Introducción a la Computación e Información Cuántica

Módulo 2: Fundamentos y Motivaciones

6 al 10 de Octubre de 2025

Dr. Andres A. REYNOSO

XXIX Escuela Internacional de Ingeniería y Computación

Conceptos AYER

1. **Superposición**: Un qubit puede estar en $\alpha|0\rangle + \beta|1\rangle$
2. **Medición en la base computacional**: Colapsa el estado a $|0\rangle$ o $|1\rangle$ según probabilidades $|\alpha|^2$ o $|\beta|^2$, respectivamente.
3. **Observables incompatibles**: Los resultados obtenidos no conmutan
4. **Evolución unitaria**: Sin medición, el sistema evoluciona **reversiblemente**
5. **Matrices de Pauli**: Operadores fundamentales con autovalores ± 1
6. **Notación de Dirac**: NOTACION DE DIRAC (BRAs y KETs) lenguaje elegante para producto internos de estados, para expresar operadores, valores esperados de operadores, etc

Contenidos

El Qubit: Sistema Cuántico de Dos Niveles

Definición: Un qubit es cualquier sistema cuántico con dos estados distinguibles

Ejemplos físicos:

- Espín de un electrón: $|\uparrow\rangle$, $|\downarrow\rangle$
- Polarización de fotón: $|H\rangle$, $|V\rangle$
- Niveles de energía de un átomo: $|g\rangle$, $|e\rangle$
- Estado de carga de un punto cuántico: $|0e\rangle$, $|1e\rangle$
- Flujo magnético en un SQUID superconductor: $|\circlearrowleft\rangle$, $|\circlearrowright\rangle$

Notación estándar: $|0\rangle$ y $|1\rangle$ (base computacional)

Diferencia con un Bit Clásico

Bit Clásico:

- Estado: 0 o 1
- **Un bit**: 2 estados posibles
- Solo puede estar en *uno* a la vez
- **N bits**: Uno entre 2^N estados posibles (LUEGO)

Qubit:

- Estado: $\alpha |0\rangle + \beta |1\rangle$
- **Un qubit**: ∞ estados (esfera de Bloch)
- Está en **superposición**
- **N qubits**: describe 2^N amplitudes **simultáneamente** (LUEGO)

¡La superposición es el recurso fundamental para la computación cuántica!

NOTACION DE DIRAC, Vectores de Estado: Kets

Paul Dirac introdujo una notación elegante para estados cuánticos

Ket: $|\psi\rangle$ representa un vector columna en el espacio de Hilbert

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

Superposición:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

Normalización: $\langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2 = 1$

Vectores Duales: Bras

Bra: $\langle\psi|$ es el vector fila (dual, conjugado hermítico)

$$\langle 0| = \begin{pmatrix} 1 & 0 \end{pmatrix}, \quad \langle 1| = \begin{pmatrix} 0 & 1 \end{pmatrix}$$

Si $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$, entonces:

$$\langle\psi| = \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix}$$

Producto interno ("bracket"):

$$\langle\phi|\psi\rangle = \text{número complejo}$$

Ortogonalidad: $\langle 0|1\rangle = 0$, $\langle 0|0\rangle = 1$

Producto Externo y Operadores

Producto externo: $|\psi\rangle\langle\phi|$ es una **matriz**

Ejemplo:

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

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

Relación de completitud:

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

Esta identidad es fundamental para cambios de base

Las Matrices de Pauli

Operadores fundamentales para qubits:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

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

Propiedades:

- Hermíticas: $\sigma^\dagger = \sigma$
- Unitarias: $\sigma^\dagger \sigma = I$
- Autovalores: ± 1
- Traza: $\mathrm{Tr}(\sigma) = 0$ (excepto I)
- Anticonmutan: $XY = -YX$, etc.

Interpretación Física de las Matrices de Pauli

Compuerta X (NOT cuántico):

$$X|0\rangle = |1\rangle, \quad X|1\rangle = |0\rangle$$

Compuerta Z (cambio de fase):

$$Z|0\rangle = |0\rangle, \quad Z|1\rangle = -|1\rangle$$

Compuerta Y:

$$Y|0\rangle = i|1\rangle, \quad Y|1\rangle = -i|0\rangle$$

En notación de Dirac:

$$X = |0\rangle\langle 1| + |1\rangle\langle 0|, \quad Z = |0\rangle\langle 0| - |1\rangle\langle 1|$$

Estados Propios de las Matrices de Pauli

Base Z (computacional):

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

Base X:

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

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

Base Y:

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

La Esfera de Bloch

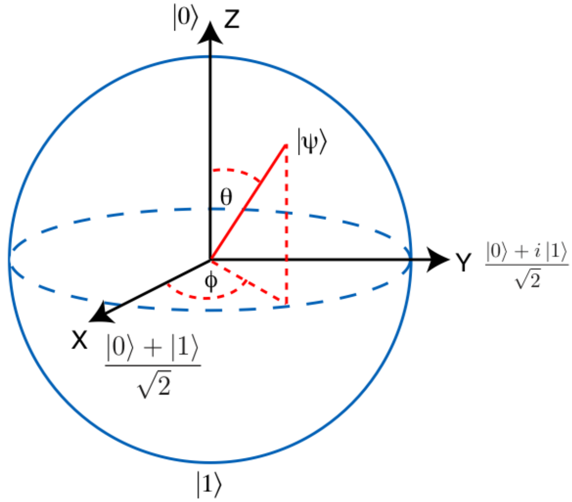
Todo estado puro de un qubit se puede escribir:

