

Introducción a la computación cuántica

Nicolás Alberto Monzón

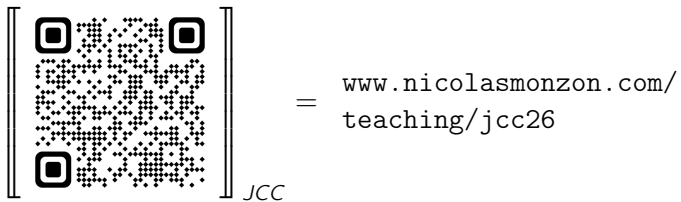
Universidad de la República, Uruguay

XXIV Jornadas de Ciencias de la Computación (JCC)

FCEIA, Universidad Nacional de Rosario

(Versión del 23 de octubre de 2026)

Diapositivas de la clase



Clase $|1\rangle$

Contenido

Sistemas multi-qubit y entrelazamiento

Operador densidad

Traza parcial y operador densidad reducido

Algoritmo de Deutsch

Algoritmo de Deutsch–Jozsa

Sistemas de n qubits

Por el postulado 4, n qubits viven en

$$\mathcal{H}_n = \underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_n = \mathbb{C}^{2^n}$$

con base computacional $\{|x\rangle : x \in \{0, 1\}^n\}$, donde $|x_1 \dots x_n\rangle = |x_1\rangle \otimes \cdots \otimes |x_n\rangle$.

Sistemas de n qubits

Por el postulado 4, n qubits viven en

$$\mathcal{H}_n = \underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_n = \mathbb{C}^{2^n}$$

con base computacional $\{|x\rangle : x \in \{0, 1\}^n\}$, donde $|x_1 \dots x_n\rangle = |x_1\rangle \otimes \cdots \otimes |x_n\rangle$.

Un estado general es

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle, \quad \sum_x |\alpha_x|^2 = 1 :$$

hacen falta 2^n amplitudes.

Sistemas de n qubits

Por el postulado 4, n qubits viven en

$$\mathcal{H}_n = \underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_n = \mathbb{C}^{2^n}$$

con base computacional $\{|x\rangle : x \in \{0, 1\}^n\}$, donde $|x_1 \dots x_n\rangle = |x_1\rangle \otimes \cdots \otimes |x_n\rangle$.

Un estado general es

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle, \quad \sum_x |\alpha_x|^2 = 1 :$$

hacen falta 2^n amplitudes.

Ejemplo: con 50 qubits hay $2^{50} \approx 10^{15}$ amplitudes complejas: describir el estado ya es un problema para una computadora clásica.

Operadores sobre varios qubits

Si A actúa sobre un qubit y B sobre otro, $A \otimes B$ actúa sobre los dos:

$$(A \otimes B) |a\rangle |b\rangle = A|a\rangle \otimes B|b\rangle$$

Para actuar sólo sobre una parte, se completa con la identidad: $A \otimes I$.

Operadores sobre varios qubits

Si A actúa sobre un qubit y B sobre otro, $A \otimes B$ actúa sobre los dos:

$$(A \otimes B) |a\rangle |b\rangle = A|a\rangle \otimes B|b\rangle$$

Para actuar sólo sobre una parte, se completa con la identidad: $A \otimes I$.

Ejemplo: H en cada uno de n qubits en $|0\rangle$ da la superposición uniforme:

$$H^{\otimes n} |0\rangle^{\otimes n} = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right)^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

Operadores sobre varios qubits

Si A actúa sobre un qubit y B sobre otro, $A \otimes B$ actúa sobre los dos:

$$(A \otimes B) |a\rangle |b\rangle = A|a\rangle \otimes B|b\rangle$$

Para actuar sólo sobre una parte, se completa con la identidad: $A \otimes I$.

Ejemplo: H en cada uno de n qubits en $|0\rangle$ da la superposición uniforme:

$$H^{\otimes n} |0\rangle^{\otimes n} = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right)^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

Nota: hay operadores sobre varios qubits que no son de la forma $A \otimes B$, como CNOT.

Medir una parte del sistema

Para medir sólo el primer qubit en la base computacional se usan los operadores $M_0 \otimes I$ y $M_1 \otimes I$, con $M_0 = |0\rangle\langle 0|$ y $M_1 = |1\rangle\langle 1|$.

Medir una parte del sistema

Para medir sólo el primer qubit en la base computacional se usan los operadores $M_0 \otimes I$ y $M_1 \otimes I$, con $M_0 = |0\rangle\langle 0|$ y $M_1 = |1\rangle\langle 1|$.

Ejemplo: midiendo el primer qubit de $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$:

- ▶ sale 0 con probabilidad $\frac{1}{2}$, y el estado pasa a ser $|00\rangle$;
- ▶ sale 1 con probabilidad $\frac{1}{2}$, y el estado pasa a ser $|11\rangle$.

Medir una parte del sistema

Para medir sólo el primer qubit en la base computacional se usan los operadores $M_0 \otimes I$ y $M_1 \otimes I$, con $M_0 = |0\rangle\langle 0|$ y $M_1 = |1\rangle\langle 1|$.

Ejemplo: midiendo el primer qubit de $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$:

- ▶ sale 0 con probabilidad $\frac{1}{2}$, y el estado pasa a ser $|00\rangle$;
- ▶ sale 1 con probabilidad $\frac{1}{2}$, y el estado pasa a ser $|11\rangle$.

Medir el primer qubit determina también el segundo: los resultados están **correlacionados**. Esto pasa aunque los qubits estén lejos, pero no transmite información: el resultado es aleatorio.

Entrelazamiento

Recordemos: $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H}'$ es **producto** si $|\psi\rangle = |a\rangle |b\rangle$, y **entrelazado** si no.

Entrelazamiento

Recordemos: $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H}'$ es **producto** si $|\psi\rangle = |a\rangle |b\rangle$, y **entrelazado** si no.

Para dos qubits, $|\psi\rangle = c_{00} |00\rangle + c_{01} |01\rangle + c_{10} |10\rangle + c_{11} |11\rangle$ es producto si y sólo si

$$c_{00} c_{11} = c_{01} c_{10}.$$

Entrelazamiento

Recordemos: $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H}'$ es **producto** si $|\psi\rangle = |a\rangle |b\rangle$, y **entrelazado** si no.

