Compuertas de Múltiples Qubits

La Interacción Cuántica

La Necesidad de la Interacción: Compuertas Controladas

En la clase anterior vimos cómo aplicar compuertas de 1 qubit en paralelo $(H^{\otimes N})$, pero llegamos a una conclusión clave: estas operaciones **nunca pueden crear entrelazamiento**. Para para construir algoritmos complejos, necesitamos **interacción condicional**.

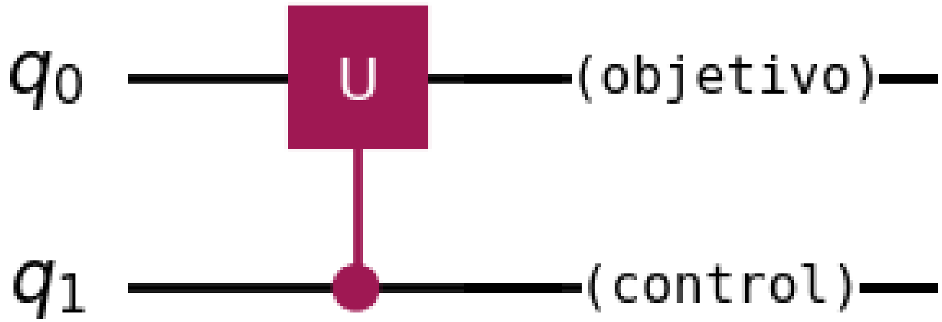
La Pregunta Clave:

> ¿Cómo podemos implementar una lógica del tipo ***if-then*** en una computadora cuántica? Es decir, "**Si** un qubit (el control) está en un estado específico, **entonces** aplica una compuerta (la operación) a otro qubit (el objetivo)"?

La solución es una **Compuerta Controlada-U** (CU), donde U es una operación unitaria.

Anatomía de una Compuerta Controlada

Diagrama de Circuito General:



- El punto (●) indica el qubit de control.
- El cuadro (U) es la operación unitaria que se aplica condicionalmente al qubit objetivo.

Anatomía de una Compuerta Controlada

Una compuerta controlada es una operación de múltiples qubits que se divide en dos roles:

1. **Qubit de Control:**
   - Este qubit actúa como el "interruptor" o la condición del ***if***.
   - Su estado **no se modifica** durante la operación.
   - La operación se activa (generalmente) solo si este qubit está en el estado $|1\rangle$.
2. **Qubit Objetivo (Target):**
   - Este es el qubit (o qubits) sobre el cual se aplica una operación unitaria $\hat{U}$.
   - La operación $\hat{U}$ se aplica **solo si** la condición del qubit de control se cumple.

La Lógica: Construyendo un Operador por "Casos"

Para construir la matriz de una compuerta controlada, podemos pensar en la **suma de todas las situaciones posibles**. Hay dos "casos" que definen la operación:

Caso A: "El qubit de control es $|0\rangle$".

- En esta situación, no queremos hacer nada en el qubit objetivo. La acción sobre el objetivo es la **Identidad ($\hat{I}$)**.

Caso B: "El qubit de control es $|1\rangle$".

- En esta situación, sí queremos actuar. La acción sobre el objetivo es la compuerta **Unitaria ($\hat{U}$)**.

El operador total CU debe ser una combinación que ejecute la acción correcta para cada caso. Para construirlo, usaremos los **operadores de proyección** como "filtros".

Usando Proyectores para "Filtrar" los Casos

¿Cómo podemos "filtrar" matemáticamente la parte de un estado que corresponde a cada caso? ¡Con los **operadores de proyección**!

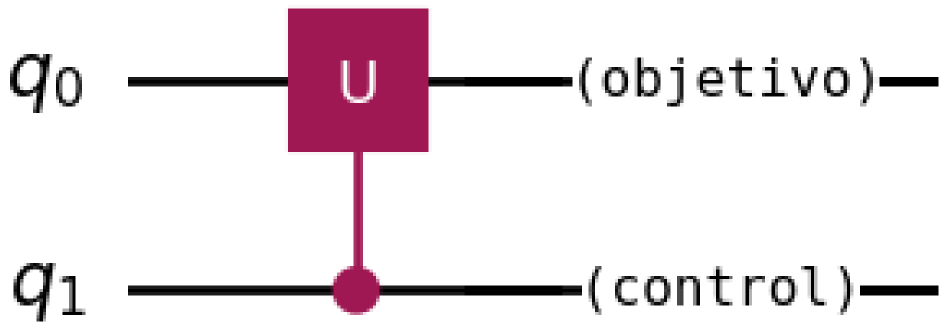
- El proyector $\hat{P}_0 = |0\rangle\langle 0|$ actúa como un filtro que selecciona solo la parte de un estado donde un qubit es $|0\rangle$.
- El proyector $\hat{P}_1 = |1\rangle\langle 1|$ selecciona solo la parte donde el qubit es $|1\rangle$.

Es decir que dado $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$:

- $\hat{P}_0|\psi\rangle = |0\rangle\langle 0|(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle$
- $\hat{P}_1|\psi\rangle = |1\rangle\langle 1|(\alpha|0\rangle + \beta|1\rangle) = \beta|1\rangle$

Ahora podemos traducir nuestra lógica de "casos" a una fórmula matemática precisa.

La Receta Universal: Control en q_1 (el más significativo)



La Lógica:

- **Caso A (q_1=0):** Aplica $\hat{P}_0$ al qubit q_1 y, simultáneamente (⊗), aplica $\hat{I}$ al qubit q_0. El operador para este caso es $\hat{P}_0 \otimes \hat{I}$.
- **Caso B (q_1=1):** Aplica $\hat{P}_1$ al qubit q_1 y, simultáneamente (⊗), aplica $\hat{U}$ al qubit q_0. El operador para este caso es $\hat{P}_1 \otimes \hat{U}$.

El operador total es la **suma** de los operadores de cada caso:

$$CU = (|0\rangle\langle 0|) \otimes \hat{I} + (|1\rangle\langle 1|) \otimes \hat{U}$$

Ejercicio: Probando la "Receta Universal" en la Base

Vamos a verificar que nuestra fórmula para la compuerta controlada implementa correctamente la lógica ***if-then***.

Problema:
Aplica el operador $CU = (|0\rangle\langle 0| \otimes \hat{I}) + (|1\rangle\langle 1| \otimes \hat{U})$ a los cuatro estados base y demuestra que los resultados coinciden con la lógica esperada:

- $CU|00\rangle \stackrel{?}{=} |00\rangle$
- $CU|01\rangle \stackrel{?}{=} |01\rangle$
- $CU|10\rangle \stackrel{?}{=} |1\rangle \otimes (U|0\rangle)$
- $CU|11\rangle \stackrel{?}{=} |1\rangle \otimes (U|1\rangle)$

Instrucción:
Para cada estado base (o al menos 2 casos, uno para cuando el qubit de control es 0 y otro para cuando el qubit de control es 1), aplica la suma de operadores y usa la linealidad. Recuerda cómo actúa un proyector: $\hat{P}_i|j\rangle$ es $|i\rangle$ si $i = j$ y $\vec{0}$ si $i \neq j$.

Solución (Caso A: El Qubit de Control es $|0\rangle$)

Apliquemos la fórmula completa a $|00\rangle$:

$$CU|00\rangle = \Big((|0\rangle\langle 0| \otimes \hat{I}) + (|1\rangle\langle 1| \otimes \hat{U}) \Big) |00\rangle$$

Por linealidad, distribuimos:

$$= \underbrace{(|0\rangle\langle 0| \otimes \hat{I})|00\rangle}_{\text{Término 1}} + \underbrace{(|1\rangle\langle 1| \otimes \hat{U})|00\rangle}_{\text{Término 2}}$$

- **Término 1:** El proyector $|0\rangle\langle 0|$ "activa" este término.

$$(|0\rangle\langle 0|0\rangle) \otimes (I|0\rangle) = (1 \cdot |0\rangle) \otimes |0\rangle = |00\rangle$$

- **Término 2:** El proyector $|1\rangle\langle 1|$ "anula" este término.

$$(|1\rangle\langle 1|0\rangle) \otimes (U|0\rangle) = (0 \cdot |1\rangle) \otimes (U|0\rangle) = \vec{0}$$

Resultado: $CU|00\rangle = |00\rangle + \vec{0} = |00\rangle$. ✅

> Un cálculo idéntico para $|01\rangle$ nos da como resultado $|01\rangle$. La receta funciona para el Caso A.

