Tema 7

Bloque 2. Espacios cuánticos

Operadores lineales en computación cuántica

Índice

Esquema

- **Operadores en $\mathcal{C}$**
  - Matriz adjunta y operadores especiales
  - Operadores hermitianos y unitarios
  - Descomposición espectral
- **Puertas Cuánticas de Un cúbit**
  - Matrices de Pauli: X, Y, Z
  - Puerta de Hadamard
  - Puertas de fase: S, T, rotaciones
- **Geometría en la Esfera de Bloch**
  - Rotaciones como operadores unitarios
  - Visualización geométrica
  - Generación de puertas arbitrarias
- **Operadores en $\mathcal{C}^n$**
  - Sistemas de múltiples cúbits
  - Operadores producto tensorial
  - Operadores no separables
- **Puertas Cuánticas Controladas**
  - CNOT y puertas controladas generales
  - Puertas de múltiples controles
  - Universalidad cuántica
- **Evolución Temporal y Hamiltonianos**
  - Operadores hermitianos como generadores
  - Matrices exponenciales
  - Simulación de evolución cuántica

Ideas clave

7.1 Introducción y objetivos

Habiendo establecido la teoría general de operadores lineales en el Tema 3, ahora nos enfocamos en los operadores específicos en $\mathcal{C}$ y $\mathcal{C}^n$ que forman el corazón de la computación cuántica. Estos operadores, cuando satisfacen la condición de unitariedad, se conocen como **puertas cuánticas** y constituyen los bloques de construcción fundamentales de los algoritmos cuánticos.

Los objetivos específicos de este tema son:

- Caracterizar completamente los operadores unitarios y hermitianos en $\mathcal{C}$.
- Estudiar las puertas cuánticas fundamentales y su interpretación geométrica.
- Analizar cómo los operadores producto tensorial describen sistemas multicúbit.
- Desarrollar puertas controladas y entender su implementación.
- Conectar operadores hermitianos con la evolución temporal cuántica.

7.2 Operadores lineales en $\mathcal{C}$

Empecemos con el espacio de un solo cúbit, $\mathcal{C}$. Aquí, los operadores se representan como matrices 2×2, y su estudio es fundamental para entender la computación cuántica. La dimensión del espacio de matrices 2×2 es 4, lo que implica que éste es el número de matrices linealmente independientes que cualquier base va a tener.

Resultado 1

Las matrices de Pauli X, Y, Z junto con la identidad I es una base de $\mathcal{M}_2(\mathbb{C})$.

Demostración.

Al coincidir el número de matrices del conjunto con la dimensión del espacio, podemos estudiar solo una condición de base, ser linealmente independiente o generar el espacio.

Veamos que son linealmente independientes. Si existen $a, b, c, d \in \mathcal{C}$ tales que

$$aI + bX + cY + dZ = 0\,,$$

entonces

$$\begin{aligned} 0 &= aI + bX + cY + dZ \\ &= a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + c\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} + d\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ &= \begin{pmatrix} a+d & b-ic \\ b+ic & a-d \end{pmatrix} \Rightarrow \begin{cases} a+d=0 \\ b-ic=0 \\ b+ic=0 \\ a-d=0 \end{cases} \Rightarrow a=b=c=d=0\,. \end{aligned}$$

□

Cualquier matriz hermítica $A = \begin{pmatrix} a & b \\ \overline{b} & c \end{pmatrix}$ con $a, c \in \mathbb{R}$ y $b \in \mathbb{C}$ puede expresarse en esta base de la siguiente manera

$$A = \frac{a+c}{2} I + \mathfrak{Re}(b) X - \mathfrak{Im}(b) Y + \frac{a-c}{2} Z\,.$$

El postulado 3 de la teoría cuántica establece que la ecuación de Schrödinger para la evolución temporal de un cúbit debe ser un operador unitario.

En cuanto a los operadores unitarios, la condición $U^\dagger U = I$ impone restricciones no lineales sobre los coeficientes de la combinación lineal. Por lo tanto, el conjunto de operadores unitarios no forma un espacio vectorial, sino un grupo bajo la multiplicación de matrices.

Definición 1

Llamaremos **puertas cuánticas** a los operadores unitarios en $\mathcal{C}^n$.