Para dos qubits, $|\psi\rangle = c_{00} |00\rangle + c_{01} |01\rangle + c_{10} |10\rangle + c_{11} |11\rangle$ es producto si y sólo si

$$c_{00} c_{11} = c_{01} c_{10}.$$

Ejemplo:

- ▶ $\frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle) = |+\rangle |+\rangle$: $\frac{1}{4} = \frac{1}{4}$, producto.
- ▶ $|\beta_{00}\rangle$: $c_{00}c_{11} = \frac{1}{2} \neq 0 = c_{01}c_{10}$, entrelazado.

Entrelazamiento

Recordemos: $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H}'$ es **producto** si $|\psi\rangle = |a\rangle |b\rangle$, y **entrelazado** si no.

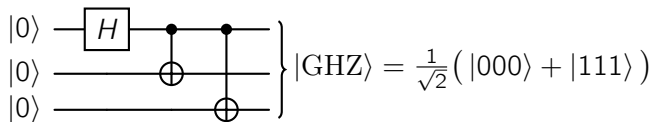
Para dos qubits, $|\psi\rangle = c_{00} |00\rangle + c_{01} |01\rangle + c_{10} |10\rangle + c_{11} |11\rangle$ es producto si y sólo si

$$c_{00} c_{11} = c_{01} c_{10}.$$

Ejemplo:

- ▶ $\frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle) = |+\rangle |+\rangle$: $\frac{1}{4} = \frac{1}{4}$, producto.
- ▶ $|\beta_{00}\rangle$: $c_{00}c_{11} = \frac{1}{2} \neq 0 = c_{01}c_{10}$, entrelazado.

Un ejemplo con tres qubits es el estado **GHZ**, que se genera con H y dos CNOT:


$$\left. \begin{array}{l} |0\rangle \text{---} [H] \text{---} \bullet \text{---} \bullet \\ |0\rangle \text{---} \oplus \\ |0\rangle \text{---} \oplus \end{array} \right\} |\text{GHZ}\rangle = \frac{1}{\sqrt{2}} (|000\rangle + |111\rangle)$$

Ejercicio

a) Indique si cada estado es producto o entrelazado:

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

$$\frac{1}{\sqrt{3}}(|00\rangle + |01\rangle + |11\rangle)$$

b) Escriba $|\beta_{00}\rangle$ en la base $\{|++\rangle, |+-\rangle, |-+\rangle, |--\rangle\}$. ¿Con qué probabilidad se obtiene cada resultado al medir en esa base?

c) Calcule $H^{\otimes 2}|11\rangle$.

Contenido

Sistemas multi-qubit y entrelazamiento

Operador densidad

Traza parcial y operador densidad reducido

Algoritmo de Deutsch

Algoritmo de Deutsch–Jozsa

Cuando no conocemos el estado

Se tira una moneda: si sale cara se prepara $|0\rangle$, y si sale ceca, $|1\rangle$. Para quien no vio la moneda, ¿en qué estado está el qubit?

Cuando no conocemos el estado

Se tira una moneda: si sale cara se prepara $|0\rangle$, y si sale ceca, $|1\rangle$. Para quien no vio la moneda, ¿en qué estado está el qubit?

No es un vector de estado, sino un **conjunto de estados**:

$$\{(p_i, |\psi_i\rangle)\} = \{(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)\}$$

Cuando no conocemos el estado

Se tira una moneda: si sale cara se prepara $|0\rangle$, y si sale ceca, $|1\rangle$. Para quien no vio la moneda, ¿en qué estado está el qubit?

No es un vector de estado, sino un **conjunto de estados**:

$$\{(p_i, |\psi_i\rangle)\} = \{(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)\}$$

Esto no es lo mismo que $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$: los dos dan 0 o 1 con probabilidad $\frac{1}{2}$ en la base computacional, pero

- ▶ $|+\rangle$ medido en la base $\pm$ da $+$ con probabilidad 1;
- ▶ la moneda medida en la base $\pm$ da $+$ con probabilidad $\frac{1}{2}$.

Repaso: traza

La **traza** de una matriz es la suma de los elementos de su diagonal: $\text{tr}(A) = \sum_i a_{ii}$.

Repaso: traza

La **traza** de una matriz es la suma de los elementos de su diagonal: $\text{tr}(A) = \sum_i a_{ii}$.

Propiedades:

- ▶ $\text{tr}(A + B) = \text{tr}(A) + \text{tr}(B)$ y $\text{tr}(\lambda A) = \lambda \text{tr}(A)$;
- ▶ $\text{tr}(AB) = \text{tr}(BA)$, y por eso $\text{tr}(UAU^\dagger) = \text{tr}(A)$ si U es unitario;
- ▶ $\text{tr}(|\psi\rangle\langle\varphi|) = \langle\varphi|\psi\rangle$;
- ▶ si $|\psi\rangle$ es unitario, $\text{tr}(A|\psi\rangle\langle\psi|) = \langle\psi|A|\psi\rangle$.

Repaso: traza

La **traza** de una matriz es la suma de los elementos de su diagonal: $\text{tr}(A) = \sum_i a_{ii}$.

Propiedades:

- ▶ $\text{tr}(A + B) = \text{tr}(A) + \text{tr}(B)$ y $\text{tr}(\lambda A) = \lambda \text{tr}(A)$;
- ▶ $\text{tr}(AB) = \text{tr}(BA)$, y por eso $\text{tr}(UAU^\dagger) = \text{tr}(A)$ si U es unitario;
- ▶ $\text{tr}(|\psi\rangle\langle\varphi|) = \langle\varphi|\psi\rangle$;
- ▶ si $|\psi\rangle$ es unitario, $\text{tr}(A|\psi\rangle\langle\psi|) = \langle\psi|A|\psi\rangle$.

Ejemplo: $\text{tr}(|+\rangle\langle-|) = \langle-|+\rangle = 0$.

