Modelo de Computación Cuántica

Jesús García López de Lacalle

Grupo de Investigación
Mathematical Modeling and Biocomputing (MMBC)

ETS de Ingeniería de Sistemas Informáticos

Universidad Politécnica de Madrid

jglopez@etsisi.upm.es

Modelo de Computación Cuántica

1. Un poco de historia...
2. Unidad de información cuántica
3. Qubits entrelazados
4. Puertas cuánticas
5. Propiedades de los qubits:
   - Imposibilidad de copiar qubits
   - Qubits no distinguibles
   - Teletransporte de qubits
6. Algoritmos cuánticos básicos
   - Problema de Deutsch
   - Problema de Deutsch-Jozsa
   - Problema de Simon

1. Un poco de historia...

Los inicios de la computación cuántica

- Paul Benioff (1982):

  Quantum mechanical Hamiltonian models of Turing machines,
  J. Stat. Phys. **29**, (1982)

- David Deutsch (1985):

  Quantum theory, the Church-Turing principle and the universal quantum computer,
  Proc. of the Royal Society of London Ser. A, **A400**, (1985)

- Richard Feynman (1982):

  Simulating physics with computers,
  International Journal of Theoretical Physics **21**, 6-7, (1982)

1. Un poco de historia...

Los inicios de la criptografía cuántica

- Stephen Wiesner (196...):

  Conjugate coding,
  Sigact News, **15** (1), (1983)

- Charles H. Bennett y Gilles Brassard (1984):

  Quantum cryptography: Public key distribution and coin tossing,
  IEEE Int. Conf. on Computers, Systems and Signal Processing, (1984)

- Artur K. Ekert (1991):

  Quantum Cryptography Based on Bell's Theorem,
  Phys. Rev. Lett., **67** (661), (1991)

- Charles H. Bennett (1992):

  Quantum cryptography using any two nonorthogonal states,
  Phys. Rev. Lett., **68** (21), (1992)

1. Un poco de historia...

Algoritmos cuánticos importantes

- Lov K. Grover (1995):

  Quantum mechanics helps in searching for a needle in a haystack,
  Phys. Rev. Lett., **79** (2), (1997)

  Determinar si un elemento pertenece o no a un conjunto desordenado de tamaño N

  $$O\left(\sqrt{N}\right)$$

- Peter W. Shor (1994):

  Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comp., **26** (5), (1997)

  - Calcular un divisor no trivial de un entero N
  - Calcular el logaritmo discreto en base B de A módulo N

  $$O\left(\log^4(N)\log\log(N)\right)$$

2. Unidad de información cuántica

Representación de la información

Unidad elemental de información:

- **bit**: $b = 0$ ó 1
- **qubit**: $q = |0\rangle, |1\rangle$ ó $a|0\rangle + b|1\rangle$ con $a, b \in \mathbb{C}$ $(|a|^2 + |b|^2 = 1)$

$q \in H = L(|0\rangle, |1\rangle)$, $B_1 = [\,|0\rangle, |1\rangle\,]$ base de computación (ortonormal)

Implementación física de un qubit:

- En criptografía el soporte físico es un fotón:

$|0\rangle =$ polarización horizontal del fotón

$|1\rangle =$ polarización vertical del fotón

- En computación el soporte físico es un ión:

$|0\rangle =$ espín del electrón externo $-1/2$

$|1\rangle =$ espín del electrón externo $+1/2$

2. Unidad de información cuántica

Lectura de la información

- Consideremos el qubit $q = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$
- Al medirlo sólo pueden darse dos resultados: $|0\rangle$ ó $|1\rangle$
- La medida del qubit q es un experimento aleatorio:

Estado final	Probabilidad	Medida
$\|0\rangle$	$p_0 = \left\|\frac{1}{2}\right\|^2 = \frac{1}{4}$	0
$\|1\rangle$	$p_1 = \left\|\frac{\sqrt{3}}{2}\right\|^2 = \frac{3}{4}$	1

2. Unidad de información cuántica

Representación de un $\mathbf{2}-$qubit

- $q = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$
- $q \in H^2 = L(\,|00\rangle, |01\rangle, |10\rangle, |11\rangle\,)$
- $H^2 = H \otimes H$ y $|00\rangle = |0\rangle \otimes |0\rangle, \ldots |11\rangle = |1\rangle \otimes |1\rangle$

