

Una introducción práctica a la computación cuántica

Elías F. Combarro (Universidad de Oviedo)

Doctorado en Informática - Universidad de Almería -
Octubre 2019



Parte I

Introducción: computación cuántica... ¿el futuro de la computación?

¿Por qué estudiar computación cuántica?

IBM's new 53-qubit quantum computer is its biggest yet

The system will go online in October.

BY STEPHEN SHANKLAND | SEPTEMBER 18, 2019 5:05 AM PDT



This Startup Raised \$2.7 Million To Build The Java Of Quantum Computing



Alex Knapp
Forbes Staff
Science

I write about the future of science, technology, and culture.



HOME | GLOBAL

IBM's Quantum Computing Project Backed Up By Berlin's 650 Million Euros

By Ritchelle Ann De Castro
Sep 11, 2019 07:26 PM

Google Says That They Have Just Reached Quantum Supremacy

Quantum computing will change the world.

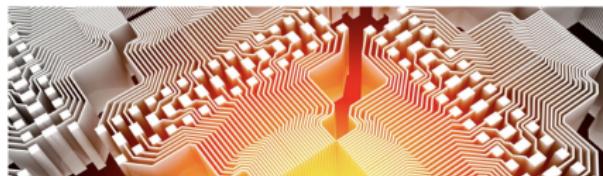


By Donovan Alexander
September 22nd, 2019

Q-CTRL raises \$15M for software that reduces error and noise in quantum computing hardware

Ingrid Lunden @ingridlunden | 3:00 pm CEST • September 10, 2019

Comment



Quantum Computing Holds Promise for the Public Sector

Quantum computers can vault far past today's systems. They could help resolve issues around health care and policy outcomes, but technologists, academia and government will need to collaborate to make them truly useful.

BY TOD NEWCOMBE / SEPTEMBER 2019

Department of Energy

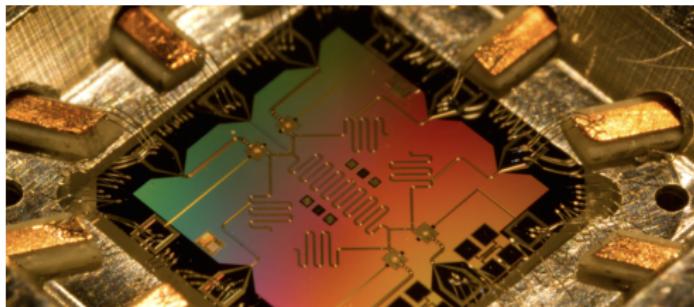
Department of Energy Announces \$60.7 Million to Advance Quantum Computing and Networking

AUGUST 29, 2019



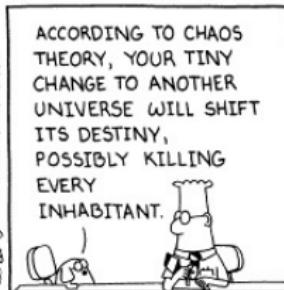
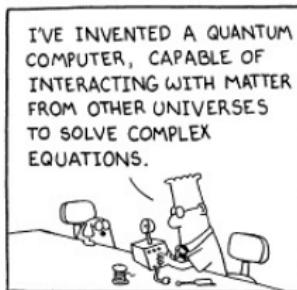
¿Qué problemas podremos resolver con un ordenador cuántico?

- Aceleración de tareas de búsqueda
- Factorización de números
- Resolución de sistemas de ecuaciones lineales
- Criptografía y comunicación cuánticas
- Simulación de procesos químicos y físicos
- Problemas de optimización
- Quantum Machine Learning



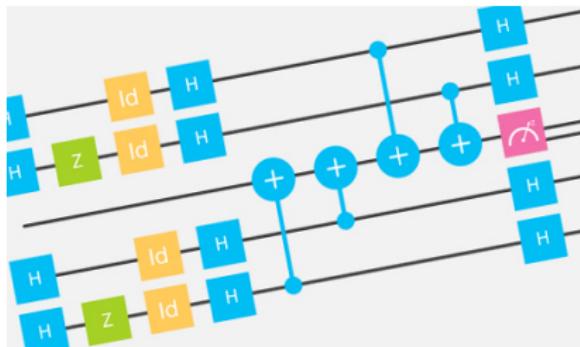
Objetivos de este curso

- Comprender los conceptos fundamentales de la computación cuántica
- Conocer algunos de los principales algoritmos cuánticos
- Practicar con simuladores cuánticos
- Ejecutar algoritmos... **¡en un ordenador cuántico real!**
- Todo ello sin morir en el intento (si es posible)



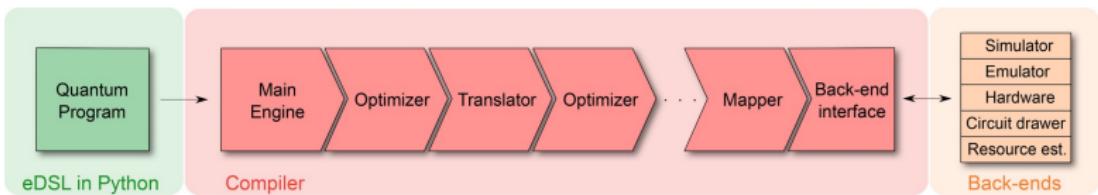
Recursos

- IBM Quantum Experience
 - Acceso online gratuito a simuladores (hasta 32 qubits) y **ordenadores cuánticos reales** (5 y 14 qubits)
 - Diferentes topologías y lenguajes (python, qasm)
 - Lanzado en mayo de 2016
 - <https://quantum-computing.ibm.com/>
- Quirk
 - Simulador online (hasta 16 qubits)
 - Gran número de puertas y opciones de visualización
 - <http://algassert.com/quirk>



Recursos (2)

- ProjectQ
 - Librería en python para circuitos cuánticos
 - Alto nivel
 - Independiente de la plataforma (distintos backends)
 - Simuladores y emuladores optimizados
 - <https://projectq.ch/>
- Ocean
 - Librería en python para computación cuántica adiabática (D-Wave)
 - Orientada a problemas específicos (QUBO, Quantum annealing...)
 - <https://ocean.dwavesys.com/>



Así es (y así suena) el IBM Q

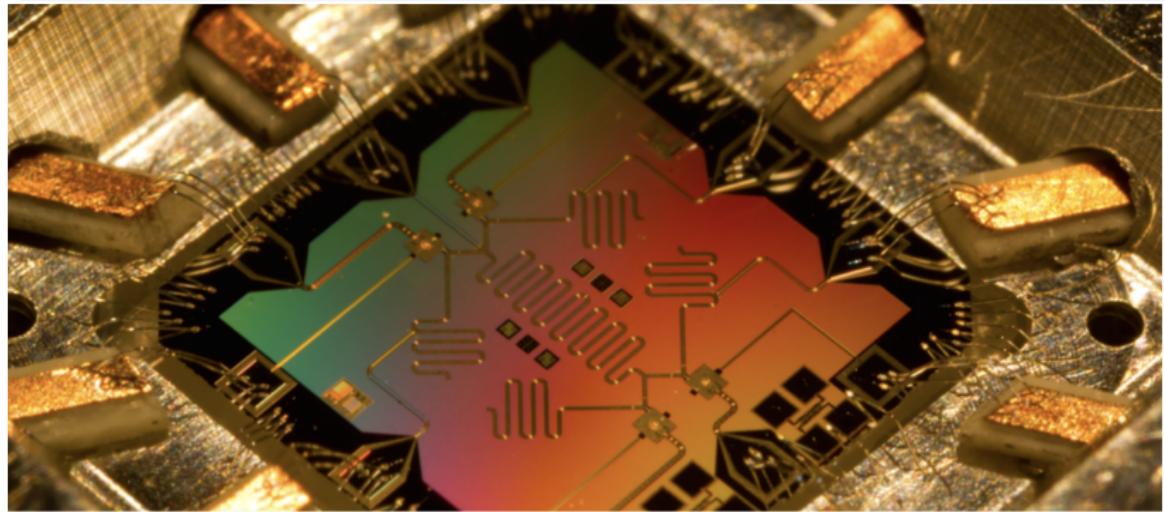


The Sounds of IBM: IBM Q

¿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



Parte II

Sistemas de un qubit: un qubit para gobernarlos a todos

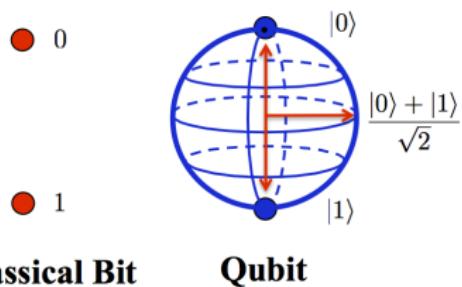
Qubits

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

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

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

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



Medida de un qubit

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



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).

$$H(t)|\psi(t)\rangle = i\hbar \frac{\partial}{\partial t}|\psi(t)\rangle$$

- 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

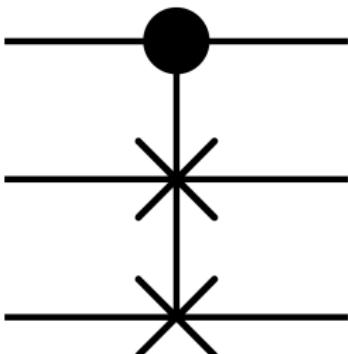
$$UU^\dagger = U^\dagger U = I$$

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
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
siendo $\bar{a}, \bar{b}, \bar{c}, \bar{d}$ los conjugados de los números complejos a, b, c, d .

