COMPUTACIÓN CUÁNTICA

Andrés Sicard (email: asicard@eafit.edu.co)
Mario Vélez (email: mvelez@eafit.edu.co)

Grupo Lógica y Computación
Escuela de Ciencias y Humanidades
Universidad EAFIT

Fundaciones computabilidad

Kurt Gödel: Funciones primitivas recursivas (1931).

Kurt Gödel, Stephen Kleene: Funciones recursivas (1934, 1936).

Alonso Church, Stephen Kleene: λ-cálculo (1936).

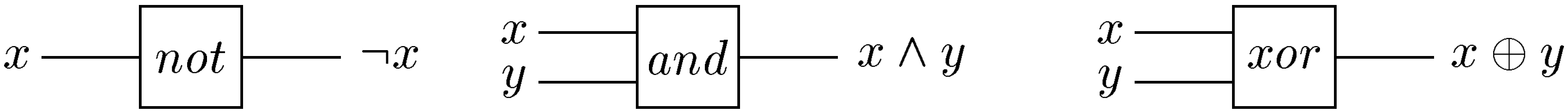
Alan Turing: Máquina de Turing, máquina universal de Turing (1936).

Emil Post: Máquina de Post (1936).

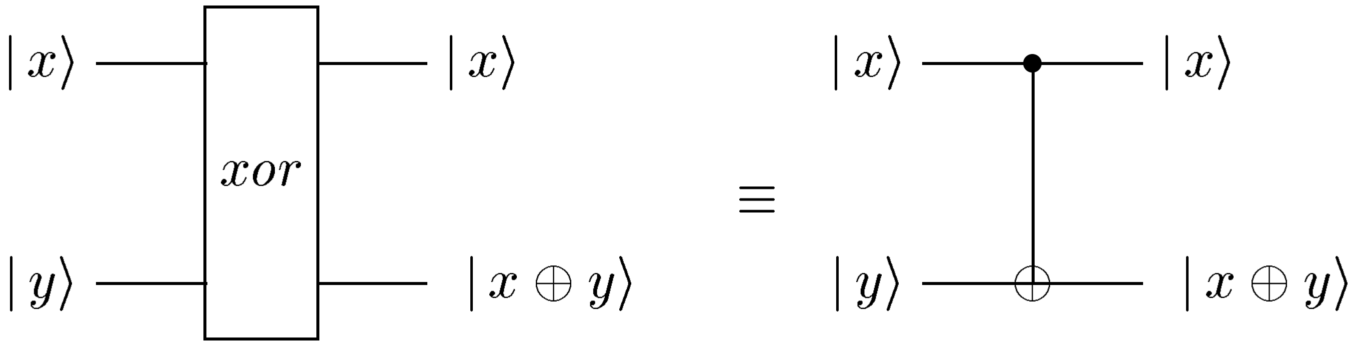
Computación reversible

Charles H. Bennett (1973) [1]:

Compuertas no reversibles:



Compuerta reversible:



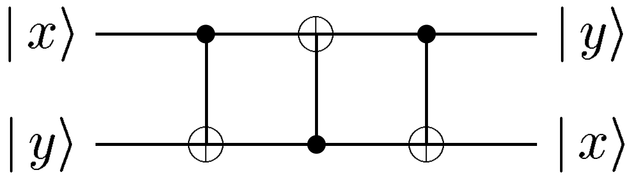
Compuertas universales reversibles

Edward Fredkin y Tommaso Toffoli (1982) [2]:

$$z \oplus (x \wedge y) = \begin{cases} x \wedge y & \text{sii } z = 0 \text{ (compuerta } \textit{and}\text{)}, \\ x \oplus z & \text{sii } y = 1 \text{ (compuerta } \textit{xor}\text{)}, \\ \neg z & \text{sii } x = y = 1 \text{ (compuerta } \textit{not}\text{)}, \\ x & \text{sii } x = 0; y = 1 \text{ (compuerta } \textit{identidad}\text{)}. \end{cases}$$

Circuitos cuánticos

Intercambio de qubits:



