Introducción a la Computación e Información Cuántica

Módulo 4: Algoritmos Cuánticos Fundamentales

6 al 10 de Octubre de 2025

Dr. Andrés A. REYNOSO

XXIX Escuela Internacional de Ingeniería y Computación

Contenidos

Contenidos

Si la clonacion cuantica fuera cierta se podria transmitir info superando la velocidad de la luz (1)

En esta versión (construida para mostrar que si la clonacion fuera posible permitiria que se puedan transmitir mensajes a mas de la velocidad de la luz) Alice va a medir su particula en dos direcciones diferentes segun si quiere transmitir un 0 o un 1 y Bob usaria la maquina de clonacion para saber muy rapido como midió Alice.

Al comenzar suponemos que siempre Alice y Bob disponen de una particula de este par EPR:

$$|\Psi^{+}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B\right)$$

dado que $|0\rangle = (|+\rangle + |-\rangle)/\sqrt{2}$ y que $|1\rangle = (|+\rangle - |-\rangle)/\sqrt{2}$ reemplazando este par puede ser escrito en la base $\{|+\rangle, |-\rangle\}$ como

$$|\Psi^{+}\rangle = \frac{1}{\sqrt{2}}\left(|+\rangle_A |+\rangle_B - |-\rangle_A |-\rangle_B\right)$$

Si la clonacion cuantica fuera cierta se podria transmitir info superando la velocidad de la luz (2)

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B\right) = \frac{1}{\sqrt{2}}\left(|+\rangle_A |+\rangle_B - |-\rangle_A |-\rangle_B\right)$$

Alice codifica 1 bit clásico de información aplicando una de las dos siguientes mediciones:

*M_0: Si el mensaje clásico a mandar es 0 Alice procede a medir su qubit en la base Z, es decir colapsará su qubit 50 % entre los estados $\{|0\rangle, |1\rangle\}$.

* M_1:Si el mensaje clásico a mandar es 1 Alice procede a medir su qubit en la base X, es decir colapsará su qubit 50 % entre los estados $\{|+\rangle, |-\rangle\}$

Si la clonacion cuantica fuera cierta se podria transmitir info superando la velocidad de la luz (3)

$$|\Psi^{+}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B\right) = \frac{1}{\sqrt{2}}\left(|+\rangle_A |+\rangle_B - |-\rangle_A |-\rangle_B\right)$$

Bob siempre mide su qubit en la base computacional.

* **Caso M_0 hay dos posibilidades con igual probabilidad**:

Alice mide $|0\rangle$ lo que hace a Bob tener $|1\rangle$ y por tanto $P(0) = 0$ y $P(1) = 1$

Alice mide $|1\rangle$ lo que hace a Bob tener $|0\rangle$ y por tanto $P(0) = 1$ y $P(1) = 0$

En ambos casos de M_0 uno de los dos resultados tiene probabilidad nula.

* **Caso M_1 hay dos posibilidades con igual probabilidad**:

Alice mide $|+\rangle$ lo que hace a Bob tener $|+\rangle$ y por tanto $P(0) = P(1) = 1/2$

Alice mide $|-\rangle$ lo que hace a Bob tener $|-\rangle$ y por tanto $P(0) = P(1) = 1/2$

En ambos casos de M_1 los dos resultados tienen igual probabilidad.

Si la clonacion cuantica fuera cierta se podria transmitir info superando la velocidad de la luz (4)

- Si antes de medir Bob pudiera clonar su qubit generaria muchas copias sobre las que puede hacer muchas mediciones y acceder a $P(0)$ y $P(1)$ distinguiendo M_0 (cuando encuentra que hay solo 0's o solo 1's apareciendo entre los clones) de M_1 (cuando entre los clones aparecen con probabilidad pareja los 0's y los 1's). Por lo tanto Bob podria saber lo que quiso mandar Alice mas rapido que la velocidad de la luz!! ALARMA de que algo anda mal!!
- En cambio siendo que la clonacion cuantica imposible (ya lo vimos) Bob puede medir solo una vez sobre LA VERSION ORIGINAL de su qubit y por tanto no tiene certeza de si es una situacion M_0 o M_1. Porque la probabilidad de 0 o de 1 en una sola medicion es pareja en ambos casos. Si Alice hizo M_0 Bob tiene con igual chance $|0\rangle$ o $|1\rangle$. Y si Alice hizo M_1 Bob tiene el estado $|+\rangle$ o el estado $|-\rangle$ lo cual en ambos casos también es $1/2$ de probabilidad en la base computacional.

