Exploring the Possibilities Through Quantum Computing

Malaya Jove, Buruk Yimesgen
Advisor: Dr. Ryan Card

August 25, 2026

Abstract

Quantum computing is a developing technology that has the potential to change several aspects of computing as we know it. In this paper, we introduce several essential components of quantum computing such as qubits, superposition, and entanglement. In addition, we discuss two examples of quantum computing: quantum teleportation and Grover's Algorithm. Our coverage of quantum teleportation provides an example of a property of quantum computing that is impossible using classical computing. In addition to this property, we cover Grover's Algorithm which is a key advancement in quantum computing, providing quadratic speedup for unstructured search problems compared to classical algorithms. We explain the algorithm's principles, including amplitude amplification and the role of the oracle. Our findings underscore the significant potential of quantum computing in solving complex problems more efficiently than classical methods. This paper aims to be a concise resource for understanding foundational quantum computing concepts, the basics of quantum teleportation, and Grover's Algorithm.

Keywords: Quantum Computing, Quantum Teleportation, Grover's Algorithm

Contents

1 Introduction

Sans artificial intelligence, one could argue that quantum computing is the next big thing in technology. Currently, well-known companies are working to develop their own quantum computers in the hopes that they can set the precedent for future quantum use. These companies include Google's Quantum AI, Microsoft Azure Quantum, AWS Braket, and many more [5]. In addition, government organizations also view use for quantum computing. For example, the NASA Ames Research Center contains the Quantum Artificial Intelligence Lab (QuAIL) whose mandate is to "determine the potential for quantum computation to enable more ambitious and safer NASA missions in the future"[1]. To further demonstrate its relevance, once quantum computers can compute currently hypothesized algorithms, it would require a radical change in "old" processes such as information encryption methods. This is because quantum computing can break currently uncrackable encryption methods. So, it is of benefit to be familiar with the basics of quantum computing as we approach a more obtainable reality of quantum computers.

Although quantum computers are just now becoming a reality, their creation has been in the works for several years. In the early 1900s, classical physics dictated behavior at the subatomic (e.g. protons and electrons) level that did not actually occur[9]. In response, physicists had to develop a new framework to describe microscopic behavior. This morphed into quantum mechanics or quantum physics, which focuses on the funky behavior of really small particles in contrast to the intuitive behavior of easily-observable objects. An example of quantum mechanics versus classical physics is the Heisenberg Uncertainty Principle [8]. It states that one cannot know for certain both the speed and position of a subatomic particle. However, if we observe an object at the macroscopic level, we can find both the position and speed of an object. Theories such as this one unlocked completely new ways of viewing the natural world, and people began wondering how to use it. In 1985, the physicist David Deutsch studied quantum mechanics to develop an theoretical computation device that was more *efficient* than previous abstract devices. His work set the groundwork for what is now a quantum computer. Computer scientists applied this information further, developing algorithms function only on the beginnings of quantum computing. The first breakthrough algorithm was developed by Peter Shor in 1994 and involved an efficient solution to finding the prime factors of an integer [11]. This question still has no efficient solution on a classical computer. So, this discovery solidified the relevance and capabilities of quantum computing.

By studying quantum computing now, we can understand the benefits and challenges that it will pose to our current ways of technology. We are currently at the beginning of this field and, though it may be difficult, it is possible to grow one's quantum knowledge as the field continues to grow. While learning, it is important to note that, while quantum computing can vastly improve certain problems, it is not a universal solution to speeding up every algorithm. For example, this paper explores a quantum search algorithm that is faster than classical search algorithms. However, algorithms that do not rely on probabilities cannot be improved using quantum computing.

This paper covers the basic information necessary to understand quantum computing and then explores two key quantum techniques with most information from Nielson and Chuang's textbook [9]. We begin with the double-slit experiment, a foundational quantum physics experiment often used to build the intuition necessary for understanding qubit behavior. Then, we provide a section outlining the preliminary knowledge required for understanding the specifics of quantum computing. Following this, we explore the four main postulates of quantum computing. These contain key definitions and begin the discussion of necessary quantum information. We give a theoretical example of quantum teleportation, following that we track through the teleportation quantum circuit and show how the qubits can be transmitted by exploring the mechanics of superposition entanglement and quantum gates with mathematic representation [4]. Finally, we examine our last example: Grover's algorithm [7]. This quantum search algorithm efficiently finds the index of a target element using quantum techniques, an impossible outcome on a classical computer. To illustrate this, we walk through Grover's quantum circuit step by step, explaining the function of each component along the way. We also demonstrate how to extend Grover's algorithm to handle cases with multiple or no solutions, showcasing its flexibility and power in solving more complex search problems. Finally, we highlight areas of quantum computing that we could not include in this paper, potential research areas for continuations of this research, and potential impacts of quantum computing in the real world.

2 Double Slit Experiment

This experiment provides intuition of qubit behavior. In the experiment, an object can traverse one of two paths. Not knowing which path the particle traversed demonstrates superposition where the particle went along both paths. Trying to detect which path the particle traversed eliminates superposition and changes the behavior of the particle, mimicing the collapsing measurement property of qubits. The results from the experiment demonstrated that light behaves both as waves and as particles. This experiment illustrates how observation can collapse possibilities.

Thomas Young first published the Double Slit Experiment in 1807 [12]. The experiment involved two slits in a blocking surface. Young beamed small particles at the surface, and these passed throught the slits to illuminate a backboard. This should have revealed only two illuminated spaces on the back surface. However, it showed an interference pattern similar to wave behavior.

With wave behavior, a single wave passes through two or more slits simultaneously. This leads to an interference pattern. An interference pattern shows varying degrees of intensity based on the peaks and dips of multiple waves amplifying or destroying each other. When two wave peaks meet, they amplify the result. When a peak and a dip meet, they cancel each other out, resulting in smaller peaks. In contrast, a particle object would only be able to pass through one slit. Since the experiment led to an interference pattern, it demonstrated that small particles behave differently from traditional expectations and can traverse multiple paths simultaneously, an impossible property in classical physics.

Figure (1) represents the expected and actual outcomes of this experiment. Figure 1a shows the interference pattern from waves, figure 1b illustrates expected pattern for particles, and figure 1c shows the actual result of particles which closely resembles the pattern in figure 1a.

