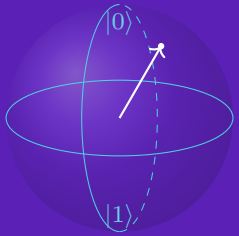
COMPUTACIÓN CUÁNTICA · UNA INTRODUCCIÓN

Capítulo 1

Computación Cuántica y Aplicaciones



Alcides Montoya Cañola

Universidad Nacional de Colombia · Sede Medellín | 2026-II

A dónde nos lleva este capítulo

- **Por qué** existe la computación cuántica
  la muralla exponencial de la Naturaleza
- **Los inicios**
  Feynman → Deutsch → Shor → Grover
- **La carrera del hardware hoy**
  superconductores, iones, átomos, fotones
- **Dónde va a importar**
  química, materiales, optimización, criptografía
- **Qué es mito y qué es real**
  un mapa crítico y honesto

Nuestra brújula

Aún no hay ecuaciones que memorizar — hoy construimos *intuición* y un *vocabulario*. Las matemáticas empiezan en el Capítulo 2.

Tres ideas que rompen la intuición clásica

Superposición

Un sistema puede estar en muchos estados *a la vez* — hasta que se mide.

Entrelazamiento

Correlaciones sin causa clásica — la *"acción fantasmal"* de Einstein.

Incertidumbre

Algunos pares de propiedades *no* pueden ser nítidos a la vez: $\Delta x \, \Delta p \geq \frac{\hbar}{2}$.

La física clásica usa **números reales**. La mecánica cuántica *exige* **números complejos** — la fuente de la interferencia.

Del bit al qubit al qudit

- **Bit:** exactamente 0 *o* 1.
- **Qubit:** una superposición de ambos,

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

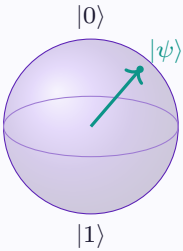
- **Qudit:** d niveles a la vez — más allá de lo binario.

Regla de Born

Al medir se obtiene $|0\rangle$ con prob. $|\alpha|^2$, y $|1\rangle$ con prob. $|\beta|^2$.

bit clásico

qubit (esfera de Bloch)



? Pausa socrática #1 — la medición

Si un qubit realmente es "0 y 1 a la vez", entonces:

- ¿Qué ocurre *físicamente* en el instante en que lo observamos?
- ¿A dónde va el "otro" resultado — y podremos recuperarlo alguna vez?
- ¿La superposición es un hecho sobre *el mundo*, o sobre *nuestro conocimiento*?

Déjenlas abiertas. Hoy no las responderemos — el Capítulo 3 da los postulados.

Sección 1.1

Los inicios

1981 — Feynman lanza el desafío

> *"La Naturaleza no es clásica, maldita sea, y si quieres hacer una simulación de la Naturaleza, más te vale hacerla mecánico-cuántica, y por Dios que es un problema maravilloso, porque no se ve nada fácil."*

- **La semilla:** para simular la Naturaleza con eficiencia, el computador debe *ser* cuántico.
- El costo clásico de los sistemas cuánticos crece **exponencialmente**: $\mathcal{O}(e^N)$.

1.ª Conferencia sobre la Física de la Computación
MIT, 1981

Cuatro hitos que construyeron un campo

- **Shor** convirtió una curiosidad en una amenaza estratégica: RSA se vuelve vulnerable.
- **Grover** — una aceleración menor ($\sqrt{N}$), pero para una clase *mucho* más amplia de problemas.

Fragilidad y las dos caras de lo “cuántico”

Decoherencia

Los estados cuánticos son *frágiles*: se fugan hacia el entorno.

La **corrección cuántica de errores** (Shor, Steane, años 90) demostró que la información *sí* puede protegerse — la clave para escalar.

Dos campos distintos

- **Computación** — algoritmos (Shor, Grover).
- **Comunicación** — distribución de claves **BB84**: seguridad desde la *física*, no desde supuestos de dificultad.