Medida del primer y segundo qubit del estado $q = \dfrac{|00\rangle + |11\rangle}{\sqrt{2}}$

Estado	Prob	Medida 1		Estado	Prob	Medida 2
$\|00\rangle$	$p_0 = \frac{1}{2}$	0	$\Longrightarrow$	$\|00\rangle$	$p_0 = 1$	0
$\|11\rangle$	$p_1 = \frac{1}{2}$	1	$\Longrightarrow$	$\|11\rangle$	$p_1 = 1$	1

- La medida de los dos qubits coincide siempre

2. Unidad de información cuántica

Representación de un n−qubit

- $n-$qubit: $q = \sum_{x_1} \cdots \sum_{x_n} a_{x_1 x_2 \cdots x_n} |x_1 x_2 \cdots x_n\rangle \quad \left(\sum_{x_1} \cdots \sum_{x_n} |a_{x_1 x_2 \cdots x_n}|^2 = 1 \right)$

$$q = \sum_{x=0}^{2^n-1} a_x |x\rangle \quad \left(\sum_{x=0}^{2^n-1} |a_x|^2 = 1 \right)$$

- Estados básicos: $|x\rangle = |x_1 x_2 \ldots x_n\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle$
- Espacio vectorial: $H^n = L(|0\rangle|1\rangle \ldots |2^n - 1\rangle) = H \otimes H \otimes \cdots \otimes H$
- Base de computación: $B_n = [|0\rangle, |1\rangle, \ldots, |2^n - 1\rangle]$ (ortonormal)
- Medida del j−ésimo qubit:

Prob: $p_b = \sum_{x_j = b} |a_x|^2$ Estado resultante: $\overline{q} = \frac{1}{\sqrt{p_b}} \sum_{x_j = b} a_x |x\rangle$

3. Qubits entrelazados

Característica esencial de la información cuántica

- Estado producto: $q = \frac{|00\rangle - |01\rangle - |10\rangle + |11\rangle}{2} = \left(\frac{|0\rangle - |1\rangle)}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$
- Estado entrelazado: $q = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$
- La "mayoría"de los estados son entrelazados
- Pares EPR: $q = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$
  - Son estados con entrelazamiento máximo
  - Son fundamentales en criptografía, teletransporte, etc

4. Puertas cuánticas

Transformación de la información

- Un $n-$qubit se transforma mediante una aplicación $U : H^n \longrightarrow H^n$ tal que:
  - U es lineal y conserva la norma
  - Por tanto, U es una transformación unitaria

- Para evaluar U es preciso descomponerla en puertas cuánticas elementales:
  - Negación: $X : \begin{array}{lcl} |0\rangle & \to & |1\rangle \\ |1\rangle & \to & |0\rangle \end{array} \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
  - Negación controlada: $C : \begin{array}{lcl} |00\rangle & \to & |00\rangle \\ |01\rangle & \to & |01\rangle \\ |10\rangle & \to & |11\rangle \\ |11\rangle & \to & |10\rangle \end{array} \qquad C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$
  - Hadamard: $H : \begin{array}{lcl} |0\rangle & \to & |+\rangle = |0\rangle + |1\rangle \\ |1\rangle & \to & |-\rangle = |0\rangle - |1\rangle \end{array} \qquad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

4. Puertas cuánticas

Transformación de la información

- Aplicación de la puerta $\boldsymbol{X}$ al segundo qubit en un $\mathbf{2}-$qubit:

$$\boldsymbol{X_2}: \begin{array}{lcl} |00\rangle & \to & |01\rangle \\ |01\rangle & \to & |00\rangle \\ |10\rangle & \to & |11\rangle \\ |11\rangle & \to & |10\rangle \end{array} \qquad \boldsymbol{X_2} = \left(\begin{array}{cc|cc} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{array}\right)$$

