Computación cuántica

José Manuel Huidobro

Revista Digital de ACTA

Diciembre 2019

Publicación patrocinada por

CEDRO

ACTA representa en CEDRO los intereses de los autores científico-técnicos y académicos. Ser socio de ACTA es gratuito.

Solicite su adhesión en acta@acta.es

Computación cuántica

COMPUTACIÓN CUÁNTICA

Recientemente, el 15 de octubre de 2019, la compañía IBM anunciaba la disponibilidad de un ordenador cuántico, (en enero había presentado el IBM Q System One), el más grande y potente de forma comercial. Un ordenador de 53 cúbits (alternativa breve de bit cuántico, o "qubits", como también se denominan) –con más del doble de capacidad de procesamiento que el ordenador cuántico predecesor–, que entró en operación para sus clientes de computación cuántica, y que operará en el Centro de Computación Cuántica que IBM tiene en Poughkeepsie (Nueva York).

No es el más grande del mundo, pues Google dispone de uno de 72 cúbits, pero que es solo para uso propio, para calcular sus sofisticados algoritmos de búsqueda, y que no está disponible para uso de otras compañías externas. También, en el verano de 2018 la compañía de computación cuántica Rigetti anunció sus avances en un chip de 128 cúbits, superando así al de Google.

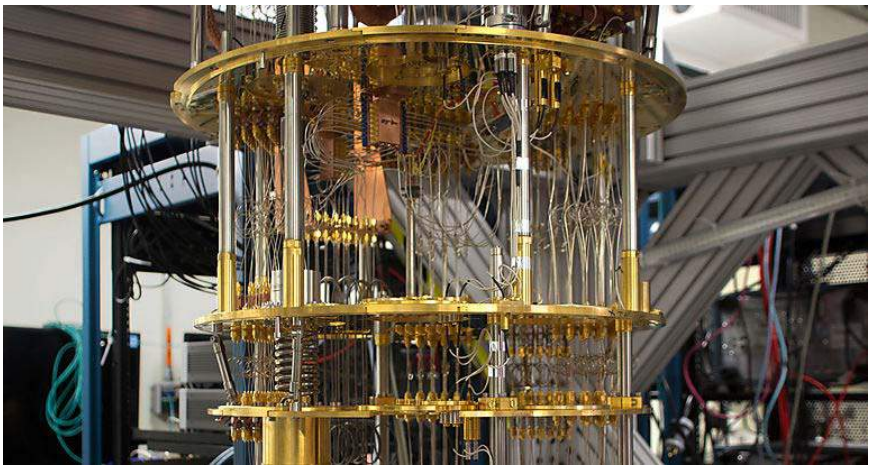

Figura 1. Ordenador cuántico de IBM.

Este nuevo ordenador cuántico es el decimocuarto de IBM, que actualmente compite contra compañías como Google, Microsoft, Honeywell, Rigetti Computing, IonQ, Intel y NTT, que llevan algunos años desarrollando proyectos centrados en computación cuántica. Los primeros se desarrollaron en el año 1998.

INTRODUCCIÓN

Aunque se ha realizado este anuncio, a día de hoy, la computación cuántica sigue más dentro del campo experimental, puesto que aún depende de otros factores que pueden afectar su desempeño, como es la refrigeración de las máquinas, pues éstas deben mantenerse a temperaturas muy próximas al cero absoluto. Lo que es un hecho, es que este tipo de ordenadores son capaces de resolver problemas que prácticamente son imposibles para cualquier otro tipo de ordenador tradicional, por potente que sea.

De una forma muy simple, se puede decir que un ordenador clásico, digital, se base en transistores (que forman parte de los microchips que lo integran), además de en bits; su capacidad y velocidad de proceso viene determinada por el número de éstos, cuanto más alto sea, mayor será; pero ello tiene un límite, pues si bien los transistores son cada vez más pequeños (Ley de Moore –el número de transistores en cada microprocesador se duplica cada dos años aproximadamente, aunque la ley originalmente fue formulada para establecer que la duplicación se realizaría cada

año), ello tiene un límite físico, y si se sobrepasase ya no se seguirían las leyes de la física newtoniana, sino la de la física cuántica y no podrían funcionar, por el llamado “efecto túnel”.