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

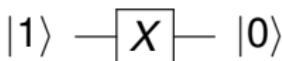
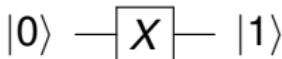
$$|(a\alpha + b\beta)|^2 + |(c\alpha + d\beta)|^2 = 1$$

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 (notación del modelo de circuitos)



es decir, actúa como un NOT

- Su acción sobre un qubit general sería

$$\alpha |0\rangle + \beta |1\rangle \xrightarrow{\boxed{X}} \beta |0\rangle + \alpha |1\rangle$$

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

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

$$|1\rangle \xrightarrow{H} \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

- Se suele denotar

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

y

$$|-\rangle := \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

La puerta Z

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

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

- Su acción es

$$|0\rangle \xrightarrow{\boxed{Z}} |0\rangle$$

$$|1\rangle \xrightarrow{\boxed{Z}} -|1\rangle$$

Otras puertas

- Puerta Y

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

- Puerta T

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

- Puerta S

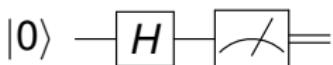
$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{pmatrix}$$

- La puerta $R(\alpha)$ o puerta de fase, que depende de un parámetro (el ángulo α)

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

Hello, quantum world!

- ¡Nuestro primer circuito cuántico!



- Tras aplicar la puerta H el estado del qubit será

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

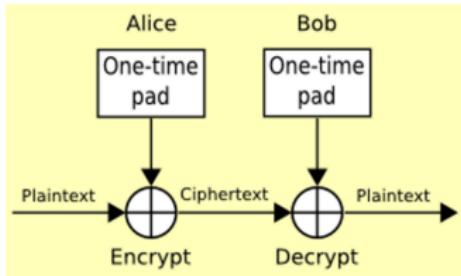
- Al medir, obtendremos 0 o 1, cada uno con el 50 % de probabilidad: tenemos un circuito que produce bits perfectamente aleatorios

Parte III

El protocolo BB84: Alice, Eve, Bob
y otras chicas del montón

One-time pad: la pescadilla que se muerde la cola

- Alice quiere enviarle un mensaje m a Bob sin que la cotilla Eve se entere de su contenido
- Si Alice y Bob comparten previamente una cadena k de bits aleatorios, la solución es fácil
 - Alice calcula $x = m \oplus k$ y se lo envía a Bob
 - Para Eve, x tiene toda la apariencia de una cadena aleatoria
 - Pero Bob puede obtener m con la operación $x \oplus k$
- El problema es que k tiene que ser tan larga como m y no se puede reutilizar así que... ¿cómo enviar k ?



BB84: En casa de Alice

- En 1984, Bennett y Brassard propusieron un protocolo cuántico para enviar k de forma segura
- Alice comienza generando una cadena de bits aleatorios
- Esto lo puede hacer fácilmente con un ordenador cuántico (puerta H + medida)
- A continuación, para cada bit elige aleatoriamente si lo codifica en la base $\{|0\rangle, |1\rangle\}$ o en la base $\{|+\rangle, |-\rangle\}$ (con $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ y $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$)
- De nuevo, esto lo puede hacer fácilmente con puertas H y X
- Alice envía los qubits resultantes a Bob

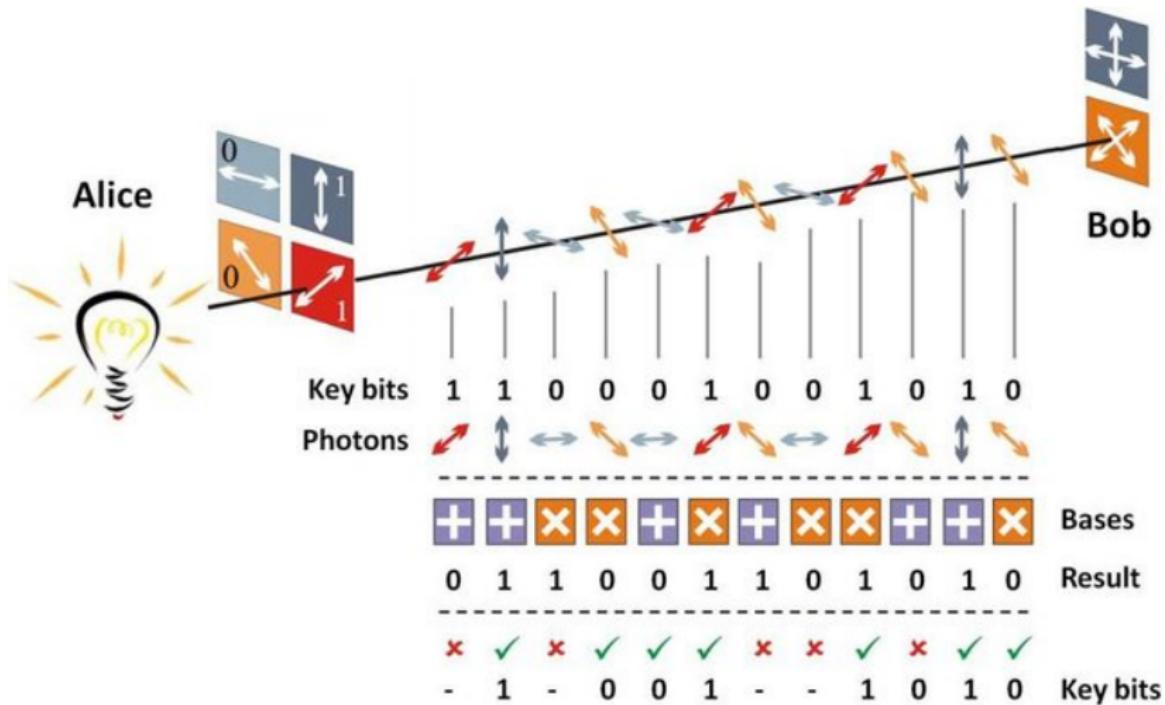
BB84: En casa de Bob

- Por cada qubit que recibe, Bob decide si medirlo en la base $\{|0\rangle, |1\rangle\}$ o en la base $\{|+\rangle, |-\rangle\}$
- Esto lo puede hacer aplicando (o no) la puerta H antes de medir
- Anota el resultado de cada medida y la base en la que la obtuvo:
 - Si midió en la base $\{|0\rangle, |1\rangle\}$ anota 0 si obtiene $|0\rangle$ y 1 si obtiene $|1\rangle$
 - Si midió en la base $\{|+\rangle, |-\rangle\}$ anota 0 si obtiene $|+\rangle$ y 1 si obtiene $|-\rangle$

BB84: Alice y Bob al teléfono

- Tras el proceso de envío y medición, Alice y Bob se ponen en contacto por un canal de comunicación clásico (no necesariamente seguro)
- Bob anuncia en qué base ha medido cada qubit y Alice le dice en qué base lo había codificado
- Bob NO anuncia qué resultados ha obtenido
- En aquellos qubits que Bob ha medido en la base correcta, sabe el bit que quería enviar Alice
- El resto se descartan (conservarán aproximadamente la mitad)

BB84: El protocolo en una imagen

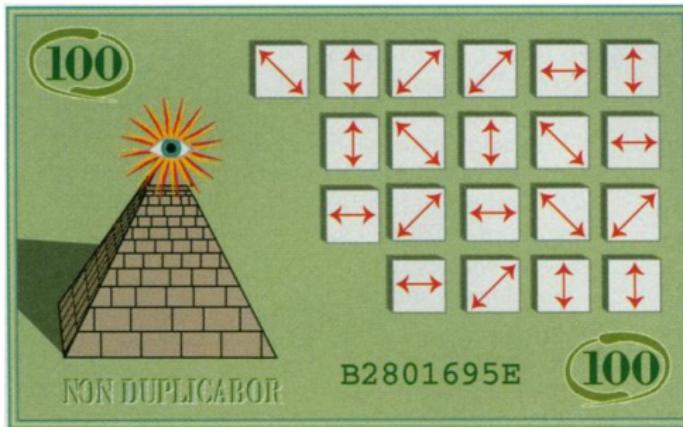


BB84: Mientras tanto, en casa de Eve...

