An Introduction to Quantum Computing

Suhas P K

Department of Physics,
AMCEC

Contents

1 Introduction **3**
1.1 What you'll learn? . . . 3
1.2 Ket spaces . . . 3
1.3 Inner Product Space . . . 5

2 Wave Function in Ket Notation **6**
2.1 Understanding wave function. . . . 6
2.2 Linear Operators . . . 6
2.3 Identity Operator . . . 6
2.4 Qubits! . . . 6
2.5 Special States . . . 7
2.5.1 Schrödinger's cat . . . 7
2.5.2 Implications . . . 8
2.6 Identity operator and qubit . . . 8
2.7 Pauli matrices . . . 8
2.8 Unitary and Hermitian Matrices . . . 8
2.8.1 Unitary Matrices . . . 8
2.8.2 Hermitian Matrices . . . 8
2.9 Probability . . . 9

3 Principles of Quantum Information & Quantum Computing **10**
3.1 Moore's Law . . . 11
3.2 Difference between Classical and Quantum computing . . . 12
3.3 Quantum superposition . . . 12

4 Properties of a qubits **12**
4.1 Mathematical representation . . . 12
4.2 Representation of qubit by Bloch sphere . . . 13
4.3 Quantum computation . . . 14

5 Quantum Gates **14**
5.1 Single qubit gates . . . 14
5.1.1 Quantum Gates Basic . . . 16
5.2 Multi Qubit System . . . 18
5.2.1 Multi-Qubit gates . . . 18
5.2.2 Single vs Multi Qubits . . . 19
5.2.3 Multiple Qubits and **CNOT** Gate . . . 19
5.2.4 Controlled Z gate . . . 20
5.2.5 SWAP Gate . . . 20
5.2.6 Toffoli gate . . . 21

6 WARNING! **22**

1 Introduction

The objective of this module is to give a brief introduction to the Quantum Computing and its mathematical structure. Most of the concepts in quantum mechanics are highly mathematical and thought experimental. For example take "*Teleportation*", the key understanding of the quantum superposition makes us understand teleportation, even better if one can understand the linear algebra, and ket notations the concept can be appreciated even more.
Rest assured, even though these concepts are highly mathematical, this is an experimental attempt to make the topics easily understanding for beginners.

1.1 What you'll learn?

In this section, you will be introduced to **Linear Vector Spaces**. Familiarity with the *arrow notations* to represent vectors and vector spaces from elementary physics is one way to understand both magnitude and direction. But you will appreciate the *ket notations* better when we try to incorporate matrices to describe the system in the ket notations, which saves a lot of time.
Throughout this document, our to go notation to represent vectors will bra-ket notation, developed by P. A. M. Dirac. The theory of linear vector spaces had been known to mathematicians prior to the birth of quantum mechanics, but Dirac's way of introducing vector spaces has many advantages.

1.2 Ket spaces

We consider a **complex vector space** whose dimensionality is specified according to the nature of a physical system under consideration. In quantum mechanics, a physical state is represented by a **state vector** in a complex vector space. We represent it of the form $|\alpha\rangle$, where is some state in a complex vector space.

Definition 1. A linear vector space $\mathbb{V}$ is a collection of objects $|1\rangle, |2\rangle, ..., |V\rangle, ..., |W\rangle$ called vectors, for which there exists

1. A definite rule for forming the vector sum $|V\rangle + |W\rangle$.
2. A definite rule of multiplication by scalar, $a, b, c, \cdot$ denoted $a|V\rangle$ with the following features:
   - The result of these operations is another element of the space, a feature called *Closure*:$|V\rangle + |W\rangle \in \mathbb{V}$.
   - Scalar multiplication is distributive in the vectors: $a(|V\rangle + |W\rangle) = a|V\rangle + a|W\rangle$.
   - Scalar multiplication is distributive in the scalars: $(a+b)|V\rangle = a|V\rangle + b|V\rangle$.
   - Scalar multiplication is associative: $a(b|V\rangle = ab|V\rangle$.
   - Addition is commutative: $|V\rangle + |W\rangle = |W\rangle + |V\rangle$.
   - Addition is associative: $|V\rangle + (|W\rangle + |Z\rangle = |V\rangle + |W\rangle + |Z\rangle)$.
   - There exists a null vector $|0\rangle$ obeying $|V\rangle + |0\rangle = |V\rangle$.
   - For every vector $|V\rangle$ there exists an inverse under addition, $|-V\rangle$, such that $|V\rangle + |-V\rangle = |0\rangle$.

Definition 2. The numbers $a, b, ...$ are called the field over which the vector space is defined. If the field consists of all real numbers, we have a *real vector space*, if they are complex, we have a *complex vector space*.
Note that the above axioms imply

- $|0\rangle$ is unique, i.e., if $|0'\rangle$ has all the properties of $|0\rangle$, then $|0\rangle = |0'\rangle$.
- $0|V\rangle = |0\rangle$.
- $|-V\rangle = |V\rangle$.
- $|-V\rangle$ is the unique additive inverse of $|V\rangle$.

Definition 3. The set of vectors is said to be linearly independent if the only such linear relation as

$$\sum_{i=1}^{n} a_i |i\rangle = |0\rangle \tag{1}$$

is a trivial one with all $a_i = 0$. If the set of vectors is not linearly independent, we say they are *linearly dependent*.