Aunque ya en la década de los años cincuenta físicos como Richard Feynman hablaron del potencial de la computación cuántica, realmente la idea de computación cuántica surgió en 1981, cuando Paul Benioff, basándose en las teorías del físico alemán Max Planck, expuso su teoría para aprovechar las leyes cuánticas en el entorno de la computación. En vez de trabajar a nivel de voltajes eléctricos, se trabaja a nivel de cuanto.

Figura 2. Paul Benioff.

La solución a este problema viene de la mano de los ordenadores cuánticos, un avance significativo, que usan las propiedades de las partículas subatómicas, como son los protones, electrones y los fotones, que tienen una serie de propiedades, como es que su estado no solo puede representar un 0 o un 1, como los bits, sino que puede ser 0 y 1 a la vez (*dos estados ortogonales de una partícula subatómica, lo que permite que se puedan realizar varias operaciones simultáneamente, según el número de cúbits*), por lo que con ellos el crecimiento de capacidad con el aumento de “cúbits” no es lineal como en el caso de emplear “bits”, sino exponencial. Por ejemplo, con 1 bit tenemos un estado (0 o 1), con dos, 2, con diez, 10, con veinte, 20, mientras que con 10 cúbits, tenemos 2^{10} = 1.024 y con 20 cúbits: 10^{20} = 1.048.576, y así sucesivamente. Como se puede apreciar, la diferencia es más que notable conforme aumenta su número, pues al añadir nuevos cúbits la capacidad se dispara exponencialmente.

El concepto de cúbit –viene del inglés *quantum bit* o bit cuántico–, unidad básica de información en computación cuántica, es abstracto y no lleva asociado un sistema físico concreto.

> En el cómputo cuántico la unidad mínima de información es el cúbit (*quantum bit*) que, a diferencia del bit que sólo puede tomar los valores 0 y 1, se encuentra en una superposición simultánea de dos estados cuánticos, y en N cúbits se encuentran simultáneamente superpuestos 2^N estados. Esta superposición cuántica permite la posibilidad de realizar un procesamiento paralelo a gran escala. Es decir, la capacidad operacional de un ordenador cuántico aumenta exponencialmente con el tamaño del mismo, el número de cúbits.

