Computación cuántica: 25 años después

Alba Cervera Lierta

Analizamos los avances en computación cuántica 25 años después del primer artículo publicado en la *Revista Española de Física*. En estos años se han desarrollado pocos algoritmos cuánticos fundamentalmente diferentes a los ya conocidos en los noventa, aunque su rango de aplicación se ha multiplicado. Por otro lado, las tecnologías cuánticas han avanzado sustancialmente haciendo posible el uso (cada vez más extendido) de ordenadores cuánticos. Curiosamente, las tecnologías cuánticas para computación que se anticipaban hace 25 años no son las más utilizadas hoy en día. ¿Qué maravillas nos deparará la futura computación cuántica que no somos capaces de aventurar hoy?

> Los primeros experimentos sobre computación cuántica están teniendo lugar. Sin embargo, todavía es muy pronto para saber si algún día tendremos ordenadores cuánticos.
>
> Juan Ignacio Cirac Sasturain,
> Quanta y Computación,
> *Revista Española de Física* **14**(1), 48 (2000).

Han pasado 25 años desde el primer artículo sobre computación cuántica publicado en la *Revista Española de Física* [1]. Su autor fue un joven Juan Ignacio Cirac, que pocos años después empezó a cosechar reconocimientos de la talla del premio Príncipe de Asturias, premio Wolf, medalla Max Planck entre muchos otros. En su artículo, Cirac presentaba las ideas básicas de la computación cuántica y cómo podrían implementarse experimentalmente. Veinticinco años después de ese artículo, ¿qué ha cambiado? ¿Superamos los retos tecnológicos para conseguir el tan ansiado ordenador cuántico?

Lo cierto es que en la comunidad impera una superposición de sensaciones. Por un lado, hace años que se pronostica que "quizás de aquí a cinco años" tendremos un ordenador cuántico capaz de hacer tareas mejor que uno clásico (a veces se cambia el cinco por el diez, dependiendo del pesimismo de la persona). Por otro lado, año tras año somos testigos de avances relevantes que nos acercan más y más al ordenador cuántico tolerante a fallos, lo que provoca (sobre todo entre los investigadores e investigadoras más jóvenes) ilusión y motivación por formar parte de un campo en plena expansión. En cualquier caso, es innegable que el campo ha avanzado muchísimo desde el 2000. Los ordenadores cuánticos son una realidad, y aunque todavía no son tolerantes a fallos, empezamos a entrar en el régimen donde la corrección cuántica de errores no solo es posible, sino que ya se ha demostrado.

¿Para qué queremos un ordenador cuántico? Los retos algorítmicos

La primera aplicación obvia de un computador cuántico es la simulación cuántica. Simular sistemas cuánticos requiere de una memoria que crece exponencialmente con el número de partículas, haciendo inviable una simulación exacta de grandes sistemas. Aunque existen técnicas de simulación clásica muy eficientes como las redes de tensores (RT), estas tienen sus limitaciones cuando tratamos sistemas cuánticos con mucha correlación.

Hay varias formas de simular sistemas cuánticos con un dispositivo cuántico programable. La primera es la de usar un simulador cuántico, es decir, un sistema físico que pueda emular al sistema que queremos estudiar. Típicamente, se emplean sistemas descritos con hamiltonianos del modelo de Ising 2D o de Hubbard. Su programabilidad radica en poder manipular las interacciones de estos hamiltonianos para adecuarlas a los parámetros del sistema teórico que queremos estudiar. Una vez preparado ese sistema, podemos experimentar directamente sobre él: observar su estado fundamental, medir sus propiedades magnéticas o estudiar sus propiedades fuera del equilibrio [2]. El reto algorítmico en este caso es encontrar el modo de representar los sistemas físicos de interés usando los hamiltonianos de los simuladores cuánticos. Experimentalmente, la tecnología líder en estos momentos son los átomos neutros. Cientos, incluso miles, de estos átomos (típicamente de rubidio o estroncio) se atrapan y manipulan con pinzas ópticas, siendo de las tecnologías cuánticas que más ha escalado (ver imágenes de la parte inferior de la figura 1). Hay que tener en cuenta que no son considerados ordenadores cuánticos universales, dado que solo pueden simular ciertos modelos físicos y no cualquier operación unitaria. Sin embargo, se están desarrollando nuevas técnicas de manipulación de átomos neutros para poder ser usados para computación cuántica digital universal.

