Week-1

Introduction to Quantum Computing: From Fundamentals to Quantum Algorithms

May 22, 2025

Why Linear Algebra for Quantum Computing?

$$\begin{tikzcd}
\text{Abstract Setting} \arrow[rr, leftrightarrow, "\text{Abstract Operation}"] \arrow[d, leftrightarrow, "\text{Matrix Vector Representation}"'] & & \text{Abstract Setting} \arrow[d, leftrightarrow, "\text{Matrix Vector Representation}"] \\
\text{Linear Algebra Setting} \arrow[rr, leftrightarrow, "\text{Linear Algebra Operation}"'] & & \text{Linear Algebra Setting}
\end{tikzcd}$$

Hilbert space and its meaning

- A Hilbert space is a complete complex vector space with an inner product, capable of representing all valid states of a quantum system.
- Note that once we define the quantum system, the Hilbert space is fixed. We might choose different representations (bases) inside that space, but the underlying structure doesn't change.
- This Hilbert space contains all possible states the system can be in.
- For a space to be termed as a Hilbert space it must follow the following constraints:
  - It must be a vector space over C, i.e. it must satisfy all vector space axioms like Additivity, Associativity, Distributivity, etc. over all complex numbers.
  - Inner product must be defined on that space.(We will later see what we mean by this)
  - It must be complete, i.e. every cauchy sequence of vectors in the space should converge to a vector in that space.
- Hilbert space itself is abstract, but it can be represented concretely once we choose a basis like position or momentum. Let's see what we mean by this in the next slide

State Vectors

- The standard quantum mechanical notation for a vector in a vector space is a ket denoted as $|\psi\rangle$
- $|\psi\rangle$ is the abstract notation of the state in the Hilbert space, i.e. it exists independently of any basis.
- We can represent it concretely using column vectors once we choose a discrete basis like energy (if it is quantized in a system), spin etc. or represent it using a wavefunction in the case of continuous basis like position, momentum, energy (if it takes continuous values in a system), etc.
- If a basis is chosen then both the representation become equivalent, i.e.

$$|\psi\rangle \equiv \begin{bmatrix} v_1 \\ v_2 \\ v_3 \\ . \\ . \\ v_n \end{bmatrix}$$

The intuition behind all the 'Abstract' talk

Let's take an analogy of the 3D vector space of real numbers [1] for a better understanding. The 3D coordinate space exists wheater or not we pick the x, y, z coordinate or not (showcasing its abstract nature), we can just represent our vectors using $\vec{v}$ (analogus to $|\psi\rangle$) but when we choose our basis as x, y and z direction then we can write it as $\vec{v} = a\vec{x} + b\vec{y} + c\vec{z}$ or as

$$\begin{bmatrix} a \\ b \\ c \end{bmatrix}$$

Now, different choice of bases will result in different column vectors but the vector we are trying to represent remains the same.

[1] In fact 3D real space itself qualifies as a Hilbert space as it satisfies all the necessary conditions for a vector space to be a Hilbert space. Hence, in this case $\mathcal{H} = \mathbb{R}^3$

Inner Product

- An inner product is a function that takes as input two vectors $|v\rangle$ and $|w\rangle$ from a vector space and produces a complex number as output. We represent inner product of $|v\rangle$ and $|w\rangle$ as $\langle v|w\rangle$. This is a standard way of representation.
- You have learnt that we can define inner product as per our requirement, but generally we define as a integral over Hilbert space of two state vectors with a weight factor.

$$\langle v|w\rangle = \int v^*(x)w(x)t(x)dx \tag{1}$$

  Where t is the weight factor. For example in cartesian coordinate t is just 1, but for spherical coordinate it is $r^2 sin\theta$.
- Going back to our 3D space analogy, this can be thought of as a dot product between 2 vectors.
- There are some noteworthy features of inner product which should be mentioned below.

