# INTRO COMPUTACIÓN CUÁNTICA

- Un bit puede estar en estado 0 o en estado 1 y para saber en qué estado se encuentra, basta con examinarlo.

- Un qubit puede estar en estado $|0\rangle$ o en estado $|1\rangle$ (que correspon- (llamados estados básicos) den a los clásicos 0 y 1) pero también puede estar en una combinación lineal de ambos: $\alpha_0 |0\rangle + \alpha_1 |1\rangle$ donde $\alpha_0, \alpha_1 \in \mathbb{C}$ tales que $|\alpha|^2 + |\beta|^2 = 1$. (llamado superposición).

  Pero no podemos observar un qubit para conocer su estado, (es decir, conocer el valor de $\alpha$ y $\beta$) ocurre que al observarlo (medirlo) obtenemos o bien el valor 0 (con una probabilidad $|\alpha|^2$) o el valor 1 (con probabilidad $|\beta|^2$).

  [El modelo matemático para qubits consiste en ver $|0\rangle$ y $|1\rangle$ como los vectores $\begin{pmatrix}1\\0\end{pmatrix}$ y $\begin{pmatrix}0\\1\end{pmatrix}$ que forman una base de $\mathbb{C}^2$].

- El hecho de medir un qubit cambia su estado, que ya no estará en superposición, sino en estado $|0\rangle$ ó $|1\rangle$, con una medición únicamente obtenemos un bit de información.

- Podemos extender este tratamiento a múltiples qubits, por ejemplo, para dos qubits su estado es descrito como

$$\alpha_0 |00\rangle + \alpha_{01} |01\rangle + \alpha_{10}|10\rangle + \alpha_{11} |11\rangle$$

  y los estados básicos son $|00\rangle$, $|01\rangle$, $|10\rangle$ y $|11\rangle$.

- Cada coeficiente $\alpha_{ij}$ de un estado de un qubit se llama amplitud.

- Algunos estados particulares: $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ $\quad |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

  par EPR (estado de Bell): $\dfrac{|00\rangle + |11\rangle}{\sqrt{2}}$

- Para manipular la información almacenada en bits usamos puertas lógicas, p. ej NOT, que es una puerta unitaria, o AND que es una puerta binaria.

- Para manipular información sobre qubits usamos puertas cuánticas, por ejemplo el análogo a NOT sería una puerta que envíe $|0\rangle$ a $|1\rangle$, $|1\rangle$ a $|0\rangle$ y actúe linealmente $\alpha_0|0\rangle + \alpha_1|1\rangle \longrightarrow \alpha_0|1\rangle + \alpha_1|0\rangle$

  Las puertas cuánticas se modelizan algebraicamente como matrices unitarias, en el ejemplo, el análogo a NOT es $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

  Algunos ejemplos de puertas cuánticas:

  $$Z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad , \quad H \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \text{ que envía } \begin{array}{l} |0\rangle \longrightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \\ |1\rangle \longrightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \end{array}$$

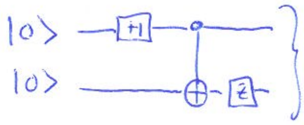
  su acción se describe como

  $$\alpha_0|0\rangle + \alpha_1|1\rangle \begin{array}{l} \xrightarrow{X} \alpha_1|0\rangle + \alpha_0|1\rangle \\ \xrightarrow{Z} \alpha_0|0\rangle - \alpha_1|1\rangle \\ \xrightarrow{H} \alpha_0 \dfrac{|0\rangle + |1\rangle}{\sqrt{2}} + \alpha_1 \dfrac{|0\rangle - |1\rangle}{\sqrt{2}} \end{array}$$

- También existen puertas de varios qubits. El ejemplo principal es CNOT cuyo efecto es $|A\,B\rangle \longrightarrow |A\ B\oplus A\rangle$ donde $A$ y $B$ son 0 y 1 y $\oplus$ es XOR o equivalentemente, suma módulo 2. El efecto se describe como: el primer qubit es llamado de control y el segundo el qubit objetivo. Si el control vale 0, el objetivo no cambia, y si el control vale 1, el objetivo se niega. El bit de control no varía.

  La matriz de CNOT es $$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

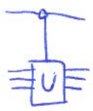
· Una concatenación de puertas cuánticas forman un circuito cuántico. Constan de ~~Se representan con~~ cables horizontales que representan los qubits, y se leen de izquierda a derecha.

ejemplo:  $\dfrac{|00\rangle + |11\rangle}{\sqrt{2}}$

ejercicio: ¿qué hace el siguiente circuito? 

solución: $|a,b\rangle \longrightarrow |b,a\rangle$

· Algunas puertas particulares que aparecen en circuitos cuánticos son:

 - Controlled-U donde U es una operación en n qubits dada por la matriz U. Es una puerta de n+1 qubits. El primero es de control, y si es 0 el resto de qubits permanecen inalterados, pero si es 1, a los n últimos qubits se les aplica U. Por ejemplo, CNOT es controlled-X.

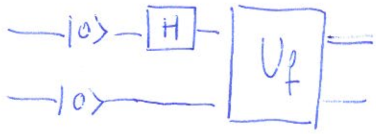
 - Medida: Convierte un qubit en estado $\alpha_0|0\rangle + \alpha_1|1\rangle$ en un bit que será 0 con probabilidad $|\alpha_0|^2$ y 1 con probabilidad $|\alpha_1|^2$. El bit clásico se representa en el circuito con un cable doble.

- Una característica fundamental de la computación cuántica es el llamado 'paralelismo cuántico'. Básicamente es la capacidad de evaluar una función $f(x)$ para diferentes valores de $x$ de forma simultánea.

Dado un par de qubits $|x,y\rangle$ podemos construir una cadena de puertas que transformen $|x,y\rangle$ en $|x, y \oplus f(x)\rangle$. El primer qubit se llama 'dato' y el segundo 'objetivo'. Esta transformación se suele denotar $U_f$ y es unitaria [ejercicio]. Si $y=0$ el estado final del bit objetivo es $f(x)$.

- Dado un circuito clásico para calcular $f$ existe un circuito cuántico de eficiencia comparable que calcula $U_f$. nos

ejemplo:



$$|00\rangle \longrightarrow \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle \longrightarrow \frac{1}{\sqrt{2}}|0, f(0)\rangle + \frac{1}{\sqrt{2}}|1, f(1)\rangle$$

En general, ~~aplicando~~ podemos preparar $n+1$ qubits en estado $|0\rangle$, aplicar una puerta Hadamard a los primeros $n$ (en realidad $H^{\otimes n}$) después aplicar $U_f$ a los $n+1$ qubits y obtendremos $\frac{1}{\sqrt{2^n}} \sum_x |x, f(x)\rangle$

- El algoritmo de Deutsch

  Dada ~~f(x)~~ $f: \{0,1\} \rightarrow \{0,1\}$ queremos saber si $f(0) = f(1)$ ó $f(0) \neq f(1)$.

  En realidad esto viene dado por el bit $f(0) \oplus f(1)$

  Usamos el siguiente circuito: