3° Escuela de Computación Cuántica MIRO
Introducción a la Mecánica Cuántica
Parte II

Dr. Omar Jiménez Henríquez
Centro Multidisciplinario de Física
Universidad Mayor

Santiago, 06 enero 2025

Temas de la Presentación

1. Teoría Clásica de la Información
   - El bit
   - ¿Qué es información?
   - Entropía de Shannon
2. Postulados de la Mecánica Cuántica
   - Postulado 1: Estado del sistema cuántico
   - Postulado 2: Evolución unitaria
   - Postulado 3: Mediciones cuánticas
   - Postulado 4: Sistemas Compuestos
3. Computación Cuántica
   - Compuertas de un qubit
   - Compuertas de dos qubits

Teoría Clásica de la Información

El bit clásico

Los valores $\{0 \text{ ó } 1\}$ son estados distinguibles de algún sistema físico.
Nos permite procesar, distribuir y almacenar la información.

Teoría Clásica de la Información

El bit clásico

Los valores $\{0$ ó $1\}$ son estados distinguibles de algún sistema físico.
Nos permite procesar, distribuir y almacenar la información.

Para representar las letras se usan 8 bit equivalente a 1 byte.

0110 0010 = b
0110 1001 = i
0111 0100 = ?

1Kb = 10^3 byte
1Mb = 10^6 byte
1Tb = 10^{12} byte, computador.

Teoría Clásica de la Información

El bit clásico

Los valores {0 ó 1} son estados distinguibles de algún sistema físico.
Nos permite procesar, distribuir y almacenar la información.

Bit = **0** o **1**

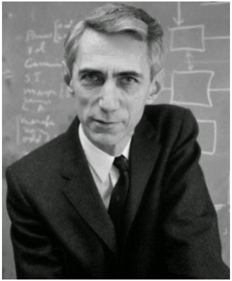
Para representar las letras se usan 8 bit equivalente a 1 byte.

0110 0010 = b
0110 1001 = i
0111 0100 = ?

$$\begin{array}{ccccccc} 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ \uparrow & \uparrow & \uparrow & \downarrow & \uparrow & \uparrow & \uparrow \end{array}$$

¿ Qué es información?

Claude Shannon (1948) relacionó la información con la incerteza.



Dado que **obtener información** puede ser considerado como la **disminución de la incerteza** que se tiene de que ocurra un evento.

Variable Aleatoria

Una variable aleatoria X es aquella en que sus resultados están descritos por probabilidades. Por ejemplo lanzar una moneda

Variable Aleatoria

Una variable aleatoria X es aquella en que sus resultados están descritos por probabilidades. Por ejemplo lanzar una moneda

los dos posibles resultados son:

Cara o sello

con probabilidades de aparición iguales a 1/2 cada una.

Entropía de Shannon $H(X)$

$H(X)$ de una variable aleatoria X con símbolos x que aparecen con probabilidad p_x, se define como la cantidad promedio de información obtenida al conocer el valor de la variable X.

$$H(X) = -\sum_x p_x \log_2 p_x$$

Entropía de Shannon $H(X)$

$H(X)$ de una variable aleatoria X con símbolos x que aparecen con probabilidad p_x, se define como la cantidad promedio de información obtenida al conocer el valor de la variable X.

$$H(X) = -\sum_{x} p_x \log_2 p_x$$

- Se expresa en bits. Es $H(X) \geq 0$, su mínimo valor es cero, $H(X) = 0$, para una variable determinista.
- La entropía es una medida de la incerteza de la variable aleatoria X antes de obtener los resultados de la medida.
- Para el caso de la moneda (cara o sello) nos entrega un bit de información.

El bit cuántico (qubit o quantum bit)

En información cuántica se reemplaza el bit clásico por el bit cuántico (qubit).