La seguridad de BB84 descansa en el principio de *no-clonación*: un estado cuántico desconocido no se puede copiar.

Sección 1.2

Motivación — la muralla exponencial

Por qué los computadores clásicos chocan contra un muro

Simular la **penicilina** — apenas 41 átomos:

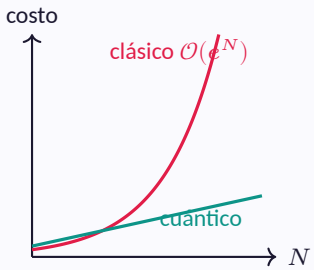
La catástrofe del almacenamiento

$\underbrace{\sim 2^{286}}_{\text{amplitudes complejas}} \gg$ átomos en el universo observable

Un computador cuántico solo necesita

286 qubits

porque la superposición codifica un espacio **exponencialmente** grande en un número *lineal* de qubits.



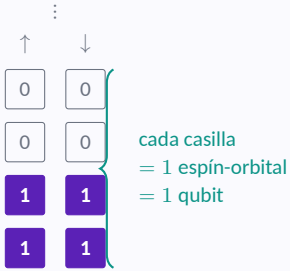
La brecha no es un detalle de ingeniería — es *exponencial*.

De dónde salen los 286 qubits

- Cada electrón ocupa **orbitales**; con el espín ($\uparrow\downarrow$) hablamos de **espín-orbitales**.
- Cada espín-orbital es una *casilla*: **vacía (0)** u **ocupada (1)** — ¡es un qubit!
- N.º de qubits = n.º de espín-orbitales $= 2 \times$ (orbitales espaciales).

La cuenta para la penicilina

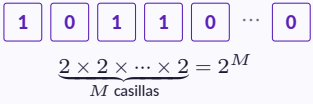
$$\underbrace{41 \text{ átomos}}_{C_{16}H_{18}N_2O_4S} \Rightarrow \underbrace{143}_{\text{orb. espaciales}} \Rightarrow \underbrace{2 \times 143 = 286}_{\text{espín-orbitales = qubits}}$$



176 electrones acomodados en 286 casillas.

Por qué el costo es 2^{286}

El estado electrónico es una cadena de ocupaciones; la función de onda, su *superposición*:



Superposición de determinantes de Slater

$$|\Psi\rangle = \sum_{\vec{n}} c_{\vec{n}} \; |n_1 n_2 \cdots n_M\rangle \,, \quad n_i \in \{0, 1\}$$

El número

$$2^{286} \approx 1.2 \times 10^{86}$$

$\sim 10^6\times$ los átomos del universo (10^{80})

- M casillas independientes $\Rightarrow 2^M$ configuraciones.
- Producto tensorial: $\dim \left(\mathbb{C}^2\right)^{\otimes M} = 2^M$ — las dimensiones se *multiplican*.

Un problema digno de un computador de nuevo tipo

- El **cofactor FeMo** (nitrogenasa) — la enzima detrás de la fijación natural de nitrógeno.
- Simulación clásica exacta: *más memoria que átomos en el universo*.
- Al alcance de una máquina **tolerante a fallos** con unos miles de qubits lógicos.

Puente con la IA. La IA moderna también se enfrenta a espacios exponenciales, pero[AI] los aborda *al revés*. El aprendizaje profundo *renuncia a la exactitud*: aproxima la solución con datos y descenso por gradiente. La computación cuántica hace lo contrario: *representa el espacio de estados exponencial de forma exacta*, encarnándolo en el hardware. En breve: la IA sacrifica *rigor* para ganar *escala*; lo cuántico conserva el *rigor*, al precio de un hardware todavía pequeño.

? Pausa socrática #2 — ¿qué es “ventaja”?

- Si un computador cuántico guarda 2^{286} amplitudes, ¿por qué no podemos simplemente *leerlas todas*?
- Un clúster de GPU también se siente “exponencialmente poderoso”. ¿Qué hace *diferente* al exponencial cuántico?
- ¿La “aceleración exponencial” es una propiedad de la *máquina* o del *problema*?