La otra estrategia de simulación cuántica consiste en "trocear" la evolución temporal de un cierto hamiltoniano de modo que cada pieza pueda ser implementada con unas pocas puertas lógicas cuánticas que actúan en pequeños grupos de cúbits. Esta técnica de computación cuántica digital emplea el formalismo de la descomposición de Lie o Trotter. Dado un operador $C = A + B$, su evolución temporal se puede expresar con la expansión $e^{-itC} = \lim_{n\to\infty} \left(e^{-\frac{it}{n}A} e^{-\frac{it}{n}B}\right)^n$. Si A y B son términos que actúan entre parejas de espines, se pueden implementar fácilmente con puertas lógicas cuánticas. Por ejemplo, si $A = \sigma_x \otimes \sigma_x$, $e^{-\frac{it}{n}A}$ es una puerta lógica a dos cúbits. Al ser una serie infinita, la evolución que se simula tiene que

truncarse en un cierto n, de modo que, para conseguir mucha precisión, se requerirá de un circuito cuántico de muchas puertas, lo cual puede ser un factor limitante a corto y medio plazo. Y es que los mejores ordenadores cuánticos digitales actuales contienen alrededor de 100 cúbits con tiempos de coherencia limitados. Con esta técnica nos encontramos en un régimen donde las RT pueden todavía simular estos sistemas. Para tratar de reducir los requerimientos experimentales de la simulación cuántica digital, han surgido una familia de algoritmos cuánticos llamados "variacionales" o "híbridos" que proponen una suerte de ingeniería inversa: se propone un circuito cuántico modelo cuyos parámetros pueden ser ajustables, y, mediante la aplicación del teorema variacional, se busca qué parámetros minimizan el valor esperado del hamiltoniano en cuestión. Estos algoritmos cuánticos tienen la ventaja de ser muy versátiles en cuanto a aplicaciones, además de adaptarse al estado del arte del *hardware* cuántico experimental. Sin embargo, son algoritmos heurísticos que sufren de problemas fundamentales en el proceso de minimización, provocando que sea muy difícil converger hacia una solución cercana a la teórica.

Más allá de las aplicaciones en simulación cuántica, la computación cuántica abre las puertas a resolver problemas matemáticos complejos que la computación tradicional no puede resolver eficientemente. El ejemplo por excelencia es el de la factorización de números enteros, que forma parte de una familia más amplia de problemas llamados "problemas del grupo oculto" para grupos abelianos finitos. Un ordenador cuántico puede teóricamente resolver estos problemas de forma eficiente mediante el uso de técnicas como la transformada de Fourier cuántica. La principal limitación es experimental: para que estos algoritmos cuánticos puedan implementarse correctamente, se requiere de puertas lógicas ideales y largos tiempos de

