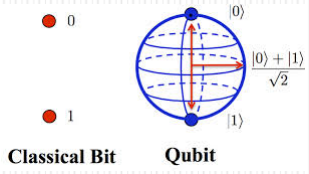
Computación y Criptografía Cuánticas

Alfonsa García, Francisco García[1] y Jesús García[1]
[1]Grupo de investigación en Información y Computación Cuántica (GIICC)



Modelo cuántico de computación

1. Introducción
2. Representación de la información
3. Estados de 2-qubits. Entrelazamiento
4. Estados de n-qubits
5. Transformación de la información. Puertas cuánticas
6. Teorema de no-cloning

1. Introducción

- La computación cuántica surgió, a principios de los 80 del siglo pasado, de la necesidad de simular procesos cuánticos, lo que supone un coste computacional inabordable para un ordenador clásico.
- Propuestas de Benioff, Deutsh y Feynman: La evolución de un sistema cuántico se puede considerar como herramienta de cálculo.
- El algoritmo de Shor (1994) abre la posibilidad de que los ordenadores cuánticos puedan romper el criptosistema RSA.

R. Feynman

P.W. Shor

2. Representación de la información

La unidad de información en computación cuántica es el qubit: $|0\rangle$, $|1\rangle$

Se representa mediante un sistema cuántico de dos estados.
Por ejemplo el spin de un electrón, o la polarización de la luz.

Un estado cuántico puede ser superposición de los dos estados básicos:

$\phi = a|0\rangle + b|1\rangle$ con a, b números complejos tales que $|a|^2 + |b|^2 = 1$

Un estado cuántico de un qubit es un vector unitario de un espacio de Hilbert bidimensional complejo **H**

$B_1 = [|0\rangle, |1\rangle]$ es base ortonormal del espacio de Hilbert

Medir un estado de un qubit

Sistema de medida ⟷ Base ortonormal

Se mide

Instrumento de medida

$\phi = a|0\rangle + b|1\rangle$ $\quad B_1 = [|0\rangle, |1\rangle]$

Medida	Estado resultante	Probabilidad
0	$\frac{a}{\|a\|}\|0\rangle$	$\|a\|^2$
1	$\frac{b}{\|b\|}\|1\rangle$	$\|b\|^2$

Cuando se mide un estado, se modifica de modo irreversible proyectándose sobre uno de los estados de la base

Medir con otra base ortonormal

$B_X = [|+\rangle, |-\rangle]$ $\quad |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ $\quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

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

Estado	Medido con B_1 se obtiene	Medido con B_X se obtiene
$\|0\rangle$	$\|0\rangle$, con probabilidad p=1	$\|+\rangle$ con prob. p=1/2 $\|-\rangle$ con prob. p=1/2
$\|1\rangle$	$\|1\rangle$, con probabilidad p=1	$\|+\rangle$ con prob. p=1/2 $\|-\rangle$ con prob. p=1/2
$\|+\rangle$	$\|0\rangle$, con probabilidad p=1/2 $\|1\rangle$, con probabilidad p=1/2	$\|+\rangle$ con prob. p=1
$\|-\rangle$	$\|0\rangle$, con probabilidad p=1/2 $\|1\rangle$, con probabilidad p=1/2	$\|-\rangle$ con prob. p=1

3. Estados de 2-qubits. Entrelazamiento

Un 2-qubit es un vector de norma 1 de Hilbert $H_2 = H \otimes H$

Una base ortonormal de este espacio es

$$B_2 = [|00\rangle, |01\rangle, |10\rangle, |11\rangle]$$

Si no ha lugar a confusión, se puede escribir B_2=[|0>,|1>,|2>,|3>]

Hay estados de $\mathbf{H_2}$, que son producto tensorial de 2 estados de 1-qubit

$$\frac{1}{4}|00\rangle - \frac{\sqrt{3}}{4}|01\rangle + \frac{\sqrt{3}}{4}|10\rangle - \frac{3}{4}|11\rangle = \left(\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right) \otimes \left(\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle\right)$$

Y estados entrelazados (entangled) que no se pueden poner como producto tensorial de dos estados de 1-qubit

Un ejemplo de estado entrelazado

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

No puede haber números complejos a,b,c,d tales que

$$(a\,|\,0\rangle > + b\,|\,1\rangle) \otimes (c\,|\,0\rangle + d\,|\,1\rangle) = \frac{1}{\sqrt{2}}(|\,00\rangle + |\,11\rangle)$$

Ya que para que esto ocurra debería ser

$$ac \neq 0,\ bd \neq 0,\ ad = 0,\ bc = 0$$

… y esto es imposible

Medir un qubit en un estado de 2-qubits

Usamos B_1 para medir el primer qubit de $\phi = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ (con $|a|^2+|b|^2+|c|^2+|d|^2=1$)

Medida:	Probabilidad:	Estado resultante
0	$\|a\|^2+\|b\|^2$	$\frac{a}{\sqrt{\|a\|^2+\|b\|^2}}\|00\rangle + \frac{b}{\sqrt{\|a^2+\|b\|^2}}\|01\rangle$
1	$\|c\|^2+\|d\|^2$	$\frac{c}{\sqrt{\|c\|^2+\|d\|^2}}\|10\rangle + \frac{d}{\sqrt{\|c^2+\|d\|^2}}\|11\rangle$

Si el estado es entrelazado

$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

Medida:	Prob:	Est. resultante
$\|0\rangle$	1/2	$\|00\rangle$
$\|1\rangle$	1/2	$\|11\rangle$

Si se mide el segundo qubit se obtiene el mismo resultado de la medida con probabilidad 1.

