Universität Bremen

AGRA

IRQ: Mathematical Foundations

Dr. Kamalika Datta

Dr. Abhoy Kole

M. Sc. Lennart Weingarten

Lecture - 2

WINTER SEMESTER 2024-2025

Lecture Coverage

- Linear independence, basis and dimension
- Inner product, Hilbert Space, outer product

Recap of Previous Lecture

- Arithmetic of complex numbers
- Basic concept of vector space
- A quantum state $|\varphi\rangle$ can be expressed as the superposition (linear combination) of the basis states:

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

- Quantum state can be represented using vectors and gate operations as unitary matrices
- Spanning Set

Basis and Dimension

- A minimal spanning set is referred to as a basis.
- It can be shown that any two sets of **linearly independent** vectors that span a vector space V contain the same number of elements.
- Such a set of linearly independent vectors is called a ***basis*** for V.
- The number of elements in the basis is called the ***dimension*** of V.

Linearly Dependent Vectors

- A set of non-zero vectors $|v_1\rangle, \ldots, |v_n\rangle$ are said to be ***linearly dependent*** if there exists a set of complex numbers $a_1, \ldots, a_n$ with $a_i \neq 0$ for at least one value of i, such that

$$a_1 |v_1\rangle + a_2 |v_2\rangle + \ldots + a_n |v_n\rangle = 0$$

Linearly Dependent Vectors

- Consider three vectors a, b and c where $c = a + 3b$

- Any linear combination of a, b and c say
  - $2a + b + c \quad = 2a + b + a + 3b$

    $\quad = 3a + 4b$

- As c can be written in terms of a and b and hence it is linearly dependent and we do not require it for the solution.

Example

- The set of vectors $\left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ -1 \\ -1 \end{bmatrix} \right\}$ is linearly dependent because

$$\mathbf{0} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} = x \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} + y \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} + z \begin{bmatrix} 2 \\ -1 \\ -1 \end{bmatrix}$$

can happen when x = 2, y = -3, z = -1.

Linearly Independent Vectors

- A set of vectors is ***linearly independent*** if they are not linearly dependent.
- A set of non-zero vectors $|v_1\rangle, \ldots, |v_n\rangle$ are said to be ***linearly independent*** if there exists a set of complex numbers $a_1, \ldots, a_n$ with all $a_i = 0$ for all value of i, such that

$$a_1 |v_1\rangle + a_2 |v_2\rangle + \cdots + a_n |v_n\rangle = 0$$

Example

- Let v1 $= \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ v2 $= \begin{bmatrix} 1 \\ -1 \end{bmatrix}$ check whether they are linearly independent or dependent.

$$c1 \begin{bmatrix} 1 \\ 1 \end{bmatrix} + c2 \begin{bmatrix} 1 \\ -1 \end{bmatrix} = 0 \Rightarrow \begin{bmatrix} c1 \\ c1 \end{bmatrix} + \begin{bmatrix} c2 \\ -c2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$c1 + c2 = 0$, $c1 - c2 = 0$

Add the above equation: $2c1 = 0, \Rightarrow \ c1 = 0 \Rightarrow c2 = 0$

Hence the vector v1 and v2 are linearly independent

Example

- The set of vectors is linearly independent because the only way that can occur is if $0 = x$, $0 = x + y$, $0 = x + y + z$.

  This implies $x = y = z = 0$.

$$\left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}$$

$$\mathbf{0} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} = x \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} + y \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} + z \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

Basis (Z) : $|\mathbf{0}\rangle$ and $|\mathbf{1}\rangle$

- $|\mathbf{0}\rangle$ **and** $|\mathbf{1}\rangle$ is a basis because it satisfies two conditions:
  - Any vector $\begin{bmatrix} a \\ b \end{bmatrix}$ can be expressed as linear combination of $|\mathbf{0}\rangle$ **and** $|\mathbf{1}\rangle$

$$\begin{bmatrix} a \\ b \end{bmatrix} = a\,|\mathbf{0}\rangle + b|\mathbf{1}\rangle$$

  - $|\mathbf{0}\rangle$ **and** $|\mathbf{1}\rangle$ are linearly independent

- $|\mathbf{0}\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|\mathbf{1}\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

