Algoritmos cuánticos

Andrés Sicard

Grupo de Lógica y Computación
Departamento de Ciencias Básicas
Universidad EAFIT, Medellín, Colombia

Computación Cuántica

- Implementación $(70\,\%)$
- Algorítmica $(10\,\%)$
  - Clases de complejidad
  - Problemas NP-completos
- Modelos $(20\,\%)$
  - CC discreta
  - CC continua
  - CC (no) adiabática
  - CC geométrica (holonómica)
    - abeliana
    - no abealina
  - ¡¡ Hipercomputación !!

$1, 2, \ldots, n$-qubits

n-qubit	base computacional	dim
1-qubit	$\{\|0\rangle, \|1\rangle\}$	2^1
2-qubit	$\{\|00\rangle, \|01\rangle, \|10\rangle, \|11\rangle\}$ $\{\|0\rangle_2, \|1\rangle_2, \|2\rangle_2, \|3\rangle_2\}$	2^2
$\vdots$	$\vdots$	$\vdots$
n-qubit	$\{\|0\rangle_n, \ldots, \|2^{n-1}\rangle_n\}$	2^n

Crecimiento lineal en el número de qubits
vs
Crecimiento exponencial en el espacio computacional

Representación n-qubits

n-qubit	superposición	vector
1-qubit	$\|\psi\rangle = \alpha_0 \|0\rangle + \alpha_1 \|1\rangle$	$\begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix}$
2-qubit	$\|\psi\rangle = \sum_{j=0}^{2^2-1} \alpha_j \|j\rangle$	$\begin{bmatrix} \alpha_0 \\ \vdots \\ \alpha_3 \end{bmatrix}$
$\vdots$	$\vdots$	$\vdots$
n-qubit	$\|\psi\rangle = \sum_{j=0}^{2^n-1} \alpha_j \|j\rangle$	$\begin{bmatrix} \alpha_0 \\ \vdots \\ \alpha_{2^n-1} \end{bmatrix}$

Compuertas cuánticas (1)

- 1-qubit

Negación $\begin{cases} U_{NOT}\,|0\rangle = |1\rangle \\ U_{NOT}\,|1\rangle = |0\rangle \end{cases}$

Representación matricial:

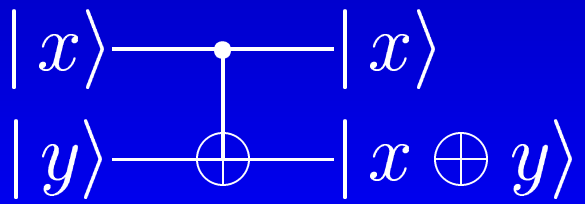
$$\underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}_{U_{NOT}} \underbrace{\begin{bmatrix} 1 \\ 0 \end{bmatrix}}_{|0\rangle} = \underbrace{\begin{bmatrix} 0 \\ 1 \end{bmatrix}}_{|1\rangle}, \qquad \underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}_{U_{NOT}} \underbrace{\begin{bmatrix} 0 \\ 1 \end{bmatrix}}_{|1\rangle} = \underbrace{\begin{bmatrix} 1 \\ 0 \end{bmatrix}}_{|0\rangle}$$

Compuertas cuánticas (2)

- 1-qubit

Hadamard
$$\begin{cases} U_H\,|\,0\rangle = \dfrac{1}{\sqrt{2}}(|\,0\rangle + |\,1\rangle) \\ U_H\,|\,1\rangle = \dfrac{1}{\sqrt{2}}(|\,0\rangle - |\,1\rangle) \\ U_H = \dfrac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \end{cases}$$

- 2-qubit
  NOT Controlado: $U_{CNOT}\,|\,x,y\rangle \mapsto |\,x, x \oplus y\rangle$



Compuertas cuánticas (3)

1. Operadores lineales

$$U(\alpha\,|\,x\rangle + \beta\,|\,y\rangle) = \alpha U\,|\,x\rangle + \beta U\,|\,y\rangle$$