El operador densidad

Definición

El operador densidad del conjunto de estados $\{(p_i, |\psi_i\rangle)\}$ es

$$\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|.$$

El operador densidad

Definición

El operador densidad del conjunto de estados $\{(p_i, |\psi_i\rangle)\}$ es

$$\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|.$$

Ejemplo: para $\{(\frac{1}{4}, |+\rangle), (\frac{3}{4}, |1\rangle)\}$:

$$\rho = \frac{1}{4} |+\rangle \langle +| + \frac{3}{4} |1\rangle \langle 1| = \begin{pmatrix} 1/8 & 1/8 \\ 1/8 & 7/8 \end{pmatrix}$$

El operador densidad

Definición

El operador densidad del conjunto de estados $\{(p_i, |\psi_i\rangle)\}$ es

$$\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|.$$

Ejemplo: para $\{(\frac{1}{4}, |+\rangle), (\frac{3}{4}, |1\rangle)\}$:

$$\rho = \frac{1}{4} |+\rangle \langle +| + \frac{3}{4} |1\rangle \langle 1| = \begin{pmatrix} 1/8 & 1/8 \\ 1/8 & 7/8 \end{pmatrix}$$

- ▶ Si el estado se conoce exactamente, es **puro**: $\rho = |\psi\rangle \langle \psi|$.
- ▶ Si no, es **mixto**. Por ejemplo, la moneda: $\rho = \frac{1}{2} |0\rangle \langle 0| + \frac{1}{2} |1\rangle \langle 1| = \frac{I}{2}$.

Caracterización

Teorema

ρ es el operador densidad de algún conjunto de estados si y sólo si

1. $\text{tr}(\rho) = 1$, y
2. ρ es positivo: $\langle \varphi | \rho | \varphi \rangle \geq 0$ para todo $|\varphi\rangle$.

Caracterización

Teorema

ρ es el operador densidad de algún conjunto de estados si y sólo si

1. $\text{tr}(\rho) = 1$, y
2. ρ es positivo: $\langle \varphi | \rho | \varphi \rangle \geq 0$ para todo $|\varphi\rangle$.

Teorema

Para todo operador densidad, $\text{tr}(\rho^2) \leq 1$, con igualdad si y sólo si ρ es puro.

Caracterización

Teorema

ρ es el operador densidad de algún conjunto de estados si y sólo si

1. $\text{tr}(\rho) = 1$, y
2. ρ es positivo: $\langle \varphi | \rho | \varphi \rangle \geq 0$ para todo $|\varphi\rangle$.

Teorema

Para todo operador densidad, $\text{tr}(\rho^2) \leq 1$, con igualdad si y sólo si ρ es puro.

Ejemplo: $\text{tr}(|+\rangle\langle+|^2) = \text{tr}(|+\rangle\langle+|) = 1$, pero $\text{tr}((I/2)^2) = \frac{1}{2} < 1$.

Los postulados con operadores densidad

- **Estado:** un operador ρ positivo con $\text{tr}(\rho) = 1$.

Los postulados con operadores densidad

- ▶ **Estado:** un operador ρ positivo con $\text{tr}(\rho) = 1$.
- ▶ **Evolución:** con un operador unitario U ,

$$\rho \longmapsto U\rho U^\dagger.$$

Los postulados con operadores densidad

- ▶ **Estado:** un operador ρ positivo con $\text{tr}(\rho) = 1$.
- ▶ **Evolución:** con un operador unitario U ,

$$\rho \longmapsto U\rho U^\dagger.$$

- ▶ **Medición:** con $\{M_m\}$, el resultado m sale con probabilidad

$$p(m) = \text{tr} (M_m^\dagger M_m \rho) \quad \text{y el estado pasa a ser} \quad \frac{M_m \rho M_m^\dagger}{p(m)}.$$

Los postulados con operadores densidad

- **Estado:** un operador ρ positivo con $\text{tr}(\rho) = 1$.
- **Evolución:** con un operador unitario U ,

$$\rho \longmapsto U\rho U^\dagger.$$

- **Medición:** con $\{M_m\}$, el resultado m sale con probabilidad

$$p(m) = \text{tr} (M_m^\dagger M_m \rho) \quad \text{y el estado pasa a ser} \quad \frac{M_m \rho M_m^\dagger}{p(m)}.$$

- **Sistemas compuestos:** si las partes están en $\rho_1, \dots, \rho_n$, el sistema está en $\rho_1 \otimes \dots \otimes \rho_n$.

Ejemplo: medir un estado mixto

Sea $\rho = \frac{1}{4} |+\rangle \langle +| + \frac{3}{4} |1\rangle \langle 1| = \frac{1}{8} |0\rangle \langle 0| + \frac{1}{8} |0\rangle \langle 1| + \frac{1}{8} |1\rangle \langle 0| + \frac{7}{8} |1\rangle \langle 1|$.

Ejemplo: medir un estado mixto

Sea $\rho = \frac{1}{4} |+\rangle \langle +| + \frac{3}{4} |1\rangle \langle 1| = \frac{1}{8} |0\rangle \langle 0| + \frac{1}{8} |0\rangle \langle 1| + \frac{1}{8} |1\rangle \langle 0| + \frac{7}{8} |1\rangle \langle 1|$.

Medimos en la base computacional, con $P_0 = |0\rangle \langle 0|$ y $P_1 = |1\rangle \langle 1|$:

$$p(1) = \text{tr}(P_1 \rho) = \frac{1}{8} \text{tr}(|1\rangle \langle 0|) + \frac{7}{8} \text{tr}(|1\rangle \langle 1|) = \frac{7}{8}$$

Ejemplo: medir un estado mixto

Sea $\rho = \frac{1}{4} |+\rangle \langle +| + \frac{3}{4} |1\rangle \langle 1| = \frac{1}{8} |0\rangle \langle 0| + \frac{1}{8} |0\rangle \langle 1| + \frac{1}{8} |1\rangle \langle 0| + \frac{7}{8} |1\rangle \langle 1|$.

Medimos en la base computacional, con $P_0 = |0\rangle \langle 0|$ y $P_1 = |1\rangle \langle 1|$:

$$p(1) = \text{tr}(P_1 \rho) = \frac{1}{8} \text{tr}(|1\rangle \langle 0|) + \frac{7}{8} \text{tr}(|1\rangle \langle 1|) = \frac{7}{8}$$

Coincide con razonar por casos: con probabilidad $\frac{3}{4}$ el estado es $|1\rangle$ (sale 1 seguro), y con probabilidad $\frac{1}{4}$ es $|+\rangle$ (sale 1 con probabilidad $\frac{1}{2}$):

$$\frac{3}{4} \cdot 1 + \frac{1}{4} \cdot \frac{1}{2} = \frac{7}{8}$$

Ejemplo: medir un estado mixto

Sea $\rho = \frac{1}{4} |+\rangle \langle +| + \frac{3}{4} |1\rangle \langle 1| = \frac{1}{8} |0\rangle \langle 0| + \frac{1}{8} |0\rangle \langle 1| + \frac{1}{8} |1\rangle \langle 0| + \frac{7}{8} |1\rangle \langle 1|$.

