

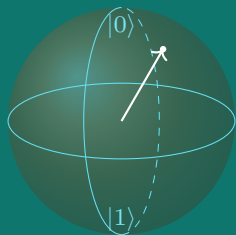
COMPUTACIÓN CUÁNTICA • UNA INTRODUCCIÓN

Capítulo 4

Información en la mecánica cuántica

Alcides Montoya Cañola

Universidad Nacional de Colombia • Sede Medellín | 2026-II



Del qubit a la información

▶ El qubit

superposición, esfera de Bloch, realizaciones físicas

▶ Varios qubits

producto tensorial, explosión 2^n , entrelazamiento

▶ No-localidad

EPR, Bell y sus experimentos

▶ Medidas de información

valor esperado, fidelidad

▶ Teoremas de no-clonación

la información cuántica se conserva

La pregunta del capítulo

Ya tenemos la física. ¿Cómo se *codifica, mide y protege* la información en un mundo cuántico?

Información clásica: bits y estados

Seis monedas “cara/sello” $\rightarrow$ 001011, o en Dirac $|001011\rangle$.

Número de estados posibles

$$N_s = 2^n \quad \Leftrightarrow \quad \log_2 N_s = n$$

Con n bits se representa cualquier magnitud física:
temperatura, campo, brillo...

Reversible vs. singular

Un interruptor *vuelve* a su estado inicial (reversible). La información no se pierde — solo se limita nuestra capacidad de *distinguir* estados.

Estado clásico vs. estado cuántico

Estado clásico

Descripción completa: posición, velocidad...

Determinista: conocido el presente, el futuro es predecible.

Estado cuántico

Superposición y entrelazamiento; nuevas magnitudes (espín, polarización). *Probabilístico*: solo predecimos probabilidades.

La diferencia esencial: es *imposible* predecir con certeza el futuro de un sistema cuántico.

Decoherencia: el nexa con el mundo clásico

Al interactuar con el entorno, la superposición se *desfasa*. Por eso no vemos el “gato de Schrödinger”.

Escalas en un qubit superconductor

$$T_1 \sim 50\text{--}100 \mu s, \quad T_2 \sim 50\text{--}200 \mu s$$

$$\text{compuerta} \sim 20\text{--}100 \text{ ns}$$

El límite práctico

$\sim 10^3\text{--}10^4$ operaciones antes de perder la coherencia. *Por eso* la corrección de errores es indispensable.

? Pausa socrática #1 — ¿dónde termina lo cuántico?

La decoherencia hace “clásico” lo cuántico al crecer el sistema.



- ▶ ¿Hay un tamaño exacto donde “lo cuántico” se vuelve “lo clásico”, o es gradual?
- ▶ Si la información no se destruye, ¿a dónde “se va” la superposición del gato?
- ▶ ¿Es la medición un tipo de decoherencia, o algo distinto?

Sección 4.1

Elementos para representar la información

Matrices como operadores

Una matriz *actúa* sobre un vector y lo transforma:

Escalar la componente y

$$\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} V_x \\ V_y \end{bmatrix} = \begin{bmatrix} V_x \\ 2V_y \end{bmatrix}$$

Rotar 90°

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} V_x \\ V_y \end{bmatrix} = \begin{bmatrix} V_y \\ -V_x \end{bmatrix}$$

Dos familias (Cap. 2)

Hermíticas $M = M^\dagger$: observables (autovalores reales).

Unitarias $UU^\dagger = I$: operaciones reversibles (compuertas).

La Hadamard $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ es hermítica y unitaria.

Valor esperado: la media estadística

Promedio pesado por probabilidades

$$\langle M \rangle_\psi = \langle \psi | M | \psi \rangle = \sum_i \lambda_i |\langle \lambda_i | \psi \rangle|^2$$

Ejemplo: $|\psi\rangle = \frac{1}{\sqrt{2}} |E_1\rangle + \frac{1}{\sqrt{2}} |E_2\rangle$ con $E_1 = 1 \text{ eV}$,
 $E_2 = 3 \text{ eV}$.

$$\langle E \rangle = \frac{1}{2}(1) + \frac{1}{2}(3) = 2 \text{ eV}$$

Cuidado conceptual

2 eV *no* es un autovalor: ninguna medición individual lo da. Es la media sobre un *ensamble*.