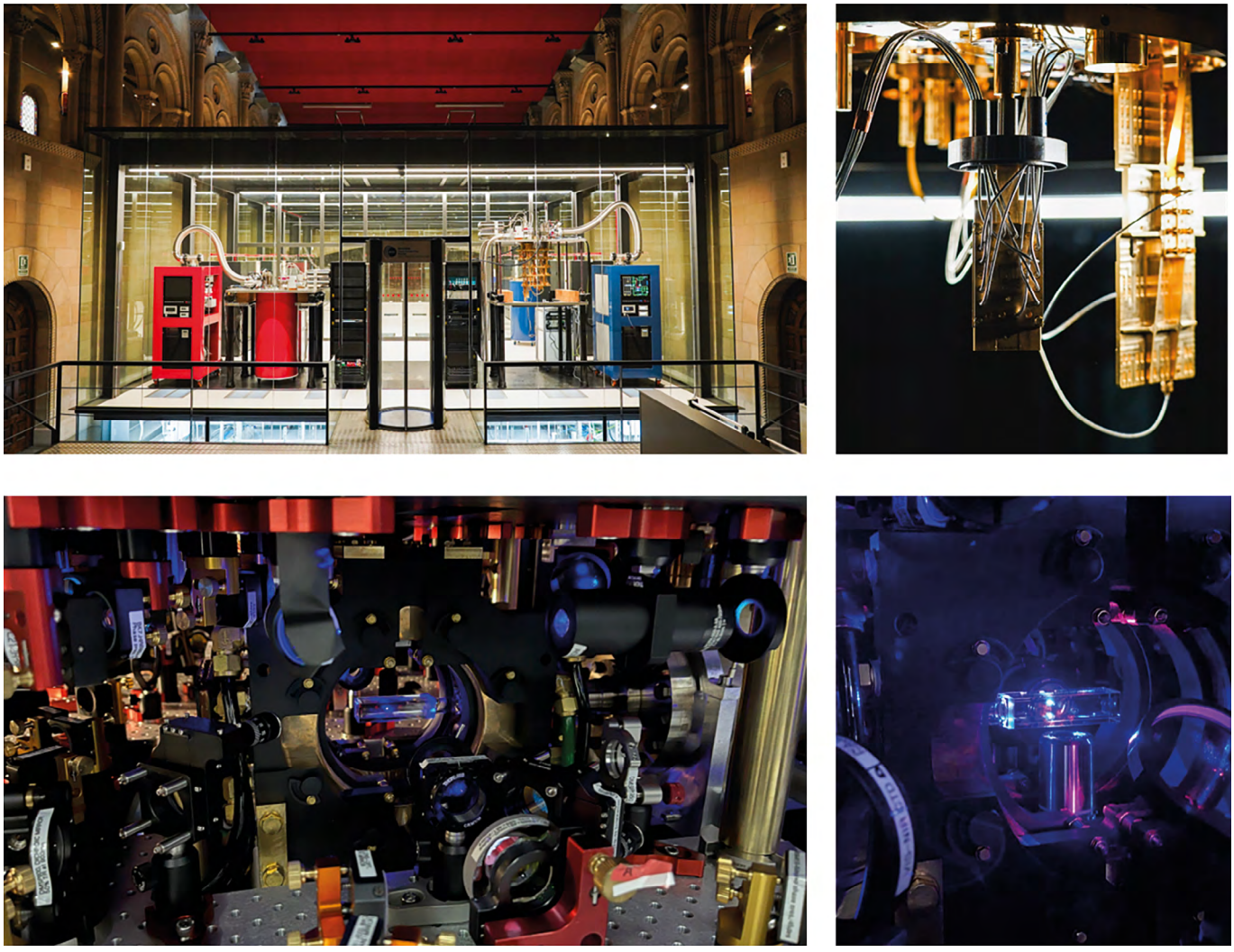

Figura 1. dos ejemplos de ordenadores cuánticos actuales desarrollados e instalados en España. *Superior*: Ordenador cuántico digital instalado en el Barcelona Supercomputing Center – Centro Nacional de Supercomputación (BSC-CNS). Forma parte de la partición cuántica del superordenador MareNostrum5, llamada "MareNostrum Ona". Su tecnología es de cúbits superconductores. El chip se encuentra en la parte inferior del criostato del refrigerador de dilución (ver detalle a la derecha), que enfría sus componentes hasta temperaturas cercanas al cero absoluto. *Inferior*: Ordenador cuántico analógico "Quione" desarrollado en el Institut de Ciències Fotòniques (ICFO). Su tecnología es de átomos neutros. A la derecha, detalle de la nube de átomos de estroncio generada para poder realizar experimentos de simulación cuántica (Créditos de las imágenes: Mario Ejarque [BSC-CNS], Sandra Buob [ICFO] y Alina Hirschmann [ICFO]).

coherencia, es decir, se requiere de corrección cuántica de errores (CCE) [3].