Inner Product

- **Linearity in the second argument:**

$$\langle v | a w_1 + b w_2 \rangle = a \langle v | w_1 \rangle + b \langle v | w_2 \rangle$$

- **Conjugate symmetry:**

$$\langle v | w \rangle = \overline{\langle w | v \rangle}$$

- **Positive-definiteness:**

$$\langle v | v \rangle \geq 0, \quad \text{and} \quad \langle v | v \rangle = 0 \iff |v\rangle = 0$$

- **Orthogonality condition:**

$$\langle v | w \rangle = 0 \quad \text{if } |v\rangle \text{ and } |w\rangle \text{ are orthogonal}$$

Inner Product

- **Norm induced by the inner product:**

$$\|v\| = \sqrt{\langle v|v\rangle}$$

- **Cauchy–Schwarz inequality:**

$$|\langle v|w\rangle|^2 \leq \langle v|v\rangle \langle w|w\rangle$$

- **Triangle inequality:**

$$\|v + w\| \leq \|v\| + \|w\|$$

- **Projection of one vector onto another:**

$$\mathrm{proj}_w(v) = \frac{\langle w|v\rangle}{\langle w|w\rangle}|w\rangle$$

Outer Product

Definition: The outer product of two coordinate vectors is the matrix whose entries are all products of an element in the first vector with an element in the second vector. If the two coordinate vectors have dimensions n and m, then their outer product is an n $\times$ m matrix.

Key Uses in Quantum Mechanics:

- **Projection operator:**

$$P = |v\rangle\langle v|$$

  Projects any state onto —v$\rangle$.

- **Density matrix (pure state):**

$$\rho = |v\rangle\langle v|$$

- **Density matrix (mixed state):**

$$\rho = \sum_i p_i |v_i\rangle\langle v_i|$$

Outer Product

- **Operator construction:** Used in building Hamiltonians, observables, and quantum gates.
- **Measurement theory:** Appears in projective measurements and spectral decomposition.

Linear operators and its equivalent matrix representation

- Before moving forward I would like to mention that in quantum computing we generally take finite dimensional Hilbert space i.e. $\mathcal{H} = \mathbb{C}^n$
- Now, you all must have read about linear operators in both MA110 and PH110 and how it maps vectors from one vector space V to another vector space W. In PH110 you might have seen operators like momentum operator $\hat{P}$ or position operator $\hat{X}$.
- In QM you any operator $\hat{A}$ or A defined on a Hilbert space i.e. A : $\mathcal{H} \longrightarrow \mathcal{H}$
- Since we will be looking only at finite dimensional Hilbert space hence we can equivalently represent a linear operator as a matrix once a basis is chosen (As seen in MA110).
- As $\mathcal{H} = \mathbb{C}^n$, we can write any operator as a $n \times n$ matrix.

Orthonormalization

Suppose that we are given a spanning set for a vector space V containing the set of vectors $|v_1\rangle, |v_2\rangle, .., |v_n\rangle$. Such a set of vectors can be used as a basis for our vector space. Again going back to our 3D space analogy, such a set can be $\hat{x}, \hat{x} + \hat{y}, 4\hat{x} - \hat{z}$. But any such set need not be an orthonormal basis. But there is a very handy process through which we can turn any linearly independent set of vectors into an orthonormal set. Lets see how we can do this in the next slide.

Orthonormalization (contd.)

Goal: Convert a set of linearly independent vectors into an **orthonormal** set.