Definition 4. A vector space has *dimension n* if it can accommodate a maximum of n linearly independent vectors. It will be denoted by $\mathbb{V}^n(R)$ if the field is real and by $\mathbb{V}^n(C)$ if the field is complex.
Note: Any vector $|V\rangle$ in an n-dimensional space can be written as a linear combination of n linearly independent vectors.

Definition 5. A set of n linearly independent vectors in a n-dimensional space is called a *basis*. Thus, based on the above definition

$$|V\rangle = \sum_{i=1}^{n} v_i |i\rangle \tag{2}$$

where the vectors $|i\rangle$ form a basis.

Definition 6. The coefficients of expansion v_i of a vector in terms of a linearly independent basis $|i\rangle$ are called the components of the vector in that basis.

1.3 Inner Product Space

Definition 7. A vector space with an inner product is called an inner product space.
It is denoted by $\langle V|W\rangle$ and we demand that it obey the following axioms:

- $\langle V|W\rangle = \langle W|V\rangle^*$ (skew symmetric)
- $\langle V|V\rangle \geq 0$ 0 if and only if $|V\rangle = |0\rangle$ (positive semidefiniteness)
- $\langle V|(aW\rangle + b|Z\rangle) \equiv \langle V|aW + bZ\rangle = a\langle V|W\rangle + b\langle V|W\rangle$ (linearity in ket)

Note:

$$\langle aW + bZ|V\rangle = \langle V|aW + bZ\rangle^* \tag{3}$$

Definition 8. We say that two vectors are orthogonal or perpendicular if their inner product vanishes.

$$\langle V|W\rangle = 0 \tag{4}$$

Definition 9. We will refer to $\sqrt{\langle V|V\rangle} \equiv |V|$ as the norm or length of the vector. A normalizes vector has a unit norm.
Definition 10. A set of basis vectors all of unit norm, which are pairwise orthogonal, will be called an orthonormal basis.

$$\langle i|i\rangle = 1 \tag{5}$$

Note: Frequently, the inner or scalar product will be referred as dot product.
Given $|V\rangle$ and $|W\rangle$,

$$|V\rangle = \sum_i v_i |i\rangle \; and \; |W\rangle = \sum_j w_j |j\rangle$$

we follow the axioms obeyed by the inner product to obtain:

$$\langle V|W\rangle = \sum_i \sum_j v_i^* w_j \langle i|j\rangle \tag{6}$$

Condition for Kronecker delta:

$$\langle i|j\rangle \equiv \delta_{ij} = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{if } i \neq j. \end{cases} \tag{7}$$

For $i = j$ condition,

$$\langle V|W\rangle = \sum_i v_i^* w_i \tag{8}$$

This is called "the double sum collapses to a single one due to the Kronecker delta."
We can appreciate the first axiom more if we consider our components to be complex numbers. If the components are complex, then

$$\langle V|V\rangle = \sum_i |v_i|^2 \geq 0 \tag{9}$$

Since, the vector $|V\rangle$ is uniquely specified by its components in a given basis, we may, in this basis, write it as a column vector:

$$|V\rangle = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} \tag{10}$$

and

$$|W\rangle = \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} \tag{11}$$

The inner product $\langle V|W\rangle$ is given by the matrix product of the transpose conjugate of the column vector representing $|V\rangle$ with the column vector representing $|W\rangle$:

$$\langle V|W\rangle = \begin{bmatrix} v_1^* & v_2^* & \dots & v_n^* \end{bmatrix} \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} \tag{12}$$

2 Wave Function in Ket Notation

2.1 Understanding wave function.

Now, using the above definitions, we use the relation to describe the quantum state that the particle is in,

$$|\psi\rangle = \sum_i \phi_i |i\rangle \tag{13}$$

This abstract relation becomes in this basis,

$$|\psi\rangle = \begin{bmatrix} \phi_1 \\ \phi_2 \\ \vdots \\ \phi_n \end{bmatrix} = \phi_1 \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \phi_2 \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} + \dots + \phi_n \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} \tag{14}$$

Note: In this section $|\phi\rangle$ and $|\psi\rangle$ is used, as it more of a traditional approach to use ψ to represent any wavefunction and ϕ, its components.

2.2 Linear Operators

An operator $\hat{A}$ is an instruction for transferring any vector $|V\rangle$ into another, $|V'\rangle$. The action of the operator is represented as follows:

$$\hat{A}|V\rangle = |V'\rangle \tag{15}$$

2.3 Identity Operator

The simplest operator is the identity operator, I, which carries the instruction:

$$I \longrightarrow \text{"Leave the vector alone!"}$$

(Joke source : *Principles of Quantum Mechanics, R. Shankar*)
Thus,

$$I|V\rangle = |V\rangle \; and \; \langle V|I = \langle V| \tag{16}$$

2.4 Qubits!

The bit is the fundamental concept of classical computation and classical information. Quantum computation and quantum information are built upon an analogous concept, the quantum bit, or qubit for short.
For the most part, we treat qubits as abstract mathematical objects. The beauty of treating qubits as abstract entities is that it gives us the freedom to construct a general theory of quantum computation and quantum information which does not depend upon a specific system for its realization.
To make use of the definitions again, let use consider a linear vector space made of complex element. Specifically, two dimension complex linear vector space $\mathbb{C}^2$.
Now that we have established that the two-dimensional complex linear vector space is the one that we will be working with, we will use the classical notations to represent the wavefunction $|\psi\rangle$.
This $|\psi\rangle$ can be written in terms of linear combination of linearly independent basis vector. It can be represented of the form:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{17}$$