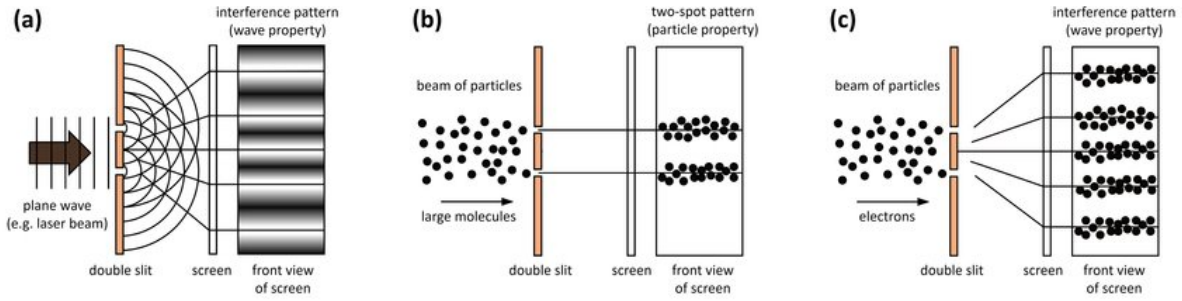


Figure 1: Different cases of Double Slit Experiement[2]

The next twist to the experiment involved trying to detect which slit the particles went through. A particle detector was placed next to both slits to detect particles that passed through. When this occurred, the pattern on the backboard was the two slits expected from particle behavior. The act of detecting the light collapsed the possible paths of the light and it behaved such that light photons acted like singular particles instead of waves.

With quantum computing, a similar phenomenon occurs. The light photons of the experiment went through "both" slits before observation. Then, when they were observed, they only went through one slit. A qubit has the ability to exist in "both" a zero and one state (go through both slits). However, when it is observed, it only shows a zero or a one. It does not show both. So observation destroys the possibilities. This presents an issue with quantum computing. A qubit in superposition can store lots of information. However, the information cannot be accessed without collapsing the qubit and consequently destroying the information. With this additional intuition into a counterintuitive concept, we can proceed with more specific discussions of quantum computing.

3 Postulates

Quantum computing is built on the fundamental principles of quantum mechanics, which govern the behavior of quantum bits (*qubits*). Unlike classical bits that store information as either 0 or 1, qubits can exist in a *superposition* of both states simultaneously. This property, along with *entanglement*, allows quantum computers to perform computations in ways that classical computers cannot.

To formalize how quantum systems behave and evolve, quantum mechanics is structured around four fundamental *postulates*. These postulates define the mathematical framework for quantum states, their transformations, and measurement outcomes. Understanding these postulates is crucial for both the **theoretical foundation** of quantum computing and its **practical implementation** in designing quantum circuits. By applying these principles, we can construct quantum gates, develop algorithms, and ultimately build quantum processors that harness the power of quantum mechanics[3].

The following sections will introduce and explain each of the four postulates, providing the necessary groundwork for understanding quantum computation.

3.1 Postulate 1

The first postulate of quantum mechanics establishes the domain in which quantum mechanics take place.

Postulate 1 *A quantum system is represented by a complex vector space in an ideal system known as the state space of the system. The state space is represented by a unit vector in complex space known as its state vector[3].*

In quantum mechanics, the simplest system, a qubit, is described by a two-dimensional complex vector space. This space is spanned by two fundamental basis states, denoted as $|0\rangle$ and $|1\rangle$, which correspond to the possible outcomes of a measurement. These basis states can also be expressed in vector form as:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Superposition of States:

A general quantum state of a qubit is a superposition of the basis states[9].

Definition 1 *A superposition is where a quantum system occupies every probabilistic state until it is observed, represented as*

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

Here and throughout this paper, the notation $|\cdot\rangle$ (pronounced "ket") is the standard notation for qubit states, the greek letter ψ represents an arbitrary qubit, and α and β are complex numbers called amplitudes. These amplitudes encode the probabilities of measuring the qubit in either basis state. The probability of observing $|0\rangle$ is $|\alpha|^2$, and the probability of observing $|1\rangle$ is $|\beta|^2$. Since these are the only possible outcomes, the total probability must sum to one:

$$|\alpha|^2 + |\beta|^2 = 1.$$

This normalization condition reflects the unit vector requirement of the state vector in the complex vector space.

Example: The $|+\rangle$ State:

An illustrative example of a qubit in superposition is the state $|+\rangle$, which has an equal probability of collapsing into $|0\rangle$ or $|1\rangle$ upon measurement. This state is defined as:

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle.$$

3.2 Postulate 2

The significance of postulate 2 plays an important role in constructing quantum algorithms. From this postulate, we can define how a qubit $|\psi\rangle$ changes with time. First, we must define several terms to understand fully Postulate 2.

Definition 2 *A number $z \in \mathbb{C}$ has a complex conjugate, denoted as z^* with $z = (x + iy)$ and $z^* = x - iy$[9].*

Definition 3 *A matrix complex conjugate, denoted as U^*(read as "U star"), is a matrix consisting of complex conjugates for all of its elements.*

An example of this is as follows:

$$U = \begin{bmatrix} 3+i & 1 \\ 1-i & 5-2i \end{bmatrix}$$
$$U^* = \begin{bmatrix} 3-i & 1 \\ 1+i & 5+2i \end{bmatrix}$$

Definition 4 *The Hermitian conjugate of U, denoted as $U^\dagger$ (read as "U dagger"), is defined as:*

$$U^\dagger = (U^T)^*,$$

Continuing our examples of matrix U, we get

$$U = \begin{bmatrix} 3+i & 1 \\ 1-i & 5-2i \end{bmatrix}$$
$$U^T = \begin{bmatrix} 3+i & 1-i \\ 1 & 5-2i \end{bmatrix}$$
$$U^\dagger = (U^T)^* = \begin{bmatrix} 3-i & 1+i \\ 1 & 5+2i \end{bmatrix}$$

Definition 5 *A unitary gate is a matrix U that satisfies the condition:*

$$U^\dagger U = I,$$

In other words, a matrix U is unitary if its Hermitian conjugate is also its inverse:

$$U^\dagger = U^{-1}.$$

In quantum computing, unitary gates are essential because they ensure that quantum operations are reversible and preserve probability, meaning no information is lost.

Definition 6 *A linear transformation through a unitary gate is known as a unitary transformation.*

Postulate 2 *The evolution of a closed quantum system is described by a unitary transformation. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2,*

$$|\psi'\rangle = U|\psi\rangle.$$

It is from postulate 2 that we are able to define a quantum gate.

Definition 7 *A quantum gate is a unitary transformation on a qubit that goes through it, represented as a matrix.*

Example: Hadamard Gate

First we will define Hadamard gate and then prove that it is a unitary gate.

Definition 8 *The Hadamard gate is a unitary operator defined as:*

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

The hadamard gate plays a key role in creating superposition, transforming a qubit $|\psi\rangle$ into an equal probability state of $|0\rangle$ and $|1\rangle$.