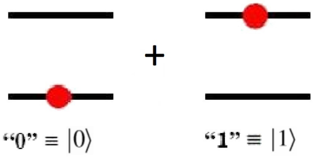
Bit clásico

0
1

Bit cuántico

$|0\rangle$
$|1\rangle$

El cero cuántico $|0\rangle$ y el uno cuántico $|1\rangle$ son estados cuánticos que se llaman ket 0 y ket 1. En mecánica cuántica es posible tener una **superposición de estados cuánticos**, $|0\rangle + |1\rangle$

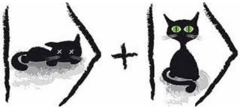


Estados cuánticos

Superposición de estados

$$|\psi\rangle = |0\rangle + |1\rangle$$

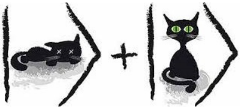
Función de Onda Cuántica



Estados cuánticos

Superposición de estados

$$|\psi\rangle = |0\rangle + |1\rangle$$

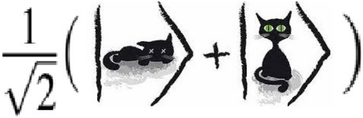


Función de Onda Cuántica

La función de onda debe estar bien normalizada. Es decir, la longitud del vector de estado $|\psi\rangle$ debe ser igual a 1.

Superposición de estados

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



Función de Onda bien normalizada

Probabilidades

Consideremos el vector de estado cuántico

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

los coeficientes a y b son números complejos. Si estos son números reales, la condición de normalización es

$$a^2 + b^2 = 1$$

Probabilidad de encontrar $|0\rangle$

$$a^2 + b^2 = 1$$

La suma de las probabiliades es igual a uno.

Probabilidad de encontrar $|1\rangle$

Qubit (quantum bit)

La unidad básica de información cuántica es el qubit,

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

- es una superposición de los elementos de la base lógica $\{|0\rangle, |1\rangle\}$ de un espacio de Hilbert bi-dimensional.

Qubit (quantum bit)

La unidad básica de información cuántica es el qubit

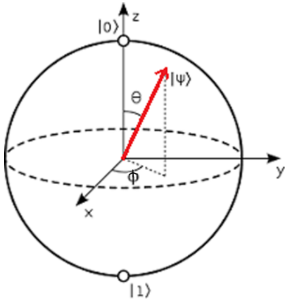
$$|\psi\rangle = a|0\rangle + b|1\rangle$$

- es una superposición de los elementos de la base lógica $\{|0\rangle, |1\rangle\}$ de un espacio de Hilbert bi-dimensional.

Una representación del qubit está dada por la esfera de Bloch,

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

los ángulos están definidos en los intervalos $0 \leq \theta \leq \pi$ y $0 \leq \phi \leq 2\pi$.



Postulados de la mecánica cuántica

La teoría cuántica es un modelo matemático que junto con conceptos físicos, permite describir los fenómenos físicos a escala atómica.

El comportamiento de los sistemas cuánticos se describe con:

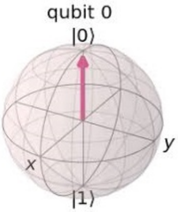
- el estado del sistema,
- la evolución del estado
- las mediciones realizadas sobre el sistema cuántico.

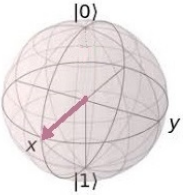
Estos conceptos toman forma con los cuatro postulados de la Mecánica Cuántica.

Postulado 1: Estado del sistema cuántico

Los estados de los sistemas físicos en mecánica cuántica son representados por **vectores** $|\psi\rangle$ en un espacio de Hilbert $\mathcal{H}$.

$|\psi\rangle = |0\rangle$





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

Un estado $|\psi\rangle$ especifica completamente nuestro conocimiento sobre el sistema físico. Todas las posibles predicciones del sistema cuántico son descritas por un **vector unitario** $|\psi\rangle$ llamado el **vector de estado**.