Solución (Caso B: El Qubit de Control es $|1\rangle$)

Ahora apliquemos la fórmula a $|10\rangle$:

$$CU|10\rangle = \Big((|0\rangle\langle 0| \otimes \hat{I}) + (|1\rangle\langle 1| \otimes \hat{U}) \Big)|10\rangle$$

$$= \underbrace{(|0\rangle\langle 0| \otimes \hat{I})|10\rangle}_{\text{Término 1}} + \underbrace{(|1\rangle\langle 1| \otimes \hat{U})|10\rangle}_{\text{Término 2}}$$

- **Término 1:** El proyector $|0\rangle\langle 0|$ "anula" este término.

$$(|0\rangle\langle 0|1\rangle) \otimes (I|0\rangle) = (0 \cdot |0\rangle) \otimes |0\rangle = \vec{0}$$

- **Término 2:** El proyector $|1\rangle\langle 1|$ "activa" este término.

$$(|1\rangle\langle 1|1\rangle) \otimes (U|0\rangle) = (1 \cdot |1\rangle) \otimes (U|0\rangle) = |1\rangle \otimes (U|0\rangle)$$

Resultado: $CU|10\rangle = \vec{0} + |1\rangle \otimes (U|0\rangle) = |1\rangle(U|0\rangle)$. ✅

> Un cálculo idéntico para $|11\rangle$ nos da como resultado $|1\rangle(U|1\rangle)$. La receta funciona para el Caso B.

Conclusión: ¡La Receta Funciona!

Hemos demostrado matemáticamente que la fórmula constructiva con proyectores implementa perfectamente la lógica condicional que define a una compuerta controlada.

Resumen de la Acción sobre la Base:

- **Para $|00\rangle$ (control en $|0\rangle$):** El estado no cambia: $CU|00\rangle = |00\rangle$
- **Para $|01\rangle$ (control en $|0\rangle$):** El estado no cambia: $CU|01\rangle = |01\rangle$
- **Para $|10\rangle$ (control en $|1\rangle$):** Se aplica U al objetivo: $CU|10\rangle = |1\rangle \otimes (U|0\rangle)$
- **Para $|11\rangle$ (control en $|1\rangle$):** Se aplica U al objetivo: $CU|11\rangle = |1\rangle \otimes (U|1\rangle)$

> Esta demostración nos muestra cómo la suma de los dos operadores proyectados $(P_0 \otimes I + P_1 \otimes U)$ actúa como un "interruptor" cuántico, eligiendo la operación correcta para cada parte de la superposición. Ahora podemos usar esta receta con total confianza.

Una Notación Precisa: Especificando Control y Objetivo

Para evitar ambigüedades, podemos usar subíndices para denotar qué qubit actúa como control y cuál como objetivo.

Notación General:

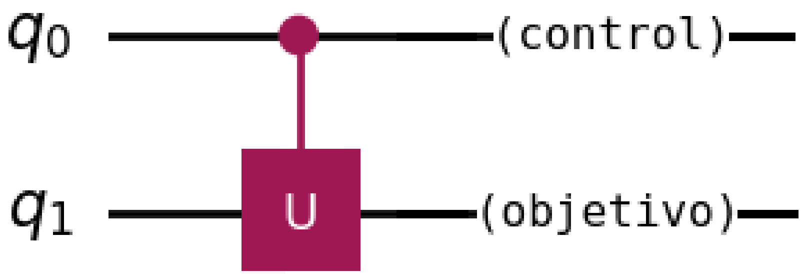
> La compuerta CU con el **qubit de control en el índice** i y el **qubit objetivo en el índice** j se escribe como:
>
> $$CU_{i,j}$$

- **Convención por Defecto:** Si no se especifican los subíndices, asumiremos la configuración más común: el control en el qubit de mayor índice (q_1) y el objetivo en el de menor índice (q_0).

$$CU \equiv CU_{1,0}$$

> **NOTA:** Desafortunadamente no hay un consenso universalmente aceptado sobre la manera de denotar el control y el destino en las compuertas controladas

La Receta para $CU_{0,1}$ (Control en q_0)



La Lógica (se invierte el orden en el producto tensorial):

- **Caso A (q_0=0):** Aplica $\hat{I}$ a q_1 y $\hat{P}_0$ a q_0. El operador es $\hat{I} \otimes |0\rangle\langle 0|$.
- **Caso B (q_0=1):** Aplica $\hat{U}$ a q_1 y $\hat{P}_1$ a q_0. El operador es $\hat{U} \otimes |1\rangle\langle 1|$.

El operador total es la **suma**:

$$CU_{0,1} = \hat{I} \otimes |0\rangle\langle 0| + \hat{U} \otimes |1\rangle\langle 1|$$

> Las fórmulas de $CU_{1,0}$ y $CU_{0,1}$ son la **receta universal** para construir la matriz de cualquier compuerta controlada de 2 qubits. La única diferencia es el orden de los operadores en el producto tensorial.

Ejercicio: Verificando la Receta Invertida

Ahora, vamos a verificar que la fórmula para una compuerta con el **control en** q_0 también funciona como se espera.

Problema:

Aplica el operador $CU_{0,1} = (\hat{I} \otimes |0\rangle\langle 0|) + (\hat{U} \otimes |1\rangle\langle 1|)$ a los cuatro estados base. Demuestra que la compuerta U solo se aplica cuando el qubit de control q_0 es $|1\rangle$.

Verifica que se cumplen las siguientes igualdades:

- $CU_{0,1}|00\rangle \stackrel{?}{=} |00\rangle$
- $CU_{0,1}|10\rangle \stackrel{?}{=} |10\rangle$
- $CU_{0,1}|01\rangle \stackrel{?}{=} (U|0\rangle) \otimes |1\rangle$
- $CU_{0,1}|11\rangle \stackrel{?}{=} (U|1\rangle) \otimes |1\rangle$

Solución (Caso A: El Qubit de Control q_0 es $|0\rangle$)

Apliquemos la fórmula completa a $|00\rangle$:

$$CU_{0,1}|00\rangle = \Big((\hat{I} \otimes |0\rangle\langle 0|) + (\hat{U} \otimes |1\rangle\langle 1|)\Big)|00\rangle$$

$$= \underbrace{(\hat{I} \otimes |0\rangle\langle 0|)|00\rangle}_{\text{Término 1}} + \underbrace{(\hat{U} \otimes |1\rangle\langle 1|)|00\rangle}_{\text{Término 2}}$$

- **Término 1:** El proyector $|0\rangle\langle 0|$ en el segundo qubit "activa" este término.

$$(I|0\rangle) \otimes (|0\rangle\langle 0|0\rangle) = |0\rangle \otimes (1 \cdot |0\rangle) = |00\rangle$$

- **Término 2:** El proyector $|1\rangle\langle 1|$ en el segundo qubit "anula" este término.

$$(U|0\rangle) \otimes (|1\rangle\langle 1|0\rangle) = (U|0\rangle) \otimes (0 \cdot |1\rangle) = \vec{0}$$

Resultado: $CU_{0,1}|00\rangle = |00\rangle + \vec{0} = |00\rangle$. ✅

> Un cálculo idéntico para $|10\rangle$ nos da como resultado $|10\rangle$. La receta funciona cuando el control es $|0\rangle$.

Solución (Caso B: El Qubit de Control q_0 es $|1\rangle$)

Ahora apliquemos la fórmula a $|01\rangle$:

$$CU_{0,1}|01\rangle = \Big((\hat{I} \otimes |0\rangle\langle 0|) + (\hat{U} \otimes |1\rangle\langle 1|)\Big)|01\rangle$$

$$= \underbrace{(\hat{I} \otimes |0\rangle\langle 0|)|01\rangle}_{\text{Término 1}} + \underbrace{(\hat{U} \otimes |1\rangle\langle 1|)|01\rangle}_{\text{Término 2}}$$

- **Término 1:** El proyector $|0\rangle\langle 0|$ "anula" este término.

$$(I|0\rangle) \otimes (|0\rangle\langle 0|1\rangle) = |0\rangle \otimes (0 \cdot |0\rangle) = \vec{0}$$

- **Término 2:** El proyector $|1\rangle\langle 1|$ "activa" este término.

$$(U|0\rangle) \otimes (|1\rangle\langle 1|1\rangle) = (U|0\rangle) \otimes (1 \cdot |1\rangle) = (U|0\rangle) \otimes |1\rangle$$

Resultado: $CU_{0,1}|01\rangle = \vec{0} + (U|0\rangle) \otimes |1\rangle$. ✅

> Un cálculo idéntico para $|11\rangle$ nos da como resultado $(U|1\rangle) \otimes |1\rangle$. ¡La receta funciona perfectamente!