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle.$$

$$\alpha = \frac{1}{\sqrt{2}}, \quad \beta = \frac{1}{\sqrt{2}}$$

by definition 1 that says The probability of observing $|0\rangle$ is $|\alpha|^2$ and the probability of observing $|1\rangle$ is $|\beta|^2$ we can conclude,

$$|\beta|^2 = |\alpha|^2 = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2} = 50\%.$$

This ability to generate superposition is essential for many quantum algorithms, including quantum teleportation and many quantum algorithms[9].

Verification of Unitarity:

To verify that the Hadamard gate satisfies Postulate 2, we check its unitarity:

1. **Calculate** $H^\dagger$: The Hermitian conjugate of H is:

$$H^\dagger = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

2. **Verify** $H^\dagger H = I$:

$$H^\dagger H = \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\right)\left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\right) = \frac{1}{2} \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Since $H^\dagger H = I$, the Hadamard gate is unitary and conforms to Postulate 2. This gate along with others is used often and will appear again in sections 5 and 6.

3.3 Postulate 3

Postulate 3 describes the effects of measurements on quantum systems, allowing us to solve problems of distinguishing quantum states.

Definition 9 *In quantum mechanics, $|\psi\rangle$ (ket) and $\langle\psi|$ (bra) are mathematical notations used to describe the state of a quantum system. A ket $|\psi\rangle$ is represented as a column vector, while the corresponding bra $\langle\psi|$ is the Hermitian conjugate (complex conjugate transpose) of the ket, represented as a row vector.[9]*

The mathematical relationship between a bra and a ket is expressed as:

$$\langle\psi| = (|\psi\rangle)^\dagger,$$

where $(^\dagger)$ represents the Hermitian conjugate operation. When a bra and a ket are combined, as in $\langle\psi|\phi\rangle$, they form an *inner product*, which is a complex scalar measuring the overlap between the quantum states $|\psi\rangle$ and $|\phi\rangle$. This scalar provides crucial information about the similarity or orthogonality of the states. Conversely, when a ket and a bra are combined in the form $|\psi\rangle\langle\phi|$, they form an *outer product*. This operator is often used in quantum mechanics to project states or describe density matrices in quantum systems.

Definition 10 *A Measurement Operator M is a mathematical representation of the process of observing a quantum state, which collapses the state into one of the possible classical outcomes.*

Postulate 3 *Quantum measurements are described by a collection $\{M_m\}$ of measurement operators[9]. The index m refers to the possible measurement outcomes in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement, then the probability of obtaining the result m is given by:*

$$P(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$$

The state of the system after the measurement is:

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$$

The measurement operators satisfy the completeness equation:

$$\sum_m M_m^\dagger M_m = I$$

The completeness equation expresses that the probabilities sum to one, so:

$$\sum_m P(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle = \langle\psi|\left(\sum_m M_m^\dagger M_m\right)|\psi\rangle = \langle\psi|I|\psi\rangle = \langle\psi|\psi\rangle = 1$$

Example: Measurement of a Qubit in the Computational Basis

An important example of quantum measurement is the measurement of a qubit in the quantum computational basis, where the result is either $|0\rangle$ or $|1\rangle$. A measurement on a single qubit with two outcomes is defined by two measurement operators, $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$.

$$|0\rangle\langle 0| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad |1\rangle\langle 1| = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

Each measurement operator is Hermitian, also $M_0^2 = M_0$ and $M_1^2 = M_1$. Thus, we have the completeness relation $I = M_0 + M_1$. If the state being measured is $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, then the probability of getting measurement outcome $|0\rangle$ is:

$$\begin{aligned} P(|0\rangle) &= \langle\psi|M_0^\dagger M_0|\psi\rangle \\ &= \langle\psi|M_0 M_0|\psi\rangle = \langle\psi|M_0^2|\psi\rangle \\ &= \langle\psi|M_0|\psi\rangle = |\alpha|^2 \end{aligned}$$

Similarly, the probability of getting the measurement outcome $|1\rangle$ is $P(|1\rangle) = |\beta|^2$. For example, if we have the superposition state:

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

It will be reduced to a single state when measured. If we square the complex numbers of the states, we get $\frac{1}{2}$ for $|0\rangle$ and $\frac{1}{2}$ for $|1\rangle$. Thus, it will be reduced to either the $|0\rangle$ state with a 50% probability or the $|1\rangle$ state with a 50% probability. This also satisfies postulate 1, which states:

$$|\alpha|^2 + |\beta|^2 = 1.$$

This specific measurement outcome resembles a coin flip. If we flip a coin, we would only get either heads or tails, never both.

3.4 Postulate 4

Postulate 4 *The state space of a composite quantum system is the tensor product of the state spaces of its component systems. For n components, the combined state is represented as:*

$$|\psi_{total}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle,$$

where $\otimes$ denotes the tensor product[9].

Tensor Product ($\otimes$): The tensor product combines the state spaces of multiple quantum systems into a single composite state space. For vectors $|a\rangle = \begin{bmatrix} a_1 \\ a_2 \end{bmatrix}$ and $|b\rangle = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}$, their tensor product is:

$$|a\rangle \otimes |b\rangle = |ab\rangle = |a\rangle|b\rangle \begin{bmatrix} a_1 b_1 \\ a_1 b_2 \\ a_2 b_1 \\ a_2 b_2 \end{bmatrix}$$

Intuitively, it represents every combination of $|a\rangle$ and $|b\rangle$.

Superposition in Composite Systems: A composite system can exist in a superposition of all possible combinations of its component states. For two qubits, the state is represented as:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle,$$

where $|\alpha_{ij}|^2$ gives the probability of measuring the system in the basis state $|ij\rangle$.

Entangled States and the Role of the CNOT Gate: Composite quantum systems allow for the creation of *entangled states*, where the states of individual components are not independent. An example of an entangled state is the Bell state:

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

where the measurement of one qubit determines the state of the other.

In a composite quantum system, we often need operations that manipulate multiple qubits in a controlled manner. The *Controlled-NOT (CNOT) gate* is a fundamental two-qubit gate that acts on a **control qubit** and a **target qubit**. The CNOT gate flips the target qubit if and only if the control qubit is in the $|1\rangle$ state. Mathematically, it operates as follows:

$$\text{CNOT}|00\rangle = |00\rangle, \quad \text{CNOT}|01\rangle = |01\rangle,$$
$$\text{CNOT}|10\rangle = |11\rangle, \quad \text{CNOT}|11\rangle = |10\rangle.$$

The matrix representation of the CNOT gate in the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ is:

$$U_{\text{CNOT}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Measurement in Composite Systems: A measurement on a composite system collapses the entire state into one of the possible basis states of the combined system. For example, measuring the entangled state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

might result in either $|00\rangle$ or $|11\rangle$, each with a 50% probability.