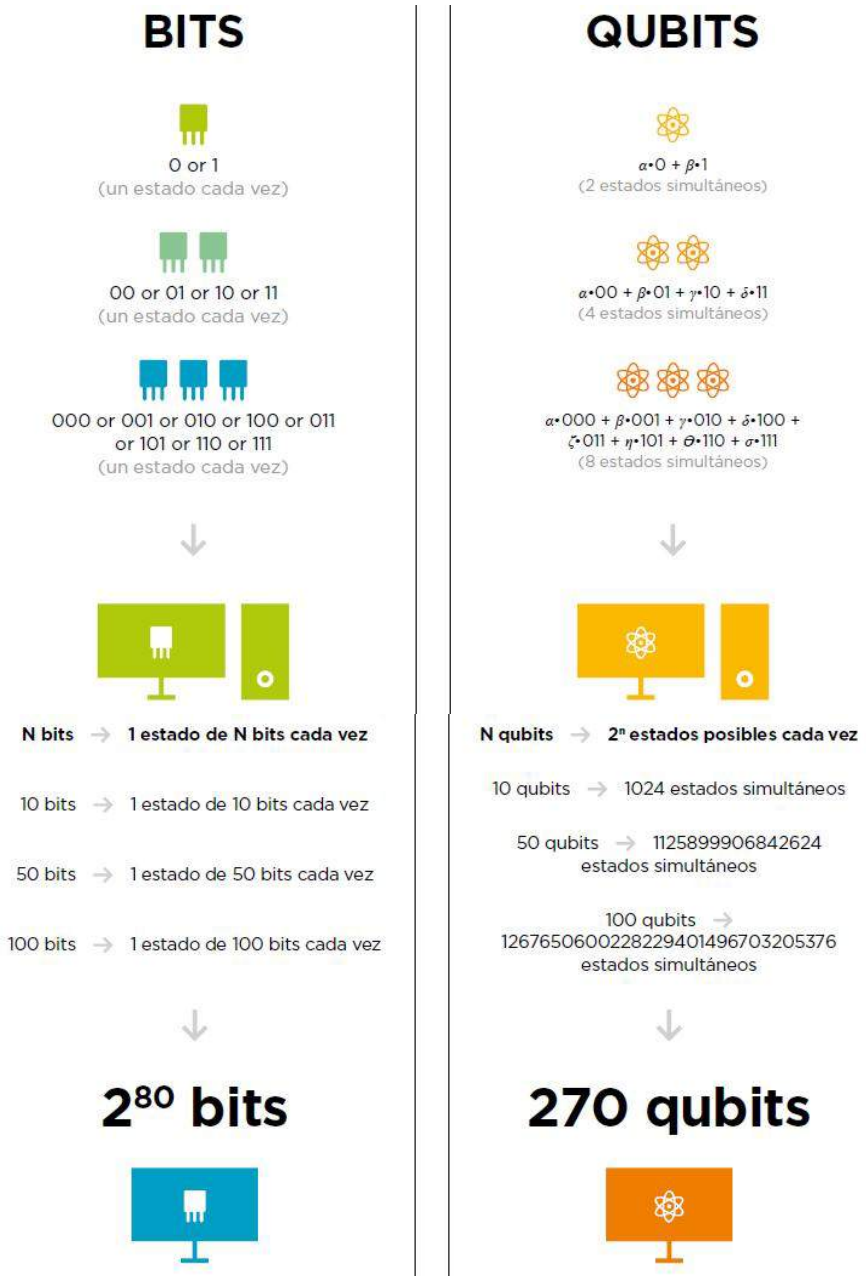

Figura 3. Bits versus Cúbits

Como curiosidad, se estima que con 270 cúbits se podrían tener más estados diferentes –más cadenas de caracteres diferentes y simultáneas– en un ordenador cuántico que el número de átomos en el universo, que se estima en 2^{80}.

Para estas partículas subatómicas se presentan dos modelos diferentes: "superposición" (una misma partícula puede estar en múltiples estados, realidades o probabilidades. al mismo tiempo), y "entrelazado" (un par de partículas evolucionan de la misma manera, están sincronizadas), lo que puede utilizarse, en condiciones controladas, para aumentar la capacidad y potencia de los ordenadores basados en ellas. Luego veremos con más detalle su funcionamiento.

Figura 4. Representación mediante 0 y 1.

Con ellos su capacidad supera los límites de los ordenadores digitales, y pueden utilizarse para resolver problemas que requieren gran potencia de cálculo, como son el estudio de nuevos materiales, nuevos fármacos, inteligencia artificial, análisis y cálculos económicos complejos, de riesgos de activos financieros, predicción del tiempo y cambio climático, seguridad en la nube, criptografía, etc. abriendo el camino a nuevos desarrollos en el campo científico, de la innovación y comercial.

Actualmente, la industria farmacéutica es una de las que más se benefician de esta tecnología. La razón es que para elaborar algunos medicamentos hay que calcular muchas variables. Un ordenador convencional puede realizar multitud de combinaciones, pero de manera lenta. Un ordenador cuántico reduce la espera y puede generar mejores resultados. Esto mismo puede aplicarse a otros campos, como el desarrollo de nuevos materiales por parte de la industria, como es el desarrollo de nuevas baterías para los automóviles eléctricos, acelerando todo el proceso y proporcionando una fiabilidad de resultados nunca visto.

En un artículo aparecido en el MIT Technology Review, que se reproduce a continuación en parte, se explica el funcionamiento de estos conceptos muy claramente. Se cuenta qué son y cómo funcionan estas máquinas, cuáles son los fenómenos cuánticos que aprovechan para ser tan potentes y cuales son sus aplicaciones, además de los retos que tienen por delante antes de cumplir su promesa de revolucionar industrias enteras. Accesible en el siguiente enlace:

https://www.technologyreview.es/s/10920/que-es-un-ordenador-cuantico-definicion-y-conceptos-clave

Ley de Moore

La gráfica de la Figura 5 ilustra cómo los microprocesadores creados por Intel se han ajustado a la Ley de Moore en los últimos 45 años. Los puntos de la gráfica corresponde a algunos de los microprocesadores de Intel, mostrando su fecha de comercialización en el eje X y el número de transistores en el eje Y. La línea continua de la gráfica corresponde a la progresión teórica de acuerdo con la Ley de Moore (duplicación cada dos años).

