MSE802 Assessment 1

270700435

June 2025

1 Introduction

Quantum computing is an emerging field that leverages the principles of quantum mechanics to process information in fundamentally new ways. Unlike classical computing, which relies on binary bits, quantum computing uses qubits that can exist in multiple states simultaneously. This report explores the essential concepts of quantum mechanics as they relate to quantum computation, major quantum algorithms, their real-world applications, current hardware technologies, and the future outlook for this rapidly developing field.

2 Task 1: Research and Explain Quantum Principles

Quantum mechanics provides the scientific foundation for quantum computing. While classical physics is deterministic and based on continuous variables, quantum mechanics introduces several unique principles:

- **Probabilistic Nature:** Quantum outcomes are fundamentally probabilistic.
- **Discrete States:** Quantum systems occupy discrete, quantized energy levels.
- **Wave-Particle Duality:** Quantum entities display both wave-like and particle-like behavior.

Among these, three concepts are especially crucial for quantum computation: superposition, entanglement, and quantum gates.

2.1 Basic Principles of Quantum Mechanics

2.1.1 Superposition

Quantum systems can exist in a superposition of states. For example, a qubit can represent both 0 and 1 simultaneously until measured. This is expressed as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

where α and β are complex amplitudes. These coefficients must satisfy the normalization condition $|\alpha|^2 + |\beta|^2 = 1$, ensuring that the total probability of measuring the qubit in either state is one. The phenomenon of superposition not only reflects the wave-particle duality of quantum systems but is also a fundamental aspect of quantum mechanics and quantum computation (Nielsen & Chuang, 2010).

2.1.2 Entanglement

Entanglement links the states of two or more qubits such that the state of one instantly affects the state of the other, regardless of distance. A famous example is the Bell state:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Entanglement enables nonlocal correlations, which are crucial for quantum communication protocols such as quantum key distribution and provide the foundation for quantum speedup in distributed quantum computing (Nielsen & Chuang, 2010).

2.1.3 Quantum Gates

Quantum gates perform operations on qubits, creating superpositions and entangled states. The Hadamard gate (H) transforms a classical basis state into an equal superposition, and the CNOT gate performs a conditional flip of a target qubit based on the control qubit, enabling the creation of entanglement and complex quantum logic circuits. Quantum gates are generally reversible and based on unitary transformations, in contrast to many classical logic gates (Nielsen & Chuang, 2010).

2.2 Qubits vs Classical Bits

Classical bits and quantum bits (qubits) represent and process information in fundamentally different ways. While classical bits can only be in one of two definite states (0 or 1), qubits can exist in a superposition of both states, enabling quantum computers to handle information much more efficiently for certain tasks. Furthermore, qubits can be entangled, allowing for nonlocal correlations between particles—a phenomenon not present in classical systems.

The manipulation of qubits using quantum gates allows quantum computers to perform parallel computations, vastly increasing computational power for specific problems compared to classical computers (Nielsen & Chuang, 2010).

The following table summarizes the key differences between classical bits and qubits:

Property	**Classical Bit (Bit)**	**Quantum Bit (Qubit)**
State Representation	Only 0 or 1 (definite)	Superposition of 0 and 1 ($\|\psi\rangle = \alpha\|0\rangle + \beta\|1\rangle$)
Information Capacity	n bits represent n binary values	n qubits represent 2^n superposed states, enabling parallel computation
Correlation	Independent, no nonlocal effect	Nonlocal entanglement through quantum correlations
Logic Operations	Irreversible (AND, OR, NOT)	Reversible quantum gates (Hadamard, CNOT), based on unitary transformations
Physical Implementation	Semiconductor devices (CPU, GPU)	Superconducting circuits, trapped ions, photons, etc.
Measurement	Direct deterministic readout	Probabilistic, requires repeated measurements for statistics

Table 1: Comparison between classical bits and quantum bits

As shown in the table above, qubits possess unique properties such as superposition and entanglement, allowing quantum computers to solve certain problems much more efficiently than classical computers (Nielsen & Chuang, 2010).