Desarrollos actuales

La carrera del hardware, 2026

Qubits superconductores — IBM y Google

IBM Quantum

- Condor (1,121 q, 2023), Heron (133 q, alta fidelidad).
- System Two — procesadores modulares enlazados.
- Hoja de ruta: **Starling** (2029) ≈ 200 qubits lógicos; **Blue Jay** (2033) ≈ 2,000.

Google Quantum AI

- Sycamore (2019): afirmación de *supremacía cuántica*.
- **Willow** (2024): corrección de errores **por debajo del umbral** — más qubits, *menos* error.

El hito que sí importa

Willow mostró que agregar qubits a un qubit lógico de código de superficie puede hacer que los errores caigan *exponencialmente* — validando décadas de teoría de corrección.

Aún no hay ganador — un zoológico de qubits

Iones atrapados — IonQ, Quantinuum
las fidelidades más altas, conectividad todos-con-todos; compuertas más lentas

Átomos neutros — QuEra, Pasqal
pinzas ópticas, reconfigurables; 6,100 átomos (2025)

Fotónica — PsiQuantum, Xanadu
temperatura ambiente; lucha contra la pérdida de fotones

Recocido (annealing) — D-Wave
4,400+ qubits; solo optimización, no universal

También: **qubits topológicos** (Microsoft, Majorana 1) — prometedores pero aún *en disputa*. Acceso en la nube: **IBM Quantum**, **Amazon Braket**.

Dos eras: NISQ ahora, FTQC después

NISQ — hoy

Noisy Intermediate-Scale Quantum. Cientos de qubits físicos ruidosos + *mitigación* de errores. Sirve para química pequeña, heurísticas, experimentos.

FTQC — la meta

Fault-Tolerant Quantum Computing. Qubits lógicos con errores *corregidos*. Necesario para Shor a escala y biomoléculas exactas.

Los computadores cuánticos *no* reemplazarán a los clásicos — serán **aceleradores especializados** dentro de flujos de HPC.

? Pausa socrática #3 — leyendo el bombo

Un comunicado de prensa dice: *"5 minutos frente a* 10^{25} *años"*.

- ¿En *qué tarea*? ¿Sería esa una tarea que de verdad necesitas resolver?
- ¿La "supremacía" en un test artificial implica *utilidad*?
- ¿Por qué tantas hojas de ruta cuentan qubits *lógicos* — y no físicos?

Sección 1.3

Aplicaciones — promesa vs. realidad

Tres horizontes honestos

Corto plazo (NISQ) — química pequeña, heurísticas de optimización

Mediano plazo (FTQC temprana) — miles de qubits lógicos

Largo plazo (FTQC madura) — millones de qubits · Shor a escala, biomoléculas

La destreza que enseña este capítulo: clasificar cada afirmación en el horizonte *correcto*.

Química y materiales — el hogar natural

- Los datos *nacen cuánticos* — no hay cuello de botella de carga.
- **VQE** (NISQ): minimización híbrida cuántico-clásica de energía.
- **QPE** (FTQC): energías del estado fundamental exactas.
- Objetivos: unión de fármacos, **Haber–Bosch**, superconductores, baterías.

El cuello de botella clásico

El estándar de oro CCSD(T) escala como

$$\mathcal{O}(M^7)$$

en el número de orbitales M — brutal.

Mapeo de fermiones sin signo vía Jordan–Wigner / Bravyi–Kitaev $\Rightarrow$ el modelo de Fermi–Hubbard.

Optimización — finanzas, logística, industria

- Muchos problemas industriales son **NP-difíciles**: rutas, agendamiento, portafolios.
- Se codifican como **QUBO** — optimización binaria cuadrática.
- Se resuelven con **QAOA** (compuertas) o **recocido** cuántico (D-Wave).
- Pilotos de Volkswagen, Airbus, DHL, JPMorgan.

