Mitos cuánticos

LA COMPUTACIÓN CUÁNTICA

Gerardo Herrera Corral

Las computadoras cuánticas han generado expectativas muy altas. Para muchos, estos dispositivos serán capaces de todo, de manera que los que se encuentran en desarrollo se han convertido poco a poco en un mito.

Hace unos años, el 20 de septiembre de 2019, el *Financial Times* anunciaba:

"Google afirma haber alcanzado la supremacía cuántica", Poco después, el 23 de octubre, la prestigiosa revista *Nature* publicó que Google había conseguido oficialmente la supremacía cuántica usando el procesador Sycamore. La noticia acaparó los titulares en todo el mundo.

De esa manera, la empresa pretendía haber ganado la carrera en la que se quería mostrar que un dispositivo cuántico había superado a las computadoras convencionales en algún proceso de cálculo específico.

A la "supremacía cuántica" también se la conoce como "ventaja cuántica" y se usa para señalar áreas o problemas determinados en que las computadoras clásicas no resuelven, o, si lo hacen, será con más lentitud que su contraparte cuántica.

Un año después, investigadores chinos publicaban en la revista *Science* que habían alcanzado la supremacía cuántica utilizando un procesador superconductor llamado Zuchongzhi, y hace apenas unos días IBM presentó su ordenador cuántico más avanzado. El System two, que lleva un procesador Heron de 156 qubits con una tasa de error menor.

Aunque las computadoras cuánticas son la sensación del momento y parecen comenzar a mostrar capacidades especiales, es muy probable que no logren superar a las computadoras clásicas en la mayoría de los problemas de cálculo.

Las computadoras cuánticas no son ese dispositivo mágico del futuro que vendrá a resolverlo todo; tendrán ventajas, sí, en ciertas áreas de cálculo como ciberseguridad, simulación de procesos físicos y químicos y quizás en Inteligencia Artificial. Pero no necesariamente serán el súper dispositivo con cualidades misteriosas que mucha gente está pensando.

Sin embargo, el que las computadoras cuánticas no sean mejores en todo no hace que su desarrollo sea poco interesante.

Si lo que queremos es desmitificar la mecánica cuántica y sus aplicaciones, entonces, para el caso de las computadoras cuánticas, esto es lo mismo que matizar.

¿Las computadoras cuánticas son más rápidas que las convencionales?

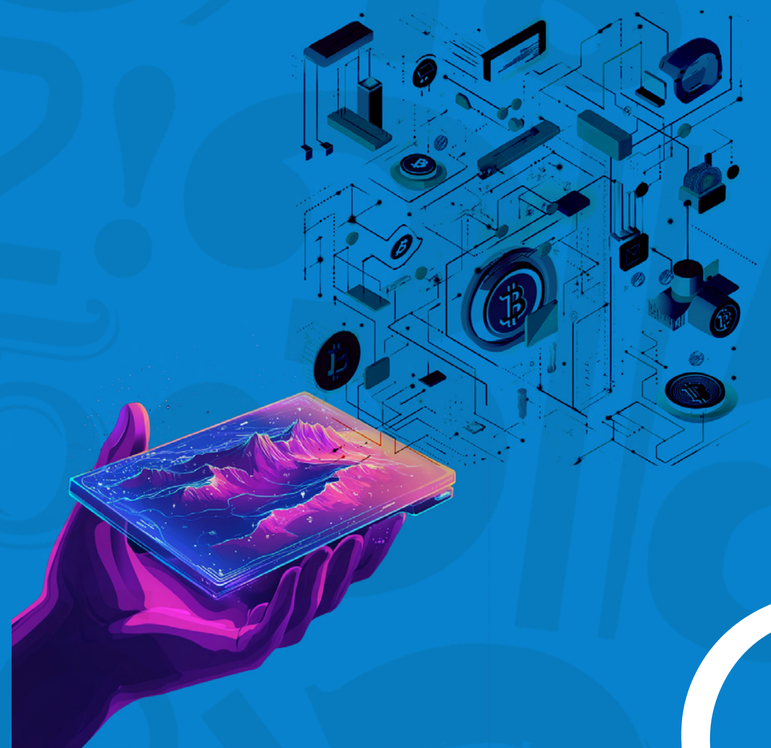
No, en general. Las computadoras cuánticas podrían ser más rápidas que las convencionales en algunas operaciones.