Sobre un cúbit, ya hemos visto que los kets pueden representarse como puntos de la esfera de Bloch, y por tanto, aplicar una puerta cuántica a un punto de la esfera, debe llevarlo a otro punto de la esfera. De manera similar, los operadores unitarios en $\mathcal{C}$ pueden interpretarse como rotaciones de esta esfera.

Resultado 2

Un operador U en $\mathcal{C}$ es unitario si y solo si puede escribirse como

$$U = \begin{pmatrix} e^{i(\alpha - \frac{\beta}{2} - \frac{\delta}{2})} \cos\left(\frac{\gamma}{2}\right) & -e^{i(\alpha - \frac{\beta}{2} + \frac{\delta}{2})} \sin\left(\frac{\gamma}{2}\right) \\ e^{i(\alpha + \frac{\beta}{2} - \frac{\delta}{2})} \sin\left(\frac{\gamma}{2}\right) & e^{i(\alpha + \frac{\beta}{2} + \frac{\delta}{2})} \cos\left(\frac{\gamma}{2}\right) \end{pmatrix},$$

con $\alpha, \beta, \delta, \gamma \in \mathbb{R}$.

Demostración.

Sea $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ un operador unitario en $\mathcal{C}$, entonces de la condición $U^\dagger U = I$ se tiene que

$$\begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

De donde se deduce el sistema de ecuaciones

$$|a|^2 + |b|^2 = 1\,. \tag{1}$$
$$|c|^2 + |d|^2 = 1\,. \tag{2}$$
$$a\bar{c} + b\bar{d} = 0\,. \tag{3}$$

Distinguimos tres casos:

1. $c = 0$.

De la segunda ecuación nos dice que $d \neq 0$, y de la tercera ecuación nos obliga a que $b = 0$. Entonces de la primera ecuación $|a|^2 = 1$ y de la segunda $|d|^2 = 1$, por lo que

$$U = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{i\phi} \end{pmatrix},$$

con $\theta, \phi \in \mathbb{R}$.

Ahora solo basta tomar $\alpha = \frac{\theta+\phi}{2}$, $\delta = \gamma = 0$, y $\beta = \phi - \theta$, para obtener la expresión del enunciado.

2. $a = 0$.

Usando el mismo razonamiento, llegamos a que

$$U = \begin{pmatrix} 0 & -e^{i\phi} \\ e^{i\theta} & 0 \end{pmatrix},$$

y tomando $\alpha = \frac{\theta+\phi}{2}$ y $\beta = \frac{\theta-\phi}{2}$, $\gamma = \pi$ y $\delta = 0$ obtenemos la expresión del enunciado.

3. $a\bar{c} \neq 0$.

La tercera ecuación se puede reescribir como

$$\bar{a}c + \bar{b}d = 0 \Rightarrow a = -\frac{b}{\bar{c}}\bar{d} \Rightarrow a = \frac{|b|}{|c|}|d|\,.$$

Sustituyendo en la primera ecuación:

$$\begin{aligned} 1 &= |a|^2 + |b|^2 \\ &= \left(\frac{|b|}{|c|}|d|\right)^2 + |b|^2 \\ &= |b|^2\left(\frac{|d|^2}{|c|^2} + 1\right) \\ &= |b|^2\left(\frac{|d|^2 + |c|^2}{|c|^2}\right) && \text{por la ecuación (2)} \\ &= \frac{|b|^2}{|c|^2} \end{aligned}$$

Por lo tanto, $|b| = |c|$ y de la ecuación (1) y (2) se deduce que $|a| = |d|$. Podemos por tanto encontrar $\gamma, \theta, \phi, \psi, \chi \in \mathbb{R}$ tales que

$$\begin{aligned} |a| = |d| &= \cos\left(\frac{\gamma}{2}\right). \\ |b| = |c| &= \sin\left(\frac{\gamma}{2}\right). \\ a &= |a|e^{i\theta} \\ b &= -|b|e^{i\phi} \\ c &= |c|e^{i\psi} \\ d &= |d|e^{i\chi} \end{aligned}$$

Como $a\bar{c} + b\bar{d} = 0$, se tiene que

$$|a||c|e^{i(\theta-\psi)} - |b||d|e^{i(\phi-\chi)} = 0 \Rightarrow e^{i(\theta-\psi)} = e^{i(\phi-\chi)} \Rightarrow \theta - \psi = \phi - \chi\,,$$

Tomando $\alpha = \frac{\theta+\chi}{2}$, $\beta = \chi - \theta$, y $\delta = \phi - \chi$, obtenemos la expresión del enunciado.