Definitions:

- **Orthogonal:** $\langle v_i | v_j \rangle = 0 \quad \text{for } i \neq j$
- **Normalized:** $\langle v_i | v_i \rangle = 1$
- **Orthonormal:** Both orthogonal and normalized:

$$\langle v_i | v_j \rangle = \delta_{ij}$$

Gram-Schmidt Process

Given: A set of linearly independent vectors $\{|u_1\rangle, |u_2\rangle, \ldots, |u_n\rangle\}$

Construct: An orthonormal set $\{|v_1\rangle, |v_2\rangle, \ldots, |v_n\rangle\}$

- Step 1: Normalize the first vector

$$|v_1\rangle = \frac{|u_1\rangle}{\||u_1\|}$$

- Step 2: Subtract projection and normalize

$$|v_2\rangle = \frac{|u_2\rangle - \langle v_1|u_2\rangle|v_1\rangle}{\||u_2\rangle - \langle v_1|u_2\rangle|v_1\rangle\|}$$

- Repeat for $|v_3\rangle, |v_4\rangle, \ldots$ similarly.

Adjoint of an Operator

- The adjoint of a linear operator A, denoted $A^\dagger$, is defined by:

$$\langle \phi | A\psi \rangle = \left\langle A^\dagger \phi \middle| \psi \right\rangle \quad \text{for all } |\phi\rangle, |\psi\rangle$$

- In matrix form:

$$A^\dagger = (\overline{A})^T \quad \text{(conjugate transpose)}$$

- Properties:
  - $(A^\dagger)^\dagger = A$
  - $(AB)^\dagger = B^\dagger A^\dagger$
  - $(\alpha A + \beta B)^\dagger = \overline{\alpha} A^\dagger + \overline{\beta} B^\dagger$
- Adjoint generalizes the concept of the transpose to complex inner product spaces.

Hermitian Operators

- A linear operator A is called **Hermitian** if:

$$A = A^\dagger$$

- Properties:
  - All eigenvalues of a Hermitian operator are real.
  - Eigenvectors corresponding to different eigenvalues are orthogonal.
  - Hermitian operators are diagonalizable.
- Significance in quantum mechanics:
  - Observables are represented by Hermitian operators.
  - Measurement outcomes are the eigenvalues of Hermitian operators.

Dual vector space

Definition:

- Given a complex vector space V, the **dual space** V^* is the set of all linear functionals:

$$V^* = \{f : V \to \mathbb{C} \,|\, f \text{ is linear}\}$$

- If $|v\rangle \in V$, then its corresponding dual vector (or bra) is $\langle v| \in V^*$.
- The dual vector $\langle v|$ maps any $|w\rangle \in V$ to a complex number:

$$\langle v|w\rangle \in \mathbb{C}$$

Dirac Notation:

- $|v\rangle$ is a column vector (in V), $\langle v|$ is its Hermitian adjoint (a row vector in V^*).
- Inner product: $\langle v|w|v|w\rangle = \langle v|w\rangle$

Dual Vector Space

Key Properties:

- If $\{|i\rangle\}$ is a basis for V, then $\{\langle i|\}$ is a dual basis for V^*:

$$\langle i|j\rangle = \delta_{ij}$$

- The mapping $V \to V^*$ given by $|v\rangle \mapsto \langle v| = |v\rangle^\dagger$ is conjugate-linear.
- The dual space V^* has the same dimension as V.

Examples

Ket vector: $|v\rangle = \begin{bmatrix} 1+i \\ 2 \end{bmatrix}$

Corresponding Bra:

$$\langle v| = (1-i,\ 2)$$

Inner Product Example:

$$\langle v|w\rangle = (1-i,\ 2) \cdot \begin{bmatrix} 3 \\ i \end{bmatrix} = (1-i)\cdot 3 + 2\cdot i = 3 - 3i + 2i = 3 - i$$

Matrix Multiplication View:

- $\langle v|w\rangle$ = row vector $\times$ column vector = scalar
- $|v\rangle\langle v|$ = column $\times$ row = matrix (a projector)

Tensor Products

Tensor product is a way of putting vector spaces together to form larger vector spaces. This construction is crucial for understanding the quantum mechanics of multiparticle systems.
Suppose V and W are vector spaces of dimension m and n respectively (assume they are Hilbert spaces).
Then $V \otimes W$ (read "V tensor W") is an mn-dimensional vector space.