- Imaginemos que Eve tiene acceso a los qubits que Alice envía a Bob
- Eve puede intentar medir y reenviar el qubit a Bob
- Por el principio de incertidumbre, es imposible que Eve distinga entre las cuatro posibilidades $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ ya que no sabe la base en que ha codificado Alice
- Si elige una base al azar, se equivocará en la mitad de las ocasiones en promedio y Alice y Bob pueden detectarlo (compartiendo algunos de los bits de la clave para comprobar)
- Eve tampoco puede copiar los qubits y esperar a la comunicación pública de Alice y Bob (teorema de no clonación)

Otros protocolos que usan qubits independientes

- Aunque el uso de qubits independientes no explota toda la potencia de la computación cuántica, sí que permite algunas aplicaciones muy importantes
- Por ejemplo:
 - Otros protocolos criptográficos de distribución de claves (QKD): B92, SARG04, Six-state protocol...
 - El concepto de dinero cuántico (Wiesner)
 - El detector de bombas de Elitzur y Vaidman



Parte IV

Sistemas de dos qubits: mucho
más que uno más uno

Trabajando con dos qubits

- Cada qubit puede estar en los estados $|0\rangle$ y $|1\rangle$
- Así que para dos qubits tenemos cuatro posibilidades:

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

que también se denotan

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

o

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

- Como podemos tener superposiciones, 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

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

Medida de 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 ambos qubits, obtendremos:
 - 00 con probabilidad $|\alpha_{00}|^2$ y el nuevo estado será $|00\rangle$
 - 01 con probabilidad $|\alpha_{01}|^2$ y el nuevo estado será $|01\rangle$
 - 10 con probabilidad $|\alpha_{10}|^2$ y el nuevo estado será $|10\rangle$
 - 11 con probabilidad $|\alpha_{11}|^2$ y el nuevo estado será $|11\rangle$
- Es una situación análoga a la que teníamos con un solo qubit, pero ahora con cuatro posibilidades

Medida de un qubit en un estado de dos qubits

- Sobre un estado

$$|\psi\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle$$

también podemos medir solo un qubit

- 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

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

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:

$$|00\rangle \rightarrow |00\rangle \quad |01\rangle \rightarrow |01\rangle$$

$$|10\rangle \rightarrow |11\rangle \quad |11\rangle \rightarrow |10\rangle$$

La puerta *CNOT*

- Su acción con elementos $x, y \in \{0, 1\}$ es, por tanto:

$$\begin{array}{c} |x\rangle \xrightarrow{\bullet} |x\rangle \\ |y\rangle \xrightarrow{\oplus} |y \oplus x\rangle \end{array}$$

- Es una puerta muy importante, puesto que nos permite:
 - Realizar entrelazamientos (más sobre ello enseguida)
 - Copiar información clásica, ya que:

$$|00\rangle \rightarrow |00\rangle$$

$$|10\rangle \rightarrow |11\rangle$$

El teorema de no clonación

- **No hay** ninguna puerta cuántica de dos qubits (tampoco de más) que nos permita copiar un qubit cualquiera
- La demostración es sencilla: supongamos que hay una puerta U tal que $U|00\rangle = |00\rangle$ y $U|10\rangle = |11\rangle$
- Entonces, por linearidad

$$U\left(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)\right) = \frac{1}{\sqrt{2}}(U|00\rangle + U|10\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

- Pero

$$\frac{|00\rangle + |10\rangle}{\sqrt{2}} = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)|0\rangle$$

así que debería ser

$$U\left(\frac{|00\rangle + |10\rangle}{\sqrt{2}}\right) = \frac{(|0\rangle + |1\rangle)}{\sqrt{2}} \frac{(|0\rangle + |1\rangle)}{\sqrt{2}} \neq \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Entrelazamiento cuántico: la fantasmal acción a distancia

- Un estado de dos qubits $|\psi\rangle$ es un estado producto si se puede escribir como

$$|\psi\rangle = |\psi_1\rangle |\psi_2\rangle$$

donde $|\psi_1\rangle$ y $|\psi_2\rangle$ son estados de un qubit

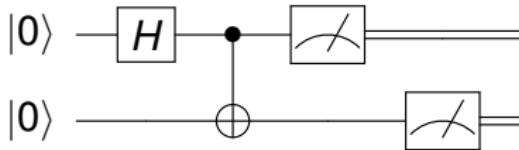
- Un estado **entrelazado** es un estado que no es un estado producto
- Ejemplos de estados entrelazados (estados de Bell):

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

$$\frac{|01\rangle + |10\rangle}{\sqrt{2}} \quad \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Hello, entangled world!

- Podemos construir los estados de Bell con circuitos sencillos



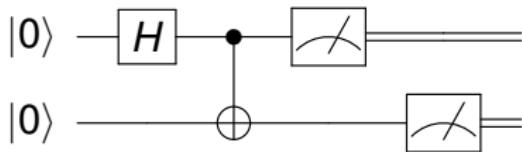
- Inicialmente, el estado del sistema es $|00\rangle$
- Tras aplicar la puerta H el estado es

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

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

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

Hello, entangled world!



- Antes de 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!

Parte V

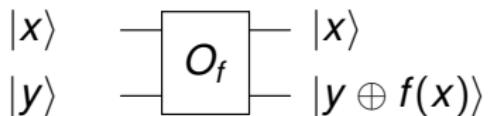
El algoritmo de Deutsch: el primer
algoritmo cuántico

El algoritmo de Deutsch: planteamiento del problema

- En 1985, David Deutsch propuso un algoritmo que ilustra las capacidades de los ordenadores cuánticos
- El problema que resuelve es de mayor importancia teórica que práctica y fue luego generalizado por el propio Deutsch en colaboración con Jozsa
- Nos dan un circuito (**oráculo**) que implementa una función booleana de un bit y nos piden distinguir si es constante (siempre devuelve el mismo valor) o equilibrada (devuelve 0 para una entrada y 1 para la otra)
- En el caso clásico necesitaríamos evaluar la función en las dos entradas. En el caso cuántico, basta con una evaluación... en superposición

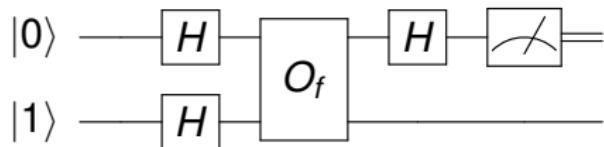
El algoritmo de Deutsch: el oráculo

- Un oráculo es una caja negra, un circuito del que desconocemos su interior
- Este circuito computa, de forma reversible, una cierta función f (en nuestro caso, de una sola entrada)
- Para que sea reversible, necesita tener tantas entradas como salidas e implementar el resultado a través de un XOR



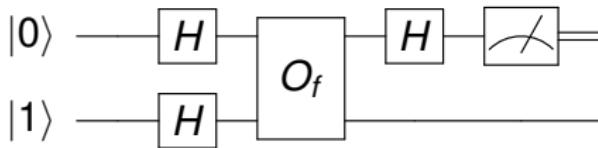
El algoritmo de Deutsch: el circuito

- El circuito cuántico para resolver el problema es muy sencillo



- Si el resultado de la medida es 0, la función era constante
- Si el resultado de la medida es 1, la función era equilibrada

El algoritmo de Deutsch: la magia



- El estado inicial de los qubits es $|0\rangle |1\rangle$
- Tras las puertas H tenemos

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

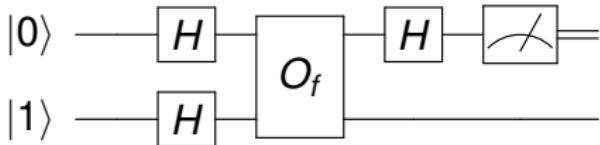
que es lo mismo que

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

- Al aplicar el oráculo, que es lineal, obtenemos

$$\frac{|0\rangle (|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle)}{2} + \frac{|1\rangle (|0 \oplus f(1)\rangle - |1 \oplus f(1)\rangle)}{2}$$

El algoritmo de Deutsch: la magia (2)



- Si $f(0) = 0$, tenemos

$$|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle = |0\rangle - |1\rangle$$

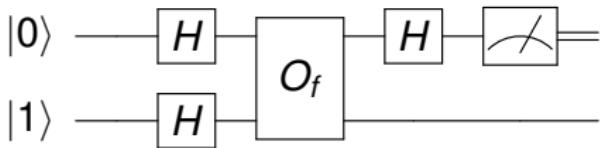
- Sin embargo, si $f(0) = 1$ tendremos

$$|0 + f(0)\rangle - |1 \oplus f(0)\rangle = |0 \oplus 1\rangle - |1 \oplus 1\rangle = |1\rangle - |0\rangle = -(|0\rangle - |1\rangle)$$

- Para $f(1)$ sucede lo mismo, por lo que el estado total es

$$\frac{(-1)^{f(0)} |0\rangle (|0\rangle - |1\rangle)}{2} + \frac{(-1)^{f(1)} |1\rangle (|0\rangle - |1\rangle)}{2}$$

El algoritmo de Deutsch: la magia (3)



- Ese estado también se puede escribir como

$$\frac{|0\rangle(|0\rangle - |1\rangle)}{2} + \frac{(-1)^{f(0)+f(1)}|1\rangle(|0\rangle - |1\rangle)}{2}$$

- Así que si $f(0) = f(1)$, tendremos

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

y al aplicar la última H y medir obtendremos 0

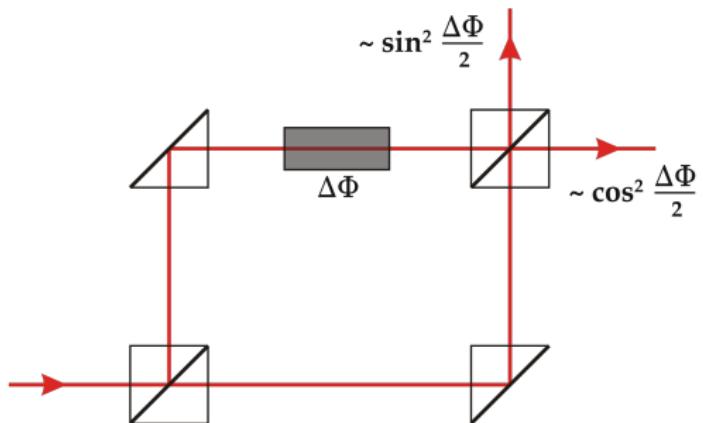
- Pero si $f(0) \neq f(1)$, el estado es