Medimos en la base computacional, con $P_0 = |0\rangle \langle 0|$ y $P_1 = |1\rangle \langle 1|$:

$$p(1) = \text{tr}(P_1 \rho) = \frac{1}{8} \text{tr}(|1\rangle \langle 0|) + \frac{7}{8} \text{tr}(|1\rangle \langle 1|) = \frac{7}{8}$$

Coincide con razonar por casos: con probabilidad $\frac{3}{4}$ el estado es $|1\rangle$ (sale 1 seguro), y con probabilidad $\frac{1}{4}$ es $|+\rangle$ (sale 1 con probabilidad $\frac{1}{2}$):

$$\frac{3}{4} \cdot 1 + \frac{1}{4} \cdot \frac{1}{2} = \frac{7}{8}$$

Si sale 1, el estado pasa a ser $\frac{P_1 \rho P_1}{7/8} = |1\rangle \langle 1|$.

Ejercicio

Sea el conjunto de estados $\{(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |+\rangle)\}$.

- a) Calcule su operador densidad ρ , en notación de Dirac y como matriz.
- b) Verifique que $\text{tr}(\rho) = 1$. ¿Es puro o mixto? Calcule $\text{tr}(\rho^2)$.
- c) Calcule las probabilidades de cada resultado al medir en la base computacional y en la base $\pm$.
- d) Calcule $H\rho H^\dagger$. ¿A qué conjunto de estados corresponde?

Contenido

Sistemas multi-qubit y entrelazamiento

Operador densidad

Traza parcial y operador densidad reducido

Algoritmo de Deutsch

Algoritmo de Deutsch–Jozsa

Traza parcial

Definición

La traza parcial sobre B es el operador lineal que cumple

$$\text{tr}_B \left(|a_1\rangle \langle a_2| \otimes |b_1\rangle \langle b_2| \right) = \langle b_2 | b_1 \rangle |a_1\rangle \langle a_2|.$$

Es decir: se calcula la traza sólo de la parte B , y queda un operador sobre A .

Traza parcial

Definición

La traza parcial sobre B es el operador lineal que cumple

$$\mathrm{tr}_B \left(|a_1\rangle \langle a_2| \otimes |b_1\rangle \langle b_2| \right) = \langle b_2|b_1\rangle |a_1\rangle \langle a_2|.$$

Es decir: se calcula la traza sólo de la parte B , y queda un operador sobre A .

Ejemplo: si $\rho_{AB} = \rho \otimes \sigma$ (un estado producto), entonces

$$\mathrm{tr}_B(\rho \otimes \sigma) = \rho \, \mathrm{tr}(\sigma) = \rho.$$

Operador densidad reducido

Definición

Si el sistema AB está en ρ_{AB} , el operador densidad reducido de A es

$$\rho_A = \text{tr}_B(\rho_{AB}).$$

Operador densidad reducido

Definición

Si el sistema AB está en ρ_{AB} , el operador densidad reducido de A es

$$\rho_A = \text{tr}_B(\rho_{AB}).$$

ρ_A describe todo lo que se puede observar midiendo sólo A . Para una medición $\{M_m\}$ sobre A :

$$p(m) \stackrel{(1)}{=} \text{tr} \left((M_m^\dagger M_m \otimes I) \rho_{AB} \right) \stackrel{(2)}{=} \text{tr} (M_m^\dagger M_m \rho_A).$$

Operador densidad reducido

Definición

Si el sistema AB está en ρ_{AB} , el operador densidad reducido de A es

$$\rho_A = \text{tr}_B(\rho_{AB}).$$

ρ_A describe todo lo que se puede observar midiendo sólo A . Para una medición $\{M_m\}$ sobre A :

$$p(m) \stackrel{(1)}{=} \text{tr} \left((M_m^\dagger M_m \otimes I) \rho_{AB} \right) \stackrel{(2)}{=} \text{tr} (M_m^\dagger M_m \rho_A).$$

- (1) Medir sólo A es medir todo el sistema con $\{M_m \otimes I\}$: la identidad no toca a B . Por el postulado 3 con operadores densidad, y como $(M_m \otimes I)^\dagger (M_m \otimes I) = M_m^\dagger M_m \otimes I$, sale la primera igualdad.

Operador densidad reducido

Definición

Si el sistema AB está en ρ_{AB} , el operador densidad reducido de A es

$$\rho_A = \text{tr}_B(\rho_{AB}).$$

ρ_A describe todo lo que se puede observar midiendo sólo A . Para una medición $\{M_m\}$ sobre A :

$$p(m) \stackrel{(1)}{=} \text{tr} \left((M_m^\dagger M_m \otimes I) \rho_{AB} \right) \stackrel{(2)}{=} \text{tr} (M_m^\dagger M_m \rho_A).$$

- (1) Medir sólo A es medir todo el sistema con $\{M_m \otimes I\}$: la identidad no toca a B . Por el postulado 3 con operadores densidad, y como $(M_m \otimes I)^\dagger (M_m \otimes I) = M_m^\dagger M_m \otimes I$, sale la primera igualdad.
- (2) Es la propiedad que caracteriza a la traza parcial (próxima diapositiva).

Por qué vale la igualdad (2)

Queremos ver que $\text{tr}((X \otimes I) \rho_{AB}) = \text{tr}(X \text{tr}_B(\rho_{AB}))$ para cualquier X sobre A .