3 Task 2: Investigate Quantum Algorithms

3.1 Chosen Algorithm: [Grover's Algorithm]

4 Functioning and Mathematical Basis

Grover's algorithm provides a quadratic speedup for searching an unstructured database of $N = 2^n$ items (Grover, 1996; Nielsen & Chuang, 2010). The key is to amplify the amplitude of the marked state by repeatedly applying two quantum operations: the Oracle and the Diffusion operator.

4.0.1 Overview and Algorithm Steps

Pseudocode:

```
Grover_Search(f, n):
    Initialize n-qubit state |0⟩
    Apply Hadamard gates
    repeat R times:
        Oracle (mark solution)
        Diffusion operator
    Measure and return result
```

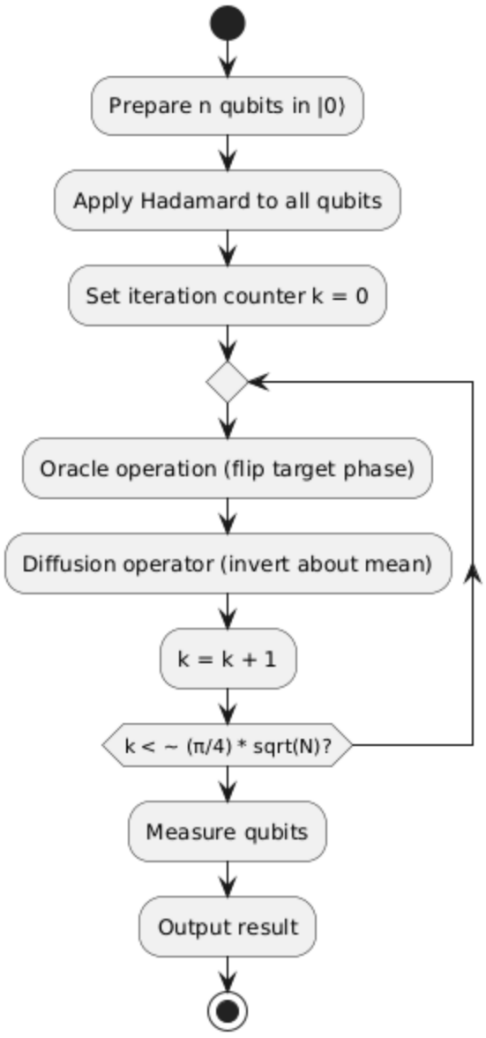

Figure 1: Flowchart of Grover's Algorithm. $R \approx \frac{\pi}{4}\sqrt{N}$ is based on Nielsen and Chuang (2010, p. 254).

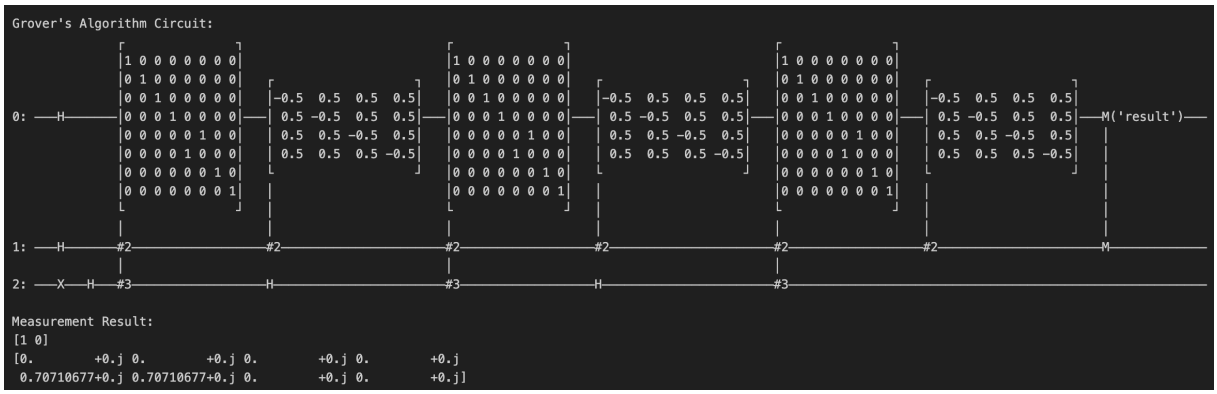

Figure 2: Quantum circuit for Grover's algorithm: Initial Hadamard, repeated Oracle and Diffusion, and final measurement.