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

donde $\theta \in [0, \pi]$ y $\phi \in [0, 2\pi)$

- Cada punto en una esfera = un estado cuántico
- Polo norte: $|0\rangle$
- Polo sur: $|1\rangle$
- Ecuador: superposiciones equitativas
- Estados opuestos = ortogonales

La Esfera de Bloch



Esfera de Bloch

Dirección Arbitraria: $|S \cdot \hat{n}, \pm\rangle$

Vector unitario arbitrario:

$$\hat{n} = \sin\theta\cos\phi\,\hat{x} + \sin\theta\sin\phi\,\hat{y} + \cos\theta\,\hat{z}$$

Estados propios del espín en dirección $\hat{n}$:

$$|S \cdot \hat{n}, +\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle$$

$$|S \cdot \hat{n}, -\rangle = \sin\frac{\theta}{2}\,|0\rangle - e^{i\phi}\cos\frac{\theta}{2}\,|1\rangle$$

Operador de Pauli en dirección $\hat{n}$:

$$\hat{\sigma}_n = \sin\theta\cos\phi\,X + \sin\theta\sin\phi\,Y + \cos\theta\,Z$$

Tiene autovalores ± 1 con autovectores $|S \cdot \hat{n}, \pm\rangle$

Los 4 Postulados Fundamentales de la mecánica cuántica

Postulado 1: El estado de un sistema cuántico se describe por un vector $|\psi\rangle$ en un espacio de Hilbert

Postulado 2: La evolución temporal está dada por la ecuación de Schrödinger

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

Solución: $|\psi(t)\rangle = e^{-i\hat{H}t/\hbar} |\psi(0)\rangle = \hat{U}(t) |\psi(0)\rangle$

$\hat{U}$ es un operador **unitario**: $\hat{U}^\dagger \hat{U} = \mathbb{I}$

La evolución cuántica sin medición es unitaria y reversible

Los 4 Postulados Fundamentales (cont.)

Postulado 3: Cada observable físico está asociado a un operador hermítico $\hat{A}$

- Los resultados posibles son los autovalores de $\hat{A}$
- Después de medir y obtener a_i, el estado colapsa al autoestado $|a_i\rangle$

Postulado 4 (Regla de Born): La probabilidad de obtener a_i al medir $\hat{A}$ en el estado $|\psi\rangle$ es:

$$P(a_i) = |\langle a_i|\psi\rangle|^2$$

Valor esperado: $\langle\hat{A}\rangle = \langle\psi|\hat{A}|\psi\rangle$

Operadores Hermíticos y sus Propiedades

Operador hermítico: $\widehat{H}^\dagger = \widehat{H}$

Teorema: Los autovalores de un operador hermítico son reales

Demostración:

$$\widehat{H}\,|\psi\rangle = \lambda\,|\psi\rangle$$
$$\langle\psi|\,\widehat{H}\,|\psi\rangle = \lambda\,\langle\psi|\psi\rangle = \lambda$$
$$\langle\psi|\,\widehat{H}^\dagger\,|\psi\rangle = (\langle\psi|\,\widehat{H}\,|\psi\rangle)^* = \lambda^*$$
$$\text{Pero } \widehat{H}^\dagger = \widehat{H} \Rightarrow \lambda = \lambda^* \Rightarrow \lambda \in \mathbb{R}$$

Consecuencia: Los observables físicos tienen valores medibles reales

Autovectores de Distintos Autovalores son Ortogonales

Teorema: Si $\hat{H}\left|\psi_1\right\rangle = \lambda_1\left|\psi_1\right\rangle$ y $\hat{H}\left|\psi_2\right\rangle = \lambda_2\left|\psi_2\right\rangle$ con $\lambda_1 \neq \lambda_2$, entonces $\left\langle\psi_1|\psi_2\right\rangle = 0$

Demostración:

$$
\begin{aligned}
\left\langle\psi_1\right|\hat{H}\left|\psi_2\right\rangle &= \lambda_2\left\langle\psi_1|\psi_2\right\rangle \\
\left(\left\langle\psi_1\right|\hat{H}\left|\psi_2\right\rangle\right)^* &= \left\langle\psi_2\right|\hat{H}^\dagger\left|\psi_1\right\rangle = \left\langle\psi_2\right|\hat{H}\left|\psi_1\right\rangle \\
&= \lambda_1\left\langle\psi_2|\psi_1\right\rangle = \lambda_1\left\langle\psi_1|\psi_2\right\rangle^* \\
\Rightarrow \lambda_2\left\langle\psi_1|\psi_2\right\rangle &= \lambda_1\left\langle\psi_1|\psi_2\right\rangle^* = \lambda_1\left\langle\psi_1|\psi_2\right\rangle \\
(\lambda_2 - \lambda_1)\left\langle\psi_1|\psi_2\right\rangle &= 0
\end{aligned}
$$

Como $\lambda_1 \neq \lambda_2 \Rightarrow \left\langle\psi_1|\psi_2\right\rangle = 0$

Operadores Unitarios

Operador unitario: $\hat{U}^\dagger \hat{U} = \hat{U}\hat{U}^\dagger = \mathbb{I}$

Teorema: Los autovalores de un operador unitario tienen módulo 1: $\lambda = e^{i\phi}$

Demostración:

$$\begin{aligned}
\hat{U}\,|\psi\rangle &= \lambda\,|\psi\rangle \\
\langle\psi|\,\hat{U}^\dagger \hat{U}\,|\psi\rangle &= |\lambda|^2\,\langle\psi|\psi\rangle \\
\langle\psi|\,\mathbb{I}\,|\psi\rangle &= |\lambda|^2 \\
1 &= |\lambda|^2 \Rightarrow |\lambda| = 1
\end{aligned}$$

Propiedades importantes:

- Los operadores unitarios preservan el producto interno
- Representan evoluciones temporales y compuertas cuánticas

Unitaridad: Conservación del Producto Interno

¿Qué significa que la evolución sea unitaria?

