Bloque 1. Fundamentos matemáticos

Operadores lineales y representación matricial

Índice

Esquema 3

Ideas clave 4

3.1 Introducción y objetivos 4

3.2 Transformaciones lineales 4

3.3 Operadores lineales 7

3.4 Representación matricial de transformaciones lineales 7

3.5 Matrices complejas como operadores 9

3.6 Valores y vectores propios 10

3.7 Espacios de operadores 12

Problemas 13

Esquema

- **Transformaciones lineales**
  - Definición y propiedades
  - Núcleo e imagen
  - Inyectividad y sobreyectividad
- **Operadores lineales**
  - Operadores como endomorfismos
  - Composición de operadores
  - Operador inverso
- **Representación matricial**
  - Matriz asociada a una transformación
  - Cambio de base
  - Isomorfismo con matrices
- **Matrices complejas**
  - Operaciones matriciales
  - Matrices especiales

Ideas clave

3.1 Introducción y objetivos

Los operadores lineales constituyen el puente conceptual entre la estructura algebraica abstracta de los espacios vectoriales y su representación computacional mediante matrices. En computación cuántica, este concepto es fundamental ya que todas las operaciones que pueden realizarse sobre sistemas cuánticos se describen mediante operadores lineales unitarios.

La importancia de los operadores lineales en computación cuántica se refleja en múltiples aspectos:

- Las **puertas cuánticas** son operadores unitarios que actúan sobre qubits.
- La **evolución temporal** de sistemas cuánticos se describe mediante operadores unitarios.
- Los **observables cuánticos** son operadores hermitianos.
- Los **algoritmos cuánticos** se construyen como secuencias de operadores lineales.

En este tema desarrollaremos la teoría de transformaciones lineales entre espacios vectoriales complejos, con especial énfasis en los operadores (transformaciones de un espacio en sí mismo) y su representación matricial. Esta conexión entre conceptos abstractos y representaciones concretas es esencial para la implementación práctica de algoritmos cuánticos.

3.2 Transformaciones lineales

Definición 1: Transformación lineal

Sean V y W espacios vectoriales complejos. Una función $T : V \to W$ es una transformación lineal si para todos $\mathbf{u}, \mathbf{v} \in V$ y $\alpha, \beta \in \mathbb{C}$:

$$T(\alpha\mathbf{u} + \beta\mathbf{v}) = \alpha T(\mathbf{u}) + \beta T(\mathbf{v}) \, .$$

Equivalentemente, T es lineal si:

1. $T(\mathbf{u} + \mathbf{v}) = T(\mathbf{u}) + T(\mathbf{v})$ (preserva la suma).
2. $T(\alpha\mathbf{v}) = \alpha T(\mathbf{v})$ (preserva el producto por escalar).

Ejemplo 1: Transformaciones lineales básicas

1. **Transformación identidad:** $I : V \to V$ definida por $I(\mathbf{v}) = \mathbf{v}$.
2. **Transformación cero:** $O : V \to W$ definida por $O(\mathbf{v}) = \mathbf{0}$.
3. **Escalamiento:** $S_\alpha : \mathbb{C}^n \to \mathbb{C}^n$ definida por $S_\alpha(\mathbf{v}) = \alpha\mathbf{v}$.
4. **Proyección:** $P : \mathbb{C}^3 \to \mathbb{C}^2$ definida por $P\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$.
5. **Rotación en $\mathbb{C}^2$:** $R_\theta : \mathbb{C}^2 \to \mathbb{C}^2$ definida por

$$R_\theta\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x\cos\theta - y\sin\theta \\ x\sin\theta + y\cos\theta \end{pmatrix}.$$

Resultado 1

Si $T : V \to W$ es una transformación lineal, entonces:

1. $T(\mathbf{0}) = \mathbf{0}$.
2. $T(-\mathbf{v}) = -T(\mathbf{v})$ para todo $\mathbf{v} \in V$.
3. T está completamente determinada por su acción sobre cualquier base de V. Es decir, si existe $\mathcal{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ una base de V y $U : V \to W$ otra transformación lineal tal que $U(\mathbf{v}_i) = T(\mathbf{v}_i)$ para todo i, entonces $U = T$.

