

# Seasons of Science 2025

Midterm Report

## Quantum Computing and Quantum Information

**Yaswanth Ram Kumar**

Electrical Engineering, IIT Bombay

**Mentor: Harsh Sharma**

*"I think I can safely say that nobody understands quantum mechanics."*

- Richard Feynman

*"The postulates of quantum mechanics are not deduced but postulated"*

- Dirac

14 June, 2025

## Introduction

Quantum Computing and Quantum Information is one of the most fascinating and rapidly evolving fields at the intersection of physics, computer science, and information theory. This report presents a comprehensive study based on the initial chapters of the book *Quantum Computation and Quantum Information* by Michael A. Nielsen and Isaac L. Chuang (10th Anniversary Edition), which serves as the primary reference unless otherwise stated.

I would like to express my gratitude to my mentor, Harsh Sharma, for recommending this book to me. The book presents complex ideas in a story-driven manner, making the concepts of quantum information and quantum computing significantly easier to understand and appreciate.

This report is structured as a point-wise summary of fundamental concepts and key insights, I have tried to follow the order in which they are introduced in the book. But in some cases, I explored topics mentioned only briefly in Chapter 1 out of fear that I wasn't understanding them. I later realized that the authors were merely introducing those ideas to provide historical context, with more rigorous treatment appearing in later chapters. However, I have tried to include everything I have learned so far, including content from outside sources where I felt were necessary and simple to understand.

1. **Church-Turing Thesis:** Alan Turing developed an in detail abstract notion of what we would now call a programmable computer, a model for computation now known as the *Turing machine*. Turing showed that there is a **Universal Turing Machine** that can be used to simulate any other Turing machine. He claimed that the Universal Turing Machine completely captures what it means to perform a task by algorithmic means. That is, if an algorithm can be performed on any piece of hardware (say, a modern personal computer), then there is an equivalent algorithm for a Universal Turing Machine which performs exactly the same task as the algorithm running on the personal computer.
2. **Von Neumann Architecture:** Von Neumann built a computer as we now know with electronic components which is also called Harvard architecture for CPUs. These are still in classical use today and taught in Universities.

The Von Neumann architecture is a classical model of how most computers work, first proposed by John von Neumann in 1945. It uses a single memory space to store both the data and the program instructions. A central processing unit (CPU), which includes a control unit and an arithmetic logic unit (ALU), reads instructions one by one, fetches the required data, performs computations, and stores results back in memory.

This architecture enables a computer to program any task just by changing the stored instructions, making it incredibly flexible and foundational to modern computing.

3. **Limitations of Classical Computing:** Later on, as time passed, we saw that classical computers had limitations with respect to time and space. We weren't able to *efficiently* simulate a physical system on a classical computer. We weren't able to factorize a large number (which Peter Shor's Algorithm can do with a Quantum Computer). This led to a change in the Church-Turing thesis, resulting in the Strong form of Church-Turing thesis:

*Any algorithmic process can be simulated efficiently using a Turing machine.*

4. **Moore's Law:** Moore's Law stated that there will be a *doubling in computer power every two years*. But as we know it, it is eventually failing in the 21st century. This failure is attributed to quantum effects coming into play as the size limit is reached with the silicon transistors we are using today. This scenario is explained in a better video: <https://youtu.be/Q1v5pB6u534?si=frlDxilyANtCrbJ7>
5. **Analog Computers vs Turing Machines:** Analog computers appeared to outperform Turing machines by leveraging continuous mathematics and idealized precision, potentially solving very hard problems quickly. But in real-world physics, noise and imprecision mean that analog computers can't maintain the ultra-fine precision needed to achieve that speed. Therefore, under realistic situations, analog computers cannot violate the Strong ChurchTuring Thesis, they do not solve problems more efficiently than Turing machines when noise is accounted for.

#### What are Analog Computers?

An analog computer is a type of computer that uses the continuously changeable aspects of physical phenomena, such as electrical, mechanical, or hydraulic quantities, to model the problem being solved. In contrast to digital computers, analog computers do not operate using discrete values, but rather manipulate continuous data.

*Source: Wikipedia Analog Computer*

6. **Quantum Computing and Noise Tolerance:** Unlike analog computers, quantum computation can in principle tolerate a finite amount of noise and still maintain its computational advantages. Quantum error codes have been developed by scientists over a period to contribute to this too, just like we have in classical computation like Hamming code, parity-based correction, CRC, checksum etc., but obviously more complicated.

### Power of Parity: Detecting and Correcting a Single Bit Error

In digital systems, data may get corrupted during transmission due to noise. To ensure reliability, we often add redundancy in the form of **parity bits**.

For example, say we want to transmit a  $3 \times 3$  matrix with binary entries. To detect and correct any single-bit error, we add one extra parity bit per row and per column:

1	0	1	0
0	1	0	1
1	1	1	1
0	0	0	

Each row and column has even parity. Now, suppose one bit is corrupted during transmission, say the center bit flips from 1 to 0:

1	0	1	0
0	0	0	1
1	1	1	1
0	0	0	

The parity in **Row 2** and **Column 2** now fails, indicating an error at position (2,2). Simply flipping that bit corrects the message.

