

QUANTUM SEARCH AND CLASSICAL SEARCH

By

Ayush Raj Sethi

Submitted to the Department of Computer Science
BACHELOR OF SCIENCE IN COMPUTER SCIENCE
at the
RAJENDRA UNIVERSITY, BALANGIR
2025

AAKASH PADHUCHU BELE BHAL AE JANMI MC

ABSTRACT

Quantum search represents one of the most influential breakthroughs in quantum algorithm design, offering a provable quadratic speedup over classical unstructured search. This thesis undertakes a comprehensive theoretical and experimental investigation of both classical and quantum search paradigms, focusing on Grover's Algorithm as the primary quantum model and linear search as the classical baseline. It explores the underlying mathematical foundations, circuit architecture, amplitude amplification dynamics, and the algorithm's convergence behaviour.

Unlike classical search, which requires an average of $N/2$ comparisons to locate a target in an unsorted dataset of size N , Grover's Algorithm exploits quantum superposition and interference to reduce the search time to $O(\sqrt{N})$. This acceleration is driven by the iterative application of two core operators: (1) the oracle, which marks the target by inverting its phase, and (2) the diffusion operator, which amplifies the probability amplitude of the marked state. A geometric interpretation reveals that each Grover iteration rotates the quantum state vector toward the target state within a two-dimensional Hilbert subspace.

To evaluate the algorithm's behaviour in practical environments, the study implements full quantum circuits using Qiskit's AerSimulator. Experiments analyse probability distributions, iteration counts, and measurement convergence across datasets ranging from 2 to 256 elements, comparing these outcomes with classical search performance. Additionally, the work presents detailed quantum circuit diagrams, benchmark graphs, and complete code listings.

The findings confirm consistency between theoretical predictions and simulation results: amplitude amplification occurs predictably, success probability increases sharply after successive iterations, and the number of required operations aligns closely with the theoretical $\pi/4\sqrt{N}$ bound. The thesis concludes by discussing limitations arising from classical simulation, lack of noise, and hardware constraints, while emphasizing the significance of Grover's Algorithm as an early demonstration of quantum advantage.

Chapter 1 — Introduction

The rapid growth of data generation in modern computational systems has highlighted the need for more efficient search algorithms capable of handling large unstructured datasets. Classical search methods, such as linear search, are limited fundamentally by their sequential nature, requiring $O(N)$ time to locate a target element. This constraint becomes increasingly restrictive as datasets scale into millions or billions of entries. In contrast, quantum computing introduces a profoundly different computational paradigm that enables a dramatic reduction in search time through the exploitation of quantum mechanical principles.

Grover's Algorithm, introduced in 1996, stands as one of the most celebrated demonstrations of quantum computational advantage. Although not exponential like Shor's factoring algorithm, Grover's quadratic speedup is optimal for unstructured search problems. It provides a clear and mathematically provable improvement over classical techniques, making it a critical algorithm in understanding the practical potential of quantum computing.

1.1 Motivation for Research

The motivation behind investigating quantum search stems from current trends in computation: exponential data growth, increasing algorithmic complexity, and diminishing returns in classical hardware scaling. Quantum systems, with their inherent ability to represent and process multiple states simultaneously, offer a compelling approach for future-proof algorithm design. By studying Grover's Algorithm in detail—mathematically, architecturally, and experimentally—this thesis aims to provide foundational insights relevant to students and researchers in the field of quantum information science.

1.2 Research Objectives

The primary objective of this research is to perform a rigorous comparative analysis of classical linear search and Grover's Quantum Search Algorithm from theoretical, architectural, and experimental viewpoints. The study aims to bridge the gap between high-level algorithmic descriptions and practical implementations using modern quantum simulation frameworks. To achieve this overarching goal, the following specific research objectives are defined:

1. **Formulate a detailed mathematical foundation** for Grover's Algorithm, including amplitude amplification, oracle construction, diffusion operator analysis, and geometric rotation interpretation within a reduced Hilbert subspace.
2. **Develop complete quantum circuit implementations** using Qiskit, incorporating multi-controlled gates, oracle logic synthesis, and amplitude amplification blocks aligned with theoretical constructs.
3. **Implement classical linear search algorithms** as a computational baseline, enabling a controlled comparison between classical $O(N)$ and quantum $O(\sqrt{N})$ runtimes.