where, α and β are complex in nature.
Note: For two-dimensional Complex linear vector space, there exists 2 linearly independent basis vectors. Using the above equation, we can store binary information in $|0\rangle$ and $|1\rangle$ in the same time. The discussion can be extrapolated for multiple qubits and storing the classical bit information in the multiple qubits. But for now, let us restrict ourselves to two qubits and make our life less complicated.
If a quantum states represents of this (17) format, then they are said to be in superposition.
And the special states $|0\rangle$ and $|1\rangle$ are known as computational basis states, and form an orthonormal basis for this vector space.

2.5 Special States

As we already mentioned, special states like $|0\rangle$ and $|1\rangle$ are known as computational basis states, and form an orthonormal basis for this vector space, and we can store binary information in $|0\rangle$ and $|1\rangle$ in the same time. But how can that be represented?
Be hold!

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \textit{and} \, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{18}$$

With is new information, we can represent some quantum state $|\psi\rangle$ as,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{19}$$

To interpret this expression even more, one needs to understand the infamous thought experiment meme, **"Schrödinger's cat"**.

2.5.1 Schrödinger's cat

In quantum mechanics, Schrödinger's cat is a thought experiment that illustrates a paradox of quantum superposition. In the thought experiment, a hypothetical cat may be considered simultaneously both alive and dead as a result of its fate being linked to a random subatomic event that may or may not occur.

> One can even set up quite ridiculous cases. A cat is penned up in a steel chamber, along with the following device (which must be secured against direct interference by the cat): in a Geiger counter, there is a tiny bit of radioactive substance, so small, that perhaps in the course of the hour one of the atoms decays, but also, with equal probability, perhaps none; if it happens, the counter tube discharges and through a relay releases a hammer that shatters a small flask of hydrocyanic acid. If one has left this entire system to itself for an hour, one would say that the cat still lives if meanwhile no atom has decayed. The first atomic decay would have poisoned it. The psi-function of the entire system would express this by having in it the living and dead cat (pardon the expression) mixed or smeared out in equal parts.

Then, the wavefunction $|\psi\rangle$ which determines the state whether the cat is dead or alive in the closed box, can be represented of the form

$$(|\psi\rangle)_{\text{closed box}} = |alive\rangle + |dead\rangle$$

2.5.2 Implications

Since Schrödinger's time, other interpretations of quantum mechanics have been proposed that give different answers to the questions posed by Schrödinger's cat of how long superposition last and when (or whether) they collapse.

- Copenhagen interpretation
- Von Neumann–Wigner interpretation
- Bohr's interpretation
- Many-worlds interpretation

and the list goes on!

2.6 Identity operator and qubit

As we have already discussed how the Identity operator works, let use try to understand what happens if the identity operator, operates on the computational basis.
The Identity operator is represented by,

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{20}$$

Now, the following steps are trivial.

$$I\,|0\rangle = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle \tag{21}$$

Do try for $|1\rangle$ also!

2.7 Pauli matrices

In mathematical physics and mathematics, the Pauli matrices are a set of three 2×2 complex matrices which are Hermitian, involuntary and unitary.
In further sections, we will discuss what does Hermitian and Unitary mean.

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\ \sigma_y = \begin{bmatrix} 0 & -i \\ +i & 0 \end{bmatrix} \text{ and } \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{22}$$

These matrices place a very important role in quantum mechanics and in quantum computation.

2.8 Unitary and Hermitian Matrices

2.8.1 Unitary Matrices

In linear algebra, a complex square matrix U is **Unitary** if its conjugate transpose U^* is also its inverse. Mathematically, the representation can be as follows:

$$(U^*)U = U(U^*) = I \tag{23}$$

2.8.2 Hermitian Matrices

A Hermitian matrix is a matrix that is equal to its conjugate transpose. Mathematically, a Hermitian matrix A is defined as

$$A = (\overline{A})^T = A^\dagger \tag{24}$$

2.9 Probability

For a particle in some quantum state *ket*ψ, can be written as a linear combination of orthonormal basis vectors, which can be represented of the form,

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ **Note:** We are considering only a state made up of two orthonormal basis vectors.

Now, we cannot precisely tell where the particle exists. So, we calculate the probability of finding the particle in that particular state. Mathematically, this can be calculated by,

$$P(|\psi\rangle) = |\langle\psi|\psi\rangle|^2 = 1, \quad \textbf{Note: } P(|\psi\rangle) \text{ is the probability.} \tag{25}$$

Further, if the quantum state is not normalized, we can use this relation to normalize.

3 Principles of Quantum Information & Quantum Computing

Quantum information is problem-solving and data processing using a quantum system as the information carrier, rather than binary '1's and '0's used in conventional computation. Quantum information, like classical information, can be processed using digital computers, transmitted from one location to another, manipulated with algorithms, and analyzed with computer science and mathematics. Just like the basic unit of classical information is the bit, quantum information deals with qubits.Quantum information systems could be able to transmit data that is fundamentally secure and solve problems that are beyond the power of modern computers.