Definición 2: Núcleo

Sea $T : V \to W$ una transformación lineal. Llamamos **núcleo (o kernel)** de T a $\text{Ker}(T) = \{\mathbf{v} \in V : T(\mathbf{v}) = \mathbf{0}\}$

Resultado 2

Sea $T : V \to W$ una transformación lineal. Entonces:

1. $\text{Ker}(T)$ es un subespacio de V.
2. $\text{Im}(T)$ es un subespacio de W.
3. T es inyectiva si y solo si $\text{Ker}(T) = \{\mathbf{0}\}$.

Ejemplo 2: Cálculo de núcleo e imagen

Considerar la transformación $T : \mathbb{C}^3 \to \mathbb{C}^2$ definida por:

$$T\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x + iy \\ 2x - z \end{pmatrix}$$

Núcleo: Resolver $T(\mathbf{v}) = \mathbf{0}$:

$$x + iy = 0$$
$$2x - z = 0$$

De la primera ecuación: $x = -iy$. De la segunda: $z = 2x = -2iy$. Por tanto:

$$\text{Ker}(T) = \left\{ \begin{pmatrix} -iy \\ y \\ -2iy \end{pmatrix} : y \in \mathbb{C} \right\} = \text{gen}\left\{ \begin{pmatrix} -i \\ 1 \\ -2i \end{pmatrix} \right\}$$

Imagen: Como T es lineal, $\text{Im}(T) = \text{gen}\{T(\mathbf{e}_1), T(\mathbf{e}_2), T(\mathbf{e}_3)\}$:

$$T(\mathbf{e}_1) = T\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \quad T(\mathbf{e}_2) = T\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} i \\ 0 \end{pmatrix}, \quad T(\mathbf{e}_3) = T\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix}$$

Como los vectores $\mathbf{e}_2$ y $\mathbf{e}_3$ son linealmente independientes en $\mathbb{C}^2$, $\text{Im}(T) = \mathbb{C}^2$.

Teorema 3

Sea $T : V \to W$ una transformación lineal entre espacios vectoriales de dimensión finita, entonces:

- Existe $V' \subseteq V$ tal que $V = \text{Ker}(T) \oplus V'$.
- Existe $W' \subseteq W$ tal que $W = \text{Im}(T) \oplus W'$.
- $V / \text{Ker}(T) \cong \text{Im}(T)$.

Como consecuencia directa del Teorema 3 obtenemos el siguiente resultado fundamental.

Teorema 4

Sea $T : V \to W$ una transformación lineal entre espacios vectoriales de dimensión finita. Entonces:

$$\dim(V) = \dim(\text{Ker}(T)) + \dim(\text{Im}(T))$$

3.3 Operadores lineales

Definición 3: Operador lineal

Un operador lineal en un espacio vectorial V es una transformación lineal $T : V \to V$. El conjunto de todos los operadores lineales en V se denota $\mathcal{L}(V)$.

Los operadores lineales tienen propiedades especiales debido a que el espacio de salida coincide con el de entrada, lo que permite usar conceptos como la composición o la inversa.

Resultado 5

La composición de operadores lineales satisface:

1. **Asociatividad:** $(R \circ S) \circ T = R \circ (S \circ T)$.
2. **Elemento neutro:** $I \circ T = T \circ I = T$.
3. **Distributividad:** $R \circ (S + T) = R \circ S + R \circ T$.

Teorema 6: Caracterización de la invertibilidad

Un operador $T \in \mathcal{L}(V)$ es invertible si y solo si es biyectivo. Equivalentemente:

1. T es inyectivo ($\text{Ker}(T) = \{\mathbf{0}\}$).
2. T es sobreyectivo ($\text{Im}(T) = V$).

Aplicando el Teorema 3 a operadores lineales obtenemos la siguiente consecuencia.