4.0.2 Mathematical Basis and Geometric Interpretation

Grover's algorithm begins by preparing n qubits in the $|0\rangle$ state and applying Hadamard gates to create a uniform superposition:

$$|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

This initial state lies in a two-dimensional subspace spanned by the equal superposition of all non-solution states ($|\alpha\rangle$) and the marked state ($|\beta\rangle$) (Nielsen & Chuang, 2010, Sec. 6.1.3).
The algorithm then repeatedly applies the Grover iteration, consisting of:

- **Oracle (U_f):** Flips the phase of the marked state:

$$U_f|x\rangle = \begin{cases} -|x\rangle, & \text{if } x = x_0 \\ |x\rangle, & \text{if } x \neq x_0 \end{cases}$$

- **Diffusion Operator (D):** Reflects all amplitudes about the average:

$$D = 2|\psi_0\rangle\langle\psi_0| - I$$

Each Grover iteration (oracle plus diffusion) acts as a rotation by angle θ in this two-dimensional space, incrementally amplifying the amplitude of the marked state. After k iterations, the quantum state is:

$$|\psi_k\rangle = \cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle$$

where $\sin(\theta/2) = 1/\sqrt{N}$ for a single solution. The optimal number of iterations is $R \approx \frac{\pi}{4}\sqrt{N}$ (Nielsen & Chuang, 2010, p. 254), maximizing the probability of measuring the marked item.
This geometric perspective is visualized in Figure 6.3 of Nielsen and Chuang (2010), where each iteration brings the state vector closer to the solution by a fixed angle. The amplitude amplification mechanism illustrated here is the key to Grover's quadratic speedup (Nielsen & Chuang, 2010, Fig. 6.3).

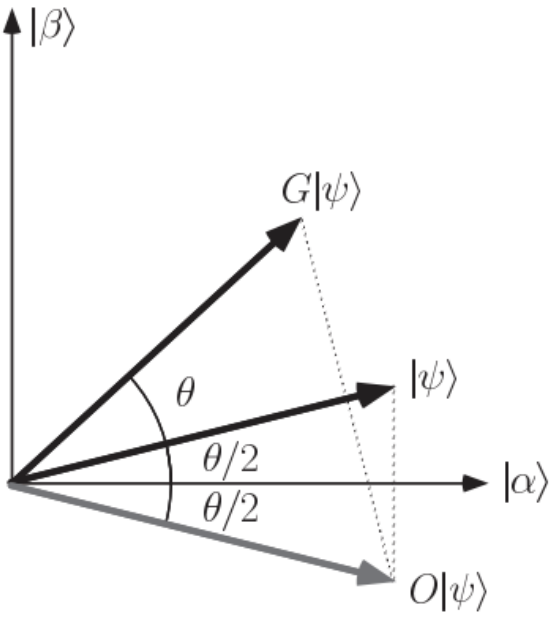

Figure 3: Geometric visualization of Grover's algorithm as a sequence of 2D rotations in the Hilbert space, adapted from Nielsen and Chuang (2010, Fig. 6.3).

4.0.3 Comparison with Classical Algorithms

Classical search in an unstructured database requires checking each entry one at a time, so the process takes $O(N)$ steps. Grover's quantum algorithm, however, can find the target in just $O(\sqrt{N})$ steps—much faster for large databases (Nielsen & Chuang, 2010, p. 248).
This quadratic speedup doesn't just look good on paper; it's also been proven to be the best possible for this type of problem (Brassard et al., 2002; Montanaro, 2016). In other words, no quantum algorithm can do better for unstructured search. Grover's approach is a textbook example of how quantum principles like superposition and interference can outperform classical brute-force methods, even if it's not an exponential leap.