It is an interdisciplinary field that involves quantum mechanics, computer science, information theory, philosophy, and cryptography among other fields. Information is something physical that is encoded in the state of a quantum system. While quantum mechanics deals with examining properties of matter at the microscopic level, quantum information science focuses on extracting information from those properties, and quantum computation manipulates and processes information – performs logical operations – using quantum information processing techniques.

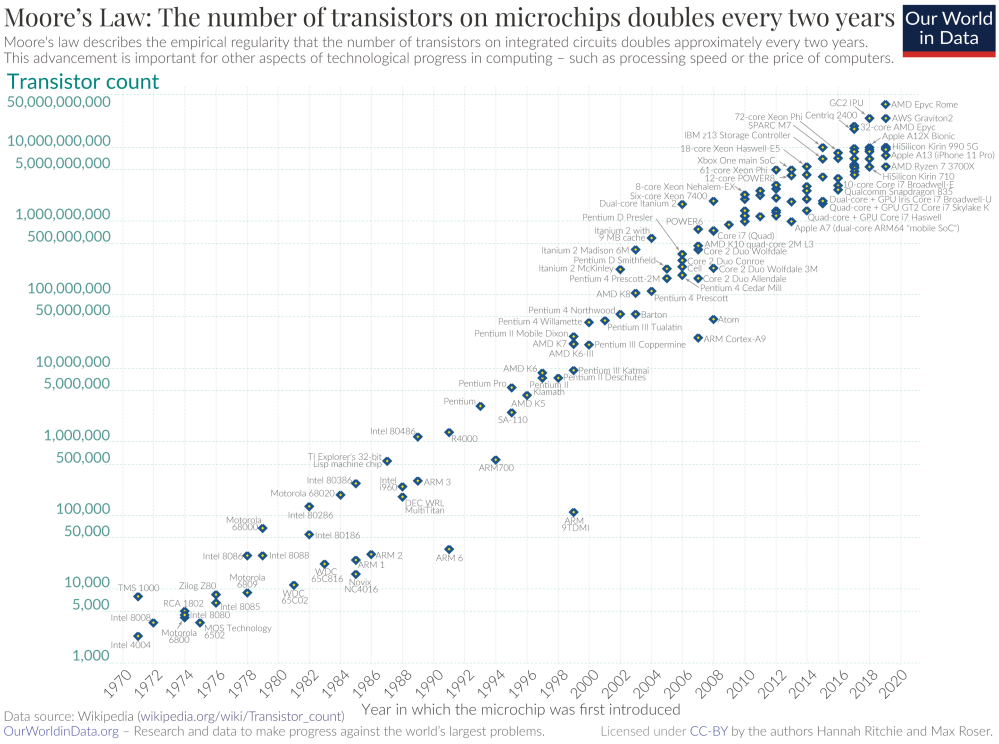
Quantum information, like classical information, can be processed using digital computers, transmitted from one location to another, manipulated with algorithms, and analyzed with computer science and mathematics. Just like the basic unit of classical information is the bit, quantum information deals with qubits.

3.1 Moore's Law

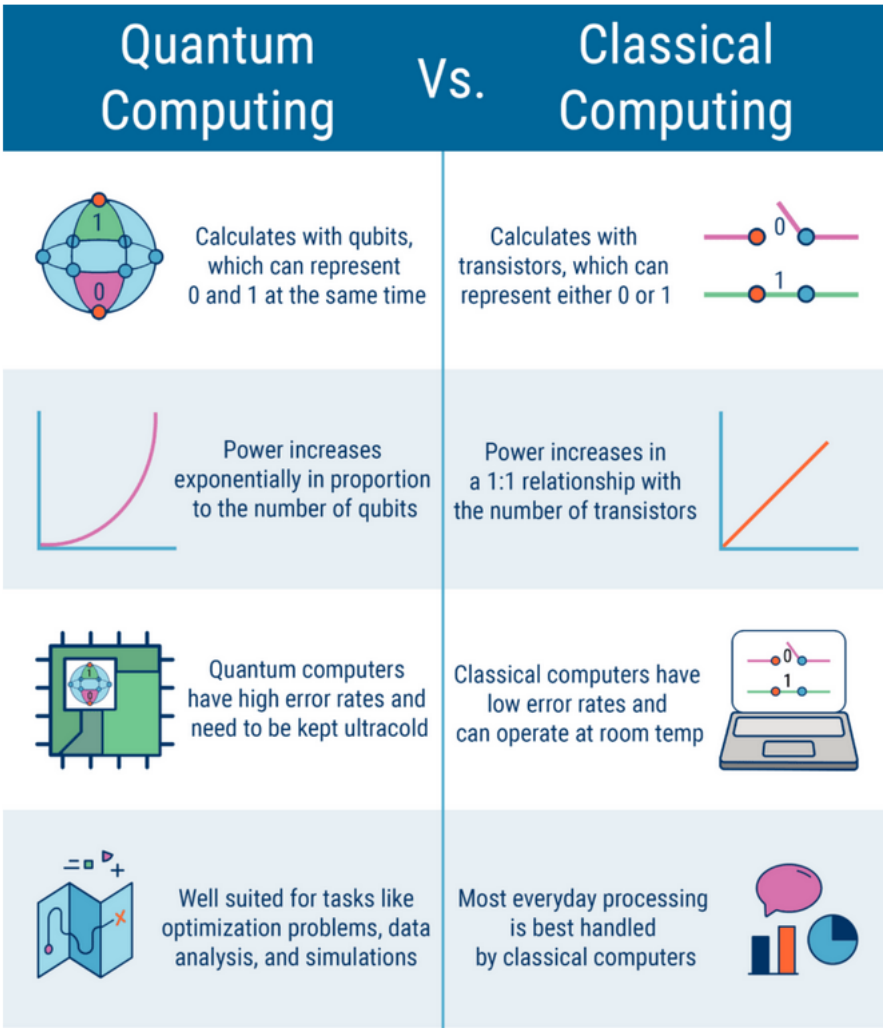
Moore's Law is an observation that the number of transistors in a computer chip doubles every two years or so. As the number of transistors increases, so does process power. The law also states that,