Compuertas Controladas Fundamentales

La Compuerta Controlada-NOT (CNOT)

Ahora aplicaremos nuestra "receta universal" para construir la compuerta de dos qubits más famosa: la **Compuerta Controlada-NOT**, también conocida como **CNOT** o **CX**.

La Lógica de la CNOT:

> Es una compuerta Controlada-U donde la operación unitaria $\hat{U}$ es la compuerta **Pauli-X (NOT)**.
> Su lógica es: "**Si** el qubit de control es $|1\rangle$, **entonces** aplica una compuerta NOT ($\hat{X}$) al qubit objetivo."

Acción sobre la Base Computacional (Control en q_1, Objetivo en q_0):

- CNOT $|00\rangle \rightarrow |00\rangle$ *(Control es 0, no pasa nada)*
- CNOT $|01\rangle \rightarrow |01\rangle$ *(Control es 0, no pasa nada)*
- CNOT $|10\rangle \rightarrow |11\rangle$ *(Control es 1, se aplica X a $|0\rangle \rightarrow |1\rangle$)*
- CNOT $|11\rangle \rightarrow |10\rangle$ *(Control es 1, se aplica X a $|1\rangle \rightarrow |0\rangle$)*

La Fórmula Constructiva de la CNOT

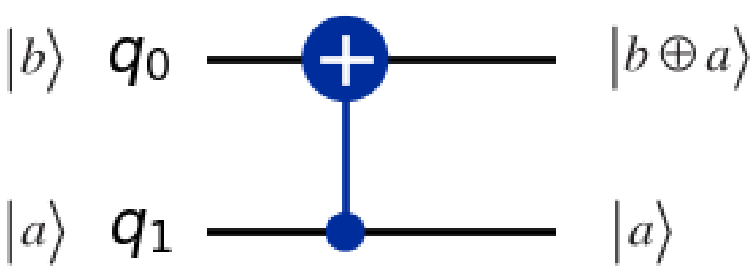
Usando nuestra receta $CU = |0\rangle\langle 0| \otimes \hat{I} + |1\rangle\langle 1| \otimes \hat{U}$ y sustituyendo $\hat{U}$ por $\hat{X}$, obtenemos la fórmula para la CNOT.

Fórmula (Control en q_1, Objetivo en q_0):

$$\mathrm{CNOT} = |0\rangle\langle 0| \otimes \hat{I} + |1\rangle\langle 1| \otimes \hat{X}$$

Diagrama de Circuito:

El símbolo para la compuerta X en el objetivo es un $\oplus$ (que representa la suma modular o XOR, ya que $b \to b \oplus a$ si a es el control).



$$|a, b\rangle \to |a, b \oplus a\rangle$$

Ejercicio: Construyendo la Matriz CNOT (Control en q_1)

Problema:

Usa la fórmula constructiva para derivar la matriz de 4×4 para la compuerta CNOT con **control en q_1 y objetivo en q_0**.

Fórmula: $\text{CNOT} = |0\rangle\langle 0| \otimes \hat{I} + |1\rangle\langle 1| \otimes \hat{X}$

Instrucción:

1. Calcula la matriz para el primer término, $|0\rangle\langle 0| \otimes \hat{I}$.
2. Calcula la matriz para el segundo término, $|1\rangle\langle 1| \otimes \hat{X}$.
3. Suma las dos matrices resultantes.

Solución (Control en q_1)

1. Primer Término ("Control es 0"):

$$|0\rangle\langle 0| \otimes \hat{I} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 \cdot I & 0 \cdot I \\ 0 \cdot I & 0 \cdot I \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

2. Segundo Término ("Control es 1"):

$$|1\rangle\langle 1| \otimes \hat{X} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 \cdot X & 0 \cdot X \\ 0 \cdot X & 1 \cdot X \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

3. Suma Final:

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

Verificando la Acción de la Matriz CNOT

Vamos a comprobar que la matriz que hemos construido hace lo que dice la tabla de verdad.

- **CNOT** $|00\rangle$:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |00\rangle$$

- **CNOT** $|01\rangle$:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |01\rangle$$

Verificando la Acción de la Matriz CNOT (Continuación)

- **CNOT**$|10\rangle$:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |11\rangle$$

- **CNOT**$|11\rangle$:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |10\rangle$$

¡Correcto! La matriz funciona como se esperaba.

Ejercicio: Invirtiendo los Roles (Control en q_0)

Problema:

Deriva la matriz para la $\mathrm{CNOT}_{0,1}$ con **control en** q_0 **y objetivo en** q_1.

Fórmula (orden invertido):

$$\mathrm{CNOT}_{0,1} = \hat{I} \otimes |0\rangle\langle 0| + \hat{X} \otimes |1\rangle\langle 1|$$

Instrucción:

Repite el mismo procedimiento de cálculo y suma.

Solución (Control en q_0)

1. Primer Término ("Control es 0"):

$$\hat{I} \otimes |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 \cdot P_0 & 0 \cdot P_0 \\ 0 \cdot P_0 & 1 \cdot P_0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

2. Segundo Término ("Control es 1"):

$$\hat{X} \otimes |1\rangle\langle 1| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 \cdot P_1 & 1 \cdot P_1 \\ 1 \cdot P_1 & 0 \cdot P_1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

3. Suma Final:

$$\mathrm{CNOT}_{0,1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

> ¡Observa que la matriz es diferente! El orden del control y el objetivo es crucial y resulta en una operación completamente distinta.

Ejercicio: La CNOT es una Compuerta Válida

Hemos establecido que toda evolución cuántica (toda compuerta) debe ser descrita por un **operador unitario**. Ahora que hemos construido la matriz para la CNOT, debemos verificar que cumple esta condición fundamental.

Problema:
Demuestra que la compuerta CNOT (con control en q_1) es unitaria.

Matriz a Verificar:

$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Instrucción:
Utiliza la definición formal de un operador unitario que hemos estudiado:

$$U^\dagger U = I$$

Para ello, primero calcula el adjunto hermitiano ($\mathrm{CNOT}^\dagger$) y luego realiza la multiplicación de matrices.

Solución: Usando la Definición Formal $U^\dagger U = I$

Vamos a seguir los pasos de la definición formal para demostrar que CNOT es unitaria.

Paso 1: Calcular el adjunto hermitiano ($\text{CNOT}^\dagger$).
La operación de adjunto hermitiano (†) consiste en transponer y luego conjugar. Como la matriz CNOT es real, la conjugación no tiene efecto. Por lo tanto, solo necesitamos calcular su transpuesta.

$$\text{CNOT}^T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}^T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Observamos que la matriz CNOT es **simétrica**, es decir, es igual a su propia transpuesta. Por lo tanto:

$$\text{CNOT}^\dagger = \text{CNOT}$$

Solución (Continuación):

Paso 2: Calcular el producto $\mathrm{CNOT}^\dagger \mathrm{CNOT}$.

Ahora que sabemos que $\mathrm{CNOT}^\dagger = \mathrm{CNOT}$, la expresión a calcular se convierte en $\mathrm{CNOT} \cdot \mathrm{CNOT}$.

$$\mathrm{CNOT}^\dagger \mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Podemos usar la estructura de bloques $\begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix}$ para simplificar el cálculo:

$$= \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix} \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix} = \begin{pmatrix} I \cdot I & 0 \\ 0 & X \cdot X \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & X^2 \end{pmatrix}$$

Como $X^2 = I$, el resultado es:

$$= \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = I_{4\times 4}$$

Solución (Final):

Paso 3: Conclusión Final.

Hemos calculado explícitamente el producto $\mathrm{CNOT}^{\dagger}\mathrm{CNOT}$ y el resultado es la matriz Identidad de 4×4.

$$\mathrm{CNOT}^{\dagger}\mathrm{CNOT} = I$$

Esto satisface la definición formal de un operador unitario.

> ✅ Hemos demostrado que la CNOT es una compuerta cuántica válida.

Una Perspectiva Diferente: El Efecto en el Vector de Estado

Hemos derivado las matrices para las dos versiones de la CNOT. Ahora, en lugar de pensar en la lógica condicional, analicemos directamente su **efecto sobre las amplitudes** de un estado general de 2 qubits.