*Source: Wikipedia Parity Bit*

7. **Probabilistic Computing:** In later stages, again the strong form of the Church-Turing thesis has been challenged because of the **Solovay-Strassen Primality Test**. In simpler terms, it uses random numbers to check whether a given number is prime. So there has been an *ad hoc* addition to the Strong Church-Turing Thesis:

*Any algorithmic process can be simulated efficiently using a probabilistic Turing machine.*

*ad hoc* means 'necessary'

8. **Deutsch's Quantum Computing Vision:** In 1985, David Deutsch asked whether the laws of physics could be used to derive an even stronger version of the Church-Turing thesis, instead of adopting *ad hoc* hypotheses whenever a challenge arises. He attempted to define a computational device that would be capable of *efficiently simulating any arbitrary physical system*. Because the laws of physics are ultimately quantum mechanical, Deutsch was naturally led to consider computing devices based upon the principles of **quantum mechanics**.

9. **Shor's Algorithm Impact:** In 1994, Peter Shor at MIT demonstrated that two enormously important problems can be solved in a faster, efficient manner with a quantum computer:

- Finding prime factors for a very large integer
- The Discrete Logarithm Problem

People in Cryptography realized then that this can break most of the encryption systems in seconds when in a hacker's hands. Most security systems like our credit cards use the Rivest-Shamir-Adleman (RSA) Encryption, and one of the sole foundations on which this encryption relies is the fact that a very large number cannot be prime factorized fast enough. To give you a little context, in order for us to crack RSA, we need to find the two coprime factors of a very large number, which now can be done in seconds with Shor's Algorithm, which used to take many years for a hacker on a classical computer since we don't have a proper efficient algorithm on classical computers.

10. **Grover's Search Algorithm:** In 1995, Lov Grover solved yet another interesting problem: "conducting a search through some unstructured search space" using a quantum computer efficiently.

**Note:** These algorithms haven't been covered yet in this book at the time of writing this report. That said, the recent video by *3Blue1Brown* does help in building some intuition around Grover's Search. Ironically though, and I say this as a loyal follower, I feel it might just be his least intuitive video to date, but some may disagree: *Watch here*

11. **Feynman's Quantum Simulation Insight:** Richard Feynman had suggested this in 1982. Feynman had pointed out that there seemed to be essential difficulties in simulating quantum mechanical systems on classical computers, and suggested that building computers based on the principles of quantum mechanics would allow us to avoid those difficulties. This indeed turned out to be true, as shown by many researchers in the 1990s.
12. **Classical Intuition Warning:** One of the main key insights the authors of the book pose is that when you try to design an algorithm for a quantum computer, there is one thing you should do: turn classical intuition "off".
13. **Shannon's Information Theory:** Claude Shannon in 1948 laid out the future for information when he proposed his two theorems: noiseless channel communication and noisy channel with error codes. But this is for classical systems. Is there a quantum analogue to this?

14. **Schumacher's Quantum Information Theory:** In 1995, Ben Schumacher proposed a quantum analogue to Shannon's noiseless coding theorem and also defined a "qubit".
15. **Classical Bits vs Qubits:** In classical computers, computation is done on bits, the binary number system is at the heart of classical computation, allowing arithmetic and logical operations. A classical *bit* can be either a 0 or a 1. A similar quantum analogue that Schumacher proposed is the quantum bit or 'qubit'. But they are not at all the same. At any point in time, we can tell the state of a classical bit with 100% certainty, but a qubit, on the other hand, is in a superposition of the  $|0\rangle$  and  $|1\rangle$  states. This notation is called Dirac notation, usually used to describe a quantum state.
16. **Abstract Approach to Qubits:** In this beginning part of the book at least, an intuition of qubits hasn't been posed by the authors, but they've taken rather an abstract approach towards qubits to evaluate their help in building a much more universal theory. The authors pose an open question that still a better quantum analog to qubit might be built someday, or the qubits which we are dealing with today might be the state of the art that nature gives us.

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

Here  $\psi$  is a qubit. Here  $\alpha$  and  $\beta$  are the *amplitudes*.  $|\alpha|^2 + |\beta|^2 = 1$ . Amplitude squared is the probability that the qubit is in that state.

17. **Quantum Measurement:** The act of observation collapses a quantum system from a superposition of states into a single outcome, a phenomenon at the heart of the *measurement problem* in quantum mechanics. This remains one of the most puzzling and debated aspects of the field. Astrophysicist Neil deGrasse Tyson offers an intuitive take on this in a short podcast clip: *Watch here*.

18. **Bloch Sphere Representation:**  $|\psi\rangle = e^{i\gamma} \left( \cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle \right)$

Here  $\gamma$ ,  $\theta$ , and  $\phi$  belong to  $\mathbb{R}$ . We can neglect the  $e^{i\gamma}$  term here since the contribution towards its probability is anyway going to be nullified.

19. **Bloch Sphere Visualization:** The numbers  $\theta$  and  $\phi$  define a point on the unit three-dimensional sphere. This sphere is often called the Bloch sphere, it provides a useful means of visualizing the state of a single qubit.

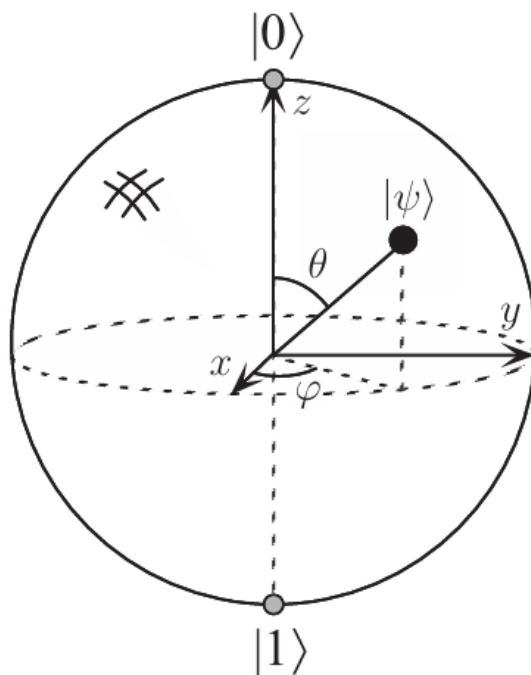


Figure 1: Bloch sphere representation of a qubit<sup>[1]</sup>

Bloch representation for multi-qubit systems has not been developed properly yet.

