El modelo de circuitos cuánticos

Elías F. Combarro (Universidad de Oviedo)
efernandezca@uniovi.es

Universidad de Almería - Octubre 2022

Elementos de la computación cuántica

- Toda computación tiene tres elementos: datos, operaciones y resultados.
- En la computación cuántica, estos elementos se corresponden con los siguientes conceptos:
  - Datos = **qubits**
  - Operaciones = **puertas cuánticas** (transformaciones unitarias)
  - Resultados = **mediciones**
- Todos ellos se rigen por las leyes de la mecánica cuántica, por lo que pueden ser contrarios a la intuición

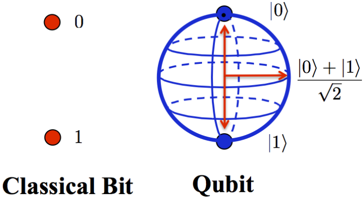
Qubits

- Un bit clásico es un elemento que puede tomar dos valores distintos (0 ó 1). Es discreto.
- Un qubit puede "tener" **infinitos** valores. Es continuo.
- Los qubits viven en un **espacio vectorial de Hilbert** que tiene por base dos elementos que denotamos $|0\rangle$ y $|1\rangle$.
- Un qubit genérico tiene la forma de una **superposición**

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

donde α y β son **números complejos** que cumplen

$$|\alpha|^2 + |\beta|^2 = 1$$



Medida de un qubit

- La única forma de conocer el estado de un qubit es realizar una medida. Sin embargo:
  - El resultado de la medida es aleatorio
  - Al medir, solo obtenemos un bit (clásico) de información
- Si medimos el estado $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ obtendremos 0 con probabilidad $|\alpha|^2$ y 1 con probabilidad $|\beta|^2$.
- Además, el nuevo estado de $|\psi\rangle$ después de realizar la medida será $|0\rangle$ o $|1\rangle$ según el resultado que se haya obtenido (colapso de la función de onda)
- Es más, no podemos realizar varias medidas de $|\psi\rangle$ porque no se puede copiar el estado (**teorema de no clonación**)

La esfera de Bloch

- Una forma habitual de representar el estado de un qubit es mediante la llamada esfera de Bloch
- Si $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ con $|\alpha|^2 + |\beta|^2 = 1$ podemos encontrar ángulos γ, δ, θ tales que

$$\alpha = e^{i\gamma} \cos \frac{\theta}{2}$$

$$\beta = e^{i\delta} \sin \frac{\theta}{2}$$

- Como las fases globales son físicamente irrelevantes, podemos reescribir

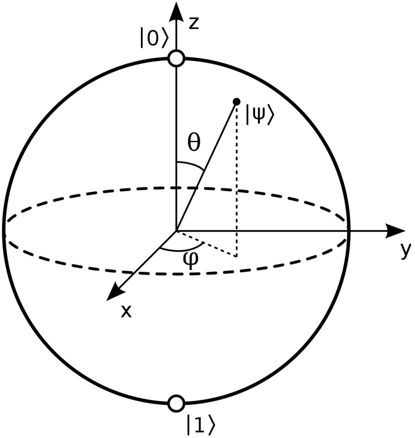
$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle$$

con $0 \leq \theta \leq \pi$ y $0 \leq \varphi < 2\pi$.

La esfera de Bloch (2)

- De los ángulos en $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$ podemos obtener coordenadas esféricas para un punto en $\mathbb{R}^3$

$$(\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$$



Producto escalar, notación de Dirac y esfera de Bloch

- El producto escalar de dos estados $|\psi_1\rangle = \alpha_1 |0\rangle + \beta_1 |1\rangle$ and $|\psi_2\rangle = \alpha_2 |0\rangle + \beta_2 |1\rangle$ viene dado por

$$\langle\psi_1|\psi_2\rangle = \left(\overline{\alpha_1}\ \overline{\beta_1}\right)\begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix} = \overline{\alpha_1}\alpha_2 + \overline{\beta_1}\beta_2$$

- Nótese que $\langle 0|0\rangle = \langle 1|1\rangle = 1$ and $\langle 0|1\rangle = \langle 1|0\rangle = 0$
- Esto nos permite calcular del siguiente modo

$$\begin{aligned}\langle\psi_1|\psi_2\rangle &= \left(\overline{\alpha_1}\langle 0| + \overline{\beta_1}\langle 1|\right)\left(\alpha_2|0\rangle + \beta_2|1\rangle\right)\\ &= \overline{\alpha_1}\alpha_2\langle 0|0\rangle + \overline{\alpha_1}\beta_2\langle 0|1\rangle + \overline{\beta_1}\alpha_2\langle 1|0\rangle + \overline{\beta_1}\beta_2\langle 1|1\rangle\\ &= \overline{\alpha_1}\alpha_2 + \overline{\beta_1}\beta_2\end{aligned}$$

