NOTA DE FUTURO 5/2017

27 de noviembre de 2017

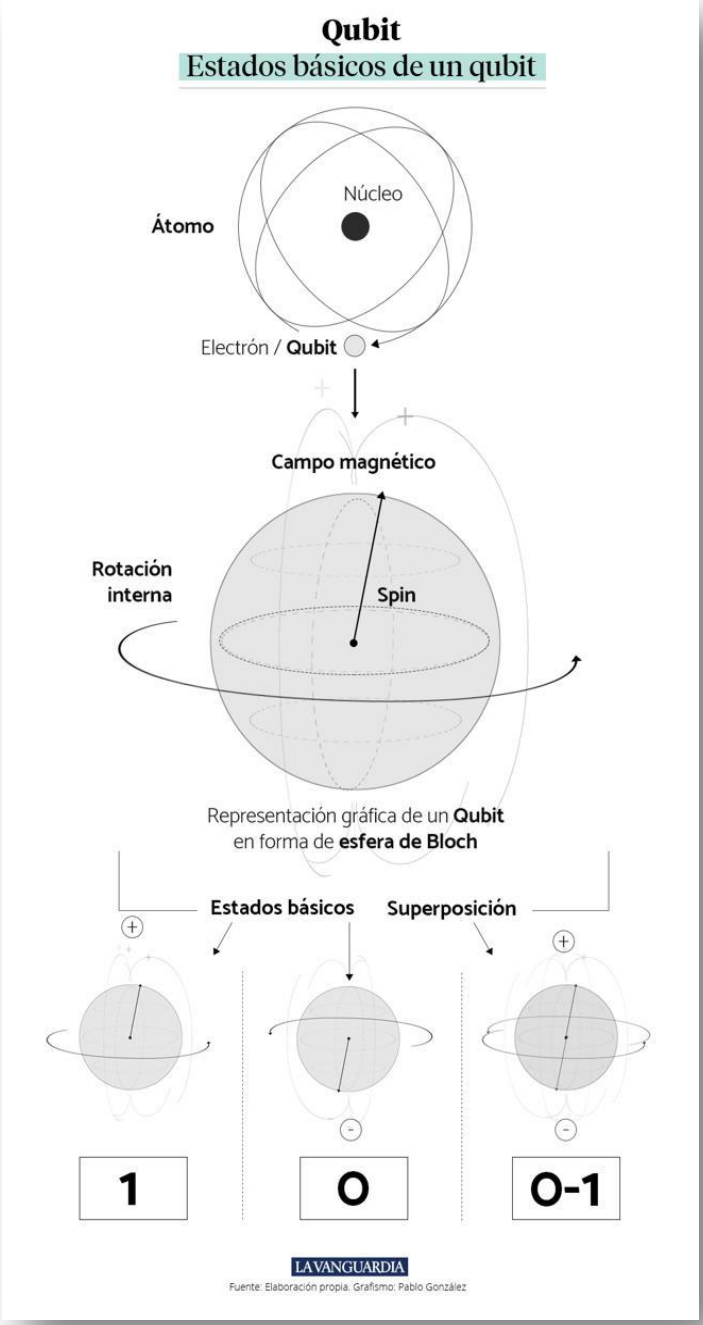
*Laura Gascón y Ana García**

Computación cuántica

Nota de futuro: Computación cuántica

¿Qué es un ordenador cuántico?

Un computador o un ordenador cuántico es un paradigma de computación que, a diferencia de la computación clásica, utiliza los qubits, cúbits o bits cuánticos para realizar las operaciones en vez de los tradicionales bits, esto le permite resolver problemas a mayor velocidad y también crear nuevas lógicas posibles de formas nuevos algoritmos. Los qubits se basan en elementos cuánticos, como átomos, iones o fotones que, por naturaleza, pueden entrelazarse y superponerse.



La idea de la computación cuántica surgió en 1981, cuando Paul Benioff decidió aprovechar las leyes cuánticas en la computación en vez de los voltajes eléctricos. Es decir, los bits usan el lenguaje binario que solo toma dos valores: 0 y 1, mientras que los cúbits usan las leyes de la mecánica cuántica, por lo que dichos valores pueden estar en superposición coherente y pueden formar miles de combinaciones, permitiendo así que se realicen varias operaciones a la vez y que se rompa cualquier tipo de encriptación de manera instantánea.