- Encontrar un algoritmo $\boldsymbol{U}$ que transforme $\begin{array}{lcl} |0\rangle \otimes |00\rangle & \longrightarrow & |000\rangle \\ |1\rangle \otimes |00\rangle & \longrightarrow & |111\rangle \end{array}$

$$\boldsymbol{U = C_{1,3}\, C_{1,2}}$$

- Encontrar un algoritmo $\boldsymbol{U}$ que transforme $|0\rangle \otimes |00\rangle \longrightarrow \dfrac{|000\rangle + |111\rangle}{\sqrt{2}}$

$$\boldsymbol{U = C_{1,3}\, C_{1,2}\, H_1}$$

5. Propiedades de los qubits

Propiedades fundamentales

- Las medidas modifican los estados cuánticos
- Las medidas no dan información suficiente para conocer los estados cuánticos
- Un estado cuántico no se puede copiar

  No existe $\boldsymbol{U}$ tal que: $\boldsymbol{U}\left(\boldsymbol{\Psi} \otimes |\mathbf{0}\rangle\right) = \boldsymbol{\Psi} \otimes \boldsymbol{\Psi}$ para todo $\boldsymbol{\Psi}$

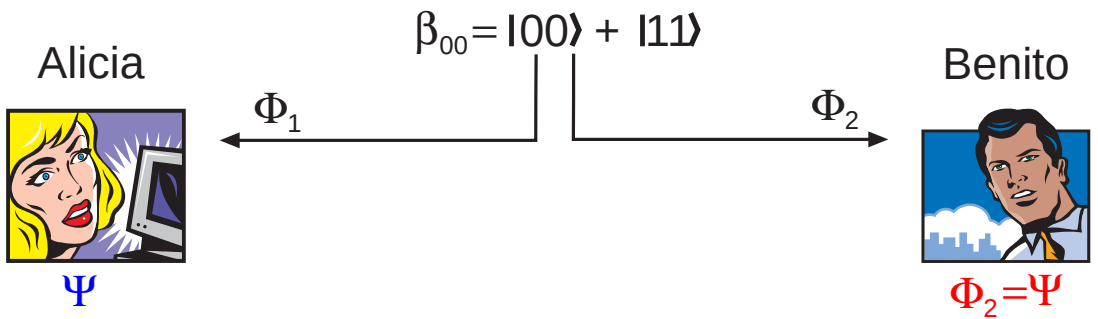
$$\begin{aligned} \boldsymbol{U}\left((|\mathbf{0}\rangle + |\mathbf{1}\rangle) \otimes |\mathbf{0}\rangle\right) &= \boldsymbol{U}\left(|\mathbf{0}\rangle \otimes |\mathbf{0}\rangle\right) + \boldsymbol{U}\left(|\mathbf{1}\rangle \otimes |\mathbf{0}\rangle\right) \\ &= |\mathbf{0}\rangle \otimes |\mathbf{0}\rangle + |\mathbf{1}\rangle \otimes |\mathbf{1}\rangle \neq (|\mathbf{0}\rangle + |\mathbf{1}\rangle) \otimes (|\mathbf{0}\rangle + |\mathbf{1}\rangle) \end{aligned}$$

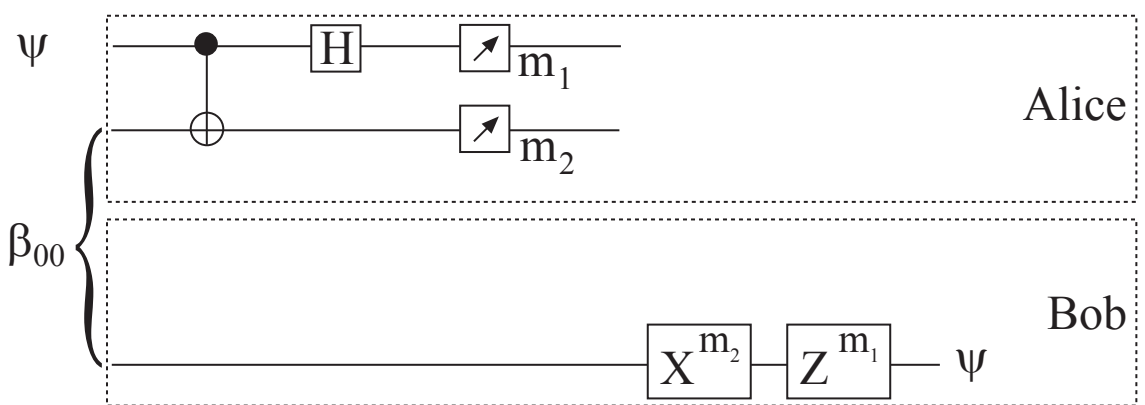
- Dos estados no ortogonales son indistinguibles