$\langle M \rangle$ es real porque M es hermítico — la razón profunda de que los observables sean hermíticos.

El espín como unidad básica de información

- ▶ Momento angular *intrínseco*, sin análogo clásico (no es algo que “gira”).
- ▶ Cuantizado: al medir en una dirección solo da $+\frac{\hbar}{2}$ o $-\frac{\hbar}{2}$.
- ▶ Base de S_z para $s = \frac{1}{2}$:

$$|\uparrow\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |\downarrow\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

El doble papel de Pauli

$\sigma_x, \sigma_y, \sigma_z$ son a la vez *observables* (componentes del espín) y *compuertas* X, Y, Z .

Fermiones: espín semientero; bosones: entero.

? Pausa socrática #2 — un promedio imposible



El valor esperado puede ser un número que *nunca* se mide.

- ▶ ¿Qué información nos da $\langle M \rangle$ que una sola medición no da?
- ▶ Si el espín “no gira”, ¿por qué se comporta como un momento angular?
- ▶ ¿Cuántas repeticiones necesito para estimar $\langle M \rangle$ con precisión ϵ ?

Sección 4.2

Qubits

¿Qué es un qubit?

Un sistema cuántico coherente de *dos niveles*:

Estado general

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

$\alpha, \beta \in \mathbb{C}$: infinitos estados, no solo $\{0, 1\}$. El bit clásico es un caso particular.

Realizaciones físicas

Polarización de fotones · niveles de energía de un átomo · espín de un electrón · corriente en un circuito superconductor.

Paralelismo cuántico — y una advertencia

Un qubit en superposición “representa” 0 y 1 a la vez. Con 3 qubits:

$$|\psi\rangle = \frac{1}{\sqrt{8}} \sum_{k=0}^7 |k\rangle$$

“explora” las 8 entradas de f simultáneamente.

Malentendido común. Al medir se obtiene **un solo** resultado clásico. El poder *no* viene de “calcular todo a la vez”, sino de manipular *amplitudes* con *interferencia* para amplificar lo correcto y cancelar lo incorrecto.

? Pausa socrática #3 — el mito del “todo a la vez”

Con n qubits hay 2^n amplitudes, pero medir da n bits.



- ▶ Si no podemos leer las 2^n amplitudes, ¿en qué sentido “existen”?
- ▶ ¿Por qué un algoritmo cuántico necesita *interferencia* y no solo superposición?
- ▶ ¿Qué tienen en común Grover y Shor en su forma de usar la interferencia?

Varios qubits: la explosión exponencial

El estado conjunto es un *producto tensorial*:

$$|\Psi\rangle = |\gamma_1\rangle \otimes |\gamma_2\rangle \otimes |\gamma_3\rangle = \sum_{k=0}^7 c_k |k\rangle$$

Qubits	Estados / memoria
10	1,024 (~16 KB)
50	$\sim 10^{15}$ (~16 PB)
300	$\sim 10^{90}$ (> átomos del universo)

Espacio de Hilbert de dimensión 2^n .

Esta explosión es a la vez la *fuerza* del poder cuántico y la *barrera* para simularlo clásicamente.

Separable vs. entrelazado

Estado separable (producto)

$$|\psi\rangle_{\text{sep}} = |\phi_1\rangle \otimes \cdots \otimes |\phi_n\rangle$$

Estados de Bell (máx. entrelazados)

$$\Phi^{\pm} = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$$

$$\Psi^{\pm} = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$$

No factoriza

$\Phi^+ = (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle)$
exigiría $\alpha\delta = \beta\gamma = 0$ y $\alpha\gamma = \beta\delta = \frac{1}{\sqrt{2}}$
— imposible.

Separable: solo correlaciones clásicas (LOCC).

Entrelazado: interacción genuinamente cuántica.

Ejercicio ilustrativo — ¿separable o entrelazado?