Además de los algoritmos cuánticos mencionados, existen también aquellos basados en oráculos. Como su nombre indica, dada una superposición de estados cuánticos, es posible "marcar" aquellos que representan la solución a un cierto problema mediante la aplicación sucesiva de una operación unitaria sobre la superposición (el oráculo) [4]. El reto en este caso es doble: ¿cómo se crea este oráculo? Alguien tiene que "programarlo" sin saber la respuesta al problema. Además, se requiere de nuevo de un ordenador cuántico tolerante a fallos. Volvemos de nuevo a la necesidad de la CCE.

Y con esto concluimos la revisión de las grandes familias de algoritmos cuánticos. Es evidente que no hay mucha variedad. Y este es en el fondo el gran reto de la algoritmia cuántica: la búsqueda de nuevos algoritmos. Sabemos como hacer CCE, el *hardware* cuántico tiene claros sus retos y objetivos, pero necesitamos seguir innovando en técnicas cuánticas que permitan resolver problemas más allá de las capacidades de la computación tradicional.

Receta para construir un ordenador cuántico

La lista de sistemas físicos que se han propuesto para implementar la computación cuántica es extensa. Muchas de las tecnologías cuánticas se han terminado descartando para computación, aunque se puedan utilizar para otras aplicaciones, como las comunicaciones o la sensórica. Hace 25 años, David P. DiVicenzo estableció una lista de criterios básicos que una tecnología cuántica debía cumplir para poder hacer computación universal [5]:

1. **Un sistema físico escalable capaz de caracterizar cúbits**

   Un cúbit es un sistema cuántico con dos niveles energéticos separados por un cierto "gap". Para que un cúbit pueda estar bien definido, estos niveles deben estar protegidos de algún modo del resto de niveles cuánticos del sistema y bien aislados de su entorno. Al mismo tiempo, tenemos que ser capaces de controlar individualmente varios cúbits y controlar la interacción entre ellos para realizar operaciones programables.

   Hay varias tecnologías capaces de fabricar cúbits bien caracterizados. De las primeras fueron los iones atrapados (propuestos por Cirac y Zoller en 1995). Se atrapan iones con trampas magnéticas para manipularlos individualmente con láseres. Se utilizan dos de los niveles energéticos de los iones para definir los estados $|0\rangle$ y $|1\rangle$. Mediante pulsos de láser y emisión estimulada se implementan las puertas lógicas cuánticas [1]. Actualmente, los ordenadores cuánticos iónicos están compuestos de alrededor de 20 cúbits. Para escalar estos dispositivos se requiere de campos magnéticos cada vez más sofisticados, pues es fácil que, a medida que la interacción de Coulomb entre iones crece por la cantidad de estos, se puedan "perder" algunos antes de terminar de ejecutar el circuito.

   Otra tecnología capaz de construir cúbits son los circuitos superconductores. Estos circuitos son similares a los circuitos LC resonantes, pero sustituyendo la inductancia por una unión de Josephson. En consecuencia, cuando el circuito está en régimen de superconductividad, los niveles energéticos correspondientes corresponden a los de un oscilador cuántico anharmónico. Los cúbits superconductores se controlan enviando ondas en la frecuencia de resonancia de cada uno de los circuitos superconductores del chip. Estos ordenadores cuánticos están compuestos de alrededor de 100 cúbits (aunque la fabricación ya va por los mil), y es de las tecnologías más extendidas. Escalarla es complejo por dos principales motivos. El primero es que se requiere de un sistema de enfriamiento para que los circuitos estén en superconductividad, es decir, se requiere de refrigeradores de dilución capaces de enfriar hasta mK. La otra dificultad se haya en la fabricación de los circuitos: es casi imposible no introducir pequeños defectos que provoquen que los cúbits no estén bien acoplados o que sus frecuencias de resonancia sean demasiado cercanas entre sí, lo que provoca errores de "cross-talk".