Esta progresión ha sido posible gracias a los avances en la tecnología de fabricación de microprocesadores. Estas tecnologías se suelen denominar por la escala del proceso litográfico utilizado en la fabricación (expresada en micrómetros en los años 70 y 80, y en nanómetros desde los 90).

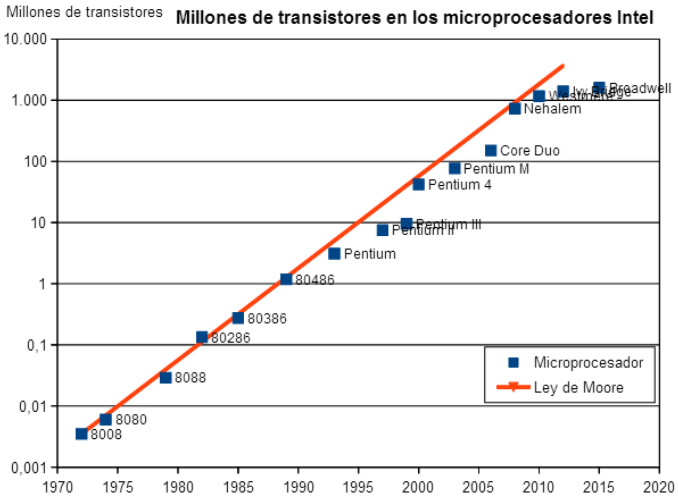

Figura 5. Crecimiento según la Ley de Moore

Cada vez se fabrican microchips más pequeños ya que, cuanto más pequeño es el dispositivo, mayor velocidad de proceso se alcanza. Sin embargo no se pueden hacer los chips infinitamente pequeños, pues hay un límite en el cual dejan de funcionar correctamente. Cuando se llega a la escala de nanómetros los electrones se escapan de los canales por donde deben circular por el llamado "efecto túnel", un fenómeno típicamente cuántico.

ORDENADOR CUÁNTICO. CONCEPTOS CLAVE

Un ordenador cuántico aprovecha algunos de los fenómenos casi místicos de la mecánica cuántica para lograr grandes aumentos de potencia de procesamiento. Las máquinas cuánticas prometen superar incluso a los superordenadores tradicionales más poderosos, un hito conocido como supremacía cuántica.

En 1998 nació la primera máquina de 2 cúbits, que fue presentada en la Universidad de Berkeley (California). Un año más tarde, en 1999, en los laboratorios de IBM se diseñó la primera máquina de 3 cúbits, que además fue capaz de ejecutar por primera vez el algoritmo de búsqueda de Grover, en el 2000 ya con 5 y 7 cúbits, en el 2005 con 8, en 2006 con 12, en 2007 con 16, etc.

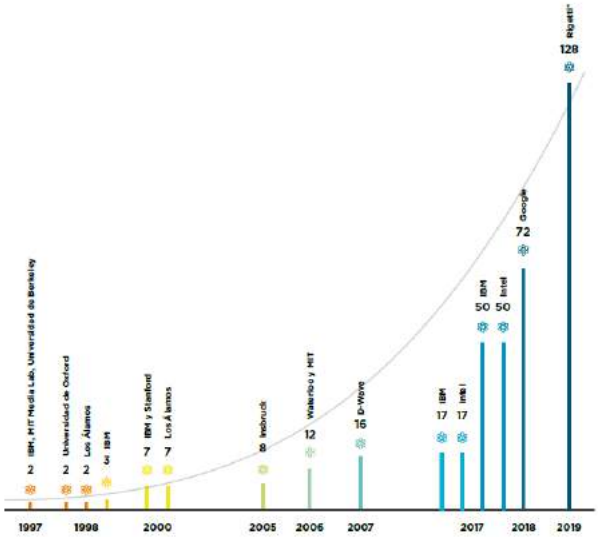

Figura 6. Evolución de los ordenadores cuánticos, por el número de cúbits.

La evolución, desde entonces ha sido rápida, y veinte años más tarde, los últimos ordenadores cuánticos superan ya los 50 cúbits.