Paradoja EPR (Einstein, Podolsky, Rosen)

4. Estados de n-qubits

Un n-qubit es un vector unitario del espacio $\mathbf{H}_n = \mathbf{H} \otimes \overset{(n)}{\ldots} \otimes \mathbf{H}$.

Una base

$$B_n = [|x_j\rangle, j = 1..2^n - 1], \text{ con } x_j \in \{0,1\}^n$$

Un estado: $\phi = \sum_{j=0}^{2^n-1} a_j |x_j\rangle$, $\sum_{j=0}^{2^n-1} |a_j|^2 = 1$.

Notación: Si no hay lugar a confusión escribiremos:

$$B_n = [|0\rangle, \cdots, |2^n - 1\rangle] \text{ y } \phi = \sum_{j=0}^{2^n-1} a_j |j\rangle.$$

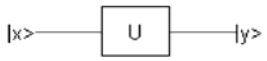
Medir el qubit k-ésimo en un n-qubit

Estado	Medida	Estado final	Probabilidad
$\sum_{0 \le x < 2^n} a_x \lvert x\rangle$	0	$\frac{1}{\sqrt{p_0}} \sum_{\substack{0 \le x < 2^n \\ x_k = 0}} a_x \lvert x\rangle$	$p_0 = \sum_{\substack{0 \le x < 2^n \\ x_k = 0}} \lvert a_x\rvert^2$
$\sum_{0 \le x < 2^n} a_x \lvert x\rangle$	1	$\frac{1}{\sqrt{p_1}} \sum_{\substack{0 \le x < 2^n \\ x_k = 1}} a_x \lvert x\rangle$	$p_1 = \sum_{\substack{0 \le x < 2^n \\ x_k = 1}} \lvert a_x\rvert^2$

5. Transformación de la información

Transformaciones cuánticas →operadores unitarios

Puertas de un qubit:



Como son aplicaciones lineales, para describir una puerta cuántica, basta conocer las imágenes de los elementos de la base (B_1).

Ejemplos

Identidad: $I(|0\rangle) = |0\rangle$, $I(|1\rangle) = |1\rangle$

Negación: $X(|0\rangle) = |1\rangle$, $X(|1\rangle) = |0\rangle$

Cambio de fase: $Z(|0\rangle) = |0\rangle$, $Z(|1\rangle) = -|1\rangle$

Hadamard: $H(|0\rangle) = |+\rangle$, $H(|1\rangle) = |-\rangle$

Expresiones matriciales

Matrices de Pauli:

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

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

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

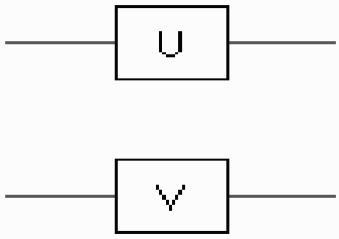
Las transformaciones ortogonales son reversibles. La matriz asociada a la transformación inversa de U es la matriz inversa de la asociada a U.

Se verifica que *HXH=Z y HZH=X*

Puertas de 2-qubits

Una puerta de 2-qubits es una transformación ortogonal en $\mathbf{H}_2$ que, por ejemplo, puede ser el producto tensorial de puertas de 1-qubit:

$$U \otimes V(|x_1 x_2\rangle) = U(|x_1\rangle) \otimes V(|x_2\rangle)$$



La matriz asociada es el producto tensorial de las matrices

Ejemplos:

1. **Negación en el primer qubit**:

$$X_1 = X \otimes I$$

$$X_1 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

2. **Transformación Walsh-Hadamard**:

$$W_2 = H \otimes H$$

$$W_2 = \begin{pmatrix} 1/2 & 1/2 & 1/2 & 1/2 \\ 1/2 & -1/2 & 1/2 & -1/2 \\ 1/2 & 1/2 & -1/2 & -1/2 \\ 1/2 & -1/2 & -1/2 & 1/2 \end{pmatrix}$$

$$W_2(|00\rangle) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

Puertas C_{NOT}

Negación condicionada → cambia un bit cuando el otro es 1.
Es una puerta de 2-qubits que no es producto tensorial de dos puertas de 1 qubit

$$C_{12}|x_1x_2\rangle = |x_1\, x_1 \oplus x_2\rangle, \qquad C_{21}|x_1x_2\rangle = |x_1 \oplus x_2\, x_2\rangle$$

La negación condicionada y las puertas de 1-qubit constituyen un sistema universal de puertas cuánticas.

