Una pequeña introducción práctica a la computación cuántica

Elías F. Combarro - Universidad de Oviedo

Alcalá de Henares - Febrero de 2018

Contenidos

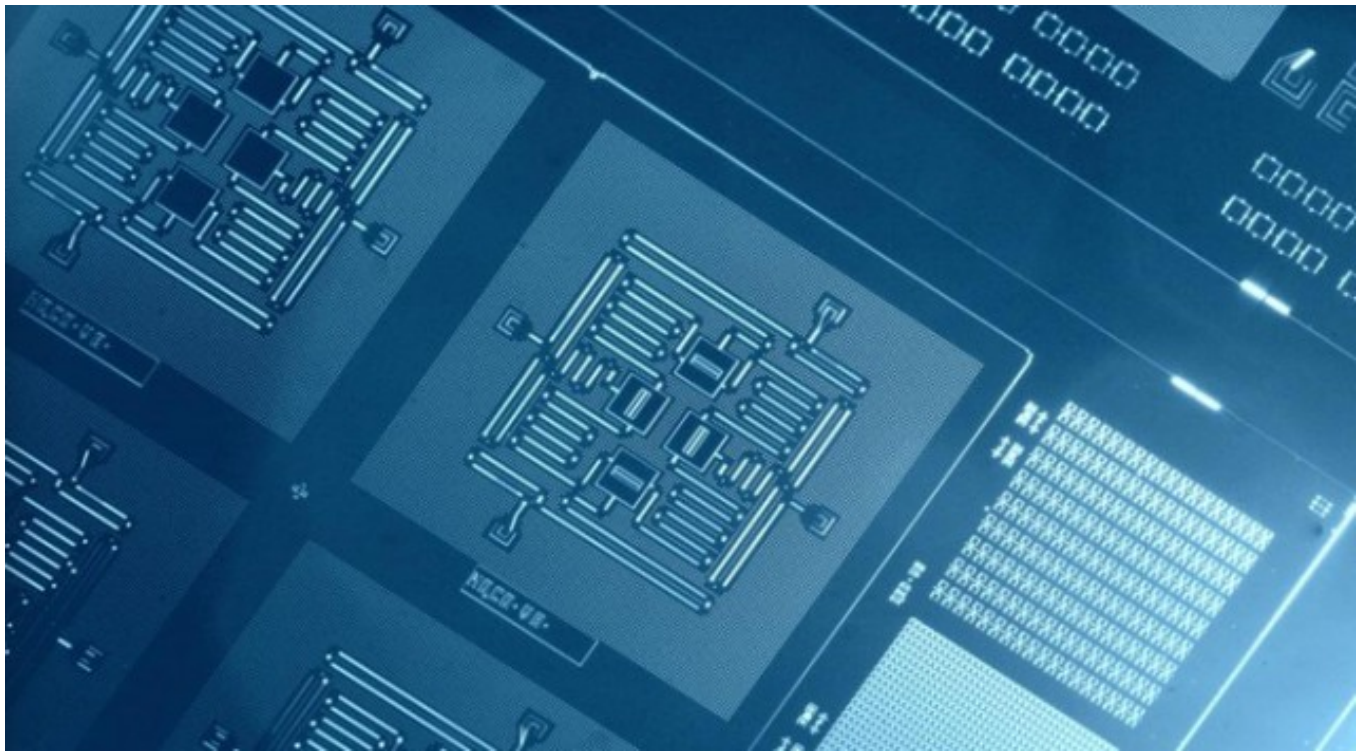
Parte I

Conceptos básicos

¿Qué fotones es la computación cuántica?

