Información cuántica

Posted on 1 de marzo de 2002 by José Ignacio Latorre

Construir un ordenador cuántico es un reto difícil de resistir para un espíritu científico. Su lógica de cálculo permitiría descomponer un número en sus factores primos en un tiempo exponencialmente menor que los ordenadores basados en lógica clásica. Todos los mensajes encriptados que circulan por Internet, incluyendo datos bancarios y secretos del Pentágono, quedarían desprotegidos. Un ordenador cuántico también podría organizar una base de datos y recuperar una de sus entradas en un tiempo muy inferior al que precisan los ordenadores actuales. Desde un punto de vista conceptual más elevado, la lógica cuántica redefine las clases de complejidad computacional y abre un área de investigación de aplicaciones prácticas insospechadas. Una profunda revolución nos espera, pero no con tanta urgencia como para no poder revisar sus orígenes.

Uno de los descubrimientos científicos más importantes y de consecuencias más profundas del siglo XX ha sido la formulación de la mecánica cuántica. Nuestra comprensión de los fundamentos de esta disciplina y el análisis de sus posibles aplicaciones han sido constantemente investigados desde su aparición, de forma que la mecánica cuántica ha ido generando nuevas y vastas ramas de la ciencia y la tecnología. Cada tesis doctoral dirigida por Niels Bohr en Copenhague entre los años 1920 y 1930 dio lugar a una disciplina independiente de la Física, como son por ejemplo la física molecular, la física atómica, la física nuclear, las partículas elementales o el estado sólido. Más tarde, las ramificaciones de la mecánica cuántica dieron lugar a la óptica cuántica o a la mecánica estadística cuántica, e incluso forman la base de la especulación teórica que intenta comprender el origen del universo, la gravitación cuántica. Otras disciplinas como la Química, la Medicina (scaner, resonancia nuclear magnética, láser), la biología molecular (determinación de estructuras espaciales como la del ADN) o las comunicaciones (láseres, fibras ópticas) han alcanzado un grado de desarrollo muy elevado gracias a la aplicación de avances cuánticos.

Desde un punto de vista tecnológico, el impacto de la revolución cuántica es impresionante. Se calcula que alrededor del 50% del producto nacional bruto americano está asociado en forma directa o indirecta a la mecánica cuántica, con especial énfasis en el campo de los ordenadores (basados en semiconductores cuánticos de silicio). Otras disciplinas han ideado técnicas derivadas de los conocimientos sobre la estructura cuántica de los átomos. Por ejemplo, se utilizan los rayos X para estudiar subcapas de pinturas, el carbono 14 para datar restos arqueológicos o los relojes cuánticos para marcar la hora oficial de toda la Tierra y fijar nuestra posición sobre su superficie mediante el sistema de posicionamiento global GPS. En

pocos años la calidad de visión de muchos miopes e hipermétropes ha mejorado gracias a la corrección de sus córneas por medio de cirugía refractaria por láser LASIK. De hecho, el número de láseres en el mundo se cifra en miles de millones, hallándose principalmente en equipos de música (CD) y, en el futuro, en los DVD. Sin embargo, es en el cambio de siglo cuando la mecánica cuántica está llegando a su madurez y, como un buen vino o un gran compositor, nos depara una inesperada joya intelectual: el nacimiento de la información cuántica.

Esta vigorosa y reciente línea de investigación se basa tanto en la formulación de la mecánica cuántica como en la teoría clásica de la Información. Ambas disciplinas arrancan en la primera mitad del siglo y tienen una profunda relación a veces olvidada. Los trabajos de Church, Post y Turing en los años treinta establecieron una definición operativa de computabilidad en términos de máquinas de Turing. Así pues, calculable implica calculable en una máquina de Turing en el paradigma computacional clásico. El concepto de computabilidad queda ligado a una reducción de algoritmos lógicos a procesos mecánicos que, ejecutados en una máquina de Turing, se rigen por las leyes de la física clásica. Esta observación es relevante para comprender las nuevas ideas asociadas a la posibilidad de aprovechar la mecánica cuántica para construir ordenadores capaces de realizar cálculos en forma eficiente. Una forma directa de formular la apuesta cuántica es la siguiente: las clases de complejidad computacional deben su esencia y sus relaciones (aún no completamente establecidas) a las leyes de Newton que subyacen a la forma en que se realizan los cálculos. La mecánica cuántica cambia estos fundamentos básicos de la ciencia de la computación porque sustituye el sustrato físico que define el concepto de computabilidad. Nos enfrentamos a un cambio de paradigma computacional. Entramos en la computación cuántica.