□

Podemos parametrizar por tanto toda matriz unitaria en $\mathcal{C}$ con cuatro parámetros reales, y dee ellos, uno solo afecta a las probabilidades de medición, el parámetro γ. Los otros tres parámetros corresponden a fases globales o relativas que no afectan a las probabilidades de medición. Llamaremos puerta genérica a la expresión $U(\alpha, \beta, \delta, \gamma)$ dada por la proposición anterior.

Podemos simplificar la expresión anterior y obtener un bonito resultado geométrico. Para ello vamos a introducir las matrices de rotación sobre los ejes de la esfera de Bloch.

Definición 2

Sea U una matriz unitaria en $\mathcal{C}$. Llamamos matriz de rotación de U a la matriz parametrizada por

$$R_U(\theta) = e^{-i\theta U/2}\,.$$

Sin entrar en detalles sobre la definición de la exponencial de una matriz, podemos calcular las matrices de rotación sobre las matrices de Pauli.

Resultado 3

Las matrices de rotación sobre las matrices de Pauli son:

$$R_X(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix},$$
$$R_Y(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix},$$
$$R_Z(\theta) = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}.$$

Ahora podemos expresar cualquier puerta cuántica en $\mathcal{C}$ como una combinación de rotaciones alrededor de los ejes de la esfera de Bloch.

Resultado 4

Toda puerta cuántica en $\mathcal{C}$ puede escribirse como

$$U = e^{i\alpha}R_Z(\beta)R_Y(\gamma)R_Z(\delta)\,,$$

donde $\alpha, \beta, \delta, \gamma \in \mathbb{R}$.

Como la fase global no tiene efectos en las observaciones, podemos prescindir de este parámetro y dejar la expresión como

$$U = U(\alpha,\beta,\gamma) = R_Z(\beta)R_Y(\alpha)R_Z(\gamma) = \begin{pmatrix} \cos\frac{\alpha}{2} & -e^{i\gamma}\sin\frac{\alpha}{2} \\ e^{i\beta}\sin\frac{\alpha}{2} & e^{i(\beta+\gamma)}\cos\frac{\alpha}{2} \end{pmatrix},$$

donde $\alpha, \beta, \gamma \in \mathbb{R}$.

Ejemplo 1.

Las puertas de rotación de Pauli expresadas como puertas genéricas son:

- $R_X(\theta) = U(\theta, -\frac{\pi}{2}, \frac{\pi}{2})$.
- $R_Y(\theta) = U(\theta, 0, 0)$.
- $R_Z(\theta) = U(0, \theta, 0)$.

7.3 Puertas cuánticas fundamentales de un cúbit

Las matrices de Pauli son las puertas cuánticas más fundamentales y corresponden con rotaciones de $\pi/2$ alrededor de los ejes de la esfera de Bloch. Como puertas dentro del contexto de la computación cuántica, se suelen denotar por las letras X, Y, Z, aunque también reciben otros nombres.

Definición 3: Puertas de Pauli

$$X = U(\pi, 0, \pi) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{(puerta NOT)}$$

$$Y = U(\pi, \pi/2, \pi/2) = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$Z = U(\pi, 0, 0) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{(puerta de fase)}$$

La puerta X a veces se representa como $\oplus$ porque esencialmente es un sumador binario. Para ello solo tenemos que ver como actúa sobre los estados de la base computacional

$$X|0\rangle = |1\rangle \quad \text{que es } |0 \oplus 1\rangle$$
$$X|1\rangle = |0\rangle \quad \text{que es } |1 \oplus 1\rangle\,,$$

donde $\oplus$ es la operación de **suma binaria**. Por este motivo, podemos expresar la acción de X sobre la base computacional como

$$X|a\rangle = |a \oplus 1\rangle\,,$$

para $a \in \{0, 1\}$.

Para la puerta Z podemos representar su acción sobre la base computacional como

$$Z|a\rangle = (-1)^a|a\rangle\,,$$

para $a \in \{0, 1\}$.