Computación cuántica

La computación cuántica es un paradigma **probabilista** de computación que utiliza las propiedades de la mecánica cuántica para realizar cálculos



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 en algunos casos

Qubits

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

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

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

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

Dos qubits

- El estado de un sistema de 2 qubits es el producto tensorial de los estados de cada uno de los qubits
- Una base de ese producto tensorial es:

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

que también se denota

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

o

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

- 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

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

Sistemas de n qubits

- El estado de un sistema de *n* qubits es un elemento del producto tensorial de los espacios de cada uno de los qubits
- Este espacio tiene dimensión 2^n y una base suya es:

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

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

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

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).
- 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

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

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

$$|0\rangle \text{ —}\boxed{X}\text{— } |1\rangle$$

$$|1\rangle \text{ —}\boxed{X}\text{— } |0\rangle$$

  es decir, actúa como un *not*
- Su acción sobre un qubit general sería

$$\alpha\,|0\rangle + \beta\,|1\rangle \text{ —}\boxed{X}\text{— } \beta\,|0\rangle + \alpha\,|1\rangle$$

La puerta Y

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

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

- Su acción es

$$|0\rangle \text{ —[}Y\text{]— } i\,|1\rangle$$

$$|1\rangle \text{ —[}Y\text{]— } -i\,|0\rangle$$

La puerta Z

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

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

- Su acción es

$$|0\rangle \text{ —} \boxed{Z} \text{—} \; |0\rangle$$

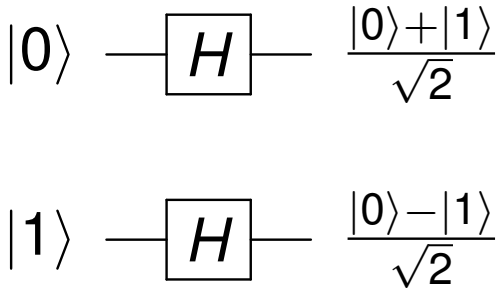
$$|1\rangle \text{ —} \boxed{Z} \text{—} \; -|1\rangle$$

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



La puerta T

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

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

- Su acción es

$$|0\rangle \text{ —}\boxed{T}\text{— } |0\rangle$$

$$|1\rangle \text{ —}\boxed{T}\text{— } e^{i\frac{\pi}{4}}|1\rangle$$

La puerta S

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

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

- Su acción es

$$|0\rangle \text{ —}\boxed{S}\text{— } |0\rangle$$

$$|1\rangle \text{ —}\boxed{S}\text{— } e^{i\frac{\pi}{2}}\,|1\rangle$$

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

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

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

La puerta *CNOT*

- La puerta *CNOT* (controlled-NOT) viene definida por la matriz (unitaria)

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

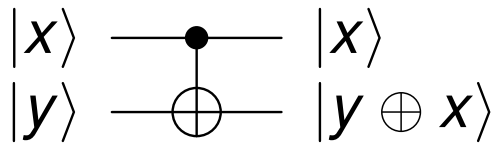
- Si el primer qubit es $|0\rangle$, no se hace nada. Si es $|1\rangle$, se invierte el segundo qubit (y el primero queda igual)
- Es decir:

$$|00\rangle \to |00\rangle \qquad |01\rangle \to |01\rangle$$

$$|10\rangle \to |11\rangle \qquad |11\rangle \to |10\rangle$$

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. Si aplicamos la puerta *CNOT* al estado

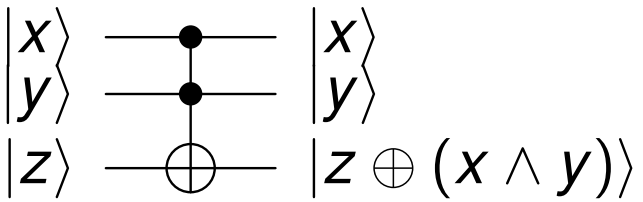
$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle$$

obtenemos

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

La puerta de Toffoli

- La puerta de Toffoli (o *CCNOT*) es una puerta de 3 qubits. Por tanto, está representada por una matriz 8×8
- Su acción con elementos $x, y, z \in \{0, 1\}$ es:



- La puerta de Toffoli es **universal para la lógica clásica**, lo que implica que **cualquier circuito clásico se puede implementar mediante un circuito cuántico**
- Sin embargo, la puerta de Toffoli, por sí sola, **no es universal para la computación cuántica** (y ni siquiera es imprescindible, puesto que se puede simular con otras puertas de menos qubits)