  Por ejemplo: $|\mathbf{0}\rangle$ y $|+\rangle$

5. Propiedades de los qubits

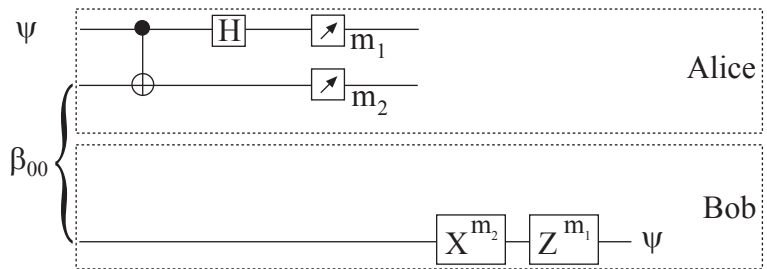
Teletransporte





5. Propiedades de los qubits

Teletransporte



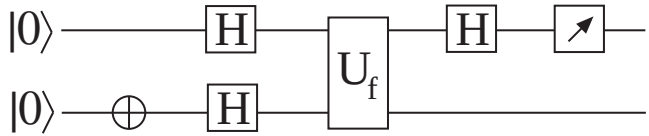
$$
\begin{aligned}
\Psi \otimes \beta_{00} &= \frac{1}{\sqrt{2}}\left[a|0\rangle \otimes (|00\rangle + |11\rangle) + b|1\rangle \otimes (|00\rangle + |11\rangle)\right] \\
&\longrightarrow \frac{1}{\sqrt{2}}\left[a|0\rangle \otimes (|00\rangle + |11\rangle) + b|1\rangle \otimes (|10\rangle + |01\rangle)\right] \\
&\longrightarrow \frac{1}{2}\left[a(|0\rangle + |1\rangle) \otimes (|00\rangle + |11\rangle) + b(|0\rangle - |1\rangle) \otimes (|10\rangle + |01\rangle)\right] \\
&= \frac{1}{2}\left[|00\rangle \otimes (a|0\rangle + b|1\rangle) + |01\rangle \otimes (a|1\rangle + b|0\rangle)\right. \\
&\quad \left. + |10\rangle \otimes (a|0\rangle - b|1\rangle) + |11\rangle \otimes (a|1\rangle - b|0\rangle)\right]
\end{aligned}
$$

6. Algoritmos cuánticos básicos

Problema de Deutsch

Dada una función booleana $f : \{0,1\} \to \{0,1\}$ y su transformación unitaria asociada U_f, encontrar un algoritmo que determine si f es constante o no aplicando U_f el menor número posible de veces

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

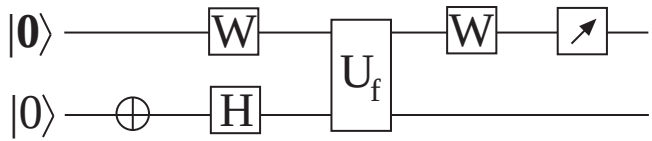


$$\begin{aligned}
|0\rangle \otimes |0\rangle &\longrightarrow |0\rangle \otimes |1\rangle \\
&\longrightarrow \tfrac{1}{2}\left(|0\rangle + |1\rangle\right) \otimes \left(|0\rangle - |1\rangle\right) \\
&\longrightarrow \tfrac{1}{2}\left(|0\rangle \otimes \left(|f(0)\rangle - |\bar{f}(0)\rangle\right) + |1\rangle \otimes \left(|f(1)\rangle - |\bar{f}(1)\rangle\right)\right) \\
&= \tfrac{1}{2}\left(|0\rangle + (-1)^{\alpha}|1\rangle\right) \otimes \left(|f(0)\rangle - |\bar{f}(0)\rangle\right) \\
&\longrightarrow \tfrac{1}{\sqrt{2}}|\alpha\rangle \otimes \left(|f(0)\rangle - |\bar{f}(0)\rangle\right) \\
&\longrightarrow \alpha \quad \text{(probabilidad = 1)}
\end{aligned}$$