Resultado 5

La representación de las puertas de Pauli en términos del producto exterior es:

1. $X = |0\rangle\langle 1| + |1\rangle\langle 0|$.
2. $Y = i|0\rangle\langle 1| - i|1\rangle\langle 0|$.
3. $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$.

Otra puerta comúmente usada es la puerta de Hadamard, que es una puerta cuántica que crea superposiciones equiprobables.

Definición 4: Puerta de Hadamard

$$H = U(\pi/2, 0, \pi) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

La puerta de Hadamard es fundamental para crear superposiciones, y su acción sobre los estados de la base computacional es:

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

Definición 5: Base de Hadamard

Llamaremos base de Hadamard a la base ortonormal $\{|+\rangle, |-\rangle\}$.

Las siguientes identidades conectan las puertas de Pauli y la puerta de Hadamard

$$HXH = Z$$
$$HZH = X$$
$$HYH = -Y\,.$$

Para la puerta H podemos representar su acción sobre la base computacional como

$$H|a\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^a|1\rangle)\,,$$

para $a \in \{0, 1\}$.

Resultado 6

La representación de la puerta de Hadamard en términos del producto exterior es

$$H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |1\rangle\langle 1|)\,.$$

Otras puertas más genéricas son las puertas de fase.

Definición 6: Puertas de fase

$$R_\theta = U(0,0,\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \qquad \text{(puerta de fase general)}$$

$$S = U(0,0,\pi/2) = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad R_{\frac{\pi}{2}}$$

$$T = U(0,0,\pi/4) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \qquad R_{\frac{\pi}{4}}$$

Las puertas de fase introducen una fase relativa entre los estados $|0\rangle$ y $|1\rangle$, y son cruciales para muchos algoritmos cuánticos. Estas puertas se relacionan entre sí mediante las siguientes identidades:

- $S^2 = Z$
- $T^2 = S$
- $T^4 = Z$
- $T^8 = I$

Resultado 7

La representación de las puertas de fase en términos del producto exterior es

1. $R_\phi = |0\rangle\langle 0| + e^{i\phi}|1\rangle\langle 1|$.
2. $S = |0\rangle\langle 0| + i|1\rangle\langle 1|$.
3. $T = |0\rangle\langle 0| + e^{i\pi/4}|1\rangle\langle 1|$.

7.4 Operadores en $\mathcal{C}^n$: Sistemas multicúbit

Recordemos que el espacio de estados de un sistema de n cúbits es el producto tensorial de n copias de $\mathcal{C}$ y tiene dimensión 2^n, y por construcción de la base computacional, la base canónica de $\mathcal{C}^n$ es

$$\{|b_1 b_2 \dots b_n\rangle : b_i \in \{0,1\}\}$$

Ejemplo 2: Sistema de 2 cúbits

Para $n = 2$, tenemos $\mathcal{C}^2$ con base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

Algunos ejemplo de como actuan las puertas construidas como tensoriales:

$$(X \otimes I)|01\rangle = X|0\rangle \otimes I|1\rangle = |1\rangle \otimes |1\rangle = |11\rangle$$
$$(I \otimes Z)|10\rangle = I|1\rangle \otimes Z|0\rangle = |1\rangle \otimes |0\rangle = |10\rangle\,.$$

Sin embargo, no todas las puertas sobre dos cúbits se puede poner como un producto tensorial de dos puertas de un cúbit. Por ejemplo, la puerta CNOT.

Definición 7: Puerta CNOT

La puerta Controlled-NOT actúa sobre dos cúbits, y se define por

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

La puerta CNOT puede expresarse como suma de productos tensoriales de puertas de un cúbit

$$\text{CNOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X\,.$$

Y como productos externos también se puede expresar como

$$\text{CNOT} = |00\rangle\langle 00| + |11\rangle\langle 11| + |01\rangle\langle 10| + |10\rangle\langle 01|\,.$$

Ejemplo 3.

$$\text{CNOT}|00\rangle = |00\rangle$$
$$\text{CNOT}|01\rangle = |01\rangle$$
$$\text{CNOT}|10\rangle = |11\rangle$$
$$\text{CNOT}|11\rangle = |10\rangle$$

El nombre de CNOT es Control NOT, pues el primer cúbit actúa como control, esta puerta solo actúa si el primer cúbit está en $|1\rangle$, en tal caso aplica X al segundo cúbit.