Applications of Postulate 4

Postulate 4 enables us to describe and manipulate systems with multiple qubits. Here is an example:

Example: Two-Qubit System Suppose two qubits are in the following states:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |\psi_2\rangle = |0\rangle.$$

The state $|\psi_1\rangle$ is in *superposition*, meaning it has a 50% probability of being $|0\rangle$ and a 50% probability of being $|1\rangle$. On the other hand, $|\psi_2\rangle$ is always in the state $|0\rangle$. When taking the *tensor product* of these two qubits, the resulting system will be in one of the following states:

$$|0\rangle \otimes |0\rangle = |00\rangle, \quad (\text{if } |\psi_1\rangle = |0\rangle)$$

$$|1\rangle \otimes |0\rangle = |10\rangle, \quad (\text{if } |\psi_1\rangle = |1\rangle)$$

Since $|\psi_1\rangle$ is equally likely to be $|0\rangle$ or $|1\rangle$, the system has a 50% probability of being in $|00\rangle$ and a 50% probability of being in $|10\rangle$, as shown mathematically below:

$$|\psi_{12}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle.$$

Expanding this:

$$|\psi_{12}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |0\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle).$$

Significance of Postulate 4:

Postulate 4 is fundamental for constructing quantum circuits involving multiple qubits. It introduces the concept of *entanglement*, a phenomenon unique to quantum mechanics, where the state of one qubit is intrinsically linked to another. This is crucial for quantum computing tasks such as quantum teleportation, superdense coding, and algorithms like Grover's search. The **CNOT gate**, in particular, plays a central role in entanglement generation, making it a critical component in quantum computation and quantum information processing.

4 Quantum Curcuit Diagrams

Quantum circuits are visual representations of quantum algorithms, illustrating the sequence of quantum gates and measurements applied to qubits. Understanding how to read these diagrams is crucial for grasping the flow and operations within a quantum algorithm. This section provides a guide to interpreting quantum circuit diagrams, using the context and concepts discussed in previous sections.

4.1 Basic Components of Quantum Circuits

4.1.1 Qubits and Wires

- **Qubits**: Represented by horizontal lines, each qubit corresponds to a quantum state that evolves over time.
- **Wires**: The horizontal lines in the circuit diagram represent the timeline of a qubit. Time flows from left to right.

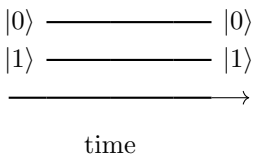


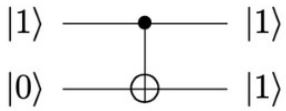
Figure 2: An example of qubits and wires in a quantum circuit. The horizontal lines represent qubits, and time flows from left to right.

4.1.2 Quantum Gates

- **Single-Qubit Gates**: Operations that act on a single qubit. This includes the previously described Hadamard gate (H).
- **Multi-Qubit Gates**: Operations that act on multiple qubits. Examples include the CNOT gate (controlled-NOT).
- **Gate Notation**: Gates are represented by specific symbols placed on the qubit lines. For example, the Hadamard gate is often depicted as a box with an "H" inside.

1: Example of Hadamard gate acting on one qubit.

2: Example of a *not* gate acting on one qubit.



3: Example of a controlled-*not* gate.

Figure 3: Examples of the Hadamard gate (H), not gate, and CNOT gate are on a single qubit.

4.1.3 Measurements

- **Measurement Operations**: Represented by a meter symbol, measurements collapse the quantum state into a classical bit (0 or 1).
- **Classical Bits**: After measurement, the result is often represented by a double line leading to a classical bit register.

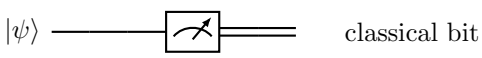


Figure 4: When a qubit is measured it collapses into a classical bit.

4.2 Reading a Quantum Circuit

1. **Identify Qubits and Initial States**:
   - Determine the number of qubits and their initial states. Typically, qubits start in the $|0\rangle$ state unless specified otherwise.
2. **Follow the Sequence of Gates**:
   - Trace the sequence of gates applied to each qubit from left to right. Note how gates affect the state of the qubits.
   - Pay attention to control lines in multi-qubit gates (e.g., in a CNOT gate, the control qubit influences the target qubit).
3. **Observe Measurements**:
   - Identify where measurements occur and which qubits are being measured. Understand how the measurement collapses the quantum state.
4. **Interpret the Final State**:
   - After all gates and measurements, interpret the final state of the qubits. This often involves understanding the probabilities of different outcomes.

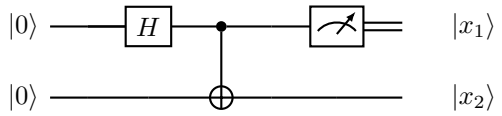


Figure 5: Basic quantum circuit with Hadamard, CNOT, and measurement gates

5 Quantum Teleportation

Quantum teleportation is a key piece in many quantum algorithms and is a primary example of the properties of quantum computers that are impossible with classical computing[9]. With figure 6, we will explain how quantum teleportation works.

Example: Quantum Teleportation Between Earth and Moon

To perform quantum teleportation, suppose Alice is on Earth and Bob is on the Moon. Before they begin, they share an entangled pair of qubits, with Alice keeping one qubit on Earth and Bob taking the other with him to the Moon. Alice then takes an unknown quantum state that she wants to send and interacts it with her half of the entangled pair. By applying a series of quantum gates and then measuring her qubits, she effectively transfers information about the original state to Bob's qubit on the Moon.