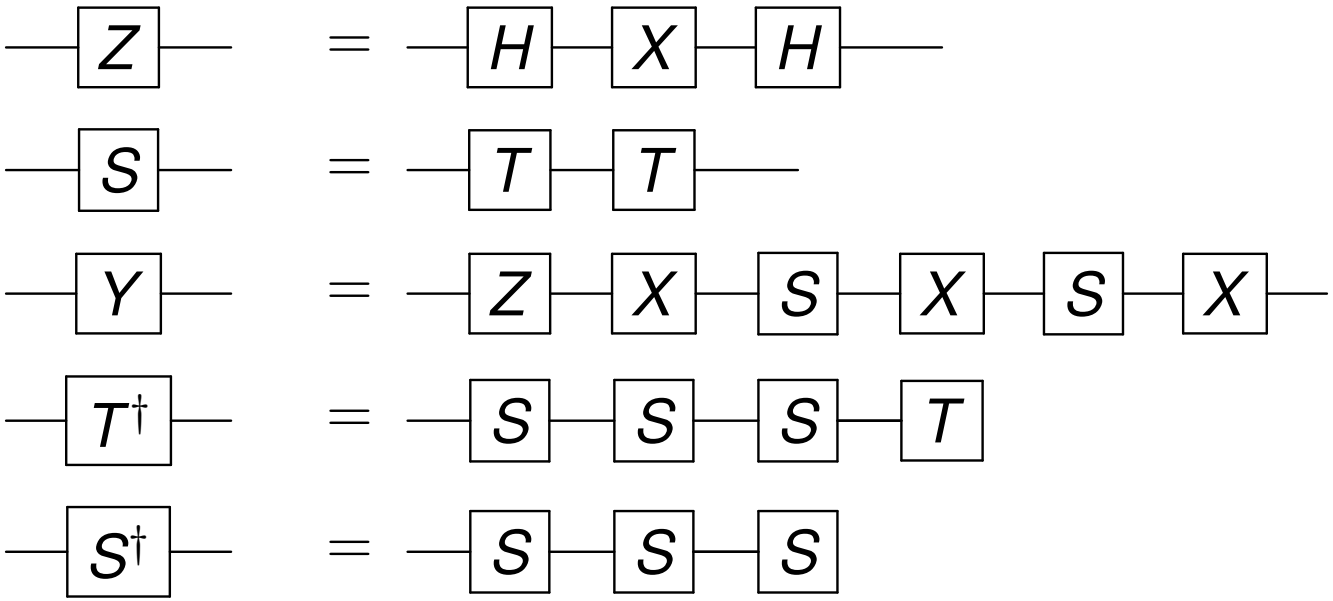
Puertas universales en la computación cuántica

- 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

Equivalencias entre puertas cuánticas



Sin embargo, tanto Z como S, Y, $S^\dagger$ y $T^\dagger$ se incluyen entre las puertas disponibles en algunos ordenadores cuánticos (como la serie imbqx de IBM).

Equivalencias entre puertas cuánticas

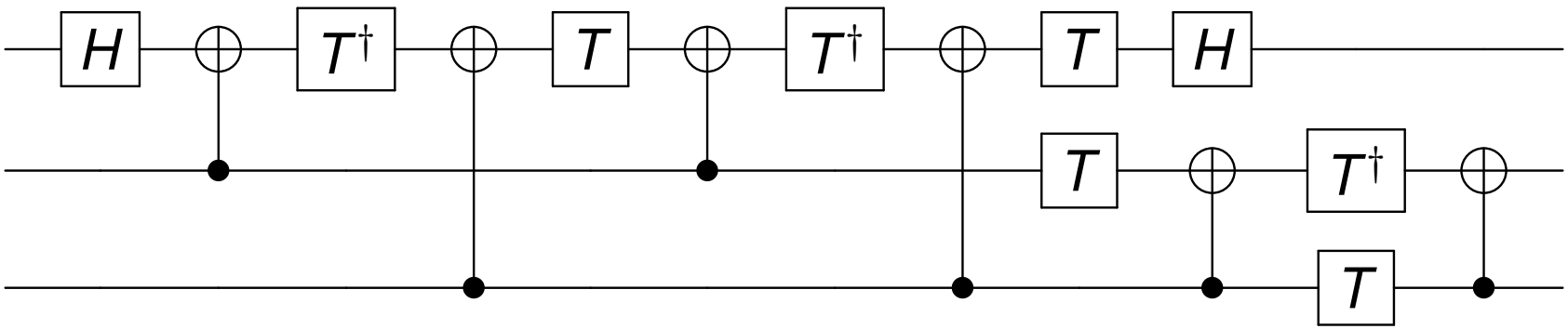


Figura: Puerta de Toffoli (con target en el bit superior y control en los dos inferiores) a partir de *CNOT*s y puertas de un qubit