Algunas veces debemos aplicar puertas de un cúbit a sistemas de varios cúbits, y simplemente por el nombre de la puerta no es suficiente para saber dónde actúa la puerta. Lo habitual es usar el producto tensorial con la unidad para construir nuevas puertas.

Ejemplo 4.

La puerta de Hadamard sobre tres cúbits pero actuando solo sobre el segundo se puede construir como $I \otimes H \otimes I$.

Una notación más compacta y clara es indicar con un subíndice el cúbit sobre el que actúa la puerta.

Ejemplo 5.

H_2 denota la puerta de Hadamard aplicada al cúbit 2.

$$H_2|001\rangle = \frac{|001\rangle + |011\rangle}{\sqrt{2}}$$

7.4.1 Puertas controladas generales

Definición 8: Puerta controlada general

Para cualquier operador unitario U de un cúbit:

$$C_U = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U = \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}$$

Al igual que las puertas unitarias de un cúbit, actuando sobre varios cúbits, las puertas controladas también tienen el problema de no indicar claramente cuál cúbit es el control y cuál es el objetivo. Para ello introducimos la notación de indicar con un superíndice la posición del cúbit control y un subíndice el cúbit objetivo.

Ejemplo 6.

La puerta CNOT se puede escribir como X_2^1.

$$X_2^1 H_1|00\rangle = X_2^1 \frac{|00\rangle + |10\rangle}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \left|\Phi^+\right\rangle.$$

Ejemplo 7: Otras puertas controladas importantes

- **Controlled-Z**: $C_Z = \text{diag}(1, 1, 1, -1)$
- **Controlled-Hadamard**: $C_H = \begin{pmatrix} I & 0 \\ 0 & H \end{pmatrix}$
- **Controlled-Phase**: $C_{R_\phi} = \text{diag}(1, 1, 1, e^{i\phi})$

Podemos expresar relaciones entre las puertas cuánticas con esta nueva notación.

Resultado 8

Se dan las siguientes igualdades:

$$X_1^2 = (H \otimes H) X_2^1 (H \otimes H)\,.$$
$$Z_1^2 = Z_2^1\,.$$
$$X_2^1 = H_1 Z_2^1 H_2\,.$$

7.4.2 Puerta SWAP

Definición 9

La puerta SWAP intercambia la posición de los dos cúbits

$$\text{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Actuando sobre la base computacional la puerta SWAP es

$$\text{SWAP}|00\rangle = |00\rangle$$
$$\text{SWAP}|01\rangle = |10\rangle$$
$$\text{SWAP}|10\rangle = |01\rangle$$
$$\text{SWAP}|11\rangle = |11\rangle\,.$$

Resultado 9

La puerta SWAP cumple

$$\text{SWAP} = X_1^2 X_2^1 X_1^2\,.$$

7.4.3 Puertas de múltiples controles

Definición 10

Sea U una puerta cuántica de un cúbit. Denotamos por $U_k^{j_1 j_2 \cdots j_m}$ a la puerta controlada de U con el cúbit $j_1, j_2, \ldots, j_m$ como control y el cúbit k como objetivo.

Definición 11: Puerta Toffoli (CCNOT)

La puerta Toffoli es un CNOT con dos controles

$$\text{CCNOT} = X_3^{12} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Aplica X al tercer cúbit solo si los primeros dos están en $|11\rangle$.

7.5 Evolución Temporal y Hamiltonianos

Recordemos que la evolución temporal de un sistema cuántico aislado está gobernada por la ecuación de Schrödinger estacionaria

$$\frac{d}{dt}|\psi(t)\rangle = -\frac{i}{\hbar}H|\psi(t)\rangle\,,$$

donde H es el Hamiltoniano (operador hermitiano).

La solución formal es:

$$|\psi(t)\rangle = e^{-iHt/\hbar}|\psi(0)\rangle$$

Ejemplo 8: Evolución bajo Hamiltoniano de Pauli

Para $H = \omega Z/2$ tenemos que

$$e^{-iHt} = e^{-i\omega t Z/2} = \cos\frac{\omega t}{2}I - i\sin\frac{\omega t}{2}Z = \begin{pmatrix} e^{-i\omega t/2} & 0 \\ 0 & e^{i\omega t/2} \end{pmatrix}.$$

Un cúbit inicialmente en $|+\rangle$ evoluciona como

$$|\psi(t)\rangle = \frac{1}{\sqrt{2}}(e^{-i\omega t/2}|0\rangle + e^{i\omega t/2}|1\rangle)\,.$$

Como sabemos calcular la exponencial de una matriz a partir de sus valores propios y vectores propios, podemos calcular la exponencial de un Hamiltoniano.