Significa que la transformación **conserva el producto interno** entre dos estados cuánticos cualesquiera. Si dos estados $|\phi\rangle$ y $|\psi\rangle$ evolucionan a $|\phi'\rangle$ y $|\psi'\rangle$, sus ángulos y longitudes relativas no cambian.

Demostración

Partimos de dos estados $|\phi\rangle$ y $|\psi\rangle$ que evolucionan según $|\phi'\rangle = \hat{U}|\phi\rangle$ y $|\psi'\rangle = \hat{U}|\psi\rangle$. Calculemos su nuevo producto interno:

$$\begin{aligned}\langle\phi'|\psi'\rangle &= (\langle\phi|\hat{U}^\dagger)(\hat{U}|\psi\rangle) \\ &= \langle\phi|(\hat{U}^\dagger\hat{U})|\psi\rangle = \langle\phi|\mathbb{I}|\psi\rangle \\ &= \langle\phi|\psi\rangle\end{aligned}$$

Consecuencia clave: Las probabilidades se conservan. Si la norma de un estado es 1 antes de la evolución, ($\langle\psi|\psi\rangle = 1$), se mantiene en 1 después, ya que $\langle\psi'|\psi'\rangle = \langle\psi|\psi\rangle = 1$.

La Estructura de una Matriz Unitaria

La condición $\hat{U}^\dagger \hat{U} = \mathbb{I}$ impone una restricción muy fuerte sobre la forma de la matriz U. **Las Columnas de U forman una Base Ortonormal (ONB)** Si escribimos U en términos de sus vectores columna $U = [|c_1\rangle, |c_2\rangle, \ldots, |c_n\rangle]$, entonces $U^\dagger$ tiene los correspondientes "brasçomo filas.

$$U^\dagger U = \begin{pmatrix} \text{—}\langle c_1|\text{—} \\ \text{—}\langle c_2|\text{—} \\ \vdots \\ \text{—}\langle c_n|\text{—} \end{pmatrix} \begin{pmatrix} | & | & & | \\ |c_1\rangle & |c_2\rangle & \ldots & |c_n\rangle \\ | & | & & | \end{pmatrix} = \begin{pmatrix} 1 & 0 & \ldots \\ 0 & 1 & \ldots \\ \vdots & \vdots & \ddots \end{pmatrix}$$

Al realizar el producto, se deduce que $\langle c_i|c_j\rangle = \delta_{ij}$. ¡Los vectores columna son ortonormales entre sí!

- De la misma forma, al analizar $\hat{U}\hat{U}^\dagger = \mathbb{I}$, se demuestra que los **vectores fila** de U también forman una base ortonormal.
- **Intuición:** Una transformación unitaria es el análogo a una **rotación** en un espacio vectorial complejo. No estira ni encoge los vectores, y preserva los ángulos entre ellos.

Proyectores (Utiles para medición)

Proyector: $\widehat{P}^2 = \widehat{P}$ y $\widehat{P}^\dagger = \widehat{P}$

Teorema: Los autovalores de un proyector son 0 o 1

Demostración:

$$\begin{aligned} \widehat{P}\,|\psi\rangle &= \lambda\,|\psi\rangle \\ \widehat{P}^2\,|\psi\rangle &= \widehat{P}(\lambda\,|\psi\rangle) = \lambda\widehat{P}\,|\psi\rangle = \lambda^2\,|\psi\rangle \\ \text{Pero } \widehat{P}^2 = \widehat{P} &\Rightarrow \lambda\,|\psi\rangle = \lambda^2\,|\psi\rangle \\ &\Rightarrow \lambda = \lambda^2 \Rightarrow \lambda(\lambda - 1) = 0 \end{aligned}$$

Por lo tanto: $\lambda = 0$ o $\lambda = 1$

Ejemplo: $\widehat{P}_0 = |0\rangle\,\langle 0|$ proyecta sobre $|0\rangle$

Traza de un Operador

Definición: $\mathrm{Tr}(\hat{A}) = \sum_i \langle i | \hat{A} | i \rangle$ (suma de elementos diagonales)

Propiedad cíclica: $\mathrm{Tr}(\hat{A}\hat{B}\hat{C}) = \mathrm{Tr}(\hat{B}\hat{C}\hat{A}) = \mathrm{Tr}(\hat{C}\hat{A}\hat{B})$

Demostración:

$$\begin{aligned}
\mathrm{Tr}(\hat{A}\hat{B}\hat{C}) &= \sum_i \langle i | \hat{A}\hat{B}\hat{C} | i \rangle \\
&= \sum_{i,j,k} \langle i|j\rangle \langle j| \hat{A} |k\rangle \langle k|l\rangle \langle l| \hat{B} |m\rangle \langle m|n\rangle \langle n| \hat{C} |i\rangle \\
&= \sum_{j,k,l} \langle j| \hat{A} |k\rangle \langle k| \hat{B}\hat{C} |j\rangle = \mathrm{Tr}(\hat{B}\hat{C}\hat{A})
\end{aligned}$$