Medida de un qubit

- La única forma de conocer el estado de un qubit es realizar una medida
- Sin embargo:
  - El resultado de la media 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 del mismo estado porque no se puede copiar el estado $|\psi\rangle$ (teorema de no clonación)

Medida de un qubit en 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 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

$$\frac{\alpha_{10}\,|10\rangle + \alpha_{11}\,|01\rangle}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}}$$

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

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

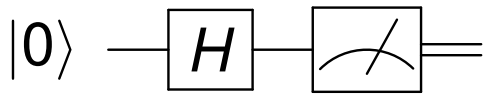
    donde I_0 es el conjunto de números i cuyo j-ésimo bit es 0
  - En ese caso, el nuevo estado de $|\psi\rangle$ será

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

  - El caso en el que se obtiene 1 es análogo

Hello, quantum world!

- Un circuito sencillo



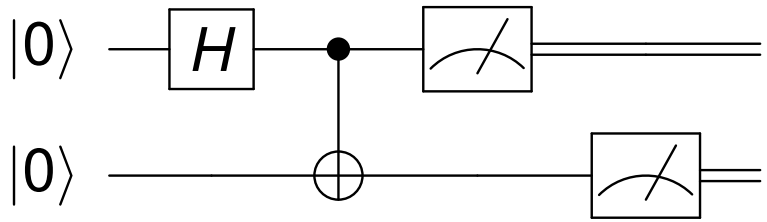
- Tras aplicar la puerta H el estado del qubit será

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

- Al medir, obtendremos 0 o 1, cada uno con el 50 % de probabilidad

Hello, entangled world!

- Un circuito ligeramente más complejo



- Inicialmente, el estado del sistema es $|00\rangle$
- Tras aplicar la puerta *H* el estado es

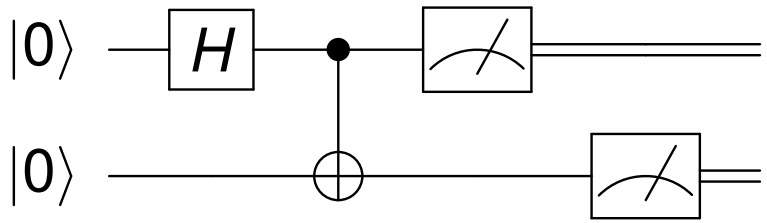
$$\frac{|00\rangle + |10\rangle}{\sqrt{2}}$$

- Al aplicar la puerta *CNOT* el estado cambia a

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

que es un estado entrelazado

Hello, entangled world!



- Al medir el primer qubit, tenemos el estado $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$
- Obtendremos 0 o 1, cada uno con probabilidad $\frac{1}{2}$
- Supongamos que obtenemos 0, entonces el nuevo estado será $|00\rangle$
- Entonces, al medir el segundo qubit obtendremos 0 ¡con probabilidad 1!
- Si en el primer qubit obtenemos 1, en el segundo ¡también obtendremos 1!
- Este comportamiento es la base de **la criptografía y la teleportación cuánticas**

¿Qué puede hacer la computación cuántica por mí?

- Gran parte del poder la computación cuántica se basa en la combinación de la **superposición** y la **interferencia** (constructiva y destructiva)
- Algunos de los algoritmos que (se cree que) superan a cualquier correlato clásico son:
  - Algoritmo de Deutsch-Jozsa (funciones constantes vs. perfectamente balanceadas)
  - Algoritmo de Bernstein- Vazirani (funciones booleanas lineales)
  - Algoritmo de Simon (determinación de s tal que $f(x) = f(x \oplus s)$
  - Algoritmo de Shor (factorización de números)
  - Algoritmo de Grover (búsqueda un elemento que cumpla una condición)

¿Qué puedo hacer yo por la computación cuántica?