Elements and Basis of the Tensor Product

The elements of $V \otimes W$ are linear combinations of "tensor products" $|\psi\rangle \otimes |\omega\rangle$ of elements $|\psi\rangle$ of V and $|\omega\rangle$ of W.
If $\{|i\rangle\}$ and $\{|j\rangle\}$ are orthonormal bases for V and W, then $\{|i\rangle \otimes |j\rangle\}$ is a basis for $V \otimes W$.
Abbreviated notations: $|\psi\rangle|\omega\rangle$, $|\psi, \omega\rangle$, or $|\psi\omega\rangle$.

Example: If V is 2D with basis $\{|0\rangle, |1\rangle\}$, then $|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$, $|1\rangle \otimes |1\rangle$ form a basis for $V \otimes V$.

Basic Properties of the Tensor Product

By definition, the tensor product satisfies the following properties:

$$
\begin{aligned}
&\text{For any scalar } z \text{ and elements } |\psi\rangle \in V, |\omega\rangle \in W: \\
&\quad z(|\psi\rangle \otimes |\omega\rangle) = (z|\psi\rangle) \otimes |\omega\rangle = |\psi\rangle \otimes (z|\omega\rangle) \\
&\text{For } |\psi_1\rangle, |\psi_2\rangle \in V, |\omega\rangle \in W: \\
&\quad (|\psi_1\rangle + |\psi_2\rangle) \otimes |\omega\rangle = |\psi_1\rangle \otimes |\omega\rangle + |\psi_2\rangle \otimes |\omega\rangle \\
&\text{For } |\psi\rangle \in V, |\omega_1\rangle, |\omega_2\rangle \in W: \\
&\quad |\psi\rangle \otimes (|\omega_1\rangle + |\omega_2\rangle) = |\psi\rangle \otimes |\omega_1\rangle + |\psi\rangle \otimes |\omega_2\rangle
\end{aligned}
$$

Linear Operators on Tensor Product Spaces

Suppose $|\psi\rangle \in V$, $|\omega\rangle \in W$, and A, B are linear operators on V and W respectively. Define a linear operator $A \otimes B$ on $V \otimes W$ by:

$$(A \otimes B)(|\psi\rangle \otimes |\omega\rangle) = (A|\psi\rangle) \otimes (B|\omega\rangle)$$

This extends linearly to all of $V \otimes W$:

$$(A \otimes B)\left(\sum_i a_i|\psi_i\rangle \otimes |\omega_i\rangle\right) = \sum_i a_i(A|\psi_i\rangle \otimes B|\omega_i\rangle)$$

General Linear Operators and Inner Product

Any linear operator C mapping $V \otimes W$ to $V' \otimes W'$ can be represented as:

$$C = \sum_i c_i A_i \otimes B_i$$

where

$$\left(\sum_i c_i A_i \otimes B_i \right) |\psi\rangle \otimes |\omega\rangle = \sum_i c_i A_i |\psi\rangle \otimes B_i |\omega\rangle$$

The inner products on V and W define a natural inner product on $V \otimes W$:

$$\left\langle \sum_i a_i |\psi_i\rangle \otimes |\omega_i\rangle \middle| \sum_j b_j |\psi'_j\rangle \otimes |\omega'_j\rangle \right\rangle = \sum_{i,j} a_i^* b_j \langle \psi_i | \psi'_j \rangle \langle \omega_i | \omega'_j \rangle$$

Kronecker Product: Matrix Representation

For matrices A $(m \times n)$ and B $(p \times q)$, the Kronecker product is:

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix}$$

Example:

$$A \otimes B = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \otimes \begin{pmatrix} 0 & 5 \\ 6 & 7 \end{pmatrix} = \begin{pmatrix} B & 2B \\ 3B & 4B \end{pmatrix}$$

Finally if you expand it you will get a $4\times$ 4 matrix, and by far you could understand that you will get all possible term as each element is related to other element.