Consecuencia: $\mathrm{Tr}(\hat{U}^\dagger \hat{A}\hat{U}) = \mathrm{Tr}(\hat{A})$

La traza es independiente de la base (invariante bajo transformaciones unitarias)

Ejemplo: Traza de las Matrices de Pauli

Calculamos explícitamente:

$$\mathrm{Tr}(X) = \mathrm{Tr}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = 0 + 0 = 0$$

$$\mathrm{Tr}(Y) = \mathrm{Tr}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = 0 + 0 = 0$$

$$\mathrm{Tr}(Z) = \mathrm{Tr}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = 1 + (-1) = 0$$

$$\mathrm{Tr}(I) = \mathrm{Tr}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1 + 1 = 2$$

Observación: Todas las matrices de Pauli (excepto I) tienen traza cero

Cambios de Base

Pregunta: ¿Cómo expresar $|+\rangle$ en la base Y?

Usamos la relación de completitud: $|+\rangle = (|+i\rangle\langle +i| + |-i\rangle\langle -i|)\,|+\rangle$
$= \langle +i|+\rangle\,|+i\rangle + \langle -i|+\rangle\,|-i\rangle$

Calculamos los productos internos:

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

Similarmente: $\langle -i|+\rangle = \frac{1}{2}(1 + i)$

$\Rightarrow |+\rangle = \frac{1-i}{2}\,|+i\rangle + \frac{1+i}{2}\,|-i\rangle$

Propiedades del Producto Interno

Un producto interno hermitiano $(|v\rangle, |w\rangle) \equiv \langle v|w\rangle$ satisface:

1. **Linealidad en el segundo argumento**: $\langle w| \sum_i \lambda_i v_i\rangle = \sum_i \lambda_i \langle w|v_i\rangle$
2. **Simetría hermítica**: $\langle w|v\rangle = \langle v|w\rangle^*$
3. **Positividad**: $\langle v|v\rangle \geqslant 0, \quad \langle v|v\rangle = 0 \Leftrightarrow |v\rangle = 0$

Antilinealidad en el Primer Argumento

Pregunta: ¿Qué pasa con $\langle \sum_i \lambda_i w_i | v \rangle$?

Demostración:

$$\begin{aligned}
\langle \sum_i \lambda_i w_i | v \rangle &= \left(\langle v | \sum_i \lambda_i w_i \rangle \right)^* && \text{(por simetría hermítica)} \\
&= \left(\sum_i \lambda_i \langle v | w_i \rangle \right)^* && \text{(por linealidad)} \\
&= \sum_i \lambda_i^* \langle v | w_i \rangle^* \\
&= \sum_i \lambda_i^* \langle w_i | v \rangle
\end{aligned}$$

Conclusión: El producto interno es **antilineal** en el primer argumento: $\langle \sum_i \lambda_i w_i | = \sum_i \lambda_i^* \langle w_i |$

Proyectores como operadores de Medición

Proyectores sobre la base computacional

$$M_0 = |0\rangle\langle 0| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad , \quad M_1 = |1\rangle\langle 1| = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

Regla de Born para Probabilidades

Para un qubit en estado $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$:

$$p(0) = \langle\psi|M_0|\psi\rangle = |\alpha|^2$$
$$p(1) = \langle\psi|M_1|\psi\rangle = |\beta|^2$$

Normalización y Conservación

La conservación de probabilidad garantiza:

$$p(0) + p(1) = |\alpha|^2 + |\beta|^2 = 1$$

Probabilidad Intrínseca vs. Probabilidad por Ignorancia

Caso Clásico: Probabilidad Epistémica

- La aleatoriedad surge de **ignorancia** o información incompleta
- Ejemplo: Moneda clásica - resultado determinado por condiciones iniciales exactas
- En principio, **predicible** con información suficiente

Caso Cuántico: Probabilidad Ontológica

- La aleatoriedad es **intrínseca** y fundamental
- Ejemplo: Qubit en superposición $|\psi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$
- **No predecible** incluso con información completa del estado

Fundamentos Matemáticos del Qubit Estados Bases y Operadores Fundamentales

Representación Vectorial del Qubit

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \triangleq \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

Bases Ortogonales

Base Computacional:

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

Base Hadamard:

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

Operadores de Pauli Fundamentales

Identidad:

$$I \triangleq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Pauli-X:

$$X \triangleq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Pauli-Z:

$$Z \triangleq \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Operador General de Cambio de Base

Para transformar un sistema de una base ortonormal $B_v = \{|v_i\rangle\}$ a otra base ortonormal $B_w = \{|w_i\rangle\}$, se construye un operador unitario U que mapea cada vector de la base original a su correspondiente en la nueva base. La forma general de este operador es una suma de proyectores externos ("ket-bras"):

$$U = \sum_i |w_i\rangle \langle v_i|$$

Si aplicamos el operador U a un vector de la base original, por ejemplo $|v_j\rangle$:

$$\begin{aligned} U|v_j\rangle &= \left(\sum_i |w_i\rangle \langle v_i|\right)|v_j\rangle \\ &= \sum_i |w_i\rangle \left(\langle v_i|v_j\rangle\right) = \sum_i |w_i\rangle \delta_{ij} \\ &= |w_j\rangle \end{aligned}$$

El operador convierte exitosamente cada $|v_j\rangle$ en su correspondiente $|w_j\rangle$.