However, this process alone does not immediately give Bob the correct quantum state—he also needs a classical message from Alice, which she sends through a conventional communication channel, such as a radio signal. Once Bob receives this classical information, he applies specific quantum gate operations to his qubit, allowing him to perfectly reconstruct the quantum state that Alice originally had. Despite being light-years apart, the entanglement between their qubits ensures that Bob can receive the exact quantum information without the qubit itself ever physically traveling from Earth to the Moon. The official process can be visualized as follows:

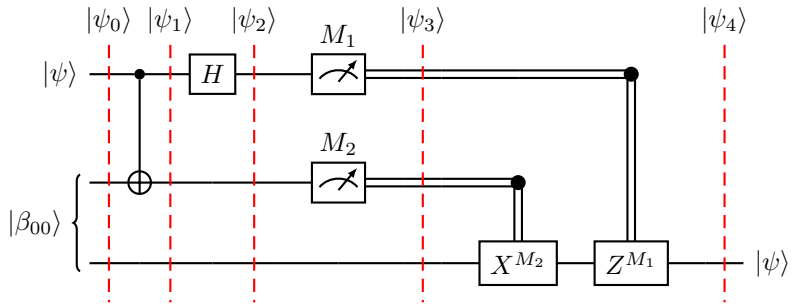


Figure 6: Quantum Teleportation Circuit

5.1 Initial State

The Tensor product of the qubit $|\psi\rangle$ and the entangled pair $|\beta_{00}\rangle$:

$$|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle = (\alpha|0\rangle + \beta|1\rangle)\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right).$$

Expanding this:

$$|\psi_0\rangle = \frac{\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle}{\sqrt{2}}.$$

5.2 Applying the CNOT Gate

The CNOT gate ($\oplus$) is applied to the first two qubits:

$$|A, B\rangle \longrightarrow |A, B \oplus A\rangle,$$

where $\oplus$ represents addition mod 2. Applying this to our state:

$$|\psi_1\rangle = \frac{\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle}{\sqrt{2}}.$$

5.3 Applying the Hadamard Gate

The Hadamard gate (H) is applied to the first qubit. Recall that the Hadamard gate matrix is:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Applying this gate:

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Transforming our state:

$$|\psi_2\rangle = \frac{\alpha}{2}(|0\rangle + |1\rangle)|00\rangle + \frac{\alpha}{2}(|0\rangle + |1\rangle)|11\rangle + \frac{\beta}{2}(|0\rangle - |1\rangle)|10\rangle + \frac{\beta}{2}(|0\rangle - |1\rangle)|01\rangle.$$

Simplifying:

$$|\psi_2\rangle = \frac{\alpha}{2}|000\rangle + \frac{\alpha}{2}|100\rangle + \frac{\alpha}{2}|011\rangle + \frac{\alpha}{2}|111\rangle + \frac{\beta}{2}|010\rangle - \frac{\beta}{2}|110\rangle + \frac{\beta}{2}|001\rangle - \frac{\beta}{2}|101\rangle.$$

5.4 Measuring Qubits

The first and second qubits are measured. There are four possible outcomes for the measurements: $[0,0]$, $[0,1]$, $[1,0]$, and $[1,1]$. Upon measurement, each qubit collapses to either 0 or 1. Specific gates will be applied to the third qubit depending on the measurement outcome. If a qubit collapses to 0, the corresponding gate will not be used. If a qubit collapses to 1, the corresponding gate will be applied. The combination of measurement outcomes determines the exact operations applied to the third qubit:

- **If** $M_1 = 0$ **and** $M_2 = 0$: No operations are applied.
- **If** $M_1 = 0$ **and** $M_2 = 1$: Apply the X gate to the third qubit.
- **If** $M_1 = 1$ **and** $M_2 = 0$: Apply the Z gate to the third qubit.
- **If** $M_1 = 1$ **and** $M_2 = 1$: Apply the X and Z gates to the third qubit.

Where X flips the probability of the α and β and Z flips the sign of β with matrix representations of:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$
$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Cases

Case 1: $M_1 = 0$ **and** $M_2 = 0$

$$|\psi_3\rangle = \alpha|000\rangle + \beta|001\rangle$$

No operations are applied

$$|\psi_4\rangle = \alpha|000\rangle + \beta|001\rangle = \alpha|0\rangle + \beta|1\rangle$$

Case 2: $M_1 = 0$ **and** $M_2 = 1$

$$|\psi_3\rangle = \alpha|011\rangle + \beta|010\rangle$$

Applying the X gate

$$|\psi_4\rangle = \alpha|010\rangle + \beta|011\rangle = \alpha|0\rangle + \beta|1\rangle$$

Case 3: $M_1 = 1$ **and** $M_2 = 0$

$$|\psi_3\rangle = \alpha|100\rangle - \beta|101\rangle$$

Applying the Z gate

$$|\psi_4\rangle = \alpha|100\rangle + \beta|101\rangle = \alpha|0\rangle + \beta|1\rangle$$

Case 4: $M_1 = 1$ **and** $M_2 = 1$

$$|\psi_3\rangle = \alpha|111\rangle - \beta|110\rangle$$

Applying the X and Z gates

$$|\psi_4\rangle = \alpha|110\rangle + \beta|111\rangle = \alpha|0\rangle + \beta|1\rangle$$

In all cases, the third qubit collapses to the state:

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

successfully teleporting the original quantum state. This highlights the power and potential of quantum teleportation as a demonstration of the fundamental principles of quantum mechanics. By leveraging entanglement and precise measurement protocols, quantum teleportation ensures that the original qubit's state is perfectly reconstructed at the destination, even though the qubit itself is not physically transmitted.

6 Grover's Algorithm

Grover's Algorithm is a quantum search algorithm that returns the index of a desired element (we denote the number of desired elements to be M and assume $M = 1$) out of an unsorted list of N elements. On a classical computer, this has no efficient solution. One must check each element one at a time. However, using quantum computing, Grover's Algorithm provides an efficient solution to this problem because it searches every element simultaneously. As in the previous section, we will follow the cricuit diagrams. Figure 7 shows the overall circuit, and Figure 8 shows what each G in the Figure 7 represents.To justify the motivation behind Grover's Algorithm, we must first briefly cover algorithm efficiency.

6.1 Big-O Notation

In quantum computing, as in classical computing, we analyze the efficiency of algorithms using Big-O notation. Big-O notation describes the upper bound of an algorithm's time complexity as a function of the input size. It provides a way to classify algorithms by how their runtime or resource usage scales with the size of the problem.

- $O(1)$: Constant time, where the algorithm's performance is unaffected by input size.
- $O(\log n)$: Logarithmic time, often seen in divide-and-conquer algorithms.
- $O(\sqrt{n})$: Square-root time, where the runtime scales with the square root of the input size. This is commonly achieved in quantum algorithms.
- $O(n)$: Linear time, where the runtime grows proportionally to the input size n.
- $O(n^2)$: Quadratic time, where the runtime grows as the square of the input size.

