

Introducción a la computación cuántica

Nicolás Alberto Monzón

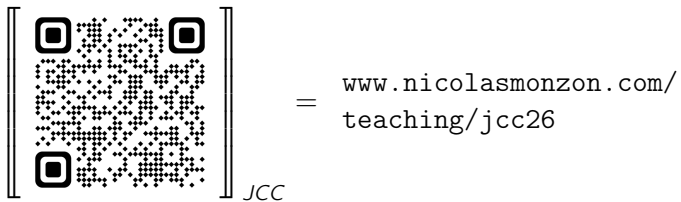
Universidad de la República, Uruguay

XXIV Jornadas de Ciencias de la Computación (JCC)

FCEIA, Universidad Nacional de Rosario

(Versión del 22 de octubre de 2026)

Diapositivas de la clase



Clase $|0\rangle$

Contenido

Introducción y motivación

Postulados de la computación cuántica

Teoremas de no clonado y no borrado

Compuertas cuánticas

Circuitos cuánticos

Teleportación cuántica

Introducción: ¿por qué algoritmos cuánticos?

Algoritmo	Ganancia
Deutsch–Jozsa (1992) f es constante o balanceada?	Exponencial frente a cualquier algoritmo clásico determinista
Shor (1997) Factorizar enteros	Exponencial frente al mejor algoritmo clásico conocido
Grover (1996) Búsqueda sin estructura	Cuadrática frente a cualquier algoritmo clásico

Motivación

*“And I’m not happy with all the analyses that go with just the classical theory, because **nature isn’t classical**, dammit, and if you want to make a simulation of nature, you’d better make it **quantum mechanical**, and by golly it’s a wonderful problem, because it doesn’t look so easy. Thank you”*

— Richard P. Feynman (1981)

Contenido

Introducción y motivación

Postulados de la computación cuántica

Teoremas de no clonado y no borrado

Compuertas cuánticas

Circuitos cuánticos

Teleportación cuántica

Postulado 1: espacio de estados

Postulado 1 (Espacio de estados)

A cada sistema cuántico aislado le corresponde un espacio vectorial complejo con producto interno: su espacio de estados. En cada instante, el sistema queda descrito por completo por un vector de norma 1 de ese espacio: su vector de estado.

Repaso: espacios vectoriales

Un **espacio vectorial** sobre $\mathbb{C}$ es un conjunto $V \neq \emptyset$ con

- ▶ una suma $|u\rangle + |v\rangle \in V$, y
- ▶ un producto por escalares $c |u\rangle \in V$, con $c \in \mathbb{C}$.

Repaso: espacios vectoriales

Un **espacio vectorial** sobre $\mathbb{C}$ es un conjunto $V \neq \emptyset$ con

- ▶ una suma $|u\rangle + |v\rangle \in V$, y
- ▶ un producto por escalares $c|u\rangle \in V$, con $c \in \mathbb{C}$.

Nota: usamos la notación de Dirac: los vectores se escriben $|u\rangle$ (“ket u ”), salvo el vector nulo, que es 0.

Repaso: espacios vectoriales

Un **espacio vectorial** sobre $\mathbb{C}$ es un conjunto $V \neq \emptyset$ con

- ▶ una suma $|u\rangle + |v\rangle \in V$, y
- ▶ un producto por escalares $c|u\rangle \in V$, con $c \in \mathbb{C}$.

Nota: usamos la notación de Dirac: los vectores se escriben $|u\rangle$ (“ket u ”), salvo el vector nulo, que es 0.

Una **base** es un conjunto $\{|v_1\rangle, \dots, |v_n\rangle\}$ linealmente independiente tal que todo vector se escribe como

$$|u\rangle = c_1 |v_1\rangle + \dots + c_n |v_n\rangle, \quad c_i \in \mathbb{C}.$$

La cantidad n de elementos de la base es la **dimensión** de V .

Repaso: bra y producto interno

Si $|u\rangle = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$, su **bra** es el **ket daga**, es decir, su transpuesto conjugado:

$$\langle u| = |u\rangle^\dagger = (u_1^* \quad \cdots \quad u_n^*)$$

Repaso: bra y producto interno

Si $|u\rangle = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$, su **bra** es el **ket daga**, es decir, su transpuesto conjugado:

$$\langle u| = |u\rangle^\dagger = (u_1^* \quad \cdots \quad u_n^*)$$

El **producto interno** es el producto “bra por ket”:

$$\langle u|v\rangle = \langle u| \, |v\rangle = \sum_{i=1}^n u_i^* v_i \in \mathbb{C}$$

Repaso: bra y producto interno

Si $|u\rangle = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$, su **bra** es el **ket daga**, es decir, su transpuesto conjugado:

$$\langle u| = |u\rangle^\dagger = (u_1^* \quad \cdots \quad u_n^*)$$

El **producto interno** es el producto “bra por ket”:

$$\langle u|v\rangle = \langle u| \, |v\rangle = \sum_{i=1}^n u_i^* v_i \in \mathbb{C}$$

Ejemplo: si $|u\rangle = \begin{pmatrix} 1 \\ i \end{pmatrix}$ y $|v\rangle = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$, entonces $\langle u| = (1 \quad -i)$ y $\langle u|v\rangle = 2 - i$.

Repaso: norma, bases ortonormales y espacios de Hilbert

La **norma** es $\| |v\rangle \| = \sqrt{\langle v|v\rangle}$, y

- ▶ $|v\rangle$ es **unitario** si $\| |v\rangle \| = 1$;
- ▶ $\{|u_1\rangle, \dots, |u_n\rangle\}$ es una **base ortonormal** si es base y $\langle u_i|u_j\rangle = \delta_{ij}$.

Repaso: norma, bases ortonormales y espacios de Hilbert

La **norma** es $\| |v\rangle \| = \sqrt{\langle v|v\rangle}$, y

- ▶ $|v\rangle$ es **unitario** si $\| |v\rangle \| = 1$;
- ▶ $\{|u_1\rangle, \dots, |u_n\rangle\}$ es una **base ortonormal** si es base y $\langle u_i|u_j\rangle = \delta_{ij}$.