* Alumnas en prácticas de la Universidad Pontificia de Comillas

Si observamos una serie de 3 bits, veremos su estado en el momento dado y, por lo tanto, pueden estar combinados de ocho maneras diferentes: 000, 001, 010, 011, 100, 101, 110, 111. Con 4 bits tendremos 16 combinaciones, con 5 serán 32, etc. Mientras que, si tenemos una serie de 3 qubits, estos pueden representar las ocho combinaciones mencionadas al mismo tiempo.

La superposición del átomo consiste en que un átomo puede adoptar un estado de 0 y de 1 como usan los bits en el lenguaje binario, pero además puede adoptar ambos estados al mismo tiempo. Los computadores cuánticos son capaces de probar simultáneamente todas las posibilidades que existen para la solución concreta de un problema, en lugar de probar todas las posibilidades consecutivamente, como se hace actualmente con los ordenadores tradicionales.

Por otra parte, los átomos también cuentan con otra característica llamada entrelazamiento atómico. Gracias a esta particularidad, un átomo puede transmitir determinadas propiedades a otro sin que haya nada de por medio. Podríamos decir que es como una telepatía entre átomos, ya que cuando se produce un cambio en uno se transmite al instante en el otro. Estos cambios suponen un enorme avance en la potencia de computación, que permiten realizar cálculos complejos que actualmente son inalcanzables incluso en los superordenadores. Asimismo, permiten crear una red de átomos que funcionan de forma armónica.

Hasta la fecha, Google y NASA cuentan con una computadora cuántica que usan en su búsqueda por alcanzar mayor velocidad de resolución de problemas y en su análisis de datos de manera más precisa. Esta máquina se llama D-WAVE 2X y les ha permitido, por ejemplo, que desarrollen más proyectos en temas de inteligencia artificial. La primera versión de este prototipo funcionaba con 512 qubits y costaba alrededor de 11 millones de euros. La nueva versión de este prototipo se dio a conocer en 2013 y, según afirman sus desarrolladores, es hasta 108 millones de veces más rápido que un ordenador tradicional.

Además, Google ha comenzado a realizar pruebas de seguridad en su navegador Chrome ante las posibles amenazas de la computación cuántica, ya que los actuales sistemas y protocolos de seguridad se verían comprometidos. Las empresas están trabajando para que, en unos 10 o 15 años, los ordenadores cuánticos sean una realidad cotidiana para toda la población, aunque todavía queda un largo camino por recorrer ya que, para su correcto funcionamiento, los ordenadores cuánticos necesitan unas condiciones muy concretas sobre las que se expondrán los problemas más adelante.

En un procesador cuántico no se utilizan ni monitores, ni discos duros, ni ningún tipo de hardware tal y como lo conocemos en el ámbito de la informática actual. Todas las operaciones tienen lugar

en una unidad de procesamiento que debe permanecer aislada, ya que los estados cuánticos del átomo son muy frágiles.

Por otro lado, IBM ha puesto a disposición del público general un ordenador cuántico a través de Internet, que podrá usarse mediante la descarga de un software. Esta tecnología permitirá a cualquier científico, investigador o programador encontrar errores y proponer mejoras a través de una computadora mucho más potente que una ordinaria.

Posibles usos de la computación cuántica

Las investigaciones indican que se solucionarán problemas en distintas áreas que mejorarán la calidad de vida de muchas personas. Aunque aún los resultados no hayan alcanzado el nivel que se espera de ellos, ya han arrojado atisbos de que van por muy buen camino.

Existen numerosos campos donde el qubit tendrá gran relevancia, como la tele transportación de información cuántica tanto en la tierra como en el espacio, las comunicaciones con seguridad definitiva (infranqueable) y el comienzo de big data a niveles inimaginables.

La D-WAVE ya ha logrado reconocer el 90% de los árboles de una fotografía aérea de Mill Valley, California. Aunque un ordenador actual de alto procesamiento también podría haber cumplido la tarea, esto se ha hecho a mayor velocidad. Así, se ha demostrado que las computadoras ya pueden procesar una mayor cantidad de data para resolver problemas más complejos. Entre los cuales encontramos:

- Detección de objetos: más de 500.000 problemas de optimización discreta fueron resueltos durante la fase de aprendizaje, accediendo al sistema D-WAVE de forma remota. Por ejemplo, Google ha intentado aplicarlo para identificar un automóvil en una imagen con un algoritmo binario de clasificación.

