Computadores cuánticos: ¿para qué y para cuándo?

ALBERTO PRIETO ESPINOSA
MIEMBRO DE LA ACADEMIA DE CIENCIAS MATEMÁTICAS, FÍSICO-QUÍMICAS Y NATURALES DE GRANADA

Se tardarán al menos de 10 a 15 años en que sean asequibles para su uso de forma convencional

El pasado 8 de enero IBM anunció la disponibilidad comercial del primer ordenador cuántico, pero esta noticia hay que analizarla con rigor para comprender su alcance. En gran parte, los progresos en la ingeniería de computadores son debidos a la miniaturización de los circuitos electrónicos. Pero estamos alcanzando el límite porque llega un momento en que las leyes físicas convencionales (macroscópicas) dejan de cumplirse y la descripción del mundo físico debe realizarse según los principios de la Física Cuántica. Si fabricásemos nuestros chips electrónicos en esas dimensiones nanoscópicas no funcionarían.

La Física Cuántica es difícil de entender y la encontramos incluso misteriosa y exótica. Es porque nosotros desarrollamos nuestra actividad en un contexto 'macroscópico'. Entendemos e intuimos lo que ocurre en el mudo macroscópico; sin embargo, no conocemos ni experimentamos directamente el mundo nanoscópico, donde aparecen propiedades y fenómenos muy alejados de nuestras experiencias directas y de nuestra intuición.

:: IDEAL

Los procesadores cuánticos utilizan unidades de información denominadas qubits. A diferencia de un bit clásico, que puede adquirir uno entre dos estados que denominamos 0 y 1, un qubit puede almacenar además de 0 y 1, simultáneamente, ambos valores; y en ese caso decimos que se encuentra en estado de 'superposición'. En el instante en que leemos o medimos un qubit, su estado de superposición colapsa, obteniéndose un 0 o un 1 clásico. El gran poder de la computación cuántica radica en la superposición. Cuando realizamos cálculos en un computador clásico, para entradas diferentes tenemos que efectuar ejecuciones nuevas. Sin embargo, en uno cuántico, en superposición, con una sola ejecución se realizan los cálculos simultáneamente para todas las entradas posibles. Así, si tuviésemos un procesador cuántico con 30 qubits con sus entradas en superposición se realizarían ¡1.073.741.824 operaciones simultáneamente!

La computación cuántica será muy útil para la resolución de problemas científicos e industriales de envergadura dentro de los que se encuentran: aprendizaje automático, buscadores superrápidos, obtención de métodos óptimos de tratamiento para un paciente, análisis de posibles estructuras de moléculas complejas, desarrollo de nuevos materiales, minería de datos, simulación de proteínas, simulación de sistemas cuánticos, etc.

Uno de los problemas que se resuelve cuánticamente en tiempos razonables es la factorización de números enteros. Los estándares actuales de criptografía se fundamentan precisamente en la imposibilidad práctica de realizar la factorización de números grandes; así, factorizar un numero de 1.024 bits podría tardar varios siglos utilizando computadores actuales. Sin embargo, hay un procedimiento cuántico (Algoritmo de Short) con el que este problema se resuelve con tiempos de ejecución razonables por lo que en el momento de que se disponga de procesadores cuánticos con gran número de qubits (del orden de 10.000) se podrán descifrar los mensajes encriptados con los estándares actuales. Esto es muy grave, además de porque tengamos que cambiar dichos estándares, porque se podrán descifrar los mensajes previos almacenados desde muchos años antes. Podemos concluir que no se vislumbra el uso de la computación cuántica para uso cotidiano (emails, generar documentos, consultar la web, etc.), sino como complemento a supercomputadores y, como estos, se proyectan usar remotamente, en la nube.

Un qubit puede implementarse por medio de una partícula, tal como un ion o un fotón. Manipulando el ion con un haz láser o con microondas se pueden efectuar cambios controlados del estado del qubit que dan lugar a los cálculos cuánticos.

Pero se presentan diversos problemas tecnológicos extremadamente difíciles de superar. El primero es cómo conseguir un ion aislado. Esto se logra 'atrapándolo' en una cavidad por medio de campos eléctricos o magnéticos y enfriándolo mediante láser. Otro problema es que el ion debe estar completamente aislado, no interactuando con su entorno, ya que si no entra en 'decoherencia', desapareciendo las propiedades cuánticas que tratamos de aprovechar. Incluso la temperatura o la luz ambiental provocan la salida de coherencia. Por estos motivos los procesadores cuánticos deben estar en cápsulas herméticamente cerradas, en un entorno de muy alto vacío y a muy bajas temperaturas. Por ejemplo, el procesador D:Wave 20000 funciona a -273,13 grados Kelvin (es decir, a tan sólo 0,02 grados por encima del cero absoluto). Las dificultades de aislamiento se disparan al tener que actuar externamente sobre los iones para operar, y si aumentamos el número de qubits del procesador.

Aunque en las dos últimas décadas se han desarrollado algunas plataformas, los esfuerzos para construir un computador cuántico universal, programable y funcional, está en sus primeras etapas; como lo estaba la computación clásica a mediados del siglo XX. Los sistemas ofrecidos por distintas empresas pueden considerarse prototipos, a muy pequeña escala (pocos qubits) no superando en prestaciones a los supercomputadores actuales. Además, tienen unas tasas de error de los resultados muy altas. No obstante, se están comercializando dispositivos cuánticos que realizan funciones concretas: encriptado criptográfico totalmente seguro (a distancias entre emisor y receptor de decenas de kilómetros), sensores, métodos de medida de precisión, etc.

A pesar de los anuncios en la prensa, y como indica Ignacio Cirac, uno de los pioneros e investigadores más acreditados en computación cuántica, se tardarán al menos de 10 a 15 años en conseguir computadores cuánticos asequibles para su uso de forma convencional con objeto de resolver problemas del mundo real. Para esto se necesitará disponer del orden de 500 qubits para cálculo básico, y muchos más (del orden de 5.000) si incluimos redundancias para corrección de errores y lograr la tolerancia a fallos.