Teorema 7

Sea $T \in \mathcal{L}(V)$ un operador lineal en un espacio vectorial de dimensión finita. Entonces:

$$V = \text{Ker}(T) \oplus \text{Im}(T)$$

3.4 Representación matricial de transformaciones lineales

La representación matricial establece una correspondencia biyectiva entre transformaciones lineales y matrices, permitiendo cálculos computacionales eficientes.

Definición 4: Matriz de una transformación lineal

Sean V y W espacios vectoriales de dimensiones finitas con bases $\mathcal{B}_V = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ y $\mathcal{B}_W = \{\mathbf{w}_1, \ldots, \mathbf{w}_m\}$ respectivamente. Sea $T : V \to W$ una transformación lineal. Para cada $j = 1, \ldots, n$, expresamos $T(\mathbf{v}_j)$ en la base $\mathcal{B}_W$:

$$T(\mathbf{v}_j) = \sum_{i=1}^{m} a_{ij}\mathbf{w}_i$$

La matriz de T respecto a las bases $\mathcal{B}_V$ y $\mathcal{B}_W$ es:

$$[T]_{\mathcal{B}_V}^{\mathcal{B}_W} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

En el caso de considerarse $\mathcal{B}_V$ y $\mathcal{B}_W$ las bases canónicas, la matriz de la transformación se denota simplemente como $[T]$.

Nota: La j-ésima columna de $[T]_{\mathcal{B}_V}^{\mathcal{B}_W}$ contiene las coordenadas de $T(\mathbf{v}_j)$ respecto a la base $\mathcal{B}_W$.

Ejemplo 3: Matriz de una transformación

Sea $T : \mathbb{C}^2 \to \mathbb{C}^3$ definida por $T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+iy \\ 2x \\ x-y \end{pmatrix}$.

Usando las bases canónicas:

$$T(\mathbf{e}_1) = T\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}, \quad T(\mathbf{e}_2) = T\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} i \\ 0 \\ -1 \end{pmatrix}$$

Por tanto:

$$[T] = \begin{pmatrix} 1 & i \\ 2 & 0 \\ 1 & -1 \end{pmatrix}$$

Teorema 8: Cambio de base

Sean $T : V \to W$ una transformación lineal entre espacios vectoriales de la misma dimensión finita, $\mathcal{B}_1$ y $\mathcal{B}_2$ dos bases de V y $\mathcal{B}_3$ y $\mathcal{B}_4$ dos bases de W. Entonces existe una matriz P invertible tal que las matrices $[T]_{\mathcal{B}_1}^{\mathcal{B}_3}$ y $[T]_{\mathcal{B}_2}^{\mathcal{B}_4}$ están relacionadas por:

$$[T]_{\mathcal{B}_2}^{\mathcal{B}_4} = P^{-1}[T]_{\mathcal{B}_1}^{\mathcal{B}_3}P$$

Llamamos a P la matriz de **cambio de base**.

El teorema de cambio de base 8 es muy importante, pues nos permite verificar muchas propiedades sobre las transformaciones lineales, con solo comprobarlo con la matriz asociada a las bases canónicas.

Teorema 9: Correspondencia entre transformaciones y matrices

La representación matricial establece un isomorfismo de espacios vectoriales:

$$\mathcal{L}(V, W) \cong \mathbb{C}^{m\times n}$$

donde $\dim(V) = n$ y $\dim(W) = m$.
Además, si $S : U \to V$ y $T : V \to W$ son transformaciones lineales, entonces:

$$[T \circ S] = [T][S]$$

3.5 Matrices complejas como operadores

Cada matriz compleja $A \in \mathbb{C}^{m\times n}$ define naturalmente una transformación lineal $T_A : \mathbb{C}^n \to \mathbb{C}^m$ mediante $T_A(\mathbf{v}) = A\mathbf{v}$. Esta correspondencia permite estudiar propiedades algebraicas de las matrices a través de la teoría de operadores.

Junto con las operaciones matriciales estándar, se definen conceptos clave como la transpuesta conjugada, las matrices hermitianas y unitarias, que son fundamentales en computación cuántica.