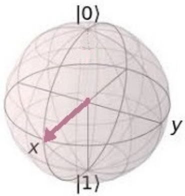
Postulado 1: Estado del sistema cuántico

Un espacio de Hilbert $\mathcal{H}$ es un espacio vectorial. Una de las propiedades de un espacio vectorial es que una combinación de vectores, en una de las bases, también es un vector.

Con la **base lógica**, $\{|0\rangle, |1\rangle\}$, podemos representar cualquier estado bi-dimensional $|\psi\rangle$

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

donde, $\langle 1|0\rangle = 0$, es decir, $|0\rangle$ y $|1\rangle$ son ortogonales.



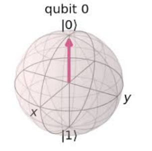
$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Postulado 1: Estado del sistema cuántico

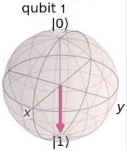
Existen infinitas bases en las cuales se puede representar o describir un vector de estado cuántico $|\psi\rangle$.

Base lógica, base Z

$|0\rangle$



$|1\rangle$

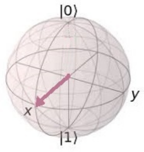


$$|\psi\rangle = a|0\rangle + b|1\rangle$$

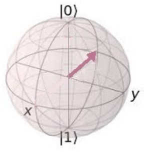
Un estado cuántico $|\psi\rangle$ se representa como una combinación lineal de los elementos de la base.

Postulado 1: Estado del sistema cuántico

Base X



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



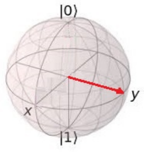
$$|x_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$|\psi\rangle = a_x|x_+\rangle + b_x|x_-\rangle$$

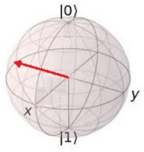
Postulado 1: Estado del sistema cuántico

Base Y

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



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



$$|\psi\rangle = a_y|y_+\rangle + b_y|y_-\rangle$$

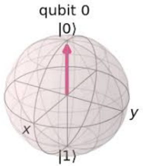
Vector de estado, ket

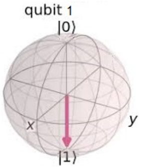
El qubit

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

se puede representar como un vector de dos componentes

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





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

Luego,

$$|\psi\rangle = a \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$$

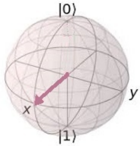
Operador cuántico, ketbra

Un operador $\hat{O}$ es un mapeo lineal de vectores sobre vectores.

$$|\psi\rangle \qquad \rightarrow \qquad \hat{O}|\psi\rangle = |\phi\rangle$$

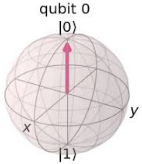
se representa por una matriz. Por ejemplo, $|0\rangle\langle 0|$ es un ketbra de la forma

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



Si inicialmente el estado es

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



El estado $|\psi\rangle$ cambia a

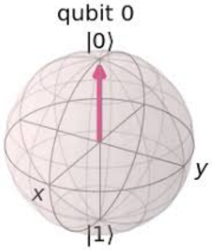
$$|0\rangle\langle 0|\psi\rangle = |0\rangle$$

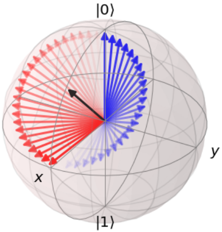
con una probabilidad 1/2

Postulado 2: Evolución unitaria

La evolución temporal de un sistema es unitaria y es generada por un operador autoadjunto llamado Hamiltoniano.

El vector que representa el estado del sistema físico puede cambiar con el paso del tiempo.





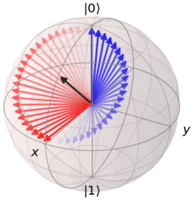
La evolución unitaria se puede representar como una rotación del vector de estado.

Postulado 2: Evolución unitaria

La evolución de un sistema cuántico aislado que no interactúa con otro sistema es

$$|\psi_f\rangle = U|\psi_i\rangle$$

$|\psi_i\rangle$ y $|\psi_f\rangle$ son los estados del sistema en el tiempo inicial y en el tiempo final. U es la transformación unitaria que transforma el estado inicial en el estado final.