> Para hacerse una idea del gran avance que esto supone, un ordenador cuántico de 30 cúbits equivaldría a un procesador convencional de 10 teraflops (millones de millones de operaciones en coma flotante por segundo).

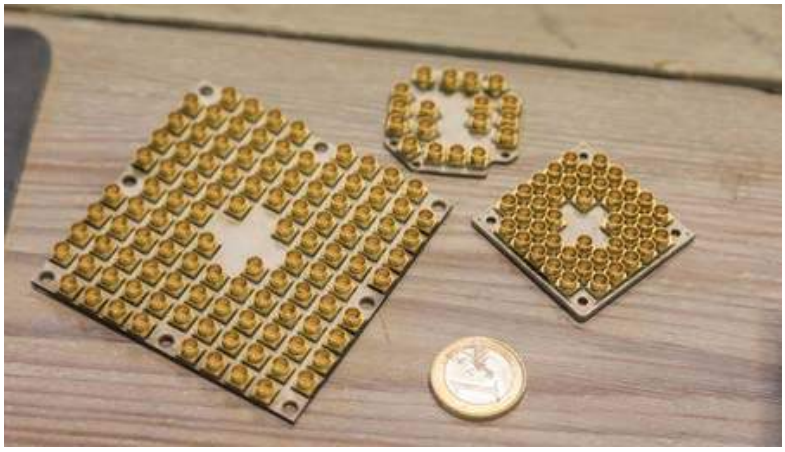

Figura 7. Procesador cuántico de 49 cúbits de Intel.

En un ordenador cuántico no hay memoria, ni disco duro, tan sólo tenemos un procesador al que se hacen llegar las señales de microondas necesarias para gestionar los estados de los cúbits. El receptáculo donde se enfría al procesador es el componente más llamativo y está compuesto por diferentes niveles de enfriamiento hasta llegar a la zona donde trabaja el procesador.

Una de las características principales de los ordenadores cuánticos es el método de enfriamiento, pues estos dispositivos deben enfriarse hasta un valor cercano al cero absoluto pero sin sobreenfriarse, pues los cúbits perderían sus propiedades en muy poco tiempo. Este hecho dificulta su programación y requiere de algoritmos que trabajen de forma eficiente y rápida para que los cúbits no pierdan su coherencia.

Figura 8. Ordenador cuántico con el procesador de Intel

Aunque usar una máquina clásica seguirá siendo la solución más fácil y económica para resolver la mayoría de los problemas, los ordenadores cuánticos prometen impulsar impresionantes avances en varios campos, desde la ciencia de los materiales hasta la investigación farmacéutica. Las empresas ya están experimentando con ellos para desarrollar las baterías más ligeras y más potentes para los coches eléctricos y para ayudar a crear nuevos fármacos.

Actualmente Estados Unidos y China son «la punta de lanza» mundial en computación cuántica.

El secreto del poder de un ordenador cuántico reside en su capacidad para generar y manipular los bits cuánticos o cúbits.

¿Qué es un cúbit?

Los ordenadores actuales usan bits: un flujo de pulsos eléctricos u ópticos que representan unos o ceros. Todo el mundo digital, desde los tuits y correos electrónicos a las canciones de iTunes y vídeos de YouTube son en esencia largas cadenas de ceros y unos.

Ejemplo: con 1 bit se tiene bien un 0 o un 1, pero solo uno de ellos, es decir un número o dígito; con 2 bits se tiene (0 o 1, 0 o 1) es decir dos números; con 3 bits se tiene (0 o 1, 0 o 1, 0 o 1) es decir tres números, con 4 cuatro números o dígitos, así sucesivamente. Por ejemplo, en la secuencia digital 01100010 tenemos bits u 8 dígitos, con independencia de que sean ceros o unos.

Los ordenadores cuánticos usan cúbits, medida del estado de partículas subatómicas como electrones o fotones. Generar y manejar los cúbits es un enorme desafío científico y de ingeniería. El enfoque de algunas compañías, como IBM, Google y Rigetti Computing, se basa en circuitos superconductores enfriados a temperaturas más bajas que el espacio profundo. Otras empresas, como IonQ, atrapan átomos individuales en los campos electromagnéticos en un chip de silicio en una cámara de vacío ultra alto. En ambos casos, el objetivo es aislar a los cúbits en un estado cuántico controlado.