Example: Pauli Matrices Tensor Product

The tensor product of Pauli matrices:

$$X \otimes Y = \begin{pmatrix} 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \\ 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \end{pmatrix}$$

This is useful in quantum mechanics for describing multi-qubit systems.

Commutator and Anticommutator

Commutator:

- For operators A and B, the commutator is defined as:

$$[A, B] = AB - BA$$

- Measures the extent to which two operators fail to commute.
- If $[A, B] = 0$, then A and B are said to commute.
- Important in quantum mechanics: $[\hat{x}, \hat{p}] = i\hbar$

Anticommutator:

- Defined as:

$$\{A, B\} = AB + BA$$

- Arises in contexts involving fermions and certain symmetries.
- If $\{A, B\} = 0$, the operators are said to anticommute.

Use: Both structures appear in operator algebra, quantum observables, and Lie algebras.

Pauli Matrices

Pauli Matrices:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Commutators:

- $[X, Y] = 2iZ$
- $[Y, Z] = 2iX$
- $[Z, X] = 2iY$

Anticommutators:

- $\{X, Y\} = 0$
- $\{Y, Z\} = 0$
- $\{Z, X\} = 0$
- $\{A, A\} = 2I$ for any Pauli matrix A

The State Space

- Every isolated quantum system is associated with a complex Hilbert space $\mathcal{H}$.
- The system's state is fully described by a unit vector $|\psi\rangle \in \mathcal{H}$:

$$\langle\psi|\psi\rangle = 1$$

- Two vectors that differ by a global phase represent the same physical state:

$$|\psi\rangle \sim e^{i\theta} |\psi\rangle$$

Example:

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

Evolution of Quantum States

- The evolution of a closed quantum system is described by a unitary transformation U.
- If a system is in state $|\psi\rangle$ at time t_0, its state at a later time t_1 is:

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

- U must satisfy: $U^\dagger U = I$

Implications:

- Evolution is reversible i.e. no information is lost.
- The norm of the state vector is preserved:

$$\left\langle\psi'\middle|\psi'\right\rangle = \langle\psi| U^\dagger U |\psi\rangle = \langle\psi|\psi\rangle$$

Why Unitary Evolution is So Powerful

- Unlike classical mechanics, quantum evolution is linear and happens in complex space.
- The system doesn't move in space but rotates in Hilbert space along the surface $\langle\psi|\psi\rangle = 1$.
- This postulate applies only to isolated systems (i.e. no measurements have been made yet).

How to find the matrix representation of an arbitrary linear operator?

- Suppose $A : V \longrightarrow W$ is a linear operator between the vector spaces V and W.
- Assuming the orthonormal basis for vector space V is $|v_1\rangle, |v_2\rangle, ..., |v_m\rangle$ and that for W is $|w_1\rangle, |w_2\rangle, ..., |w_n\rangle$.
- Now, any vector in vector space V is mapped to a vector in vector space W. There for we can write the action of A on any basis vector $|v_i\rangle$ as:

$$A|v_i\rangle = |w'\rangle = \sum_j A_{ij}|w_j\rangle$$

  Since $|w'\rangle$ is a vector in vector space W hence we can write it as a linear combination of the basis vectors $|w_i\rangle$, as we have done.
- Therefore, we can see that $A_{ij} = \langle w_j| A |v_i\rangle$

General state in quantum computing

- In quantum computing, we denote a single qubit's state as $|\psi = \alpha |0\rangle + \beta |1\rangle\rangle$, where $|0\rangle$ and $|1\rangle$ are the orthonormal basis vectors in the Hilbert space $\mathcal{H} = \mathbb{C}^2$.
- As you might have studied in PH110, the prob. of finding the qubit in state $|0\rangle$ is $|\alpha|^2$ and that in state $|1\rangle$ is $|\beta|^2$. By the above statement you can deduce that $|\alpha|^2 + |\beta|^2 = 1$ (Normalization condition).
- You can verify the statement you might have heard multiple times about QIC that a qubit unlike a classical bit remains in superposition of 0 and 1.