6. Algoritmos cuánticos básicos

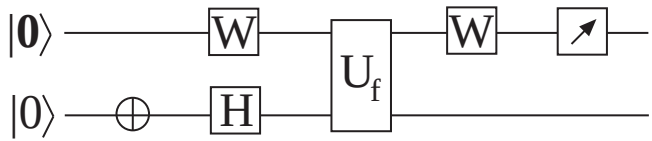
Problema de Deutsch-Jozsa

Dada una función booleana $\boldsymbol{f : \{0,1\}^n \to \{0,1\}}$ constante o balanceada y su transformación unitaria asociada $\boldsymbol{U_f}$, encontrar un algoritmo que determine si $\boldsymbol{f}$ es constante o es balanceada aplicando $\boldsymbol{U_f}$ el menor número posible de veces



6. Algoritmos cuánticos básicos

Problema de Deutsch-Jozsa

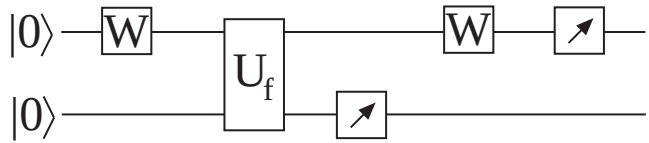


$$
\begin{aligned}
|0\rangle \otimes |0\rangle &\longrightarrow |0\rangle \otimes |1\rangle \\
&\longrightarrow \frac{1}{\sqrt{2^{n+1}}} \sum_{0 \le x < 2^n} (|x\rangle \otimes (|0\rangle - |1\rangle)) \\
&\longrightarrow \frac{1}{\sqrt{2^{n+1}}} \sum_{0 \le x < 2^n} (|x\rangle \otimes (|f(x)\rangle - |\bar{f}(x)\rangle)) \\
&\longrightarrow \frac{1}{2^n\sqrt{2}} \sum_{0 \le x < 2^n} \sum_{0 \le y < 2^n} ((-1)^{x \cdot y} |y\rangle \otimes (|f(x)\rangle - |\bar{f}(x)\rangle)) \\
&= \frac{1}{2^n\sqrt{2}} |0\rangle \otimes \sum_{0 \le x < 2^n} (|f(x)\rangle - |\bar{f}(x)\rangle) + \\
&\quad \frac{1}{2^n\sqrt{2}} \sum_{0 < y < 2^n} \left(|y\rangle \otimes \sum_{0 \le x < 2^n} ((-1)^{x \cdot y} (|f(x)\rangle - |\bar{f}(x)\rangle)) \right)
\end{aligned}
$$

6. Algoritmos cuánticos básicos

Problema de Simon

Dada una función booleana $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ 2 a 1 y periódica, encontrar un algoritmo que calcule en periodo de f aplicando U_f el menor número posible de veces



$$
\begin{aligned}
|0\rangle \otimes |0\rangle &\longrightarrow \frac{1}{\sqrt{2^n}} \sum_{0 \le k < 2^n} (|k\rangle \otimes |0\rangle) \longrightarrow \frac{1}{\sqrt{2^n}} \sum_{0 \le k < 2^n} (|k\rangle \otimes |f(k)\rangle) \\
&\longrightarrow \frac{1}{\sqrt{2}} (|l\rangle + |l \oplus T\rangle) \otimes |j\rangle \quad \left(\text{medida } j, \Rightarrow \{ l, l \oplus T \} = f^{-1}(j)\right) \\
&\longrightarrow \frac{1}{\sqrt{2^{n+1}}} \sum_{0 \le k < 2^n} \left((-1)^{l \cdot k} + (-1)^{(l \oplus T) \cdot k} \right) |k\rangle \otimes |j\rangle \\
&= \frac{1}{\sqrt{2^{n+1}}} \sum_{0 \le k < 2^n} (-1)^{l \cdot k} \left(1 + (-1)^{T \cdot k}\right) |k\rangle \otimes |j\rangle \\
&\longrightarrow k \quad \text{tal que} \quad T \cdot k = 0
\end{aligned}
$$