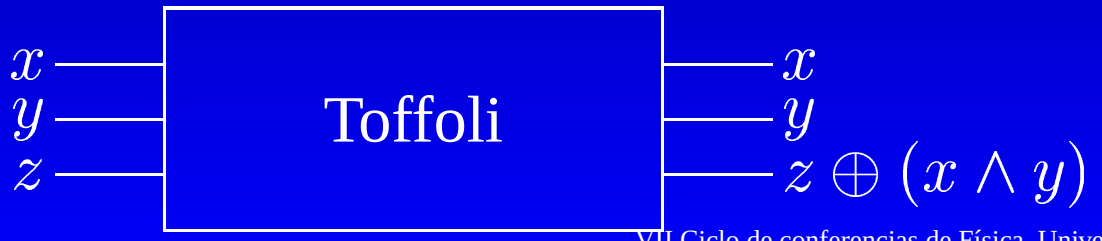
2. Operadores unitarios de evolución

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

3. Reversibles

$$\text{Si } U\,|\,x\rangle = |\,x'\rangle\,,\ \text{entonces } U^\dagger\,|\,x'\rangle = |\,x\rangle$$

4. Universales



Paralelismo cuántico

La capacidad de un sistema cuántico de estar en varios estados de la base computacional simultáneamente es denominada paralelismo cuántico.

Un operador U_f implementa una función f si

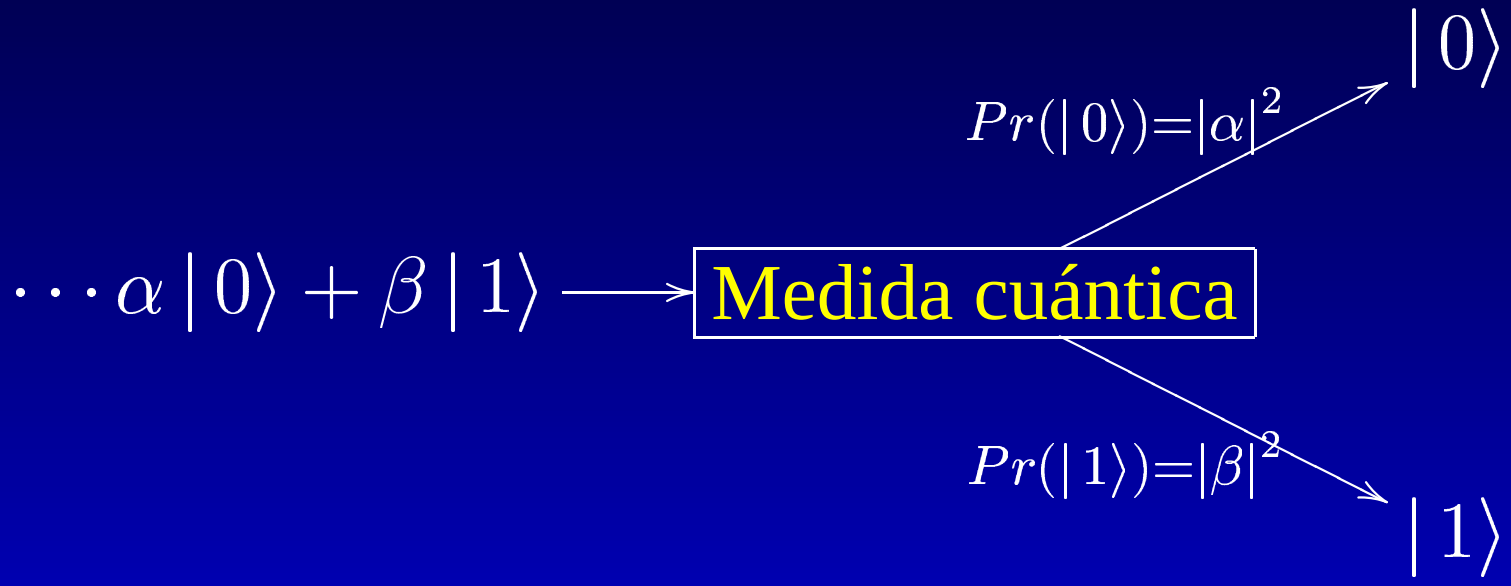
$$U_f \,|\, x, 0\rangle = |\, x, f(x)\rangle \,.$$