La computación cuántica se inscribe en el amplio marco de la información cuántica. Este término intenta aunar todas las nuevas ideas basadas en el empleo de los propios postulados de la mecánica cuántica para codificar, tratar y transmitir información. Los bits dan paso a los qubits (quantum bits), las puertas lógicas pasan a ser evoluciones cuánticas reversibles del sistema y los canales de transmisión han de preservar las correlaciones cuánticas de la información transmitida. Si bien el término de ordenador cuántico ha sido considerado por los medios de comunicación como símbolo inequívoco del sorprendente futuro que nos espera, la información cuántica ha obtenido avances notables en líneas de investigación con objetivos muy diferentes. En especial, los dos logros realmente excepcionales en este incipiente mundo de la información cuántica corresponden a la encriptación cuántica y la teleportación. Vale la pena detenerse y analizar estas ideas antes de volver a la computación cuántica.

Una inesperada aplicación de la mecánica cuántica está desarrollándose en el campo de la criptografía. La comunicación secreta de datos es una necesidad en el mundo de las finanzas y de la empresa. Las operaciones que realiza un cliente con su banco a través de Internet precisan de un protocolo que encripte su identificación y el contenido del mensaje. También deben ser codificadas las transacciones entre bancos, los datos confidenciales que fluyen dentro de la red de una empresa o cualquier otro informe que se desee secreto. El método que hoy en día se considera más seguro a la hora de codificar en forma secreta cualquier tipo de información es el llamado protocolo RSA. Este método se basa en una original aplicación de la teoría de números. La idea consiste en utilizar la descomposición de números primos muy grandes (con centenares de dígitos) como base para establecer una clave. Cualquier espía puede, en principio, descodificarla, pero el tiempo necesario para hacerlo con los ordenadores actuales es elevadísimo (mayor que la edad del universo), porque la factorización de un número en sus factores primos requiere un tiempo que crece exponencialmente con el tamaño del número.

El protocolo RSA es, pues, muy seguro. No existen hoy en día atisbos de lograr ordenadores clásicos tan rápidos que hagan peligrar el secreto de las transacciones que se están realizando. Sin embargo, es a priori posible hallar un algoritmo potentísimo que factorice números primos o considerar la construcción de un nuevo tipo de ordenadores (¡cuánticos!) mucho más rápidos que los actuales. La solución definitiva a estas objeciones consiste en sustituir el protocolo RSA por otro, a ser posible, inviolable. Este sustituto viene de la mano de la criptografía cuántica.

La idea básica que sustenta la criptografía cuántica consiste en el hecho aparentemente remoto de que toda observación de un estado cuántico afecta al estado medido. Es imposible conocer un estado cuántico arbitrario sin afectarlo. Para entender este hecho imaginemos que hemos aparcado nuestro coche en la calle. Lo contemplamos con admiración, es nuevo. Pensemos por un momento cómo hemos sabido que nuestro coche está precisamente ahí, parado delante de nosotros. En el fondo, lo que ha sucedido es que fotones procedentes, por ejemplo, del sol han rebotado en la chapa del coche y han llegado a nuestros ojos. Nuestra retina ha procesado el cambio energético producido por la absorción de los fotones y envía una señal al cerebro que a su vez desata la consiguiente reacción de placer. Lo importante para nuestra discusión es que la información que hemos obtenido se debe a una colisión de fotones con el coche.

En el mundo subatómico las cosas no son tan idílicas. Si en lugar de un coche tenemos un electrón, y un fotón muy energético incide sobre él, se produce una catástrofe: el fotón lanza al electrón a un lugar desconocido. Podemos saber dónde estaba el electrón, pero éste ha dejado de estar quieto. Sin mediar una nueva observación perderemos inmediatamente la

pista del electrón. Ya no sabemos dónde encontrarlo. El propio proceso de medida afecta al sistema medido. En el mundo macroscópico este hecho no es relevante porque la influencia del proceso de medida es menospreciable. En el mundo cuántico, en cambio, el proceso de medida es esencial.

La mecánica cuántica que limita nuestro conocimiento del mundo permite una aplicación sorprendente. Podemos codificar información secreta en estados cuánticos. Si un espía interfiere nuestro mensaje y lo intenta leer, el mensaje quedará modificado. Está desarrollándose un prototipo comercial de criptografía cuántica entre Ginebra y Nyon. Los mensajes se codifican en polarizaciones de fotones que se transmiten por fibras ópticas.

Una parte de los fotones se reservan para verificar la ausencia de espías. Los demás codifican la señal.

La criptografía cuántica es inviolable en tanto que las leyes de la mecánica cuántica sean ciertas.

Un segundo desarrollo realmente sorprendente de la mecánica cuántica cuya base teórica se ha descubierto recientemente es la teleportación cuántica. Una famosa película de ciencia ficción presentaba una máquina capaz de destruir cualquier objeto o persona en un lugar y hacerlo reaparecer en otro lugar, de ahí la palabra teleportación. Lo insólito de la idea es que la mecánica cuántica ofrece la posibilidad real de teletransportar estados cuánticos.