Una transformación unitaria es un proceso reversible. Un operador U es unitario si se cumple que

$$UU^\dagger = U^\dagger U = \mathbb{1}$$

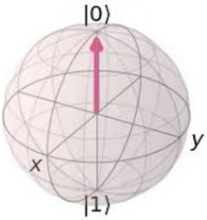
Postulado 2: Evolución unitaria

Ejemplos de operadores unitarios son las matrices de Pauli, muy usadas en computación cuántica.

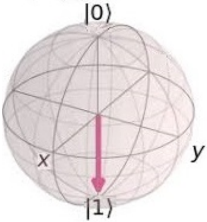
$$
\begin{aligned}
\mathbb{1} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = |0\rangle\langle 0| + |1\rangle\langle 1| \\
X &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0| \\
Y &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = i|1\rangle\langle 0| - i|0\rangle\langle 1| \\
Z &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|
\end{aligned}
$$

Postulado 2: Evolución unitaria

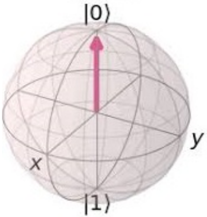
Si el estado inicial es



al aplicar el operador unitario X el estado cambia a

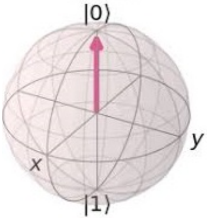


al aplicar nuevamente el operador unitario X el estado cambia a

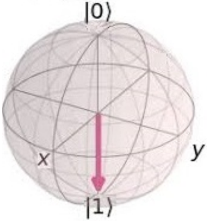


Postulado 2: Evolución unitaria

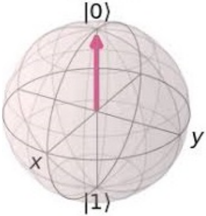
Si el estado inicial es



al aplicar el operador unitario X el estado cambia a



al aplicar nuevamente el operador unitario X el estado cambia a



Al aplicar dos veces el operador X el estado vuelve al estado inicial, esto ocurre porque

$$X \cdot X = X \cdot X^{\dagger} = \mathbb{1}$$

Es decir, el operador X es unitario.

Postulado 2: Evolución unitaria

Los operadores unitarios Z, X, Y tienen autovalores iguales a $\lambda_+ = 1$, $\lambda_- = -1$ y los respectivos autovectores son

$$
\begin{aligned}
|z_+\rangle &= |0\rangle && \text{y} && |z_-\rangle = |1\rangle \\
|x_+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) && \text{y} && |x_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
|y_+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) && \text{y} && |y_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)
\end{aligned}
$$

Postulado 2: Evolución unitaria

Los operadores unitarios Z, X, Y tienen autovalores iguales a $\lambda_+ = 1$, $\lambda_- = -1$ y los respectivos autovectores son

$$
\begin{aligned}
|z_+\rangle &= |0\rangle && \text{y} && |z_-\rangle = |1\rangle \\
|x_+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) && \text{y} && |x_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
|y_+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) && \text{y} && |y_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)
\end{aligned}
$$

Los autovalores de una matriz M se determinan desde la condición $det(M - \lambda\mathbb{1}) = 0$. Los autovectores se determinan de la condición $M|\lambda\rangle = \lambda|\lambda\rangle$.