El estado de un cúbit puede verse como un punto en la superficie de una esfera (llamada esfera de Bloch). En esta representación los polos de la esfera representan los bits clásicos “0’’ y “1’’ y todos los demás puntos son las distintas posibilidades que puede tomar un cúbit.

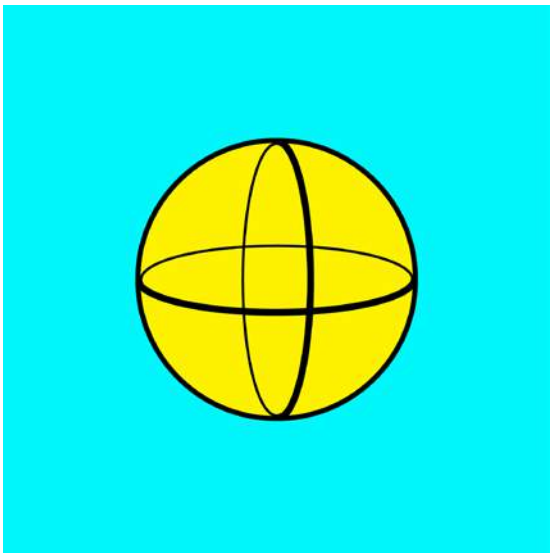

Figura 9. Representación idealizada de un cúbit.

Los cúbits tienen algunas propiedades cuánticas peculiares que logran que un grupo de ellos sea capaz de proporcionar mucha más potencia de procesamiento que la misma cantidad de bits binarios. Una de esas propiedades es la superposición y la otra el entrelazamiento cuántico.

La mecánica cuántica nos enfrenta a otro tipo de reglas de la física que implican una forma de calcular diferente. Ya no tenemos 0 y 1. Tenemos estados cuánticos y también el estado de superposición, que consiste en la posibilidad de tener distintas probabilidades de los estados 0 y 1.

Superposición cuántica

Los cúbits pueden representar numerosas combinaciones posibles de unos y ceros al mismo tiempo. La capacidad de estar simultáneamente en múltiples estados se llama superposición cuántica. Para poner los cúbits en superposición, los investigadores los manipulan con láseres de precisión o haces de microondas.

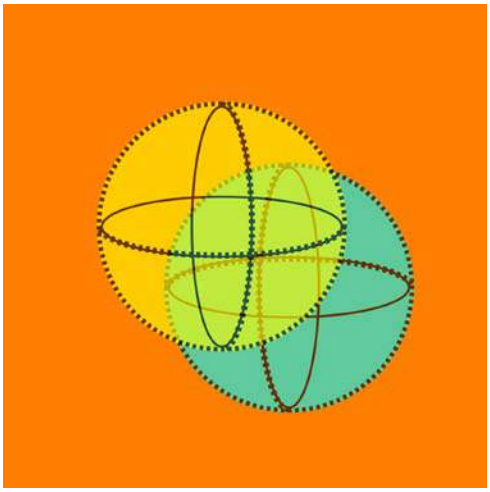

Figura 10. Superposición cuántica.

Gracias a este contradictorio fenómeno, un ordenador cuántico con varios cúbits en superposición puede llegar a una gran cantidad de posibles resultados de forma simultánea. El resultado final del cálculo solo emerge cuando se miden los cúbits, lo que inmediatamente hace que su estado cuántico se "colapse" en forma de cero o de uno.

Entrelazamiento cuántico

Los investigadores pueden generar parejas de cúbits "entrelazados", lo que significa que ambos existen en un mismo estado cuántico. Cambiar el estado de uno de los cúbits altera instantánea-mente el estado del otro de una manera predecible. Esto sucede incluso si están separados por distancias muy largas, la misma base de la “tele transportación).

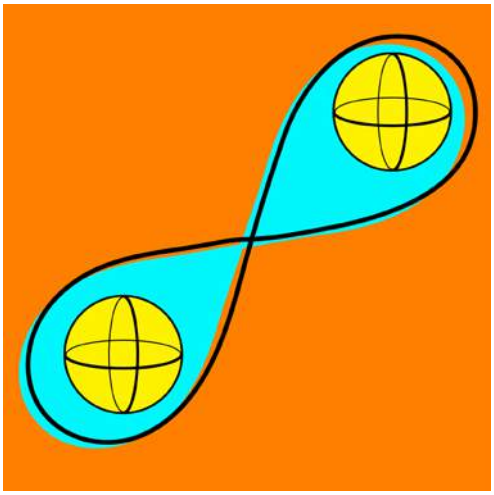

Figura 11. Entrelazamiento cuántico.