Causalidad preservada

La no-clonación garantiza:

1. Bob no puede extraer información de su mitad sola
2. La información de Alice solo se manifiesta cuando *ambos* qubits se reúnen
3. El qubit debe viajar físicamente ($v \leqslant c$)
4. No hay comunicación superluminal

Moraleja: Las leyes cuánticas protegen la causalidad relativista

Contenidos

¿Qué significa pureza = 0.5?

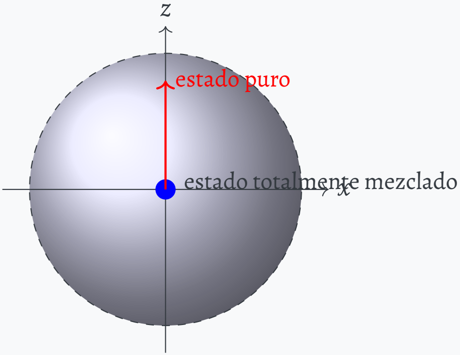
En el simulador de IBM, cada círculo indica el estado de un qubit individual.

- El anillo gris externo representa el máximo de pureza ($= 1$).
- El círculo azul interno representa la **pureza actual**.
- En un par entrelazado (como en $|\Phi^+\rangle$), el simulador muestra:

$$\mathrm{Prob}(|1\rangle) = 50\,\%, \quad \mathrm{Pureza} = 0{,}5$$

- Es decir: el qubit aislado de Bob se comporta como si estuviera a la mitad del camino entre $|0\rangle$ y $|1\rangle$.

Visualización en la esfera de Bloch



La pureza mide qué tan "lejos del centro" está el vector de Bloch.

$$\text{pureza} = |\vec{r}|^2$$

donde $\vec{r}$ es el vector en la esfera de Bloch.

De la superposición al mezclado

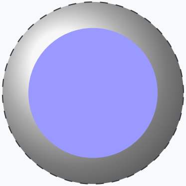
- Un qubit aislado en estado puro tiene un vector de Bloch de longitud 1.

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

- Si el qubit está entrelazado con otro, su vector de Bloch “se acorta”.
- Longitud $|\vec{r}| < 1$ significa que hay **incertidumbre adicional** debida a correlaciones con otro sistema.
- En el caso de Bell: $|\vec{r}| = 0 \Rightarrow$ pureza $= 0{,}5$.

Interpretación conceptual

- El qubit de Bob no tiene un estado definido.
- Es una mezcla uniforme: 50 % $|0\rangle$ y 50 % $|1\rangle$.
- Esa "mezcla" no proviene de ignorancia clásica, sino de entrelazamiento cuántico.
- El simulador indica esto reduciendo el radio azul (pureza < 1).



Pureza = 0.5

Hacia una definición más formal

Tiene que ver con utilizar el concepto de la **matriz densidad**:

$$\rho = \frac{1}{2}(I + \vec{r} \cdot \vec{\sigma})$$

y la pureza se expresa como:

$$\mathrm{Pur}(\rho) = \mathrm{Tr}(\rho^2) = \frac{1 + |\vec{r}|^2}{2}$$

Casos límite:

$$\text{Estado puro: } |\vec{r}| = 1 \Rightarrow \text{Pur} = 1 \quad \text{Estado mezclado: } |\vec{r}| = 0 \Rightarrow \text{Pur} = 0{,}5$$

De amplitudes a matriz densidad

Un qubit puro se representa como:

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

Su **matriz densidad** es:

$$\rho = |\psi\rangle\langle\psi| = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix}$$

- Los términos diagonales son las **poblaciones**: probabilidades de estar en $|0\rangle$ o $|1\rangle$.
- Los términos fuera de la diagonal son las **coherencias**: indican la superposición cuántica.