Postulado 2: Evolución unitaria

Por ejemplo, el operador unitario X

$$X = |0\rangle\langle 1| + |1\rangle\langle 0|$$

puede ser escrito como

$$X = |x_+\rangle\langle x_+| - |x_-\rangle\langle x_-|$$

donde los estados $\{|x_+\rangle, |x_-\rangle\}$ forman una base, ya que son ortogonales $\langle x_-|x_+\rangle = 0$ y se cumple

$$|x_+\rangle\langle x_+| + |x_-\rangle\langle x_-| = \mathbb{1}$$

Postulado 3: Mediciones cuánticas

Las mediciones son descritas por un conjunto de operadores de proyección mutuamente ortogonales. Por ejemplo,

$$\{\, |0\rangle\langle 0|, |1\rangle\langle 1| \,\}$$

El resultado de la medida de un observable M es un autovalor, por ejemplo, λ_m asociado al autovector $|m\rangle$ del operador M. Si el estado antes de la medida es $|\psi\rangle$ entonces la probabilidad de obtener el resultado m es

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$$

y el estado $|\psi'\rangle$ después de la medida es $|\psi'\rangle = \dfrac{M_m|\psi\rangle}{\sqrt{p(m)}}$

Postulado 3: Mediciones cuánticas

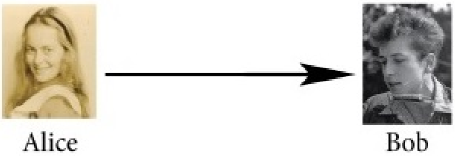
Un **observable** es una propiedad del sistema que puede ser medida. Por ejemplo, la energía, la posición o la cantidad de movimiento de una partícula.

Las medidas en mecánica cuántica:

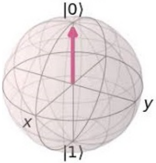
- Implican una proyección ortogonal.
- Son probabilísticas.
- En general, cambian el estado del sistema cuántico.
- En general, son un proceso irreversible. Con la cual, se obtiene información del sistema cuántico.

Postulado 3: Mediciones cuánticas

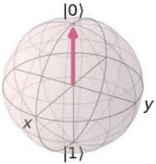
En un protocolo de comunicación cuántica Alice le envía información cuántica a Bob. De manera que Bob debe medir de manera cuántica el estado enviado por Alice.



Si Alice envía $|0\rangle$



Bob en su medida obtendrá $|0\rangle$ si mide en la base lógica.

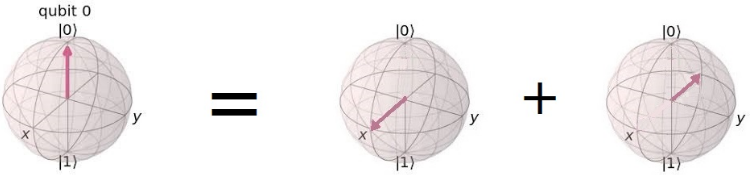


En este caso no cambia el estado.

Alice y Bob comparten 1 bit de información clásica.

Superposición cuántica.

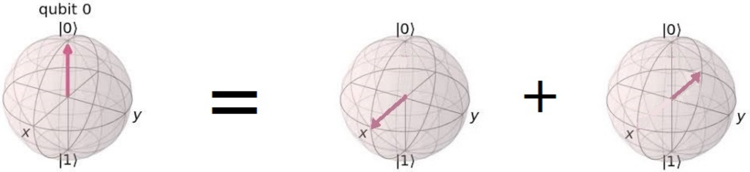
El estado puede estar simultáneamente en dos o más estados.



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

Superposición cuántica.

El estado puede estar simultáneamente en dos o más estados.



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

Si consideramos

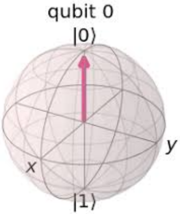
$$|x_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |x_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

entonces

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

Medida cuántica.

Las medidas cambian el estado.



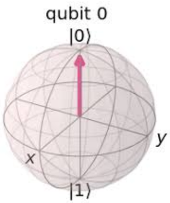
Una medida cuántica en la dirección X, nos entrega uno de los dos posibles resultados.

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad \text{ó} \qquad \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Con probabilidad $1/2$ cada uno.

Medida cuántica.

Las medidas cambian el estado.



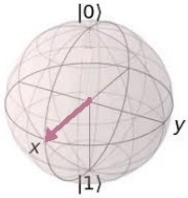
Una medida cuántica en la dirección X, nos entrega

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

Con probabilidad $1/2$.