#### Point to Ponder

A single classical bit can carry 1 unit of information. Two classical bits can represent  $2^2 = 4$  possible states. In general,  $n$  bits can represent  $2^n$  distinct configurations.

Then, how many units of information can a qubit carry?

20. Paradoxically, there are infinitely many points on the surface of the unit sphere (the Bloch sphere), so in principle, one could encode an enormous even infinite amount of information in a qubit's continuous parameters (like  $\theta$  and  $\phi$ ). You could theoretically store all of Netflix in the infinite binary expansion of just one angle!

However, this idea is misleading. When a qubit is measured, it yields only a single bit of information either 0 or 1. Even more mysteriously, measurement collapses the state, destroying the rich quantum information in superposition and leaving only a classical outcome.

But why does measurement behave this way? *Nobody knows*. So instead... it became a **postulate** of quantum mechanics (See the quote by *Paul Dirac* on title page).

## Point to Ponder

Can we estimate the values of  $\alpha$  and  $\beta$  (i.e., the amplitudes in a qubit state like  $\alpha|0\rangle + \beta|1\rangle$ ) by simply measuring the *same* qubit again and again?

Does the law of large numbers help us here?

21. No, we cannot determine  $\alpha$  and  $\beta$  by measuring the same qubit repeatedly. Once a qubit is measured, it collapses to either  $|0\rangle$  or  $|1\rangle$ . Further measurements on the same qubit just repeat the same result with 100% certainty, they provide no new information.
22. However, if we have the ability to **prepare multiple identical copies** of the same qubit (say, in the state  $\alpha|0\rangle + \beta|1\rangle$ ), then measuring each copy individually *once* and aggregating the results does allow us to estimate  $|\alpha|^2$  and  $|\beta|^2$  via the law of large numbers.
23. Its important to note that this is not cloning, we are preparing identical copies because we know the state. In contrast, cloning an **unknown** quantum state is a completely different thing in quantum mechanics and it is fundamentally forbidden.
24. The **No-Cloning Theorem** is so central to preserving the consistency of quantum theory and relativity. This video explains and proves the no-cloning theorem in a nice manner: No-cloning theorem

The same math is worked here:

Suppose we have a quantum state  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ , and we want to clone it using a unitary operation  $U$ . We assume that the cloning machine acts as:

$$U|\psi\rangle \otimes |0\rangle = |\psi\rangle \otimes |\psi\rangle$$

Now take a superposition of both as an input to test this:

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

Apply  $U$  on this:

$$U|\psi\rangle|0\rangle = U\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle\right) = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$$

But if cloning were possible, we would expect:

$$|\psi\rangle \otimes |\psi\rangle = \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) \otimes \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$



Finally,

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \neq \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

So the cloning transformation cannot be linear and unitary (more on this soon), which every valid quantum operation must be. **Hence, perfect cloning of unknown quantum states is impossible.**

### Why Cloning Would Break Physics: Faster-than-Light Communication

Imagine two people, **Alice** and **Bob**, share an entangled pair of qubits in the Bell state:

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

Alice holds one qubit, and Bob holds the other, far away (say, on Mars).

Now, suppose Bob has a **cloning machine** that can perfectly clone any arbitrary quantum state, even unknown ones.

**Step-by-step:**

- Alice decides to measure her qubit in either the  $|0\rangle, |1\rangle$  (computational) basis or the  $|+\rangle, |-\rangle$  (Hadamard) basis. (*more on this later*)
- Her measurement instantly collapses the entangled state, affecting Bobs qubit nonlocally.
- If Bob could **clone** his qubit into many copies, he could perform quantum state tomography (by measuring in many bases) to determine the state *precisely*.
- From this, Bob could infer *which basis Alice used* even though no classical information has been transmitted.
- Thus, Alice would be able to send a bit of information to Bob *instantly*, just by choosing a measurement basis.

**Why this is a problem:** This communication would happen **faster than light**, violating the principle of causality in special relativity. No signal should propagate faster than light, yet cloning would make this possible.

**Conclusion:** To preserve causality and prevent such paradoxes, **quantum mechanics forbids cloning of arbitrary unknown quantum states.**

## Multiple Qubit Systems

25. Suppose we have two qubits,

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

here note that the notation  $|01\rangle$  means that qubit-1 is in  $|0\rangle$  state, and qubit-2 is in the  $|1\rangle$ , now suppose say we have measured the qubit-1, and say it turned out to be  $|1\rangle$ , then the second qubit will be in a new state  $|\psi'\rangle$ .

$$|\psi\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

here  $\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}$  factor is used to normalise the  $|\psi'\rangle$  state.

26. Another interesting 2-qubit system is the **Bell State** or **EPR Pair**:

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

If one qubit is measured, the result of the second qubit is instantly known even if it's far away. For example, if the first qubit is found to be  $|0\rangle$ , the second must be  $|0\rangle$ ; if it's  $|1\rangle$ , the other is also  $|1\rangle$ . Yet, before measurement, neither qubit has a definite value, only the entangled whole has meaning.

27. It turns out that other types of measurements can be performed on the Bell state, by first applying some operations to the first or second qubit, and that interesting *correlations* still exist between the result of a measurement on the first and second qubit.