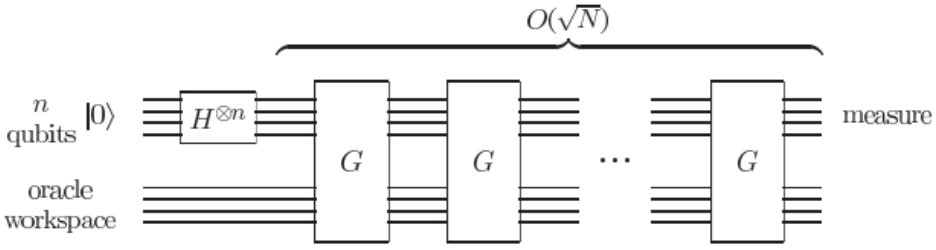


Figure 7: Grover's Algorithm Quantum Circuit [9]

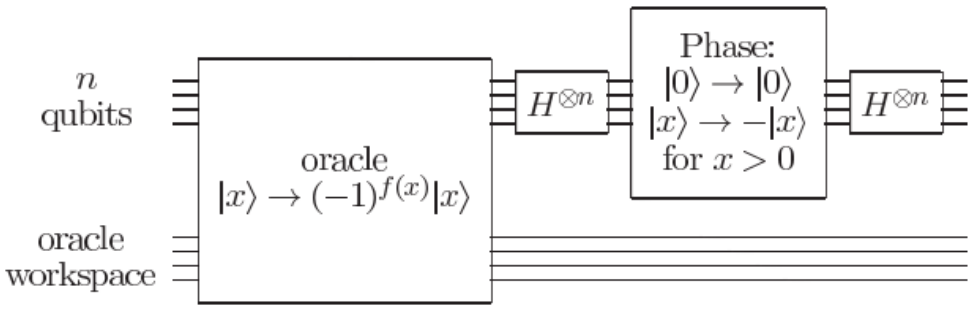


Figure 8: Quantum circuit for Grover Iteration G [9]

6.2 Grover's Algorithm Setup

We will assume $N = 2^n$. The algorithm begins with n qubits, each initialized in the $|0\rangle$ state. This initial state is expressed as

$$|0\rangle^{\otimes n} = |0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle,$$

where the notation $|0\rangle^{\otimes n}$ denotes the tensor product of n identical single-qubit states. Explicitly, for small values of n, we have:

- For $n = 1$, $|0\rangle^{\otimes 1} = |0\rangle$.
- For $n = 2$, $|0\rangle^{\otimes 2} = |0\rangle \otimes |0\rangle$.
- For $n = 3$, $|0\rangle^{\otimes 3} = |0\rangle \otimes |0\rangle \otimes |0\rangle$.

In general, this notation compactly represents a system of n qubits, each starting in the computational basis state $|0\rangle$. The algorithm then applies a Hadamard gate to each qubit, transforming this initial state into an equal superposition of all possible computational basis states.

The algorithm then repeats a process called a *Grover Iteration*, which involves an *oracle*, a second Hadamard gate, and a *phase shift*. The algorithm performs a fixed number of these iterations, which we will explore in detail, including how to determine the optimal number of trials.

First, we must define the oracle. The oracle recognizes whether a certain index contains the desired element. If the index is a solution, a qubit called the *oracle qubit* (or the output of the function) will be flipped to a 1. If the index is not a solution, the oracle qubit will remain zero. Observing the oracle qubit tells us the index of the desired element. The oracle process is summarized below where $|x\rangle$ is the index qubit (that could either be a solution or not), $|q\rangle$ is the oracle qubit that can be flipped, and $f(x)$ represents 0 if x is not a solution, 1 if x is a solution, and $\oplus$ is addition mod 2:

$$|x\rangle|q\rangle \xrightarrow{\text{O}} |x\rangle|q \oplus f(x)\rangle$$

6.3 Initial State

The algorithm begins with n qubits in the zero state. We write this as $|0\rangle^{\otimes n}$ which is just the tensor product of itself n times. The first Hadamard transform is applied to each qubit. A Hadamard transform applied to n qubits in a zero state result in the following:

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle$$

Since $N = 2^n$, we get

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

These superposed qubits can be written as a starting vector $|\psi\rangle$. The term $\sum_x''$ indicates qubits that are not solutions, and $\sum_x'$ indicates qubits that are solutions. We use these define normalized states as follows:

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_{x}'' |x\rangle$$
$$|\beta\rangle = \frac{1}{\sqrt{M}} \sum_{x}' |x\rangle$$

Since the sum of all qubits that are not solutions added to the sum of all qubits that are solutions is equal to all qubits, we can substitute into the $|\psi\rangle$ equation to get the initial state as an object that is in the space spanned by $|\alpha\rangle$ and $|\beta\rangle$.

$$|\psi\rangle = \sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle$$

The Oracle

Then we apply the oracle. Recall that the oracle recognizes whether an index contains a solution. It changes the superimposed state of the single oracle qubit by swapping $|0\rangle$ and $|1\rangle$ having a net change as follows:

$$|x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \xrightarrow{O} \begin{cases} -|x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} & \text{if } x \text{ is a solution} \\ |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} & \text{if } x \text{ is not a solution} \end{cases}$$

This can be written more succinctly as the following:

$$|x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \xrightarrow{O} (-1)^{f(x)}|x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

where $f(x)$ is 0 if x is not a solution and 1 if x is a solution. The oracle qubit's state (represented by the fraction quantity) is not changed by the oracle because we pull out the negative sign. So, we can omit this from our equation. Then we apply a second Hadamard transform.

6.4 Phase Shift

Then, we apply a phase shift. The phase shift is another reflection, this time around the initial vector. It's net effect is described below.

$$|x\rangle \rightarrow -(-1)^{\delta_{x0}}|x\rangle$$

where δ_{x0} is either 0 or 1. If the input qubit is $|0\rangle$, then it remains unchanged. If the input qubit is anything other than zero, then it's effect is $|x\rangle \rightarrow -|x\rangle$. The oracle combined with the phase shift is equivalent to two reflections about two different vectors. These actions combine to produce a rotation in the plane spanned by α and β. By applying the Grover Iteration (the oracle, second hadamard, and phase shift), we can rotate the qubit state vector until it produces a vector that is $|\psi\rangle = 0|\alpha\rangle + 1|\beta\rangle$. The entire Grover iteration is summarized by the equation $G = (2|\psi\rangle\langle\psi| - I)O$.