Nadie sabe realmente cómo o por qué funciona el entrelazamiento cuántico. El fenómeno desconcertó incluso a Albert Einstein, quien lo describió como "una espeluznante acción a distancia". Pero el entrelazamiento resulta clave para que los ordenadores cuánticos adquieran su poder. En un ordenador convencional, duplicar el número de bits duplica su capacidad de procesamiento. Pero gracias al entrelazamiento, añadir cúbits adicionales a una máquina cuántica produce un aumento exponencial en su capacidad de procesamiento.

¿Qué es la decoherencia?

Los ordenadores cuánticos son mucho más propensos a errores que los ordenadores clásicos debido a la decoherencia.

Este es el fenómeno mediante el cual la interacción de los cúbits con su entorno provoca que su comportamiento cuántico decaiga y finalmente desaparezca. Su estado cuántico es extremadamente frágil. La más leve vibración o cambio en la temperatura (alteraciones conocidas como "ruido" en el lenguaje cuántico) puede hacer que salgan de la superposición antes de que su trabajo se haya realizado correctamente. Es por eso que los investigadores hacen todo lo posible para proteger los cúbits del mundo exterior en esas neveras y cámaras de vacío muy enfriadas.

Pero a pesar de sus esfuerzos, el ruido todavía causa muchos errores que se infiltran en los cálculos. Los algoritmos cuánticos inteligentes capaces de compensar y agregar más cúbits también ayudan. Sin embargo, es probable que se necesiten miles de cúbits estándar para crear uno único, altamente fiable, conocido como cúbit "lógico". Esto debilitará la capacidad computacional de un ordenador cuántico.

Y ahí está el problema, pues hasta ahora, los investigadores no sido capaces de generar más de 128 cúbits estándar. Por lo tanto, aún faltan muchos años para tener ordenadores cuánticos de gran utilidad, pero eso no ha reducido las esperanzas de los pioneros de ser los primeros en demostrar la "supremacía cuántica".

Supremacía cuántica

Es el punto en el que un ordenador cuántico puede completar un cálculo matemático imposible incluso para el superordenador más poderoso en un tiempo razonable.

Todavía no está claro cuántos cúbits exactamente serán necesarios para lograrlo porque los investigadores siguen encontrando nuevos algoritmos para mejorar el rendimiento de las máquinas clásicas, y el hardware supercomputacional sigue mejorando.

Pero los investigadores y las compañías están trabajando arduamente para reclamar el título, realizando pruebas contra algunos de los superordenadores más poderosos del mundo. Así, Google explicaba en un borrador de «Nature», de septiembre´19, cómo su ordenador cuántico había realizado un cálculo más allá del alcance del procesador clásico más avanzado del mundo (tardó 200 segundos en ejecutar una tarea que a la máquina más rápida le habría llevado 10.000 años), aunque IBM rechazó poco después que el hito se hubiese conseguido.

APLICACIONES DE LOS ORDENADORES CUÁNTICOS

Estos ordenadores están orientados, mayormente, al mundo de los cálculos matemáticos, físicos, estadísticos y financieros. Son una de las herramientas más prometedoras en el mundo de la ciencia; sin embargo, es una tecnología que preocupa seriamente al mundo de la criptografía y cifrados de seguridad. La complejidad de los cálculos que realiza esta tecnología podría vulnerar en pocos minutos cualquier sistema de cifrado o encriptado presente en plataformas tradicionales. Por tanto, es una de las tecnologías que cuenta con mayor seguimiento por parte de los diversos gobiernos y de los organismos de seguridad informática.

Una de las aplicaciones más prometedoras de los ordenadores cuánticos será la de simular el comportamiento de la materia hasta el nivel molecular. Fabricantes de coches como Volkswagen y Daimler están usando ordenadores cuánticos para simular la composición química de las baterías de los vehículos eléctricos para encontrar nuevas formas de mejorar su rendimiento. Y las compañías farmacéuticas los están aprovechando para analizar y comparar compuestos que podrían llevar a la creación de nuevos medicamentos.