## A brief intro to Quantum Circuits and Gates

One of the ways this book works is that it first, poses a classical computer related concept, and then providing a Quantum analogue, if it exists, else poses that as a open question for Physicists in future.

28. Classical computers are able to perform arithmetic and logical operations using different combinations and configurations of logic gates. The simplest logic gate in classical computation is the NOT gate, which takes a single bit input and flips it.

Now, can we have a quantum analogue of this a QUANTUM NOT gate? One of the first things that comes to mind is that a qubit has no fixed or certain state, it exists in a superposition of the two basis states, say  $|0\rangle$  and  $|1\rangle$ , with probabilities  $|\alpha|^2$  and

$|\beta|^2$  respectively. Then, what sense does it make to think about a **QUANTUM NOT** gate acting on a qubit  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ ?

A **QUANTUM NOT** gate, also called the **X-gate** or **Pauli-X gate**, acts on a qubit by flipping its amplitudes:

$$\alpha|0\rangle + \beta|1\rangle \xrightarrow{\boxed{X}} \beta|0\rangle + \alpha|1\rangle$$

29. This gate can be understood as a matrix operation on the qubit vector  $|\psi\rangle$ .

The Quantum NOT gate is represented by the **Pauli-X matrix**:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Let the qubit state be:

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

Then the action of the gate is:

$$X|\psi\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$$

30. **Definition:** A **Unitary Operator**  $U$  is a linear operator that satisfies the condition:

$$U^\dagger U = I$$

where  $U^\dagger$  is the Hermitian conjugate (conjugate transpose) of  $U$ , and  $I$  is the identity matrix. This condition ensures that the transformation preserves the total probability (i.e., quantum state remains normalized).

31. **Definition: Reversibility** means that given the output of an operation, we can always recover the input uniquely. This is important in quantum computing because all quantum gates must be reversible, as unitary operators are by definition reversible.

**Example:** A classical **OR** gate is not reversible. If we get an output of 1, we cannot determine whether the input was (1,0), (0,1), or (1,1). So multiple inputs give the same output, making it impossible to reverse the computation.

## Point to Ponder

We can observe that the QUANTUM NOT gate is a linear operation. Is it necessary for a Quantum Gate to be a linear operation? What will happen if they are allowed to be non-linear?

Is there a constraint on what quantum gates are realisable? For example, in classical computation, for a single bit, the only gate we can have is the NOT gate, which flips the state of the input bit. But for a single qubit, we can have multiple gates, since we can realise them as  $2 \times 2$  matrices with complex entries. It seems we can have an infinite number of quantum gates for a single qubit system, right?

32. There is a constraint on what quantum gates we can have. The quantum gate we construct should be such that the final output state still satisfies the condition for a qubit, that the total probability should be 1. This can be taken care of mathematically by putting a constraint on our gate operator matrix  $U$  that it must be unitary, as defined earlier.
33. For the very same reason we can't have a non-linear quantum gate. It will never be a unitary operation.
34. But suppose we could have an operator which is non-linear in real life, then it will have the following implications:
  - Time travel is possible
  - Faster-than-light communication is possible with entanglement
  - Second law of thermodynamics is invalid
  - No-cloning theorem is invalid. Cloning can indeed be made possible, which is shown in the below section.

## What is entanglement by the way again?

This video by Veritasium - Derek Muller explains entanglement in a simple manner:

*Quantum Entanglement & Spooky Action at a Distance*

## Recall the Second Law of Thermodynamics

***In any spontaneous process, the total entropy of an isolated system always increases or remains constant.***

Why this will be rendered invalid because of non-linearity is not discussed.

### Why Cloning Is Possible If Non-Linear Operators Are Allowed in QM

Recall from the **No-Cloning Theorem** <sup>pt.24</sup> that for an unknown quantum state

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

it is **impossible** to construct a linear unitary operator  $U$  such that:

$$U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$$

for all  $\alpha, \beta \in \mathbb{C}$ , due to the failure of linearity when applied to superpositions.

For example:

$$U\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle\right) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

but

$$\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) \otimes \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

are **not equal**, violating linearity.

**However**, if we *drop the constraint of linearity*, we could define a hypothetical **non-linear operator**  $M$  such that:

$$M(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$$

for *any*  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ .

This is mathematically possible if  $M$  behaves non-linearly, for instance:

$$M(\alpha|0\rangle + \beta|1\rangle \otimes |0\rangle) = (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)$$

which clearly depends quadratically on the input coefficients  $\alpha, \beta$ , violating linearity but achieving perfect cloning.

Thus, to preserve the consistency of quantum theory and the structure of space-time, only **linear, unitary** transformations are allowed ruling out any possibility of such non-linear cloning operations.

35. A few more important quantum gates are the **Pauli Gates** and the **Hadamard Gate**. These gates are fundamental in quantum computing, representing simple but powerful operations on single qubits.


- **Pauli-X Gate (NOT gate)**

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \Rightarrow X |\psi\rangle = \alpha |1\rangle + \beta |0\rangle$$

Quantum Circuit: 


- **Pauli-Y Gate**

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \Rightarrow Y |\psi\rangle = -i\beta |0\rangle + i\alpha |1\rangle$$

Quantum Circuit: 


- **Pauli-Z Gate**

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \Rightarrow Z |\psi\rangle = \alpha |0\rangle - \beta |1\rangle$$

Quantum Circuit: 

- **Hadamard Gate (H)**

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \Rightarrow H |\psi\rangle = \frac{1}{\sqrt{2}} [(\alpha + \beta) |0\rangle + (\alpha - \beta) |1\rangle]$$

Quantum Circuit: 

