Día 1: Introducción

Álgebra lineal, postulados de la mecánica cuántica y computación cuántica

1°CICC x QFF 2025 @ CIC - IPN

13 de octubre de 2025


1ER CONGRESO
IBEROAMERICANO
DE COMPUTACIÓN
CUÁNTICA
13 al 17 de octubre del 2025
CENTRO DE INVESTIGACIÓN EN COMPUTACIÓN
CDMX


100
$\Delta x \Delta p \geq \frac{\hbar}{2}$

Álgebra lineal: Motivación

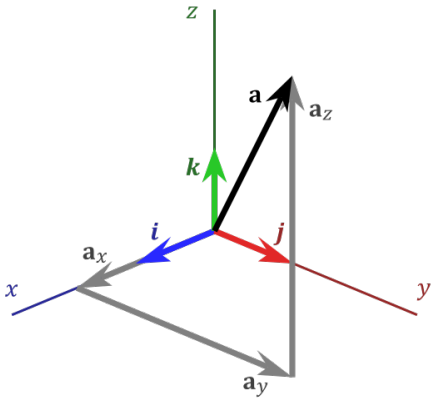


Figura: [1]

[1] Acdx, Wikimedia Commons, CC BY-SA 3.0

Matrices

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}_{m \times n}$$

con $a_{ij} \in \mathbb{R}$ ó $\mathbb{C}$.

- Operaciones
  - Suma
  - Producto por escalar
  - Producto de matrices

Un *espacio vectorial* V sobre un campo $\mathbb{F}$ (comúnmente $\mathbb{R}$ o $\mathbb{C}$) es un conjunto, cuyos elementos llamamos *vectores*, equipado con dos operaciones:

1. Suma de vectores $+ : V \times V \to V$
2. Multiplicación por escalares $\cdot : \mathbb{F} \times V \to V$

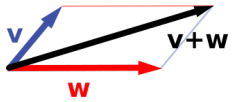


Figura: Suma de vectores

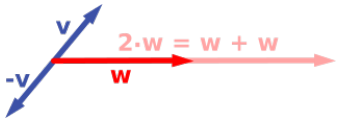


Figura: Multiplicación por escalares

Figuras[2]

[2] Jakob.scholbach, Wikimedia Commons, CC BY-SA 3.0

tales que, para todos $u, v, w \in V$ y $a, b \in \mathbb{F}$, se satisfacen las siguientes propiedades:

1. Cerradura bajo la suma: $u + v \in V$
2. Conmutatividad: $u + v = v + u$
3. Asociatividad de la suma: $(u + v) + w = u + (v + w)$
4. Elemento neutro aditivo: Existe $0 \in V$ tal que $u + 0 = u$
5. Inverso aditivo: Para cada $u \in V$, existe $-u \in V$ tal que $u + (-u) = 0$
6. Cerradura bajo la multiplicación escalar: $av \in V$
7. Asociatividad de escalares: $a(bv) = (ab)v$
8. Elemento neutro escalar: $1v = v$, donde 1 es el neutro multiplicativo de $\mathbb{F}$
9. Distributividad en la suma de vectores: $a(u + v) = au + av$
10. Distributividad en la suma de escalares: $(a + b)v = av + bv$

Base y dimensión

Una *base* de un espacio vectorial V sobre un campo $\mathbb{F}$ es un conjunto de vectores en V, linealmente independientes y que generan a V.

La *dimensión* de un espacio vectorial V, denotada por $\dim V$, se define como el número de vectores en una base de V.

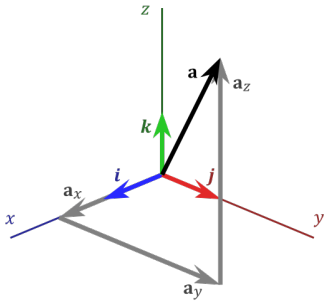


Figura: Acdx, Wikimedia Commons, CC BY-SA 3.0

Espacios vectoriales: Ejemplos

- Ejemplo canónico: El conjunto de n-adas $(a_1, a_2, \ldots, a_n)$ con entradas en $\mathbb{R}$.
- $\mathbb{C}^2 := \{a \begin{bmatrix} 1 \\ 0 \end{bmatrix} + b \begin{bmatrix} 0 \\ 1 \end{bmatrix} | a, b \in \mathbb{C}\}$
- El conjunto de matrices de tamaño $m \times n$ con entradas en $\mathbb{C}$, $\mathcal{M}_{m\times n}(\mathbb{C})$, junto con las operaciones usuales de suma y producto por escalar forman un espacio vectorial sobre $\mathbb{C}$ de dimensión mn.