La forma de proceder consiste en obtener estados cuánticos llamados embrollados o entrelazados. Estos estados pueden estar compuestos por varias partículas que mantienen sus correlaciones cuánticas aun estando muy separados. El protocolo de teleportación se inicia haciendo una medida conjunta del estado que deseamos teleportar y una de las partes del estado entrelazado. Esta medida destruye el estado inicial. A continuación, enviamos de forma clásica el resultado de la medida a otro lugar donde se halla la segunda parte del estado entrelazado. La información recibida permite actuar sobre esta segunda parte del estado entrelazado y reconstruir el estado inicial.

Los primeros intentos de llevar a la práctica estas ideas han resultado muy esperanzadores. Hoy en día se han teleportado ciertos estados de fotones. Será necesaria mucha más investigación para lograr teleportar electrones o estructuras más complejas. Si algún día se consigue, podremos transportar objetos a la velocidad de la luz, ya que los estados entrelazados pueden prepararse con antelación y la señal clásica puede ser enviada con fotones. Star Trek ya no es pura ciencia ficción.

Pero será, sin duda, la investigación en los futuros ordenadores cuánticos la que recibirá más financiación y de la que se esperan aplicaciones más revolucionarias. Los ordenadores actuales, basados en chips de silicio, han logrado una miniaturización impresionante de sus circuitos. Sin embargo, esta reducción de tamaño está llegando a su límite. Hoy en día la conducción de electrones en un chip se hace por hilos de unos pocos miles de átomos. Si el tamaño de estos hilos se reduce empezarán a aparecer fenómenos cuánticos. El ordenador dejará de comportarse en forma determinista.

Un ordenador cuántico se basa en una filosofía totalmente diferente. Los estados cuánticos de un sistema físico se utilizan como bits cuánticos, o qubits. A diferencia de los bits clásicos, que corresponden a una unidad de información que puede tomar valores 0 ó 1, un estado cuántico puede corresponder a una superposición de los estados base 0 y 1. La lógica cuántica es, pues, necesariamente diferente de la clásica. Las operaciones lógicas que se realizan sobre qubits deben ser realizadas mediante puertas lógicas cuánticas. Puesto que un conjunto de qubits pueden estar en una suma coherente de estados cuánticos base, las operaciones que se realicen sobre estas superposiciones actúan en forma paralela sobre cada estado base. Un ordenador cuántico sería un ordenador que actuaría sobre estructuras microscópicas que aceptarían superposiciones de estados. El resultado global proporcionaría una inmensa ganancia de potencia. Tanto es así que ya ha sido demostrado que un ordenador cuántico permitiría descomponer un número en sus factores primos en un tiempo exponencialmente menor que un ordenador clásico. La criptografía RSA se volvería obsoleta.

Experimentalmente se ha logrado construir estados cuánticos controlados de unos pocos qubits. También se han obtenido puertas lógicas cuánticas en diferentes sistemas físicos. El colosal problema experimental que afronta la comunidad cuántica es el de mantener las propiedades cuánticas que relacionan a los qubits. Los estados cuánticos son, de hecho, muy frágiles y cualquier influencia externa destruye lo que se denomina coherencia. Esta pérdida de coherencia es muy sensible al tipo de implementación de ordenador cuántico que se intente. A pesar de que los logros más recientes en computación cuántica se han realizado en trampas de iones, es previsible que el verdadero avance tecnológico venga de las implementaciones de estas ideas en el campo del estado sólido.

La encriptación cuántica, la teleportación cuántica y los ordenadores cuánticos serán temas de investigación dominantes a comienzos del siglo XXI. Pero es de sabios aceptar que las mejores aplicaciones de la mecánica cuántica nos son todavía completamente desconocidas. Podemos especular que el control que hoy en día se está logrando sobre los condensados de Bose-Einstein llevará a la construcción de láseres atómicos (haces de materia coherente) de aplicaciones imprevisibles. Tal vez serán los puntos cuánticos (potenciales que pueden retener hasta un único electrón ligado) una fuente de manipulación de qubits. O triunfará el

campo de la mecánica cuántica mesoscópica, donde grandes moléculas podrían presentar efectos genuinamente cuánticos o constituir la base de memorias de ordenador del tamaño de una punta de alfiler. No existe sistema físico que escape al escrutinio de sus posibles propiedades cuánticas. Se piensa en corrientes superconductoras que se hallan en un estado superposición de girar a izquierda y derecha, en moléculas de carbón 60 capaces de encarcelar nitrógeno y manipular a voluntad el spin de su núcleo, se construyen fotones en estados de varios momentos angulares utilizando hologramas y óptica paraxial. Los pobres evaluadores científicos de la Unión Europea padecen una fiebre de propuestas inverosímiles, pero de financiación asequible, que requiere el establecimiento de directrices políticas claras.

Será el sexto programa marco el momento en el que Europa fijará sus prioridades científicas y donde se espera un fortísimo impulso a la información cuántica, al menos comparable al norteamericano. Permítanme no comentar el caso español y así eludir una momentánea depresión. En cualquier caso, les garantizo que será un privilegio presenciar la llegada a la madurez de la mecánica cuántica.