◇ El test $ad = bc$ para dos qubits

Un estado $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ es *separable* si y solo si $ad = bc$.

Caso A

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

- ▶ $ad = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4} = bc$ ✓
- ▶ Factoriza: $|\psi_A\rangle = |+\rangle \otimes |+\rangle$.
- ▶ **Separable**. (concurrency $C = 2|ad - bc| = 0$)

Caso B

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

- ▶ $ad = \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} = \frac{1}{2}$, pero $bc = 0$.
- ▶ $ad \neq bc \Rightarrow$ no factoriza.
- ▶ **Entrelazado** máximo. ($C = 1$)

? Pausa socrática #4 — el recurso entrelazamiento

Un estado de Bell no se puede escribir como producto de dos qubits. ?

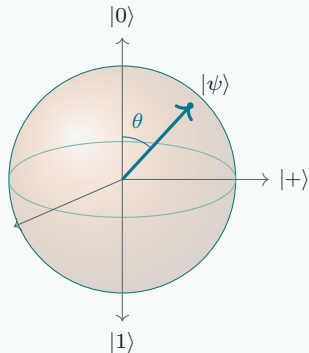
- ▶ Si ninguno de los dos qubits tiene estado propio, ¿dónde “vive” la información?
- ▶ ¿Por qué el entrelazamiento se considera un *recurso* que se consume?
- ▶ ¿Puede haber superposición sin entrelazamiento? ¿Y al revés?

La esfera de Bloch

Todo estado puro es un punto en la esfera

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle$$

- ▶ Eje z : $|0\rangle, |1\rangle$; eje x : $|+\rangle, |-\rangle$; eje y : $|+i\rangle, |-i\rangle$.
- ▶ Estados puros en la superficie; mixtos en el interior.



Realizaciones: átomo de hidrógeno y transmón

Átomo de hidrógeno — dos niveles

$$E_n = -\frac{13.6 \text{ eV}}{n^2}$$

$|0\rangle$ (fundamental, $n=1$) y $|1\rangle$ (excitado, $n=2$):

$\Delta E \approx 10.2 \text{ eV}$ (Lyman- α).

El transmón

La unión *Josephson* vuelve *anarmónicos* los niveles: $\Delta E_2 < \Delta E_1$. Eso permite aislar el subespacio $\{|0\rangle, |1\rangle\}$ con un pulso de microondas ($\omega_{01} \sim 5 \text{ GHz}$).

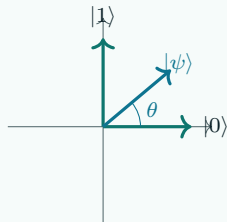
Qubits con polarización de fotones

El campo eléctrico oscila horizontal ($|0\rangle$) o vertical ($|1\rangle$):

Estado de un fotón polarizado

$$|\psi\rangle = \cos \theta |\downarrow\rangle + \sin \theta |\uparrow\rangle$$

Probabilidad de pasar un polarizador a ángulo θ : $\cos^2 \theta$;
de ser bloqueado: $\sin^2 \theta$ (ley de Malus).



? Pausa socrática #5 — muchas caras del mismo qubit

Un fotón, un átomo, un espín, un circuito — todos “son” el mismo qubit.?

- ▶ ¿Qué hace que sistemas físicos tan distintos compartan las mismas matemáticas?
- ▶ Si $|\psi\rangle$ es un punto en la esfera de Bloch, ¿qué representa *físicamente* la fase φ ?
- ▶ ¿Por qué necesitamos anarmonicidad (Josephson) para un buen qubit de estado sólido?

Ejercicio ilustrativo — leer la esfera de Bloch

◇ Del vector de estado a los ángulos (θ, φ)

Dado $|\psi\rangle = \frac{1}{2} |0\rangle + \frac{\sqrt{3}}{2} e^{i\pi/3} |1\rangle$, halla θ , φ y el vector de Bloch $\vec{r}$.