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

$$\begin{aligned} U_f \,|\,\psi\rangle &= \frac{1}{\sqrt{2}}(U_f \,|\,0,0\rangle + U_f \,|\,1,0\rangle) \\ &= \frac{1}{\sqrt{2}}(|\,0, f(0)\rangle + |\,1, f(1)\rangle) \end{aligned}$$

Medida cuántica

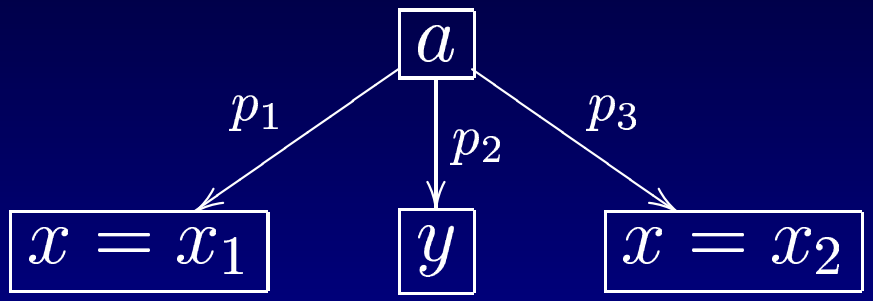
Los algoritmos cuánticos son probabilistas debido al indeterminismo de los resultados de una medida cuántica.



Por lo tanto, es necesario que $|\alpha|^2 + |\beta|^2 = 1$ y α, β son denominadas amplitudes de probabilidad.

Interferencia (1)

Computación probabilista



$$p_1 + p_2 + p_3 = 1$$

$$Pr(x_1) = p_1$$

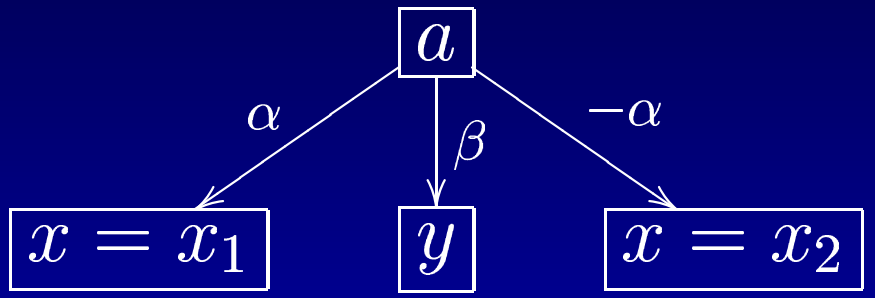
$$Pr(x_2) = p_3$$

$$Pr(x) = Pr(x_1) + Pr(x_2) = p_1 + p_3$$

Interferencia (2)

Computación cuántica: interferencia destructiva

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



$$Am(x_1) = \alpha, \qquad Pr(x_1) = |\alpha|^2 = \alpha^2$$

$$Am(x_2) = -\alpha, \qquad Pr(x_2) = |-\alpha|^2 = \alpha^2$$

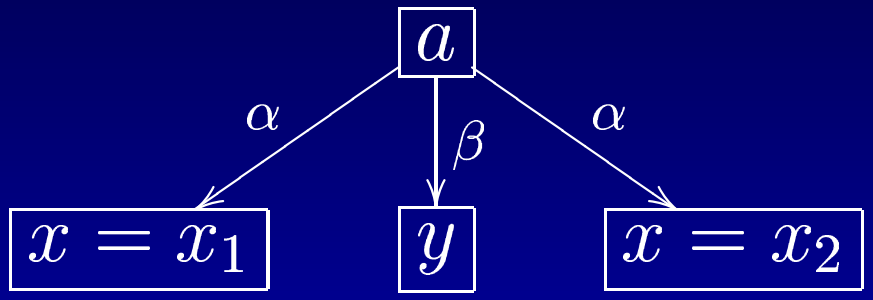
$$Am(x) = Am(x_1) + Am(x_2), \qquad Pr(x) = |Am(x)|^2$$

$$= 0 \qquad = 0$$

Interferencia (3)