Sea un estado arbitrario $|\Psi\rangle$:

$$|\Psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle = \begin{pmatrix} c_{00} \\ c_{01} \\ c_{10} \\ c_{11} \end{pmatrix}$$

¿Qué le hace exactamente la CNOT a este vector de amplitudes?

CNOT con Control en q_1 (el de abajo)

Matriz: $\mathrm{CNOT}_{1,0} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

Acción sobre el Vector de Amplitudes:

$$\mathrm{CNOT}_{1,0} \begin{pmatrix} c_{00} \\ c_{01} \\ c_{10} \\ c_{11} \end{pmatrix} = \begin{pmatrix} c_{00} \\ c_{01} \\ \boldsymbol{c_{11}} \\ \boldsymbol{c_{10}} \end{pmatrix}$$

La Regla de Permutación:

> La CNOT con control en q_1 **intercambia** las amplitudes de los estados base $|10\rangle$ y $|11\rangle$.
>
> Intuitivamente: "Cuando el primer qubit (q_1) es '1', se intercambian las amplitudes del segundo qubit (q_0)."

CNOT con Control en q_0 (el de arriba)

Matriz: $$\text{CNOT}_{0,1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Acción sobre el Vector de Amplitudes:

$$\text{CNOT}_{0,1} \begin{pmatrix} c_{00} \\ c_{01} \\ c_{10} \\ c_{11} \end{pmatrix} = \begin{pmatrix} c_{00} \\ \boldsymbol{c_{11}} \\ c_{10} \\ \boldsymbol{c_{01}} \end{pmatrix}$$

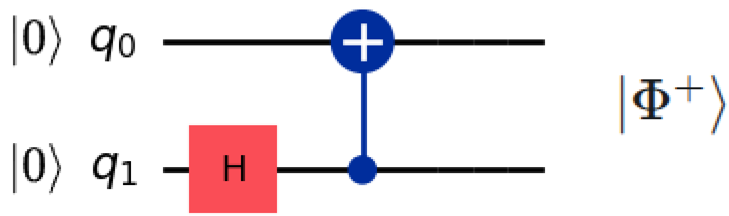
La Regla de Permutación:

> La CNOT con control en q_0 **intercambia** las amplitudes de los estados base $|01\rangle$ y $|11\rangle$.
>
> Intuitivamente: "Cuando el segundo qubit (q_0) es '1', se intercambian las amplitudes del primer qubit (q_1)."

La Magia de la CNOT: Creando Entrelazamiento

La CNOT es la compuerta de entrelazamiento por excelencia. Por sí sola, si se aplica a estados base, solo permuta los estados base. Pero si el **qubit de control está en superposición**, ocurre la magia.

El Circuito Creador de Estados de Bell:



1. **Estado Inicial:** $|\psi_0\rangle = |00\rangle$.
2. **Aplicar H a q_1:** $|\psi_1\rangle = (H \otimes I)|00\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$.
3. **Aplicar CNOT (control q_1):** $|\psi_2\rangle = \text{CNOT}|\psi_1\rangle = \frac{1}{\sqrt{2}}(\text{CNOT}|00\rangle + \text{CNOT}|10\rangle)$.

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

> La CNOT ha "copiado" la superposición del control al objetivo, creando un estado máximamente entrelazado.

Una Herramienta Mental

Si recordamos la perspectiva del intercambio de las amplitudes que hace la CNOT en el vector de estado global podemos ver que:

$$(H \otimes I)|00\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\1\\0\end{pmatrix}$$

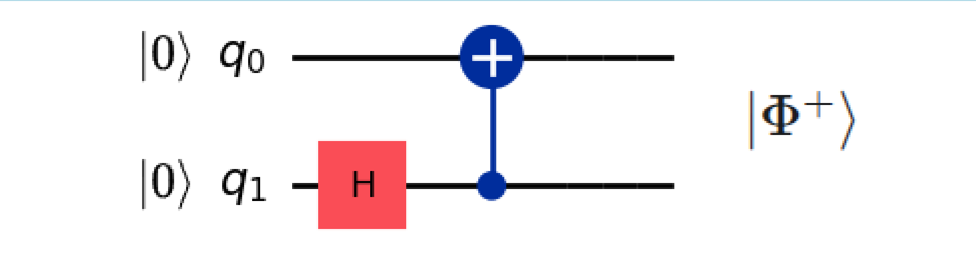
Aplicar $\mathrm{CNOT}_{1,0}$ (Control en q_1): implica intercambiar la 3ª y 4ª amplitud (c_{10} y c_{11}). Por lo tanto será igual a:

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\\mathbf{0}\\\mathbf{1}\end{pmatrix} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Phi^+\rangle$$

> Este método nos permite "ver" directamente cómo la CNOT transforma un estado separable en uno entrelazado, reorganizando las amplitudes de su vector de estado.

Ejercicio: La "Fábrica" de Estados de Bell

Hemos visto que el circuito H-CNOT transforma $|00\rangle$ en el estado de Bell $|\Phi^+\rangle$. Pero, ¿qué sucede si partimos de los otros tres estados de la base computacional?



Problema:

Calcula algebraicamente el estado final que produce este circuito para cada uno de los siguientes estados iniciales:

1. $|\psi_{inicial}\rangle = |01\rangle$
2. $|\psi_{inicial}\rangle = |10\rangle$
3. $|\psi_{inicial}\rangle = |11\rangle$

> **Pista:** Sigue el mismo proceso de dos pasos: primero aplica $H \otimes I$, y luego aplica CNOT al resultado intermedio.

Solución: La Fábrica de Estados de Bell

Vamos a analizar cada caso por separado. El operador total del circuito es $\hat{U} = \text{CNOT} \cdot (H \otimes I)$.

1. Estado Inicial: $|01\rangle$

- **Paso 1 (Aplicar H a q_1):**

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

- **Paso 2 (Aplicar CNOT):**

$$\text{CNOT}\left(\frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)\right) = \frac{1}{\sqrt{2}}(\text{CNOT}|01\rangle + \text{CNOT}|11\rangle)$$
$$= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = |\Psi^+\rangle$$

Solución (Continuación)

2. Estado Inicial: $|10\rangle$

- **Paso 1 (Aplicar H a q_1):**

$$(H \otimes I)|10\rangle = (H|1\rangle) \otimes (I|0\rangle) = |-\rangle|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle)$$

- **Paso 2 (Aplicar CNOT):**

$$\mathrm{CNOT}\left(\frac{1}{\sqrt{2}}(|00\rangle - |10\rangle)\right) = \frac{1}{\sqrt{2}}(\mathrm{CNOT}|00\rangle - \mathrm{CNOT}|10\rangle)$$

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

Solución (Final)

3. Estado Inicial: $|11\rangle$

- **Paso 1 (Aplicar H a q_1):**

$$(H \otimes I)|11\rangle = (H|1\rangle) \otimes (I|1\rangle) = |-\rangle|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|1\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle)$$

- **Paso 2 (Aplicar CNOT):**

$$\mathrm{CNOT}\left(\frac{1}{\sqrt{2}}(|01\rangle - |11\rangle)\right) = \frac{1}{\sqrt{2}}(\mathrm{CNOT}|01\rangle - \mathrm{CNOT}|11\rangle)$$

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

Resumen: La Transformación a la Base de Bell

Este simple circuito de dos compuertas realiza una transformación de base extraordinariamente importante.

