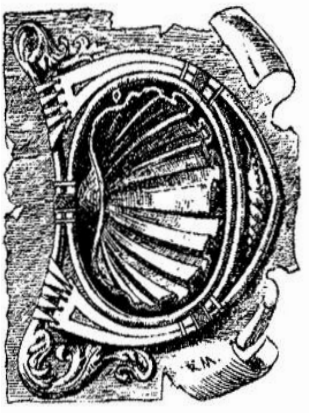
COMPUTACIÓN CUÁNTICA Y APLICACIONES

Antonio GONZÁLEZ GARCÍA

(Ing.)



DURANTE el primer fin de semana de confinamiento a causa de la pandemia del COVID-19, pensando en cómo ocupar el tiempo en casa, se me ocurrió escribir un artículo divulgativo sobre la computación cuántica que fuera sencillo y a la vez útil, a pesar de su complejidad. Espero conseguir al menos acercarme al objetivo.

Introducción

En la computación clásica, el almacenamiento y procesamiento de información está basado en *bits*, conocidos por todos, que tienen un valor binario, discreto y determinista; sin embargo, la computación cuántica trata la información mediante *qubits*, capaces de mantener dos estados simultáneamente con una cierta probabilidad. En consecuencia, se pueden procesar ambos estados a la vez, reduciendo enormemente el tiempo de procesamiento.

La computación cuántica puede acelerar ciertos procesos, utilizando algoritmos propios, hasta el punto de influir sustancialmente sobre campos como la criptografía, basada hoy día en la *seguridad computacional*, esto es, en la certeza de que el descifrado de un texto cifrado necesitaría, en promedio, miles de años en un ordenador convencional; sin embargo, esta seguridad computacional es inservible cuando el descifrado puede realizarse en segundos utilizando la computación cuántica.

Antes de continuar tengo que advertir que se van a mencionar de forma sencilla algunos conceptos nada intuitivos, cuya total comprensión solo está al alcance de los expertos en mecánica cuántica, que obviamente, no es el público a quien está dirigido este artículo.

Qué es un *qubit*?

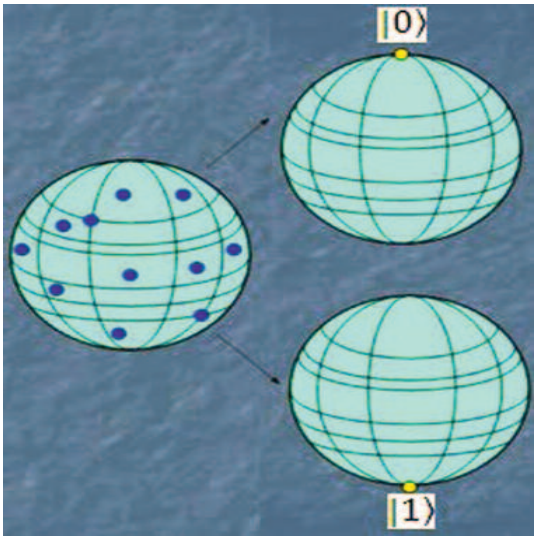


Figura 1. Presentación de Dan Cristian Marinescu, *School of Computer Science University of Central Florida, Orlando, Florida, (Computing Frontiers, Ischia*, April 14, 2004)

El elemento básico de la computación cuántica es el *bit* cuántico o *qubit* (del inglés, *quantum bit*). Un *qubit* representa ambos estados simultáneamente, un «0» y un «1» lógico, correspondientes, por ejemplo, a los dos estados (1) ortogonales de una partícula subatómica. El valor del *qubit* solo se particulariza a «0» a «1» cuando se mide el *qubit* (2). Hay que tener en cuenta que cualquier interacción con el mundo subatómico produce un cambio en este, es decir, toda medición o lectura conlleva indefectiblemente una modificación del estado de las partículas.

Lo enunciado tiene una interpretación gráfica que puede ayudar: la esfera de la izquierda de la figura 1 representa varios estados superpuestos de un *qubit* antes de medir, mientras que después de la medida el valor del *qubit* se particulariza o bien para «0» o bien para «1».

Fundamentos de la computación cuántica

La computación cuántica está basada en dos propiedades de la interacción cuántica entre partículas subatómicas: la superposición y el entrelazado.

La *superposición cuántica* es la propiedad de las partículas subatómicas de tener múltiples estados simultáneos, por ejemplo un «0» y un «1» a la vez. Si asociamos estos estados a un *qubit*, esta propiedad permite operar matemáticamente con todos los valores del *qubit* simultáneamente. En definitiva, un vector de *n qubits* representa a la vez 2^n estados.