Ejemplo: Para $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$,

$$\rho_+ = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

Pureza del estado

La **pureza** mide cuán “puro” o “mezclado” está un estado:

$$\boxed{\text{Purity} = \mathrm{Tr}(\rho^2)}$$

- Para un **estado puro**: $\rho = |\psi\rangle\langle\psi|$, se cumple $\mathrm{Tr}(\rho^2) = 1$.
- Para un **estado mixto**: $\mathrm{Tr}(\rho^2) < 1$.

Ejemplo:

$$\rho = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \Rightarrow \quad \mathrm{Tr}(\rho^2) = \tfrac{1}{2}.$$

Interpretación: el sistema está “difuso” entre $|0\rangle$ y $|1\rangle$.

Reducción por traza parcial

Para un sistema de dos qubits A y B:

$$\rho_{AB} = |\Phi^+\rangle \langle\Phi^+|, \quad |\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

El estado local de Bob se obtiene **tomando la traza parcial** sobre A:

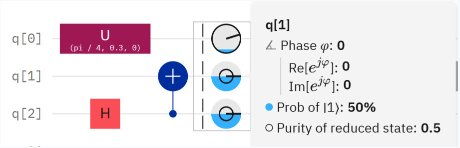
$$\rho_B = \mathrm{Tr}_A(\rho_{AB})$$

$$\rho_B = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{I}{2}$$

Resultado: Bob tiene un **estado completamente mezclado**, sin información sobre Alice.

Interpretando el simulador de Qiskit

En la visualización de IBM Q:



- El **círculo exterior** indica la **pureza**.
  - Estado puro $\Rightarrow$ círculo lleno (Purity $= 1$)
  - Estado mezclado $\Rightarrow$ círculo hueco (Purity < 1)
- El **vector azul** indica la probabilidad de $|1\rangle$.

Ejemplo del simulador:

$$\text{Prob}(|1\rangle) = 50\,\%, \quad \text{Purity} = 0{,}5$$

Interpretación: el qubit está en $\rho = \frac{1}{2}I$, un estado totalmente mezclado.

Contenidos

Motivación: Criptografía moderna

Criptografía clásica actual:

- RSA: seguridad basada en dificultad de factorizar
- Diffie-Hellman: logaritmos discretos
- AES: seguro si la clave es secreta y aleatoria

Problema: Distribución segura de claves entre Alice y Bob

Solución cuántica: QKD permite generar clave compartida detectando cualquier espionaje

Protocolo BB84: Bases cuánticas

Alice usa dos bases no conmutativas:

Base computacional (Z):

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

Base diagonal (X o Hadamard):

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

Propiedad clave: $\{|0\rangle\,, |1\rangle\}$ y $\{|+\rangle\,, |-\rangle\}$ son bases incompatibles

BB84: Codificación

Mapeo de bits clásicos a estados cuánticos:

Bit	Base Z	Base X
0	$\|0\rangle$	$\|+\rangle$
1	$\|1\rangle$	$\|-\rangle$

Alice elige aleatoriamente:

1. Bit a enviar (0 o 1)
2. Base a usar (Z o X)

BB84: Ejemplo de transmisión

Bit Alice	0	1	1	0	1	0	1
Base Alice	Z	X	Z	X	Z	X	Z
Estado	$\|0\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$
Base Bob	Z	Z	Z	X	X	Z	Z
Medida Bob	0	0/1	1	0	0/1	0/1	1
¿Mantener?	✓	×	✓	✓	×	×	✓