Common operators in quantum computing

- Operators on single qubit states can be denoted using 2×2 matrices.
- Four extremely useful matrices which we often see in QIC are the Pauli matrices. These are :

$$\sigma_0 \equiv I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad \sigma_1 \equiv \sigma_x \equiv X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\sigma_2 \equiv \sigma_y \equiv Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \qquad \sigma_3 \equiv \sigma_z \equiv Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Spectral Decomposition

- Spectral decomposition expresses a linear operator as a sum over its eigenvalues and eigenvectors.
- Any normal operator M on a vector space V is diagonal with respect to some orthonormal basis for V. Conversely, any diagonalizable operator is normal.
- For a normal operator M, we can write:

$$M = \sum_i \lambda_i |i\rangle \langle i|$$

- λ_i are the eigenvalues and $|i\rangle$ form an orthonormal basis.
- Commonly used when M is Hermitian or unitary.

Properties of Spectral Decomposition

- The operator M is diagonal in the basis of its eigenvectors.
- The eigenvectors form a complete orthonormal set:

$$\langle i|j\rangle = \delta_{ij}, \quad \sum_i |i\rangle \langle i| = I$$

- The decomposition is unique if all eigenvalues are distinct.
- Useful for simplifying operator functions: $f(M) = \sum_i f(\lambda_i) |i\rangle \langle i|$

Example: Hermitian Operator

- Consider a Hermitian matrix:

$$A = \begin{bmatrix} 3 & 0 \\ 0 & -1 \end{bmatrix}$$

- It has eigenvalues 3 and -1 with corresponding eigenvectors $|0\rangle$ and $|1\rangle$.
- Spectral decomposition:

$$A = 3\,|0\rangle\,\langle 0| - |1\rangle\,\langle 1|$$

Polar Decomposition

- Any linear operator A on a complex Hilbert space can be written as:

$$A = UP$$

  where:
  - U is a unitary operator (or partial isometry)
  - $P = \sqrt{A^\dagger A}$ is a positive semi-definite operator
- This is known as the polar decomposition of A
- P is uniquely defined, even if U is not always unique.
- U is unique if A is invertible.

Example of Polar Decomposition

- Let

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \Rightarrow A^\dagger A = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

- Then

$$P = \sqrt{A^\dagger A} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \quad U = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

- So $A = UP$ is the polar decomposition.

What happens when we perform measurements on a quantum system?

- We have already studied in PH110 that when we perform measurement on any quantum state $|\psi\rangle$ corresponing to any observable $\hat{A}$, possible results are the eigenvalues of that observable and the state collapses to the corresponding eigenspace[1] of that eigenvalue.
- Now, let's try to get a proper mathemaitical formulation of this for the detailed study of quantum measurements.

[1] Eigenspace corresponding to any eigenvalue λ of the oberesvable $\hat{A}$ is the vector space spanned by all the eigenvectors $|v_i\rangle$ of $\hat{A}$ that satisfy $\hat{A}\,|v_i\rangle = \lambda\,|v_i\rangle$. If the dimension of the eigenspace if 1 then we say that the eigenvalue λ corresponding to it is non-degenerate meanwhile if it is n-dimensional, λ is said to be n-fold degenerate.

Quantum measurement theory

- Quantum measurements are described by a collection $\{M_m\}$ of measurement operators that is formulated beforehand depending on the observable corresponding to which measurement is going to be made or based on what information we are trying to extract, where the index m refers to the measurement outcomes that may occur in the experiment.
- The probability p(m) with which we get the result m is given by

$$\langle\psi| M^{\dagger} M |\psi\rangle$$

and the state of the system after the measurement is given by

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

Quantum measurement theory (contd.)