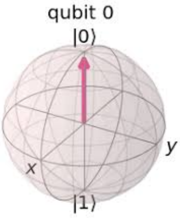
Proceso probabilista

Colapso de la función de onda!!



Medida cuántica.

Las medidas cambian el estado.



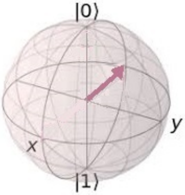
Una medida cuántica en la dirección X, nos entrega

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

Con probabilidad $1/2$.

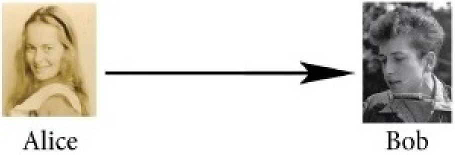
Proceso probabilista

Colapso de la función de onda!!

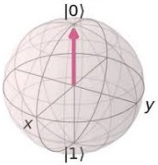


Postulado 3: Mediciones cuánticas

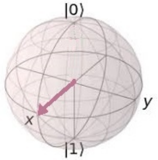
En un protocolo de comunicación cuántica Alice le envía información cuántica a Bob.



Si Alice envía $|0\rangle$



Si Bob mide en la base X, él obtendrá $|x_+\rangle$ o bien $|x_-\rangle$ con probabilidad 1/2 cada uno.



En este caso cambia el estado.

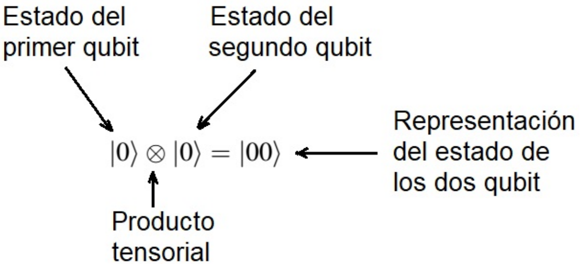
Alice y Bob no comparten información clásica.

Postulado 4: Sistemas Compuestos

El espacio de Hilbert de un sistema cuántico compuesto es el producto tensorial de los espacios de Hilbert de los componentes del sistema cuántico.

$$|\Psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle$$

Para 2-qubits el estado se expande en una base producto



Postulado 4: Sistemas Compuestos

Para 2-qubits el estado se expande en una base producto

Alice

$$
\begin{aligned}
|0\rangle \otimes |0\rangle &= |00\rangle \\
|0\rangle \otimes |1\rangle &= |01\rangle \\
|1\rangle \otimes |0\rangle &= |10\rangle \\
|1\rangle \otimes |1\rangle &= |11\rangle
\end{aligned}
$$

Bob

La base lógica de 2-qubits es $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. La forma de representar 2-qubits es

$$|\Psi\rangle = c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle$$

los coeficientes c_i en general son números complejos y que cumplen con la condición de normalización.

Ejemplo: estado separable

Alice

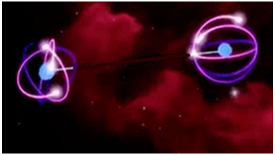
$$|\Psi\rangle_{AB} = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

Bob

Este estado se puede escribir como un estado separable

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A + |1\rangle_A) \otimes \frac{1}{\sqrt{2}}(|0\rangle_B + |1\rangle_B)$$

No hay correlación, 0 bit, entre los estados de Alice y Bob.



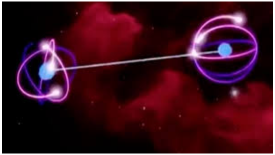
Ejemplo: estado entrelazado

Alice

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

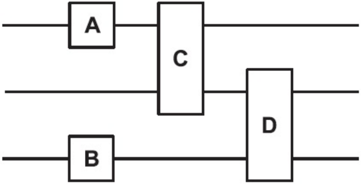
Bob

Correlación 1 bit clásico más 1 ebit un bit de entrelazamiento.