> "As, the number of transistors in a dense integrated circuit (IC) doubles about every two years, the cost per transistor falls. So not only will the processing power of computer chips grow exponentially, but the cost per transistor will also decline exponentially."

For the past five decades, Moore's Law has accurately predicted developments in computer technology. In the 55 years since Moore first made his prediction, processors have gone from 3,500 transistors per chip to close to 50B.But this law will likely hit a wall eventually. At a certain point, transistors will become so small that the effects of quantum physics will prevent them from functioning properly. When Moore's Law comes to an end, there may be a severe slowdown in computer hardware growth, which has some computer scientists and economists worried.



3.2 Difference between Classical and Quantum computing



3.3 Quantum superposition

Quantum superposition is a fundamental principle of quantum mechanics. It states that, much like waves in classical physics, any two (or more) quantum states can be added together ("superposed") and the result will be another valid quantum state; and conversely, that every quantum state can be represented as a sum of two or more other distinct states.

4 Properties of a qubits

4.1 Mathematical representation

Consider a coin toss. Once the coin is tossed in the air, let's say an invisible cloak, masks the coin. Based on this situation, we can store the coin toss result information in this format,

$$result = \begin{bmatrix} heads \\ tails \end{bmatrix}$$

As the tossed coin is masked by the invisibility cloak, if the result of the coin toss is heads, then this information will be represented in the form,

$$result(heads) = |0\rangle = \begin{bmatrix} heads = 1 \\ tails = 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \tag{26}$$

Else, if the result of the coin toss is assumed to be tails, then the information of this result will be stored in the format,

$$result(tails) = |1\rangle = \begin{bmatrix} heads = 0 \\ tails = 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Note: There is very particular reason why we use these notations and representation. Based on this type of matrix notation, we can store much information in concise and understandable format.

Now that you have gone through the topics := Special states, Schrödinger's cat and Qubits!, we can apply these concepts for the coin toss problem. So, the information of the overall result, of the coin toss can be represented in the form,

$$\text{Total result} = \text{result (heads)} + \text{result (tails)} = |0\rangle + |1\rangle = \begin{bmatrix} heads = 1 \\ tails = 0 \end{bmatrix} + \begin{bmatrix} heads = 0 \\ tails = 1 \end{bmatrix}$$

or, simply a quantum superposed state,

$$|\psi\rangle = \begin{bmatrix} heads = 1 \\ tails = 0 \end{bmatrix} + \begin{bmatrix} heads = 0 \\ tails = 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{27}$$

So, now we can say that the result of the coin toss is a superposed state. This information of the coin toss which is represented by the above equation can be referred as 1 qubit.

Note: $|\psi\rangle$ is not normalized. You can do it as a small exercise.

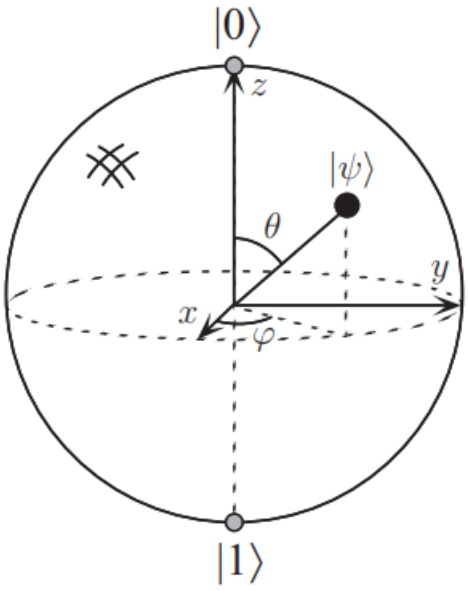
If the invisibility cloak is unmasked, and I observe the result of the coin toss is heads, then the result of the above equation will be of the form,

$$\text{invisibility cloak unmasked}(|\psi\rangle) = \begin{bmatrix} heads = 1 \\ tails = 0 \end{bmatrix} + \cancel{\begin{bmatrix} heads = 0 \\ tails = 1 \end{bmatrix}} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \cancel{\begin{bmatrix} 0 \\ 1 \end{bmatrix}}$$

The act of unmasking the invisibility cloak is called an act of measurement.