Producto interno

El *producto interno*, en un espacio vectorial V se define como una operación binaria $\langle\cdot|\cdot\rangle : V \times V \to \mathbb{F}$ que satisface para todos $\mathrm{u}, \mathrm{v}, \mathrm{w} \in V$, $a, b \in \mathbb{F}$:

- Conjugada simétrica: $\langle \mathrm{u}|\mathrm{v}\rangle = \langle \mathrm{v}|\mathrm{u}\rangle^*$.
- Linealidad en el segundo argumento*: $\langle \mathrm{w}|a\mathrm{u} + b\mathrm{v}\rangle = a\langle \mathrm{w}|\mathrm{u}\rangle + b\langle \mathrm{w}|\mathrm{v}\rangle$.
- Definida positiva: $\langle \mathrm{u}|\mathrm{u}\rangle \geq 0$ y $\langle \mathrm{u}|\mathrm{u}\rangle = 0$ si y solo si $\mathrm{u} = 0$.

Producto interno en $\mathbb{C}^n$

$$\langle \mathrm{u}|\mathrm{v}\rangle = \sum_{i=1}^{n} u_i^* v_i = \begin{bmatrix} u_1^* & u_2^* & \cdots & u_n^* \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}$$

para $\mathrm{u} = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix}$ y $\mathrm{v} = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}$, donde v_i^* representa el conjugado complejo de v_i.

Notación de Dirac

Sea $V = \mathbb{C}^n$, dotado con el producto interno canónico $\langle \cdot | \cdot \rangle : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$.

Un ket $|\psi\rangle$ representa un vector en V:

$$|\psi\rangle = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix}.$$

Un bra $\langle \phi |$ es el *dual* de un ket. Es decir:

$$\langle \phi | = (|\phi\rangle)^\dagger = \begin{bmatrix} b_1^* & b_2^* & \dots & b_n^* \end{bmatrix}.$$

Luego

$$\langle \phi | \psi \rangle = \sum_{i=1}^{n} b_i^* a_i.$$

Norma de un vector

Una *norma* en un espacio vectorial V sobre un campo $\mathbb{F}$ es una función $\|\cdot\| : V \to \mathbb{R}$ que asigna a cada vector $\mathrm{v} \in V$ un número real no negativo $\|\mathrm{v}\|$, y que satisface las siguientes propiedades:

- No negatividad: Para todo $\mathrm{v} \in V$, se cumple que $\|\mathrm{v}\| \geq 0$. Además, $\|\mathrm{v}\| = 0$ si y solo si $\mathrm{v} = 0$.
- Homogeneidad escalar: Para todo escalar $a \in \mathbb{F}$ y todo vector $\mathrm{v} \in V$, se cumple que $\|a\mathrm{v}\| = |a|\|\mathrm{v}\|$.
- Desigualdad triangular: Para cualesquiera vectores $\mathrm{u}, \mathrm{v} \in V$, se cumple que $\|\mathrm{u} + \mathrm{v}\| \leq \|\mathrm{u}\| + \|\mathrm{v}\|$.

Una norma en un espacio vectorial proporciona una noción de longitud para los vectores en tal espacio. Observe que el producto induce una norma a través de la relación:

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

Espacio de Hilbert

Un *espacio de Hilbert* es un espacio vectorial, usualmente denotado por $\mathcal{H}$, sobre $\mathbb{R}$ o $\mathbb{C}$, equipado con un producto interno y que es *completo* con respecto a la norma inducida por dicho producto interno.

Postulado I. Espacio de estados

Asociado a cualquier sistema cuántico existe un espacio de Hilbert $\mathcal{H}$ complejo y el estado del sistema queda completamente determinado por un vector $\psi \in \mathcal{H}$ tal que $\langle\psi|\psi\rangle = 1$ y todo vector $\psi \in \mathcal{H}$ tal que $\langle\psi|\psi\rangle = 1$ representa un estado físicamente posible.

A menudo se hace referencia a estos vectores como *estados cuánticos*, *funciones de onda*, etc.

Operadores

Un operador lineal sobre el espacio vectorial V, es una función $A : V \to V$ que satisface para todos los vectores $u, v \in V$ y para todo escalar $a \in \mathbb{F}$:

1. $A(u + v) = A(u) + A(v)$.
2. $A(au) = aA(u)$.

Observaciones:

- El conjunto de operadores lineales sobre V forma un espacio vectorial con las operaciones usuales de suma y producto por escalar de funciones.
- **Si** $\dim V = n$**, existe una correspondencia 1-1 entre el espacio de operadores lineales sobre** V **el espacio de matrices** $\mathcal{M}_{n\times n}(\mathbb{F})$**.**

Adjunto de un operador

Dado un operador A sobre un espacio V de dimensión finita, existe un operador $A^\dagger$ tal que

$$(|u\rangle, A|v\rangle) = (A^\dagger|u\rangle, |v\rangle), \quad \text{para todo } u, v \in V,$$

donde $(\cdot, \cdot)$ denota el producto interno en V.