4. **Design and execute comprehensive simulation experiments**, evaluating probability distributions, iteration behaviour, measurement convergence, and circuit-level performance across increasing problem sizes.
5. **Analyse benchmark results quantitatively**, comparing classical steps, quantum iterations, theoretical speedup factors, and success probabilities under ideal simulation conditions.
6. **Identify limitations and constraints** inherent in classical simulation of quantum algorithms, including scalability bottlenecks, gate depth restrictions, and the absence of decoherence effects.
7. **Provide reproducible appendices and circuit schematics** that allow future researchers to extend or replicate the study.

1.3 Structure of the Thesis

To maintain clarity and coherence, the thesis is organized into the following major chapters:

- **Chapter 2:** Provides foundational quantum computing concepts.
- **Chapter 3:** Derives the mathematical framework of Grover's Algorithm.
- **Chapter 4:** Discusses classical search and computational constraints.
- **Chapter 5:** Presents quantum circuit architecture and component design.
- **Chapter 6:** Details the simulation environment and experimental setup.
- **Chapter 7:** Evaluates results with probability graphs and benchmark tables.
- **Chapter 8:** Discusses implications, limitations, and theoretical considerations.
- **Chapter 9:** Summarizes findings and outlines future research directions.

1.4 Scope and Limitations

This study focuses specifically on unstructured search problems and idealized quantum conditions. Real quantum hardware introduces noise, decoherence, and limited qubit connectivity—factors not present in classical simulations. Therefore, the presented results should be viewed as theoretical upper bounds on Grover's performance. Expanding beyond these bounds requires specialized hardware or error-corrected quantum systems, which remain in early development.

Chapter 2 — Background

Quantum computing is fundamentally rooted in the mathematical formalism of linear algebra and the physical principles of quantum mechanics. Unlike classical bits that assume definite binary values from the set {0,1}, quantum bits (qubits) inhabit a continuous state space defined over complex amplitudes. A single qubit can be expressed as a vector in a two-dimensional Hilbert space:

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

where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$

This representation allows for *superposition*, one of the foundational phenomena enabling quantum algorithms to outperform classical ones. When extended to n qubits, the state space grows exponentially to 2^n dimensions, enabling simultaneous representation of all computational basis states.

Another key property is *entanglement*, a non-classical correlation between qubits that permits global transformations without independent manipulation of individual subsystems. Entanglement enables powerful algorithmic constructs such as quantum teleportation, Shor's factoring algorithm, and key components of Grover's search.

Quantum computation proceeds through *unitary evolution*, where transformations are applied through quantum gates represented by unitary matrices ($U^\dagger U = I$). Unlike classical logic gates that may destroy information, unitary operations are reversible, requiring careful circuit planning. Measurement collapses superpositions into classical outcomes, introducing probabilistic behaviour into computations.

Quantum algorithms gain efficiency by structuring these phenomena into constructive interference patterns, routing amplitude toward correct solutions while diminishing amplitude elsewhere. Grover's algorithm stands as the most elegant demonstration of this principle.

Chapter 3 — Quantum Computing Foundations

Quantum computing is built upon a mathematical and physical framework fundamentally different from classical computation. While classical information is encoded using binary states that exist in distinct and well-defined positions, quantum information is encoded in quantum states that can exist in superpositions, evolve through unitary transformations, and exhibit non-classical correlations such as entanglement. These properties enable quantum algorithms to achieve breakthroughs in computational speed and efficiency that are impossible in classical models.

This chapter presents a thoroughly expanded and academically rigorous treatment of the core principles underlying quantum computation. These foundations are essential for understanding the mechanisms that make Grover's Algorithm possible, including superposition, quantum interference, reversible computation, and measurement theory.

3.1 Quantum States and Hilbert Spaces

At the mathematical core of quantum computing lies the **Hilbert space**, a complete complex vector space equipped with an inner product. Each quantum system is represented as a vector in this space, and operations on quantum systems correspond to linear transformations that preserve vector norms.

A single qubit lives in a 2-dimensional Hilbert space \mathcal{H}_2 , and its state is expressed as:

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

Where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$

The coefficients α and β are called **probability amplitudes**, and their squared magnitudes represent the probabilities of obtaining $|0\rangle$ or $|1\rangle$ upon measurement.

