La Gaceta de Salamanca
Salamanca

03/11/19

Prensa: Diaria
Tirada: 10.757 Ejemplares
Difusión: 8.855 Ejemplares

Cod: 128806385

Página: 31

Sección: OPINIÓN Valor: 4.780,00 € Área (cm2): 1046,5 Ocupación: 100 % Documento: 1/1 Autor: • ÁNGEL MARTÍN DEL REY (*) Núm. Lectores: 87000

• ÁNGEL MARTÍN DEL REY (*)

Computación cuántica

El último avance de Google no ha estado exento de polémica puesto que su gran competidor IBM, ha indicado que más que hablar de "supremacía cuántica" de Google se debería hablar de "ventaja cuántica"

LA manera de trabajar de las máquinas de cálculo (desde la computadora mecánica de Charles Babbage al último modelo del Mac Pro, pasando por la máquina Bombe diseñada por Alan Turing para tratar de descifrar los mensajes alemanes encriptados durante la II Guerra Mundial) es, en esencia, la misma: ejecutan secuencialmente las operaciones en las que el programa divide la tarea que se quiere realizar.

Gracias a esta forma de proceder y a los enormes avances tecnológicos producidos en las últimas décadas, nuestra sociedad ha iniciado un proceso de transformación y desarrollo que conducirá a una dependencia prácticamente total del correcto funcionamiento de los sistemas informáticos. A pesar de todo ello, el principio de funcionamiento de los ordenadores actuales presenta serias limitaciones cuando se pretenden resolver problemas difíciles (básicamente problemas que no son de clase P). Es aquí donde es necesario un cambio en el paradigma tecnológico y en los principios computacionales. El candidato más firme para liderar esta transición es la tecnología cuántica. Ello podría dar lugar a una revolución científico-tecnológica sin precedentes en la historia de la humanidad

Los hipotéticos ordenadores cuánticos resolverían de manera eficiente problemas totalmente inabordables para los ordenadores actuales y abrirían la puerta al desarrollo de herramientas y técnicas computacionales inimaginables. Los resultados experimentales que se están obteniendo en el ámbito de la Computación Cuántica son muy prometedores (uno de ellos, muy reciente, ha sido el anuncio por parte de Google Al Quantum del desarrollo del ordenador cuántico de uso específico Sycamore), y tal vez sería posible disponer de ordenadores cuánticos de propósito general para mediados de este siglo.

La Computación cuántica

Esta es una historia que se inicia en los últimos meses del año 1900 cuando el físico alemán y Premio Nobel Max Planck propuso que la radiación no se emite ni se absorbe de manera continua sino de forma discontinua mediante "cuantos" de energía. Este resultado, junto con las aportaciones inmediatamente posteriores de Albert Einstein, suponen el comienzo de la Teoría Cuántica. El inicio de la Computación Cuántica podemos fecharlo en los primeros años de la década de los 80 con los trabajos de Paul Benioff aunque el hito principal se produce en 1981 cuando otro Premio Nobel de Física, Richard Feynman, durante la impartición de un curso en el CalTech se preguntó si un ordenador podía ser capaz de simular un sistema físico. Como conclusión a su disertación mostró la necesidad de desarrollar ordenadores cuánticos para superar las limitaciones de los ordenadores clásicos y, de esa manera, poder simular de forma eficaz procesos cuánticos. Posteriormente, en 1985, David Deutsch describió la primera computadora cuántica universal capaz de simular cualquier otro computador cuántico. Desde entonces se han venido sucediendo avances constantes en este ámbito: durante la década de los 90 los desarrollos teóricos empiezan a cristalizar en aplicaciones y experimentos apareciendo los primeros algoritmos cuánticos, y ya en el nuevo siglo las grandes empresas tecnológicas en colaboración con el ámbito académico comienzan a desarrollar las primeras máquinas capaces de realizar cálculos cuánticos.

Los fenómenos cuánticos de mayor interés en el ámbito de la computación (y que no tienen equivalentes en el ámbito de la Física clásica) son tanto la superposición de estados como el entrelazamiento cuántico. La superposición de estados establece que un sistema cuántico se puede encontrar simultáneamente en todos los estados posibles de manera que al realizar una medición sobre dicho sistema sólo obtendremos uno de ellos. Por su parte, el entrelazamiento cuántico, predicho por Albert Einstein, Boris Podolsky y Nathan Rosen en 1935, nos dice que en un sistema cuántico formado por muchas componentes la actuación sobre alguna de ellas influye en el estado en el que se encuentran las demás, hecho que se manifiesta de manera instantánea aún estando dichas componentes separadas por grandes distancias.

Computación cuántica versus computación clásica

En la computación actual (computación clásica) los ordenadores realizan los cálculos procesando unidades básicas de información llamadas "bits" (acrónimo en inglés de "binary digit" -dígito binario-). Cada bit contiene uno de dos estados posibles (0 o 1) y la unión de ellos da lugar a otras unidades como el "byte" (8 bits), el "megabyte" (un millón de bytes) o el "terabyte" (un billón de bytes). Los cómputos se realizan empleando operaciones lógicas (AND, OR, NOT, XOR,...) que son fácilmente implementables en hardware gracias a los circuitos electrónicos.