Por qué vale la igualdad (2)

Queremos ver que $\text{tr}((X \otimes I) \rho_{AB}) = \text{tr}(X \text{tr}_B(\rho_{AB}))$ para cualquier X sobre A .
Como las dos trazas son lineales, alcanza con verlo para $\rho_{AB} = |a_1\rangle \langle a_2| \otimes |b_1\rangle \langle b_2|$:

$$\begin{aligned} \text{tr}((X \otimes I)(|a_1\rangle \langle a_2| \otimes |b_1\rangle \langle b_2|)) &\stackrel{(a)}{=} \text{tr}(X |a_1\rangle \langle a_2|) \cdot \text{tr}(|b_1\rangle \langle b_2|) \\ &\stackrel{(b)}{=} \text{tr}(X |a_1\rangle \langle a_2|) \langle b_2|b_1\rangle \\ &\stackrel{(c)}{=} \text{tr}(X (\langle b_2|b_1\rangle |a_1\rangle \langle a_2|)) \\ &\stackrel{(d)}{=} \text{tr}(X \text{tr}_B(|a_1\rangle \langle a_2| \otimes |b_1\rangle \langle b_2|)) \end{aligned}$$

(a) $\text{tr}(A \otimes B) = \text{tr}(A) \text{tr}(B)$; (b) $\text{tr}(|\psi\rangle \langle \varphi|) = \langle \varphi|\psi\rangle$; (c) $\langle b_2|b_1\rangle$ es un número, y $\lambda \text{tr}(XA) = \text{tr}(X(\lambda A))$; (d) definición de tr_B .

Por qué vale la igualdad (2)

Queremos ver que $\text{tr}((X \otimes I) \rho_{AB}) = \text{tr}(X \text{tr}_B(\rho_{AB}))$ para cualquier X sobre A .
Como las dos trazas son lineales, alcanza con verlo para $\rho_{AB} = |a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|$:

$$\begin{aligned} \text{tr}\left((X \otimes I)(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|)\right) &\stackrel{(a)}{=} \text{tr}(X |a_1\rangle\langle a_2|) \cdot \text{tr}(|b_1\rangle\langle b_2|) \\ &\stackrel{(b)}{=} \text{tr}(X |a_1\rangle\langle a_2|) \langle b_2|b_1\rangle \\ &\stackrel{(c)}{=} \text{tr}\left(X (\langle b_2|b_1\rangle |a_1\rangle\langle a_2|)\right) \\ &\stackrel{(d)}{=} \text{tr}\left(X \text{tr}_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|)\right) \end{aligned}$$

(a) $\text{tr}(A \otimes B) = \text{tr}(A) \text{tr}(B)$; (b) $\text{tr}(|\psi\rangle\langle\varphi|) = \langle\varphi|\psi\rangle$; (c) $\langle b_2|b_1\rangle$ es un número, y $\lambda \text{tr}(XA) = \text{tr}(X(\lambda A))$; (d) definición de tr_B .

Con $X = M_m^\dagger M_m$ sale la igualdad (2): para calcular probabilidades de medir sólo A , alcanza con ρ_A .

Ejemplo: el estado reducido de $|\beta_{00}\rangle$

$$\rho = |\beta_{00}\rangle \langle \beta_{00}| = \frac{1}{2} \left(|00\rangle \langle 00| + |11\rangle \langle 00| + |00\rangle \langle 11| + |11\rangle \langle 11| \right)$$

Ejemplo: el estado reducido de $|\beta_{00}\rangle$

$$\rho = |\beta_{00}\rangle \langle \beta_{00}| = \frac{1}{2} \left(|00\rangle \langle 00| + |11\rangle \langle 00| + |00\rangle \langle 11| + |11\rangle \langle 11| \right)$$

Trazando el segundo qubit, término por término:

$$\begin{aligned} \rho_1 = \text{tr}_2(\rho) &= \frac{1}{2} \left(\langle 0|0\rangle |0\rangle \langle 0| + \langle 0|1\rangle |1\rangle \langle 0| + \langle 1|0\rangle |0\rangle \langle 1| + \langle 1|1\rangle |1\rangle \langle 1| \right) \\ &= \frac{1}{2} \left(|0\rangle \langle 0| + |1\rangle \langle 1| \right) = \frac{I}{2} \end{aligned}$$

Ejemplo: el estado reducido de $|\beta_{00}\rangle$

$$\rho = |\beta_{00}\rangle \langle \beta_{00}| = \frac{1}{2} \left(|00\rangle \langle 00| + |11\rangle \langle 00| + |00\rangle \langle 11| + |11\rangle \langle 11| \right)$$

Trazando el segundo qubit, término por término:

$$\begin{aligned} \rho_1 = \text{tr}_2(\rho) &= \frac{1}{2} \left(\langle 0|0\rangle |0\rangle \langle 0| + \langle 0|1\rangle |1\rangle \langle 0| + \langle 1|0\rangle |0\rangle \langle 1| + \langle 1|1\rangle |1\rangle \langle 1| \right) \\ &= \frac{1}{2} \left(|0\rangle \langle 0| + |1\rangle \langle 1| \right) = \frac{I}{2} \end{aligned}$$

El estado de los dos qubits es puro, pero cada qubit por separado está en un estado mixto: $\text{tr}((I/2)^2) = \frac{1}{2} < 1$.

De vuelta a la teleportación

Después de que Alice mide, y antes de que Bob reciba los bits, Bob tiene cada uno de los cuatro estados $|\psi_3(M_1 M_2)\rangle$ con probabilidad $\frac{1}{4}$. Su estado reducido es

$$\rho_B = \frac{1}{4} \sum_{M_1 M_2} |\psi_3(M_1 M_2)\rangle \langle \psi_3(M_1 M_2)| = \frac{2(|\alpha|^2 + |\beta|^2)(|0\rangle\langle 0| + |1\rangle\langle 1|)}{4} = \frac{I}{2}.$$

De vuelta a la teleportación

Después de que Alice mide, y antes de que Bob reciba los bits, Bob tiene cada uno de los cuatro estados $|\psi_3(M_1 M_2)\rangle$ con probabilidad $\frac{1}{4}$. Su estado reducido es

$$\rho_B = \frac{1}{4} \sum_{M_1 M_2} |\psi_3(M_1 M_2)\rangle \langle \psi_3(M_1 M_2)| = \frac{2(|\alpha|^2 + |\beta|^2)(|0\rangle\langle 0| + |1\rangle\langle 1|)}{4} = \frac{I}{2}.$$

ρ_B no depende de α ni de β : ninguna medición de Bob da información sobre $|\psi\rangle$ hasta que recibe los bits de Alice. Ésta es la versión precisa de “la teleportación no es más rápida que la luz”.