La Compuerta Hadamard: Creando Superposición

El Rol Fundamental de Hadamard (H)

La compuerta Hadamard es posiblemente la compuerta de un qubit más importante. Su principal función es tomar los estados de la base computacional (que son çlásicos", 0 o 1) y ponerlos en una **superposición equitativa**.

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

Esta capacidad de crear superposición a partir de estados definidos es el primer paso y el corazón de la mayoría de los algoritmos cuánticos, ya que permite el paralelismo cuántico.

Derivación de Hadamard como Cambio de Base

La matriz de Hadamard es simplemente el resultado de aplicar la fórmula del frame anterior para cambiar de la base $Z = \{|0\rangle, |1\rangle\}$ a la base $X = \{|+\rangle, |-\rangle\}$:

$$\begin{aligned} H &= |+\rangle\langle 0| + |-\rangle\langle 1| \\ &= \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|) \\ &= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \end{aligned}$$

Hadamard: Cambio de Base y Propiedad Inversa

Derivación como Cambio de Base

La matriz de Hadamard es el resultado de aplicar la fórmula de cambio de base para ir de la base $Z = \{|0\rangle, |1\rangle\}$ a la base $X = \{|+\rangle, |-\rangle\}$:

$$\begin{aligned} H &= |+\rangle\langle 0| + |-\rangle\langle 1| \\ &= \frac{1}{\sqrt{2}}\left(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|\right) \\ &= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \end{aligned}$$

Hadamard es su Propia Inversa ($H \cdot H = \mathbb{I}$)

Una propiedad fundamental de H es que si se aplica dos veces, deshace su propia operación. Esto se demuestra multiplicando la matriz por sí misma:

$$\begin{aligned} H \cdot H &= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbb{I} \end{aligned}$$

Tomografía: ¿Qué información nos falta?

La Limitación de Medir en una Sola Base

La medición en la base computacional (eje Z) con los proyectores $M_0 = |0\rangle\langle 0|$ y $M_1 = |1\rangle\langle 1|$ nos da las probabilidades $p(0) = |\alpha|^2$ y $p(1) = |\beta|^2$.

Esto solo nos informa sobre las **magnitudes** de las amplitudes, pero perdemos toda la información sobre la **fase relativa** entre α y β.

La Solución: Medir en Otras Bases

Para reconstruir el estado completo, necesitamos medir en bases que sean superposiciones de $|0\rangle$ y $|1\rangle$. Esto es análogo a necesitar vistas desde los ejes X e Y (además del Z) para ubicar un punto en una esfera.

Protocolo de Tomografía de un Qubit

Para determinar completamente α y β, realizamos tres conjuntos de mediciones sobre un gran número de copias idénticas del estado $|\psi\rangle$.

1. Medición en Base Z

- Mide directamente.
- Proyectores: $|0\rangle\langle 0|, |1\rangle\langle 1|$.
- Obtienes: $|\alpha|^2, |\beta|^2$.

2. Medición en Base X

- Aplica **Hadamard (H)** y luego mide.
- Proyectores: $|+\rangle\langle +|, |-\rangle\langle -|$.
- Obtienes: $\frac{|\alpha+\beta|^2}{2}, \frac{|\alpha-\beta|^2}{2}$.

3. Medición en Base Y

- Aplica $S^\dagger$ y **H**, y luego mide.
- Proyectores: $|i\rangle\langle i|, |-i\rangle\langle -i|$.
- Obtienes: $\frac{|\alpha+i\beta|^2}{2}, \frac{|\alpha-i\beta|^2}{2}$.

Reconstrucción del Estado

Al combinar las estadísticas de estas tres mediciones ortogonales, obtenemos un sistema de ecuaciones que nos permite resolver para las partes real e imaginaria de las amplitudes α y β.
Esto es equivalente a determinar los valores esperados $\langle\sigma_x\rangle, \langle\sigma_y\rangle, \langle\sigma_z\rangle$ y reconstruir la posición del estado en la **esfera de Bloch**.

Contenidos

¿Cómo describimos más de un qubit?

El Postulado del Sistema Compuesto

Si tenemos un sistema cuántico A cuyo espacio de estados es $\mathcal{H}_A$, y otro sistema B con espacio $\mathcal{H}_B$, el espacio de estados del sistema compuesto AB es el **producto tensorial** de sus espacios individuales.

$$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$$

- El operador $\otimes$ (producto tensorial) es la receta"matemática para combinar sistemas cuánticos.
- Si $|i\rangle_A$ es una base para el sistema A y $|a\rangle_B$ es una base para B, entonces los estados de la forma $|i\rangle_A \otimes |a\rangle_B$ forman una base para el sistema combinado AB.
- La dimensión del nuevo espacio es el producto de las dimensiones:

$$\dim(\mathcal{H}_{AB}) = \dim(\mathcal{H}_A) \times \dim(\mathcal{H}_B)$$

Ortogonalidad de la Base Tensorial

Recordatorio: La Base de un Sistema Compuesto

Si tenemos un sistema A con base ortonormal $\{|i\rangle_A\}$ y un sistema B con base ortonormal $\{|a\rangle_B\}$, la base del sistema compuesto AB está formada por todos los posibles productos tensoriales:

$$\text{Base}_{AB} = \{|i\rangle_A \otimes |a\rangle_B\}$$

Pero, ¿cómo sabemos que esta nueva base también es ortonormal?