En dimensión finita, un **espacio de Hilbert** es un espacio vectorial complejo con producto interno.

Repaso: norma, bases ortonormales y espacios de Hilbert

La **norma** es $\| |v\rangle \| = \sqrt{\langle v|v\rangle}$, y

- ▶ $|v\rangle$ es **unitario** si $\| |v\rangle \| = 1$;
- ▶ $\{|u_1\rangle, \dots, |u_n\rangle\}$ es una **base ortonormal** si es base y $\langle u_i|u_j\rangle = \delta_{ij}$.

En dimensión finita, un **espacio de Hilbert** es un espacio vectorial complejo con producto interno.

Nota: en lo que sigue, $\mathcal{H}_d = \mathbb{C}^{2^d}$: el espacio de d qubits, de dimensión 2^d .

Postulado 1 en notación de Dirac

Postulado 1 (Espacio de estados)

El estado de un sistema cuántico aislado es un vector $|\psi\rangle \in \mathcal{H}_d$ tal que $\langle\psi|\psi\rangle = 1$.

Postulado 1 en notación de Dirac

Postulado 1 (Espacio de estados)

El estado de un sistema cuántico aislado es un vector $|\psi\rangle \in \mathcal{H}_d$ tal que $\langle\psi|\psi\rangle = 1$.

El caso más simple es el **qubit**: $d = 1$, $\mathcal{H}_1 = \mathbb{C}^2$, con la **base computacional**

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

Postulado 1 en notación de Dirac

Postulado 1 (Espacio de estados)

El estado de un sistema cuántico aislado es un vector $|\psi\rangle \in \mathcal{H}_d$ tal que $\langle\psi|\psi\rangle = 1$.

El caso más simple es el **qubit**: $d = 1$, $\mathcal{H}_1 = \mathbb{C}^2$, con la **base computacional**

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

Un qubit puede estar en una **superposición**

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1,$$

donde $\alpha, \beta \in \mathbb{C}$ se llaman **amplitudes**.

Otra base: $|+\rangle$ y $|-\rangle$

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

Otra base: $|+\rangle$ y $|-\rangle$

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

Es una base ortonormal de $\mathbb{C}^2$:

$$\langle +|+\rangle = \langle -|-\rangle = 1 \quad \langle +|-\rangle = \frac{1}{2}(1 - 1) = 0$$

Otra base: $|+\rangle$ y $|-\rangle$

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

Es una base ortonormal de $\mathbb{C}^2$:

$$\langle +|+\rangle = \langle -|-\rangle = 1 \quad \langle +|-\rangle = \frac{1}{2}(1 - 1) = 0$$

Todo qubit se puede escribir en cualquiera de las dos bases:

$$\alpha|0\rangle + \beta|1\rangle = \frac{\alpha + \beta}{\sqrt{2}}|+\rangle + \frac{\alpha - \beta}{\sqrt{2}}|-\rangle$$

Ejercicios

Considere los siguientes vectores de $\mathbb{C}^2$:

$$\alpha \begin{pmatrix} 1 \\ i \end{pmatrix} \quad \beta \begin{pmatrix} 3 \\ -4 \end{pmatrix} \quad \gamma \begin{pmatrix} 1 \\ \sqrt{3} \end{pmatrix}$$

- a) Encuentre valores de $\alpha, \beta, \gamma \in \mathbb{C}$ para los que cada vector representa un estado cuántico de un qubit.
- b) Escriba esos estados en notación de Dirac, en la base computacional $\{|0\rangle, |1\rangle\}$ y en la base $\{|+\rangle, |-\rangle\}$.

Postulado 2: evolución

Postulado 2 (Evolución, versión continua)

El estado de un sistema cuántico aislado cambia en el tiempo según la ecuación de Schrödinger:

$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle$$

- ▶ $\hbar$ es la **constante de Planck** (reducida), que se determina experimentalmente.
- ▶ H es el **hamiltoniano** del sistema: un operador hermítico fijo.

Postulado 2: evolución

Postulado 2 (Evolución, versión continua)

El estado de un sistema cuántico aislado cambia en el tiempo según la ecuación de Schrödinger:

$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle$$

- ▶ $\hbar$ es la **constante de Planck** (reducida), que se determina experimentalmente.
- ▶ H es el **hamiltoniano** del sistema: un operador hermítico fijo.

Nota: este postulado también se puede formular en términos de *observables*.

Postulado 2: la versión que vamos a usar

Postulado 2 (Evolución)

La evolución de un sistema cuántico aislado está dada por una transformación unitaria: el estado en un instante t_1 y el estado en un instante posterior t_2 se relacionan mediante un operador unitario que depende sólo de t_1 y t_2 .

Repaso: operadores

Un **operador lineal** A sobre $\mathcal{H}$ cumple

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

y, fijada una base, se representa con una matriz.

Repaso: operadores

Un **operador lineal** A sobre $\mathcal{H}$ cumple

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

y, fijada una base, se representa con una matriz.

El **adjunto** $A^\dagger$ es la matriz transpuesta conjugada, como con el bra.

- ▶ A es **hermítico** si $A^\dagger = A$.
- ▶ U es **unitario** si $U^\dagger U = UU^\dagger = I$.

Repaso: operadores

Un **operador lineal** A sobre $\mathcal{H}$ cumple

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

y, fijada una base, se representa con una matriz.

El **adjunto** $A^\dagger$ es la matriz transpuesta conjugada, como con el bra.

- ▶ A es **hermítico** si $A^\dagger = A$.
- ▶ U es **unitario** si $U^\dagger U = UU^\dagger = I$.

Un operador unitario preserva el producto interno, y en particular la norma:

$$(U|u\rangle)^\dagger U|v\rangle = \langle u| U^\dagger U|v\rangle = \langle u|v\rangle$$

Postulado 2 en notación de Dirac

Postulado 2 (Evolución)

Si el estado del sistema en t_1 es $|\psi\rangle$, en t_2 es

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

para un operador unitario U que depende sólo de t_1 y t_2 .