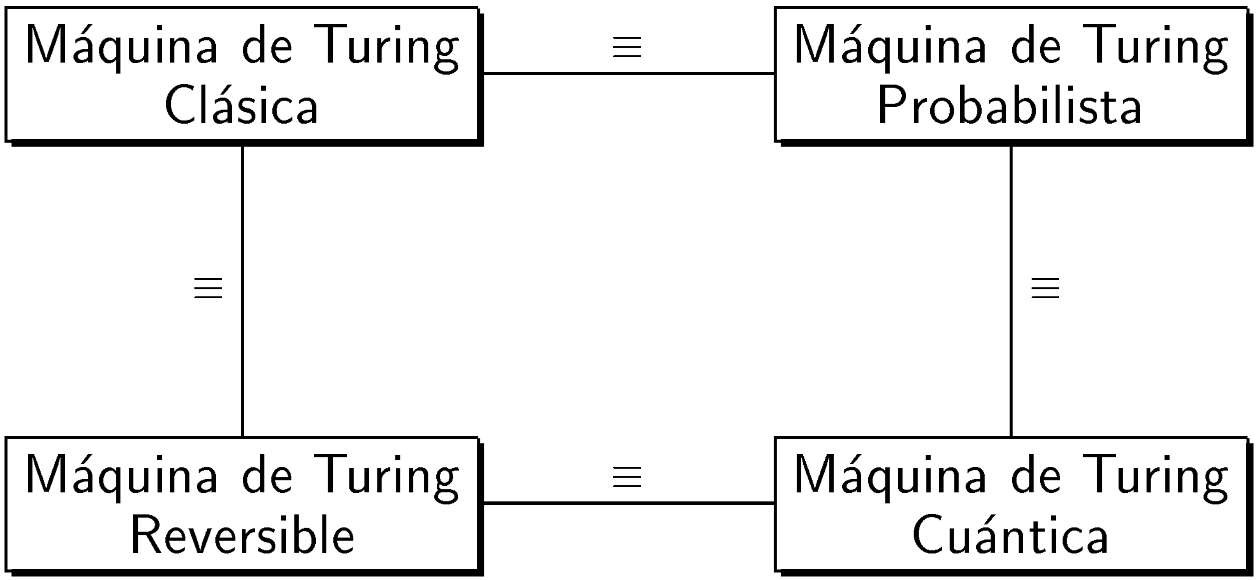
Modelos de computación cuántica

Richard Feynmann (1982, 1985): Computación mecánico-cuántica [3].

David Deutsch (1985): Máquinas de Turing cuánticas [4].

David Deutsch (1989): Circuitos cuánticos [5].

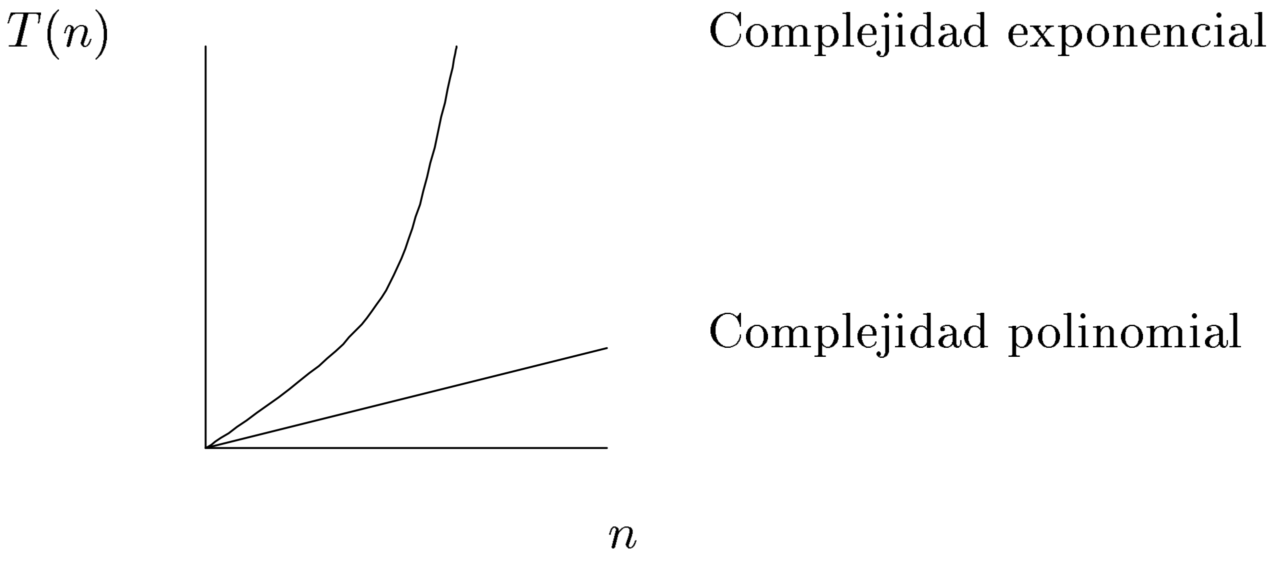
Algunos modelos de computación



Algoritmos cuánticos

Peter Shor (1994): Algoritmo para factorizar un número en sus factores primos de complejidad polinomial [6].