Estas máquinas también son excelentes para problemas de la optimización, ya que pueden llegar a vastas cantidades de posibles soluciones extremadamente rápido. Airbus, por ejemplo, los está utilizando para calcular las rutas de ascenso y descenso con mayor eficiencia de combustible para los aviones. Y Volkswagen ha presentado un servicio que calcula las rutas óptimas para autobuses y taxis en las ciudades para minimizar los atascos. Estas máquinas podrán usarse para la inteligencia artificial el “machine learning” y, también, se habla de sus posibles usos en temas relacionados con la ciberseguridad: hay algoritmos que pueden romper las claves de encriptación y otros que sirven para buscar en bases de datos, pero estos algoritmos necesitan un número de cúbits muy grandes y ahora mismo se está buscando aplicaciones que sean más compatibles con el estado actual de la computación cuántica.

> Por ejemplo, para algunas aplicaciones, como criptografía, un ordenador clásico puede tardar 1.000 millones de años en romper una clave criptográfica RSA. Un ordenador cuántico podría hacerlo en minutos.

Podrían pasar varios años hasta que los ordenadores cuánticos alcancen su máximo potencial. Las universidades y las empresas que trabajan con ellos se enfrentan a una escasez de investigadores capacitados en este campo, y a la falta de proveedores de algunos componentes clave. Pero si estas nuevas y exóticas máquinas informáticas cumplen con su promesa, podrían transformar industrias enteras e impulsar la innovación global.

CONCLUSIÓN

En las dos últimas décadas, los ordenadores clásicos han experimentado un gran aumento en su potencia y en velocidad de procesamiento. La miniaturización del tamaño de sus componentes ha facilitado el incremento de la densidad de los circuitos electrónicos que los integran. En 1995, Gordon Moore vaticinó que el número de transistores de un microprocesador se multiplicaría por dos cada dos años, una ley, que se ha venido cumpliendo hasta ahora, pero que cuenta con una limitación: cuando el tamaño de los transistores presenta medidas atómicas las leyes fundamentales de la física cambian. Los electrones experimentan comportamientos cuánticos y pueden moverse entre distintas líneas de corriente por el “efecto túnel”.

Esto produce la aparición de fugas que interfieren en el funcionamiento del circuito, pero los principios de la mecánica cuántica, aplicados en la computación auguran una nueva revolución, que ya está comenzando a dar los primeros resultados.

Figura 12. Estructura de un ordenador cuántico.

En un ordenador cuántico se trabaja con conceptos, algoritmos y tecnologías completamente diferentes a los que se usan en un ordenador digital binario. Propiedades de la mecánica cuántica como superposición, entrelazamiento e interferencia se usan en un ordenador cuántico para manejar los estados de los cúbits y recrear las operaciones necesarias para procesar algoritmos.

Figura 13. Detalle de un ordenador cuántico.

Actualmente, un aspecto especialmente relevante en el que se está trabajando es en la corrección de errores. Sin un sistema que sea capaz de corregir errores derivados de la naturaleza de los estados cuánticos, poco se podrá avanzar en este campo.

No obstante, los ordenadores cuánticos aún siguen siendo difíciles de construir, alojar y programar, por lo que no estarán listos para su comercialización masiva en el futuro próximo.

La consultora Deloitte ha formulado las siguientes previsiones en este ámbito:

- Los ordenadores cuánticos no reemplazarán a los ordenadores tradicionales, en al menos las próximas décadas.
- El mercado de los ordenadores cuánticos del futuro tendrá aproximadamente la misma envergadura que el mercado de los superordenadores: alrededor de 50.000 millones de dólares al año.
- Es probable que los primeros ordenadores cuánticos comerciales de uso general aparezcan a finales de la década de 2030.

A pesar de que en el mercado hay varios modelos de ordenadores cuánticos, aún no se ha desarrollado uno que supere las capacidades algorítmicas de los ordenadores clásicos, aunque sí su rapidez. No se ha logrado aquello que los expertos llaman “ventaja cuántica”, es decir hacer las tareas específicas que solo los ordenadores cuánticos pueden realizar.