- Algoritmos cuánticos (Quantum zoo)
- Simulación (álgebra matricial, GPUs...)
- Transformada cuántica de Fourier (QFT)
- Quantum Machine Learning
- Comunicaciones y criptografía cuánticas
- Quantum Adiabatic Optimization (Quantum Annealing)

Parte II

Nuestro problema

El estudio de los semicuerpos finitos

- Un semicuerpo (finito) es una estructura algebraica semejante a un cuerpo pero cuya multiplicación no es necesariamente asociativa
- Su estudio tiene interés por su relación con la teoría de códigos y con las geometrías finitas
- Durante más de diez años hemos aplicado técnicas de computación paralela y de altas prestaciones para:
  - Clasificar todos los semicuerpos de 64 elementos (problema abierto durante 40 años)
  - Clasificar todos los semicuerpos de tamaños mayores (por ejemplo, 5^4 y 7^4)
  - Estudiar semicuerpos con condiciones particulares (conmutatividad, centro $GF(4)$...)
  - ...
- Los casos más complejos requieren **millones de horas de computación**

Conmutatividad de álgebras finito-dimensionales

- El estudio de la conmutatividad de semicuerpos es importante en la clasificación
- Se puede generalizar fácilmente al estudio de conmutatividad en álgebras finito-dimensionales
- La multiplicación de un álgebra de dimensión n se puede especificar mediante una serie de constantes M_{ijk} que cumplen

$$x_i x_j = \sum_{k=1}^{n} M_{ijk} x_k$$

  donde $\{x_1, \ldots, x_n\}$ es una base del álgebra.
- Es fácil ver que se tiene conmutatividad si y sólo si

$$M_{ijk} = M_{jik} \ \forall i, j, k \in \{1, \ldots, n\}$$

Conmutatividad de álgebras finito-dimensionales

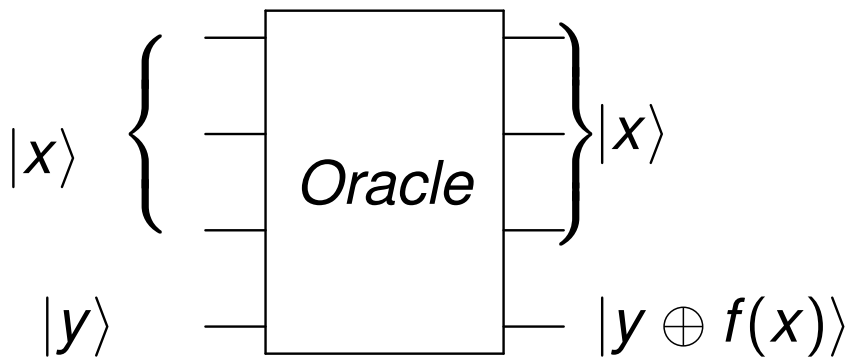
- Si el álgebra no es conmutativa, el número de elementos tales que $M_{ijk} \neq M_{jik}$ está entre 2 y $n^3 - n^2$
- Cualquier algoritmo clásico (probabilista o no) necesitará $\Omega(n^3)$ consultas de M_{ijk}
- Nótese que el problema es similar a comprobar si una matriz es simétrica
- Mediante la computación cuántica podemos mejorar sensiblemente el número de consultas