Para una matriz hermitiana H con descomposición espectral $H = \sum_i \lambda_i P_i$ donde P_i son las

proyecciones sobre los subespacios propios, tenemos que

$$e^{-iHt} = \sum_i e^{-i\lambda_i t} P_i \, .$$

Ejemplo 9: Exponencial de combinaciones de Pauli

Para $H = \alpha X + \beta Y + \gamma Z$ con $|\vec{n}| = \sqrt{\alpha^2 + \beta^2 + \gamma^2}$,

$$e^{-iHt} = \cos(|\vec{n}|t)I - i \sin(|\vec{n}|t)\frac{\vec{n} \cdot \vec{\sigma}}{|\vec{n}|} \, .$$

Teorema 10

Cualquier operador unitario en $\mathcal{C}^n$ puede aproximarse arbitrariamente bien usando solo las puertas H, T, y CNOT.

Este resultado es fundamental para la computación cuántica práctica, ya que muestra que solo necesitamos implementar físicamente un pequeño conjunto de puertas para realizar cualquier cálculo cuántico.

Ejemplo 10: Estados de Bell

A partir del estádo básico $|00\rangle$ podemos construir cualquier estado de Bell aplicando las puertas H y X_2^1. Por ejemplo

$$X_2^1 H_1 |00\rangle = X_2^1 \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \left|\Phi^+\right\rangle \, .$$

Ejemplo 11: Estado GHZ

El estado Greenberger-Horne-Zeilinger (GHZ) es un estado de tres cúbits que es un estado de Bell generalizado. Su construcción es similar a la de los estados de Bell, pero en lugar de aplicar X_2^1 aplicamos $X_2^1 X_3^2$.

$$X_3^2 X_2^1 H_1 |000\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) = |\text{GHZ}\rangle \, .$$

Este último resultado, nos hace preguntarnos por la existencia de algún conjunto de puertas cuánticas que permitan construir cualquier operador unitario en $\mathcal{C}^n$ de forma exacta y no aproximada. La respuesta es negativa.

Sin embargo, podemos construir cualquier operador unitario en $\mathcal{C}^n$ de forma aproximada usando solo las puertas H, T, y CNOT.

De forma exacta, podemos construir cualquier operador unitario en $\mathcal{C}^n$ usando puertas controladas de un cúbit y puertas de un cúbit parametrizadas, obteniendo una conjunto infinito

no numerable de puertas, pero construibles. En particular el siguiente conjunto permite esta construcción

$$\{U(\alpha,\beta,\gamma), X_j^i \mid \alpha,\beta,\gamma \in \mathbb{R} \quad 1 \leq i \neq j \leq 2^n\}\,.$$

Ejemplo 12.

Veamos algunos ejemplos de puertas comunmente usadas en computación cuántica y como se puede construir a partir de las puertas H, T y CNOT.

- **Puerta SWAP**: intercambia dos cúbits. Se puede construir como

$$\text{SWAP} = X_1^2 X_2^1 X_1^2\,.$$

- **Puerta Fredkin (CSWAP)**: es una puerta de tres cúbits que intercambia los dos últimos cúbits si el primero está en $|1\rangle$. Se puede construir como

$$\text{CSWAP} = X_2^{13} X_3^{12} X_2^{13}\,.$$

- **Puerta fase 90º**: es una puerta de un cúbit que introduce una fase de 90 grados al estado $|1\rangle$. Se puede construir como

$$\text{S} = TT\,.$$

- textbfPuerta NOT: es una puerta de un cúbit que invierte los estados $|0\rangle$ y $|1\rangle$. Se puede construir como

$$X = HTTTTH\,.$$

Por último veamos el teorema de no clonación. Este teorema nos impide clonar estados cuánticos arbitrariamente y es el motivo por el que no podemos implementar clonadores cuánticos o dicho de otra manera, no podemos hacer copias de estados cuánticos.