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

y, entonces, obtendremos 1

El algoritmo de Deutsch: algunos comentarios

- Al aplicar el oráculo se produce un retroceso de fase (phase kickback): aunque sólo actuamos sobre un qubit hay un efecto sobre todo el estado
- El algoritmo de Deutsch explota un fenómeno de interferencia semejante al de algunos procesos físicos (experimento de la doble rendija, interferómetro de Mach-Zender)

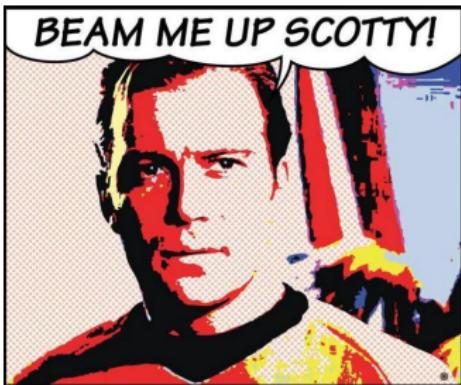


Parte VI

Teleportación cuántica y
codificación superdensa:
explotando el entrelazamiento

Teleportación cuántica: Quantum me up, Scotty!

- ¿Cómo podemos hacer llegar a Bob un qubit $|\psi\rangle$ que tiene Alice?
- Nos interesa el caso en que $|\psi\rangle$ es genérico (Alice no tiene por qué saber qué estado tiene)
- Lo podemos conseguir si Alice y Bob comparten previamente un par de qubits entrelazados $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$



Teleportación cuántica: la parte de Alice

- Alice y Bob comparten el par de Bell $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- Alice aplica una puerta CNOT al qubit $|\psi\rangle = a|0\rangle + b|1\rangle$ y a su parte del par de Bell. Tendremos

$$\frac{1}{\sqrt{2}}(a(|000\rangle + |011\rangle) + b(|110\rangle + |101\rangle))$$

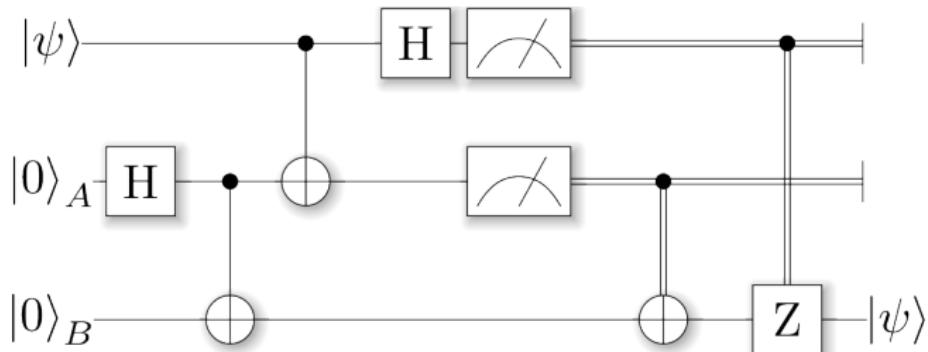
- Alice aplica una puerta H al qubit a teleportar. Se obtiene

$$\begin{aligned} \frac{1}{\sqrt{2}}(&|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(b|0\rangle + a|1\rangle) \\ &+ |10\rangle(a|0\rangle - b|1\rangle) + |11\rangle(-b|0\rangle + a|1\rangle)) \end{aligned}$$

- Alice mide sus dos qubits y envía el resultado a Bob por un canal clásico

Teleportación cuántica: la parte de Bob

- Bob usa el segundo bit recibido de Alice para decidir si aplica una puerta X a su qubit
- Y usa el primero para decidir si le aplica una puerta Z



Teleportación cuántica: la letra pequeña

- Obviamente, no se teletransporta materia sino solo información
- Cuando Alice mide su qubit, lo pierde (si no, no se cumpliría el teorema de no clonación)
- Para teletransportar un qubit, son necesarios dos bits y un par de qubits entrelazados
- La teletransportación no se puede producir de forma instantánea, es necesaria la comunicación clásica (teorema de no comunicación)
- La teletransportación cuántica se ha demostrado experimentalmente a distancias de varios kilómetros

Codificación superdensa: dos por el precio de uno (o algo así)

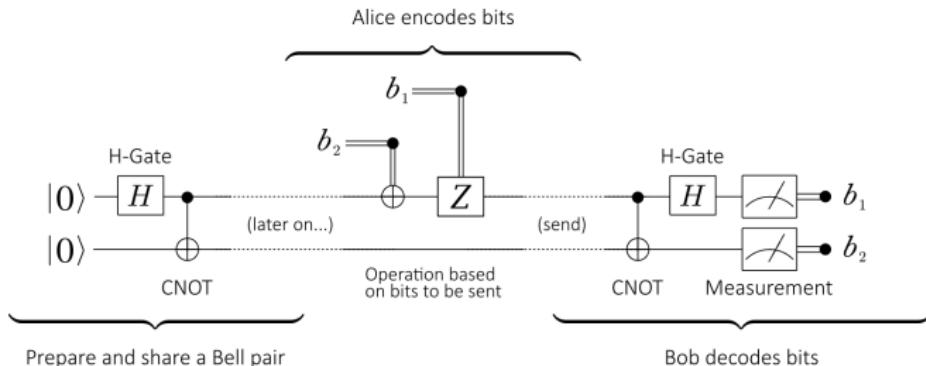
- Hemos visto que, en presencia de un par de Bell, podemos enviar un qubit mediante dos bits clásicos
- Pero... ¿cuántos bits clásicos podemos enviar por cada qubit?
- Un qubit sólo nos permite comunicar un bit clásico (Teorema de Holevo)
- Sin embargo, si Alice y Bob ya comparten un par de Bell... ¡podemos transmitir dos bits con un solo qubit!
- Este protocolo es, en cierto modo, el inverso de la teletransportación cuántica

Codificación superdensa: la parte de Alice

- Necesitamos que Alice y Bob hayan compartido previamente un estado $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- Alice quiere enviar a Bob dos bits b_1 y b_2
- Si $b_2 = 1$, aplica una puerta X sobre su parte del par compartido
- Si $b_1 = 1$, aplica una puerta Z sobre su parte del par compartido
- A continuación, envía su qubit a Bob

Codificación superdensa: la parte de Bob

- Bob recibe el qubit enviado por Alice
- Aplica una puerta CNOT controlada por el qubit recibido
- Aplica una puerta H al qubit de Alice
- Mide y recupera b_1 y b_2



Codificación superdensa: un ejemplo

- Supongamos que Alice quiere transmitir 11
- Comenzamos con $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- Tras las operaciones de Alice, tendremos $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$
- Con el CNOT de Bob se obtiene

$$\frac{1}{\sqrt{2}}(|01\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|1\rangle$$

- Y con la H se consigue $|11\rangle$

Parte VII

Sistemas de muchos qubits:
creciendo exponencialmente

Sistemas de n qubits

- Cada uno de los n qubits puede estar en los estados $|0\rangle$ y $|1\rangle$
- Así que para el conjunto de los n qubits tenemos 2^n posibilidades:

$$|00\dots0\rangle, |00\dots1\rangle, \dots, |11\dots1\rangle$$

o simplemente

$$|0\rangle, |1\rangle, \dots, |2^n - 1\rangle$$

- Un estado genérico del sistema será

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \dots + \alpha_{2^n-1} |2^n - 1\rangle$$

donde los α_i son números complejos que cumplen

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

Medida de un estado de n qubits

- Supongamos que tenemos un estado genérico de n qubits

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \dots + \alpha_{2^n-1} |2^n - 1\rangle$$

- Si medimos todos los qubits, obtendremos:
 - 0 con probabilidad $|\alpha_0|^2$ y el nuevo estado será $|0\dots00\rangle$
 - 1 con probabilidad $|\alpha_1|^2$ y el nuevo estado será $|0\dots01\rangle$
 - ...
 - $2^n - 1$ con probabilidad $|\alpha_{2^n-1}|^2$ y el nuevo estado será $|1\dots11\rangle$
- Es una situación análoga a la que teníamos con un solo qubit, pero ahora con 2^n posibilidades

Medida de un qubit en un estado de n qubits

- Tenemos un estado

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \dots + \alpha_{2^n-1} |2^n - 1\rangle$$

- 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

Puertas cuánticas de n qubits

- Un estado de n qubits es

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \dots + \alpha_{2^n-1} |2^n - 1\rangle$$

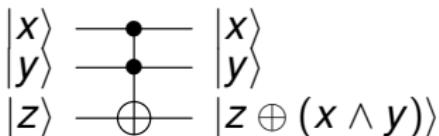
- Se representa mediante el vector columna

$$\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{2^n-1} \end{pmatrix}$$

- Así, una puerta cuántica de dos qubits es una matriz unitaria U de tamaño $2^n \times 2^n$

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)

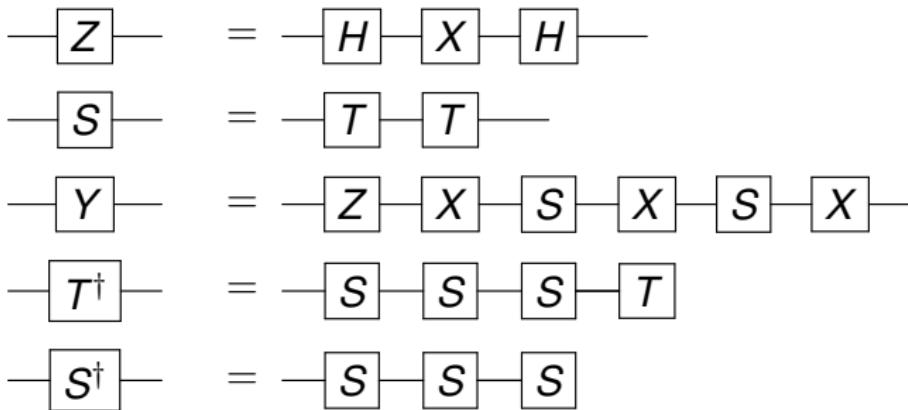
Puertas universales en la computación cuántica

- 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 imaqx de IBM).