- Optimización de radioterapias: la radioterapia se utiliza para el tratamiento del cáncer, destruyendo las células cancerígenas e impidiendo que se reproduzcan o muten. Sin embargo, la radioterapia tiene efectos colaterales, ya que puede dañar células sanas. Las computadoras cuánticas pueden facilitar una aplicación de radioterapia perfecta en el área afectada por el cáncer.

- Optimización del traslado de agua por tuberías en la industria: ayudado del HPC y un programa denominado EPANET, el ordenador cuántico permite el análisis de sistemas

de distribución de agua potable, dando las herramientas necesarias para diseñar la red óptima, penalizando los resultados indeseables y compensando los resultados deseables (bajo coste, bajo riesgo o seguridad).

- Mejores simuladores virtuales: una gran parte de la potencia de supercomputación actual se utiliza para realizar simulaciones moleculares y de materiales. Físicos o biólogos podrán hacer simulaciones mucho más realistas, que podrían incluso sustituir a algunos experimentos reales y ayudar al avance de la ciencia. También los meteorólogos podrán simular mejor el clima, es decir, entenderlo y predecirlo con mayor exactitud.

- Sistemas criptográficos: un ordenador cuántico podría descifrar todos los mensajes encriptados. Las comunicaciones se podrían basar en la criptografía cuántica, unos mensajes que sí que serían imposibles de descifrar. Además, a la hora de descifrar una contraseña, el qubit puede procesar todas esas opciones en simultáneo y dar una respuesta casi inmediata. En el sector de la banca, el sistema criptográfico RSA, que se integra en los navegadores y protege la banca online, se puede quebrar rápidamente con un ordenador cuántico potente, mientras que uno convencional tardaría incluso años. Fuentes cubanas han publicado que China está ensayando un sistema más seguro de intercambio de mensajes basado en los principios de la computación cuántica que sería imposible de hackear.

Inconvenientes y soluciones de los computadores cuánticos

La superposición de los átomos puede alterarse por el contacto con un campo electromagnético o ante la más mínima vibración o cambio de la temperatura. Esta alteración provocaría errores de cálculo. Por este motivo, los procesadores en los que se encuentran los qubits, han de enfriarse y mantenerse a cero absoluto (-273 grados Celsius).

Asimismo, las transferencias de energía se dan desde un mayor estado energético hasta uno menor para lograr su estabilidad. Y los qubits, al ser unidades subatómicas, no escapan de dicha transferencia. Según una investigación publicada en NIST, la velocidad de un cambio de estado cuántico estaría limitada por la cantidad de energía que contiene.

Otro inconveniente es el coste. Su desarrollo está costando millones de dólares, por lo que solo empresas como Google o NASA han sido capaces de costear la investigación.

Ante estos problemas se pueden plantear las siguientes soluciones:

Al trabajar con partículas subatómicas, se necesitan soluciones que involucren campos magnéticos y eléctricos que promuevan las interacciones subatómicas. La Universidad de Sussex ya ha implementado diseños que impulsan el uso de campos eléctricos para que los iones se muevan entre los módulos del procesador.

Igualmente, los niveles de energía pueden ser corregidos con una «correcta arquitectura del ordenador». Podría ser posible limitar el efecto que causa la bajada de energía de las partículas subatómicas.

También se han llevado a cabo mejoras en el sistema de coherencia de resultados. La coherencia es importante en este proceso: al arrojar muchas soluciones, solo una vendría a ser una solución real al problema introducido a la computadora cuántica. Al no haber restricciones de energía, no existe la limitación natural del proceso, haciendo que arroje muchos datos al mismo tiempo y provocando sobre-soluciones al problema.

Bibliografía

Barredo, Á. (5 de Mayo de 2017). Computación cuántica: el futuro de los ordenadores. *La Vanguardia* .

Benjamin, S. (s.f.). *Oxford Quantum*. Obtenido de http://oxfordquantum.org

Computación, Información y Criptografía Cuántica. (s.f.). Obtenido de https://quitemadorg.wordpress.com/

cuánticas, G. d. (s.f.). *Observatorio I+D+i UPM*. Obtenido de http://www.gcc.fi.upm.es/es/

TEKNAUTAS. (4 de Mayo de 2016). Ya puedes utilizar un ordenador cuántico desde tu casa a través de internet. *El Confidencial* .