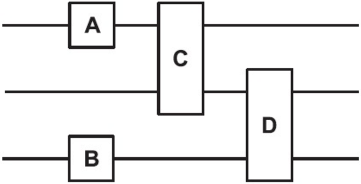
Circuito cuántico

En un circuito cuántico, podemos diseñar y en teoría construir un sistema cuántico de n qubits cuya evolución dinámica está completamente bajo nuestro control.



Circuito cuántico

En un circuito cuántico, podemos diseñar y en teoría construir un sistema cuántico de n qubits cuya evolución dinámica está completamente bajo nuestro control.



La evolución se representa como una secuencia de operadores unitarios, cada uno de los cuales actúa sobre uno o más de los qubits. La idea es que operaciones unitarias muy complicadas sobre n qubits pueden ser construidas paso por paso desde simples operaciones sobre uno, dos o unos pocos qubits.

Circuitos cuánticos

Los pasos individuales de la evolución, es decir, las operaciones elementales sobre uno, dos o más qubits son usualmente llamados compuertas cuánticas (quantum gates).

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

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

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

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

Las compuertas más simples son operaciones unitarias U que afectan a un único qubit. Por ejemplo, $\mathbb{1}$, X, Y, Z.

Circuitos cuánticos

Se considera que inicialmente todos los qubits están preparados en el estado $|0\rangle$.

Circuitos cuánticos

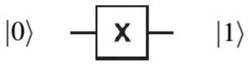
Se considera que inicialmente todos los qubits están preparados en el estado $|0\rangle$. De manera que si aplicamos la compuerta X a un qubit tenemos

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

Circuitos cuánticos

Se considera que inicialmente todos los qubits están preparados en el estado $|0\rangle$. De manera que si aplicamos la compuerta X a un qubit tenemos

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



$$|0\rangle \Rightarrow X|0\rangle \Rightarrow |1\rangle$$

Estado inicial

Estado final

Circuitos cuánticos

La compuerta Z multiplica el estado $|1\rangle$ por -1 cambiando su fase relativa con respecto al estado $|0\rangle$.

Circuitos cuánticos

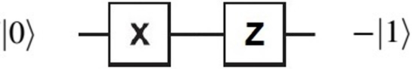
La compuerta Z multiplica el estado $|1\rangle$ por -1 cambiando su fase relativa con respecto al estado $|0\rangle$. De manera que si aplicamos la compuerta X y luego la compuerta Z a un qubit tenemos

$$Z\,X|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix} = -|1\rangle$$

Circuitos cuánticos

La compuerta Z multiplica el estado $|1\rangle$ por -1 cambiando su fase relativa con respecto al estado $|0\rangle$. De manera que si aplicamos la compuerta X y luego la compuerta Z a un qubit tenemos

$$Z\,X|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix} = -|1\rangle$$



$|0\rangle \Rightarrow Z\,X|0\rangle \Rightarrow -|1\rangle$

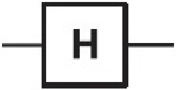
Estado inicial

Estado final

Circuitos cuánticos

Otra útil compuerta es llamada la compuerta Hadamard H, la cual en forma matricial es

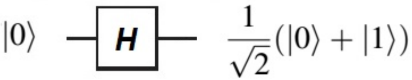
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$



Circuitos cuánticos

La compuerta Hadamard genera superposición cuántica de los qubits.

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



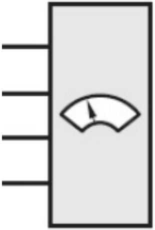
$$|0\rangle \Rightarrow H|0\rangle \Rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Estado inicial

Estado final

Circuitos cuánticos

Después de incluir todas las operaciones unitarias necesarias para generar la transformación requerida se miden todos los qubits en la base estandar o computacional. Es decir cada qubit se mide en la base $\{|0\rangle, |1\rangle\}$. Esto se representa en el circuito de la siguiente manera



Compuertas de dos qubits

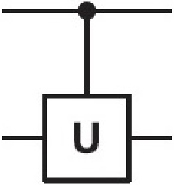
Ahora, consideramos compuertas de dos qubits. Entre las más útiles se encuentran las compuertas de control. En las compuertas de control, un qubit se emplea como control y el otro qubit se emplea como objetivo.