- Puntos antipodales en la esfera de Bloch se corresponden con estados ortogonales

Puertas cuánticas

- Las leyes de la mecánica cuántica nos dicen que la evolución de un sistema responde a la ecuación de Schrödinger (si no se realiza una medida).

$$H(t)|\psi(t)\rangle = i\hbar\frac{\partial}{\partial t}|\psi(t)\rangle$$

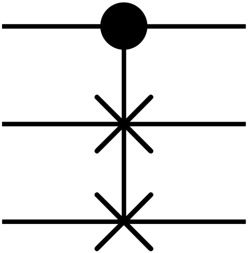
- En el caso de la computación cuántica, esto implica que las operaciones que se pueden realizar son transformaciones lineales que vienen dadas por matrices unitarias. Es decir, matrices U de números complejos que verifican

$$UU^\dagger = U^\dagger U = I$$

  donde $U^\dagger$ es la transpuesta conjugada de U.
- Cada matriz de este tipo es una posible puerta cuántica en un circuito cuántico

Computación reversible

- Como consecuencia, todas las operaciones tienen una inversa: **computación reversible**
- Todas las puertas tienen el mismo número de entradas que de salidas
- No podemos implementar directamente operaciones como *or*, *and*, *nand*, *xor*...
- Teóricamente, podríamos realizar cualquier computación sin gastar energía



Puertas cuánticas de un qubit

- Si tenemos un solo qubit $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$, habitualmente lo representamos como un vector columna $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$
- Entonces, una puerta cuántica de un qubit se corresponderá con una matriz $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ que verifica

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

siendo $\overline{a}, \overline{b}, \overline{c}, \overline{d}$ los conjugados de los números complejos a, b, c, d.

Acción de una puerta cuántica de un qubit

- Un estado $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ es transformado en

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} a\alpha + b\beta \\ c\alpha + d\beta \end{pmatrix}$$

  es decir, en el estado $|\psi\rangle = (a\alpha + b\beta)\,|0\rangle + (c\alpha + d\beta)\,|1\rangle$
- Como U es unitaria, se cumple que

$$|(a\alpha + b\beta)|^2 + |(c\alpha + d\beta)|^2 = 1$$

La puerta *X* o *NOT*

- La puerta *X* viene definida por la matriz (unitaria)

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

- Su acción es (notación del modelo de circuitos)

$$|0\rangle \;-\boxed{X}-\; |1\rangle$$

$$|1\rangle \;-\boxed{X}-\; |0\rangle$$

  es decir, actúa como un *NOT*

- Su acción sobre un qubit general sería

$$\alpha\,|0\rangle + \beta\,|1\rangle \;-\boxed{X}-\; \beta\,|0\rangle + \alpha\,|1\rangle$$

La puerta H

- La puerta H o puerta de Hadamard viene definida por la matriz (unitaria)

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

- Su acción es

$$|0\rangle \;-\!\boxed{H}\!-\; \tfrac{|0\rangle+|1\rangle}{\sqrt{2}}$$

$$|1\rangle \;-\!\boxed{H}\!-\; \tfrac{|0\rangle-|1\rangle}{\sqrt{2}}$$

- Se suele denotar

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

y

$$|-\rangle := \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

La puerta Z

- La puerta Z viene definida por la matriz (unitaria)

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

- Su acción es

$$|0\rangle \quad -\boxed{Z}- \quad |0\rangle$$

$$|1\rangle \quad -\boxed{Z}- \quad -|1\rangle$$

Otras puertas

- Puerta Y

$$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

- Puerta T

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$

- Puerta S

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{pmatrix}$$

- La puerta $R(\alpha)$ o puerta de fase, que depende de un parámetro (el ángulo α)

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$$

Puertas de rotación

- Podemos definir las siguientes puertas de rotación

$$R_X(\theta) = e^{-i\frac{\theta}{2}X} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$

$$R_Y(\theta) = e^{-i\frac{\theta}{2}Y} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Y = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$

$$R_Z(\theta) = e^{-i\frac{\theta}{2}Z} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