Postulado 2 en notación de Dirac

Postulado 2 (Evolución)

Si el estado del sistema en t_1 es $|\psi\rangle$, en t_2 es

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

para un operador unitario U que depende sólo de t_1 y t_2 .

Como U preserva la norma, $|\psi'\rangle$ también es un estado: $\langle\psi'|\psi'\rangle = \langle\psi|\psi\rangle = 1$.

Postulado 2 en notación de Dirac

Postulado 2 (Evolución)

Si el estado del sistema en t_1 es $|\psi\rangle$, en t_2 es

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

para un operador unitario U que depende sólo de t_1 y t_2 .

Como U preserva la norma, $|\psi'\rangle$ también es un estado: $\langle\psi'|\psi'\rangle = \langle\psi|\psi\rangle = 1$.

Ejemplo: $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ es unitario y

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

Ejercicio

Las **matrices de Pauli** son

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

Demuestre que X , Y y Z son hermíticas y unitarias.

Postulado 3: medición

Postulado 3 (Medición)

Una medición tiene un conjunto de resultados posibles, y a cada resultado le corresponde un operador sobre el espacio de estados. El resultado que se obtiene es aleatorio: su probabilidad depende del estado del sistema justo antes de medir. Medir modifica el sistema: después de obtener un resultado, el estado pasa a ser uno que depende de ese resultado.

Repaso: producto externo y proyectores

El **producto externo** de $|u\rangle$ y $|v\rangle$ es el operador “ket por bra”:

$$|u\rangle \langle v| \quad \text{que actúa como} \quad (|u\rangle \langle v|) |w\rangle = \langle v|w\rangle |u\rangle$$

Repaso: producto externo y proyectores

El **producto externo** de $|u\rangle$ y $|v\rangle$ es el operador “ket por bra”:

$$|u\rangle \langle v| \quad \text{que actúa como} \quad (|u\rangle \langle v|) |w\rangle = \langle v|w\rangle |u\rangle$$

Ejemplo: $|0\rangle \langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

Repaso: producto externo y proyectores

El **producto externo** de $|u\rangle$ y $|v\rangle$ es el operador “ket por bra”:

$$|u\rangle \langle v| \quad \text{que actúa como} \quad (|u\rangle \langle v|) |w\rangle = \langle v|w\rangle |u\rangle$$

Ejemplo: $|0\rangle \langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

Un operador P es un **proyector** si $P^2 = P$.

- ▶ Si $|u\rangle$ es unitario, $|u\rangle \langle u|$ es un proyector.
- ▶ Si $\{|u_1\rangle, \dots, |u_n\rangle\}$ es una base ortonormal, $\sum_i |u_i\rangle \langle u_i| = I$.

Postulado 3 en notación de Dirac

Postulado 3 (Medición)

Una medición es un conjunto $\{M_m\}$ de operadores, uno por cada resultado posible m , tales que $\sum_m M_m^\dagger M_m = I$. Si el estado es $|\psi\rangle$, el resultado m se obtiene con probabilidad

$$p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle$$

y el estado pasa a ser $\frac{M_m |\psi\rangle}{\sqrt{p(m)}}$.

Postulado 3 en notación de Dirac

Postulado 3 (Medición)

Una medición es un conjunto $\{M_m\}$ de operadores, uno por cada resultado posible m , tales que $\sum_m M_m^\dagger M_m = I$. Si el estado es $|\psi\rangle$, el resultado m se obtiene con probabilidad

$$p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle$$

y el estado pasa a ser $\frac{M_m |\psi\rangle}{\sqrt{p(m)}}$.

La condición $\sum_m M_m^\dagger M_m = I$ dice que las probabilidades suman 1:

$$\sum_m p(m) = \langle \psi | \left(\sum_m M_m^\dagger M_m \right) | \psi \rangle = \langle \psi | \psi \rangle = 1$$

Medir en una base: la regla de Born

El caso que más vamos a usar: dada una base ortonormal $\{|e_k\rangle\}$, tomamos $M_k = |e_k\rangle\langle e_k|$.

Regla de Born

Al medir $|\psi\rangle$ en la base $\{|e_k\rangle\}$, el resultado k se obtiene con probabilidad

$$p(k) = |\langle e_k|\psi\rangle|^2$$

y, si sale k , el estado pasa a ser $|e_k\rangle$ (a menos de una fase).

Medir en una base: la regla de Born

El caso que más vamos a usar: dada una base ortonormal $\{|e_k\rangle\}$, tomamos $M_k = |e_k\rangle\langle e_k|$.

Regla de Born

Al medir $|\psi\rangle$ en la base $\{|e_k\rangle\}$, el resultado k se obtiene con probabilidad

$$p(k) = |\langle e_k | \psi \rangle|^2$$

y, si sale k , el estado pasa a ser $|e_k\rangle$ (a menos de una fase).

Ejemplo: midiendo $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ en la base computacional:

- ▶ sale 0 con probabilidad $|\alpha|^2$, y el estado pasa a ser $|0\rangle$;
- ▶ sale 1 con probabilidad $|\beta|^2$, y el estado pasa a ser $|1\rangle$.

Medir en una base: la regla de Born

El caso que más vamos a usar: dada una base ortonormal $\{|e_k\rangle\}$, tomamos $M_k = |e_k\rangle\langle e_k|$.

Regla de Born

Al medir $|\psi\rangle$ en la base $\{|e_k\rangle\}$, el resultado k se obtiene con probabilidad

$$p(k) = |\langle e_k | \psi \rangle|^2$$

y, si sale k , el estado pasa a ser $|e_k\rangle$ (a menos de una fase).

Ejemplo: midiendo $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ en la base computacional:

- ▶ sale 0 con probabilidad $|\alpha|^2$, y el estado pasa a ser $|0\rangle$;
- ▶ sale 1 con probabilidad $|\beta|^2$, y el estado pasa a ser $|1\rangle$.

