubits where the state of one instantaneously influences the state of another, regardless of distance. This forms the basis for complex operations between qubits, allowing the operation of quantum gates and circuits. Quantum gates manipulate qubit states, varying their probabilities to produce different output states. These gates are the building blocks of quantum circuits and, when measured, collapse to one of the basis states, rendering the solution of the calculation.

When these principles are applied, quantum computers excel in problem-solving. Quantum algorithms can solve specific problems much more efficiently. For example, Shor's algorithm uses quantum parallelism for factorizing large numbers exponentially faster than the best classical algorithms. Moreover, quantum computers are perfect for simulating other quantum systems. This ability to simulate is essential for improving materials science, chemistry, and physics.

Similarly, quantum computers can solve complex optimization problems more efficiently. This may be done by exploring multiple solutions simultaneously using superposition and quantum interference to eliminate incorrect solutions; they can find the optimal solution in fewer steps.

In short, quantum computers use the fundamental principles of quantum mechanics to significantly improve computation capabilities and problem-solving abilities with the application of quantum gates for parallel processing and output measurement.

4 Timeline of Quantum Computing

The idea of quantum computing started in the early 1980s when theorists like Richard Feynman highlighted the issues of classical computers in simulating quantum systems. This started the discussion around quantum computation.

- **1981:** Richard Feynman proposes quantum computing to simulate quantum systems efficiently.
- **1985:** David Deutsch published a paper about quantum logic gates, the theoretical framework for quantum computing.
- **1994:** Peter Shor devises an algorithm for factoring large numbers. It is exponentially faster on a quantum computer.
- **Late 1990s:** Researchers including Isaac Chuang and Neil Gershenfeld developed elementary quantum computers with a few qubits, starting a transition from theory to practice.
- **2001:** IBM and Stanford University create a 7-qubit quantum computer, demonstrating the possibility of NMR (Nuclear Magnetic Resonance) for quantum computing.
- **2019:** Google claims ”quantum supremacy” with its Sycamore processor, solving a problem that would take a supercomputer around 10,000 years in 200 seconds.

5 Current Advances in Quantum Computing

The field of quantum computing has recently made some considerable advancements. In 2023, tech companies such as Microsoft, Google, and IBM have been working hard in this area.

Microsoft has been working on its Azure Quantum ecosystem. The goal of the project is to produce a platform for the development of quantum programs on the cloud with access to quantum libraries and resources. Microsoft is working with Toshiba to create an algorithm inspired by quantum principles that can solve complex optimization problems much quicker than classical algorithms.

Google is currently working on building fault-tolerant quantum computers. They also showcased a quantum chemistry simulation, demonstrating the potential of quantum computing for advancing material science. While their progress for 2023 is not broadly documented, it is evident that they are working towards making quantum computing more practical for real-world applications.

6 Future Advancements and Challenges

6.1 Short-term Technical Advancements

Progression in hardware, algorithms, and error correction techniques is most needed to advance quantum computing for real-world problem-solving. We may expect to see the critical development of more reliable qubits that are needed to run dependable programs. Additionally, we need to improve error correction algorithms to further reduce the effects of environmental noise, a main source of error, amongst other factors. With the increased availability of quantum development to the average user, thanks to the likes of Microsoft's quantum development kit, we will see the growth of quantum algorithms that will allow us to take full advantage of the new technology. Hybrid quantum-classical algorithms, utilizing both quantum and classical resources, will help to increase the popularity of using such technology to provide solutions to real-world problems.

6.2 Long-term Technical Advancements

As the quantum era matures, long-term hopes for the technology include fully fault-tolerant quantum computers capable of handling a wide variety of complex tasks that would be impossible for classical computers alone. Assuming development continues, we will begin to see large-scale quantum computers that have thousands or even millions of qubits. Similar to the exponential increase of transistor count on classical computer chips, predicted by Moore's law. Much like when storage transitioned from HDDs to SSDs, advancements in topological qubits would increase the stability and error resistance of quantum systems. As quantum programming becomes more popular, we will see the development of high-level languages that allow the average user to take full advantage of the computing possibilities, much like the development of languages we've seen in the past.

6.3 Short-term Applications

In the near future, we will likely see quantum computing being adopted sooner in sectors where we already see a clear advantage over classical computing. Quantum algorithms like Grover's and Shor's will significantly speed up specific tasks, such as searching unsorted databases and factoring large numbers. Google has already demonstrated that quantum computing will improve material discovery and drug design by simulating molecular interactions, an area where classical computers struggle. We will see early adoption in areas where we work with big data, for example, finance, transport and infrastructure, and AI and machine learning.

6.4 Long-term Applications

As quantum technology grows, it will enter healthcare, being used for drug discovery, genetic research, and personalized medicine. In finance, it may majorly impact market analysis and financial modeling. We may see big jumps in the capability of artificial intelligence with the ability to train models faster and improved optimization algorithms.

6.5 Negative Impacts

However, this is not all without consequences. Quantum algorithms, such as Shor's, used to factorize large numbers, have the potential to crack current encryption standards, leaving sensitive data much more vulnerable to attack. Even now, we see cybercriminals gathering encrypted data in hopes they will have the computing power to decrypt it in the next five to ten years, giving them access to personal information such as bank details and passwords. Quantum computers are very expensive and require a high level of skill to operate. This may make the digital divide worse, giving the benefits of quantum computing to a small sample of people who already have lots of money and technical ability. The increased computing power coming with these systems causes some ethical concerns. The ability to process huge amounts of data would enable levels of mass prevalence magnitudes higher and restrict personal privacy.

7 Conclusion

Quantum computing has the potential to revolutionize how we deal with big data by solving complex problems that would be impossible with classical algorithms. From its theoretical formulation in the 1980s to the applied progressions we have today, with continued progress and great innovation, it will have a significant impact in many sectors, much like the adoption of classical computers before it.

Domains, including scientific research, healthcare, machine learning, and cyber security, will likely see significant changes, some good and some bad. We must harness this technology carefully due to the ethical implications. However, it is undoubtedly interesting to witness the quantum reality unfolding before us.

References

1. Wikipedia, *Quantum mechanics*, Link.
2. Wikipedia, *Quantum entanglement*, Link.
3. Wikipedia, *Uncertainty principle*, Link.
4. Wikipedia, *Quantum foundations*, Link.
5. Wikipedia, *Quantum computing*, Link.
6. Wikipedia, *Timeline of quantum computing and communication*, Link.
7. Microsoft Azure, *Quantum Ecosystem*, Link.
8. Quantum Insider, *Google Quantum Computing Advancements 2023*, Link.
9. IBM, *Quantum Computing*, Link.