Ejercicio

- a) Calcule el operador densidad reducido del primer qubit para

$$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) \quad \text{y} \quad \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle).$$

- b) Para cada uno, calcule $\text{tr}(\rho_1^2)$. ¿Qué relación observa con que el estado sea producto o entrelazado?
- c) Calcule el operador densidad reducido de cualquiera de los qubits de $|\text{GHZ}\rangle$.

Contenido

Sistemas multi-qubit y entrelazamiento

Operador densidad

Traza parcial y operador densidad reducido

Algoritmo de Deutsch

Algoritmo de Deutsch–Jozsa

Evaluar una función con un circuito

Dada $f : \{0, 1\} \rightarrow \{0, 1\}$, se define la compuerta

$$U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle .$$

U_f es unitaria para cualquier f (ejercicio).

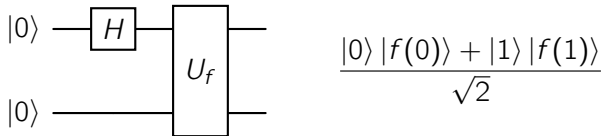
Evaluar una función con un circuito

Dada $f : \{0, 1\} \rightarrow \{0, 1\}$, se define la compuerta

$$U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle .$$

U_f es unitaria para cualquier f (ejercicio).

Paralelismo cuántico: con el primer qubit en superposición, una sola aplicación de U_f evalúa f en 0 y en 1:



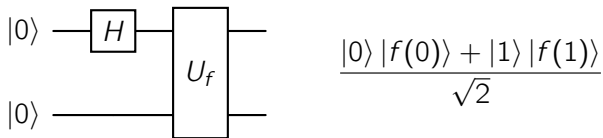
Evaluar una función con un circuito

Dada $f : \{0, 1\} \rightarrow \{0, 1\}$, se define la compuerta

$$U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle .$$

U_f es unitaria para cualquier f (ejercicio).

Paralelismo cuántico: con el primer qubit en superposición, una sola aplicación de U_f evalúa f en 0 y en 1:



Al medir se obtiene *un solo* $f(x)$. El desafío es usar la superposición para obtener algo útil.

El problema de Deutsch

Dada $f : \{0, 1\} \rightarrow \{0, 1\}$, decidir si es **constante** ($f(0) = f(1)$) o no.

El problema de Deutsch

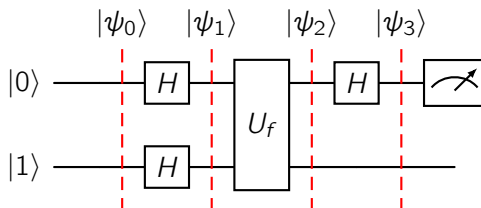
Dada $f : \{0, 1\} \rightarrow \{0, 1\}$, decidir si es **constante** ($f(0) = f(1)$) o no.

- ▶ Clásicamente hace falta evaluar f **dos veces** y comparar.
- ▶ Con el algoritmo de Deutsch alcanza con **una** aplicación de U_f .

El problema de Deutsch

Dada $f : \{0, 1\} \rightarrow \{0, 1\}$, decidir si es **constante** ($f(0) = f(1)$) o no.

- ▶ Clásicamente hace falta evaluar f **dos veces** y comparar.
- ▶ Con el algoritmo de Deutsch alcanza con **una** aplicación de U_f .



Un truco: la fase

Si el segundo qubit está en $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$:

$$U_f |x\rangle |-\rangle = |x\rangle \frac{|f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}} = \begin{cases} |x\rangle |-\rangle & \text{si } f(x) = 0, \\ -|x\rangle |-\rangle & \text{si } f(x) = 1. \end{cases}$$

Un truco: la fase

Si el segundo qubit está en $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$:

$$U_f |x\rangle |-\rangle = |x\rangle \frac{|f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}} = \begin{cases} |x\rangle |-\rangle & \text{si } f(x) = 0, \\ -|x\rangle |-\rangle & \text{si } f(x) = 1. \end{cases}$$

Es decir,

$$U_f |x\rangle |-\rangle = (-1)^{f(x)} |x\rangle |-\rangle.$$

El valor de f no queda escrito en el segundo qubit, sino en una **fase** del primero.

Paso a paso

$$|\psi_0\rangle = |01\rangle \qquad |\psi_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} |-\rangle$$

Paso a paso

$$|\psi_0\rangle = |01\rangle \qquad |\psi_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} |-\rangle$$

Por el truco de la fase,

$$|\psi_2\rangle = \frac{(-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle}{\sqrt{2}} |-\rangle = \begin{cases} \pm |+\rangle |-\rangle & \text{si } f(0) = f(1), \\ \pm |-\rangle |-\rangle & \text{si } f(0) \neq f(1). \end{cases}$$

Paso a paso

$$|\psi_0\rangle = |01\rangle \qquad |\psi_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} |-\rangle$$

Por el truco de la fase,

$$|\psi_2\rangle = \frac{(-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle}{\sqrt{2}} |-\rangle = \begin{cases} \pm |+\rangle |-\rangle & \text{si } f(0) = f(1), \\ \pm |-\rangle |-\rangle & \text{si } f(0) \neq f(1). \end{cases}$$

Como $H|+\rangle = |0\rangle$ y $H|-\rangle = |1\rangle$:

$$|\psi_3\rangle = \pm |f(0) \oplus f(1)\rangle |-\rangle.$$

Paso a paso

$$|\psi_0\rangle = |01\rangle \qquad |\psi_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} |-\rangle$$

Por el truco de la fase,

$$|\psi_2\rangle = \frac{(-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle}{\sqrt{2}} |-\rangle = \begin{cases} \pm |+\rangle |-\rangle & \text{si } f(0) = f(1), \\ \pm |-\rangle |-\rangle & \text{si } f(0) \neq f(1). \end{cases}$$

Como $H|+\rangle = |0\rangle$ y $H|-\rangle = |1\rangle$:

$$|\psi_3\rangle = \pm |f(0) \oplus f(1)\rangle |-\rangle.$$

Al medir el primer qubit se obtiene $f(0) \oplus f(1)$ con probabilidad 1: sale 0 si f es constante y 1 si no.

