



**ALBA CERVERA LIERTA.**  
Investigadora sénior en el Barcelona Supercomputing Center – Centro Nacional de Supercomputación.

FOTOS. Mario Ejarque. ©BSC-CNS 2024 y ©BSC-CNS 2021.

# Computación Cuántica

## Una nueva (r)evolución en computación

La computación de altas prestaciones sigue avanzando y buscando nuevas formas de adaptarse a los problemas computacionales actuales. La computación cuántica **surge como una evolución natural de los ordenadores pensada para resolver de forma más eficiente algunas aplicaciones científicas y tecnológicas**. Estos dispositivos, aún en su infancia, mejoran año tras año y ya se pueden encontrar y utilizar en centros de supercomputación.

El transistor, las placas fotovoltaicas, el GPS, el láser o las técnicas de imagen médica son solo algunos ejemplos de inventos que han cambiado el mundo y la tecnología. Detrás de ellos encontramos la física de los semiconductores, el efecto fotoeléctrico, el reloj atómico, la luz coherente y la resonancia magnética nuclear, respectivamente.

Todos estos efectos fueron descubiertos y descritos gracias a la física cuántica durante el siglo XX en lo que se conoce como la ‘primera revolución cuántica’. ¿Podemos ir más allá? ¿Podemos describir y controlar sistemas cuánticos individuales y descubrir nuevas aplicaciones tecnológicas? La respuesta es sí: no sólo podemos, sino que ya lo estamos haciendo.

Estamos ahora inmersos en la ‘segunda revolución cuántica’ y las tecnologías cuánticas de segunda generación ya empiezan a utilizarse. Entre ellas, destaca la computación cuántica: ser capaces de codificar y procesar información en estados cuánticos y con ello extender las capacidades computacionales actuales.

### Del bit al cúbit

La información (clásica) se codifica usando el sistema binario, los famosos ‘0’ y ‘1’, los bits. En computación cuántica, los bits cuánticos (llamados *cúbits*) tienen propiedades heredadas de su naturaleza cuántica. Las más relevantes son la ‘superposición’ y la ‘interferencia’.” No vamos a entrar a detallar en este artículo en qué consisten estas

**Estamos ahora inmersos en la ‘segunda revolución cuántica’ y las tecnologías cuánticas de segunda generación ya empiezan a utilizarse**



Edificio del Barcelona Supercomputing Center – Centro Nacional de Supercomputación, BSC.





Instalación del chip cuántico en el BSC.

propiedades, pero sí hay que destacar que gracias a ellas algunos problemas matemáticos muy complejos pueden resolverse más eficientemente que con computación tradicional.

La computación cuántica se propuso originalmente para simular sistemas cuánticos de forma eficiente. La capacidad de que las partículas cuánticas tengan propiedades como la superposición y el entrelazamiento cuántico hace que tratar de simular su dinámica con computación tradicional sea exponencialmente costoso en la mayoría de los casos.

De forma natural, surgió la idea en los años 80 del pasado siglo de construir un ordenador capaz de procesar la información bajo las mismas propiedades que los sistemas cuánticos que quiere simu-

lar; es decir, que tenga también estas propiedades cuánticas. Poder mejorar las simulaciones de los sistemas cuánticos tiene aplicaciones en química y ciencia de materiales, al ser la física cuántica la que gobierna sus propiedades.

Por otro lado, existen algunos problemas matemáticos complejos y (hasta la fecha) irresolubles eficientemente con computación tradicional, que la computación cuántica ha demostrado poder resolver eficientemente a nivel teórico. Este es el caso de la factorización de números enteros, resuelta con el algoritmo cuántico de Shor.

El hecho de que factorizar no sea eficiente está en el núcleo de la seguridad de los protocolos de criptografía de clave pública actuales. De modo que, si

se construyera un ordenador cuántico lo suficientemente potente, descifraría todos los mensajes encriptados presentes y pasados. Aunque no contamos con estos ordenadores actualmente (que sepamos), ya se está trabajando en actualizar dichos protocolos con otros resistentes a ordenadores cuánticos (criptografía post-cuántica), a la vez que se trabaja en la solución a largo plazo (criptografía cuántica).

Por último, se están explorando muchas más aplicaciones potenciales, como lo son el diseño de modelos de Inteligencia Artificial cuántica o la resolución de problemas de optimización. En algunos casos de forma heurística (sin tener demostración matemática de que existe una ventaja cuántica), pero comparando las soluciones con algoritmos tradicionales.