Basis (X) : $|+\rangle$ and $|-\rangle$

- $|+\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$ **and** $|-\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$

$$|+\rangle = \frac{1}{\sqrt{2}}\left(\begin{bmatrix}1\\0\end{bmatrix} + \begin{bmatrix}0\\1\end{bmatrix}\right) \quad \textbf{and} \quad |-\rangle = \frac{1}{\sqrt{2}}\left(\begin{bmatrix}1\\0\end{bmatrix} - \begin{bmatrix}0\\1\end{bmatrix}\right)$$

$$|+\rangle = \frac{1}{\sqrt{2}}(|\mathbf{0}\rangle + |\mathbf{1}\rangle) \quad \textbf{and} \quad |-\rangle = \frac{1}{\sqrt{2}}(|\mathbf{0}\rangle - |\mathbf{1}\rangle)$$

Basis (Y) : $|i\rangle$ and $|-i\rangle$

- $|i\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ i\end{bmatrix}$ **and** $|-i\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ -i\end{bmatrix}$

$$|i\rangle = \frac{1}{\sqrt{2}}\left(\begin{bmatrix}1\\ 0\end{bmatrix} + \boldsymbol{i}\begin{bmatrix}0\\ 1\end{bmatrix}\right) \quad \textbf{and} \quad |-i\rangle = \frac{1}{\sqrt{2}}\left(\begin{bmatrix}1\\ 0\end{bmatrix} - \boldsymbol{i}\begin{bmatrix}0\\ 1\end{bmatrix}\right)$$

$$|i\rangle = \frac{1}{\sqrt{2}}(|\mathbf{0}\rangle + \boldsymbol{i}|\mathbf{1}\rangle) \quad \textbf{and} \quad |-i\rangle = \frac{1}{\sqrt{2}}(|\mathbf{0}\rangle - \boldsymbol{i}|\mathbf{1}\rangle)$$

Important Quantum Property

- A quantum system can be defined as a system whose basis state form a vector space over complex numbers
- Or State of a quantum system corresponds to a vector in a complex vector space
- A basis is minimal and hence it is linearly independent
- We can have more than one basis in a vector space but all will have same number of elements

Operator as Matrices

Matrix Representation of Linear Operators

- Consider an $m \ x \ n$ complex matrix A with entries A_{ij}.
- *A* can be regarded as a linear operator sending vectors in the vector space $\mathbb{C}^n$ to the vector space $\mathbb{C}^m$, under matrix multiplication of A by a vector in $\mathbb{C}^n$.
- This actually means:

$$A\left(\sum_i a_i |v_i\rangle\right) = \sum_i a_i \, A(|v_i\rangle)$$

Some Important Matrices in Quantum Computing

- We shall be using four extremely useful matrices, known as ***Pauli matrices***.

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

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

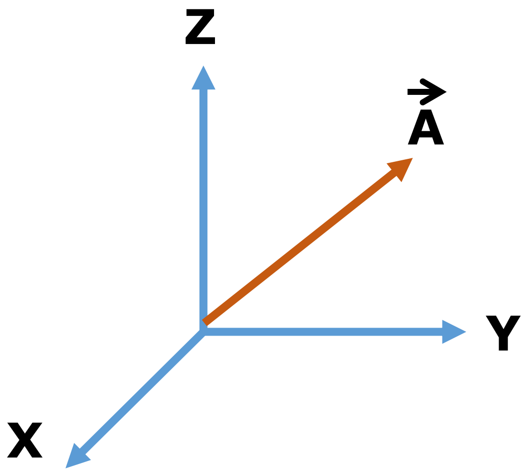
- We often omit I, and refer to X, Y and Z only as Pauli matrices.

Hilbert Space and Inner Products

Hilbert Space

- To define a Quantum System we need Hilbert space
- Hilbert space is a vector space where **complex inner product** is defined and the transformation is linear
- A Hilbert space is a complex inner product space that is complete
- A quantum System is represented by an element which belongs to Hilbert Space

Example of a Real Space



$$A = A_x\, i + A_y\, j + A_z\, k$$

Basis = {i, j, k}

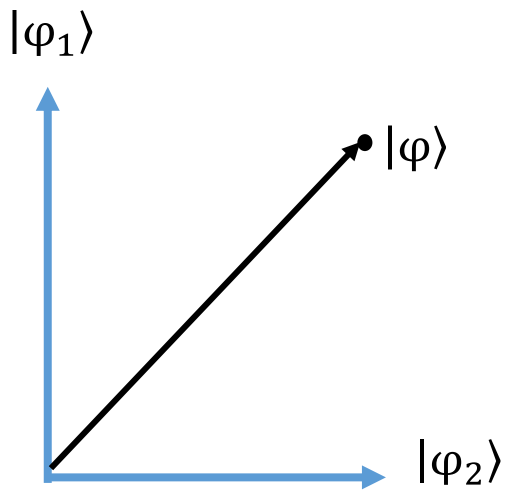
i = (1,0,0), j = (0,1,0), k = (0,0,1)

i.i = j.j =k.k = 1 — Normalized

i.j = j.k =k.i = 0 — Orthogonal

A basis which satisfies orthonormal property is said to be a Complete basis.