Qué está pasando

- ▶ $f(0) \oplus f(1)$ es una propiedad **global** de f : depende de los dos valores a la vez.

Qué está pasando

- ▶ $f(0) \oplus f(1)$ es una propiedad **global** de f : depende de los dos valores a la vez.
- ▶ El algoritmo combina dos ideas:
 - **paralelismo**: U_f actúa sobre $|0\rangle$ y $|1\rangle$ a la vez;
 - **interferencia**: la última H combina las dos alternativas, y sus amplitudes se suman o se cancelan según f .

Qué está pasando

- ▶ $f(0) \oplus f(1)$ es una propiedad **global** de f : depende de los dos valores a la vez.
- ▶ El algoritmo combina dos ideas:
 - **paralelismo**: U_f actúa sobre $|0\rangle$ y $|1\rangle$ a la vez;
 - **interferencia**: la última H combina las dos alternativas, y sus amplitudes se suman o se cancelan según f .
- ▶ Una computadora clásica que elige x al azar evalúa $f(0)$ o $f(1)$; las dos alternativas nunca interfieren.

Ejercicio

- a) Muestre que U_f es unitaria para cualquier $f : \{0, 1\} \rightarrow \{0, 1\}$.
- b) Escriba la traza del algoritmo de Deutsch para la función identidad, $f(x) = x$, calculando $|\psi_0\rangle, \dots, |\psi_3\rangle$ sin usar el truco de la fase.
- c) Escriba la matriz de U_f para las cuatro funciones $f : \{0, 1\} \rightarrow \{0, 1\}$. ¿Qué compuerta conocida es U_f cuando $f(x) = x$?

Contenido

Sistemas multi-qubit y entrelazamiento

Operador densidad

Traza parcial y operador densidad reducido

Algoritmo de Deutsch

Algoritmo de Deutsch–Jozsa

El problema de Deutsch–Jozsa

Dada $f : \{0, 1\}^n \rightarrow \{0, 1\}$, con la **promesa** de que es

- ▶ **constante**: el mismo valor para todo x , o
 - ▶ **balanceada**: vale 0 en exactamente la mitad de las entradas y 1 en la otra mitad,
- decidir cuál de las dos es.

El problema de Deutsch–Jozsa

Dada $f : \{0, 1\}^n \rightarrow \{0, 1\}$, con la **promesa** de que es

- ▶ **constante**: el mismo valor para todo x , o
 - ▶ **balanceada**: vale 0 en exactamente la mitad de las entradas y 1 en la otra mitad, decidir cuál de las dos es.
-
- ▶ Un algoritmo clásico determinista necesita, en el peor caso, $\frac{2^n}{2} + 1$ evaluaciones: puede ver 2^{n-1} ceros seguidos antes del primer 1.
 - ▶ El algoritmo de Deutsch–Jozsa usa **una** aplicación de $U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$.

$H^{\otimes n}$ sobre $|0\rangle^{\otimes n}$

Como $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ y $H^{\otimes n}$ actúa sobre cada qubit por separado:

$$H^{\otimes n} |0\rangle^{\otimes n} = H|0\rangle \otimes \cdots \otimes H|0\rangle = \frac{1}{\sqrt{2^n}} (|0\rangle + |1\rangle) \otimes \cdots \otimes (|0\rangle + |1\rangle).$$

$H^{\otimes n}$ sobre $|0\rangle^{\otimes n}$

Como $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ y $H^{\otimes n}$ actúa sobre cada qubit por separado:

$$H^{\otimes n} |0\rangle^{\otimes n} = H|0\rangle \otimes \cdots \otimes H|0\rangle = \frac{1}{\sqrt{2^n}} (|0\rangle + |1\rangle) \otimes \cdots \otimes (|0\rangle + |1\rangle).$$

Ejemplo: con $n = 2$, distribuyendo:

$$(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) = |00\rangle + |01\rangle + |10\rangle + |11\rangle,$$

así que $H^{\otimes 2} |00\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$.

$H^{\otimes n}$ sobre $|0\rangle^{\otimes n}$

Como $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ y $H^{\otimes n}$ actúa sobre cada qubit por separado:

$$H^{\otimes n} |0\rangle^{\otimes n} = H|0\rangle \otimes \cdots \otimes H|0\rangle = \frac{1}{\sqrt{2^n}} (|0\rangle + |1\rangle) \otimes \cdots \otimes (|0\rangle + |1\rangle).$$

Ejemplo: con $n = 2$, distribuyendo:

$$(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) = |00\rangle + |01\rangle + |10\rangle + |11\rangle,$$

así que $H^{\otimes 2} |00\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$.

En general, al distribuir se elige $|0\rangle$ o $|1\rangle$ de cada uno de los n factores: aparecen todas las cadenas $x \in \{0, 1\}^n$, cada una una sola vez:

$$H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle.$$

$H^{\otimes n}$ sobre $|0\rangle^{\otimes n}$

Como $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ y $H^{\otimes n}$ actúa sobre cada qubit por separado:

$$H^{\otimes n} |0\rangle^{\otimes n} = H|0\rangle \otimes \cdots \otimes H|0\rangle = \frac{1}{\sqrt{2^n}} (|0\rangle + |1\rangle) \otimes \cdots \otimes (|0\rangle + |1\rangle).$$

Ejemplo: con $n = 2$, distribuyendo:

$$(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) = |00\rangle + |01\rangle + |10\rangle + |11\rangle,$$

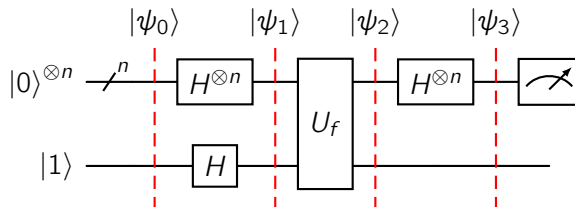
así que $H^{\otimes 2} |00\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$.

En general, al distribuir se elige $|0\rangle$ o $|1\rangle$ de cada uno de los n factores: aparecen todas las cadenas $x \in \{0, 1\}^n$, cada una una sola vez:

$$H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle.$$

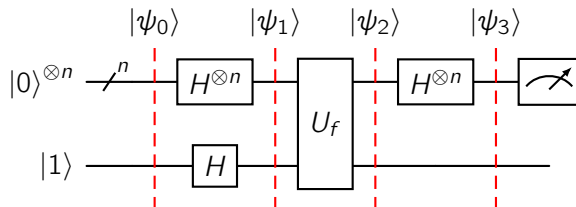
Es la **superposición uniforme**: al medir, cada una de las 2^n entradas sale con probabilidad $\frac{1}{2^n}$.