Baño de realidad. Todavía *sin* superar de forma *demostrable* a los solvers clásicos (Gurobi, CPLEX). Hoy: prueba de concepto, no producción.

Aquí lo cuántico *potencia* las heurísticas clásicas — no las reemplaza.

Criptografía — una amenaza existencial

- RSA / ECC descansan en que **factorizar** y el **logaritmo discreto** sean difíciles.
- **Shor** derrumba esa dificultad: de exponencial a polinomial.
- Las estimaciones de recursos son un *blanco móvil*:

RSA-2048: $\sim$20M qubits (2019) $\longrightarrow$ $<$1M (Gidney 2025)

Cosechar ahora, descifrar después.

Los adversarios archivan datos cifrados *hoy* para descifrarlos cuando llegue la FTQC. Todo lo que requiera 10–15 años de secreto *ya* está expuesto.

? Pausa socrática #4 — una amenaza sin máquina

La máquina que rompe RSA aún no existe. Y aun así —

- ¿Por qué debemos actuar *ya* contra un computador que puede estar a una década?
- ¿Quién decide cuáles secretos merecen 15 años de protección?
- Si la seguridad migra a *nuevos* problemas difíciles — ¿qué nos hace confiar en *esos*?

La defensa — criptografía post-cuántica

Corre en hardware *clásico*; su seguridad viene de problemas difíciles para máquinas *clásicas y* cuánticas (retículos, códigos).

ML-KEM
(Kyber) — intercambio de claves

ML-DSA
(Dilithium) — firmas

SLH-DSA
(SPHINCS+) — basada en hash

Estandarizadas por NIST (2024); **HQC** añadida en 2025 como respaldo basado en códigos. Bitcoin/Ethereum (ECDSA) también deben migrar.

Simular la física misma

La tarea central: convertir la evolución temporal en compuertas.

Simulación de hamiltonianos

$$U(t) = e^{-iHt}$$

- **Trotterización**: dividir $H = \sum_j H_j$ en pasos pequeños.
- **Qubitización / QSP**: escalamiento óptimo $\mathcal{O}(t + \log \frac{1}{\epsilon})$.

- Física de muchos cuerpos: Fermi–Hubbard, transiciones de Mott.
- Teorías gauge en red / QCD — evita el *problema del signo* clásico.
- Dispersión en tiempo real, materia de estrellas de neutrones.

Este es el sueño *original* de Feynman, por fin operativo.

? Pausa socrática #5 — la máquina como microscopio

- Si solo podemos *simular* una ley física que ya creemos, ¿puede un computador cuántico *sorprendernos* sobre la Naturaleza?
- Una simulación da números. ¿Cómo sabrías que son *correctos* sin una verificación clásica?
- ¿Dónde está la frontera entre “computar” y “hacer un experimento”?

Aprendizaje automático cuántico — promesa y límites duros

Tres paradigmas:

- **Núcleos cuánticos (kernels)**: mapean datos al espacio de Hilbert, $K(x, x') = |\langle\psi(x)|\psi(x')\rangle|^2$.
- **Circuitos variacionales (VQC)**: los ángulos de rotación $U(\theta)$ actúan como pesos entrenables.
- **qPCA** y subrutinas algebraicas.

AI

Puente con la IA. Un VQC *es* una red neuronal cuyos pesos son los ángulos de compuerta θ, entrenada por un optimizador clásico (Adam, SGD). El paso hacia adelante corre en hardware cuántico.

Por qué el QML no es “IA, pero más rápida”

Mesetas estériles (barren plateaus)

Los gradientes se desvanecen exponencialmente con el número de qubits n:

$$\mathrm{Var}[\partial_\theta C] \in \mathcal{O}(2^{-n})$$

El entrenamiento se estanca — sin dirección de descenso.