Hilbert Space



- Consider the Hilbert space which is spanned by two basis states $\{|\varphi_1\rangle, |\varphi_2\rangle\}$
- $|\varphi\rangle = c1\ |\varphi_1\rangle + c2\ |\varphi_2\rangle$
- Any quantum state is the linear combination of the basis states

Complex Inner Product

- A ***complex inner product*** is a function that takes as input two vectors $|v\rangle$ and $|w\rangle$ from a vector space, and generates a complex number as output.
- For the time being, we write the inner product of the two vectors as $\boldsymbol{(|v\rangle, |w\rangle)}$**.**
  - The standard quantum mechanical notation is $\boldsymbol{\langle v|w\rangle}$.
- A vector space equipped with an inner product is known as an ***inner product space***.

Complex Inner Product

- **Example**: For the vector space $\mathbb{C}^n$, the inner product of two vectors $(y_1, \dots, y_n)$ and $(z_1, \dots, z_n)$ is defined by

$$\langle (y_1, \dots, y_n) | (z_1, \dots, z_n) \rangle = \sum_i y_i{}^* z_i = [y_1{}^* \dots \quad y_n{}^*] \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix}$$

a* is the complex conjugate of a

An Example

- Consider the following operation that we perform with two vectors in $\mathbb{R}^3$ (that is, two vectors of size 3 with real numbers as elements):

$$\left\langle \begin{bmatrix} 5 \\ 3 \\ -7 \end{bmatrix}, \begin{bmatrix} 6 \\ 2 \\ 0 \end{bmatrix} \right\rangle = [5, 3, -7] \star \begin{bmatrix} 6 \\ 2 \\ 0 \end{bmatrix} = (5 \times 6) + (3 \times 2) + (-7 \times 0) = 36.$$

An Example of a Property

- $|\psi\mathbf{1}\rangle = \begin{bmatrix} 2 \\ 1 \\ 4i \end{bmatrix}$ $\quad |\psi\mathbf{2}\rangle = \begin{bmatrix} 1 \\ 2i \\ 3 \end{bmatrix}$

$$\langle\psi1|\ \psi2\rangle = [2 \quad 1 \quad 4i]^* \begin{bmatrix} 1 \\ 2i \\ 3 \end{bmatrix} = [2 \quad 1 \quad -4i] \begin{bmatrix} 1 \\ 2i \\ 3 \end{bmatrix} = 2 - 10i$$

$$\langle\psi2|\ \psi1\rangle = [1 \quad 2i \quad 3]^* \begin{bmatrix} 2 \\ 1 \\ 4i \end{bmatrix} = [1 \quad -2i \quad 3] \begin{bmatrix} 2 \\ 1 \\ 4i \end{bmatrix} = 2 + 10i$$

Both are complex conjugate

An Example

- $|v1\rangle = \begin{bmatrix} 2+3i \\ 5-4i \end{bmatrix}$

- $\langle v1|v1\rangle$

$$
\begin{aligned}
&= \begin{bmatrix} 2+3i & 5-4i \end{bmatrix}^* \begin{bmatrix} 2+3i \\ 5-4i \end{bmatrix} \\
&= \begin{bmatrix} 2-3i & 5+4i \end{bmatrix} \begin{bmatrix} 2+3i \\ 5-4i \end{bmatrix} \\
&= (2-3i)(2+3i) + (5+4i)(5-4i) \\
&= 54
\end{aligned}
$$

Example with $|0\rangle$ and $|1\rangle$

- $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ $\quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
- $\langle 0|0\rangle = [1 \quad 0]^* \begin{bmatrix} 1 \\ 0 \end{bmatrix} = 1$ $\quad \langle 1|1\rangle = [0 \quad 1]^* \begin{bmatrix} 0 \\ 1 \end{bmatrix} = 1$

NORMALIZED CONDITION

Norm or Length

- For every complex inner product space V, we can define a ***norm*** or ***length*** as $|V| = \sqrt{\langle V, V \rangle}$.