El circuito H-CNOT mapea la Base Computacional a la Base de Bell:

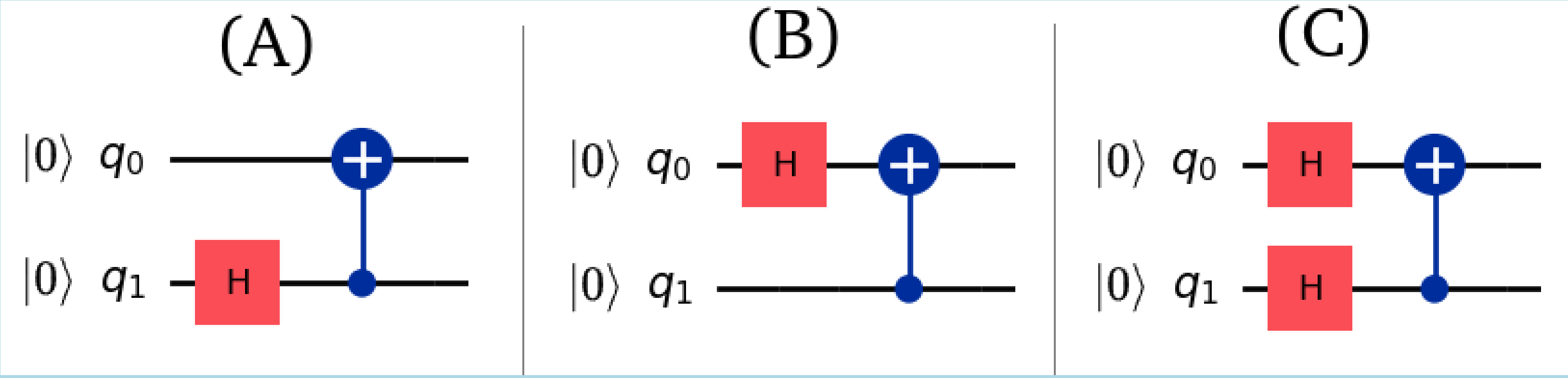
- $|00\rangle \xrightarrow{\text{H-CNOT}} |\Phi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$
- $|01\rangle \xrightarrow{\text{H-CNOT}} |\Psi^+\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}}$
- $|10\rangle \xrightarrow{\text{H-CNOT}} |\Phi^-\rangle = \frac{|00\rangle-|11\rangle}{\sqrt{2}}$
- $|11\rangle \xrightarrow{\text{H-CNOT}} |\Psi^-\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}$

> Como la operación es unitaria, también es reversible. Aplicando el **circuito inverso** se puede transformar la Base de Bell de vuelta a la Base Computacional. Esta transformación es la piedra angular de muchos algoritmos cuánticos, incluyendo la teleportación y la codificación superdensa.

Ejercicio: La Receta Precisa para el Entrelazamiento

Sabemos que el circuito **(A)** con una Hadamard en el qubit de control (q_1) crea un estado de Bell. Pero, ¿Qué pasaría si pusiéramos la Hadamard en otro lugar?

Problema:
Analiza por qué los casos **(B)** y **(C)** no logran crear entrelazamiento partiendo del estado $|00\rangle$.



Instrucción:

1. **Circuito (B):** Calcula el estado final al aplicar primero $I \otimes H$ y luego CNOT.
2. **Circuito (C):** Calcula el estado final al aplicar primero $H \otimes H$ y luego CNOT.
3. Para cada resultado, usa el **Test de Separabilidad** ($c_{00}c_{11} = c_{01}c_{10}$) para demostrar formalmente que el estado final es separable.

Solución (Caso B): Hadamard en el Qubit Objetivo

1. Estado Inicial: $|\psi_0\rangle = |00\rangle$

2. Paso 1 (Aplicar $I \otimes H$):

$$|\psi_1\rangle = (I \otimes H)|00\rangle = (I|0\rangle) \otimes (H|0\rangle) = |0\rangle \otimes |+\rangle$$

Expandiendo el estado intermedio:

$$|\psi_1\rangle = |0\rangle \otimes \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$$

3. Paso 2 (Aplicar CNOT):

$$|\psi_f\rangle = \mathrm{CNOT}|\psi_1\rangle = \mathrm{CNOT}\left(\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)\right)$$

$$= \frac{1}{\sqrt{2}}(\mathrm{CNOT}|00\rangle + \mathrm{CNOT}|01\rangle)$$

En ambos términos, el qubit de control (q_1) es $|0\rangle$, por lo que la CNOT no hace nada:

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

Solución (Caso B): Análisis

Estado Final:

$$|\psi_f\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$$

Análisis de Separabilidad:

1. **Por Factorización:** Podemos sacar $|0\rangle$ como factor común a la izquierda:

$$|\psi_f\rangle = |0\rangle \otimes \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = |0\rangle|+\rangle$$

   Como se puede escribir como un producto tensorial, el estado es **separable**.

2. **Por el Test Formal:**
   - Amplitudes: $c_{00} = \frac{1}{\sqrt{2}}, c_{01} = \frac{1}{\sqrt{2}}, c_{10} = 0, c_{11} = 0.$
   - Test: $c_{00}c_{11} \stackrel{?}{=} c_{01}c_{10} \implies (\frac{1}{\sqrt{2}})(0) \stackrel{?}{=} (\frac{1}{\sqrt{2}})(0) \implies 0 = 0.$
   - El test se cumple, confirmando que el estado es **separable**.

> **Conclusión:** Poner la superposición en el qubit objetivo no funciona. Como el qubit de control se mantiene en $|0\rangle$, la CNOT nunca se "activa" para crear las correlaciones cuánticas.

Solución (Caso C): Hadamard en Ambos Qubits

1. Estado Inicial: $|\psi_0\rangle = |00\rangle$

2. Paso 1 (Aplicar $H \otimes H$):

$$|\psi_1\rangle = (H \otimes H)|00\rangle = (H|0\rangle) \otimes (H|0\rangle) = |+\rangle \otimes |+\rangle$$

Expandiendo el estado intermedio:

$$|\psi_1\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

3. Paso 2 (Aplicar CNOT):

$$|\psi_f\rangle = \mathrm{CNOT}|\psi_1\rangle = \frac{1}{2}(\mathrm{CNOT}|00\rangle + \mathrm{CNOT}|01\rangle + \mathrm{CNOT}|10\rangle + \mathrm{CNOT}|11\rangle)$$

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

Solución (Caso C): Análisis

Estado Final:

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

¡El estado final es idéntico al estado intermedio!

Análisis de Separabilidad:

1. **Por Factorización:** Ya sabemos que este estado es la superposición uniforme, que se factoriza como:

   $$|\psi_f\rangle = |+\rangle \otimes |+\rangle$$

   Por lo tanto, es **separable**.

2. **Por el Test Formal:**
   - Amplitudes: $c_{00} = c_{01} = c_{10} = c_{11} = \frac{1}{2}$.
   - Test: $c_{00}c_{11} \stackrel{?}{=} c_{01}c_{10} \implies (\frac{1}{2})(\frac{1}{2}) \stackrel{?}{=} (\frac{1}{2})(\frac{1}{2}) \implies \frac{1}{4} = \frac{1}{4}$.
   - El test se cumple, confirmando que el estado es **separable**.

> **Conclusión:** Poner ambos qubits en superposición tampoco funciona. La CNOT simplemente permuta los estados $|10\rangle$ y $|11\rangle$, pero como ambos tienen la misma amplitud en la superposición $|++\rangle$, la permutación es invisible y el estado no cambia.

Conclusión Final del Ejercicio

Este ejercicio demuestra que la creación de entrelazamiento con el circuito H-CNOT es un proceso muy específico y delicado.

- **H en el control (Funciona):**

$$|00\rangle \to \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad \text{(Entrelazado)}$$

- **H en el objetivo (Falla):**

$$|00\rangle \to \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) \quad \text{(Separable)}$$

- **H en ambos (Falla):**

$$|00\rangle \to |++\rangle \xrightarrow{\text{CNOT}} |++\rangle \quad \text{(Separable)}$$

> **La Lección Clave:** Para que la CNOT cree entrelazamiento, el qubit de **control** debe estar en superposición. Esto permite que la compuerta actúe de forma "condicional" sobre diferentes partes de la superposición simultáneamente, "copiando" la superposición del control al objetivo y tejiendo así las correlaciones cuánticas que definen el entrelazamiento.

Compuertas Controladas Importantes

La CNOT no es la única compuerta controlada. Podemos crear una a partir de cualquier compuerta unitaria de 1 qubit. Dos de las más importantes son la **Controlada-Z (CZ)** y la **Controlada-Y (CY)**.

En esta sección, nos enfocaremos en la **Compuerta Controlada-Z**, una compuerta con propiedades de simetría muy especiales.

La Lógica de la CZ:

> "Observa el qubit de control. Si es $|1\rangle$, aplica una compuerta Z (Phase-Flip) al qubit objetivo."

La Compuerta Controlada-Z (CZ)

Acción sobre la Base Computacional (el control en q_1 y el objetivo en q_0):

- CZ $|00\rangle \rightarrow |00\rangle$ *(Control es 0, no pasa nada)*
- CZ $|01\rangle \rightarrow |01\rangle$ *(Control es 0, no pasa nada)*
- CZ $|10\rangle \rightarrow |10\rangle$ *(Control es 1, se aplica Z a $|0\rangle \rightarrow |0\rangle$)*
- CZ $|11\rangle \rightarrow -|11\rangle$ *(Control es 1, se aplica Z a $|1\rangle \rightarrow -|1\rangle$)*

La Única Acción: La compuerta CZ solo tiene un efecto visible: aplica una fase de -1 (un "phase flip") al estado $|11\rangle$.