Definición 5

Sea $A \in \mathbb{C}^n$ una matriz cuadrada, llamamos **matriz adjunta** a la matriz $A^\dagger$ definida por:

$$(A^\dagger)_{ij} = \overline{A_{ji}}\,.$$

Definición 6

Sea $A \in \mathbb{C}^n$ una matriz cuadrada, decimos que es:

- **Hermítica** si $A^\dagger = A$.
- **Unitaria** si $A^\dagger A = AA^\dagger = I$.

- **Normal** si $A^\dagger A = AA^\dagger$.

Estudiaremos con más detalle estas matrices en temas posteriores, ya que son fundamentales en computación cuántica.

Ejemplo 4: Matrices de Pauli

Las matrices de Pauli son matrices hermitianas fundamentales en computación cuántica:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{1}$$

Estas matrices satisfacen:

- $\sigma_i^2 = I$ para $i = x, y, z$.
- $\sigma_x\sigma_y = i\sigma_z$, $\sigma_y\sigma_z = i\sigma_x$, $\sigma_z\sigma_x = i\sigma_y$.
- $\{\sigma_x, \sigma_y\} = \sigma_x\sigma_y + \sigma_y\sigma_x = 0$ (anticonmutan).
- Junto con la identidad I, forman una base de $\mathbb{C}^{2\times 2}$.

Ejemplo 5: Matriz de Hadamard

La matriz de Hadamard es una matriz unitaria fundamental: $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

Se verifica que $H^2 = I$ y transforma la base computacional en:

$$H|0\rangle = H\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle \tag{2}$$

$$H|1\rangle = H\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle \tag{3}$$

3.6 Valores y vectores propios

Definición 7: Valor y vector propio

Sea $A \in \mathbb{C}^{n\times n}$. Un escalar $\lambda \in \mathbb{C}$ es un **valor propio** de A si existe un vector no nulo $\mathbf{v} \in \mathbb{C}^n$ tal que: $A\mathbf{v} = \lambda\mathbf{v}$.
El vector **v** se llama **vector propio** asociado al valor propio λ.

Para obtener los valores propios de una matriz A, se resuelve el sistema $(A - \lambda I)\mathbf{v} = \mathbf{0}$. Este sistema tiene soluciones no triviales si y solo si $\det(A - \lambda I) = 0$.

Definición 8: Polinomio característico

El **polinomio característico** de $A \in \mathbb{C}^{n\times n}$ es: $p_A(\lambda) = \det(A - \lambda I)$.

Resultado 10

Los valores propios de A son las raíces de $p_A(\lambda)$.

Ejemplo 6

Consideremos la matriz de Pauli $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, cuyo polinomio característico es:

$$p_{\sigma_z}(\lambda) = \det\begin{pmatrix} 1-\lambda & 0 \\ 0 & -1-\lambda \end{pmatrix} = (1-\lambda)(-1-\lambda) = \lambda^2 - 1\,.$$

Los valores propios son $\lambda_1 = 1$ y $\lambda_2 = -1$. Ahora calculemos los vectores propios.

Para $\lambda_1 = 1$, $(\sigma_z - I)\mathbf{v} = \begin{pmatrix} 0 & 0 \\ 0 & -2 \end{pmatrix}\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \mathbf{0} \Rightarrow v_2 = 0$. Por tanto, $\mathbf{v}_1 = \begin{pmatrix} v_1 \\ 0 \end{pmatrix}$ con $v_1 \neq 0$.

Para $\lambda_2 = -1$, $(\sigma_z + I)\mathbf{v} = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \mathbf{0} \Rightarrow v_1 = 0$. Por tanto, $\mathbf{v}_2 = \begin{pmatrix} 0 \\ v_2 \end{pmatrix}$ con $v_2 \neq 0$.