Equivalencias entre puertas cuánticas

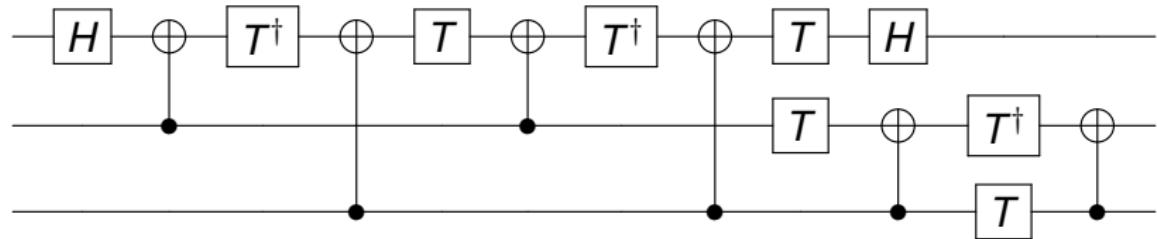


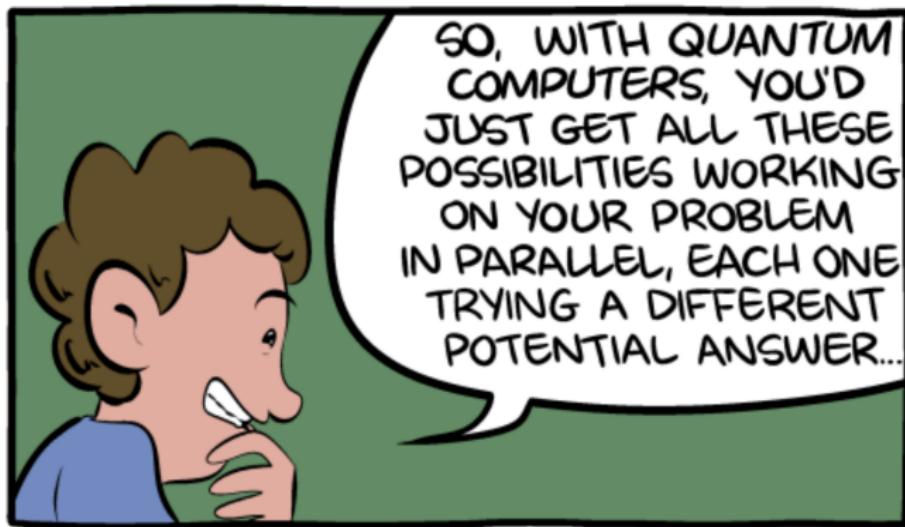
Figura: Puerta de Toffoli (con target en el bit superior y control en los dos inferiores) a partir de $CNOTs$ y puertas de un qubit

Parte VIII

Todo lo que siempre quisiste saber
sobre el paralelismo cuántico y
nunca te atreviste a preguntar

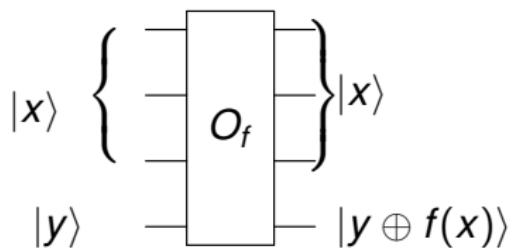
Leyendas urbanas sobre el paralelismo cuántico

- Pero... ¿los ordenadores cuánticos no prueban todas las 2^n posibilidades en paralelo?
- La respuesta es... sí y no



Evaluando una función: consultando al oráculo

- Como sabemos, en computación cuántica, todas las operaciones son reversibles
- Así que lo habitual es tener un circuito que calcula una función f sin cambiar sus entradas y “sumando” el resultado a la salida
- Este tipo de circuito se suele llamar un oráculo para f (lo hemos visto ya para f de un solo bit en el algoritmo de Deutsch)



Evaluando una función en paralelo: la magia de la superposición

- Supongamos que tenemos un oráculo para una función $f(x)$ cuya entrada es un solo bit
- Sabemos que, con la puerta H , podemos poner un qubit en superposición
- Si partimos de el estado $|0\rangle|0\rangle$ y aplicamos H sobre el primer qubit tendremos

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

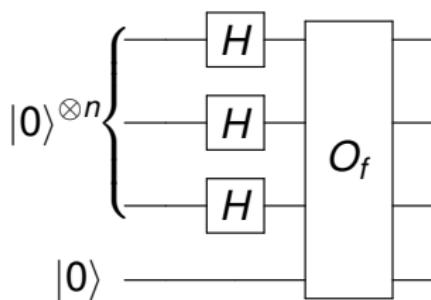
- Si ahora aplicamos O_f , por linearidad tendremos

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

- ¡Hemos evaluado la función en dos valores con una sola llamada!

Evaluando una función en paralelo: el poder del producto tensorial

- Podemos hacer lo mismo con una función $f(x_1, x_2, \dots, x_n)$ usando el circuito de la figura



- Al aplicar las puertas H tenemos

$$\frac{(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) \cdots (|0\rangle + |1\rangle)|0\rangle}{\sqrt{2^n}}$$

Evaluando una función en paralelo: el poder del producto tensorial (2)

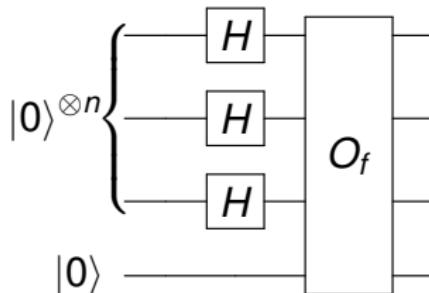
- Expadiendo todo se obtiene

$$\frac{(|0\dots 0\rangle + |0\dots 1\rangle + \dots + |1\dots 1\rangle) |0\rangle}{\sqrt{2^n}} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |0\rangle$$

- Y, al aplicar el oráculo, conseguiremos el estado

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle$$

- ¡Un número exponencial de evaluaciones por solo una!

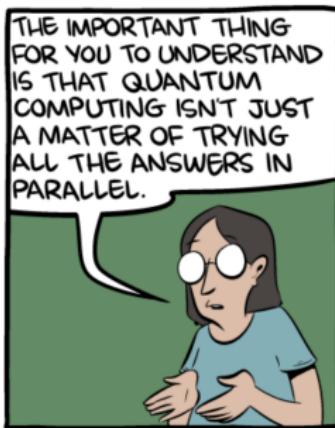


No es oro todo lo que reluce

- Y ahora... ¿cómo recuperamos los valores de $f(x)$?
- Para obtener un resultado, necesitamos realizar una medida
- Pero entonces tendremos un estado de la forma

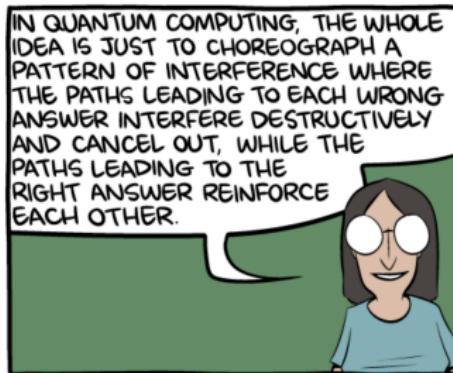
$$|c\rangle |f(c)\rangle$$

- Es decir, accedemos al valor de la función para una entrada al azar (no hemos ganado nada)



Las interferencias salen al rescate

- ¿Cómo podemos aprovechar las 2^n evaluaciones y extraer información útil?
- La solución es... ¡producir interferencias!
- Las amplitudes de los estados pueden ser negativas
- Si conseguimos “anular” entre sí las amplitudes de los estados que no nos interesan, aumentará la probabilidad de obtener la respuesta que buscamos
- Esto, en general, no es tarea sencilla, pero se puede hacer en algunos casos muy interesantes