- ▶ Forma canónica: $\cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle$.
- ▶ $\cos \frac{\theta}{2} = \frac{1}{2} \Rightarrow \frac{\theta}{2} = 60^\circ \Rightarrow \boxed{\theta = 120^\circ}$.
- ▶ Chequeo: $\sin \frac{\theta}{2} = \frac{\sqrt{3}}{2}$ ✓ y $\boxed{\varphi = \frac{\pi}{3} = 60^\circ}$.

Vector de Bloch $\vec{r} =$
 $(\sin \theta \cos \varphi, \sin \theta \sin \varphi, \cos \theta)$

$$\vec{r} = \left(\frac{\sqrt{3}}{4}, \frac{3}{4}, -\frac{1}{2} \right)$$

$|\vec{r}| = 1$: estado *puro*, sobre la superficie de la esfera.

Sistemas de k niveles — ejemplo resuelto

Para $|\psi\rangle = \left(\frac{1}{2} + \frac{i}{2}\right) |0\rangle - \frac{1}{2} |1\rangle + \frac{i}{2} |2\rangle$, con $P[j] = |\alpha_j|^2$:

$$P[0] = \left|\frac{1}{2} + \frac{i}{2}\right|^2 = \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$
$$P[1] = \left|-\frac{1}{2}\right|^2 = \frac{1}{4}, \quad P[2] = \left|\frac{i}{2}\right|^2 = \frac{1}{4}$$

Tras medir

El sistema colapsa a $|0\rangle$, $|1\rangle$ o $|2\rangle$. Suma: $\frac{1}{2} + \frac{1}{4} + \frac{1}{4} = 1$ ✓

La probabilidad es *independiente de la base*: medir en $\{|+\rangle, |-\rangle\}$ da la misma distribución física.

Fidelidad: ¿qué tan cerca están dos estados?

Solapamiento al cuadrado

$$F(|\psi\rangle, |\phi\rangle) = |\langle\psi|\phi\rangle|^2 \in [0, 1]$$

$F = 1$ si son iguales (salvo fase global); $F = 0$ si son ortogonales. Invariante bajo unitarias.

Con error ϵ : $F = \cos^2 \epsilon \approx 1 - \epsilon^2$ — sensibilidad cuadrática.

Puente con la IA. La fidelidad $|\langle\psi|\phi\rangle|^2$ ^{AI} es el análogo cuántico de la *similitud coseno* entre *embeddings*: mide alineación en un espacio vectorial. Las compuertas de calidad ($F > 99.9\%$) son el equivalente a mantener baja la “pérdida”.

Invariancia rotacional del entrelazamiento

El estado de Bell se ve *igual* en cualquier base rotada:

$$|\psi\rangle = \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle = \frac{1}{\sqrt{2}} |uu\rangle + \frac{1}{\sqrt{2}} |u^\perp u^\perp\rangle$$

Al medir ambos qubits en la base $|u\rangle$: 50% los dos $|u\rangle$, 50% los dos $|u^\perp\rangle$.

Lo invariante

La *estructura* entrelazada se conserva bajo rotación; solo cambian las probabilidades $\cos^2 \theta, \sin^2 \theta$. Clave para las desigualdades de Bell.

? Pausa socrática #6 — correlaciones perfectas

En Φ^+ , ambos qubits siempre coinciden, en *cualquier* base compartida. ?

- ▶ ¿Cómo “sabe” un qubit qué base eligió el experimentador del otro?
- ▶ ¿Es esta correlación una prueba de comunicación instantánea? ¿Por qué no?
- ▶ ¿Podría una tabla de valores predefinidos (variables ocultas) reproducir esto?

Secciones 4.3–4.4

La paradoja EPR y las desigualdades de Bell

La paradoja EPR (1935)

Einstein, Podolsky y Rosen: ¿es *incompleta* la mecánica cuántica?

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Medir la primera partícula ($\rightarrow |0\rangle$) fija instantáneamente la segunda, sin importar la distancia — la “*acción fantasmal*”.

El dilema

Parece violar la *localidad* de la relatividad. ¿Hay **variables ocultas** que predeterminan los resultados?