Nota: $|\psi\rangle$ y $e^{i\theta}|\psi\rangle$ dan las mismas probabilidades para toda medición: la **fase global** no se puede observar.

Ejercicio

Para cada uno de los estados del ejercicio del postulado 1,

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} \quad \frac{1}{5} \begin{pmatrix} 3 \\ -4 \end{pmatrix} \quad \frac{1}{2} \begin{pmatrix} 1 \\ \sqrt{3} \end{pmatrix}$$

- a) calcule la probabilidad de obtener cada resultado al medir en la base computacional $\{|0\rangle, |1\rangle\}$;
- b) ídem al medir en la base $\{|+\rangle, |-\rangle\}$.

Postulado 4: sistemas compuestos

Postulado 4 (Sistemas compuestos)

Si un sistema está formado por varias partes, su espacio de estados es el producto tensorial de los espacios de estados de cada parte. Si cada parte está en su propio estado, el estado del sistema completo es el producto tensorial de esos estados.

Repaso: producto tensorial

Si $\{|u_i\rangle\}$ es base de $\mathcal{H}$ y $\{|v_j\rangle\}$ es base de $\mathcal{H}'$, el **producto tensorial** $\mathcal{H} \otimes \mathcal{H}'$ es el espacio con base $\{|u_i\rangle \otimes |v_j\rangle\}$. Su dimensión es $\dim \mathcal{H} \cdot \dim \mathcal{H}'$.

Repaso: producto tensorial

Si $\{|u_i\rangle\}$ es base de $\mathcal{H}$ y $\{|v_j\rangle\}$ es base de $\mathcal{H}'$, el **producto tensorial** $\mathcal{H} \otimes \mathcal{H}'$ es el espacio con base $\{|u_i\rangle \otimes |v_j\rangle\}$. Su dimensión es $\dim \mathcal{H} \cdot \dim \mathcal{H}'$.

Nota: abreviamos $|u\rangle \otimes |v\rangle = |u\rangle |v\rangle = |uv\rangle$.

Repaso: producto tensorial

Si $\{|u_i\rangle\}$ es base de $\mathcal{H}$ y $\{|v_j\rangle\}$ es base de $\mathcal{H}'$, el **producto tensorial** $\mathcal{H} \otimes \mathcal{H}'$ es el espacio con base $\{|u_i\rangle \otimes |v_j\rangle\}$. Su dimensión es $\dim \mathcal{H} \cdot \dim \mathcal{H}'$.

Nota: abreviamos $|u\rangle \otimes |v\rangle = |u\rangle |v\rangle = |uv\rangle$.

En coordenadas es el **producto de Kronecker**:

$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a \begin{pmatrix} c \\ d \end{pmatrix} \\ b \begin{pmatrix} c \\ d \end{pmatrix} \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}$$

Repaso: producto tensorial

Si $\{|u_i\rangle\}$ es base de $\mathcal{H}$ y $\{|v_j\rangle\}$ es base de $\mathcal{H}'$, el **producto tensorial** $\mathcal{H} \otimes \mathcal{H}'$ es el espacio con base $\{|u_i\rangle \otimes |v_j\rangle\}$. Su dimensión es $\dim \mathcal{H} \cdot \dim \mathcal{H}'$.

Nota: abreviamos $|u\rangle \otimes |v\rangle = |u\rangle |v\rangle = |uv\rangle$.

En coordenadas es el **producto de Kronecker**:

$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a \begin{pmatrix} c \\ d \end{pmatrix} \\ b \begin{pmatrix} c \\ d \end{pmatrix} \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}$$

Los operadores actúan por separado en cada parte:

$$(A \otimes B)(|u\rangle \otimes |v\rangle) = A|u\rangle \otimes B|v\rangle.$$

Postulado 4 en notación de Dirac

Postulado 4 (Sistemas compuestos)

Si las partes $1, \dots, n$ tienen espacios de estados $\mathcal{H}^{(1)}, \dots, \mathcal{H}^{(n)}$, el sistema completo tiene espacio $\mathcal{H}^{(1)} \otimes \dots \otimes \mathcal{H}^{(n)}$. Si la parte i está en el estado $|\psi_i\rangle$, el sistema está en $|\psi_1\rangle \otimes \dots \otimes |\psi_n\rangle$.

Postulado 4 en notación de Dirac

Postulado 4 (Sistemas compuestos)

Si las partes $1, \dots, n$ tienen espacios de estados $\mathcal{H}^{(1)}, \dots, \mathcal{H}^{(n)}$, el sistema completo tiene espacio $\mathcal{H}^{(1)} \otimes \dots \otimes \mathcal{H}^{(n)}$. Si la parte i está en el estado $|\psi_i\rangle$, el sistema está en $|\psi_1\rangle \otimes \dots \otimes |\psi_n\rangle$.

Por eso $\mathcal{H}_d = \mathbb{C}^{2^d} = \underbrace{\mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2}_d$: d qubits.

Postulado 4 en notación de Dirac

Postulado 4 (Sistemas compuestos)

Si las partes $1, \dots, n$ tienen espacios de estados $\mathcal{H}^{(1)}, \dots, \mathcal{H}^{(n)}$, el sistema completo tiene espacio $\mathcal{H}^{(1)} \otimes \dots \otimes \mathcal{H}^{(n)}$. Si la parte i está en el estado $|\psi_i\rangle$, el sistema está en $|\psi_1\rangle \otimes \dots \otimes |\psi_n\rangle$.

Por eso $\mathcal{H}_d = \mathbb{C}^{2^d} = \underbrace{\mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2}_d$: d qubits.

Ejemplo: la **base computacional** de dos qubits es

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Estados producto y entrelazados

Un estado $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H}'$ es **producto** si existen $|a\rangle \in \mathcal{H}$ y $|b\rangle \in \mathcal{H}'$ tales que $|\psi\rangle = |a\rangle |b\rangle$. Si no, es **entrelazado**.