   Otra tecnología cuántica que ha emergido con fuerza es la óptica lineal. Usando la polarización de fotones como cúbits, y mediante el uso de espejos, divisores de haz y módulos de cambio de fase, se pueden implementar las operaciones lógicas. La fotónica tiene la ventaja de poder usarse también para comunicaciones cuánticas, además de ser muy limpia en términos de coherencia. Esta ventaja se torna en desventaja por la dificultad de interaccionar los fotones entre sí, lo que aumenta la complejidad de los sistemas cuánticos fotónicos y complica su escalabilidad.

   Existen otras tecnologías prometedoras, como los ya mencionados átomos neutros que mediante su excitación a niveles de Rydberg pueden usarse para computación cuántica digital, además de como simuladores cuánticos. También hace años que se está explorando el uso de puntos cuánticos o moléculas como cúbits, aunque su escalabilidad es, actualmente, limitada.

2. **La posibilidad de inicializar los cúbits a un estado de referencia**

   Cualquier algoritmo cuántico requiere el repetir las operaciones suficientes veces para poder obtener la distribución de probabilidad del estado de los cúbits. Para ello, es fundamental

que un ordenador cuántico pueda prepararse en un estado inicial estable y que esta preparación se pueda repetir las veces que haga falta. Este estado inicial suele ser el estado de energía fundamental de los cúbits (el $|000...0\rangle$) y se puede llegar a él o bien esperando a que los cúbits se "relajen" o bien acelerando el proceso con ciertas operaciones cuánticas.

En general, si el criterio 1) está resuelto, este no debería suponer un factor limitante para esa tecnología. Sin embargo, hay que tener en cuenta el tiempo requerido para esa inicialización: si es demasiado largo, el algoritmo cuántico en cuestión puede requerir de tiempos de ejecución muy largos, perdiendo así su potencial ventaja cuántica.

3. **Tiempos de coherencia suficientemente largos para implementar las operaciones cuánticas**
Para que los circuitos cuánticos de nuestro algoritmo puedan ser implementados, también se requiere que los cúbits tengan tiempos de coherencia suficientemente largos. Estos tiempos, junto con los tiempos de ejecución de las operaciones, nos dictan cuánto tiempo tenemos para implementar el circuito o cómo de largo (profundo) puede ser. Tecnologías como los iones atrapados o los átomos neutros tienen tiempos de coherencia muy largos, de segundos incluso. Sin embargo, el tiempo de ejecución de sus puertas lógicas es también largo. Por otro lado, los circuitos superconductores tienen tiempos de coherencia muy cortos, de microsegundos, pero también cuentan con puertas lógicas muy rápidas, de nanosegundos.

4. **Un *set* universal de puertas lógicas cuánticas**
A diferencia de la computación clásica, donde dado un set de puertas universal, se puede construir cualquier operación aritmética booleana con un número finito de estas puertas, en computación cuántica eso es imposible, dado que hay un número incontable de posibles operaciones unitarias. Afortunadamente esta aparente limitación tiene solución con el teorema de Solovay-Kitaev: dado un set universal de puertas lógicas cuánticas y una cierta operación unitaria, se puede aproximar tal operación usando un número polinómico de puertas. Es decir, podemos aproximar cualquier operación unitaria requiriendo un número de puertas que no crece exponencialmente. ¡Menos mal!