- **Example**: In $\mathbb{R}^3$, the norm of the vector $[3, -6, 2]^T$ is given by

$$\left\| \begin{bmatrix} 3 \\ -6 \\ 2 \end{bmatrix} \right\| = \sqrt{\left\langle \begin{bmatrix} 3 \\ -6 \\ 2 \end{bmatrix}, \begin{bmatrix} 3 \\ -6 \\ 2 \end{bmatrix} \right\rangle} = \sqrt{3^2 + (-6)^2 + 2^2} = \sqrt{49} = 7$$

Example

- Norm of $|\boldsymbol{v}\rangle = \begin{bmatrix} 2+3i \\ 5-4i \end{bmatrix}$

$$\begin{aligned} \langle v|v\rangle &= \begin{bmatrix} 2+3i & 5-4i \end{bmatrix}^* \begin{bmatrix} 2+3i \\ 5-4i \end{bmatrix} \\ &= \begin{bmatrix} 2-3i & 5+4i \end{bmatrix} \begin{bmatrix} 2+3i \\ 5-4i \end{bmatrix} \\ &= 54 \end{aligned}$$

Norm of $|\boldsymbol{v}\rangle = \sqrt{54}$

Unit Vector

- A ***unit vector*** is a vector for which the norm is 1.

- For example, $(1, 0, 0, 0)^T$.

Orthogonal Vectors

- Two vectors V_1 and V_2 in an inner product space V are orthogonal if:

$$\langle V_1, V_2 \rangle = 0$$

Linearly Independent Vectors

- **Example**: The two vectors $|w\rangle = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ and $|v\rangle = \begin{bmatrix} 1 \\ -1 \end{bmatrix}$ are orthogonal, as their inner product $\langle w|v\rangle$ is 0:

$$(1 * 1) + (1 * -1) = 0.$$

Example with $|0\rangle$ and $|1\rangle$

- $|\mathbf{0}\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|\mathbf{1}\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

- Check whether vector $|\mathbf{0}\rangle$ and $|\mathbf{1}\rangle$ are orthogonal or not?

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

Hence $|0\rangle$ and $|1\rangle$ basis are orthogonal.

ORTHOGONAL CONDITION

Orthogonal Basis and Orthonormal Basis

Definition *A basis $\mathcal{B} = \{V_0, V_1, \ldots, V_{n-1}\}$ for an inner product space $\mathbb{V}$ is called an* **orthogonal basis** *if the vectors are pairwise orthogonal to each other, i.e., $j \neq k$ implies $\langle V_j, V_k \rangle = 0$. An orthogonal basis is called an* **orthonormal basis** *if every vector in the basis is of norm 1, i.e.,*

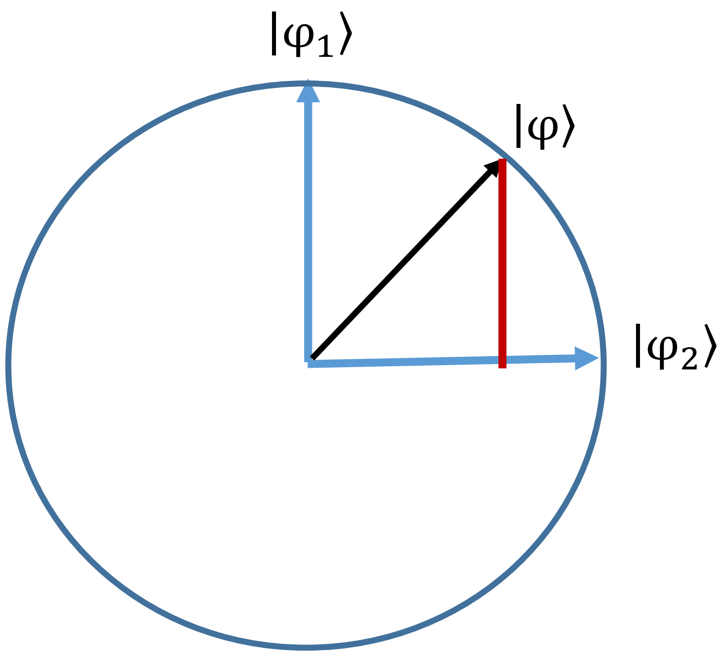
$$\langle V_j, V_k \rangle = \delta_{j,k} = \begin{cases} 1, & \text{if } j = k, \\ 0, & \text{if } j \neq k. \end{cases}$$

$\delta_{j,k}$ is called the ***Kronecker delta function***.