Lov K. Grover (1996): Algoritmo de busqueda en una base de datos desorganizada [7].



Comportamiento algoritmo de Shor

clásico: $c(x) = \exp\{(\frac{64}{9})^{1/3}(\ln x)^{1/3}(\ln\ln x)^{2/3}\}$

cuántico: $q(x) = (\ln x)^2(\ln\ln x)(\ln\ln\ln x)$

Número de dígitos	**Clásico**	**Cuántico**
129	1.85 años	45.9 minutos
250	2.1×10^6 años	3.4 horas
1000	4.5×10^{25} años	3.07 días

Simuladores

Página simuladores: *www.dcs.ex.ac.uk/~jwallace/simtable.htm*

Bernhard Ömer: *QCL: A Programming Language for Quantum Computers* [8].

Colin P. Williams y Scott H. Clearwater: Simulador implementado en *MATHEMATICA*^{TM} [9].

El Qubit

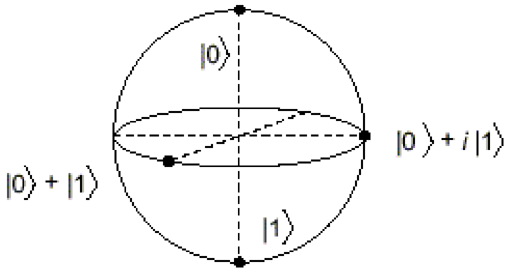
La unidad fundamental de información cuántica es el qubit:

$$|\,x\rangle = a_0\,|\,0\rangle + a_1\,|\,1\rangle \qquad \text{donde} \qquad |a_0|^2 + |a_1|^2 = 1, \tag{1}$$

los a_i con $i = 0, 1$ son números complejos e, $|\,i\rangle$ es la base de un espacio de Hilbert, el cual satisface $\langle i\,|\,j\rangle = \delta_{i,j}$. En una representación particular

$$|\,0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \qquad\qquad |\,1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

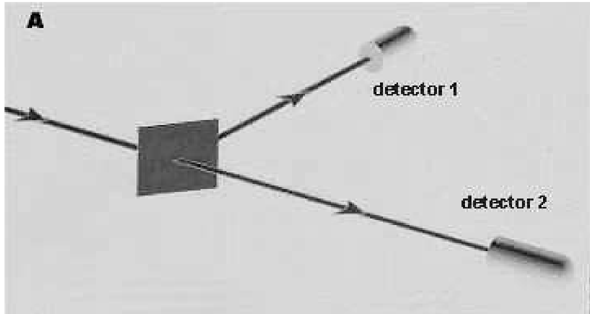
El Qubit



Representación de algunos estados del qubit.

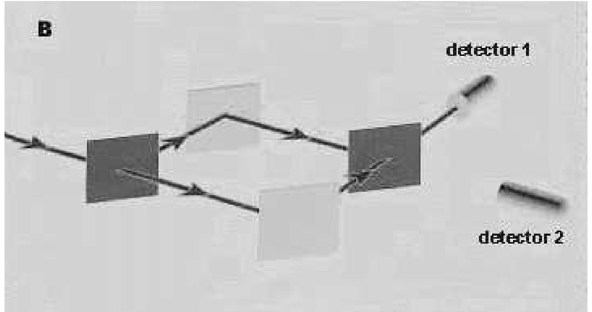
Cualquier sistema cuántico de dos estados (base), sirve para representar al qubit. En particular: electrónes, moléculas y fotones.

Un sólo fotón



Representación del estado de un fotón [10].

Un sólo fotón



La interferencia de sólo un fóton.

El n-Qubit

La noción de qubit puede ser generalizada a un sistema cuántico de n qubits. En particular un 2-qubit es el producto tensorial de dos qubits:

$$|\, x_0, x_1 \rangle = |\, x_0 \rangle \otimes |\, x_1 \rangle \qquad \text{La base tiene } 2^2 \text{ estados .} \tag{2}$$

El n-qubit es el producto tensorial de n qubits

$$|\, x_0, x_1 \ldots, x_n \rangle = |\, x_0 \rangle \otimes |\, x_1 \rangle \cdots \otimes |\, x_n \rangle \qquad \text{La base tiene } 2^n \text{ estados .} \tag{3}$$

Los n-qubits físicamente pueden ser representados con moléculas o con fotones.