Realismo + localidad $\Rightarrow$ desigualdad de Bell

Con variables ocultas λ , resultados $A, A', B, B' \in \{+1, -1\}$ y correlación

$$E(X, Y) = \int A_X(\lambda) B_Y(\lambda) \rho(\lambda) d\lambda.$$

Combinación CHSH

$$S = E(A, B) - E(A, B') + E(A', B) + E(A', B')$$

Como $|A(B - B') + A'(B + B')| \leq 2$ punto a punto:

$$\boxed{|S| \leq 2} \quad (\text{Bell / CHSH})$$

Los dos supuestos

Realismo: los valores existen antes de medir.

Localidad: nada viaja más rápido que la luz.

La predicción cuántica viola la cota

Para Φ^+ , la correlación es $E_{\text{QM}}(a, b) = \cos \theta_{a,b}$. Con $a=0^\circ, a'=90^\circ, b=45^\circ, b'=135^\circ$:

$$S_{\text{QM}} = \cos 45^\circ - \cos 135^\circ + \cos 45^\circ + \cos 45^\circ = 4 \cdot \frac{\sqrt{2}}{2} = 2\sqrt{2}$$

$$|S_{\text{QM}}| = 2\sqrt{2} \approx 2.828 > 2$$

Cota de Tsirelson

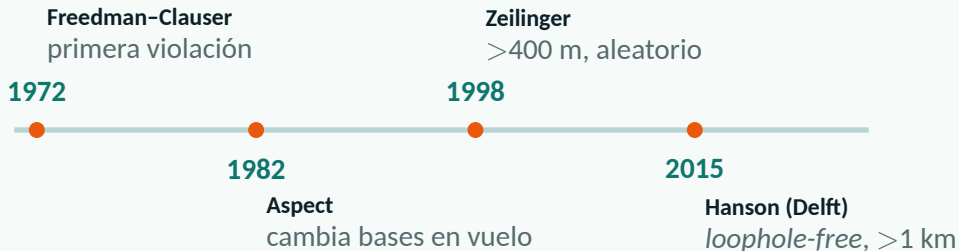
$2\sqrt{2}$ es la *máxima* violación posible.
La Naturaleza no respeta las variables ocultas locales.

? Pausa socrática #7 — realismo o localidad

La violación de Bell obliga a abandonar *al menos uno* de los dos supuestos. 

- ▶ ¿Cuál sacrificarías: el realismo (valores predefinidos) o la localidad?
- ▶ ¿Por qué $2\sqrt{2}$ y no más? ¿Qué principio limita la violación?
- ▶ ¿Es el entrelazamiento una “conexión”, o algo que nuestro lenguaje clásico no sabe nombrar?

Los experimentos que cerraron el debate



Cada experimento cerró un “resquicio” (loophole). El de 2015 los cerró *todos*: la no-localidad es real. (Nobel 2022: Aspect, Clauser, Zeilinger.)

El primer computador cuántico (MIT, 1998)

- ▶ Chuang, Gershenfeld, Kubinec: **2 qubits** por resonancia magnética nuclear (RMN) en cloroformo.
- ▶ Qubits = espines nucleares del ^{13}C y del H.
- ▶ Ejecutó el algoritmo de **Deutsch-Jozsa**.

Superposición uniforme

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

Primer algoritmo cuántico en hardware real.

? Pausa socrática #8 — de la teoría al laboratorio

En 1998 bastaban 2 qubits para “un computador cuántico”.



- ▶ ¿Qué distingue a un “computador cuántico” de un experimento de física?
- ▶ Deutsch–Jozsa resuelve un problema *artificial*. ¿Por qué importa igual?
- ▶ ¿Por qué la RMN no escaló, y sí lo hicieron los superconductores y los iones?

Sección 4.6

Teoremas de no-clonación

El teorema de no-clonación (1982)

Supongamos una máquina unitaria que copia: $U(|\psi\rangle |X\rangle) = |\psi\rangle |\psi\rangle$.