Parte III

El algoritmo de Grover

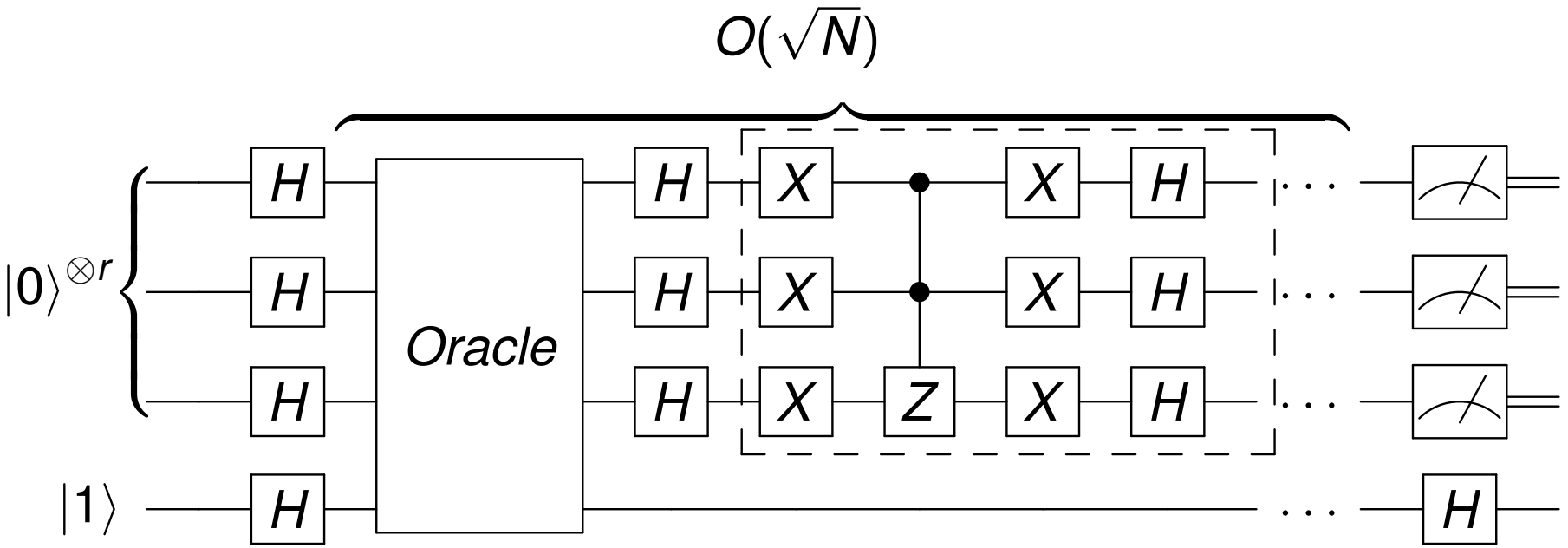
El algoritmo de Grover

- El algoritmo de Grover es un algoritmo cuántico que permite encontrar un elemento que cumple una condición en un conjunto de tamaño N usando $O(\sqrt{N})$ consultas
- Para ello, partimos de un oráculo, un circuito reversible que calcula una función booleana $f : \{0,1\}^n \Rightarrow \{0,1\}$ (entonces, $N = 2^n$)



El algoritmo de Grover

- El algoritmo usa $O(\sqrt{N})$ iteraciones, cada una con una llamada al oráculo y otra al operador de difusión de Grover
- Cada aplicación del oráculo "marca" los estados que verifican la condición
- El operador de difusión "amplifica" las probabilidades de los estados marcados



El algoritmo de Grover

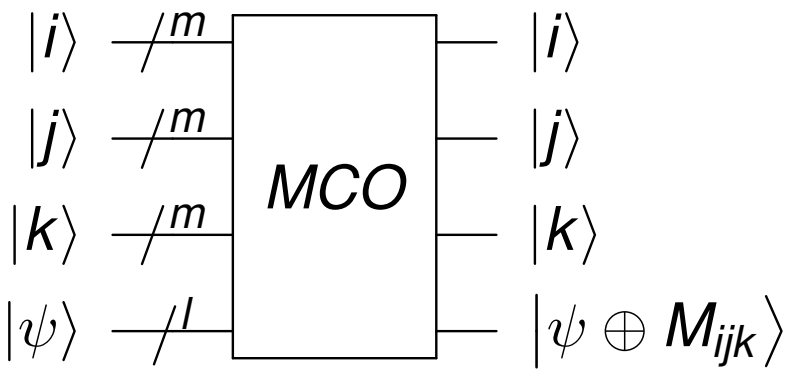
- Al medir, obtendremos un valor x tal que $f(x) = 1$ con una probabilidad que depende de:
  - El número de iteraciones realizadas
  - La proporción de valores x que verifican la condición
- Por ejemplo, si hay exactamente $\frac{N}{4}$ soluciones, entonces una iteración dará una respuesta correcta con probabilidad 1
- En el caso general, se necesitan $O(\sqrt{\frac{N}{k}})$ iteraciones, siendo k el número de soluciones (y suponiendo que $k \leq \frac{N}{2}$)