- Cuello de botella de **carga de datos / QRAM**: codificar N puntos clásicos puede costar $\mathcal{O}(N)$ — matando la aceleración.
- **Sobrecosto de medición**: precisión ϵ exige $\mathcal{O}(\epsilon^{-2})$ repeticiones.

“Lo cuántico revolucionará el *Big Data*” — en gran parte **sin fundamento**. Mejor encaje: datos que *ya* son cuánticos.

? Pausa socrática #6 — cuántico vs. clásico en aprendizaje

El aprendizaje profundo clásico está ganando casi en todas partes, ahora mismo.

- Si cargar datos clásicos es el cuello de botella, ¿dónde podría *aún* ganar el QML?
- Las mesetas estériles evocan los gradientes que se desvanecen en redes profundas — ¿coincidencia, o una ley más honda de los modelos grandes?
- ¿Cómo sería un banco de pruebas *justo* entre aprendizaje cuántico y clásico?

La frontera lejana — manéjese con cuidado

- **AdS/CFT** y gravedad cuántica — el espacio-tiempo a partir del entrelazamiento.
- **Agujeros negros** como codificadores rápidos — rastreados con OTOCs.
- **Cosmología cuántica** — funciones de onda de juguete del universo temprano.

Estatus epistémico.

Sin teoría consensuada · sin observables · sin algoritmos escalables · sin cotas de recursos. *Intuición, no aplicación.*

Contraste: la química tiene teoría *validada* + algoritmos *explícitos*. La gravedad no tiene ninguno — todavía.

? Pausa socrática #7 — ¿dónde está la frontera?

- ¿Qué separa una aplicación cuántica *científica* de una *especulativa*?
- ¿Es deshonesto publicitar simulaciones de gravedad — o es como los campos atraen fondos y talento?
- ¿Cuáles de los temas “especulativos” de hoy podrían ser *rutina* cuando te gradúes?

Sección 1.4

Cómo usar este libro

Lo que debes traer

Lo innegociable

Álgebra lineal. La mecánica cuántica *vive* en espacios vectoriales complejos.

- Espacios vectoriales y de Hilbert, notación bra-ket de Dirac.
- Valores propios, descomposición espectral.
- Operadores hermíticos (observables) y unitarios (evolución).

- **Números complejos**: fórmula de Euler, fases $e^{i\phi}$.
- **Probabilidad**: distribuciones, esperanza, varianza.
- **Python**: para de verdad *ejecutar* los algoritmos.

Cada perfil (física / computación / matemáticas) tiene su propia ruta por el libro.

Las herramientas que de verdad usaremos

SDK	Desarrollador	Papel en el curso
Qiskit	IBM Quantum	circuitos, ruido, nube de superconductores
Cirq	Google Quantum AI	optimización de circuitos NISQ de bajo nivel
Q#	Microsoft Azure	estimación de recursos tipada, a gran escala
PennyLane	Xanadu	circuitos diferenciables, QML híbrido

Validar primero en simuladores clásicos → luego desplegar a hardware real vía IBM Quantum / Amazon Braket.

Capítulo 1 — qué llevarse

- La computación cuántica existe porque simular la Naturaleza es *exponencialmente* caro en clásico.
- Superposición + entrelazamiento + interferencia = un recurso genuinamente nuevo.
- Vivimos en la era **NISQ**; la **FTQC** es la meta.
- La ventaja real es *específica del problema*: química, materiales, algo de optimización, criptografía.
- Separar el bombo de la evidencia — siempre preguntar “¿en qué tarea?”
- Sigue: las *matemáticas* que hacen todo esto preciso.

Preguntas para llevar al Capítulo 2

- ¿Por qué debería un número *complejo*, y no uno real, describir un estado del mundo?
- Si la medición da probabilidades, ¿dónde viven las *amplitudes* antes de mirar?
- ¿Cuál es el trozo mínimo de matemática que te dejaría *a ti* predecir un resultado cuántico?

¡Nos vemos en el Capítulo 2 — Fundamentos Matemáticos!