> "Grover's search algorithm provides a quadratic improvement over classical exhaustive search, but this is provably the best possible for general unstructured search problems." (Montanaro, 2016)

5 Task 3: Algorithm Application and Technologies

5.1 Real-World Problem Addressed

In practice, Grover's algorithm has been experimentally implemented on real quantum hardware, such as IBM's quantum computers (Mandviwalla et al., 2018). These experiments show that quantum search can accurately solve simple unstructured search problems involving a small number of items (e.g., 4 qubits, up to 16 entries). However, due to current hardware limitations—such as noise and error rates—the practical advantage is only observable for very small datasets. Mandviwalla et al. also highlight that the performance of Grover's algorithm depends significantly on the choice of qubits and device configuration. Thus, while Grover's algorithm demonstrates a clear quantum advantage in principle, its real-world application awaits further advancements in quantum hardware.

5.2 Quantum Computing Advantages

Grover's algorithm exemplifies how quantum computing leverages superposition and quantum parallelism to accelerate the search for a marked item in an unstructured dataset. Unlike classical computers—which must check each candidate sequentially—quantum computers can process all possible candidates in parallel within a single quantum state, updating the amplitudes through constructive interference to "amplify" the probability of the correct solution.

This mechanism enables Grover's algorithm to solve the unstructured search problem using only $O(\sqrt{N})$ queries, compared to $O(N)$ classically—a quadratic speedup that remains optimal for this task (Brassard et al., 2002; Nielsen & Chuang, 2010). In practical terms, this means that searching a database of one million entries would require only about one thousand quantum queries, rather than one million classical queries.

Real-world quantum hardware is beginning to demonstrate these advantages. For example, IBM Q and Google Sycamore are cloud-accessible quantum computers that can already implement small-scale versions of Grover's algorithm. Mandviwalla et al. (Mandviwalla et al., 2018) showed that IBM's quantum processors can reliably solve simple search problems using Grover's algorithm, verifying the theoretical speedup for datasets up to 16 entries (4 qubits). Although current machines are limited by noise and decoherence, these experiments confirm the practical feasibility of quantum-accelerated search on real hardware.

As quantum technology matures—with improvements in qubit quality, error correction, and scaling—the practical impact of Grover's algorithm and similar quantum search techniques will continue to grow, potentially enabling dramatic improvements in fields ranging from cybersecurity (e.g., cryptanalysis) to large-scale data mining.

5.3 Quantum Hardware Implementations

What do mainstream quantum computers look like, and how do they compare?

Currently, the leading types of quantum computers can be roughly grouped into three "models":

1. Superconducting Qubits (like chips in a fridge): Represented by IBM and Google's quantum computers Arute et al., 2019; IBM, 2024. These machines look like chips inside giant "refrigerators," as qubits must operate at extremely low temperatures (close to absolute zero) to remain stable. - **Pros:** Very fast, suitable for large-scale and rapid computational tasks such as searching and complex optimization. - **Cons:** Extremely sensitive to the environment—if the temperature rises or there's a bit of vibration, the quantum state collapses (decoherence). Their operational time is extremely short, like "fragile glass."

2. Trapped Ion Qubits (like an electronic bug catcher): Represented by companies such as IonQ IonQ, 2024. These systems use electromagnetic fields to "trap" a line of charged ions, then manipulate them one by one with lasers. - **Pros:** More "robust" than superconducting qubits, maintaining their quantum state for longer and being less affected by environmental factors. - **Cons:** Operations are complex and require precise control—like playing piano with lasers on each ion. It's hard to scale up to very large numbers of qubits Monroe and Kim, 2013.

3. Other Types (such as photonic qubits): There are also schemes that use photons as qubits Wang et al., 2020, but these are still in the experimental stage and far from widespread use.

Comparison Summary:

- **Superconducting qubits:** Fast, but fragile.
- **Trapped ion qubits:** Robust, but hard to scale.

- **Other new qubits:** Potential is huge, but still in the lab.