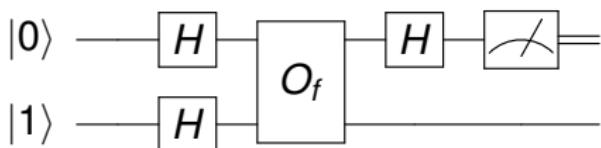


Parte IX

El algoritmo de Deutsch-Jozsa:
resolviendo muy rápido un
problema que no le interesa a nadie

Recordatorio: el algoritmo de Deutsch

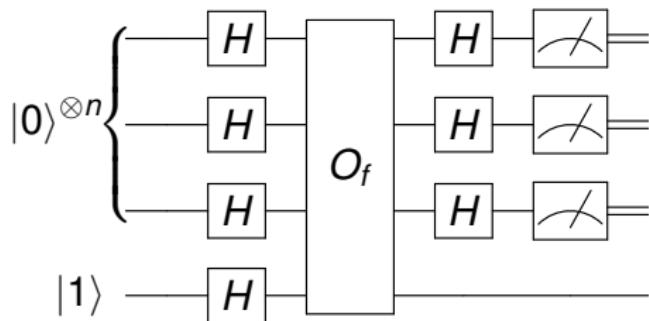
- Tenemos un oráculo para una función booleana $f(x)$ de una sola variable
- f puede ser constante (toma siempre el mismo valor) o equilibrada (toma valores distintos en 0 y en 1)
- Distinguir una situación de otra requiere, en el caso clásico, evaluar la función dos veces
- Con un ordenador cuántico, podemos resolver el problema con una sola evaluación de f
- La clave es usar el paralelismo cuántico en combinación con la interferencia



Subiendo el listón: el algoritmo de Deutsch-Jozsa

- El algoritmo de Deutsch-Jozsa resuelve un tipo de problema llamado **problema de promesa**
 - Nos dan una función booleana $f(x_1, \dots, x_n)$
 - Nos **prometen** que f es o bien constante (siempre 0 o 1) o bien equilibrada (0 para la mitad de las entradas y 1 para el resto)
 - Tenemos que determinar en cuál de los dos casos nos encontramos
- Con un algoritmo clásico determinista necesitamos (en el peor caso) $2^{n-1} + 1$ evaluaciones de f
- Con el algoritmo de Deutsch-Jozsa es suficiente con evaluar f **una sola vez**

Círculo del algoritmo de Deutsch-Jozsa



Pasos del algoritmo de Deutsch-Jozsa

- ① Creamos el estado $|0 \dots 0\rangle |1\rangle$
- ② Utilizamos puertas de Hadamard para crear la superposición

$$\sum_{x \in \{0,1\}^n} \frac{1}{\sqrt{2^{n+1}}} |x\rangle (|0\rangle - |1\rangle)$$

- ③ Aplicamos el oráculo, obteniendo

$$\sum_{x \in \{0,1\}^n} \frac{1}{\sqrt{2^{n+1}}} |x\rangle (|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle) =$$

$$\sum_{x \in \{0,1\}^n} \frac{(-1)^{f(x)}}{\sqrt{2^{n+1}}} |x\rangle (|0\rangle - |1\rangle)$$

Pasos del algoritmo de Deutsch-Jozsa (2)

- ④ Aplicamos de nuevo puertas de Hadamard en los n primeros qubits y obtenemos

$$\sum_{y \in \{0,1\}^n} \sum_{x \in \{0,1\}^n} \frac{(-1)^{f(x)+x \cdot y}}{2^n \sqrt{2}} |y\rangle (|0\rangle - |1\rangle)$$

- ⑤ Finalmente, medimos en los n primeros qubits.
- ⑥ Si obtenemos $|0\rangle$, entonces la función es constante. Si no, es equilibrada.

Prueba de corrección del algoritmo

- La probabilidad de obtener $|0\rangle$ al medir es exactamente

$$\left(\sum_{x \in \{0,1\}^n} \frac{(-1)^{f(x)+x \cdot 0}}{2^n} \right)^2 = \left(\sum_{x \in \{0,1\}^n} \frac{(-1)^{f(x)}}{2^n} \right)^2$$

- Si f es constante, entonces esa suma es 1
- Si f es equilibrada, la suma es 0

Observaciones sobre el algoritmo de Deutsch-Jozsa

- El problema que se resuelve es académico, con poco interés práctico
- Pero... muestra cómo la computación cuántica puede obtener información global de una función con una sola evaluación
- La clave es que se usa:
 - Paralelismo cuántico (a través de la superposición)
 - Interferencia (constructiva y destructiva)
- Estas ideas son utilizadas en otros algoritmos como el de Bernstein-Vazirani o el de Simon

Parte X

El algoritmo de Grover: usando un ordenador cuántico para encontrar una aguja en un pajar

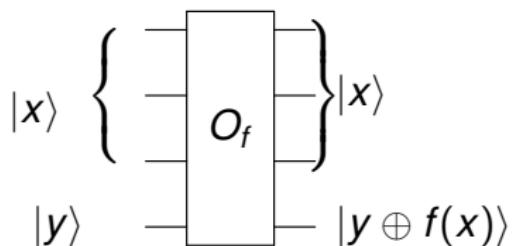
Planteamiento del problema

- El algoritmo de Grover permite resolver problemas de búsqueda
- Contamos con una lista (no estructurada) de N elementos
- De ellos, uno cumple una cierta condición y queremos encontrarlo
- Un algoritmo clásico necesitará $O(N)$ consultas de la lista
- El algoritmo de Grover requiere solo $O(\sqrt{N})$ consultas



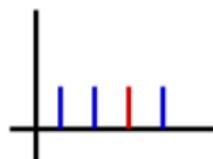
El oráculo

- Como en el algoritmo de Deutsch-Jozsa, contaremos con un oráculo
- Este oráculo calcula una función $f : \{0, 1\}^n \Rightarrow \{0, 1\}$ (con $N = 2^n$)
- El elemento buscado es aquel que verifica $f(x) = 1$

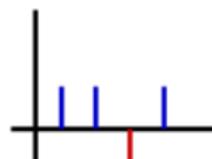


La idea del algoritmo

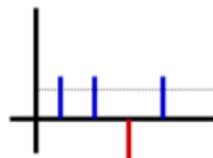
- El algoritmo de Grover se basa en la idea de **inversión con respecto a la media**



Original Amplitudes



Negate Amplitude



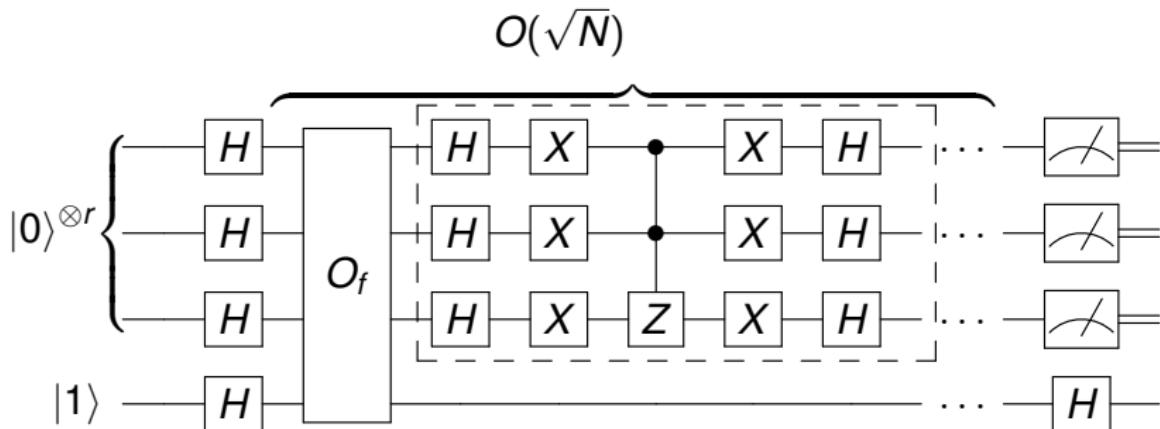
Average of all Amplitudes



Flip all Amplitudes around Avg

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



Análisis del algoritmo

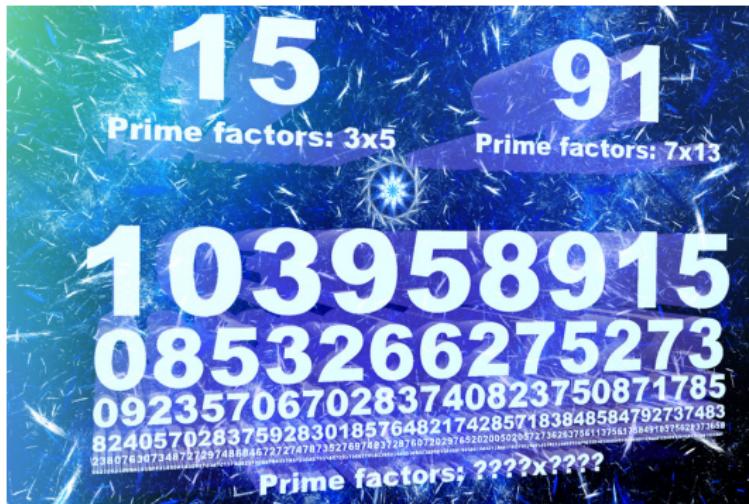
- Al medir, obtendremos un valor x tal que $f(x) = 1$ con una probabilidad que depende de:
 - El número de iteraciones realizadas
 - La proporción de valores x que verifican la condición
- Por ejemplo, si hay exactamente $\frac{N}{4}$ soluciones, entonces una iteración dará una respuesta correcta con 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 XI