Estados producto y entrelazados

Un estado $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H}'$ es **producto** si existen $|a\rangle \in \mathcal{H}$ y $|b\rangle \in \mathcal{H}'$ tales que $|\psi\rangle = |a\rangle |b\rangle$. Si no, es **entrelazado**.

Ejemplo: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ es entrelazado. Si fuera producto,

$$(a_0 |0\rangle + a_1 |1\rangle)(b_0 |0\rangle + b_1 |1\rangle) = a_0 b_0 |00\rangle + a_0 b_1 |01\rangle + a_1 b_0 |10\rangle + a_1 b_1 |11\rangle$$

y necesitaríamos $a_0 b_0 \neq 0$, $a_1 b_1 \neq 0$ y $a_0 b_1 = 0$: imposible.

Estados producto y entrelazados

Un estado $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H}'$ es **producto** si existen $|a\rangle \in \mathcal{H}$ y $|b\rangle \in \mathcal{H}'$ tales que $|\psi\rangle = |a\rangle |b\rangle$. Si no, es **entrelazado**.

Ejemplo: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ es entrelazado. Si fuera producto,

$$(a_0 |0\rangle + a_1 |1\rangle)(b_0 |0\rangle + b_1 |1\rangle) = a_0 b_0 |00\rangle + a_0 b_1 |01\rangle + a_1 b_0 |10\rangle + a_1 b_1 |11\rangle$$

y necesitaríamos $a_0 b_0 \neq 0$, $a_1 b_1 \neq 0$ y $a_0 b_1 = 0$: imposible.

Nota: el postulado 4 dice cómo combinar estados de las partes, pero no todo estado del sistema completo se obtiene así.

Ejercicio

- a) Escriba $|+\rangle \otimes |-\rangle$ y $|-\rangle^{\otimes 2} = |-\rangle \otimes |-\rangle$ en la base computacional, con productos tensoriales y con el producto de Kronecker.
- b) Indique si cada uno de los siguientes estados es producto o entrelazado:

$$\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

$$\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

Contenido

Introducción y motivación

Postulados de la computación cuántica

Teoremas de no clonado y no borrado

Compuertas cuánticas

Circuitos cuánticos

Teleportación cuántica

Teorema de no clonado

No clonado, en palabras

No existe un procedimiento cuántico que, dado un estado desconocido, produzca una copia de él.

- ▶ Wootters y Zurek (1982).
- ▶ Contraste con lo clásico: copiar un bit es trivial.

Teorema de no clonado

Teorema (No clonado)

No existen un operador unitario U y un estado $|\phi\rangle$ tales que $U |\psi\rangle |\phi\rangle = |\psi\rangle |\psi\rangle$ para todo estado $|\psi\rangle$.

Teorema de no clonado

Teorema (No clonado)

No existen un operador unitario U y un estado $|\phi\rangle$ tales que $U|\psi\rangle|\phi\rangle = |\psi\rangle|\psi\rangle$ para todo estado $|\psi\rangle$.

Demostración.

Si existieran, para dos estados $|\psi\rangle$ y $|\varphi\rangle$ cualesquiera:

- ▶ como U preserva el producto interno,
 $(U|\psi\rangle|\phi\rangle)^\dagger U|\varphi\rangle|\phi\rangle = \langle\psi|\varphi\rangle\langle\phi|\phi\rangle = \langle\psi|\varphi\rangle;$
- ▶ pero también es $(|\psi\rangle|\psi\rangle)^\dagger |\varphi\rangle|\varphi\rangle = \langle\psi|\varphi\rangle^2.$

Entonces $\langle\psi|\varphi\rangle = \langle\psi|\varphi\rangle^2$, es decir, $\langle\psi|\varphi\rangle \in \{0, 1\}$, lo que no vale para cualquier par de estados. □

Teorema de no clonado

Teorema (No clonado)

No existen un operador unitario U y un estado $|\phi\rangle$ tales que $U|\psi\rangle|\phi\rangle = |\psi\rangle|\psi\rangle$ para todo estado $|\psi\rangle$.

Demostración.

Si existieran, para dos estados $|\psi\rangle$ y $|\varphi\rangle$ cualesquiera:

- ▶ como U preserva el producto interno,
 $(U|\psi\rangle|\phi\rangle)^\dagger U|\varphi\rangle|\phi\rangle = \langle\psi|\varphi\rangle\langle\phi|\phi\rangle = \langle\psi|\varphi\rangle;$
- ▶ pero también es $(|\psi\rangle|\psi\rangle)^\dagger |\varphi\rangle|\varphi\rangle = \langle\psi|\varphi\rangle^2.$

Entonces $\langle\psi|\varphi\rangle = \langle\psi|\varphi\rangle^2$, es decir, $\langle\psi|\varphi\rangle \in \{0, 1\}$, lo que no vale para cualquier par de estados. □

Nota: sí se pueden clonar los estados de una base ortonormal *conocida*.

Teorema de no borrado

No borrado, en palabras

No existe un procedimiento cuántico que, dadas dos copias de un estado desconocido, borre una de ellas, llevándola a un estado fijo.

Es el “dual” del no clonado: así como no se puede copiar un estado desconocido, tampoco se puede borrar una de sus copias.

Teorema de no borrado

Teorema (No borrado)

No existe un operador unitario U tal que $U |\psi\rangle |\psi\rangle = |\psi\rangle |0\rangle$ para todo estado $|\psi\rangle$.

Teorema de no borrado

Teorema (No borrado)

No existe un operador unitario U tal que $U |\psi\rangle |\psi\rangle = |\psi\rangle |0\rangle$ para todo estado $|\psi\rangle$.

Demostración.

Si existiera, para dos estados $|\psi\rangle$ y $|\varphi\rangle$ cualesquiera:

- ▶ como U preserva el producto interno, $(U |\psi\rangle |\psi\rangle)^\dagger U |\varphi\rangle |\varphi\rangle = \langle \psi | \varphi \rangle^2$;
- ▶ pero también es $(|\psi\rangle |0\rangle)^\dagger |\varphi\rangle |0\rangle = \langle \psi | \varphi \rangle$.