Clave compartida: bits 1, 3, 4, 7 $\rightarrow \{0, 1, 0, 1\}$

Medición en base incorrecta

Si Bob mide $|+\rangle$ en base Z:

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

Probabilidades:

$$P(0) = |\langle 0|+\rangle|^2 = \frac{1}{2}, \quad P(1) = |\langle 1|+\rangle|^2 = \frac{1}{2}$$

Resultado aleatorio con 50 %-50 %

Esto es fundamental para detectar a Eve

Detección de Eve: Setup

Si Eve intercepta el qubit:

1. Eve debe medir (no puede clonar)
2. Eve debe elegir base Z o X (no conoce la correcta)
3. Eve reenvía lo que midió a Bob

Probabilidad de que Eve elija base correcta: $P_{\text{correcto}} = 1/2$

Si elige mal, introduce error detectable

Análisis cuantitativo de eavesdropping

Caso: Alice envía $|0\rangle$ en base Z

Sin Eve: Bob mide en Z $\rightarrow$ obtiene 0 con certeza

Con Eve que mide en X:

1. Eve mide: obtiene $|+\rangle$ o $|-\rangle$ (50 %-50 %)
2. Eve reenvía $|+\rangle$ (supongamos)
3. Bob mide en Z: $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
4. Bob obtiene 0 o 1 con igual probabilidad

¡Error del 25 % introducido!

Tasa de error cuántico (QBER)

Quantum Bit Error Rate:

$$\text{QBER} = \frac{\text{bits con error}}{\text{total de bits comparados}}$$

Sin Eve: $\text{QBER} \approx 0\,\%$ (solo ruido técnico $\sim 1 - 2\,\%$)

Con Eve: $\text{QBER} \approx 25\,\%$

Alice y Bob sacrifican muestra de bits para verificar QBER:

- QBER bajo: usar resto como clave
- QBER alto: abortar protocolo

Seguridad incondicional

La seguridad de BB84 no depende de:

- Dificultad computacional (como RSA)
- Tecnología de Eve
- Potencia computacional disponible

Solo depende de:

1. Teorema de no-cloning
2. Incompatibilidad de observables ($[X, Z] \neq 0$)
3. Colapso de la función de onda al medir

Seguridad garantizada por leyes físicas fundamentales

Contenidos

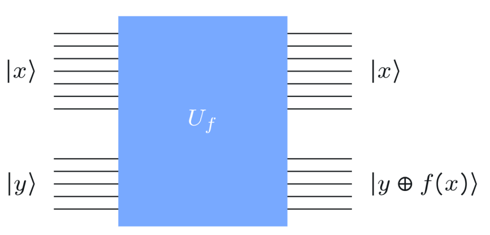
Implementación de funciones booleanas cuánticas (unitarias)

Función clásica: $f : \{0,1\}^n \to \{0,1\}^m$

Oráculo cuántico: Operador unitario U_f que implementa

$$U_f : |x\rangle\,|y\rangle \mapsto |x\rangle\,|y \oplus f(x)\rangle$$

donde $\oplus$ denota suma módulo 2 (XOR)



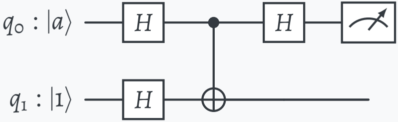
Implementación de funciones booleanas cuánticas (unitarias)

Propiedades:

- Esta construcción nos permite implementar cualquier función booleana.
- U_f es unitario (reversible)
- No modifica el registro de entrada $|x\rangle$
- Información de $f(x)$ se codifica en el registro auxiliar

Phase kick back (Dos qubits), implementación en Qiskit

Consideremos el siguiente circuito



Secuencia en notación de Dirac (convención Qiskit: $q_1 \otimes q_0$). Notar que es una CNOT con control en el segundo qubit del producto tensorial y target qubit en el primero. Se comienza con $|\psi_0\rangle = |1\rangle \otimes |a\rangle$ y se evoluciona.