36. Another important notion in classical computing is the concept of **universal gates**, with these gates alone we can realise any digital circuit we want. Two of the main Universal gates are the **NOR** and the **NAND** gates. With these gates we can realise any digital function.
37. But what makes these gates universal? Why are the other logic gates like **OR**, **AND**, **XOR** not universal? A very interesting way to look at this is posed in the book by the authors. That is through the concept of parity again, being an electrical engineer, this concept hit me fresh. The **OR**, **AND**, **XOR** gates *preserve parity*, while **NOR** and the **NAND** gates do not preserve the parity, it makes them universal. But why does preservation of parity make the logic operator non-universal?
38. When a gate preserves parity, it means that the parity of the output is directly linked to the parity of the input. So if the number of ones in the input is even or odd, the output follows a fixed pattern accordingly. This symmetry restricts the kinds of transformations the gate can perform, and hence the set of logical functions that can

be generated from such gates is limited. On the other hand, when a gate does not preserve parity, like in the case of **NAND** and **NOR**, it can break this symmetry and thus explore a wider range of logical functions. This flexibility is what makes such gates universal, because they can be combined in various ways to construct all possible truth tables.

39. Again recall what we have discussed earlier <sup>pt.31</sup>, the usual digital logic gates like **OR**, **AND**, **XOR**, or even the universal ones like **NAND** and **NOR** are not *reversible gates*, i.e. we can't determine the set of inputs which caused the visible output alone. If these operators are not *reversible*, then we cannot realise them in a quantum computer right? Then what can we do? The gates that we call as universal gates are themselves not realisable in quantum gates? Then it seems we can't have a scalable quantum circuit easily too right?
40. So, we cannot directly implement a quantum circuit which realises these gates, we need a rather indirect approach to this. It turns out that we can build almost any arbitrary quantum gate using a finite set of quantum gates as good enough approximations.

**But what do we mean by approximations here?** In quantum computing, the state space is continuous, and the set of possible unitary operations is uncountably infinite. However, a remarkable result known as the *Solovay Kitaev theorem* tells us that we do not need an infinite set of quantum gates to approximate any desired unitary operation. A finite set of quantum gates (like Hadamard, CNOT <sup>pt.42</sup> gates) is said to be *universal* if any unitary operation can be approximated to arbitrary precision using only a sequence of these gates. This means we may not reproduce a gate exactly, but we can get arbitrarily close to its effect on any quantum state, which is sufficient for computation. More on this later

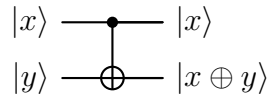
41. Also note that **NOR** and **NAND** are not the only universal gates in classical computing. Any combination of gates that is able to realise **NAND** or **NOR** will also be a universal gate when combined. For example, a  $4 \times 1$  multiplexer (MUX) is also a universal gate. This is illustrated very well in the following link: [Multiplexers as Universal Gates](#)

It might be possible that similar approximate alterations like this MUX are *reversible*, which can indeed make a *Quantum Universal Gate*.

42. **CNOT (Controlled-NOT) Gate:** CNOT gates are two-qubit gates. They have a *control* qubit, say  $x$ , and a *target* qubit, say  $y$ . The CNOT gate flips the target qubit (i.e., applies an  $X$  gate) if and only if the control qubit is in the state  $|1\rangle$ .

**Matrix Representation:**

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

**Quantum Circuit Representation:****43. Universal Quantum Gate Set:**

*Any multiple-qubit logic gate may be composed from a combination of CNOT gates and single-qubit gates.*

Proof for this is skipped for now.

**44. XOR Swap Algorithm:**

One of the most famous algorithms in digital electronics, although not widely used due to its time complexity, is the *XOR Swap Algorithm*. This algorithm allows us to swap the values of two variables using only XOR operations, without the need for a temporary variable.

---

**Algorithm 1** XOR Swap Algorithm

---

**Require:** Two classical bits or variables  $a$  and  $b$

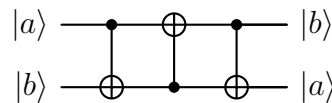
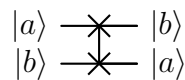
$b \leftarrow a \oplus b$

$a \leftarrow a \oplus b$

$b \leftarrow a \oplus b$

**Ensure:** The values of  $a$  and  $b$  are swapped

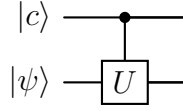
---

**Quantum Circuit for XOR Swap (Realized using 3 CNOT gates):****SWAP Gate Representation:****45. Controlled- $U$  Gate:**

The Controlled- $U$  gate is a generalization of the CNOT gate, where instead of applying the Pauli- $X$  (NOT) gate conditionally, we apply an arbitrary unitary gate  $U$  to the target qubit, depending on the control qubit's state.

Circuit representation:





It applies the unitary operator  $U$  to the second qubit only if the control qubit  $|c\rangle$  is  $|1\rangle$ .

46. A few things allowed in classical circuits are not allowed in quantum circuits:

- **No Loops:** Quantum circuits are *acyclic*, meaning we do not allow feedback loops from the output of one gate back to the input of another.

*Why?* Because quantum evolution must follow a clear, time-ordered progression through unitary operations. Feedback breaks this order and is incompatible with unitary evolution (see *II Postulate of Quantum Mechanics* <sup>pt.58</sup>).

- **No FANIN:** Classical circuits allow FANIN, where multiple wires are joined together, often combining signals via logical OR.

*Why?* This operation is not reversible, hence not allowed in quantum circuits which require all gates to be reversible (unitary) <sup>pt.30</sup>.

- **No FANOUT:** Classical circuits allow FANOUT, where the same bit is copied to multiple wires.