Hay muchos sets de puertas cuánticas universales. Como es lógico, cada tecnología escoge el que se asemeja mejor a las operaciones físicas nativas de sus cúbits. En general, suelen estar compuestos por puertas a un cúbit que puedan generar superposición (como la puerta Hadamard, $|0\rangle \rightarrow (|0\rangle + |1\rangle)/\sqrt{2}$, $|1\rangle \rightarrow (|0\rangle - |1\rangle)/\sqrt{2}$, generar entrelazamiento (como la puerta a dos cúbits CNOT, que invierte el estado del cúbit objetivo si el cúbit control se encuentra en el estado $|1\rangle$), y al menos una puerta que no forme parte del grupo de Clifford (como la puerta a un cúbit T, que introduce una fase $\pi/4$ sobre los cúbits en el estado $|1\rangle$). Este último punto es muy relevante, dado que existe un algoritmo clásico eficiente para poder representar circuitos compuestos únicamente de puertas del grupo de Clifford (teorema de Gottersman-Knill).

5. **Poder medir el estado de los cúbits**
Por último, para poder extraer información de cualquier sistema cuántico, requerimos de un proceso de medida que colapse la función de onda de los cúbits. Este proceso es en muchos casos indirecto utilizando medidas no-destructivas, y, por tanto, se puede utilizar también para la preparación de estados cuánticos (por ejemplo, la inicialización). También puede convertirse en un factor limitante, si este proceso de medida requiere de un tiempo considerable, dado que habrá que repetirlo en numerosas ocasiones.

Más allá de los criterios de DiVicenzo

Estos criterios se convirtieron en una *check list* básica que sirvió de inspiración para explorar diferentes tecnologías cuánticas para computación. Sin embargo, es evidente que 25 años después se han quedado cortos para poder ser usados como guía para el diseño de los ordenadores cuánticos actuales. En los siguientes párrafos, analizamos algunos criterios más que son fundamentales para seguir avanzando en la computación cuántica actual:

6. **Capacidad de implementar operaciones cuánticas en paralelo**
De poco sirve un ordenador cuántico capaz de implementar puertas con errores muy bajos si estas no se pueden aplicar en paralelo entre subgrupos de cúbits. La ventaja cuántica de los algoritmos desaparecería en muchos casos, además de la imposibilidad de implementar CCE. La capacidad de operar en paralelo puede conllevar nuevas fuentes de error y decoherencia en los cúbits. En cualquier caso, cualquier algoritmo cuántico debe asumir que las puertas aplicadas a cúbits distintos serán aplicadas en paralelo, y así se mide la complejidad del circuito.

7. **Medidas e inicialización de cúbits durante la ejecución del circuito**
Para poder aplicar CCE necesitamos medir los cúbits auxiliares (los que nos proporcionan información acerca del error) en mitad del circuito para así rápidamente corregir ese error antes de que se propague. A menos que descubramos una forma de tener cúbits ilimitados,

lo esperado es reutilizar estos cúbits auxiliares para el siguiente ciclo de corrección de errores, es decir, necesitamos reciclarlos e inicializarlos de nuevo una vez medidos. Las medidas e inicialización intermedias no son experimentalmente obvias, dado que hay que ingeniárselas para realizar una operación controlada sobre únicamente un grupo de cúbits del ordenador cuántico sin afectar al resto, que debe seguir en un estado superposición coherente.

8. **Rápida interconexión cuántico-clásica**
En un artículo reciente [6] ya hablamos de la necesidad de integrar los ordenadores cuánticos con los superordenadores. Además de por las aplicaciones híbridas que se pueden desarrollar, tener una rápida interfaz entre las señales que entran y salen del ordenador cuántico y el computador utilizado para procesarlas es fundamental para cualquier algoritmo cuántico. Más aun si se pretende implementar CCE, donde hay que medir el estado de los cúbits auxiliares, identificar el error y corregirlo, todo ello en paralelo sobre todos los cúbits lógicos y múltiples veces en el circuito. Si esa conexión y procesamiento clásico no es suficientemente rápido, los errores que se pretenden corregir se acumularan antes de poder ser mitigados.