El algoritmo de Shor: no diga
“factorizar”, diga “romper el RSA”

Factorización y el algoritmo de Shor

- El algoritmo de Shor es, posiblemente, el algoritmo cuántico más famoso
- Permite hallar factores de números de n bits en tiempo $O(n^2(\log n)(\log \log n))$
- El mejor algoritmo clásico conocido tiene una complejidad $O(e^{cn^{\frac{1}{3}}(\log n)^{\frac{2}{3}}})$
- Importantes consecuencias para la criptografía (RSA)



Pasos del algoritmo de Shor

- ① Dado N , comprobar que N no sea primo. Si es primo, terminar.
- ② Elegir aleatoriamente un número $1 < a < N$
- ③ Si $b = \text{mcd}(a, N) > 1$, devolver b y terminar
- ④ Encontrar el orden de a módulo N , es decir, $r > 0$ tal que $a^r \equiv 1 \pmod{N}$
- ⑤ Si r es impar, volver al paso 2
- ⑥ Calcular

$$x = a^{\frac{r}{2}} + 1 \pmod{N}$$

$$y = a^{\frac{r}{2}} - 1 \pmod{N}$$

- ⑦ Si $x = 0$, volver a 2. Si $y = 0$, tomar $r = \frac{r}{2}$ y volver a 5.
- ⑧ Calcular $p = \text{mcd}(x, N)$ y $q = \text{mcd}(y, N)$. Al menos uno de los dos será un factor no trivial de N

Prueba de la corrección del algoritmo de Shor

- Sabemos que

$$a^r \equiv 1 \pmod{N}$$

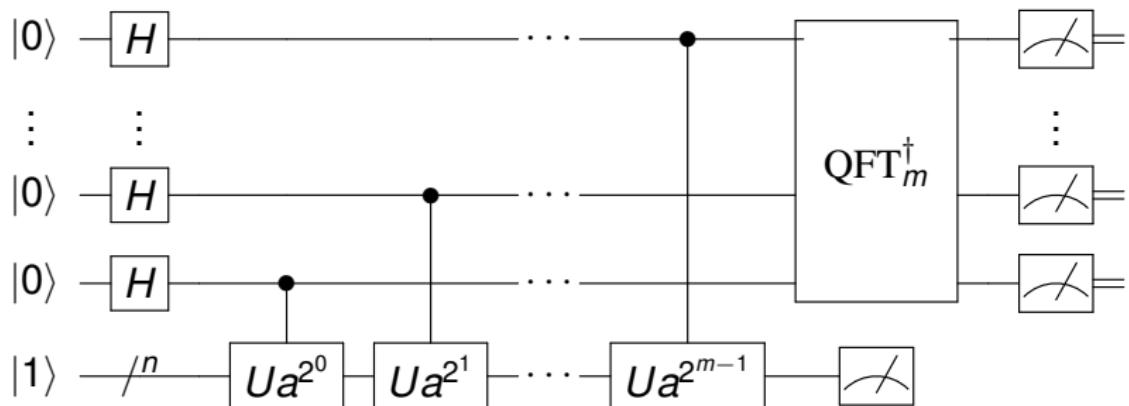
- Por tanto

$$x \cdot y \equiv (a^{\frac{r}{2}} + 1)(a^{\frac{r}{2}} - 1) \equiv (a^r - 1) \equiv 0 \pmod{N}$$

- Es decir, $x \cdot y$ es un múltiplo de N
- Como ni x ni y son múltiplos de N , p o q deben dividir a N
- Además, un análisis estadístico permite demostrar que llegaremos al paso 8 con alta probabilidad

Implementación del algoritmo de Shor

- Todos los pasos menos el 4 se hacen de forma clásica (existen algoritmos eficientes para ello)
- El paso 4 se puede hacer con un circuito cuántico que requiere una cantidad polinómica en n (el número de bits de N) de puertas

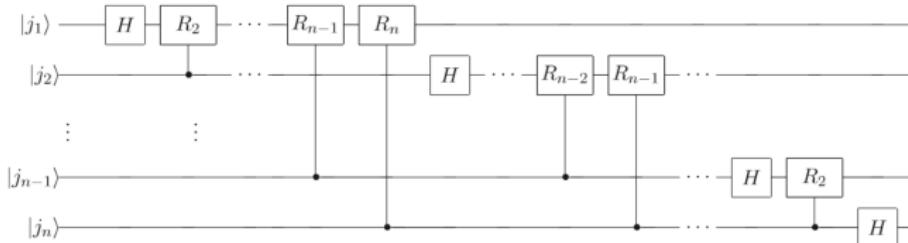


Implementación del algoritmo de Shor (2)

- El método cuántico usa un registro de m qubits (normalmente, $m \geq 2n$) y, al medirlo, obtenemos un número entero M que es una aproximación de $\frac{2^m c}{r}$, con r el periodo buscado y c un número entero no negativo.
- Tras medir M , se aproxima $\frac{M}{2^m}$ por la fracción más cercana que tiene denominador menor o igual que $N - 1$ y se devuelve como posible periodo el denominador de esa fracción.
- El circuito de la transparencia anterior es un caso particular de otro método llamado algoritmo cuántico de estimación de fase (la fase, en este caso, es $\frac{2\pi c}{r}$)
- Los ingredientes principales son:
 - Puertas para realizar la multiplicación por los valores $a, a^2, a^4, \dots, a^{2^{m-1}}$
 - La inversa de la transformada cuántica de Fourier

La (inversa de la) transformada cuántica de Fourier

- La transformada cuántica de Fourier (QFT) y su inversa son métodos de vital importancia en muchos algoritmos cuánticos
- Suponen una ganancia exponencial con respecto a su versión clásica
- En el algoritmo de Shor, se utilizan para estimar el periodo de una función
- En la figura, se muestra el circuito de la QFT a falta de unos swap finales y con $R_k = R\left(\frac{2\pi i}{2^k}\right)$

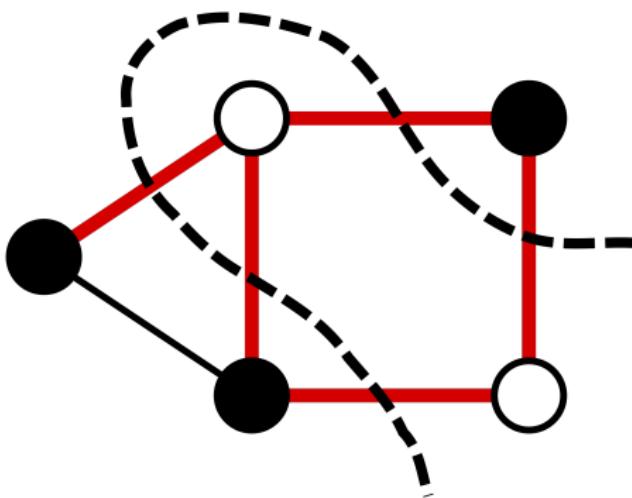


Parte XII

Optimización en ordenadores
cuánticos: cuando el tiempo es oro

El problema del corte máximo

- Consideremos el problema de dividir los vértices de un grafo en dos grupos maximizando los ejes cortados



- Es un problema NP-hard (si podemos resolverlo, podemos resolver cualquier problema que esté en NP)

Planteando el problema del corte máximo con *spins*

- Identificamos cada vértice i del grafo con una variable Z_i
- Asignamos valor 1 a los vértices de un grupo y -1 a los del otro
- Entonces, si E es el conjunto de ejes, el problema se puede plantear como

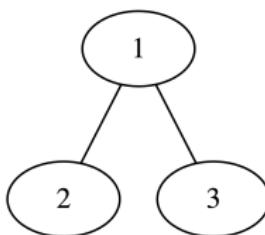
$$\text{Minimizar} \sum_{(i,j) \in E} Z_i Z_j$$

ya que vértices en distintos grupos aportan -1 a la suma y vértices del mismo grupo aportan 1

Ejemplo de corte máximo

- Para el grafo de la figura se trata de minimizar

$$H = Z_1Z_2 + Z_1Z_3$$



- Por inspección (o enumerando todas las posibilidades) se ve que las soluciones óptimas son 011 y 100

¿Y dónde metemos la computación cuántica en todo esto?

- Recordemos que la puerta Z tiene como matriz

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

y que el vector $|0\rangle$ tiene como coordenadas

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

- Entonces

$$(1 \ 0) \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1$$

- Solemos denotar el anterior producto de matrices y vectores como

$$\langle 0 | Z | 0 \rangle = 1$$

¿Y dónde metemos la computación cuántica en todo esto?