El circuito



Es el esquema de Deutsch con n qubits arriba; para $n = 1$ es exactamente el algoritmo de Deutsch.

El circuito



Es el esquema de Deutsch con n qubits arriba; para $n = 1$ es exactamente el algoritmo de Deutsch.

Hace falta saber qué hace $H^{\otimes n}$ sobre un $|x\rangle$ cualquiera:

$$H|x\rangle = \frac{1}{\sqrt{2}} \sum_{z \in \{0,1\}} (-1)^{xz} |z\rangle \quad \Rightarrow \quad H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{z \in \{0,1\}^n} (-1)^{x \cdot z} |z\rangle ,$$

donde $x \cdot z = x_1 z_1 + \cdots + x_n z_n$ (módulo 2).

Paso a paso

$$|\psi_0\rangle = |0\rangle^{\otimes n} |1\rangle$$

$$|\psi_1\rangle = \sum_{x \in \{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} |-\rangle$$

Paso a paso

$$|\psi_0\rangle = |0\rangle^{\otimes n} |1\rangle \qquad |\psi_1\rangle = \sum_{x \in \{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} |-\rangle$$

Por el truco de la fase, $U_f |x\rangle |-\rangle = (-1)^{f(x)} |x\rangle |-\rangle$:

$$|\psi_2\rangle = \sum_x \frac{(-1)^{f(x)} |x\rangle}{\sqrt{2^n}} |-\rangle$$

Paso a paso

$$|\psi_0\rangle = |0\rangle^{\otimes n} |1\rangle \qquad |\psi_1\rangle = \sum_{x \in \{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} |-\rangle$$

Por el truco de la fase, $U_f |x\rangle |-\rangle = (-1)^{f(x)} |x\rangle |-\rangle$:

$$|\psi_2\rangle = \sum_x \frac{(-1)^{f(x)} |x\rangle}{\sqrt{2^n}} |-\rangle$$

Aplicando $H^{\otimes n}$ a los primeros n qubits:

$$|\psi_3\rangle = \sum_z \sum_x \frac{(-1)^{x \cdot z + f(x)}}{2^n} |z\rangle |-\rangle$$

La amplitud de $|0\rangle^{\otimes n}$

En $|\psi_3\rangle$, la amplitud de $|z\rangle = |0\rangle^{\otimes n}$ es (como $x \cdot 0 = 0$)

$$\sum_{x \in \{0,1\}^n} \frac{(-1)^{f(x)}}{2^n}.$$

La amplitud de $|0\rangle^{\otimes n}$

En $|\psi_3\rangle$, la amplitud de $|z\rangle = |0\rangle^{\otimes n}$ es (como $x \cdot 0 = 0$)

$$\sum_{x \in \{0,1\}^n} \frac{(-1)^{f(x)}}{2^n}.$$

- Si f es **constante**, todos los términos valen lo mismo y la amplitud es ± 1 . Como el estado tiene norma 1, las demás amplitudes son 0: se mide $0 \dots 0$ con probabilidad 1.

La amplitud de $|0\rangle^{\otimes n}$

En $|\psi_3\rangle$, la amplitud de $|z\rangle = |0\rangle^{\otimes n}$ es (como $x \cdot 0 = 0$)

$$\sum_{x \in \{0,1\}^n} \frac{(-1)^{f(x)}}{2^n}.$$

- ▶ Si f es **constante**, todos los términos valen lo mismo y la amplitud es ± 1 . Como el estado tiene norma 1, las demás amplitudes son 0: se mide $0 \dots 0$ con probabilidad 1.
- ▶ Si f es **balanceada**, la mitad de los términos valen $+\frac{1}{2^n}$ y la otra mitad $-\frac{1}{2^n}$: la amplitud es 0 y *nunca* se mide $0 \dots 0$.

La amplitud de $|0\rangle^{\otimes n}$

En $|\psi_3\rangle$, la amplitud de $|z\rangle = |0\rangle^{\otimes n}$ es (como $x \cdot 0 = 0$)

$$\sum_{x \in \{0,1\}^n} \frac{(-1)^{f(x)}}{2^n}.$$

- ▶ Si f es **constante**, todos los términos valen lo mismo y la amplitud es ± 1 . Como el estado tiene norma 1, las demás amplitudes son 0: se mide $0 \dots 0$ con probabilidad 1.
- ▶ Si f es **balanceada**, la mitad de los términos valen $+\frac{1}{2^n}$ y la otra mitad $-\frac{1}{2^n}$: la amplitud es 0 y *nunca* se mide $0 \dots 0$.

Conclusión

Se miden los primeros n qubits: si sale $0 \dots 0$, f es constante; si no, es balanceada.

Para tener en cuenta

- ▶ La ventaja es frente a algoritmos clásicos **deterministas**. Si se acepta una pequeña probabilidad de error, un algoritmo clásico que evalúa f en unas pocas entradas al azar distingue los dos casos con alta probabilidad.

Para tener en cuenta

- ▶ La ventaja es frente a algoritmos clásicos **deterministas**. Si se acepta una pequeña probabilidad de error, un algoritmo clásico que evalúa f en unas pocas entradas al azar distingue los dos casos con alta probabilidad.
- ▶ El problema no tiene aplicaciones prácticas conocidas.

Para tener en cuenta

- ▶ La ventaja es frente a algoritmos clásicos **deterministas**. Si se acepta una pequeña probabilidad de error, un algoritmo clásico que evalúa f en unas pocas entradas al azar distingue los dos casos con alta probabilidad.
- ▶ El problema no tiene aplicaciones prácticas conocidas.
- ▶ Aun así, contiene ideas centrales de algoritmos más importantes: superposición, evaluación en paralelo con U_f e interferencia con $H^{\otimes n}$.

Examen

$$\left[\begin{array}{c} \text{QR Code} \end{array} \right]_{JCC} = \text{forms.gle/u1k4FRsuDzTJEu7L6}$$