4.2 Representation of qubit by Bloch sphere

Naturally, a great deal of attention has been given to the 'meaning' or 'interpretation' that might be attached to superposition states, and of the inherently probabilistic nature of observations on quantum systems. However, by and large, we shall not concern ourselves with such discussions. Instead, our intent will be to develop mathematical and conceptual pictures which are predictive. One picture useful in thinking about qubits is the following geometric representation.



$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{28}$$

where, α and β are complex numbers and obey the conditions $|\alpha|^2 + |\beta|^2 = 1$. For the context of our coin toss experiment, $\alpha = \frac{1}{\sqrt{2}}$ and $\beta = \frac{1}{\sqrt{2}}$ from which we can say what is the probability of the exact result of the coin toss. This can be written in a more generalized and in a more complicated form. But the equation that I am about to give you will be a life changing equation. Behold!

$$|\psi\rangle = e^{i\gamma}(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle) \tag{29}$$

where, θ, ϕ and γ are real numbers. Later on we will get to know that the term $e^{i\gamma}$ will not have any observable effects.
Thus, the expression will be reduced to,

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle \tag{30}$$

The number θ and ψ define a point on the unit three-dimensional sphere. The above sphere is often called the **Bloch sphere**; it provides a useful means of visualizing the state of a single qubit, and often serves as an excellent test-bed for ideas about quantum computation and quantum information.

4.3 Quantum computation

Changes occurring to a quantum state can be described using the language of quantum computation. Analogous to the way a classical computer is built from an electrical circuit containing wires and logic gates, a quantum computer is built from a quantum circuit containing wires and elementary quantum gates to carry around and manipulate the quantum information. In this section we describe some simple quantum gates, and present several example circuits illustrating their application, including a circuit which teleports qubits!

5 Quantum Gates

5.1 Single qubit gates

Classical computer circuits consist of wires and logic gates. The wires are used to carry information around the circuit, while the logic gates perform manipulations of the information, converting it from one form to another. Consider, for example, classical single bit logic gates.
The only non-trivial member of this class is the **NOT** gate, whose operation is defined by its truth table, in which $0 \rightarrow 1$ and $1 \rightarrow 0$, that is, the 0 and 1 states are interchanged.
Imagine that we had some process which took the state $|0\rangle$ to the state $|1\rangle$, and vice versa. Such a process would obviously be a good candidate for a quantum analogue to the **NOT** gate. However, specifying the action of the gate on the states $|0\rangle$ and $|1\rangle$ does not tell us what happens to the superpositions of the states $|0\rangle$ and $|1\rangle$, without further knowledge about the properties of quantum gates. In fact, the quantum **NOT** gate acts linearly, that is, it takes the state

$$\alpha|0\rangle + \beta|1\rangle \tag{31}$$

to the corresponding state in which the role of $|0\rangle$ and $|1\rangle$ have been interchanged,

$$\alpha|1\rangle + \beta|0\rangle \tag{32}$$

Note: It turns out that this linear behavior is a general property of quantum mechanics, and very well motivated empirically; moreover, nonlinear behavior can lead to apparent paradoxes such as time travel, faster than-light communication, and violations of the second laws of thermodynamics.
There is a convenient way of representing the quantum **NOT** gate in matrix form, which follows directly

from the linearity of quantum gates. Suppose we define a matrix X to represent the quantum gate as follows:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{33}$$

If the quantum state $\alpha|0\rangle + \beta|1\rangle$ is written in a vector notation as

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} \tag{34}$$

, with the top entry corresponding to the amplitude for $|0\rangle$ and the bottom entry the amplitude for $|1\rangle$, then the corresponding output from the quantum **NOT** gate is

$$X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix} \tag{35}$$

Notice that the action of the gate is to take the state $|0\rangle$ and replace it by the state corresponding to the first column of the matrix X. Similarly, the state $|1\rangle$ is replaced by the state corresponding to the second column of the matrix X. So quantum gates on a single qubit can be described by 2×2 matrices.
Are there any constraints on what matrices may be used as quantum gates?
It turns out that there are.
Recall that the normalization condition requires $|\alpha|^2 + |\beta|^2 = 1$ for a quantum state $\alpha|0\rangle + \beta|1\rangle$. This must also be true of the quantum state, $|\psi'\rangle = \alpha'|0\rangle + \beta'|1\rangle$ after the gate has acted.
It turns out that the appropriate condition on the matrix representing the gate is that the matrix U describing the single qubit gate be unitary, that is $U^\dagger U = I$, where $U^\dagger$ is the adjoint of U (obtained by transposing and then complex conjugating U), and I is the 2×2 identity matrix. For example, for the gate, it is easy to verify that $X^\dagger X = I$.
Amazingly, this unitarity constraint is the only constraint on quantum gates. Any unitary matrix specifies a valid quantum gate! The interesting implication is that in contrast to the classical case, where only one non-trivial single bit gate exists—the **NOT** gate-there are many non-trivial single qubit gates. Two important one which we need to study is Z gate:

$$Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{36}$$

which leaves $|0\rangle$ unchanged, and flips the sign of $|1\rangle$ to give $-|1\rangle$, and the **Hadamard** gate,

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{37}$$

$$\underset{\text{initial state}}{\alpha|0\rangle + \beta|1\rangle} \longrightarrow \boxed{X} \longrightarrow \alpha|1\rangle + \beta|0\rangle$$

$$\underset{\text{initial state}}{\alpha|0\rangle + \beta|1\rangle} \longrightarrow \boxed{Z} \longrightarrow \alpha|0\rangle - \beta|1\rangle$$

$$\underset{\text{initial state}}{\alpha|0\rangle + \beta|1\rangle} \longrightarrow \boxed{H} \longrightarrow \alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

Recalling the Pauli matrices, we treat these matrices as gates.