- Análogamente

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

- Así que

$$\langle 1 | Z | 1 \rangle = (0 \quad 1) \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = -1$$

- Si tenemos más qubits, evaluamos cada uno por separado y multiplicamos. Por ejemplo:

$$\langle 01 | Z_1 Z_2 | 01 \rangle = (\langle 0 | Z_1 | 0 \rangle) \cdot (\langle 1 | Z_2 | 1 \rangle) = 1 \cdot (-1) = -1$$

y

$$\langle 101 | Z_1 Z_3 | 101 \rangle = (\langle 1 | Z_1 | 1 \rangle) \cdot (\langle 1 | Z_3 | 1 \rangle) = (-1) \cdot (-1) = 1$$

Volviendo al ejemplo de corte máximo

- Teníamos el problema de corte representado por

$$H = Z_1Z_2 + Z_1Z_3$$

- Podemos identificar un posible corte con $|011\rangle$ (tomar los vértices 2 y 3 y dejar fuera el 1) y evaluar su coste mediante

$$\begin{aligned}\langle 011 | H | 011 \rangle &= \langle 011 | (Z_1Z_2 + Z_1Z_3) | 011 \rangle \\ &= \langle 011 | Z_1Z_2 | 011 \rangle + \langle 011 | (Z_1Z_3) | 011 \rangle = -1 + (-1) = -2\end{aligned}$$

- Del mismo modo

$$\begin{aligned}\langle 010 | H | 010 \rangle &= \langle 010 | (Z_1Z_2 + Z_1Z_3) | 010 \rangle \\ &= \langle 010 | Z_1Z_2 | 010 \rangle + \langle 010 | (Z_1Z_3) | 010 \rangle = -1 + 1 = 0\end{aligned}$$

El maravilloso mundo de los hamiltonianos

- Entonces, lo que nos interesa es hallar un estado cuántico $|x\rangle$ de forma que

$$\langle x| H |x\rangle$$

sea mínimo, con $H = \sum_{(i,j) \in E} Z_i Z_j$ la función de coste del problema del corte máximo

- Se trata de un caso particular de un problema muy importante en física: hallar el estado de energía mínima (**ground state**) de un hamiltoniano
- Un hamiltoniano es una matriz H hermitiana ($H = H^\dagger$)
- Físicamente, puede representar fuerzas, potenciales... en la ecuación de Schrödinger
- La energía de un estado $|\psi\rangle$ es

$$\langle \psi | H | \psi \rangle$$

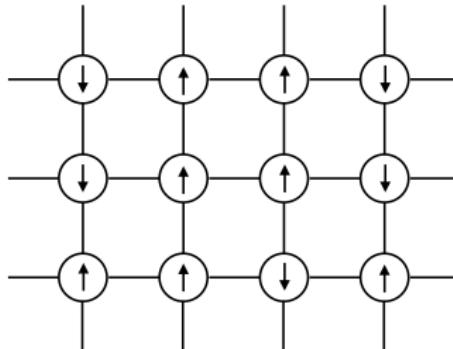
Ejemplo: el modelo de Ising

- Se tienen n partículas con spin, que interactúan entre sí con ciertas fuerzas de acoplamiento
- Su hamiltoniano es

$$H = \sum_{1 \leq i < j \leq n} J_{ij} Z_i Z_j + \sum_{i=1}^n h_i Z_i$$

con J_{ij} y h_i coeficientes reales

- Queremos encontrar una asignación de valores de spins (1 o -1) que minimice la suma
- El problema general es NP-hard



QUBO: Quadratic Unconstrained Binary Optimization

- Una formulación alternativa del modelo de Ising son los problemas QUBO (Quadratic Unconstrained Binary Optimization)
- Se plantean como

$$\text{Minimizar} \sum_{\substack{1 \leq i \leq j \leq n}} w_{ij} x_i x_j$$

donde cada x_i es una variable binaria y los w_{ij} son coeficientes reales

- Se puede reescribir como un modelo de Ising con la transformación

$$x_i = \frac{z_i + 1}{2}$$

y volver a QUBO con

$$z_i = 2x_i - 1$$

Computación cuántica adiabática

- ¿Cómo obtener el *ground state* de H ?
- Una solución natural es aplicar el propio hamiltoniano H para llegar a la solución
- El **teorema adiabático** nos asegura que si comenzamos en el estado de mínima energía de un hamiltoniano y lo vamos variando lentamente, nos mantendremos siempre en el estado de mínima energía
- La idea de la computación cuántica adiabática es:
 - Comenzar en el estado de mínima energía de un hamiltoniano sencillo H_i
 - Evolucionar el sistema hacia el estado de mínima energía del hamiltoniano del problema H_f
 - Para ello se aplica el hamiltoniano dependiente del tiempo

$$H(t) = \left(1 - \frac{t}{T}\right)H_i + \frac{t}{T}H_f$$

durante tiempo T

Computación cuántica adiabática (2)

- Para garantizar la adiabaticidad, T debe crecer como el inverso del cuadrado del *spectral gap* de $H(t)$ (diferencia entre el primer y segundo nivel de energía)
- El spectral gap es **difícil** de calcular
- En la práctica, se usa el *quantum annealing*:
 - Se toma $H_i = - \sum_{i=1}^n X_i$ (con ground state $\sum_{x=0}^{2^n-1} |x\rangle$)
 - Como H_f se toma un hamiltoniano de Ising
 - Se deja evolucionar durante un tiempo T (no necesariamente adiabático)
 - Se mide para obtener una solución
 - Se repite un cierto número de veces y se devuelve la mejor solución obtenida
- Es la base de los ordenadores cuánticos de D-Wave

Los ordenadores cuánticos de D-Wave

- Son ordenadores de propósito específico: resolver el modelo de Ising
- Accesibles gratuitamente (1 minuto/mes) a través de <https://www.dwavesys.com/take-leap>



Quantum Approximate Optimization Algorithm (QAOA)

- El QAOA está inspirado en el modelo adiabático, pero para el paradigma de circuitos cuánticos
- El hamiltoniano adiabático es $H(t) = (1 - \frac{t}{T})H_i + \frac{t}{T}H_f$
- En la resolución de la ecuación de Schrödinger aparecen expresiones de la forma

$$e^{-i\alpha H(t)}$$

- En este caso, aproximamos la solución por

$$|\beta, \gamma\rangle = e^{-i\beta_p H_i} e^{-i\gamma_p H_f} \dots e^{-i\beta_2 H_i} e^{-i\gamma_2 H_f} e^{-i\beta_1 H_i} e^{-i\gamma_1 H_f} |s\rangle$$

donde

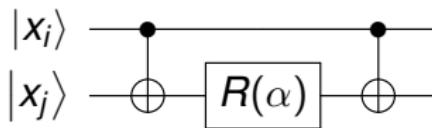
$$|s\rangle = \sum_{i=0}^{2^n-1} |x\rangle$$

Optimización con QAOA

- Se trata de un método híbrido en el que intervienen un ordenador clásico y uno cuántico
- Sus pasos son:
 - 1 Elegir un valor p y unos ángulos iniciales β, γ
 - 2 Preparar el estado $|\beta, \gamma\rangle$
 - 3 Estimar la energía $E(\beta, \gamma)$ de $|\beta, \gamma\rangle$ con respecto al hamiltoniano H_f
 - 4 Variar los parámetros β y γ para minimizar $E(\beta, \gamma)$
- El paso 2 se hace en el ordenador cuántico y los pasos 1, 3 y 4, en uno clásico

Cómo preparar el estado $|\beta, \gamma\rangle$

- El estado $|s\rangle = \sum_{i=0}^{2^n-1} |x\rangle$ se prepara fácilmente con puertas de Hadamard
- Cada $e^{-i\beta_k H_i}$ y $e^{-i\gamma_k H_f}$ se consigue con rotaciones y puertas CNOT y de Hadamard
- Para $e^{-i\alpha Z_i Z_j}$



- Para $e^{-i\alpha Z_i}$



- Para $e^{-i\alpha X_i}$



Cómo estimar la energía

- Nos reduciremos al caso en el que tenemos un hamiltoniano tipo Ising

$$H_f = \sum_{i,j=1}^n J_{ij} Z_i Z_j + \sum_{i=1}^n h_i Z_i$$

- Los pasos son:
 - Medimos el estado preparado $|\beta, \gamma\rangle$
 - Calculamos la energía de la secuencia de bits obtenida
 - Cada uno de los términos $Z_i Z_j$ y Z_i sólo puede ser 1 o -1
 - $Z_i Z_j$ sólo depende de los bits de las posiciones i y j . Será 1 si son iguales y -1 si son distintos.
 - Z_i sólo depende del bit de la posición i . Será 1 si el bit es 0 y -1 si el bit es 1.
 - Repetimos un cierto número de veces y promediamos
- Es interesante guardar el valor mínimo de energía de entre los valores medidos

Propiedades del QAOA

- Los circuitos del QAOA tienen un número de puertas polinomial en p si H_f tiene un número polinomial de sumandos
- Existen resultados teóricos sobre el ratio de aproximación del QAOA en algunos problemas (corte máximo)
- Hay dependencia de p (y otros factores) en la bondad de la aproximación
- El método se puede extender a otros problemas (factorización, Grover...)

VQE: Variational Quantum Eigensolver

- El QAOA es un caso particular de un algoritmo más general: el VQE (Variational Quantum Eigensolver)
- En lugar de $|\beta, \gamma\rangle$ se usa un estado (ansatz) que también depende de parámetros y en el que utilizamos conocimiento del problema
- Estos métodos se han usado, por ejemplo, para obtener energías de enlace de algunas moléculas