Una Nota Importante: Fases Globales y Productos Tensoriales

Una pregunta común es: ¿el estado $|1\rangle \otimes (-|1\rangle)$ es lo mismo que $-|11\rangle$?
La respuesta es SÍ.

La Regla Clave (Bilinealidad):
Recordemos que los escalares pueden "flotar libremente" fuera del producto tensorial.

$$|\phi\rangle \otimes (\alpha|\psi\rangle) = \alpha(|\phi\rangle \otimes |\psi\rangle)$$

Aplicando la Regla:
El estado $-|1\rangle$ es simplemente el escalar -1 multiplicado por el vector $|1\rangle$.

$$|1\rangle \otimes (-|1\rangle) = |1\rangle \otimes ((-1) \cdot |1\rangle)$$

Sacamos el escalar -1 fuera de toda la expresión:

$$= (-1) \cdot (|1\rangle \otimes |1\rangle)$$

Y usamos la notación abreviada:

$$= -|11\rangle$$

Ejercicio: Construyendo la Matriz CZ

Problema:

Usa la fórmula constructiva para derivar la matriz de 4×4 para la compuerta CZ con **control en q_1 y objetivo en q_0**.

Fórmula (Receta Universal con U=Z):

$$CZ = |0\rangle\langle 0| \otimes \hat{I} + |1\rangle\langle 1| \otimes \hat{Z}$$

Datos:

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

Solución: Matriz de la Compuerta CZ

1. Primer Término ("Control es 0"):

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

2. Segundo Término ("Control es 1"):

$$|1\rangle\langle 1| \otimes \hat{Z} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

3. Suma Final:

$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

> La matriz es una matriz diagonal con un -1 en la última posición, reflejando que solo actúa sobre el estado $|11\rangle$.

La Simetría de la Compuerta CZ

A diferencia de la CNOT, la compuerta CZ es **simétrica**. ¡El qubit de control y el objetivo son intercambiables!

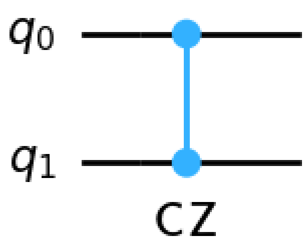
Vamos a demostrarlo calculando la matriz para una CZ con control en q_0 ($CZ_{0,1}$):

$$CZ_{0,1} = \hat{I} \otimes |0\rangle\langle 0| + \hat{Z} \otimes |1\rangle\langle 1|$$

$$= \begin{pmatrix} 1 \cdot P_0 & 0 \\ 0 & 1 \cdot P_0 \end{pmatrix} + \begin{pmatrix} 1 \cdot P_1 & 0 \\ 0 & -1 \cdot P_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

¡Obtenemos exactamente la **misma matriz**!

> **Conclusión:** Como $CZ_{1,0} = CZ_{0,1}$, la compuerta no tiene un "control" y un "objetivo" definidos. Es una operación simétrica. **Precisamente por esta razón**, su símbolo en un circuito cuántico es simétrico, con dos puntos de control.



De los Ejemplos a la Plantilla General

Hemos trabajado arduamente para construir las matrices para CNOT y CZ usando la "receta universal" de proyectores.

Ahora, vamos a dar un paso atrás y analizar el **patrón estructural** que estas matrices tienen en común.

> Al estudiar la acción de una compuerta CU genérica sobre los estados base, podemos derivar una **plantilla** o **forma de bloques** que nos permitirá construir la matriz para *cualquier* compuerta controlada de forma mucho más rápida y visual.

La Matriz General de una Compuerta $CU_{1,0}$

Podemos derivar una matriz "plantilla" para cualquier compuerta CU con control en q_1.

1. Definimos una compuerta genérica $\hat{U} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$

Esto significa que: $U|0\rangle = a|0\rangle + b|1\rangle$ y $U|1\rangle = c|0\rangle + d|1\rangle$.

2. Analizamos la acción de $CU_{1,0}$ sobre la base:

- $CU|00\rangle = |00\rangle$
- $CU|01\rangle = |01\rangle$
- $CU|10\rangle = |1\rangle \otimes (U|0\rangle) = |1\rangle \otimes (a|0\rangle + b|1\rangle) = a|10\rangle + b|11\rangle$
- $CU|11\rangle = |1\rangle \otimes (U|1\rangle) = |1\rangle \otimes (c|0\rangle + d|1\rangle) = c|10\rangle + d|11\rangle$

3. Construimos la matriz columna por columna:

$$CU_{1,0} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & a & c \\ 0 & 0 & b & d \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}$$

> La matriz de $CU_{1,0}$ es una matriz de bloques con la Identidad en la esquina superior izquierda y la matriz U en la inferior derecha.

Verificando la Fórmula General para CNOT y CZ

1. Para CNOT ($U = X$):

La matriz de X es $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, por lo que $a = 0, b = 1, c = 1, d = 0$.

Sustituyendo en la fórmula general:

$$\text{CNOT}_{1,0} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

✅ ¡Coincide con la matriz que calculamos previamente!

2. Para CZ ($U = Z$):

La matriz de Z es $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, por lo que $a = 1, b = 0, c = 0, d = -1$.

Sustituyendo en la fórmula general:

$$\text{CZ}_{1,0} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

✅ ¡También coincide!

La Matriz General de $CU_{0,1}$ (Control en q_0)

Podemos seguir el mismo procedimiento de "construcción por columnas" para el caso en que el control es el qubit q_0.

Acción sobre la base:

- $CU|00\rangle = |00\rangle$
- $CU|10\rangle = |10\rangle$
- $CU|01\rangle = (U|0\rangle) \otimes |1\rangle = a|01\rangle + b|11\rangle$
- $CU|11\rangle = (U|1\rangle) \otimes |1\rangle = c|01\rangle + d|11\rangle$

Matriz General Resultante:

$$CU_{0,1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & a & 0 & c \\ 0 & 0 & 1 & 0 \\ 0 & b & 0 & d \end{pmatrix}$$

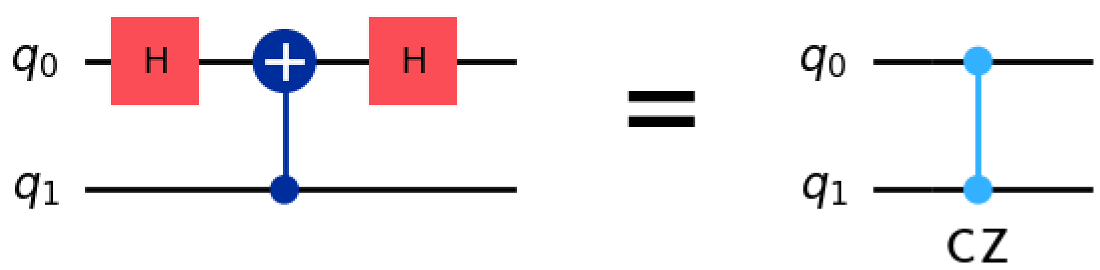
> **Observación:** La matriz ya no tiene una forma de bloques simple. Los elementos de la matriz U aparecen "intercalados" en las columnas correspondientes a los estados $|01\rangle$ y $|11\rangle$.

Una Identidad Poderosa: Conectando CNOT y CZ

Existe una relación fundamental entre las compuertas más importantes de 1 y 2 qubits. La CNOT se puede "transformar" en una CZ (y viceversa) "envolviéndola" con compuertas de Hadamard.

La Identidad "Sándwich de Hadamard":

> Aplicar una compuerta Hadamard al qubit objetivo, antes y después de una CNOT, es equivalente a realizar una CZ.
>
> $$(\hat{I} \otimes \hat{H}) \cdot \mathrm{CNOT} \cdot (\hat{I} \otimes \hat{H}) = \mathrm{CZ}$$



> Esta identidad es crucial en el diseño de circuitos, permitiendo cambiar entre tipos de interacciones.

Ejercicio: Demostración de la Identidad

Problema:

Demuestra la identidad $(\hat{I} \otimes \hat{H}) \cdot \mathrm{CNOT} \cdot (\hat{I} \otimes \hat{H}) = \mathrm{CZ}$ mediante multiplicación de matrices. (CNOT tiene control en q_1)

Instrucción:

1. Calcula el producto $\mathrm{CNOT} \cdot (\hat{I} \otimes \hat{H})$.
2. Multiplica el resultado por la izquierda por $(\hat{I} \otimes \hat{H})$.
3. Comprueba si la matriz final es la de la CZ.