- $A^\dagger$ es la conjugada transpuesta de A, en su representación matricial.

Operadores Hermitianos

Un operador lineal A en un espacio vectorial V con producto interno se dice que es *Hermitiano* si satisface

$$A = A^{\dagger}.$$

Esto significa que para todos los vectores $|u\rangle, |v\rangle \in V$, se cumple:

$$\langle u|Av\rangle = \langle Au \,|\, v\rangle$$

Postulado II. Observables

A cualquier cantidad medible físicamente, (llamada *observable* o *variable dinámica*), corresponde un operador Hermitiano cuyos eigenvectores forman una base para el espacio de Hilbert asociado al sistema.

Eigenvalores y eigenvectores

Sea A un operador lineal sobre un espacio vectorial V. Un vector $|u\rangle$ distinto de cero es un *eigenvector* de A si existe un número a tal que:

$$A|u\rangle = a|u\rangle .$$

El número a se llama *eigenvalor* asociado al eigenvector $|u\rangle$.

Eigenvalores de operadores Hermitianos

Sea $|u\rangle$ un eigenvector del operador A Hermitiano, con eigenvalor a. Entonces

$$a\langle u|u\rangle = \langle u|Au\rangle = \langle A^\dagger u|u\rangle = \langle Au|u\rangle = a^*\langle u|u\rangle.$$

Por lo tanto $a = a^*$, entonces $a \in \mathbb{R}$.

Los eigenvalores de operadores Hermitianos son números reales.

Postulado III. Mediciones

Los resultados posibles de la medición de una variable dinámica son los eigenvalores del correspondiente operador Hermitiano.

Si el resultado de la medición de un observable A, con operador $\hat{A}$, sobre un estado $|\psi\rangle$ es a_n, entonces el sistema inmediatamente después de la medición se encuentra en el estado $|\psi_n\rangle$, el eigenvector de $\hat{A}$ con correspondiente eigenvalor a_n.

La probabilidad de obtener el resultado a_n al medir el observable A de un sistema en el estado $|\psi\rangle$ está dada por

$$Pr(a_n) = |\langle\psi_n|\psi\rangle|^2.$$

Operadores unitarios

- Un operador lineal A se dice que es *invertible* si existe otro operador A^{-1}, tal que $AA^{-1} = A^{-1}A = I$.

Un operador lineal $U : V \to V$ en un espacio vectorial V con producto interno se dice que es *unitario* si su adjunto $U^\dagger$ es también su inverso, es decir, si satisface la siguiente condición:

$$UU^\dagger = U^\dagger U = I.$$

Postulado IV. Evolución temporal

La evolución temporal del estado $|\psi(t)\rangle$ que describe un sistema cuántico aislado es descrita por un operador unitario: el estado del sistema al tiempo t_1, $|\psi(t_1)\rangle$ se relaciona al estado al tiempo t_2, $|\psi(t_2)\rangle$ a través del operador $U(t_1, t_2)$:

$$|\psi(t_2)\rangle = U(t_1, t_2)\,|\psi(t_1)\rangle\,.$$

Qubits

Un *qubit* es un sistema cuántico de dos niveles, cuyo espacio de Hilbert correspondiente es $\mathcal{H} = \mathbb{C}^2$, i.e. el generado por los vectores

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

El estado general del sistema, entonces, puede describirse por la combinación lineal

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

donde los coeficientes α y β son números complejos tales que $|\alpha|^2 + |\beta|^2 = 1$, y $|\alpha|^2$, $|\beta|^2$ son las probabilidades de obtener respectivamente $|0\rangle$ o $|1\rangle$, al realizar una medición del sistema.

Qubits II

Los estados que adoptan la forma $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ con $|\alpha|^2, |\beta|^2 > 0$ se dice que están en *superposición*, y reflejan que el sistema existe físicamente en una combinación coherente de los estados base $|0\rangle$ y $|1\rangle$ antes de cualquier medición.

Esta propiedad distingue al qubit del bit clásico, que solo puede encontrarse en uno de sus dos posibles estados en cada instante.

Esfera de Bloch

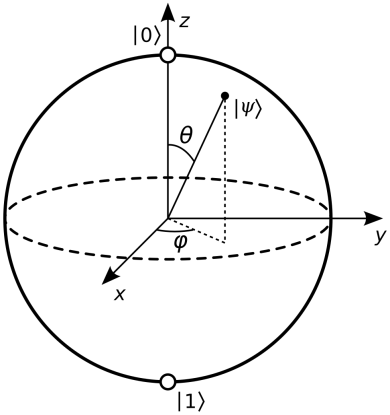


Figura: Smite-Meister, Wikimedia Commons, CC BY-SA 3.0

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle,$$
donde $0 \leq \theta \leq \pi$ y $0 \leq \phi \leq 2\pi$.