Inner Product Properties

- The inner product of two orthogonal vectors are 0
- Inner product of a unit vector is 1

Relook at Hilbert Space



- Hilbert space (H)= Orthogonal + Normal +Inner product defined
- Hence $|\boldsymbol{\varphi}\rangle \in \mathrm{H} \rightarrow \varphi$ is normalized

- $|\varphi\rangle = c1\ |\varphi_1\rangle + c2\ |\varphi_2\rangle$
- Then $|c1|^2+|c2|^2 = 1$

- $|\varphi\rangle$ is normalized i.e. total probability is 1
- **Sum of the squares of amplitude is equal to 1**

Quantum Superposition

- A quantum state can be in superposition of the basis states.

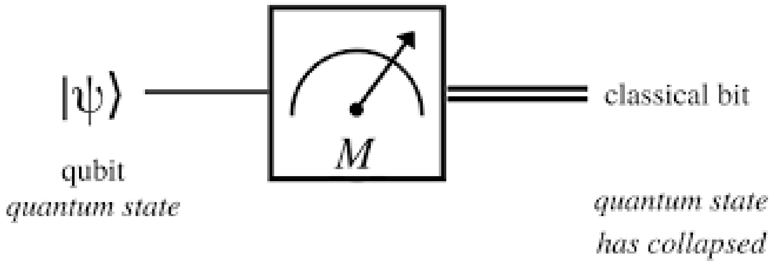
$$|\boldsymbol{\varphi}\rangle = \boldsymbol{\alpha}\,|\mathbf{0}\rangle + \boldsymbol{\beta}\,|\mathbf{1}\rangle$$

- Here $|\mathbf{0}\rangle$ **and** $|\mathbf{1}\rangle$ are the basis states, and $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are **complex numbers**

$$|\boldsymbol{\alpha}|^2 + |\boldsymbol{\beta}|^2 = \mathbf{1}$$

Quantum Measurement

- When the state of a qubit is “measured”:
  - The value returned is that of one of the basis states – the qubit state also collapses to that basis state.
  - This happens with some probability.
  - This is unlike reading the output of a circuit in conventional computing.
- Suppose the state of a qubit is: $|\boldsymbol{\varphi}\rangle = \boldsymbol{\alpha}\,|\mathbf{0}\rangle + \boldsymbol{\beta}\,|\mathbf{1}\rangle$
- When we read the state of the qubit, it returns $|0\rangle$ with probability $|\boldsymbol{\alpha}|^2$, and it returns $|1\rangle$ with probability $|\boldsymbol{\beta}|^2$.



Outer Product Representation

- There is a useful way of representing linear operators that makes use of the inner product, known as the ***outer product*** representation.
- Suppose $|v\rangle$ is a vector in an inner product space V, and $|w\rangle$ is a vector in an inner product space W.

Outer Product Representation

- We define the outer product operator $A = |w\rangle\langle v|$ from V to W which is defined as:

$$|w\rangle\langle v| = \begin{bmatrix} w_1 \\ w_2 \\ w_3 \end{bmatrix} \begin{bmatrix} v_1 & v_2 & v_3 \end{bmatrix}^* = \begin{bmatrix} w_1 v_1 & w_1 v_2 & w_1 v_3 \\ w_2 v_1 & w_2 v_2 & w_2 v_3 \\ w_3 v_1 & w_3 v_2 & w_3 v_3 \end{bmatrix}$$

- If $|i\rangle$ denote any orthonormal basis for the vector space V, it can be shown that

$$\sum_i |i\rangle\langle i| = I$$

Outer Product as Projection Operator

- Let φ_1 and φ_2 are two vectors
- $|\varphi_1\rangle = \begin{bmatrix} 1 \\ 2 \\ 3i \end{bmatrix}, \quad |\varphi_2\rangle = \begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix}$
- Outer Product $= |\varphi_1\rangle\langle\varphi_2| = \begin{bmatrix} 1 \\ 2 \\ 3i \end{bmatrix} \begin{bmatrix} 1 & 1 & 2 \end{bmatrix}$
- $= \begin{bmatrix} 1 & 1 & 2 \\ 2 & 2 & 4 \\ 3i & 3i & 6i \end{bmatrix}$

Projection Operator / Complex Matrix / Square matrix

A projection operator project any vector onto the subspace of another vector

Summary

- Basis and Dimension
- Linear independence
- Hilbert space
- Orthogonal and normal
- Inner product, outer product