*Why?* Quantum mechanics forbids the copying of an arbitrary unknown quantum state due to the **no-cloning theorem** <sup>pt.24</sup>.

47. **Hilbert Space:** A Hilbert space is a complete vector space with an inner product, used to represent quantum states. For example, a single qubit lives in a 2-dimensional Hilbert space spanned by basis vectors  $\{|0\rangle, |1\rangle\}$ . It allows us to define lengths, angles, and perform operations like superposition and measurement.

48. **Bell Basis:** The Bell basis is a set of four maximally entangled two-qubit states that form an orthonormal basis for the two-qubit Hilbert space. These are:

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

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

49. **What is Bell Measurement:** A Bell measurement is a projective quantum measurement in the Bell basis. It involves measuring two qubits and determining which of

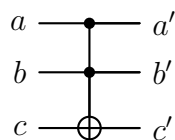
the four Bell states they are in. This measurement effectively projects the two-qubit system onto one of the four entangled states. We can use this concept to understand *Quantum Teleportation*.

50. **Quantum Teleportation** is posed as a very good example on Pg. 26 in section 1.3.7 of book<sup>[1]</sup>. I'd suggest reading it from there itself, but a rough summary is given below:

- Quantum teleportation is a protocol that allows the transfer of an **unknown quantum state** from one location (Alice) to another (Bob), **without physically transmitting** the particle itself.
- The process relies on **shared entanglement**: Alice and Bob must share an entangled pair (e.g., a Bell state <sup>pt.26</sup>) at the beginning.
- Alice performs a **Bell basis measurement** on her qubit and the unknown qubit she wants to teleport. This projects Bobs entangled qubit into a related state.
- Alice sends **two classical bits** to Bob, communicating the result of her measurement. Bob then applies a suitable **Pauli operation** based on those bits to recover the original state.
- **Limitation**: Although the quantum state is transferred, the requirement of **classical communication** prevents faster-than-light transmission of information, thereby preserving *causality* and respecting relativity.

51. As we have discussed earlier, any classical circuit can be replaced by an equivalent circuit containing only **reversible elements** <sup>pt.31</sup>, by making use of a reversible gate known as the **Toffoli gate**. It has three inputs and three outputs:

- Two are **control bits**, which remain unchanged.
- The third is a **target bit**, flipped **only when both control bits are 1**.



$$\text{Toffoli}(a, b, c) = (a, b, c \oplus (a \cdot b))$$

The Toffoli gate applied twice to a set of bits has the effect of returning the bits to their original state, and thus the Toffoli gate is a reversible gate since it is its own inverse.

$a$	$b$	$c$	$a'$	$b'$	$c'$
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	<b>1</b>
1	1	1	1	1	<b>0</b>

Truth Table for Toffoli Gate

## Quantum Parallelism

52. Quantum parallelism allows quantum computers to evaluate a function  $f(x)$  for multiple values of  $x$  simultaneously, using superposition, here's how:

- First, we have to prepare the input register in a superposition (e.g., using Hadamard gates), then apply the unitary transformation  $U_f$  defined by  $|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$ .
- For example, let's take  $f(x) : \{0, 1\} \rightarrow \{0, 1\}$  is a function with a one-bit domain and range, starting with  $(|0\rangle + |1\rangle)/\sqrt{2}$  and applying  $U_f$  gives  $(|0, f(0)\rangle + |1, f(1)\rangle)/\sqrt{2}$ , effectively encoding both function values in one quantum state.

$$U_f \left( \frac{(|0\rangle + |1\rangle)}{\sqrt{2}} \right) = \frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}$$

So, we have both  $f(0)$  and  $f(1)$  in a superposition, where multiple circuits each built to compute  $f(x)$  are executed simultaneously, here a single  $f(x)$  circuit is employed to evaluate the function for multiple values of  $x$  simultaneously, by exploiting the ability of a quantum computer to be in superpositions of different states.

- More generally, apply  $H^{\otimes n}$  on  $|0\rangle^{\otimes n}$  to get a superposition over all  $x \in \{0, 1\}^n$ , then apply  $U_f$  to get:

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle$$

- But, measurement yields only one value  $x, f(x)$ . So quantum parallelism alone doesn't give the full picture. What can we do about this?

So we need better strategies to exploit the power of quantum parallelism.

53. This can be achieved by using the *Deutsch Algorithm* and its more general version, the *Deutsch Jozsa Algorithm*. These are not discussed in this report, as they have been covered in detail in the book, considering their length, but here's the logic which makes us overcome this problem of only being able to determine  $f(x)$  for a single  $x$  value:

These algorithms cleverly use interference patterns in quantum states to amplify desirable outcomes and cancel out others. This allows us to extract **global properties** of the function  $f(x)$ , such as whether it is constant or balanced (outputs 0 for exactly half of the inputs and 1 for the other half), **without having to evaluate every input individually**, something that is infeasible for classical computers in exponential input sizes.

Note that in *pt.* 52, we wanted to evaluate  $f(0)$  and  $f(1)$ , but in *pt.* 53, using the *Deutsch algorithm*, we are rather trying to answer the question of whether they are **equal or not**. It might seem like an irrelevant question to answer, even the authors mention the same thing in the book, but the reason we went through this algorithm is that the same problem is solved more efficiently on a quantum computer than on a classical one.

#### Exercise: Classical Probabilistic Algorithm

**Question:** Suppose the goal is not to distinguish between constant and balanced functions with certainty, but rather with error probability less than  $\frac{1}{2}$ . What is the performance of the best classical algorithm?