De nuevo $\langle \psi | \varphi \rangle \in \{0, 1\}$, lo que no vale para cualquier par de estados. □

Ejercicio

La compuerta **CNOT** actúa sobre dos qubits como

$$\text{CNOT } |0\rangle |x\rangle = |0\rangle |x\rangle \quad \text{CNOT } |1\rangle |x\rangle = |1\rangle X|x\rangle \quad (x \in \{0, 1\})$$

y la compuerta de **Hadamard** cumple $H|0\rangle = |+\rangle$ y $H|1\rangle = |-\rangle$.

- a) Muestre que CNOT clona $|0\rangle$ y $|1\rangle$, tomando $|\phi\rangle = |0\rangle$.
- b) Calcule $\text{CNOT } |+\rangle |0\rangle$. ¿Es $|+\rangle |+\rangle$? ¿Es un estado producto?
- c) Usando H y CNOT, construya un operador que clone $|+\rangle$ y $|-\rangle$.

Contenido

Introducción y motivación

Postulados de la computación cuántica

Teoremas de no clonado y no borrado

Compuertas cuánticas

Circuitos cuánticos

Teleportación cuántica

Compuertas de un qubit

Compuerta	Matriz	Acción sobre la base
X (negación)	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$X 0\rangle = 1\rangle, \quad X 1\rangle = 0\rangle$
Z (cambio de fase)	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$Z 0\rangle = 0\rangle, \quad Z 1\rangle = - 1\rangle$
$Y = iXZ$	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	$Y 0\rangle = i 1\rangle, \quad Y 1\rangle = -i 0\rangle$
H (Hadamard)	$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	$H 0\rangle = +\rangle, \quad H 1\rangle = -\rangle$

I , X , Y y Z son las **matrices de Pauli**.

Una compuerta de dos qubits: CNOT

La compuerta CNOT (“NOT controlada”) tiene un qubit de **control** y uno **objetivo**: si el control es $|1\rangle$, aplica X al objetivo.

$$\text{CNOT } |0\rangle |x\rangle = |0\rangle |x\rangle \qquad \text{CNOT } |1\rangle |x\rangle = |1\rangle X|x\rangle$$

Una compuerta de dos qubits: CNOT

La compuerta CNOT (“NOT controlada”) tiene un qubit de **control** y uno **objetivo**: si el control es $|1\rangle$, aplica X al objetivo.

$$\text{CNOT } |0\rangle |x\rangle = |0\rangle |x\rangle \quad \text{CNOT } |1\rangle |x\rangle = |1\rangle X|x\rangle$$

En la base $|00\rangle, |01\rangle, |10\rangle, |11\rangle$:

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

Una compuerta de dos qubits: CNOT

La compuerta CNOT (“NOT controlada”) tiene un qubit de **control** y uno **objetivo**: si el control es $|1\rangle$, aplica X al objetivo.

$$\text{CNOT } |0\rangle |x\rangle = |0\rangle |x\rangle \quad \text{CNOT } |1\rangle |x\rangle = |1\rangle X|x\rangle$$

En la base $|00\rangle, |01\rangle, |10\rangle, |11\rangle$:

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

Con $\oplus$ la suma módulo 2: $\text{CNOT } |x\rangle |y\rangle = |x\rangle |y \oplus x\rangle$.

Ejercicio

- a) Muestre que H es hermítica y unitaria.
- b) Muestre que $HXH = Z$ y que $HZH = X$.
- c) Calcule HYH .
- d) Muestre que CNOT es unitaria.

Contenido

Introducción y motivación

Postulados de la computación cuántica

Teoremas de no clonado y no borrado

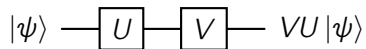
Compuertas cuánticas

Circuitos cuánticos

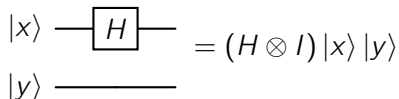
Teleportación cuántica

Cómo se lee un circuito

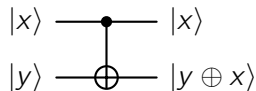
En serie: primero U , después V



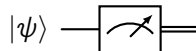
En paralelo: una compuerta por qubit



CNOT: el punto es el control, $\oplus$ el objetivo

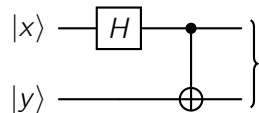


Medición en la base computacional; la línea doble es un bit clásico

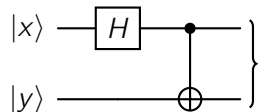


¡Ojo! en serie, el orden del dibujo es el inverso del de la fórmula: VU .

Ejemplo: los estados de Bell


$$\left. \begin{array}{l} |x\rangle \text{ --- } [H] \text{ --- } \bullet \\ |y\rangle \text{ --- } \oplus \end{array} \right\} |\beta_{xy}\rangle = \text{CNOT}(H \otimes I) |x\rangle |y\rangle$$

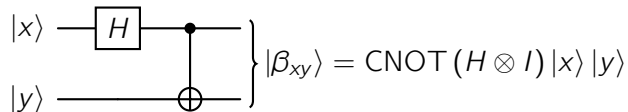
Ejemplo: los estados de Bell


$$\left. \begin{array}{l} |x\rangle \text{ --- } [H] \text{ --- } \bullet \\ |y\rangle \text{ --- } \oplus \end{array} \right\} |\beta_{xy}\rangle = \text{CNOT}(H \otimes I) |x\rangle |y\rangle$$

Ejemplo: con entrada $|00\rangle$:

$$|00\rangle \xrightarrow{H \otimes I} \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) |0\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |10\rangle) \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) = |\beta_{00}\rangle$$

Ejemplo: los estados de Bell



Ejemplo: con entrada $|00\rangle$:

$$|00\rangle \xrightarrow{H \otimes I} \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) |0\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |10\rangle) \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) = |\beta_{00}\rangle$$

Las cuatro salidas son los **estados de Bell**, todos entrelazados:

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad |\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \quad |\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \quad |\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Ejercicio

- a) Verifique las salidas $|\beta_{01}\rangle$, $|\beta_{10}\rangle$ y $|\beta_{11}\rangle$ del circuito de Bell.
- b) Dé un circuito que, a partir de $|000\rangle$, genere el estado $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$.
- c) ¿Qué resultados se pueden obtener al medir $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ en la base computacional, y con qué probabilidades?