Paralelismo cuántico

Un computador cuántico puede en un sólo paso computacional, realizar la misma operación matemática sobre 2^n estados cuánticos, codificados en una superposición coherente de n-qubits.

Un computador clásico tendría que realizar 2^n pasos computacionales para realizar la misma tarea. Una forma alterna de realizar la misma función en un computador clásico sería, conectar 2^n procesadores en paralelo.

Un computador cuántico no computa más que un computador clásico, solo la hace más rápido. La ventaja del computador cuántico sobre el computador clásico radica en que éste último requiere más memoria y su evolución es más lenta en el tiempo.

Evolución cuántica

La evolución o dinámica de un n-qubit es determinada por un operador unitario U, el cual actúa sobre el espacio de Hilbert.

$$U^\dagger U = Id. \tag{4}$$

La evolución es además reversible. El operador de evolución actúa sobre los qubits, generando nuevos qubits.

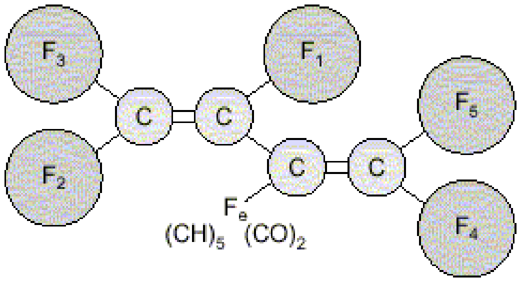
$$U \,|\, x\rangle = |\, x'\rangle\,. \tag{5}$$

Compuertas cuánticas

La evolución puede ser correctamente controlada de forma tal, que se puedan implementar compuertas lógico-cuánticas. En particular, la compuerta NOT de un qubit y la compuerta $CNOT$ de dos qubits, producen un modelo de computación universal.

$$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{6}$$

Implementación NMR



Computador cuántico de 5-qubits [11].

Textos y artículos introductorios

[Gru99] JOSEP GRUSKA. "Quantum computing". Cambridge: McGraw-Hill International (UK) Limited (1999).

[RP98] ELEANOR RIEFFEL Y WOLFGANG POLAK. An introduction to quantum computing for non-physicists. To appear in ACM Computing Surveys. Eprint: arXiv.org/abs/quant-ph/9809016 (1998).

[Sho] PETER W. SHOR. Introduction to quantum algorithms. Notes for talk given for the short course at the January 2000 AMS meeting. Eprint: arXiv.org/abs/quant-ph/0005003.

[WC97] COLIN P. WILLIAMS Y SCOTT H. CLEARWATER. "Explorations in quantum computing". New York: Springer-Telos (1997).

[1] Charles H. Bennett. Logical reversibility of computation. *IBM J. Res. Develop.* páginas 525–532 (november 1973).

[2] Edward Fredkin y Tommaso Toffoli. Conservative logic. *International Journal of Theoretical Physics* **21**(3/4), 219–253 (1982).

[3] Richard Feynman. "Feynman lectures on computation". Reading, Massachusetts: Addison-Wesley Publishing Company (1996).

[4] David Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proc. R. Soc. Lond.* **A400**, 97–117 (1985). Eprint: www.qubit.org/resource/deutsch85.ps.

[5] David Deutsch. Quantum computational networks. *Proc. R. Soc. Lond.* **A425**, 73–90 (1989).

[6] Peter W. Shor. Polinomial-time algorithms for prime factorizacion and discrete logarithms on a quantum computer. *Siam Journal on Computing* **26**(5), 1484–15090 (Octuber 1997).

[7] Lov K. Grover. A fast quantum mechanical algorithm for database search. Proceedings, 28th Annual ACM Symposium on the Theory of Computing (STOC), May 1996, pages 212-219. Eprint: arXiv.org/abs/quant-ph/9605043 (1996).

[8] Bernhard Ömer. QCL - A Programming Language for Quantum Computers. Eprint: tph.tuwien.ac.at/˜oemer/qcl.html (??)

[9] Colin P. Williams y Scott H. Clearwater. "Explorations in quantum computing". New York: Springer-Telos (1997).

[10] N. J. Cerf, C. Adami y P. G. Kwiat. Optical simulation of quantum logic. *Physical Review A* **57**, R1477 (1998). Eprint: arXiv.org/abs/quant-ph/9706022.

[11] Mathias Sttefen y Isaac L. Chuang. Toward quantum computation: A five-qubit quantum processor. *IEEE* páginas 24–34 (March-April 2001).