---

(1) A modo de ejemplo, los estados pueden ser el *spin* de un electrón, la polarización de un fotón, etcétera.

(2) Los lectores curiosos pueden encontrar una explicación algo más intuitiva en el experimento teórico llamado «el gato de Schrödinger».

El fenómeno del *entrelazado* se produce cuando dos partículas subatómicas permanecen indefectiblemente relacionadas entre sí, siempre que hayan sido generadas en un mismo proceso (por ejemplo, la desintegración de un neutrón en un positrón y un electrón). Estas partículas forman subsistemas que no pueden describirse separadamente. Cuando una de las dos sufre un cambio de estado, repercute en la otra. Y eso ocurre de forma instantánea y con independencia de la distancia que las separe en ese momento. Esta característica se desencadena cuando se realiza una medición sobre una de ellas. Este fenómeno se puede aprovechar en la *teletransportación cuántica* para transmitir información y asimismo puede utilizarse como mecanismo de seguridad en la criptografía cuántica.

Ciertos algoritmos matemáticos se han aplicado con éxito a problemas de computación convencionales utilizando los fundamentos de la computación cuántica. Se pueden citar como ejemplos el cálculo de los factores primos de un número y ciertos algoritmos de manejo de información (la búsqueda en bases de datos no ordenadas).

Criptografía cuántica

Como se ha mencionado anteriormente, emplear ordenadores cuánticos en la criptografía cambiaría completamente los sistemas actuales, basados principalmente en la seguridad computacional proporcionada por la dificultad para factorizar números en los ordenadores convencionales. Por su incidencia en la seguridad de la información, profundizaremos en las aplicaciones de la computación cuántica en la criptografía. A modo de ejemplo, el tiempo que requiere la factorización de claves de 2048 *bits* es, en promedio unos $4\ 10^{16}$ años en un ordenador convencional.

Para lograr mayor potencia de cálculo con ordenadores convencionales, se utilizaron algoritmos distribuidos en red, se logró factorizar una clave de 512 *bits* en ocho meses. Sin embargo, se estima que los algoritmos cuánticos de factorización realizarían este cálculo en apenas unos segundos. Es claro que el país que tenga disponible en el futuro la capacidad de computación adecuada tendrá ventaja en el descifrado de la información.

Además, la criptografía cuántica permite distribuir claves privadas a través de un canal cuántico, con la ventaja de que cualquier intento de medir la clave será detectado, ya que es imposible observar un *qubit* sin dejar rastro (debido a la propiedad de entrelazamiento). La distribución cuántica de claves ya es posible con la tecnología existente; en 2017 se demostró la distribución cuántica de claves entre dos nodos en China y Austria separados 7.600 km, seguida de una videoconferencia cifrada con esas claves, sin duda la semilla de una futura internet cuántica.

Ordenadores cuánticos

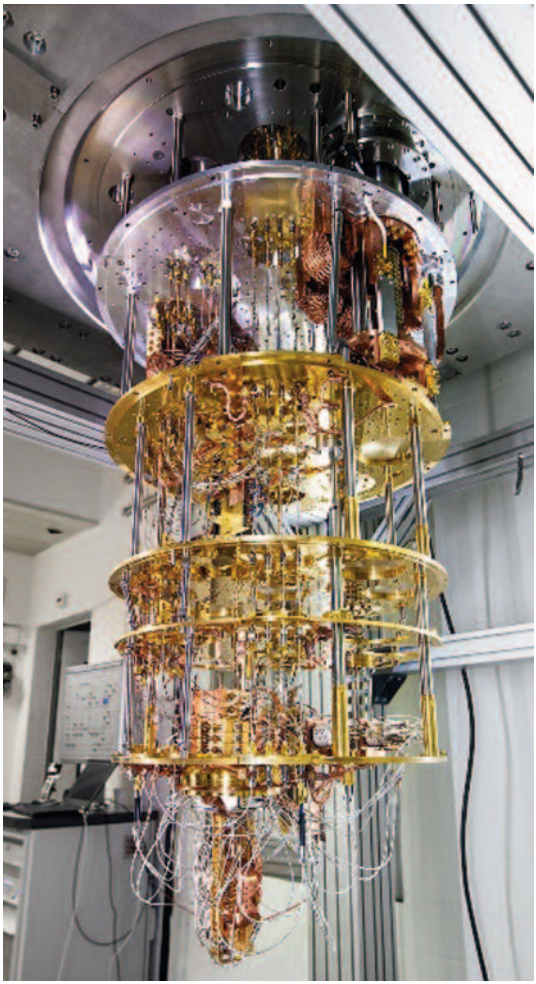


Figura 2. Ordenador cuántico de IBM.
(Foto: *www.wikipedia.org*).