9. **Calibraciones rápidas y eficientes**
La estabilidad de los sistemas cuánticos tiene que mantenerse en todo momento para que los algoritmos implementados den los resultados esperados. Para ello, las frecuencias de resonancia de los cúbits, los pulsos enviados para realizar las operaciones o las medidas tienen que estar calibradas a la respuesta física de los cúbits. Pequeñas variaciones en la temperatura, campos electromagnéticos externos o vibraciones pueden afectar a los parámetros de funcionamiento del sistema. Por ello, los protocolos de calibración tienen que realizarse con cierta periodicidad. Depende de la tecnología cuántica empleada, esas calibraciones pueden requerirse muy a menudo. Además, conforme tenemos ordenadores cuánticos de más y más cúbits, técnicas de caracterización de cada uno de ellos como la tomografía cuántica se vuelven exponencialmente costosos y toca idear protocolos más estadísticos como el "randomized benchmarking". En cualquier caso, estas calibraciones deben ser lo más rápidas posible, ya que para cada una de ellas hay que parar el ordenador cuántico.

Una mirada al futuro

En el artículo de Cirac [1] se mencionaban tres tecnologías cuánticas con potencial para la computación: las óptico-cuánticas (átomos o iones atrapados), las basadas en sólidos (circuitos superconductores o puntos cuánticos) y la resonancia magnética nuclear (RMN). De entre todas ellas, la más prometedora eran los iones atrapados. En estos momentos, podemos asegurar que estos siguen siendo de las tecnologías más empleadas, pero en algunos casos superadas por los átomos neutros y los circuitos superconductores. También han surgido otras como la fotónica, y se ha descartado casi por completo la RMN.

Los ordenadores cuánticos son una realidad. Se han hecho varios experimentos que demuestran la ventaja cuántica con simulaciones que no pueden ser replicadas ni por el mayor superordenador del planeta. También hemos entrado en la era de la CCE y empezamos a ver demostraciones de computación cuántica tolerante a fallos [7]. Computadores y simuladores cuánticos están siendo instalados en centros de supercomputación junto a máquinas de computación de altas prestaciones (ver figura 1, parte superior). Es más que probable que la tecnología cuántica que nos traiga la era tolerante a fallos todavía no haya sido descubierta en su totalidad. También que desconozcamos los algoritmos cuánticos que más se emplearán en el futuro. Espero que estas últimas líneas sirvan de inspiración para que un investigador o investigadora joven del 2050 abra su artículo sobre las maravillas, inimaginables en 2025, que nos ha deparado la computación cuántica.

Referencias

[1] J. I. Cirac Sasturain, Quanta y Computación, *Revista Española de Física* **14**(1), 48 (2000).

[2] J. Argüello Luengo y A. González Tudela, Simuladores cuánticos analógicos: Una herramienta para entender la materia que nos rodea, *Revista Española de Física* **35**(1), 5 (2021).

[3] P. J. Salas Peralta y Á. L. Sanz Sáenz, Corrección de errores en ordenadores cuánticos, *Revista Española de Física* **20**(1), 20 (2006).

[4] M. Calixto, Computación Cuántica: un reto tecnológico, *Revista Española de Física* **15**(2), 35 (2001).

[5] D. P. DiVincenzo, The Physical Implementation of Quantum Computation, *Fortschritte der Physik*, **48**(9-11), 771 (2000).

[6] A. Cervera Lierta, Supercomputación y computación cuántica: el camino hacia la integración, *Revista Española de Física* **38**(2), 37 (2024).

[7] Google Quantum AI y cols., Quantum error correction below the surface code threshold, *Nature* **638**, 920 (2025)..

Alba Cervera Lierta
Barcelona Supercomputing Center,
investigadora Ramón y Cajal