Para responder calculamos el producto interno entre dos estados base cualesquiera del sistema compuesto,

$$|i\rangle \otimes |a\rangle$$

y

$$|j\rangle \otimes |b\rangle \, .$$

Ortogonalidad de la Base Tensorial 2

Producto Interno de Estados Base

La regla clave es que el producto interno "se distribuye- en el producto tensorial:

$$\begin{aligned}(\langle j| \otimes \langle b|)(|i\rangle \otimes |a\rangle) &= \langle j|i\rangle_A \cdot \langle b|a\rangle_B \\ &= \delta_{ij} \cdot \delta_{ab}\end{aligned}$$

- El término $\delta_{ij}\delta_{ab}$ es 1 **únicamente si** $i = j$ **y** $a = b$ (es decir, si es el mismo vector base).
- Si $i \neq j$ **o** $a \neq b$, el producto es 0.
- **Interpretación física:** Los estados base del sistema compuesto son perfectamente distinguibles (ortogonales) si sus componentes son distinguibles en *al menos uno* de los subsistemas.

Espionaje Cuántico: El Escenario de Alice y Eve

Alice prepara un qubit en uno de dos posibles estados, $|\phi\rangle_A$ o $|\psi\rangle_A$, y lo envía. Una espía, Eve, intercepta el qubit y quiere descubrir cuál de los dos estados es, pero con una condición crucial: **no debe alterar ni perturbar el estado original de Alice**.

La Estrategia de Eve

Eve utiliza una "sonda", que es otro qubit (un sistema auxiliar) inicializado en un estado conocido, $|0\rangle_E$. Luego, aplica una operación unitaria U al sistema combinado (Alice+Eve) diseñada para que el estado de Alice no cambie:

$$U(|\phi\rangle_A \otimes |0\rangle_E) = |\phi\rangle_A \otimes |e\rangle_E$$
$$U(|\psi\rangle_A \otimes |0\rangle_E) = |\psi\rangle_A \otimes |f\rangle_E$$

La esperanza de Eve es que los estados de su sonda, $|e\rangle_E$ y $|f\rangle_E$, sean diferentes para poder distinguirlos y así descubrir el estado de Alice.

El Límite Cuántico: Estados No Ortogonales

La física cuántica impone una regla fundamental: toda interacción sin medición debe ser unitaria, lo que significa que **conserva el producto interno**. Esto nos lleva a una ecuación que lo gobierna todo:

$$\langle \psi | \phi \rangle = \langle \psi | \phi \rangle \cdot \langle f | e \rangle$$

Caso 1: Los estados de Alice NO son ortogonales ($\langle \psi | \phi \rangle \neq 0$)

Si los estados que Alice envía tienen un solapamiento entre sí (no son ortogonales), la ecuación nos impone una restricción matemática ineludible.

Como $\langle \psi | \phi \rangle$ no es cero, podemos dividir ambos lados por este término, forzando la conclusión:

$$\langle f | e \rangle = 1$$

Interpretación: Esto significa que los estados $|e\rangle$ y $|f\rangle$ son físicamente idénticos. La sonda de Eve termina en el **mismo estado** sin importar qué envió Alice.

$\Longrightarrow$ **Eve no obtiene absolutamente ninguna información.**

La Excepción: Copiando Información Ortogonal

Nuevamente, partimos de la ecuación fundamental que nos da la conservación del producto interno:

$$\langle\psi|\phi\rangle = \langle\psi|\phi\rangle \cdot \langle f|e\rangle$$

Caso 2: Los estados de Alice SÍ son ortogonales ($\langle\psi|\phi\rangle = 0$) Este es el caso en el que Alice codifica información de manera análoga a los bits clásicos (como con los estados $|0\rangle$ y $|1\rangle$).

Al sustituir $\langle\psi|\phi\rangle = 0$ en la ecuación, obtenemos:

$$0 = 0 \cdot \langle f|e\rangle \implies 0 = 0$$

Interpretación: Esta ecuación es una tautología. Es siempre cierta, sin importar el valor de $\langle f|e\rangle$. Esto significa que la física cuántica **no impone ninguna restricción** sobre los estados finales de la sonda de Eve. **Eve tiene la libertad** de diseñar una interacción U (como una CNOT) que haga que sus estados sonda también sean ortogonales ($\langle f|e\rangle = 0$). Al medirlos, puede determinar con 100 % de certeza cuál estado envió Alice.

Producto tensorial aplicado al Sistema de Dos Qubits

Apliquemos el concepto a nuestro bloque fundamental: el qubit.

- El espacio de un solo qubit es $\mathbb{C}^2$, con la base computacional $\{|0\rangle, |1\rangle\}$.
- Para un sistema de dos qubits, el espacio es $\mathbb{C}^2 \otimes \mathbb{C}^2 \cong \mathbb{C}^4$.

La Base Computacional de 2 Qubits

Construimos la nueva base de 4 estados combinando las bases de cada qubit:

$$|0\rangle \otimes |0\rangle \equiv |00\rangle$$
$$|0\rangle \otimes |1\rangle \equiv |01\rangle$$
$$|1\rangle \otimes |0\rangle \equiv |10\rangle$$
$$|1\rangle \otimes |1\rangle \equiv |11\rangle$$

El conjunto $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ es la nueva **base computacional**. Estos estados son ortogonales entre sí.

De Dos a N Qubits: Crecimiento Exponencial

La verdadera potencia emerge cuando generalizamos el sistema.