When multiple qubits are combined, the Hilbert space expands via the **tensor product**. For example, two qubits inhabit the space:

$$\mathcal{H}_2 \otimes \mathcal{H}_2 = \mathcal{H}_4$$

which contains four basis vectors: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.

Thus, an n -qubit system resides in a 2^n -dimensional Hilbert space. This exponential growth underpins the immense representational power of quantum systems.

3.2 Multi-Qubit Systems and Tensor Products

The state of an n-qubit quantum system is described by the tensor product of the individual qubit states. For qubits in states $|\psi_1\rangle$ and $|\psi_2\rangle$, the joint state is:

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$$

However, quantum systems are not limited to separable states. Many multi-qubit states cannot be decomposed into a tensor product of individual qubit states. These are called **entangled states**, and they reflect correlations that have no classical analogy.

An example of a highly entangled two-qubit state is the Bell state:

$$|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}.$$

Entanglement plays a central role in quantum communication, error correction, and parts of quantum computation.

3.3 Unitary Evolution and Quantum Gates

In quantum computing, allowed operations correspond to **unitary transformations**, which preserve the norm of quantum states. A unitary operator U satisfies:

$$U^\dagger U = I.$$

Some fundamental single-qubit unitary operations include:

- **Pauli-X Gate (NOT):** flips $|0\rangle \leftrightarrow |1\rangle$.
- **Hadamard Gate (H):** creates superposition states.
- **Phase Gates (S, T):** introduce controlled phase shifts.

Multi-qubit operations include:

- **CNOT Gate:** introduces entanglement.
- **CCX / Toffoli Gate:** used in oracle construction.
- **MCX (multi-controlled X):** extends control beyond two qubits.

Unitary operations are reversible, unlike most classical logic gates. This reversibility has profound implications for quantum circuit design and ensures that quantum evolution preserves probabilistic consistency.

3.4 Superposition: Parallel Representation of Information

One of the most important properties of quantum systems is superposition, enabling a qubit to represent **both** classical states simultaneously.

A single qubit in superposition has the form:

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

When extended to n qubits, superposition allows a single quantum system to represent all 2^n classical states in parallel. For example, applying Hadamard gates to each qubit produces the uniform superposition:

$$|\psi_0\rangle = (1/\sqrt{N}) \sum_x |x\rangle$$

Where $N=2^n$.

This forms the starting point of Grover's Algorithm.

3.5 Quantum Interference: Constructive and Destructive Dynamics

Quantum amplitudes behave like waves. When multiple computational paths lead to the same outcome, their amplitudes combine according to the rules of complex arithmetic. This enables two fundamental effects:

Constructive Interference

Amplitudes reinforce each other, increasing the probability of a desired outcome.

Destructive Interference

Amplitudes cancel out, decreasing the probability of undesired outcomes.

Grover's Algorithm is built entirely upon a carefully engineered interference pattern that repeatedly strengthens the amplitude of the marked state while diminishing the others.

3.6 Measurement and Probabilistic Collapse

Quantum measurement is irreversible and transforms a quantum state into a classical outcome. Measuring a qubit in state:

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

yields:

- $|0\rangle$ with probability $|\alpha|^2$
- $|1\rangle$ with probability $|\beta|^2$

In multi-qubit states, measurement may also break entanglement and collapse the entire joint wavefunction.

Grover's Algorithm delays measurement until the final step; doing so preserves the delicate amplitude relationships required for successful interference.

3.7 Significance of These Principles for Grover's Algorithm

Each of the principles in this chapter plays a key role in Grover's Algorithm:

- **Hilbert space and superposition** allow simultaneous representation of all candidate states.
- **Unitary operators** enable reversible amplitude manipulation.
- **Interference** amplifies the marked state's probability.
- **Measurement** extracts the solution at the end.
- **Entanglement** may arise depending on oracle implementation.

Grover's Algorithm functions not by searching in a classical sense, but by reshaping the probability landscape so that the marked state becomes overwhelmingly more likely upon measurement.

These foundations naturally lead into the mathematical structure of the search algorithm, discussed in detail in the next chapter.