La linealidad lo prohíbe

Para $|\psi\rangle = \alpha |\psi_1\rangle + \beta |\psi_2\rangle$:

$$U(|\psi\rangle |X\rangle) = \alpha |\psi_1\rangle |\psi_1\rangle + \beta |\psi_2\rangle |\psi_2\rangle \neq |\psi\rangle |\psi\rangle$$

No existe dispositivo que copie un estado cuántico *arbitrario y desconocido*.
Wootters-Zurek y Dieks, 1982.

Ejercicio ilustrativo — la prueba en una línea

◇ La unitariedad preserva el producto interno

Supón que una misma máquina unitaria U clona dos estados: $U |\psi\rangle |X\rangle = |\psi\rangle |\psi\rangle$ y $U |\phi\rangle |X\rangle = |\phi\rangle |\phi\rangle$. ¿Qué restricción aparece?

- ▶ U es unitaria: $\langle \psi | X \rangle \langle \phi | X \rangle = \langle U(\psi X) | U(\phi X) \rangle$.
- ▶ Lado izquierdo: $\langle \psi | \phi \rangle \underbrace{\langle X | X \rangle}_=1 = \langle \psi | \phi \rangle$.
- ▶ Lado derecho: $\langle \psi | \phi \rangle \langle \psi | \phi \rangle = \langle \psi | \phi \rangle^2$.
- ▶ Igualando: $z = z^2$ con $z = \langle \psi | \phi \rangle$.

Única salida

$$z = z^2 \Rightarrow z \in \{0, 1\}$$

$z=1$ (mismo estado) o $z=0$ (ortogonales): solo se clonan estados **mutuamente ortogonales**, nunca superposiciones.

Consecuencias de la no-clonación

Corrección de errores — no vale “votar por mayoría” con copias; se codifica en *entrelazamiento* (código de Shor).

Seguridad de BB84 — un espía no puede copiar sin *perturbar*; la seguridad viene de la física.

Teletransporte — sorteando el teorema *destruyendo* el original: nunca hay dos copias a la vez.

Clonación aproximada — posible con fidelidad óptima $F = \frac{5}{6}$; lo prohibido es la copia *exacta*.

Además protege la incertidumbre de Heisenberg y prohíbe comunicación más rápida que la luz.

No-borrado y no-ocultamiento

No-borrado

No se puede *borrar* por completo un estado cuántico desconocido sin dejar rastro en otra parte.

No-ocultamiento (2007)

Si falta información en un sistema, *reside en otra parte* del universo — no se esconde en correlaciones con el entorno. (Braunstein-Pati; confirmado 2011.)

Tres teoremas, una idea: la información cuántica *se conserva* — no se crea ni se destruye a voluntad.

? Pausa socrática #9 — la información no se pierde

No-clonación, no-borrado, no-ocultamiento: la información cuántica [?] se conserva.

- ▶ Si no se puede copiar ni borrar, ¿cómo hace la corrección de errores para funcionar?
- ▶ ¿Qué relación hay entre “la información se conserva” y la reversibilidad unitaria?
- ▶ (Adelanto) ¿Cómo mueve el teletransporte un estado sin copiarlo ni destruir la información total?

Capítulo 4 — qué llevarse

- ▶ Un qubit es un vector unitario en $\mathbb{C}^2$; la esfera de Bloch lo visualiza.
- ▶ El poder viene de la *interferencia*, no de “calcular todo a la vez”.
- ▶ n qubits $\rightarrow$ dimensión 2^n ; el entrelazamiento es el recurso clave.
- ▶ Valor esperado y *fidelidad* $|\langle \psi | \phi \rangle|^2$ miden la información.
- ▶ Bell + experimentos: la no-localidad es *real* ($|S| = 2\sqrt{2}$).
- ▶ La información cuántica se *conserva*: no-clonación, no-borrado, no-ocultamiento.

Preguntas para llevar al Capítulo 5

- ▶ Ya tenemos qubits. ¿Cuáles son las *compuertas* fundamentales (X, Y, Z, H, T)?
- ▶ ¿Cómo se construyen compuertas de varios qubits (CNOT, Toffoli) y se crea entrelazamiento?
- ▶ ¿Qué conjunto de compuertas basta para la computación cuántica *universal*?

¡Nos vemos en el Capítulo 5 — Compuertas cuánticas!