Todo lo mencionado anteriormente puede parecer pura teoría; sin embargo, como veremos a continuación, existen ordenadores cuánticos reales.

Los procesadores clásicos están llegando al límite de la miniaturización y la frecuencia de reloj, es decir, que la Ley de Moore (3) está llegando a su conclusión. Al mismo tiempo, los requisitos de disipación del calor en los microprocesadores actuales son tan enormes que pronto no será posible asumirlos. La computación cuántica puede ser la solución que permita diseñar ordenadores más rápidos. Pero las ventajas de la superposición cuántica para el procesamiento paralelo se ven oscurecidas por los problemas a la hora de leer la información sin influir en el sistema.

Por lo que respecta al *hardware* de un ordenador cuántico, en 1999 Los Alamos National Laboratory y el MIT (Massachusetts Institute of Technology) consiguieron construir un ordenador cuántico en estado sólido.

En el año 2000, IBM creó un ordenador cuántico de cinco *qubits*. En 2005, la Universidad de Innsbruck anunció la creación del primer *qbyte* (una serie de ocho *qubits*).

(3) La Ley de Moore predijo, y se ha venido cumpliendo desde los años 70, que los procesadores duplican su potencia de cálculo cada 18 meses.

Más tarde, en 2012, con un ordenador de IBM de estado sólido se calcularon los factores primos del número 15.

El año anterior, la empresa D-Wave Systems, fundada en 1999, vendió el primer ordenador cuántico comercial, el D-Wave One, a Lockheed Martin por 10 millones de dólares, basado en el procesador Rainier de 128 *qubits* de la misma empresa. El ordenador completo ocupa nueve metros cuadrados debido al volumen de los equipos necesarios para su apantallamiento y la criogenia para una temperatura de funcionamiento cercana al cero absoluto. Actualmente, D-Wave Systems publicita en su *web* su producto 2000Q, un ordenador de 2000 *qubits*.

Figura 3. El D-Wave One. (*Web* de D-Wave Systems).

En octubre de 2019, Google anunció que había logrado la *supremacía cuántica*, es decir, un ordenador cuántico basado en su procesador Sycamore de 54 *qubits* que era capaz de realizar un cálculo en 200 segundos que habría llevado 10.000 años a un superordenador convencional, aunque IBM pone en duda este hito.

Conclusión

Se ha avanzado enormemente desde el principio de siglo en el diseño y fabricación de ordenadores cuánticos. El centro de supercomputación de Barcelona anunció en 2017 su capacidad de proceso cuántico a corto plazo, aunque aún no se ha materializado. En cualquier caso, estamos muy lejos de disponer de ordenadores cuánticos en los hogares. En definitiva, su ventaja es que resuelven con complejidad lineal problemas que muestran complejidad exponencial en los ordenadores clásicos. Pero emplear ordenadores cuánticos no siempre es lo más adecuado; por ejemplo, no se aprecian ventajas en la evaluación de funciones matemáticas. En cuanto a su aplicación a la simulación, no ha sido suficientemente estudiada todavía. La aplicación de algoritmos cuánticos a la inteligencia artificial es una disciplina reciente pero prometedora.

La tendencia de la tecnología parece indicar que a corto plazo los ordenadores convencionales seguirán en servicio y los cuánticos se aplicarán a problemas específicos en los que son especialmente eficientes, como la criptografía, proporcionando una ventaja operativa decisiva y adicionalmente la distribución de claves de forma segura. La OTAN estima que no habrá ordenadores cuánticos operativos para propósitos militares antes de 15-20 años.

A medio plazo ya se habla de una internet cuántica, incluyendo una cifra cuántica que bien pudiera ser una solución cibersegura frente a enemigos que no posean ordenadores cuánticos.

China está invirtiendo significativos recursos (4) desde 2014 y lleva cierta delantera en este campo. Estados Unidos, por su parte, aprobó en 2018 su National Quantum Initiative Act, que asignaba 1.200 millones de dólares distribuidos en cinco años a I+D en tecnología cuántica, incluyendo no solo computación, sino también radares cuánticos y detectores submarinos cuánticos.

(4) Aunque no se sabe la cifra total, en 2018 aprobó el gasto de 10.000 millones de dólares para crear la planta más grande del mundo en investigación cuántica en Hefei.