**Answer:** A classical algorithm can query the function at random inputs. If it sees both 0 and 1 as outputs, the function is balanced. If it sees only 0 or only 1, it guesses the function is constant. In the worst case for a balanced function, all outputs seen are identical. The probability of this happening with say some  $k$  queries is  $(1/2)^{k-1}$ . Thus, with just 2 queries, the error probability becomes  $\frac{1}{2}$ , and for error strictly less than  $\frac{1}{2}$ , at least 3 queries are needed. We can see that the error decreases exponentially with the number of queries.

54. **Quantum Algorithms using Fourier Transform:** The Discrete Fourier Transform (DFT) is a method that takes a list of  $N$  complex numbers  $x_0, x_1, \dots, x_{N-1}$  and transforms it into another list of complex numbers  $y_0, y_1, \dots, y_{N-1}$ , where each output  $y_k$  is defined as:

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i j k / N} x_j$$

This transformation is extremely powerful and widely used in physics, engineering, and computer science. In many situations, the Fourier-transformed version of a problem becomes much easier to handle or solve than its original form.

55. In the classical case, computing the Fourier transform of  $N = 2^n$  values typically takes about  $N \log N = n2^n$  steps. But on a quantum computer, the same task can be done in just  $\log^2 N = n^2$  steps. This results in an **exponential speedup**, which is one of the major strengths of the Quantum Fourier Transform (QFT). The complete explanation and details of QFT are not covered yet.

56. **Computational Complexity Classes:**

- **P:** Problems solvable in polynomial time by a classical deterministic computer.
- **NP:** Problems whose solutions can be verified in polynomial time by a classical deterministic computer.

- **PSPACE:** Problems solvable with polynomial space (memory), regardless of the time taken.
- **BPP:** Problems solvable by a probabilistic classical computer in polynomial time with bounded error.
- **BQP:** Problems solvable by a quantum computer in polynomial time with bounded error (quantum version of BPP).

### 57. Why This Classification Matters in Quantum Computing:

- It helps us understand what problems quantum computers can solve more efficiently than classical ones.
- Algorithms like Shors and Grovers demonstrate that some problems in BQP may lie outside P and even BPP.
- Comparing BQP with NP and PSPACE gives us an understanding the true potential and limits of quantum computing.

### 58. The Postulates of Quantum Mechanics

- **Postulate 1 (State Space):** Every isolated physical system is associated with a complex vector space (Hilbert space) with an inner product. The system is completely described by a unit vector  $|\psi\rangle$  in this space.
- **Postulate 2 (Unitary Evolution):** The evolution of a closed quantum system is described by a unitary transformation. If the state at time  $t_1$  is  $|\psi\rangle$ , then at time  $t_2$ , the state becomes:

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

where  $U$  is a unitary operator that depends only on  $t_1$  and  $t_2$ .

- **Postulate 2' (Schrödinger Equation):** Alternatively, the time evolution of a closed quantum system is given by the Schrödinger equation:

$$i\hbar \frac{d}{dt}|\psi\rangle = H|\psi\rangle$$

where  $H$  is the Hamiltonian operator of the system.

- **Postulate 3 (Measurement):** Quantum measurements are described by a set  $\{M_m\}$  of measurement operators acting on the system's state space. The probability of outcome  $m$  when measuring a state  $|\psi\rangle$  is:

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

After the measurement, the state collapses to:

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

The operators satisfy the completeness relation:

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

ensuring that total probability is 1.

- **Postulate 4 (Composite Systems):** The state space of a composite system is the tensor product of the state spaces of its subsystems. If systems 1 through  $n$  are in states  $|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_n\rangle$ , then the joint state is:

$$|\psi_1\rangle \otimes |\psi_2\rangle \otimes \dots \otimes |\psi_n\rangle$$

## 59. Distinguishing Quantum States:

Another important application of *III Postulate of Measurement* in quantum mechanics is the problem of distinguishing quantum states. In the classical world, different states of a system can usually be distinguished. For example, we can always find out whether a coin has landed heads or tails, at least in the ideal case.

In the quantum world, as usual things are more complicated. In Section 1.6 of the book<sup>[1]</sup>, a basic argument was given by the authors that non-orthogonal quantum states cannot be distinguished. But now with the help of the *III Postulate*, we can give a much stronger explanation of why that is true.

Let's consider a simple game between Alice and Bob. Alice chooses a state  $|\psi_i\rangle$  (where  $1 \leq i \leq n$ ) from a known set of states and gives it to Bob. Bob's task is to find out the index  $i$  of the state he received.

If the states  $|\psi_i\rangle$  are orthonormal, then Bob can perform a quantum measurement that perfectly distinguishes the states. This is done by defining measurement operators  $M_i = |\psi_i\rangle\langle\psi_i|$  for each index  $i$ , and an additional operator  $M_0$  which is the positive square root of  $I - \sum_i |\psi_i\rangle\langle\psi_i|$ . These operators satisfy the completeness condition. If Alice sends  $|\psi_i\rangle$ , then the measurement result  $i$  happens with certainty. So orthonormal states can always be distinguished.

But if the states are not orthonormal, then there is no quantum measurement that can always tell them apart. Bob can perform a measurement with outcomes  $j$ , and then use a rule  $i = f(j)$  to guess the original state. The problem is that a state like

$|\psi_2\rangle$  may have a component along  $|\psi_1\rangle$ . So if Bob sees an outcome  $j$  that makes him guess  $|\psi_1\rangle$ , it might still happen that  $|\psi_2\rangle$  caused it, due to their overlap. This leads to a chance of error.