5.4 Challenges and Limitations

Why hasn't quantum computing become mainstream yet? The main obstacles are:
1. Qubits are Too Fragile (Decoherence): Qubits are like acrobats walking a tightrope—any environmental disturbance (temperature change, noise, etc.) can make them "fall," collapsing from being both 0 and 1 to a definite state (decoherence). For example, a superconducting qubit may decohere in a microsecond, so calculations must be finished extremely fast, or results are lost Arute et al., 2019; Preskill, 2018.
2. Error Correction is Very Costly: Qubits are error-prone. To ensure reliable results, many "backup" qubits are needed for error correction. Current technology may require 1,000 physical qubits for every 1 effective logical qubit Preskill, 2018; Wendin, 2017, but today's machines have only tens to a few hundred qubits—not nearly enough for practical applications.
3. Poor Scalability: Both superconducting and trapped ion machines can make "small machines," but scaling to thousands or millions of qubits is technically challenging and expensive, and no clear path exists yet for mass production Monroe and Kim, 2013; Preskill, 2018.
4. Limited Application Scenarios: Quantum computers are only significantly better at specific tasks, such as search, factoring large numbers, or certain optimization problems. For daily arithmetic and office computing, classical computers are still more efficient Wendin, 2017.

6 Task 4: Future Outlook

6.1 Expected Developments in Quantum Computing

In the coming years, we can expect significant progress in quantum computing technology, both in hardware and software. On the hardware side, researchers are working on building more stable and scalable qubits, extending coherence times, and developing better error correction techniques. On the software side, new quantum algorithms and improved programming frameworks are being created to unlock the potential of quantum devices. While many technical challenges remain—especially regarding qubit fragility and error correction—ongoing research is steadily moving the field forward. Experts believe that it may still take 10 to 20 years, or even longer, before large-scale, fault-tolerant quantum computers become widely available Preskill, 2018; Wendin, 2017.

6.2 Long-Term Applications and Industry Impact

If these challenges can be overcome, quantum computing could dramatically change several industries:

- **Drug Discovery:** Quantum computers can quickly search for molecules that are effective in treating diseases, speeding up the process by dozens of times compared to today's methods.

- **Weather Forecasting:** With the ability to simulate atmospheric dynamics more precisely, quantum computers could predict extreme weather events weeks in advance, helping communities better prepare.

- **Cryptography and Secure Communication:** Quantum entanglement can enable "absolutely secure" encryption—making it impossible for hackers to steal information without detection.
- **Materials Science and Optimization:** Quantum algorithms could revolutionize how we design new materials or optimize large systems, with applications in energy, transportation, and manufacturing.

However, all these breakthroughs depend on solving the fundamental problems of fragile qubits and high error rates. Until then, most quantum computers will remain in the lab, working on relatively small or specialized problems.
In summary: Quantum computing is like a "genius teenager"—it has incredible potential for certain tasks (such as searching for solutions at unprecedented speed), but it is still immature, fragile, and small-scale. Scientists worldwide are working to help quantum computers "grow up stronger." In the future, quantum computing could reshape entire industries, but for now, it is still in its "developmental phase."

7 References

References

Arute, F., Arya, K., Babbush, R., et al. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, *574*(7779), 505–510.

Brassard, G., Høyer, P., Mosca, M., & Tapp, A. (2002). Quantum amplitude amplification and estimation. *Contemporary Mathematics*, *305*, 53–74.

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 212–219.

IBM. (2024). *Ibm quantum computing* [Accessed: 2024-06-11]. https://www.ibm.com/quantum-computing/

IonQ. (2024). *Ionq* [Accessed: 2024-06-11]. https://ionq.com/

Mandviwalla, A., Ohshiro, K., & Ji, B. (2018). Implementing grover's algorithm on the ibm quantum computers. *2018 IEEE International Conference on Big Data (Big Data)*, 2537–2543.

Monroe, C., & Kim, J. (2013). Scaling the ion trap quantum processor. *Science*, *339*(6124), 1164–1169.

Montanaro, A. (2016). Quantum algorithms: An overview. *npj Quantum Information*, *2*(1), 1–8.

Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information* (10th Anniversary Edition). Cambridge University Press.

Preskill, J. (2018). Quantum computing in the nisq era and beyond. *Quantum*, *2*, 79.

Wang, J., Paesani, S., Ding, Y., et al. (2020). Integrated photonic quantum technologies. *Nature Photonics*, *14*(5), 273–284.

Wendin, G. (2017). Quantum information processing with superconducting circuits: A review. *Reports on Progress in Physics*, *80*(10), 106001.