6.5 Summary of Grover Iteration Proof

In addition to considering the literal math of Grover's Algorithm, we can also visualize it geometrically for any number of solutions. If we define $\sqrt{\frac{N-M}{N}}$ to be $\cos(\theta/2)$ and $\sqrt{\frac{M}{N}}$ to be $\sin(\theta/2)$, we can rewrite the initial state vector as $|\psi\rangle = \cos(\theta/2)|\alpha\rangle + \sin(\theta/2)$. We will apply the Grover Iteration to this initial vector to justify the effects

of the Grover Iteration multiple times. Note: $|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|\alpha\rangle + \sin\left(\frac{\theta}{2}\right)|\beta\rangle$ and $\langle\psi| = \cos\left(\frac{\theta}{2}\right)\langle\alpha| + \sin\left(\frac{\theta}{2}\right)\langle\beta|$. We want to show that $G|\psi\rangle = \cos(\frac{3\theta}{2})|\alpha\rangle + \sin(\frac{3\theta}{2})|\beta\rangle$.

$$\begin{aligned}
O|\psi\rangle &= \cos\left(\frac{\theta}{2}\right)|\alpha\rangle - \sin\left(\frac{\theta}{2}\right)|\beta\rangle \\
2|\psi\rangle &= 2\cos\left(\frac{\theta}{2}\right)|\alpha\rangle + 2\sin\left(\frac{\theta}{2}\right)|\beta\rangle \\
2|\psi\rangle\langle\psi| - I &= 2\cos^2\left(\frac{\theta}{2}\right)|\alpha\rangle\langle\alpha| + 2\cos\left(\frac{\theta}{2}\right)\sin\left(\frac{\theta}{2}\right)|\alpha\rangle\langle\beta| + 2\sin\left(\frac{\theta}{2}\right)\cos\left(\frac{\theta}{2}\right)|\beta\rangle\langle\alpha| \\
&\quad +2\sin^2\left(\frac{\theta}{2}\right)|\beta\rangle\langle\beta| - I
\end{aligned}$$

$$\begin{aligned}
(2|\psi\rangle\langle\psi| - I)O|\psi\rangle &= 2\cos^3\left(\frac{\theta}{2}\right)|\alpha\rangle\langle\alpha|\alpha\rangle + 2\cos^2\left(\frac{\theta}{2}\right)\sin\left(\frac{\theta}{2}\right)|\alpha\rangle\langle\beta|\alpha\rangle \\
&\quad +2\sin\left(\frac{\theta}{2}\right)\cos^2\left(\frac{\theta}{2}\right)|\beta\rangle\langle\alpha|\alpha\rangle + 2\sin^2\left(\frac{\theta}{2}\right)\cos\left(\frac{\theta}{2}\right)|\beta\rangle\langle\beta|\alpha\rangle \\
&\quad -2\cos^2\left(\frac{\theta}{2}\right)\sin\left(\frac{\theta}{2}\right)|\alpha\rangle\langle\alpha|\beta\rangle - 2\cos\left(\frac{\theta}{2}\right)\sin^2\left(\frac{\theta}{2}\right)|\alpha\rangle\langle\beta|\beta\rangle \\
&\quad -2\sin^2\left(\frac{\theta}{2}\right)\cos\left(\frac{\theta}{2}\right)|\beta\rangle\langle\alpha|\beta\rangle - 2\sin^3\left(\frac{\theta}{2}\right)|\beta\rangle\langle\beta|\beta\rangle \\
&\quad -\cos\left(\frac{\theta}{2}\right)|\alpha\rangle + \sin\left(\frac{\theta}{2}\right)|\beta\rangle
\end{aligned}$$

The terms $\langle\alpha|\alpha\rangle$ and $\langle\beta|\beta\rangle$ are said to "match" and simplify to 1, while the terms $\langle\alpha|\beta\rangle$ and $\langle\beta|\alpha\rangle$ do not and simplify to 0. This is because this is equal to vector multiplication. So $\langle\alpha|\alpha\rangle = \begin{bmatrix}1 & 0\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}$ which is simply equal to 1. Whereas $\langle\alpha|\beta\rangle = \begin{bmatrix}1 & 0\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}$ is equal to 0. The equation now becomes

$$\begin{aligned}
(2|\psi\rangle\langle\psi| - I)O|\psi\rangle &= 2\cos^3\left(\frac{\theta}{2}\right)|\alpha\rangle + 2\sin\left(\frac{\theta}{2}\right)\cos^2\left(\frac{\theta}{2}\right)|\beta\rangle \\
&\quad -2\cos\left(\frac{\theta}{2}\right)\sin^2\left(\frac{\theta}{2}\right)|\alpha\rangle - 2\sin^3\left(\frac{\theta}{2}\right)|\beta\rangle \\
&\quad -\cos\left(\frac{\theta}{2}\right)|\alpha\rangle + \sin\left(\frac{\theta}{2}\right)|\beta\rangle
\end{aligned}$$

We continue to simplify this by using the identity $\sin^2(\theta) + \cos^2(\theta) = 1$

$$(2|\psi\rangle\langle\psi| - I)O|\psi\rangle = \left(4\cos^3\left(\frac{\theta}{2}\right) - 3\cos\left(\frac{\theta}{2}\right)\right)|\alpha\rangle + \left(3\sin\left(\frac{\theta}{2}\right) - 4\sin^3\left(\frac{\theta}{2}\right)\right)|\beta\rangle$$

The triple angle formula states $\sin(3\theta) = 3\sin(\theta) - 4\sin^3\theta$ and $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$. So, the equation becomes the following:

$$(2|\psi\rangle\langle\psi| - I)O|\psi\rangle = \cos\left(\frac{3\theta}{2}\right)|\alpha\rangle + \sin\left(\frac{3\theta}{2}\right)|\beta\rangle$$

Therefore, $G|\psi\rangle = \cos(\frac{3\theta}{2})|\alpha\rangle + \sin(\frac{3\theta}{2})|\beta\rangle$. This is visualized through Figure 9.

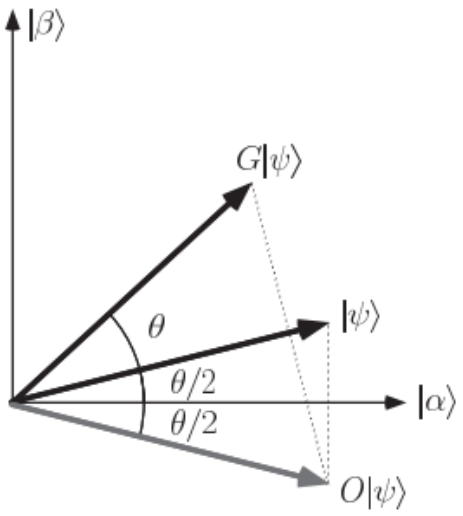


Figure 9: Geometric visualization of Grover Iteration[9]

Since we merely repeat G, our qubit $|\psi\rangle$ is rotated by $\cos(\frac{2k+3}{2}\theta) + \sin(\frac{2k+3}{2}\theta)$ for our number of trials k.