Estados con múltiples qubits

Dado un sistema compuesto de n qubits, el espacio de Hilbert correspondiente es el producto tensorial $\mathcal{H}^{\otimes n}$. Es decir, el estado general del sistema está descrito por un vector en

$$\mathcal{H}^{\otimes n} = \mathbb{C}^{2^n},$$

el cual puede escribirse como una combinación lineal de los vectores base

$$|i_1 i_2 \dots i_n\rangle = |i_1\rangle \otimes |i_2\rangle \otimes \cdots \otimes |i_n\rangle,$$

donde cada $i_k \in \{0, 1\}$ para $k = 1, \dots, n$, y la suma se extiende sobre todas las 2^n combinaciones posibles. A este conjunto de vectores se le conoce comúnmente como la *base computacional* (para un valor fijo de n).
El estado general del sistema puede entonces expresarse como

$$|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle,$$

donde cada $\alpha_i \in \mathbb{C}$, y $\sum_i |\alpha_i|^2 = 1$.

Compuertas lógicas cuánticas

Una *compuerta cuántica* que actúa sobre k qubits es un operador unitario

$$U \in \mathcal{M}_{2^k \times 2^k}(\mathbb{C}),$$

es decir, una matriz compleja de dimensión $2^k \times 2^k$ tal que $U^\dagger U = I$.
En sistemas de múltiples qubits, las compuertas de un solo qubit pueden actuar sobre un subsistema mediante el operador

$$U_i = I^{\otimes(i-1)} \otimes U \otimes I^{\otimes(n-i)},$$

donde $U \in \mathcal{M}_{2\times 2}(\mathbb{C})$ actúa sobre el i-ésimo qubit.

Algoritmos cuánticos

Un *algoritmo cuántico* es una secuencia de operaciones sobre estados cuánticos, como compuertas y mediciones, diseñada para resolver una tarea computacional específica. En general, estas operaciones actúan sobre estados superpuestos, pero es importante recalcar que toda medición produce un solo vector de la base computacional como resultado.

Circuitos cuánticos

Un *circuito cuántico* es una descripción esquemática de un algoritmo cuántico, donde los qubits se representan como líneas horizontales y las compuertas cuánticas como símbolos colocados sobre estas líneas. El tiempo avanza de izquierda a derecha.

Los circuitos cuánticos permiten visualizar y organizar algoritmos, y constituyen una representación estándar para su implementación en dispositivos cuánticos actuales.

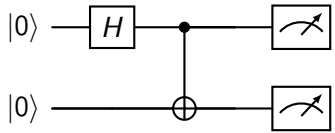


Figura: Ejemplo de un circuito cuántico simple con dos qubits.

Compuertas lógicas cuánticas: Ejemplos

Hadamard H

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

$$H|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$
$$H|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

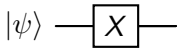
X **ó** NOT

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

$$X|0\rangle = |1\rangle$$
$$X|1\rangle = |0\rangle$$

Ejemplo: Compuerta *NOT*

Considere el estado $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$.

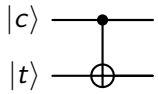


$$X\,|0\rangle = |1\rangle$$
$$X\,|1\rangle = |0\rangle$$

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

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

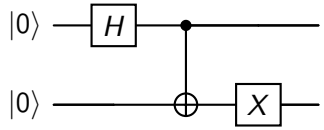
Controlled-NOT



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

$$\begin{aligned} \text{CNOT}\,|00\rangle &= |00\rangle\,, \\ \text{CNOT}\,|01\rangle &= |01\rangle\,, \\ \text{CNOT}\,|10\rangle &= |11\rangle\,, \\ \text{CNOT}\,|11\rangle &= |10\rangle\,. \end{aligned}$$

Ejemplo: Circuito de Bell



$$|00\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}\big(\,|00\rangle + |10\rangle\,\big)$$
$$\xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big)$$
$$\xrightarrow{I\otimes X} \frac{1}{\sqrt{2}}\big(\,|01\rangle + |10\rangle\,\big).$$

Estado resultante

$$|\psi_{\text{out}}\rangle = \frac{1}{\sqrt{2}}\big(\,|01\rangle + |10\rangle\,\big)$$

Estados entrelazados

Un estado cuántico compuesto $|\psi\rangle$ de dos o más qubits se dice que está *entrelazado* si no puede escribirse como un producto de estados individuales.
Es decir, $|\psi\rangle$ es entrelazado si no existe una descomposición del tipo:

$$|\psi\rangle \neq |\phi_A\rangle \otimes |\phi_B\rangle \,.$$

Por ejemplo, el estado de Bell

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