- Se cumple que $R_X(\pi) \equiv X$, $R_Y(\pi) \equiv Y$, $R_Z(\pi) \equiv Z$, $R_Z(\frac{\pi}{2}) \equiv S$, $R_Z(\frac{\pi}{4}) \equiv T$

Usando las puertas de rotación para generar puertas de un qubit

- Para cada puerta U de un qubit, existe un vector $r = (r_x, r_y, r_z)$ de longitud 1 y un ángulo θ tal que

$$U \equiv e^{-i\frac{\theta}{2} r\cdot\sigma} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2}(r_x X + r_y Y + r_z Z)$$

- Por ejemplo, eligiendo $\theta = \pi$ y $r = (\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}})$ se puede ver que

$$H \equiv e^{-i\frac{\theta}{2} r\cdot\sigma} = -i\frac{1}{\sqrt{2}}(X + Z)$$

- Además, se puede demostrar que existen ángulos α, β y γ tales que

$$U \equiv R_Z(\alpha) R_Y(\beta) R_Z(\gamma)$$

Trabajando con dos qubits

- Cada qubit puede estar en los estados $|0\rangle$ y $|1\rangle$
- Así que para dos qubits tenemos cuatro posibilidades:

$$|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle$$

que también se denotan

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

o

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle$$

- Como podemos tener superposiciones, un estado genérico del sistema será

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

donde los α_{xy} son números complejos que cumplen

$$\sum_{x,y=0}^{1} |\alpha_{xy}|^2 = 1$$

Medida de un estado de dos qubits

- Tenemos un estado

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

- Si medimos ambos qubits, obtendremos:
  - 00 con probabilidad $|\alpha_{00}|^2$ y el nuevo estado será $|00\rangle$
  - 01 con probabilidad $|\alpha_{01}|^2$ y el nuevo estado será $|01\rangle$
  - 10 con probabilidad $|\alpha_{10}|^2$ y el nuevo estado será $|10\rangle$
  - 11 con probabilidad $|\alpha_{11}|^2$ y el nuevo estado será $|11\rangle$
- Es una situación análoga a la que teníamos con un solo qubit, pero ahora con cuatro posibilidades

Medida de un qubit en un estado de dos qubits

- Sobre un estado

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

  también podemos medir solo un qubit
- Si medimos el primer qubit (el segundo es análogo):
  - Obtendremos 0 con probabilidad $|\alpha_{00}|^2 + |\alpha_{01}|^2$
  - En ese caso, el nuevo estado de $|\psi\rangle$ será

$$\frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

  - Obtendremos 1 con probabilidad $|\alpha_{10}|^2 + |\alpha_{11}|^2$
  - En ese caso, el nuevo estado de $|\psi\rangle$ será

$$\frac{\alpha_{10}|10\rangle + \alpha_{11}|11\rangle}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}}$$

Puertas cuánticas de dos qubits

- Un estado de dos qubits es

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

- Se representa mediante el vector columna

$$\begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix}$$

- Podemos calcular productos escalares teniendo en cuenta que

$$\langle 00|00\rangle = \langle 01|01\rangle = \langle 10|10\rangle = \langle 11|11\rangle = 1$$

$$\langle 00|01\rangle = \langle 00|10\rangle = \langle 00|11\rangle = \cdots = \langle 11|00\rangle = 0$$

- Una puerta cuántica de dos qubits es una matriz unitaria U de tamaño 4×4

Productos tensoriales de puertas de un qubit

- Podemos obtener una puerta de dos qubits haciendo actuar dos puertas de un qubit, A y B, simultáneamente sobre cada uno de ellos
- En este caso, la matriz de la puerta de dos qubits es el producto tensorial $A \otimes B$
- Se verifica que

$$(A \otimes B)(|\psi_1\rangle \otimes |\psi_2\rangle) = (A\,|\psi_1\rangle) \otimes (B\,|\psi_2\rangle)$$

- Por supuesto, A o B podrían ser la identidad
- NO todas las puertas de dos qubits son productos tensoriales de puertas de un qubit

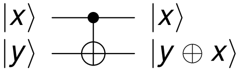
$$\begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{bmatrix} \otimes \begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} = \begin{bmatrix} a_{1,1}\begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} & a_{1,2}\begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} \\ a_{2,1}\begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} & a_{2,2}\begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} \end{bmatrix} = \begin{bmatrix} a_{1,1}b_{1,1} & a_{1,1}b_{1,2} & a_{1,2}b_{1,1} & a_{1,2}b_{1,2} \\ a_{1,1}b_{2,1} & a_{1,1}b_{2,2} & a_{1,2}b_{2,1} & a_{1,2}b_{2,2} \\ a_{2,1}b_{1,1} & a_{2,1}b_{1,2} & a_{2,2}b_{1,1} & a_{2,2}b_{1,2} \\ a_{2,1}b_{2,1} & a_{2,1}b_{2,2} & a_{2,2}b_{2,1} & a_{2,2}b_{2,2} \end{bmatrix}$$