### Proof that Non-Orthogonal States Cannot Be Perfectly Distinguished

Let us assume, for contradiction, that such a perfect measurement exists. If  $|\psi_1\rangle$  or  $|\psi_2\rangle$  is prepared, then the probability of measuring the corresponding index must be 1. Define  $E_i = \sum_{j:f(j)=i} M_j^\dagger M_j$ . Then we must have:

$$\langle\psi_1| E_1 |\psi_1\rangle = 1 \quad \text{and} \quad \langle\psi_2| E_2 |\psi_2\rangle = 1$$

Now, since the operators must sum to identity, we get:

$$\sum_i \langle\psi_1| E_i |\psi_1\rangle = 1$$

And because  $\langle\psi_1| E_1 |\psi_1\rangle = 1$ , we must also have  $\langle\psi_1| E_2 |\psi_1\rangle = 0$ , which implies  $\sqrt{E_2} |\psi_1\rangle = 0$ .

Now write  $|\psi_2\rangle = \alpha |\psi_1\rangle + \beta |\phi\rangle$ , where  $|\phi\rangle$  is orthogonal to  $|\psi_1\rangle$  and  $|\alpha|^2 + |\beta|^2 = 1$ , with  $|\beta| < 1$  because the states are not orthogonal.

Then:

$$\sqrt{E_2} |\psi_2\rangle = \beta \sqrt{E_2} |\phi\rangle \Rightarrow \langle\psi_2| E_2 |\psi_2\rangle = |\beta|^2 \langle\phi| E_2 |\phi\rangle \leq |\beta|^2 < 1$$

This contradicts our earlier assumption that  $\langle\psi_2| E_2 |\psi_2\rangle = 1$ , so our assumption must be wrong.

**Therefore, non-orthogonal states cannot be perfectly distinguished.**

### 60. Projective Measurements:

- A **projective measurement** is described by an **observable**  $M$ , which is a Hermitian operator acting on the state space of the system.
- The observable  $M$  has a spectral decomposition:

$$M = \sum_m m P_m$$

where  $P_m$  is the projector onto the eigenspace corresponding to eigenvalue  $m$ .

- The possible measurement outcomes are the eigenvalues  $m$  of  $M$ .
- If the system is in state  $|\psi\rangle$ , then the probability of obtaining the outcome  $m$  upon measurement is:

$$p(m) = \langle\psi| P_m |\psi\rangle$$

- Given that outcome  $m$  occurs, the post-measurement state collapses to (*somewhat similar analysis as in pt.25 of Multiple Qubit Systems*):

$$\frac{P_m |\psi\rangle}{\sqrt{p(m)}}$$

Projective measurements are a special case of *III Postulate*. If the measurement operators  $M_m$  satisfy:

- The completeness relation:  $\sum_m M_m^\dagger M_m = I$
- And if each  $M_m$  is a Hermitian projector:  $M_m^2 = M_m$ , and  $M_m M_{m'} = \delta_{m,m'} M_m$

then the measurement defined in *III Postulate* reduces to a projective measurement.

### Properties of Projective Measurements:

- Projective measurements allow easy calculation of averages. The average (or expected) value of an observable  $M$  for a system in state  $|\psi\rangle$  is:

$$\langle M \rangle = \sum_m m p(m) = \sum_m m \langle \psi | P_m | \psi \rangle = \langle \psi | M | \psi \rangle$$

- The standard deviation  $\Delta(M)$  of measurement results of observable  $M$  is defined as:

$$[\Delta(M)]^2 = \langle (M - \langle M \rangle)^2 \rangle = \langle M^2 \rangle - \langle M \rangle^2$$

Standard equation we see in statistics, this idea further stems towards *Heisenberg's Uncertainty Principle*, that has been skipped here.

### 61. *Can we send two classical bits of information be transmitted using just one qubit?*

**Superdense coding** says we can! It is an interesting application of the *III Postulate of Measurement* provided that the sender and receiver share an entangled pair.

- Alice and Bob initially share a Bell pair:  $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ .
- To send two classical bits, Alice applies one of four Pauli operations (I, X, Z, Y) on her qubit depending on the 2-bit message.
- She then sends her qubit to Bob.
- Bob performs a Bell basis measurement on the two qubits and learns the 2-bit message.
- Thus, one qubit physically transmitted = two classical bits communicated.



## References

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

## Further Plan of Action

Due to the upcoming intern season and other academic commitments, I have had to scale down my initial plans slightly. However, I am still keen to conclude this season with a practical implementation and comparative study of two foundational quantum algorithms: **Bernstein-Vazirani** and **Grovers Algorithm**. This would allow me to meaningfully extend the project beyond a purely reading-based exploration. I intend to complete this work according to the following timeline:

- **Week 5: Simulation of Bernstein-Vazirani Algorithm**
  - Study the working principles of the Bernstein-Vazirani algorithm.
  - Implement the algorithm using Qiskit.
  - Test the implementation for various hidden strings.
  - Analyze and visualize the circuit and output using measurement histograms.
- **Week 6: Simulation of Grover's Algorithm**
  - Study the structure and working of Grover's Algorithm for unstructured search.
  - Implement Grover's algorithm using Qiskit.
  - Validate the probability of measuring the correct solution.
  - Visualize the quantum circuit and compare outcomes with the classical approach.
- **Week 7: Comparative Analysis and Final Report**
  - Write a detailed report summarizing both algorithms.
  - Include circuit diagrams, measurement outputs, and key observations.
  - Provide a comparative table discussing efficiency, use-cases, and quantum speedup.
  - Submit the final report in PDF format along with annotated code and GitHub repository link.

If time permits, and I really hope it does, one of my main interests is to at least get a birds-eye view on how quantum circuits are implemented in real life, atleast a Toffoli gate.