Ejercicio: Demostración de la Identidad

Problema:

Demuestra la identidad $(\hat{I} \otimes \hat{H}) \cdot \mathrm{CNOT} \cdot (\hat{I} \otimes \hat{H}) = \mathrm{CZ}$ mediante multiplicación de matrices.

Datos :

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \implies I \otimes H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad (\text{Control en } q_1)$$

Instrucción:

1. Calcula el producto $\mathrm{CNOT} \cdot (\hat{I} \otimes \hat{H})$.
2. Multiplica el resultado por la izquierda por $(\hat{I} \otimes \hat{H})$.
3. Comprueba si la matriz final es la de la CZ.

Solución: Demostración de la Identidad

Datos :

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \implies I \otimes H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1 & 0 & 0\\ 1 & -1 & 0 & 0\\ 0 & 0 & 1 & 1\\ 0 & 0 & 1 & -1\end{pmatrix}$$

$$\text{CNOT} = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix} \quad (\text{Control en } q_1)$$

Paso 1: $\text{CNOT} \cdot (\hat{I} \otimes \hat{H})$

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix}\begin{pmatrix}1 & 1 & 0 & 0\\ 1 & -1 & 0 & 0\\ 0 & 0 & 1 & 1\\ 0 & 0 & 1 & -1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1 & 0 & 0\\ 1 & -1 & 0 & 0\\ 0 & 0 & 1 & -1\\ 0 & 0 & 1 & 1\end{pmatrix}$$

Paso 2: $(\hat{I} \otimes \hat{H}) \cdot (\text{Resultado Anterior})$

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1 & 0 & 0\\ 1 & -1 & 0 & 0\\ 0 & 0 & 1 & 1\\ 0 & 0 & 1 & -1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1 & 0 & 0\\ 1 & -1 & 0 & 0\\ 0 & 0 & 1 & -1\\ 0 & 0 & 1 & 1\end{pmatrix}$$

$$= \frac{1}{2}\begin{pmatrix}2 & 0 & 0 & 0\\ 0 & 2 & 0 & 0\\ 0 & 0 & 2 & 0\\ 0 & 0 & 0 & -2\end{pmatrix} = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & -1\end{pmatrix} = \text{CZ}$$

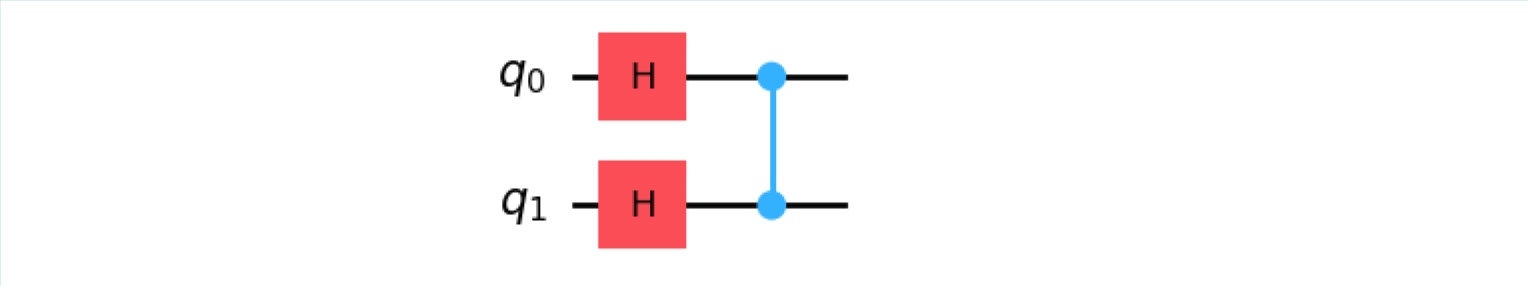
✅ ¡La identidad se cumple!

Ejercicio: La CZ como Compuerta Entrelazadora

Sabemos que la CNOT y la CZ están íntimamente relacionadas. Como una puede construir a la otra, es lógico que la CZ también pueda crear entrelazamiento.

Vamos a demostrarlo directamente con un circuito.

Problema:
Analiza el efecto del siguiente circuito sobre el estado inicial $|00\rangle$. ¿El estado final es entrelazado?



Instrucción:

1. Calcula el estado intermedio después de aplicar el operador $H \otimes H$.
2. Aplica la compuerta CZ al estado resultante.
3. Usa el Test de Separabilidad ($c_{00}c_{11} = c_{01}c_{10}$) para determinar si el estado final es entrelazado.

Solución: La CZ Creando Entrelazamiento

1. Estado Inicial: $|\psi_0\rangle = |00\rangle$

2. Paso 1 (Aplicar $H \otimes H$):

Este paso crea la superposición uniforme sobre la que actuará la CZ.

$$|\psi_1\rangle = (H \otimes H)|00\rangle = (H|0\rangle) \otimes (H|0\rangle) = |+\rangle|+\rangle$$

$$|\psi_1\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

3. Paso 2 (Aplicar CZ):

Aplicamos la CZ al estado $|\psi_1\rangle$. Recordamos que la CZ solo afecta al estado $|11\rangle$, aplicándole una fase de -1.

$$|\psi_f\rangle = \mathrm{CZ}|\psi_1\rangle = \mathrm{CZ}\left(\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)\right)$$

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

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

Solución: Análisis del Estado Final

Estado Final: $|\psi_f\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)$

Análisis de Separabilidad (Test $c_{00}c_{11} = c_{01}c_{10}$):

$$c_{00} = \frac{1}{2}, \quad c_{01} = \frac{1}{2}, \quad c_{10} = \frac{1}{2}, \quad c_{11} = -\frac{1}{2}$$

2. **Aplicamos el test:**

$$c_{00} \cdot c_{11} = \left(\frac{1}{2}\right) \cdot \left(-\frac{1}{2}\right) = -\frac{1}{4}$$

$$c_{01} \cdot c_{10} = \left(\frac{1}{2}\right) \cdot \left(\frac{1}{2}\right) = +\frac{1}{4}$$

Como $-\frac{1}{4} \neq \frac{1}{4}$, el test **no se cumple**.

> **Conclusión:** El estado final **está entrelazado**. Hemos demostrado que la compuerta CZ, al igual que la CNOT, es una compuerta de dos qubits capaz de generar entrelazamiento a partir de un estado separable. La clave fue tener superposición en ambos qubits antes de aplicar la compuerta condicional.

Compuertas de Múltiples Controles y la Compuerta SWAP

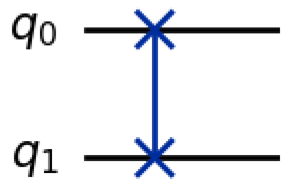
Ya dominamos las compuertas de 1 qubit y la CNOT. Ahora, expandiremos nuestro repertorio a operaciones más complejas que son esenciales para muchos algoritmos.

En este tema, exploraremos tres compuertas fundamentales:

1. **La Compuerta SWAP:** ¿Cómo intercambiamos el estado de dos qubits?
2. **La Compuerta Toffoli (CCNOT):** Implementación cuántica de una **condición AND**
3. **La Compuerta Fredkin (CSWAP):** ¿Cómo realizamos un SWAP condicional?

La Compuerta SWAP: Intercambiando Estados

A veces, la arquitectura de un ordenador cuántico requiere que movamos información de un qubit a otro. La compuerta **SWAP** realiza esta tarea.



La Lógica de la SWAP:

> Intercambia el estado cuántico completo de dos qubits.
>
> $$\mathrm{SWAP}|q_1 q_0\rangle = |q_0 q_1\rangle$$

Acción sobre la Base Computacional:

- SWAP $|00\rangle \rightarrow |00\rangle$
- SWAP $|01\rangle \rightarrow |10\rangle$
- SWAP $|10\rangle \rightarrow |01\rangle$
- SWAP $|11\rangle \rightarrow |11\rangle$

La Matriz de la Compuerta SWAP

Podemos construir la matriz de 4×4 de la SWAP observando cómo transforma los vectores de la base.
Recordemos que el vector de entrada define la columna y el de salida define la posición del '1' en esa columna.

- $|00\rangle \to |00\rangle$: Un 1 en la posición (0,0).
- $|01\rangle \to |10\rangle$: Un 1 en la posición (2,1).
- $|10\rangle \to |01\rangle$: Un 1 en la posición (1,2).
- $|11\rangle \to |11\rangle$: Un 1 en la posición (3,3).