Ejemplo $|a\rangle = |0\rangle$

Tenemos $|\psi_0\rangle = |1\rangle \otimes |0\rangle$

$$
\begin{aligned}
|\psi_1\rangle &= (H \otimes H)\,|1\rangle \otimes |0\rangle = \tfrac{1}{2}(|0\rangle - |1\rangle) \otimes (|0\rangle + |1\rangle) \\
&= \tfrac{1}{2}(|0\rangle - |1\rangle) \otimes |0\rangle + \tfrac{1}{2}(|0\rangle - |1\rangle) \otimes |1\rangle \\
|\psi_2\rangle &= CNOT_{0,1}\,|\psi_1\rangle \\
&= \tfrac{1}{2}(|0\rangle - |1\rangle) \otimes |0\rangle + \tfrac{1}{2}(|1\rangle - |0\rangle) \otimes |1\rangle \\
&= \tfrac{1}{2}(|0\rangle - |1\rangle) \otimes |0\rangle - \tfrac{1}{2}(|0\rangle - |1\rangle) \otimes |1\rangle \\
&= \tfrac{1}{2}(|0\rangle - |1\rangle) \otimes (|0\rangle - |1\rangle)
\end{aligned}
$$

La CNOT resulta en un cambio de signo de paridad en el qubit de control, que en $|\psi_1\rangle$ era $|+\rangle$ y termina en $|-\rangle$!!! Eso se conoce como el phase kick back (patada de fase hacia atras). Se aplica un Hadamark para poder leer la paridad como un 0 o 1 en la base computacional: queda $|\psi_3\rangle = (I \otimes H)\,|\psi_2\rangle = |-\rangle \otimes |1\rangle$. Se mide 1 reflejando que la paridad es $|-\rangle$.

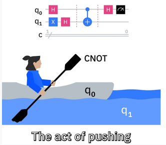
Ejemplo $|a\rangle = |1\rangle$

Tenemos $|\psi_0\rangle = |1\rangle \otimes |1\rangle$

$$\begin{aligned}
|\psi_1\rangle &= (H \otimes H)\,|1\rangle \otimes |1\rangle = \tfrac{1}{2}(|0\rangle - |1\rangle) \otimes (|0\rangle - |1\rangle) \\
&= \tfrac{1}{2}(|0\rangle - |1\rangle) \otimes |0\rangle - \tfrac{1}{2}(|0\rangle - |1\rangle) \otimes |1\rangle \\
|\psi_2\rangle &= CNOT_{0,1}\,|\psi_1\rangle \\
&= \tfrac{1}{2}(|0\rangle - |1\rangle) \otimes |0\rangle - \tfrac{1}{2}(|1\rangle - |0\rangle) \otimes |1\rangle \\
&= \tfrac{1}{2}(|0\rangle - |1\rangle) \otimes |0\rangle + \tfrac{1}{2}(|0\rangle - |1\rangle) \otimes |1\rangle \\
&= \tfrac{1}{2}(|0\rangle - |1\rangle) \otimes (|0\rangle + |1\rangle)
\end{aligned}$$

La CNOT resulta en un cambio de signo de paridad en el qubit de control, que en $|\psi_1\rangle$ era $|-\rangle$ y termina en $|+\rangle$!!! Eso se conoce como el phase kick back (patada de fase hacia atras). Se aplica un Hadamark para poder leer la paridad como un 0 o 1 en la base computacional: queda $|\psi_3\rangle = (I \otimes H)\,|\psi_2\rangle = |-\rangle \otimes |0\rangle$. Se mide 0 reflejando que la paridad es $|+\rangle$.

Intuición del phase kickback



La CNOT actúa como el remo:

- Cuando q_0 (remo) actúa, **empuja la fase** hacia el qubit q_1.
- Pero si q_1 está en $|-\rangle$, el empuje se **refleja como una fase en** q_0.
- Esta es la "patada de fase": el control sufre una rotación de fase por la estructura del blanco.
- Este efecto es clave en el algoritmo que sigue.