- To better understand this you can think of it is follows, suppose you measure a state $|\psi\rangle$ and the possible results of your measurement may be one of m's (which might be something like energy or spin). Now if m (some fixed value here) is measured then the state evolves as follows :

$$\begin{array}{ccccc} |\psi\rangle & \longrightarrow & M_m|\psi\rangle & \longrightarrow & |\psi'\rangle \\ \text{Initial State} & & \text{Intermediate State} & & \text{Final State} \end{array}$$

  where M_m represents the part of the state that is associated with obtaining the measurement result m, note that this is not necessarily a state with definite value of m, unless the measurement is projective (will see later what this is). Example in meet.

- An important property of measurement operators can be understood as follow, $\sum_m p(m) = 1 \Rightarrow \sum_m \langle\psi| M_m^\dagger M_m |\psi\rangle = 1 \Rightarrow \langle\psi| \sum_m M_m^\dagger M_m |\psi\rangle = 1 = \langle\psi|\psi\rangle \Rightarrow$ $\sum_m M_m^\dagger M_m = 1$ (This is the propery followed by the set of M_m's)

Projective measurements

- There is a special sub-class of general measurements (studied above) known as projective measurements. In the scope of QIC we will be concerned primarily with projective measurements.
- A projective measurement is a measurement described by a set of orthogonal projection operators $\{P_m\}$, (in this case $M_m = P_m$).
- These are defined corresponding to any observable $\hat{A}$ having eigenvalues m, for every m we define the corresponding projection operator as $P_m = \sum_{i=1}^{n} |m_i\rangle \langle m_i|$, given that m is n-fold degenerate.
- As we can see from the above definition P_m picks out the eigenvectors from any state $|\psi\rangle$ corresponding to the given eigenvalue m, so we can say that it projects the given state vector from its state space to the eigenspace of m, hence the name projection operators.

Projective measurements (contd.)

- Important property of projection operators $P = P^\dagger = P^2$
- As we have studied in spectral decomposition, $\hat{A} = \sum_i i \left|i\right\rangle \left\langle i\right|$, therefore we can write any observable as a linear combination of projection operators as follows, $\hat{A} = \sum_m mP_m$. There is a very subtle difference between these 2 expressions can you find it?
- In projective measurement:

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

$$|\psi'\rangle = \frac{P_m |\psi\rangle}{\sqrt{\langle\psi| P_m |\psi\rangle}}$$

POVM measurements

Positive Operator-Valued Measure (POVM) measurements

- In some cases the post-measurement state of the system is of little interest, with the main interest being the probabilities of the respective measurement outcomes.
- In those cases first formulating $\{M_m\}$ (which helps in finding $|\psi'\rangle$) then we calculating $M^\dagger M$ (which helps in finding the respective probabilities) is too much work.
- In such cases, we directly formulate $E_m = M^\dagger M$, which are positive operator (Definition in meet) hence the name POVM, called POVM elements associated with the measurement. The entire set $\{E_m\}$ is called POVM.
- In this case $p(m) = \langle\psi| E_m |\psi\rangle$.

Types of phases in typical state in QIC

Will be covered completely in today's meet.

What if we are dealing with multiple qubit system?

- The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and system number i is prepared in the state $|v_i\rangle$, then the joint state of the total system is $|v_1\rangle \otimes |v_2\rangle \otimes |v_3\rangle \otimes .... \otimes |v_n\rangle$
- Intuition and example of 2 qubit system and its linear algebra form in meet.

Some intersesting QIC protocols

- Superdense Coding : It is a quantum communication protocol using which we can send 2 classical bits from one location to another using only 1 qubit.
- Quantum Teleportation : It is a protocol that allows us to teleport any arbitrary quantum state from one location to another, without physically sending the qubit.

We will see both of these in detail in today's meet. We will see that something profound is common in both these protocol. Can you find it? We will also look at Stern-Gerlach experiment (If enough time is left)

The End

Thank you