Parte IV

Solución cuántica para nuestro problema

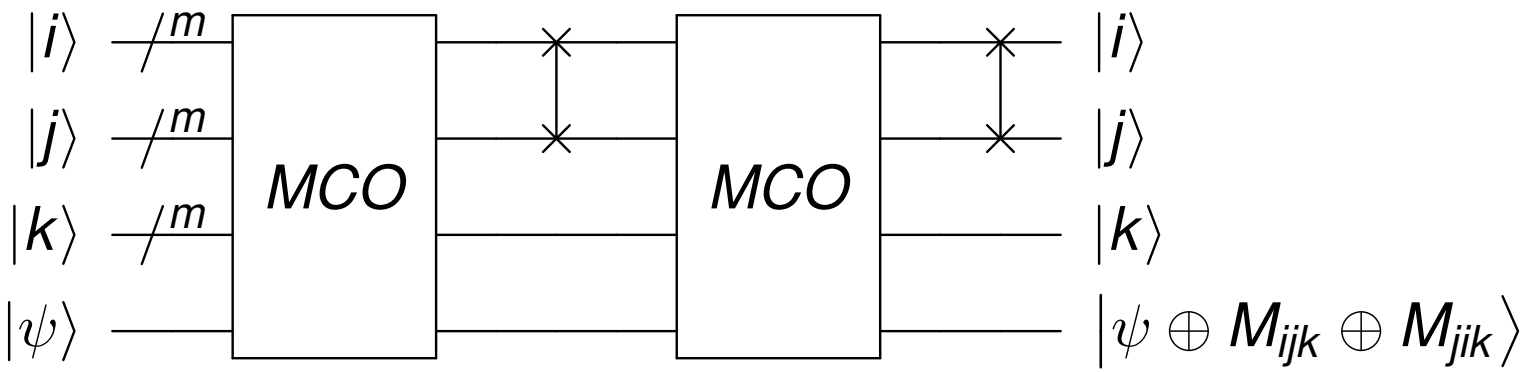
Oráculo para la constantes de multiplicación

En nuestro caso, partimos de un oráculo mediante el cual podemos consultar las constantes de multiplicación del álgebra



Oráculo para el algoritmo de Grover

A partir de ese oráculo, construimos el que se usará en el algoritmo de Grover (caso binario)



Algoritmo

Algoritmo cuántico: Determinación de la conmutatividad de un álgebra

Elegir uniformemente al azar un entero $l \in \left\{0, \ldots, \sqrt{\frac{n^3}{2}} - 1\right\}$

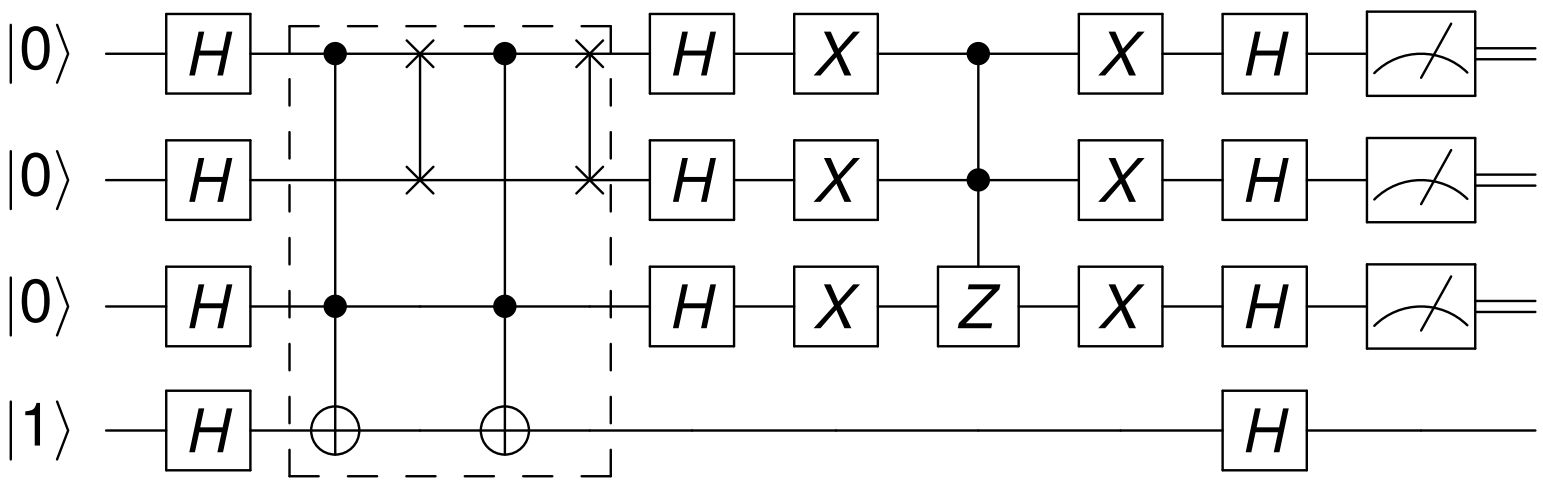
Inicializar el estado a $\sum_{x=1}^{n^3} \frac{1}{\sqrt{n^3}} |x\rangle$
Aplicar l iteraciones del algoritmo de Grover
Realizar una medición para obtener *ijk*
Consultar el oráculo de las constantes con *ijk* y con *jik*
Si $M_{ijk} \neq M_{jik}$, devolver NO
Si no, devolver SÍ