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\ \sigma_y = \begin{bmatrix} 0 & -i \\ +i & 0 \end{bmatrix} \text{and } \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{38}$$

Similar to the X-gate, which is analogous to the classical **NOT**-gate. The σ_y is the Y-gate and σ_z is the Z-gate.
To understand the above huge load of information, let us understand in summarized way.

5.1.1 Quantum Gates Basic

The Pauli Z-gate Operation

- The state vector of a qubit can be represented as two orthogonal vectors.
- The state vector of a qubit can be represented as two orthogonal vectors. $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.
- Represented by Pauli Z-matrix $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.
- It's a phase shift gate, sometime called **phase-flip**. Rotating around the Z-axis of the Bloch sphere by π radians.
- It leaves the basis state $|0\rangle$ unchanged and maps to $|1\rangle$ to $-|1\rangle$.

Introduction to Hadamard H gate

- using only the Pauli-gates, we are now able to get only the states $|0\rangle$ and $|1\rangle$, similar to classical bit 1 or 0 ('ON' or 'OFF').
- To harness the power of Qubits, we must move away from the poles of the Bloch sphere and create a superposition.
- Represented by the Hadamard matrix $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.
- It will transform the state of the qubit between the X and Z bases, as a rotation around the Bloch vectors [1,0,1] (the line between the X and Z axes)
- Change the state $|0\rangle$ to $|+\rangle$ and $|1\rangle$ to $|-\rangle$,
  $H|0\rangle = |+\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$
  $H|1\rangle = |-\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$

$R\phi$-gate

- Using a number parameter (ϕ) to tell it to performs a rotation of ϕ around the Z-axis direction. (Where ϕ is a real number)
- It is also called as RZ-gate.
- The transformation matrix for $R\phi$ gate is $R_\phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}$.
- From $R\phi$-gate we get I, Z, S and T gates.

The S-gate and $S^\dagger$-gate

- S-gate is a $R\phi$ gate with $\phi = \frac{\pi}{2}$.
- S-gate is not its own inverse.
- Two S-gate together will give only a Z-gate equivalent.
- The $S^\dagger$ gate is a $R\phi$ with $\phi = \frac{-\pi}{2}$.
- The transformation matrix for S and $S^\dagger$ are $S = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{2}} \end{bmatrix}$, $S^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{-i\pi}{2}} \end{bmatrix}$.

The T-gate and $T^\dagger$-gate

- T-gate is a $R\phi$ gate with $\phi = \frac{\pi}{4}$.
- Two T-gate together will give only a Z-gate equivalent.
- The $T^\dagger$ gate is a $R\phi$ with $\phi = \frac{-\pi}{4}$.
- The transformation matrix for T and $T^\dagger$ are $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{bmatrix}$, $T^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{-i\pi}{4}} \end{bmatrix}$

General U-gate (U_3, U_2, U_1)

- U_3 gate is the generalized version of gates like X, Y, H gates.
- It's a parameterized form of $U_3(\theta, \phi, \lambda) = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -e^{i\lambda}\sin\left(\frac{\theta}{2}\right) \\ e^{i\phi}\sin\left(\frac{\theta}{2}\right) & e^{i(\lambda+\phi)}\cos\left(\frac{\theta}{2}\right) \end{bmatrix}$
- Also there are U_2 and U_1 gates which are also U_3 gate with $\theta = \frac{\pi}{2}$, $\theta = 0$ and $\phi = 0$ respectively.

  $U_3(\frac{\pi}{2}, \phi, \lambda) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -e^{i\lambda} \\ e^{i\phi} & e^{i(\lambda+\phi)} \end{bmatrix}$

  $U_3(0, 0, \lambda) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i(\lambda)} \end{bmatrix}$

5.2 Multi Qubit System

5.2.1 Multi-Qubit gates

- Single qubits offer no computational advantage. Interaction between qubits is the true power of quantum computing.
- Gates directly implemented in hardware will act only on one or two qubits. With those gates, it is possible to build any other gate.
- A single bit has two possible states, 0 and 1.
- A qubit has two states, $|0\rangle$ and $|1\rangle$ and complex amplitude. Two bits have four possible states: 00, 01, 10 and 11.
- Like that, two qubits requires four complex amplitudes to represent its states.
- For the two separates qubits, we can describe their collective state using the tensor product:

$$|a\rangle = \begin{bmatrix} a_o \\ a_1 \end{bmatrix}, \quad |b\rangle = \begin{bmatrix} b_o \\ b_1 \end{bmatrix}$$

$$|ba\rangle = |b\rangle \otimes |a\rangle = \begin{bmatrix} b_o \times \begin{bmatrix} a_o \\ a_1 \end{bmatrix} \\ b_1 \times \begin{bmatrix} a_o \\ a_1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} b_o a_o \\ b_o a_1 \\ b_1 a_o \\ b_1 a_1 \end{bmatrix} \tag{39}$$

- Can you guess how many complex amplitudes are required to represent a three qubit state ?