La puerta *CNOT*

- La puerta *CNOT* (controlled-NOT) viene definida por la matriz (unitaria)
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$
- Si el primer qubit es $|0\rangle$, no se hace nada. Si es $|1\rangle$, se invierte el segundo qubit (y el primero queda igual)
- Es decir:
$$|00\rangle \to |00\rangle \qquad |01\rangle \to |01\rangle$$
$$|10\rangle \to |11\rangle \qquad |11\rangle \to |10\rangle$$

La puerta *CNOT*

- Su acción con elementos $x, y \in \{0, 1\}$ es, por tanto:



- Es una puerta muy importante, puesto que nos permite:
  - Realizar entrelazamientos
  - Copiar información clásica, ya que:

$$|00\rangle \rightarrow |00\rangle$$

$$|10\rangle \rightarrow |11\rangle$$

Sistemas de n qubits

- Cada uno de los n qubits puede estar en los estados $|0\rangle$ y $|1\rangle$
- Así que para el conjunto de los n qubits tenemos 2^n posibilidades:

$$|00\ldots0\rangle\,, |00\ldots1\rangle\,, \ldots, |11\ldots1\rangle$$

  o simplemente

$$|0\rangle\,, |1\rangle\,, \ldots, \left|2^n-1\right\rangle$$

- Un estado genérico del sistema será

$$|\psi\rangle = \alpha_0\,|0\rangle + \alpha_1\,|1\rangle + \ldots + \alpha_{2^n-1}\left|2^n-1\right\rangle$$

  donde los α_i son números complejos que cumplen

$$\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$$

Medida de un estado de *n* qubits

- Supongamos que tenemos un estado genérico de *n* qubits

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \ldots + \alpha_{2^n-1} \left|2^n - 1\right\rangle$$

- Si medimos todos los qubits, obtendremos:
    - 0 con probabilidad $|\alpha_0|^2$ y el nuevo estado será $|0\ldots 00\rangle$
    - 1 con probabilidad $|\alpha_1|^2$ y el nuevo estado será $|0\ldots 01\rangle$
    - $\ldots$
    - $2^n - 1$ con probabilidad $|\alpha_{2^n-1}|^2$ y el nuevo estado será $|1\ldots 11\rangle$
- Es una situación análoga a la que teníamos con un solo qubit, pero ahora con 2^n posibilidades

Medida de un qubit en un estado de *n* qubits

- Tenemos un estado

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \ldots + \alpha_{2^n-1} \left|2^n - 1\right\rangle$$

- Si medimos el qubit j-ésimo
  - Obtendremos 0 con probabilidad

$$\sum_{i \in I_0} |\alpha_i|^2$$

    donde I_0 es el conjunto de números i cuyo j-ésimo bit es 0
  - En ese caso, el nuevo estado de $|\psi\rangle$ será

$$\frac{\sum_{i \in I_0} \alpha_i |i\rangle}{\sqrt{\sum_{i \in I_0} |\alpha_i|^2}}$$

  - El caso en el que se obtiene 1 es análogo

Puertas cuánticas de n qubits

- Un estado de n qubits es

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \ldots + \alpha_{2^n-1} \left|2^n - 1\right\rangle$$

- Se representa mediante el vector columna

$$\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{2^n-1} \end{pmatrix}$$

- Para calcular productos escalares en notación de Dirac basta notar que

$$\langle i|j\rangle = \delta_{ij}$$

- Una puerta cuántica de dos qubits es una matriz unitaria U de tamaño $2^n \times 2^n$

Puertas universales en la computación cuántica

- El número de puertas cuánticas (incluso para un solo qubit) es infinito no numerable. Por tanto, ningún conjunto finito de puertas es universal en el sentido tradicional del término
- Lo que sí se puede conseguir son familias de puertas que **aproximan** cualquier puerta cuántica tanto como queramos

Teorema

Las puertas X, H, T y $CNOT$ son universales para la computación cuántica

- Y podemos tener conjuntos de puertas infinitos en uno y dos qubits que son universales

Teorema

Las puertas de rotación de un qubit junto con la puerta CNOT son universales para la computación cuántica