El Espacio de Estados de N Qubits

El espacio de Hilbert para un sistema de n qubits es el producto tensorial de n espacios de un qubit:

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

- La dimensión del espacio de estados es $d = 2^n$. ¡Crece **exponencialmente** con el número de qubits!
- Un estado base se escribe como $|x\rangle$, donde x es una cadena de n bits clásicos, $x \in \{0, 1\}^n$:

$$|x\rangle \equiv |x_{n-1}x_{n-2}...x_0\rangle = |x_{n-1}\rangle \otimes |x_{n-2}\rangle \otimes \cdots \otimes |x_0\rangle$$

La Consecuencia: El Poder del Paralelismo Cuántico

Este crecimiento exponencial no es solo una curiosidad matemática, es la fuente del poder de la computación cuántica.

- Un estado cuántico general de n qubits es una superposición de **todos** los 2^n estados base:

$$|\psi\rangle = \sum_{x=0}^{2^n-1} a_x |x\rangle$$

- Para describir completamente este estado, ¡necesitamos especificar 2^n amplitudes complejas a_x!

300 qubits ya da un número impactante

- La dimensión del espacio de estados es $2^{300} \approx 10^{90}$. Este número es **mayor que el número estimado de átomos en el universo observable**.
- Es imposible almacenar el vector de estado de un sistema así en cualquier supercomputadora clásica, presente o futura.

No existe una descripción clásica sucinta para un estado cuántico general.

Producto Tensorial de Operadores: Forma Matricial

Regla General

Si un operador A (matriz $m \times m$) actúa sobre el primer sistema y un operador B (matriz $n \times n$) actúa sobre el segundo, el operador combinado $U = A \otimes B$ es una matriz $(mn) \times (mn)$ que tiene una estructura de bloques:

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \dots \\ a_{21}B & a_{22}B & \dots \\ \vdots & \vdots & \ddots \end{pmatrix}$$

Cada elemento a_{ij} de la matriz A se multiplica por la matriz completa B.

- Para dos operadores de un qubit (2×2), el resultado es una matriz 4×4.
- Esta matriz actúa sobre el vector de estado de 2 qubits (un vector de 4 componentes).

$$(A \otimes B)(|\psi\rangle \otimes |\phi\rangle) = (A|\psi\rangle) \otimes (B|\phi\rangle)$$

Ejemplo producto tensorial

Problema: Aplicar la compuerta H al qubit de la izquierda y la compuerta X al qubit de la derecha. El operador total sigue el orden de los qubits: $U_{total} = H \otimes X$.

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$U_{total} = H \otimes X = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \cdot X & 1 \cdot X \\ 1 \cdot X & -1 \cdot X \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix}$$

Esta es la matriz 4×4 que un simulador cuántico calcula y aplica al vector de estado del sistema.

Interpretación de la Matriz del Operador

- Cada **columna** representa la transformación de un estado base de **entrada**.
- Cada **fila** corresponde a la amplitud de un estado base en la **salida**.

$$U_{total} = H \otimes X = \frac{1}{\sqrt{2}} \begin{array}{c} \\ |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \begin{array}{c} \begin{array}{cccc} \langle 00| & \langle 01| & \langle 10| & \langle 11| \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix} \end{array}$$

Ejemplo de aplicacion a un estado

Para saber qué le pasa al estado de entrada $|01\rangle$, miramos la **segunda columna**:

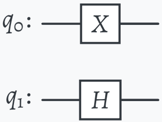
$$(H \otimes X)|01\rangle = \frac{1}{\sqrt{2}}(1|00\rangle + 0|01\rangle + 1|10\rangle + 0|11\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

Notación tensorial operadores en Qiskit

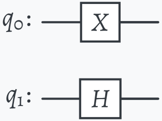
Convención de Qiskit

Qiskit ordena los qubits de izquierda a derecha segun los que aparecen desde abajo hacia arriba. Para un sistema de 2 qubits, el estado es $|q_1 q_0\rangle$.

- El **qubit 0** ($|q_0\rangle$) es el de la derecha o "de arriba".
- El **qubit 1** ($|q_1\rangle$) es el de la izquierda o "de abajo".



Representación Gráfica: Circuito Cuántico



- La línea inferior es el **qubit 1** (q_1), donde aplicamos la compuerta Hadamard (H).
- La línea inferior es el **qubit 0** (q_0), donde aplicamos la compuerta NOT (X).
- Este diagrama es la representación visual exacta del operador matricial que construimos:

$$U_{total} = H \otimes X$$

Estados Producto: Sistemas Separables

Definición

Un estado de un sistema compuesto es un **estado producto** si puede ser escrito como el producto tensorial de los estados de sus subsistemas. Para dos qubits A y B:

$$|\psi\rangle_{AB} = |\psi\rangle_A \otimes |\psi\rangle_B$$

- **Interpretación Física:** Cada subsistema tiene su propio estado bien definido, independiente de los otros. Las propiedades del sistema A pueden ser descritas *sin ninguna referencia* al sistema B, y viceversa.
- Un estado producto tiene una descripción clásica "sencilla". Para n qubits, solo se necesitan $2n$ parámetros reales para definirlo, en lugar de los $2^n - 1$ complejos de un estado general.
- Alice puede preparar su qubit en el estado $|\psi\rangle_A$ y Bob el suyo en $|\psi\rangle_B$ localmente. La descripción del sistema global es simplemente la combinación de estas partes independientes.