#### Cómo es un computador cuántico

Un ordenador o computador cuántico está compuesto por tres grandes partes: la unidad de procesamiento cuántica (la QPU, el hardware puramente cuántico, que contiene los *cúbits*), el sistema de

control de la QPU (electrónica rápida, fotónica y generadores de ondas, entre otros elementos) y el software que permite mandar instrucciones a la QPU mediante el sistema de control.

Un ordenador cuántico se programa desde un ordenador tradicional mediante el uso de librerías de software que traducen las instrucciones abstractas (circuitos cuánticos, puertas lógicas) al sistema físico que las implementa, a la vez que retorna una serie de señales que codifican el estado medido de los *cúbits* para su posterior post-procesamiento.

A diferencia de la computación tradicional, basada casi exclusivamente en semiconductores, la computación cuántica se basa en varias tecnologías potenciales, todas con sus pros y contras experimentales. Así, se pueden construir ordenadores cuánticos usando circuitos superconductores, fotónica, átomos neutros, iones atrapados, puntos cuánticos, etc. Hoy en día, no está clara qué tecnología va a ser la definitiva: varias empresas y grupos de investigación trabajan en paralelo con todas ellas.

Lo que sí tienen en común todos los tipos de ordenadores cuánticos es que no son todavía 'tolerantes a fallos', porque generan una serie de errores al ejecutar los algoritmos cuánticos que no se pueden corregir con la tecnología actual y, por tanto, el resultado de la computación no es el esperado teóricamente. Además, el número de *cúbits* es todavía bajo, siendo la escalabilidad de estos dispositivos un reto pendiente.

Estos hechos limitan las aplicaciones de la computación cuántica actual, pero también plantean un campo de investigación muy amplio y vibrante. En paralelo, la tecnología mejora año tras año, pasando de ordenadores cuánticos de apenas cinco *cúbits* a prototipos de más de 1.000 en menos de 10 años.

#### Democratizar el acceso

Además de los retos tecnológicos (mejora del hardware cuántico), es necesario que la computación cuántica se democratice, como toda tecnología disrupti-

## A la vez que crece la demanda de ordenadores cuánticos es fundamental que el acceso para la investigación se facilite

va. El acceso a los primeros ordenadores cuánticos a través de la nube ha estado dominado casi por completo por las grandes empresas tecnológicas que los desarrollan (como IBM o Google) o por *startups* que han surgido de los primeros grupos de investigación que trabajaron en este campo (Rigetti o IonQ).

Actualmente se puede solicitar acceso bajo pago a ordenadores cuánticos en plataformas como Amazon Braket o Microsoft Azure. A la vez que crece la demanda de ordenadores cuánticos por parte de la comunidad investigadora y empresarial, es fundamental que el acceso para la investigación se facilite. Al fin y al cabo, hablamos de una tecnología todavía en pañales, que necesita crecer y ser experimentada por todo tipo de investigadores e ingenieros. Por ello, los centros de supercomputación se postulan como un sitio natural donde albergar estos ordenadores cuánticos y facilitar su acceso público, del mismo modo que lo hacen para la supercomputación tradicional.

En esa dirección, Europa apuesta por ampliar la iniciativa EuroHPC-Joint Undertaking para adquirir e instalar ordenadores cuánticos en centros de supercomputación europeos. El Barcelona Supercomputing Center es uno de

estos primeros centros seleccionados, que además ya cuenta con un ordenador cuántico instalado gracias al proyecto Quantum Spain, impulsado por el Ministerio de Digitalización. Ambos ordenadores cuánticos están fabricados con tecnología 100% europea, alineándonos con la estrategia de soberanía tecnológica de la Unión Europea.

De hecho, las empresas que hay detrás de estos dispositivos son españolas (Qilimanjaro Quantum Tech, GMV y DoIT Now). Recientemente, ya se ha habilitado el acceso público y competitivo al ordenador cuántico de Quantum Spain a través de la Red Española de Supercomputación.

En resumen, la computación cuántica es una tecnología disruptiva que promete revolucionar muchos campos como la química, la criptografía o la ciencia de materiales. Se complementa con la computación tradicional y, de hecho, ordenadores cuánticos están siendo instalados e integrados en los centros de supercomputación como en el Barcelona Supercomputing Center. Es una tecnología que todavía vive su infancia y los retos que tiene por delante abren el campo a multitud de disciplinas, desde la física más básica a la ingeniería más aplicada. ▴



MareNostrum5 Ona, instalado en la capilla de la Torre Girona en el Barcelona Supercomputing Center – Centro Nacional de Supercomputación, BSC.