Se estima, por ejemplo, que las computadoras cuánticas podrán factorizar más rápidamente un número en términos de sus números primos porque existe ya un algoritmo conocido como "Algoritmo de Peter Shor", con el que se puede mostrar que esta operación es considerablemente más veloz en esos dispositivos.

La operación numérica tiene muchas consecuencias en ciertas áreas aplicadas y un ejemplo es el procedimiento de encriptación de datos que juega un papel importante en transacciones de todo tipo y comunicaciones donde se puede comprometer la seguridad de las partes.

Un ejemplo de lo que significa factorizar en términos de números primos:

150 se puede escribir como **2 × 75**
El **2** ya es un número primo.
El 75 se puede escribir como **5 × 15**
El **5** ya es primo.
El **15** se puede descomponer como **3 × 5**
Ahora todos son primos y el número **150**
se puede escribir como:
2 × 5 × 3 × 5



La búsqueda en lista de datos podría ser otra operación donde las computadoras cuánticas serían hasta cinco veces más rápidas que las tradicionales.

Los números primos se usan en criptografía y, particularmente, en el sistema asimétrico o de clave pública en certificados digitales. Con esta tecnología las personas tienen una clave pública que pueden entregar a cualquier persona y otra privada que solo ella conoce.

Con este sistema el emisor necesitará la clave pública de su destinatario para con ella cifrar el mensaje, entonces el receptor usará la clave privada para poder ver el texto. Sin ese par de claves no se puede llevar a cabo el descifrado.

La fortaleza de este método se encuentra en lo difícil que resulta factorizar número grandes. Si contamos con números primos muy grandes, y los multiplicamos para poder descifrar el mensaje, será necesario recuperar esos factores. Y como los números son grandes, resultará prácticamente imposible. Actualmente se conocen número primos tan grandes que tienen trescientas cifras, es decir, 10^{300} cifras, un uno seguido de trescientos ceros.

¿Las computadoras cuánticas aprovechan el procesamiento paralelo?

A menudo se dice que las computadoras cuánticas encuentran la solución a los problemas probando en paralelo, es decir, probando simultáneamente todas las opciones posibles.

A menudo se dice que las computadoras cuánticas encuentran la solución a los problemas probando en paralelo, es decir, probando simultáneamente todas las opciones posibles.

Los computadores cuánticos hacen uso del principio de superposición, esto es, la propiedad de los sistemas de encontrarse en todos los estados posibles y la combinación de estos. Con esto en mente se ha dicho que las computadoras cuánticas estarán viendo todas las posibles salidas durante el proceso de cálculo en un problema.

En cierta forma sí, porque las computadoras cuánticas funcionan con base en compuertas lógicas necesarias para darle forma al problema. La superposición se efectúa maximizando la probabilidad del estado correcto y minimizando la del incorrecto.

Por la naturaleza cuántica del sistema, al momento de preguntar por la solución del problema este colapsará en alguno de los estados de la superposición en una sola respuesta. En el momento del colapso todas las otras opciones desaparecerán. Sería como ensayar con una computadora clásica las soluciones hipotéticas elegidas al azar, en cuyo caso el dispositivo cuántico es más veloz. Eso no significa que todos los problemas se puedan plantear en tales términos.

*GERARDO HERRERA CORRAL *Físico de la Universidad de Dortmund y del Cinvestav, es líder de los latinoamericanos en el CERN. Ha escrito diversos libros, entre ellos* Dimensión desconocida. El hiperespacio y la física moderna *(Taurus, 2023)* y Antimateria. Los misterios que encierra y la promesa de sus aplicaciones *(Sexto piso, 2024).*