Contenido

Introducción y motivación

Postulados de la computación cuántica

Teoremas de no clonado y no borrado

Compuertas cuánticas

Circuitos cuánticos

Teleportación cuántica

Teleportación cuántica

El problema

Alice tiene un qubit en un estado desconocido $|\psi\rangle$ y quiere que Bob lo tenga. Comparten un par entrelazado $|\beta_{00}\rangle$, pero entre ellos sólo pueden enviarse bits clásicos.

Teleportación cuántica

El problema

Alice tiene un qubit en un estado desconocido $|\psi\rangle$ y quiere que Bob lo tenga. Comparten un par entrelazado $|\beta_{00}\rangle$, pero entre ellos sólo pueden enviarse bits clásicos.

- ▶ Alice no puede averiguar $|\psi\rangle$: con una sola copia, medir no alcanza para conocer el estado.
- ▶ Aunque lo conociera, describir α y β con exactitud requiere infinitos bits clásicos.

Teleportación cuántica

El problema

Alice tiene un qubit en un estado desconocido $|\psi\rangle$ y quiere que Bob lo tenga. Comparten un par entrelazado $|\beta_{00}\rangle$, pero entre ellos sólo pueden enviarse bits clásicos.

- ▶ Alice no puede averiguar $|\psi\rangle$: con una sola copia, medir no alcanza para conocer el estado.
- ▶ Aunque lo conociera, describir α y β con exactitud requiere infinitos bits clásicos.

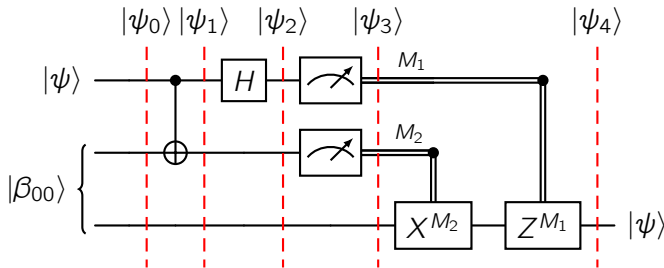
Con la **teleportación**, Alice envía sólo 2 bits clásicos y Bob reconstruye $|\psi\rangle$ (Bennett, Brassard, Crépeau, Jozsa, Peres y Wootters, 1993).

El protocolo

1. Alice y Bob preparan $|\beta_{00}\rangle$: Alice se queda con el primer qubit del par y Bob con el segundo.
2. Alice aplica CNOT entre $|\psi\rangle$ (control) y su qubit del par, y después H a $|\psi\rangle$.
3. Alice mide sus dos qubits y le envía a Bob los resultados M_1, M_2 .
4. Bob aplica $Z^{M_1} X^{M_2}$ a su qubit, y obtiene $|\psi\rangle$.

El protocolo

1. Alice y Bob preparan $|\beta_{00}\rangle$: Alice se queda con el primer qubit del par y Bob con el segundo.
2. Alice aplica CNOT entre $|\psi\rangle$ (control) y su qubit del par, y después H a $|\psi\rangle$.
3. Alice mide sus dos qubits y le envía a Bob los resultados M_1, M_2 .
4. Bob aplica $Z^{M_1} X^{M_2}$ a su qubit, y obtiene $|\psi\rangle$.



Paso a paso: antes de medir

Sea $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. El estado inicial es

$$|\psi_0\rangle = |\psi\rangle |\beta_{00}\rangle = \frac{1}{\sqrt{2}} \left[\alpha|0\rangle (|00\rangle + |11\rangle) + \beta|1\rangle (|00\rangle + |11\rangle) \right]$$

Paso a paso: antes de medir

Sea $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. El estado inicial es

$$|\psi_0\rangle = |\psi\rangle |\beta_{00}\rangle = \frac{1}{\sqrt{2}} \left[\alpha|0\rangle (|00\rangle + |11\rangle) + \beta|1\rangle (|00\rangle + |11\rangle) \right]$$

Alice aplica CNOT a sus dos qubits: si el primero es $|1\rangle$, invierte el segundo.

$$|\psi_1\rangle = \frac{1}{\sqrt{2}} \left[\alpha|0\rangle (|00\rangle + |11\rangle) + \beta|1\rangle (|10\rangle + |01\rangle) \right]$$

Paso a paso: antes de medir

Sea $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. El estado inicial es

$$|\psi_0\rangle = |\psi\rangle |\beta_{00}\rangle = \frac{1}{\sqrt{2}} \left[\alpha|0\rangle (|00\rangle + |11\rangle) + \beta|1\rangle (|00\rangle + |11\rangle) \right]$$

Alice aplica CNOT a sus dos qubits: si el primero es $|1\rangle$, invierte el segundo.

$$|\psi_1\rangle = \frac{1}{\sqrt{2}} \left[\alpha|0\rangle (|00\rangle + |11\rangle) + \beta|1\rangle (|10\rangle + |01\rangle) \right]$$

Alice aplica H a su primer qubit:

$$|\psi_2\rangle = \frac{1}{2} \left[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle) \right]$$

Paso a paso: reagrupar

Distribuyendo y agrupando según los dos qubits de Alice:

$$\begin{aligned} |\psi_2\rangle = \frac{1}{2} \bigg[& |00\rangle (\alpha |0\rangle + \beta |1\rangle) + |01\rangle (\alpha |1\rangle + \beta |0\rangle) \\ & + |10\rangle (\alpha |0\rangle - \beta |1\rangle) + |11\rangle (\alpha |1\rangle - \beta |0\rangle) \bigg] \end{aligned}$$

Paso a paso: reagrupar

Distribuyendo y agrupando según los dos qubits de Alice:

$$\begin{aligned} |\psi_2\rangle = \frac{1}{2} \bigg[& |00\rangle (\alpha |0\rangle + \beta |1\rangle) + |01\rangle (\alpha |1\rangle + \beta |0\rangle) \\ & + |10\rangle (\alpha |0\rangle - \beta |1\rangle) + |11\rangle (\alpha |1\rangle - \beta |0\rangle) \bigg] \end{aligned}$$

Cada término tiene amplitud $\frac{1}{2}$ y un estado unitario para Bob: por la regla de Born, cada resultado $M_1 M_2$ de Alice sale con probabilidad $\frac{1}{4}$.