El paradigma cuántico da lugar a un tipo de computación totalmente diferente a la actual. Aunque un posible ordenador cuántico pudiera integrar componentes que desde el punto de vista operativo fueran similares a las empleadas por los actuales (registros, compuertas lógicas, memorias, buses, etc.), desde el punto de vista físico la estructura sería radicalmente distinta. Ello es debido fundamentalmente a los fenómenos de la superposición de estados (que afecta a la gestión de los registros cuánticos) y del entrelazamiento cuántico (que influye en la forma de operar de los circuitos cuánticos).

En la computación clásica, en cada byte sólo podemos representar 2^8=256 estados (todas las posibles combinaciones de ceros y unos en ocho posiciones) y si queremos cambiar el estado de, por ejemplo, 4 bits hemos de realizar al menos 4 operaciones sobre ellos. En el paradigma cuántico, y gracias a la superposición de estados, un byte cuántico (8 cúbits o bits cuánticos) podría encontrarse en más de 2^8 estados. Por otra parte, y como consecuencia del entrelazamiento cuántico, una única operación sobre uno de los ocho cúbits podría afectar al resto; es decir, con una única operación se podrían calcular varios valores al mismo tiempo. De esta manera el principio de ejecución secuencial de operaciones (una tras otra) que rige en la computación clásica sería sustituido por la ejecución instantánea de múltiples operaciones (una transformación sobre n cúbits daría lugar a 2^n operaciones al mismo tiempo).

Ahora bien, el manejo de los cúbits plantea uno de los problemas fundamentales en la Computación Cuántica: un cúbit se puede encontrar no sólo en el estado 0 o 1 sino en una superposición de ambos pero cuando tratamos de medirlo no se obtiene toda la información sino uno de esos estados. Consecuentemente es posible realizar infinidad de operaciones al mismo tiempo pero no es posible obtener los resultados de todas ellas.

Implicaciones de la computación cuántica

La computación cuántica supondrá una revolución en muchas disciplinas científicas. Por ejemplo, el algoritmo del temple cuántico (1989) tiene extraordinarias aplicaciones tanto en Inteligencia Artificial, en Visión por Computador como en Bioinformática; de hecho, el quantum machine learning y sus aplicaciones en Medicina, Biología o Química es una de las líneas de investigación más prometedoras en la actualidad. Por otro lado, el algoritmo cuántico de Shor (1994) permite factorizar números enormes en muy poco tiempo comprometiendo totalmente la seguridad del criptosistema RSA (que se encuentra implementado en el DNI electrónico).

El último gran avance

Teniendo en cuenta las grandes expectativas depositadas en la Computación Cuántica, grandes compañías tecnológicas se han embarcado desde finales del siglo XX en la investigación y desarrollo en este ámbito. En 1998 IBM presenta la primera máquina cuántica de cálculo que disponía de sólo 2 cúbits y de uso específico para la resolución del problema de Deutsch-Jozsa. La propia IBM en colaboración con la Universidad de Stanford ejecutan en 2001 por primera vez el algoritmo de Shor en una máquina constituida por 7 cúbits. En 2007 la empresa D-Wave presenta la primera máquina cuántica de 16 cúbits capaz de ejecutar el protocolo temple cuántico, siendo mejorada apenas 4 años después con el ordenador de uso específico D-Wave One formado por 128 cúbits. Muy recientemente, a principios del año en curso, IBM ha puesto a disposición de la comunidad científica el ordenador cuántico Q System One de 20 cúbits.

El último avance en este ámbito se ha producido apenas un par de semanas atrás cuando el equipo de John M. Martinis (Google Al Quantum) anunció en la revista Nature el desarrollo de una nueva máquina cuántica de 53 cúbits para la implementación específica de un algoritmo de generación de secuencias de números aleatorios, lo cual demostraría la supremacía cuántica de este logro de Google. El concepto de supremacía cuántica fue re-introducido por John Preskill en 2012 y hace referencia a la capacidad que tiene un ordenador cuántico para realizar un cómputo imposible de llevarse a cabo con una computadora tradicional. En este sentido Google afirma que su ordenador ha realizado el cálculo requerido en 200 segundos mientras que el superordenador Summit del Laboratorio Nacional de Oak Ridge tardaría 10.000 años en realizar el mismo cálculo.

Este anuncio no ha estado exento de polémica puesto que el gran competidor de Google, IBM, se ha apresurado a indicar que más que hablar de "supremacía cuántica" de Google se debería hablar de "ventaja cuántica" ya que afirma que en realidad el cálculo realizado se podría reducir a unas 60 horas en el superordenador Summit si se aprovecharan sus 250 petabytes de disco duro.

Sea como fuere, y a la espera de nuevos análisis, es razonable afirmar que el logro de Google es sin duda un hito en la Computación Cuántica. Pero no es más que un pequeño paso ya que todavía será necesario invertir ingentes cantidades de dinero y de horas de investigación y desarrollo para que el primer ordenador cuántico genérico (capaz de poder implementar cualquier algoritmo) vea la luz. Tal vez en 20 o 30 años sea una realidad...

** Profesor del departamento de Matemática Aplicada de la Universidad de Salamanca*