Compuertas de dos qubits

En las compuertas de control, un qubit se emplea como control y el otro qubit se emplea como objetivo. Esta compuerta aplica un operador unitario U al qubit objetivo si el qubit de control está en el estado $|1\rangle$. Dado que no hay una medida, tenemos un operador unitario de la forma

$$Control - U = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes U$$

Su representación de circuito es

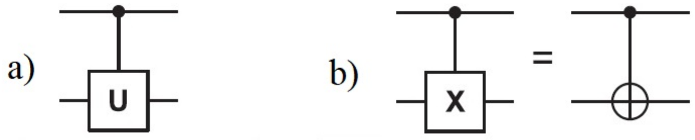


Compuertas de dos qubits

La transformación unitaria aplicada al qubits objetivo puede ser cualquiera.

Compuertas de dos qubits

La transformación unitaria aplicada al qubits objetivo puede ser cualquiera. En particular si aplicamos el operador X tenemos la compuerta CNOT (control not).



a) Compuerta control-U
b) Dos formas de representar la compuerta CNOT. En la compuerta CNOT la transformación unitaria es el operador de pauli X.

Compuertas de dos qubits

La acción de la compuerta CNOT sobre los estados de dos qubits $|0,0\rangle$ y $|1,0\rangle$ es

$$
\begin{aligned}
CNOT|0,0\rangle &= (|0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes X)|0,0\rangle \\
&= |0,0\rangle
\end{aligned}
$$

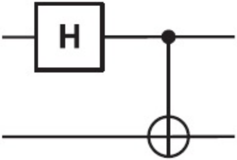
$$
\begin{aligned}
CNOT|1,0\rangle &= (|0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes X)|1,0\rangle \\
&= |1,1\rangle
\end{aligned}
$$

Con respecto a la base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ la compuerta CNOT tiene la siguiente representación matricial

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

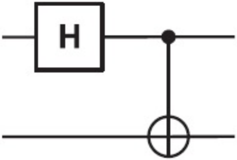
Compuertas de dos qubits

El circuito de dos qubits de la figura crea el estado de Bell maximalmente entrelazado $|\beta_{00}\rangle$ desde el estado de entrada estandar $|00\rangle$.



Compuertas de dos qubits

El circuito de dos qubits de la figura crea el estado de Bell maximalmente entrelazado $|\beta_{00}\rangle$ desde el estado de entrada estandar $|00\rangle$.



La composición de las dos transformaciones $U_T = U_2 U_1$ es

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

Compuertas de dos qubits

Si el estado inicial de entrada es $|00\rangle$, el estado final será $U_T|00\rangle = |\beta_{00}\rangle$, ya que

$$U_T|00\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Compuertas de dos qubits

Luego, si el estado inicial de entrada es $|00\rangle$, el estado final será $U_T|00\rangle = |\beta_{00}\rangle$, ya que

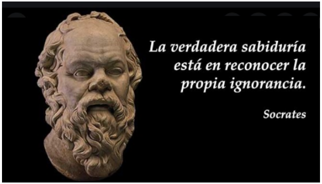
$$\begin{aligned} U_T|00\rangle &= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \\ &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\beta_{00}\rangle \end{aligned}$$

Conclusiones

- Revisamos conceptos sobre información clásica.
- Revisamos los postulados de la mecánica cuántica.
- Revisamos algunos elementos de computación cuántica.

Referencia:
Omar Jiménez. Apuntes del curso Información Cuántica I, primer semestre 2020, Universidad Mayor.

Frase célebre:
El conocimiento comienza con el asombro.
Sócrates (470-399 a.C.)



Muchas gracias.