Teorema 11: Teorema de no clonación

No existe un operador unitario que pueda clonar estados cuánticos arbitrariamente.

Demostración.

Supongamos que existe un operador unitario U que clona estados cuánticos arbitrarios, es decir, para cualquier estado $|\psi\rangle$ y un estado base $|e\rangle$,

$$U|e\psi\rangle = |\psi\psi\rangle\,.$$

Consideremos el estado cuántico $|\psi\rangle$ con respecto a la base canónica

$$|\psi\rangle = \sum_{j=0}^{2^n-1} \alpha_j |j\rangle\,.$$

Entonces el estado clonado sería

$$U|e\psi\rangle = \sum_{j=0}^{2^n-1} \alpha_j U|ej\rangle = \sum_{j=0}^{2^n-1} \alpha_j |jj\rangle \,,$$

Igualando ambas expresiones tenemos que

$$\sum_{j=0}^{2^n-1} \alpha_j |jj\rangle = |\psi\psi\rangle \,,$$

siendo esta igualdad una contradición porque el estado de la izquierda es un estado entrelazado, mientras que el de la derecha no lo es.

Por lo tanto, no existe un operador unitario que pueda clonar estados cuánticos arbitrarios. □

A fondo

Los siguientes libros pueden servir de material de apoyo y para profundizar más en los contenidos de este tema.

Nielsen, M. A., and Chuang, I. L. (2010). Quantum computation and quantum information : 10th anniversary edition. Cambridge University Press.

El capítulo 4 formaliza los conceptos de operadores lineales y matrices en espacios de Hilbert para computación cuántica. Presenta las puertas unitarias sobre un cúbit y prepara el camino para el estudio de operadores más generales.

Nakara, M. (2007). Quantum computing : from linear algebra to physical realizations. CRC Press.

En los capítulos 3 y 4 presenta las bases de la computación cuántica, cúbits, puertas cuánticas y circuitos cuánticos, haciendo uso de los conceptos de álgebra lineal.

Yanofsky, N. S., and Mannucci, M. A. (2008). Quantum computing for computer scientists. Cambridge University Press.

El capítulo 5 nos permitirá amplicar nuestro conocimiento sobre operadores cúbit y puertas cuánticas, así como la representación matricial de los mismos.

Problemas

1. Demuestre que las siguientes matrices son unitarias:

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

b) $U_2 = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & \sqrt{2} \\ \sqrt{2} & -1 \end{pmatrix}$

2. Exprese la puerta Y como producto de rotaciones R_x y R_z.

3. Construya explícitamente la matriz 4×4 para la puerta Controlled-$R_y(\pi/3)$.

4. Un qubit inicialmente en estado $|+\rangle$ evoluciona bajo el Hamiltoniano $H = \sigma_x + \sigma_z$.

a) Calcule e^{-iHt}

b) Determine $|\psi(t)\rangle$

c) ¿Cuál es el período de oscilación?

5. Utilizando la notación de Dirac, demuestre que la puerta CSWAP puede escribirse como

$$\text{CSWAP} = |0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes \text{SWAP}\,.$$

6. Demuestre que la puerta CNOT puede construirse a partir de puertas Hadamard y CZ.

7. Muestre que la puerta SWAP puede construirse a partir de tres puertas CNOT.

8. Comprueba que la matriz de Hadamard es equivalente a $\dfrac{X+Z}{\sqrt{2}}$.

9. Demuestra que todo operador unitario y hermítico tiene autovalores ± 1.

10. Demuestra las siguientes igualdades:

a) $HXH = Z$.

b) $HZH = X$.

c) $HYH = -Y$.

d) $X_1^2 = H_1 H_2 X_2^1 H_1 H_2$.

e) $Z_1^2 = Z_2^1$.

11. Considere el siguiente operador unitario sobre 3 cúbits

$$U = H_1(\text{SWAP})^1_{2,3}H_1\,.$$

Dado dos cúbits $|a\rangle$ y $|b\rangle$,

a) ¿cuál es el resultado de aplicar U al estado $|0ab\rangle$?

b) ¿Cual es la probabilidad de medir el primer cúbit en estado $|0\rangle$ tras aplicar U?

c) Indica como podemos usar este operador para comparar si los cúbits $|a\rangle$ y $|b\rangle$ son iguales.