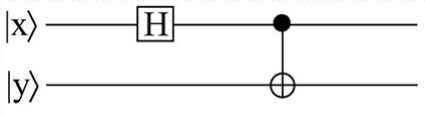
$$C_{12} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad C_{21} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Preparación de un estado entrelazado

Se puede construir un estado entrelazado, partiendo de $|00\rangle$ aplicando *H* en el primer qubit y luego C_{12}

$$H \otimes I(|00>) = \frac{1}{\sqrt{2}}(|00> + |10>)$$

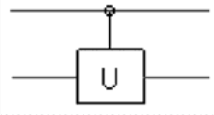
$$C_{12}\left(\frac{1}{\sqrt{2}}(|00> + |10>)\right) = \frac{1}{\sqrt{2}}(|00> + |11>)$$



Puerta control-U

Para cualquier puerta de 1-qubit U se puede definir la puerta de 2-qubits que hace actuar U sobre el segundo usando el primero como qubit de control.

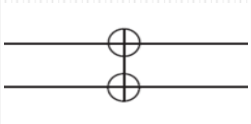
$$\Lambda U|0x\rangle = |0x\rangle, \qquad \Lambda U|1x\rangle = |1\rangle \otimes U|x\rangle.$$



$$C_{12} = \Lambda X$$

Puerta Swap

$$S|x_1x_2\rangle = |x_2x_1\rangle$$



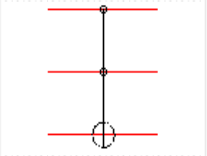
$$S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Esta transformación se puede poner como composición de puertas C_{NOT}

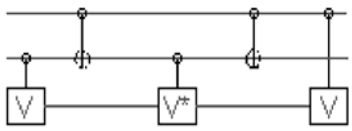
$$S = C_{12}C_{21}C_{12}$$

Puerta de Toffoly

Transformación de 3-qubits que cambia el tercero cuando los dos primeros son iguales a 1.



Se puede construir con puertas C_{NOT} y control-U



$V^2=X$

La puerta de Toffoly es universal para la computación booleana, ya que permite implementar la negación y el AND :

$$T(|1,1,x\rangle) = |1,1,\overline{x}\rangle \qquad T(|x,y,0\rangle) = |x,y,x \wedge y\rangle$$

Otras transformaciones unitarias

Transformación Walsh-Hadamard de n-qubits:

$$W_n = H \otimes \overset{(n}{\cdots} \otimes H \qquad W_n(|0\rangle) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

Transformación cuántica asociada a una función booleana:

$$f : \{0,1\}^n \to \{0,1\}^m \qquad U_f : \mathcal{H}_{n+m} \to \mathcal{H}_{n+m}$$

$$U_f(|x\rangle \otimes |b\rangle) = |x\rangle \otimes |b \oplus f(x)\rangle$$

Ejemplo

$$f : \{0,1\} \to \{0,1\} \longrightarrow U_f : \mathcal{H}_2 \to \mathcal{H}_2,$$

$$U_f(|x\rangle \otimes |b\rangle) = |x\rangle \otimes |b \oplus f(x)\rangle$$

Con $|b\rangle = |0\rangle$ $\longrightarrow$ $U_f(|x\rangle \otimes |0\rangle) = |x\rangle \otimes |f(x)\rangle$

Si ponemos $|b\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$,

$$U_f|0,b\rangle = \frac{1}{\sqrt{2}}(U_f|0,0\rangle + U_f|0,1\rangle) = \frac{1}{\sqrt{2}}(|0,f(0)\rangle + |0,f(1)\rangle)$$

Tenemos $f(0)$ y $f(1)$ en un solo qubit (ésta es la base del paralelismo cuántico)

6. Teorema de no cloning

No existe $U : \mathcal{H}_{2n} \to \mathcal{H}_{2n}$ tal que $U(\Psi \otimes |0\rangle) = \Psi \otimes \Psi$ para todo n-qubit Ψ.

Demostración. Sea U una transformación unitaria $U : \mathcal{H}_{2n} \to \mathcal{H}_{2n}$ tal que $U(|a\rangle \otimes |0\rangle) = |a\rangle \otimes |a\rangle$ y $U(|b\rangle \otimes |0\rangle) = |b\rangle \otimes |b\rangle$ tal que $a \neq b$ y $0 \leq a, b < 2^n$.

Consideremos el n-qubit $\Psi = \frac{1}{\sqrt{2}}(|a\rangle + |b\rangle)$. Entonces

$$U(\Psi \otimes |0\rangle) = \frac{1}{\sqrt{2}}(U(|a\rangle \otimes |0\rangle) + U(|b\rangle \otimes |0\rangle)) = \frac{1}{\sqrt{2}}(|a\rangle \otimes |a\rangle + |b\rangle \otimes |b\rangle) \neq \Psi \otimes \Psi$$

No existe una “fotocopiadora” cuántica