Paso a paso: medir y corregir

Si Alice obtiene $M_1 M_2$, el qubit de Bob queda en $|\psi_3(M_1 M_2)\rangle$, que se lee del término correspondiente:

$$00 \mapsto |\psi_3(00)\rangle = \alpha |0\rangle + \beta |1\rangle$$

$$01 \mapsto |\psi_3(01)\rangle = \alpha |1\rangle + \beta |0\rangle$$

$$10 \mapsto |\psi_3(10)\rangle = \alpha |0\rangle - \beta |1\rangle$$

$$11 \mapsto |\psi_3(11)\rangle = \alpha |1\rangle - \beta |0\rangle$$

Paso a paso: medir y corregir

Si Alice obtiene $M_1 M_2$, el qubit de Bob queda en $|\psi_3(M_1 M_2)\rangle$, que se lee del término correspondiente:

$$00 \mapsto |\psi_3(00)\rangle = \alpha |0\rangle + \beta |1\rangle$$

$$01 \mapsto |\psi_3(01)\rangle = \alpha |1\rangle + \beta |0\rangle$$

$$10 \mapsto |\psi_3(10)\rangle = \alpha |0\rangle - \beta |1\rangle$$

$$11 \mapsto |\psi_3(11)\rangle = \alpha |1\rangle - \beta |0\rangle$$

Cuando Bob recibe $M_1 M_2$, corrige: con 00 no hace nada, con 01 aplica X , con 10 aplica Z , y con 11 aplica X y después Z . En todos los casos,

$$|\psi_4\rangle = Z^{M_1} X^{M_2} |\psi_3(M_1 M_2)\rangle = |\psi\rangle.$$

Paso a paso: medir y corregir

Si Alice obtiene $M_1 M_2$, el qubit de Bob queda en $|\psi_3(M_1 M_2)\rangle$, que se lee del término correspondiente:

$$00 \mapsto |\psi_3(00)\rangle = \alpha |0\rangle + \beta |1\rangle$$

$$01 \mapsto |\psi_3(01)\rangle = \alpha |1\rangle + \beta |0\rangle$$

$$10 \mapsto |\psi_3(10)\rangle = \alpha |0\rangle - \beta |1\rangle$$

$$11 \mapsto |\psi_3(11)\rangle = \alpha |1\rangle - \beta |0\rangle$$

Cuando Bob recibe $M_1 M_2$, corrige: con 00 no hace nada, con 01 aplica X , con 10 aplica Z , y con 11 aplica X y después Z . En todos los casos,

$$|\psi_4\rangle = Z^{M_1} X^{M_2} |\psi_3(M_1 M_2)\rangle = |\psi\rangle.$$

¡Ojo! en $Z^{M_1} X^{M_2}$ primero se aplica X^{M_2} y después Z^{M_1} : en el circuito, X aparece antes que Z .

Observaciones

- ▶ **No contradice el no clonado**: después de medir, los qubits de Alice quedan en $|M_1 M_2\rangle$, así que $|\psi\rangle$ ya no está de su lado. El estado se *mueve*, no se copia.

Observaciones

- ▶ **No contradice el no clonado:** después de medir, los qubits de Alice quedan en $|M_1 M_2\rangle$, así que $|\psi\rangle$ ya no está de su lado. El estado se *mueve*, no se copia.
- ▶ **No es más rápido que la luz:** sin los dos bits de Alice, Bob no sabe qué corrección aplicar. Cada uno de los cuatro estados posibles sale con probabilidad $1/4$.

Observaciones

- ▶ **No contradice el no clonado:** después de medir, los qubits de Alice quedan en $|M_1 M_2\rangle$, así que $|\psi\rangle$ ya no está de su lado. El estado se *mueve*, no se copia.
- ▶ **No es más rápido que la luz:** sin los dos bits de Alice, Bob no sabe qué corrección aplicar. Cada uno de los cuatro estados posibles sale con probabilidad $1/4$.
- ▶ Alice nunca conoce α ni β : el protocolo funciona para cualquier $|\psi\rangle$.

Observaciones

- ▶ **No contradice el no clonado:** después de medir, los qubits de Alice quedan en $|M_1 M_2\rangle$, así que $|\psi\rangle$ ya no está de su lado. El estado se *mueve*, no se copia.
- ▶ **No es más rápido que la luz:** sin los dos bits de Alice, Bob no sabe qué corrección aplicar. Cada uno de los cuatro estados posibles sale con probabilidad $1/4$.
- ▶ Alice nunca conoce α ni β : el protocolo funciona para cualquier $|\psi\rangle$.
- ▶ **Intercambio de recursos:** un par entrelazado más 2 bits clásicos valen, al menos, lo mismo que enviar 1 qubit.

Ejercicio

- a) Para $|\psi\rangle = |+\rangle$, escriba $|\psi_0\rangle$, $|\psi_1\rangle$, $|\psi_2\rangle$ y el estado de Bob para cada resultado $M_1 M_2$.
- b) Use el protocolo dos veces para teleportar el estado de dos qubits $|\beta_{00}\rangle$: primero el primer qubit y después el segundo.
- c) A partir del inciso anterior, describa cómo teleportar un estado de n qubits.