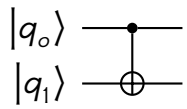
5.2.2 Single vs Multi Qubits

- Generally, if we have n qubits, we will need to keep track of 2^n complex amplitudes to describe their states.
- A modern classical computer can easily simulate a general quantum state of around 20 qubits.
- **Example:** If only one gate is applied to a 2 qubit circuit, we can do its tensor product with the identity matrix.

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

5.2.3 Multiple Qubits and CNOT Gate

- Performs a X-gate on the second qubit (called as target), if the states of the first qubit (called as CONTROL) is $|1\rangle$.



- Truth table of **CNOT** Gate when qubits are not entangled (Not in superposition).

Input (t,c)	Output (t,c)
00	00
01	11
10	10
11	01

- For the **CNOT** gate when the qubits are in entangled state, we change the basis states from $|0\rangle$,$|1\rangle$ to $|+\rangle$ and $|-\rangle$. By applying, the Hadamard gate to $|0\rangle$ and $|1\rangle$, the basis states changes to $|+\rangle$ and $|-\rangle$.
- Applying the **CNOT** gate to the $|+\rangle$ end $|-\rangle$ states, say

$$CNOT\,|-+\rangle = \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle) = |--\rangle$$

- State of the target qubit unchanged, but control qubit changes.
- **CNOT** swaps the amplitudes of $|01\rangle$ and $|11\rangle$.
- It has 25% probability of being measured in the states $|00\rangle$,$|01\rangle$,$|10\rangle$, and $|11\rangle$.
- The Bloch sphere shows both the same because **CNOT** only interchanges the amplitudes of $|01\rangle$ and $|11\rangle$.

Initial States	Computational Basis	Apply operator	Resulting basis	Final state
$\|++\rangle$	$\frac{1}{2}(\|00\rangle + \|01\rangle + \|10\rangle + \|11\rangle)$	CNOT	$\frac{1}{2}(\|00\rangle + \|01\rangle + \|11\rangle + \|10\rangle)$	$\|--\rangle$
$\|+-\rangle$	$\frac{1}{2}(\|00\rangle - \|01\rangle + \|10\rangle - \|11\rangle)$	CNOT	$\frac{1}{2}(\|00\rangle - \|01\rangle + \|11\rangle - \|10\rangle)$	$\|--\rangle$
$\|-+\rangle$	$\frac{1}{2}(\|00\rangle + \|01\rangle - \|10\rangle - \|11\rangle)$	CNOT	$\frac{1}{2}(\|00\rangle + \|01\rangle - \|11\rangle - \|10\rangle)$	$\|-+\rangle$
$\|--\rangle$	$\frac{1}{2}(\|00\rangle - \|01\rangle - \|10\rangle + \|11\rangle)$	CNOT	$\frac{1}{2}(\|00\rangle - \|01\rangle - \|11\rangle + \|10\rangle)$	$\|++\rangle$

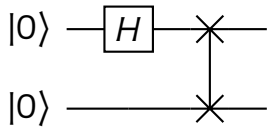
5.2.4 Controlled Z gate

- Just like **CNOT** applies X to target whenever control is 1.
- Like **CZ** applies Z to target whenever control is 1.

Input (t,c)	Output (t,c)
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|10\rangle$
$\|11\rangle$	$-\|11\rangle$

5.2.5 SWAP Gate

- **SWAP** gate is used to move the state between two qubits.
- The **SWAP** gate is represented as,

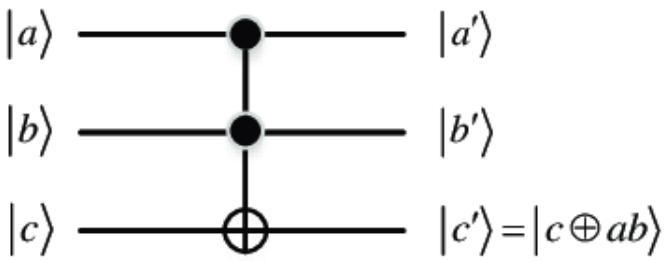


- In real Quantum computer,
  the only two-qubit gate that can be directly applied is the CNOT gate.
- So in order to get SWAP gate, we have to create identical circuit using CNOT gates.

5.2.6 Toffoli gate

- The Toffoli gate is a three qubit gate with two control and one target. It performs an X on the target only if both controls are in the state $|1\rangle$.
- It is controlled-controlled-NOT, and is also called the **CCX** gate.
- The truth table of the Toffoli gate is given by,

Inputs			Ouputs		
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	1
1	1	1	1	1	0



6 WARNING!

This document is more of a reference material. Detailed information is not provided in this document, as it requires rigorous mathematics. Please make your own notes so that you are comfortable with the concepts and notations. Apart from this document, the below listed sources are good options:

- Quantum Computing lecture series
- Moore's Law
- A Beginner's Guide to Quantum Computing