Podemos obtener una base ortonormal de $\mathbb{C}^2$ con los vectores propios de σ_z obteniendo:

- Para $\lambda_1 = 1$: $\mathbf{v}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$
- Para $\lambda_2 = -1$: $\mathbf{v}_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$

Teorema 11: Diagonalización

Una matriz $A \in \mathbb{C}^{n\times n}$ es diagonalizable si y solo si tiene n vectores propios linealmente independientes. En tal caso, existe una matriz invertible P tal que: $P^{-1}AP = D$ donde D es diagonal con los valores propios de A en la diagonal.

3.7 Espacios de operadores

Definición 9: Espacio de operadores lineales

El conjunto $\mathcal{L}(V)$ de todos los operadores lineales en un espacio vectorial V forma un espacio vectorial con las operaciones:

- $(S+T)(\mathbf{v}) = S(\mathbf{v}) + T(\mathbf{v})$
- $(\alpha T)(\mathbf{v}) = \alpha T(\mathbf{v})$

Resultado 12

Si $\dim(V) = n$, entonces $\dim(\mathcal{L}(V)) = n^2$.

Ejemplo 7: Base del espacio de operadores en $\mathbb{C}^2$

Una base para $\mathcal{L}(\mathbb{C}^2)$ está dada por las matrices:

$$E_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, E_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, E_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, E_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Cualquier operador $T \in \mathcal{L}(\mathbb{C}^2)$ se puede escribir como: $T = \sum_{i,j=1}^{2} t_{ij} E_{ij}$.

Alternativamente, se puede usar la llamada base de Pauli:

$$\{I, \sigma_x, \sigma_y, \sigma_z\}$$

Problemas

1. Verificar que las siguientes funciones son transformaciones lineales y calcular su núcleo e imagen:

a) $T : \mathbb{C}^3 \to \mathbb{C}^2$ definida por $T\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x + iy - z \\ 2x + y \end{pmatrix}$

b) $S : \mathbb{C}^2 \to \mathbb{C}^3$ definida por $S\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} u + iv \\ 2u \\ u - v \end{pmatrix}$

2. Encontrar la matriz de la transformación lineal $T : \mathbb{C}^2 \to \mathbb{C}^2$ definida por $T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} (1+i)x + y \\ ix - 2y \end{pmatrix}$ respecto a:

a) La base canónica

b) La base $\mathcal{B} = \left\{ \begin{pmatrix} 1 \\ i \end{pmatrix}, \begin{pmatrix} i \\ 1 \end{pmatrix} \right\}$

3. Sean $A = \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}$ y $B = \begin{pmatrix} 1 & 0 \\ i & 1 \end{pmatrix}$. Calcular:

a) AB y BA

b) A^* y B^*

c) det(A), det(B) y det(AB)

d) tr(A), tr(B) y tr(AB)

4. Encontrar los valores propios y vectores propios de las siguientes matrices:

a) $A = \begin{pmatrix} 2 & i \\ -i & 2 \end{pmatrix}$

b) $B = \begin{pmatrix} 1 & 1+i \\ 1-i & 2 \end{pmatrix}$

c) La matriz de Hadamard $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

5. Verificar que las siguientes matrices son unitarias y calcular sus inversas:

a) $U_1 = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$

b) $U_2 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1+i \\ 1-i & -1 \end{pmatrix}$

6. Demostrar que si A y B son matrices hermitianas, entonces:

a) $A + B$ es hermitiana

b) AB es hermitiana si y solo si $AB = BA$

c) iA es antihermitiana (i.e., $(iA)^* = -iA$)

7. Considerar la puerta cuántica de fase controlada: CZ $= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$

a) Verificar que CZ es unitaria

b) Determinar cómo actúa sobre los estados de la base computacional

c) Calcular los valores propios de CZ

8. Expresar la matriz $M = \begin{pmatrix} 3 & 1+2i \\ 1-2i & -1 \end{pmatrix}$ como combinación lineal de las matrices de Pauli y la identidad.

9. Sea $T : V \to V$ un operador lineal en un espacio vectorial de dimensión finita.

a) Demostrar que T es invertible si y solo si det$([T]) \neq 0$

b) Si T es invertible, demostrar que $[T^{-1}] = ([T])^{-1}$

c) Demostrar que tr(T) es independiente de la base elegida