Computación cuántica: interferencia constructiva

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



$$Am(x_1) = \alpha, \qquad Pr(x_1) = |\alpha|^2 = \alpha^2$$

$$Am(x_2) = \alpha, \qquad Pr(x_2) = |\alpha|^2 = \alpha^2$$

$$Am(x) = Am(x_1) + Am(x_2), \qquad Pr(x) = |Am(x)|^2$$

$$= 2\alpha \qquad = 4\alpha^2 > 2\alpha$$

Algoritmos cuánticos: complejidad algorítmica

Algoritmo	Problema	CC	CQ
Deutsch (1985)	¿Es una función f: $\{0,1\} \rightarrow \{0,1\}$ balanceada?	2	1
Deutsch-Jozsa (1992)	¿Es una función f: $\{0,1\}^n \rightarrow \{0,1\}$ balanceada?	$2^{n-1}+1$	1
Grover (1996)	Busquedad en una BD desorganizada de n elementos	n	$\sqrt{n}$
Shor (1994)	Factorizar un número entero	$Exp(n)$	$Pol(n)$

Algoritmo de Shor vs. algoritmo clásico

Nro. dígitos	Alg. clásico	Alg. de Shor
129	1,85 años	45,9 minutos
250	$2{,}1 \times 10^6$ años	3,4 horas
1000	$4{,}5 \times 10^{25}$ años	3,07 días

Algoritmos cuánticos: computa-bilidad

The term ‘hypermachine’ denotes any data processing device (theoretical or that can be implemented) capable of carrying out tasks that cannot be performed by a Turing machine

Algoritmo	Problema
Deutsch (1985)	Generación de números aleatorios
Kieu (2001-2004)	Décimo problema de Hilbert
Calude-Pavlov (2001)	Problema de la parada

Problemas abiertos

- Complejidad algoritmica
  Diseñar un algoritmo cuántico de tiempo polinomial para un problema NP-completo

- Computabilidad
  Determinar si es posible construir un hipercomputador cuántico

Implementación

- Técnicas
  - Resonancia nuclear magnética (NMR)
  - Implementación NMR con fase geométrica
  - Computador cuántico atómico
  - Iones atrapados
  - Implementación óptica
- Logros alcanzados
  - 1998: 2-qubit (University of California Berkeley)
  - 1999: 3-qubit (IBM-Almaden)
  - 2000: 5-qubit (IBM-Almaden, Los Alamos)
  - 2001: 7-qubit (IBM-Almaden)

Recursos Internet

- Servidor de los Alamos (`arXiv.org`) .
- *Virtual Journal of Quantum Computation* (`www.vjquantuminfo.org/`).
- Artículos clásicos (`pm1.bu.edu/~tt/qcl.html`).
- *Centre for Quantum Computation - Oxford* (`www.qubit.org/`)
- Simuladores (`www.vcpc.univie.ac.at/~ian/hotlist/qc/programming.shtml`).

Recursos bibliográficos

[1] Isaac L. Chuang and Michael A. Nielsen. *Quantum computation and quantum information*. Cambridge: Cambridge University Press, 2000.

[2] Eleanor Rieffel and Wolfgang Polak. An introduction to quantum computing for non-physicists. *ACM Computing Surveys*, 32(3):300–335, 2000. Preprint: `arXiv.org/abs/quant-ph/9809016`.

[3] Dorit Aharonov. Quantum computation. Eprint: `arXiv.org/abs/quant-ph/9812037`, 1998.

[4] A. Galindo and M. A. Martín-Delgado. Information and computation: classical and quantum aspects. *Rev. Mod. Phys.*, 74(2):347–423, 2002. Preprint: `arXiv.org/abs/quant-ph/0112105`.

Agradecimientos y contactos

La presentación y realización de este trabajo fue financiada por la universidad EAFIT.

Andrés Sicard

email: asicard@eafit.edu.co

homepage:
http://sigma.eafit.edu.co:90/~asicard/personal