Resultados teóricos

- El número de consultas al oráculo de nuestro algoritmo es $\Theta(\sqrt{n^3})$
- La respuesta “NO” siempre se da de forma exacta
- El error en la respuesta “SÍ” es una constante menor que 1
- Se puede demostrar que cualquier otro algoritmo cuántico con las mismas propiedades precisará también $\Theta(\sqrt{n^3})$ consultas al oráculo

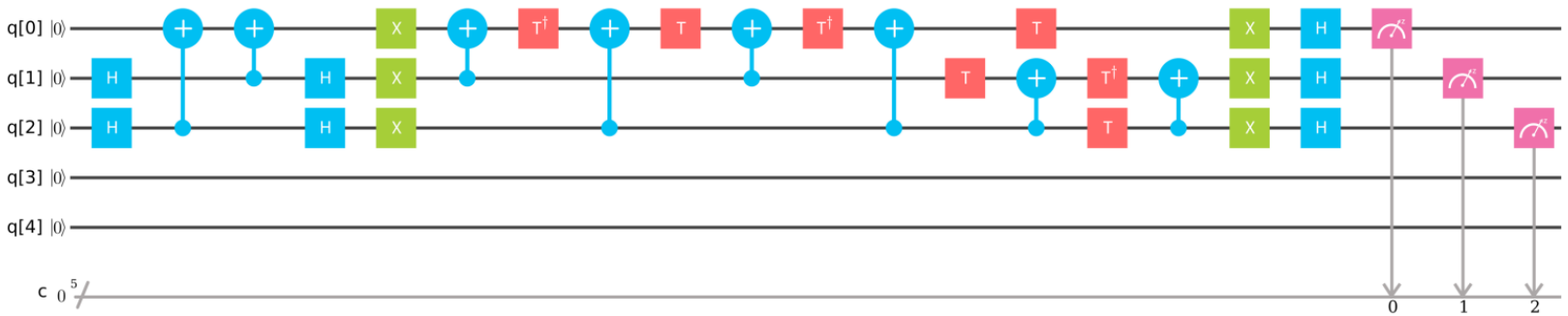
Experimentos en la IBM Quantum Experience

- Hemos probado un caso particular de nuestro algoritmo en el ordenador cuántico *ibmqx4*
- Como el ordenador tiene 5 qubits, elegimos $n = 2$ y un álgebra no conmutativa
- Nuestro circuito será



Experimentos en la IBM Quantum Experience

- Tras una serie de simplificaciones, obtenemos un circuito equivalente



Experimentos en la IBM Quantum Experience

- En el simulador, se obtiene la distribución esperada (dos estados con igual probabilidad)
- En la ejecución real se observa cierto ruido, pero se obtienen los estados correctos con probabilidad casi $\frac{2}{3}$