Entrelazamiento Cuántico (Entanglement)

Definición de Entrelazamiento

Un estado puro de un sistema compuesto que **no puede** ser escrito como un estado producto se denomina **estado entrelazado** (entangled).

- En un estado entrelazado, es **imposible** asignar un estado individual a cada subsistema. El sistema cuántico debe ser descrito como un todo.
- Las partes del sistema están intrínsecamente conectadas. Los resultados de medición en un subsistema están correlacionados con los resultados en el otro, sin importar cuán lejos estén.
- NOTAR QUE esta es una propiedad puramente cuántica, sin análogo en la física clásica.
- **Crucial:** El entrelazamiento no puede ser creado por partes que actúan localmente y se comunican por canales clásicos (LOCC - Local Operations and Classical Communication).

Test de Separabilidad para caso de dos qubits

Sea $|\psi\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle$ ¿Cómo sabemos si está entrelazado?

Hay entrelazamiento si $ad \neq bc$. Demostración

Partimos de un estado producto genérico $|\psi\rangle = |\alpha\rangle \otimes |\beta\rangle$, donde:

$$|\alpha\rangle = \alpha_0\,|0\rangle + \alpha_1\,|1\rangle \quad , \quad |\beta\rangle = \beta_0\,|0\rangle + \beta_1\,|1\rangle$$

Expandiendo el producto tensorial:

$$\begin{aligned} |\psi\rangle &= (\alpha_0\,|0\rangle + \alpha_1\,|1\rangle) \otimes (\beta_0\,|0\rangle + \beta_1\,|1\rangle) \\ &= \underbrace{(\alpha_0\beta_0)}_{a}\,|00\rangle + \underbrace{(\alpha_0\beta_1)}_{b}\,|01\rangle + \underbrace{(\alpha_1\beta_0)}_{c}\,|10\rangle + \underbrace{(\alpha_1\beta_1)}_{d}\,|11\rangle \end{aligned}$$

Ahora, comprobamos la condición con estos coeficientes:

- $a \cdot d = (\alpha_0\beta_0) \cdot (\alpha_1\beta_1) = \alpha_0\alpha_1\beta_0\beta_1$
- $b \cdot c = (\alpha_0\beta_1) \cdot (\alpha_1\beta_0) = \alpha_0\alpha_1\beta_0\beta_1$

Como ad y bc son idénticos, la condición de igualdad $ad = bc$ se cumple para cualquier estado producto **y de lo contrario** $|\psi\rangle$ **tiene entrelazamiento**.

Ejemplo: El estado de Bell $|\Phi^+\rangle$

Consideremos uno de los estados de Bell:

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

Sus coeficientes son: $a = \frac{1}{\sqrt{2}}, \quad b = 0, \quad c = 0, \quad d = \frac{1}{\sqrt{2}}$.

Aplicamos el test:

- $a \cdot d = \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} = \frac{1}{2}$
- $b \cdot c = 0 \cdot 0 = 0$

Como $\frac{1}{2} \neq 0$, la condición no se cumple. Por lo tanto, el estado $|\Phi^+\rangle$ **está entrelazado**.

El Teorema de No Clonación

Declaración del Teorema

Es **imposible** construir un dispositivo u operación universal que pueda crear una copia idéntica de un estado cuántico **arbitrario y desconocido**.

Este es un resultado fundamental que distingue la información cuántica de la clásica (que puede ser copiada libremente).

$$U(|\psi\rangle \otimes |b\rangle) = |\psi\rangle \otimes |\psi\rangle$$

No es posible

El Teorema de No Clonación

Demostración por Contradicción

1. **Hipótesis:** Existe operador unitario U tal que:

$$U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle \quad y \quad U(|\phi\rangle \otimes |0\rangle) = |\phi\rangle \otimes |\phi\rangle$$

2. **Probemos con superposición:** Sea $|\xi\rangle = \alpha|\psi\rangle + \beta|\phi\rangle$
Por linealidad de U:

$$\begin{aligned} U(|\xi\rangle \otimes |0\rangle) &= U[(\alpha|\psi\rangle + \beta|\phi\rangle) \otimes |0\rangle] \\ &= \alpha|\psi\rangle \otimes |\psi\rangle + \beta|\phi\rangle \otimes |\phi\rangle \end{aligned}$$

3. **¡Contradicción!** Si U fuera clonador debería dar:

$$|\xi\rangle \otimes |\xi\rangle = (\alpha|\psi\rangle + \beta|\phi\rangle) \otimes (\alpha|\psi\rangle + \beta|\phi\rangle)$$

$$= \alpha^2|\psi\psi\rangle + \alpha\beta|\psi\phi\rangle + \alpha\beta|\phi\psi\rangle + \beta^2|\phi\phi\rangle$$

4. **Los resultados son diferentes** a menos que $\alpha\beta = 0$ (no superposición).

Conclusión: La clonación es no-lineal, las unitarias son lineales → **INCOMPATIBLES**.

Contenidos

Próximos días continuaremos con:

- Estados entrelazados (Bell, GHZ)
- Desigualdad de CHSH
- Teleportación cuántica
- Criptografía cuántica (QKD)
- Deutsch-Jozsa, Simon
- Grover (búsqueda)
- Shor (factorización)
- Corrección de errores cuánticos *
- Machine learning cuántico **

IBM Qiskit - Composer

Recursos adicionales:

- Nielsen & Chuang: "Quantum Computation and Quantum Information"
- Popular info PREMIO NOBEL 2025 Physics (hoy) link
- IBM composer link