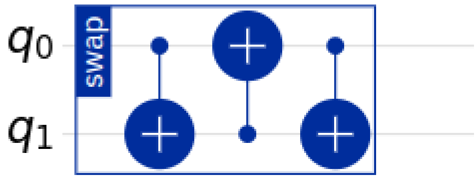
$$\mathrm{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

> La matriz SWAP es una **matriz de permutación**: simplemente reordena las filas (o columnas) de la matriz identidad.

Descomponiendo la SWAP

Un hecho muy importante en la computación cuántica es que las compuertas complejas a menudo se pueden construir a partir de otras más simples.

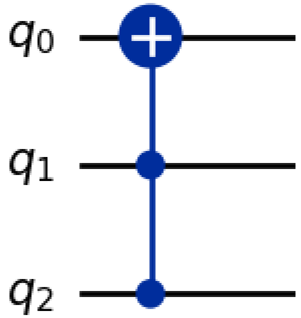
Teorema: Una compuerta SWAP se puede implementar usando **tres compuertas CNOT**.



> **Importancia Práctica:** En muchos hardwares cuánticos, la CNOT es una compuerta "nativa" más fácil de implementar que la SWAP. Los compiladores cuánticos (transpiladores) a menudo usan esta identidad para traducir un algoritmo a las operaciones que la máquina puede realizar físicamente.

Control Múltiple: La Compuerta Toffoli (CCNOT)

La CNOT tenía un qubit de control. La **Compuerta Toffoli** (o Controlada-Controlada-NOT) tiene **dos**. Es una compuerta de 3 qubits.



La Lógica de la Toffoli:

> "Aplica una compuerta NOT ($\hat{X}$) al qubit objetivo **si y solo si** el primer qubit de control **Y** el segundo qubit de control están ambos en el estado $|1\rangle$."

Es la implementación cuántica de una **condición AND**.

Aquí, q_2 y q_1 son los controles, y q_0 es el objetivo.

La Matriz de la Compuerta Toffoli

La Toffoli actúa sobre un espacio de $2^3 = 8$ dimensiones. Su matriz es de 8×8.
Su acción solo es no trivial para los estados base donde los dos primeros qubits son $|11\rangle$:

- CCNOT $|110\rangle \to |111\rangle$
- CCNOT $|111\rangle \to |110\rangle$

Para todos los demás estados base ($|000\rangle, |001\rangle, \ldots, |101\rangle$), actúa como la identidad.

$$\mathrm{CCNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

> Es una matriz identidad, excepto por un bloque NOT en la esquina inferior derecha.

La Importancia de la Toffoli: Universalidad Clásica

La compuerta Toffoli es extremadamente importante por una razón clave:

Teorema de Universalidad:

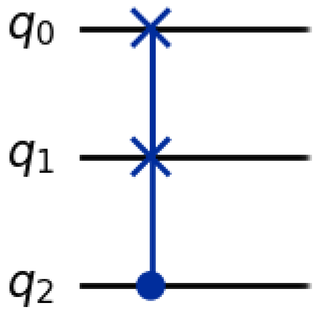
> La compuerta Toffoli, junto con la capacidad de preparar estados $|0\rangle$ y $|1\rangle$, es **universal para la computación clásica reversible**.

Esto significa que cualquier función booleana clásica (AND, OR, NAND, XOR, etc.) puede ser implementada usando únicamente compuertas Toffoli.

> La Toffoli es el puente fundamental que nos asegura que un ordenador cuántico puede hacer **todo lo que puede hacer un ordenador clásico**, pero de forma reversible.

El Intercambio Controlado: La Compuerta Fredkin (CSWAP)

La **Compuerta Fredkin** es otra compuerta universal de 3 qubits. Es una **Compuerta SWAP Controlada**.



La Lógica de la Fredkin:

> "**Si** el qubit de control es $|1\rangle$, **entonces** aplica una compuerta SWAP a los dos qubits objetivo."

Aquí, q_2 es el control, y los objetivos del SWAP son q_1 y q_0.

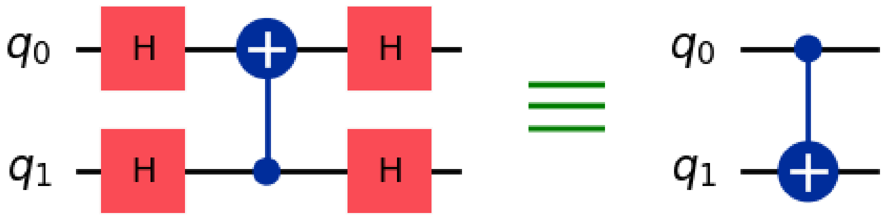
La Matriz de la Compuerta Fredkin

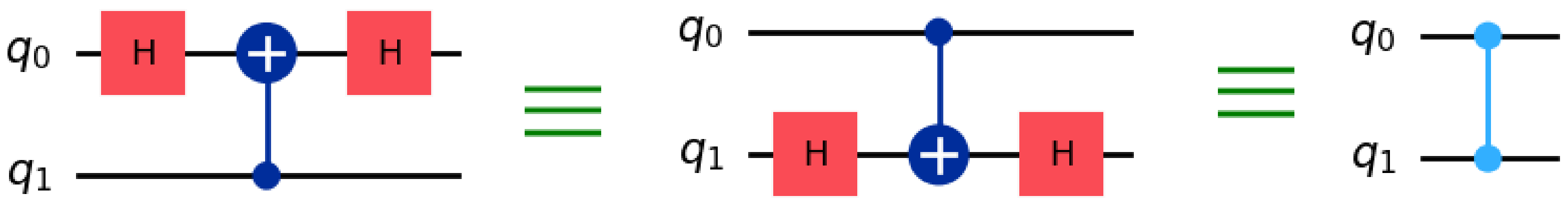
La matriz de 8×8 de la Fredkin también tiene una estructura de bloques muy clara.

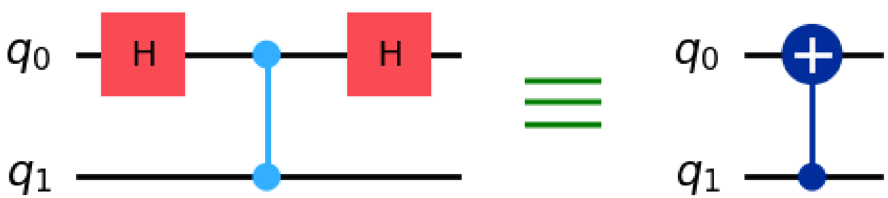
- Para los estados donde el control q_2 es 0 ($|000\rangle, \ldots, |011\rangle$), actúa como la Identidad de 4×4.
- Para los estados donde el control q_2 es 1 ($|100\rangle, \ldots, |111\rangle$), actúa como la matriz SWAP de 4×4.

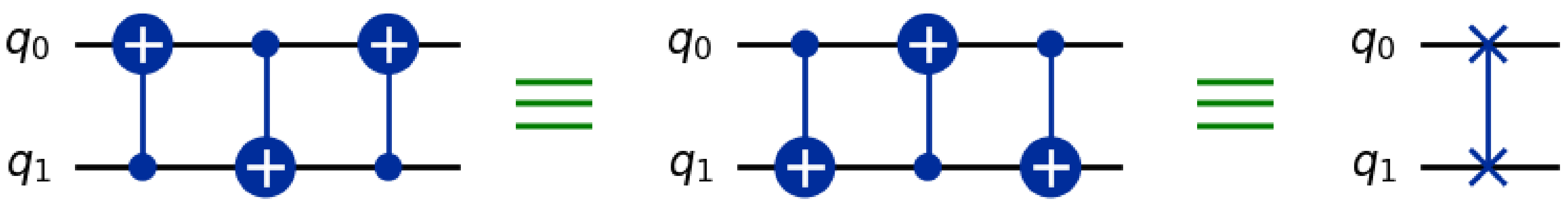
$$\mathrm{CSWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

> La matriz es una "matriz identidad por bloques", donde el bloque inferior derecho es una matriz SWAP.


q_0
q_1
H
H
H
H
q_0
q_1


q_0
q_1
H
H
q_0
q_1
H
H
q_0
q_1


q_0
q_1
H
H
q_0
q_1


q_0
q_1
q_0
q_1
q_0
q_1

Revisa el cuaderno jupyter

clase09-qiskit.ipynb