6.6 Measurement

By completing the Grover Iteration a pre-determined number of times, the algorithm alters the probability amplitude of only the solution qubit. The probability amplitude of the solution qubit is increased until the probability of measuring $|\beta\rangle$ is higher than the probability of returning $|\alpha\rangle$. The final step of the algorithm is the measurement. All the qubits collapse to show $|\alpha\rangle$ except for the solution qubit. This qubit collapses into $|\beta\rangle$ which means that the index corresponding to that qubit has the desired element.

By using quantum computing, we can search every single element for the solution simultaneously. In classical computing, we must search through every element one-by-one. With quantum computing, we speed up the process of finding a specific element by using the oracle. Then, the rest of the algorithm is to guaranteeing we don't loose the information that the oracle gives us when we measure it.

Performance

Producing this qubit state requires a specific number of Grover Iterations. If we have too many iterations, we rotate the vector too far and it will decrease the probability that it shows the solution. If we have too few iterations, we also risk having a too low probability, missing a solution again. We need to determine the number of times the Grover iteration should be repeated. The initial state of the system, $|\psi\rangle = \sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle$, rotates by an angle of $\arccos\left(\sqrt{\frac{M}{N}}\right)$ radians to reach $|\beta\rangle$. We define $\mathrm{CI}(x)$ as the integer nearest to a real number x, with the rounding convention of $\mathrm{CI}(3.5) = 3$. Thus, repeating the Grover iteration $R = \mathrm{CI}\left(\frac{\arccos\left(\sqrt{\frac{M}{N}}\right)}{\theta}\right)$ times will rotate $|\psi\rangle$ to within an angle $\theta/2 \leq \pi/4$ of $|\beta\rangle$. When the final state is observed, it yields a solution with at least a 50% success rate. For scenarios where $M \ll N$, we have $\theta \approx \sin\theta \approx 2\sqrt{\frac{M}{N}}$, resulting in an angular error of about $\theta/2 \approx \sqrt{\frac{M}{N}}$ in the final state, and consequently a success probability error of at most M/N. Note that R depends only on the number of solutions M, not on their specific identities.

If M is known, we can apply the quantum search algorithm as described. However, in Section 7.1, we discuss a method to execute the search algorithm without prior knowledge of M. The expression above gives an exact

iteration count for oracle calls in the quantum search algorithm, yet a simplified expression that approximates R's behavior is often helpful. Since $R \leq \frac{\pi}{2\theta}$, a lower bound on θ provides an upper bound on R. Assuming $M \leq N/2$, we have

$$\frac{\theta}{2} \geq \sin\frac{\theta}{2} = \sqrt{\frac{M}{N}},$$

which leads to an upper bound on the number of iterations:

$$R \leq \left\lceil \frac{\pi}{4}\sqrt{\frac{N}{M}} \right\rceil.$$

Therefore, $R = O\left(\sqrt{\frac{N}{M}}\right)$, meaning $O\left(\sqrt{\frac{N}{M}}\right)$ Grover iterations (and oracle calls) are required to find a solution with high probability. This represents a quadratic improvement over the classical requirement of $O\left(\frac{N}{M}\right)$ oracle calls. In classical computing, finding a marked item among N items, where M of them are "marked" or meet a specific criterion, typically requires sequentially checking each item one by one. On average, it takes $\frac{N}{M}$ checks to locate a marked item because there are M possible successes scattered among N items. This linear search process, with each item needing to be evaluated individually, leads to a time complexity of $O\left(\frac{N}{M}\right)$ in the classical setting. For the specific case of $M = 1$, the quantum search algorithm is outlined.

7 Further Research

In this paper, we gave a brief overview of how quantum computing operates and the fundamental elements that allow algorithms to operate successfully. We give intuition of quantum behaviors using the double slit experiment. We cover the four core postulates that define quantum systems, gates, measurement, and composite quantum systems. We then cover two specific examples of quantum computation implementation: quantum teleportation and Grover's algorithm.

A further research area of interest includes quantum encryption methods. Quantum encryption poses a serious threat to our current ways of sending information electronically, for example sending data in Cloud databases. Currently, the most common method for encrypting data is RSA Encryption first presented by Ron Rivest, Adi Shamir, and Len Adleman in 1977 [10]. The process involves multiplying two large prime numbers and using the result to hide the sent information. To read the information, one must know the two original prime numbers. However, this poses challenges with large numbers because there are so many different divisors of large numbers. In 1994, Peter Shor derived a quantum algorithm that does this factoring quickly [9]. A potential next step of quantum research is to learn this algorithm. A step further would be to explore a more recent factoring algorithm that requires less qubits [6].

Another possible area is to move beyond the purely hypothetical algorithms and explore the issues that emerge with actual implementation. One major issue is noise [9]. Noise emerges when unplanned factors interact with the innerworkings of a quantum computer, often changing the state of qubits. Noise is normally not a desired property of quantum computing so studying existing methods of preventing noise is beneficial. To explore this, one would begin researching more in-depth how information is stored in qubits, i.e. quantum information.

One last interesting potential pathway is to explore how quantum algorithms actually are built. This requires a more physical understanding of qubits, gates, and paths. Learning these allow one to explore quantum refrigerators, ion traps, and electrodynamics [9].

References

[1] *NASA Quantum Artificial Intelligence Laboratory (QuAIL)*, 2025.

[2] A. Aydin, *Quantum Shape Effects*, 02 2021.

[3] M. Bean, D. Flynn, and K. Yasumoto, *Quantum Computational Bomb Sorting*, technical report, University of Washington Tacoma, January 2021.

[4] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels*, Phys. Rev. Lett., 70 (1993), pp. 1895–1899.

[5] J. Dargan, *Quantum Computing Companies: A Full 2024 List*, 2023.

[6] C. Gidney and M. Ekerå, *How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits*, Quantum, 5 (2021), p. 433.

[7] L. K. Grover, *A Fast Quantum Mechanical Algorithm for Database Search*, in Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, 1996, pp. 212–219.

[8] W. Heisenberg, *Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik*, Zeitschrift für Physik, (1927).

[9] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, Cambridge University Press, 2010.

[10] R. L. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Commun. ACM, 21 (1978), p. 120–126.

[11] P. Shor, *Algorithms for Quantum Computation: Discrete Logarithms and Factoring*, in Proceedings 35th Annual Symposium on Foundations of Computer Science, 1994, pp. 124–134.

[12] T. Young, *A course of lectures on natural philosophy and the mechanical arts*, vol. 1, London, Printed for J. Johnson, 1807, 1807. https://www.biodiversitylibrary.org/bibliography/22458.