·Juan José García Ripoll.
·J. Ignacio Cirac.
Instituto Max-Planck de Óptica Cuántica, Garching (Alemania)

TECNOLOGÍA DE LA INFORMACIÓN CUÁNTICA

LA ÚLTIMA FRONTERA DE LA INFORMÁTICA

Los expertos pronostican que a partir de 2020 será imposible miniaturizar aún más los ordenadores fabricados con la tecnología actual. Vendrán entonces las nuevas generaciones de chips: primero serán los moleculares, posteriormente los de tamaño atómico, y finalmente los cuánticos, los más revolucionarios y sorprendentes, la verdadera última frontera de la computación.

El año en el que nos encontramos es ciertamente el Año Mundial de la Física, pero también es un año más en la denominada "Era de la Información", en el que la oferta y la demanda de datos, sean éstos páginas Web, música, noticias, videos, etc... están llevando al límite los recursos tecnológicos de que disponemos, tanto a nivel de almacenamiento masivo, como de procesamiento y comunicación.

Por poner un ejemplo, en el caso de los ordenadores la tendencia general consiste en miniaturizar los circuitos electrónicos, de forma que no sólo tengamos mas elementos de computación en cada microchip, sino que además los electrones, portadores de la información, se puedan mover más rápidamente entre ellos. El problema es que, dado el ritmo de miniaturización actual, muy pronto nos encontraremos con circuitos en los que los transistores, compuestos de muy pocos átomos, dejarán de funcionar como tales. Es el "límite cuántico", una frontera infranqueable, en la que electrones y átomos se comportan a la vez como ondas y como partículas y pueden, por ejemplo, saltar de un elemento conductor a otro *(Fig. 1)*. ⇨

¬ **Figura 1**: Para un electrón, los conductores de un microchip son pozos de potencial en los que se mueven libremente. Cuando los circuitos integrados se hacen demasiado pequeños, las reglas de la Mecánica Cuántica permiten a los electrones pueden atravesar las separaciones aislantes entre conductores.

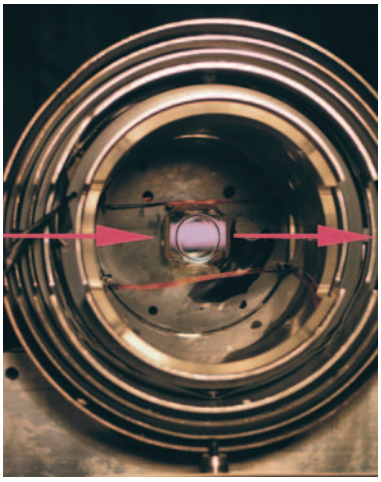
Juan José García Ripoll / J. Ignacio Cirac
Instituto Max-Planck de Óptica Cuántica, Garching (Alemania)

Algo de esta dualidad onda-corpúsculo encontramos ya en el artículo de Einstein de 1905 dedicado al efecto fotoeléctrico, y que forma parte de los cimientos de la Mecánica Cuántica. Más tarde Einstein se ocuparía también de esa teoría, aparentemente aleatoria y que él consideraba incompleta, en otro artículo, no por incorrecto menos memorable, conocido como la "paradoja de Einstein-Podolksi-Rosen". Pese a las objeciones de Einstein y muchos otros científicos, la Mecánica Cuántica se ha seguido desarrollando hasta nuestros días, permitiéndonos explicar con satisfacción el mundo de lo muy pequeño, desde el átomo de hidrógeno hasta los superconductores, y en los últimos años sugiriendo incluso una solución alternativa al problema de la información.

Hablamos de la Teoría de la Información Cuántica (I.C.), un campo de investigación relativamente joven, que propone emplear sistemas cuánticos para almacenar y procesar información de manera más eficiente que por medios clásicos. La idea básica es muy sencilla y utiliza el principio de superposición de la Mecánica Cuántica: un sistema físico (electrón, fotón, átomo...) puede encontrarse en una superposición de dos o más estados medibles. Por ejemplo, los electrones tienen un momento angular intrínseco, el espín, que dada una dirección puede estar "apuntando hacia arriba", o "hacia abajo". Pero un electrón también puede, por ejemplo, encontrarse en un estado intermedio con el 50% de probabilidad de cada sentido, y denotado por:

$$\frac{1}{\sqrt{2}}|\uparrow\rangle+\frac{1}{\sqrt{2}}|\downarrow\rangle$$

Cualitativamente, a pesar de ser nuestra partícula un sistema aparentemente biestable (los dos valores del espín), podemos usar superposiciones para almacenar más información que en el sistema binario {0,1} de los dipositivos digitales clásicos. Sin embargo, hay dos diferencias fundamentales entre un bit cuántico o qubit y la información clásica. La primera es que, hasta que no medimos el estado del electrón, éste permanece indeterminado. Ahora bien, una vez realizamos la medida, el electrón estará siempre en uno de los dos estados posibles. La segunda diferencia es que para caracterizar completamente el estado de un qubit, esto es, para conocer las probabilidades de que el espín tenga un valor u otro, debemos hacer muchas medidas sobre sistemas idénticos.



¬ **Figura 2**: Una celda de vidrio empleada en los experimentos de entrelazado y memoria cuántica en el instituto Niels Bohr, Copenhague (http://quantop.nbi.dk/). Cada celda contiene vapor de cesio y está en un cilindro metálico para evitar la influencia de campos magnéticos externos. La luz sigue el camino marcado en rojo y transmite su información a los átomos. (Cortesía de E. Polzik)

La imparable demanda de información está llevando al límite los recursos tecnológicos disponibles.

Precisamente la imposibilidad de determinar completamente un sistema cuántico arbitrario con una única medida, junto a la imposibilidad de realizar copias idénticas, constituyen los pilares de la Criptografía Cuántica, la primera rama de la I.C. con aplicaciones tecnológicas.

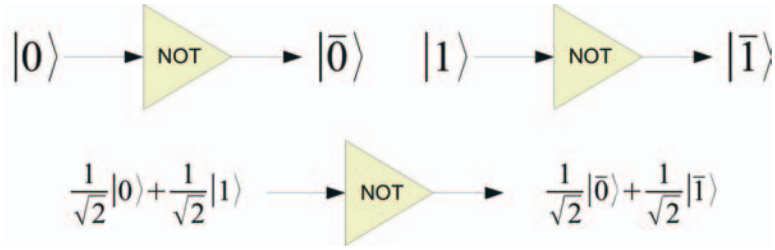
Un tercer concepto fundamental es el "entanglement" , que aquí traduciremos como "entrelazado", y que consiste en la existencia de fuertes correlaciones entre los componentes de un sistema cuántico. Tomemos por ejemplo:

$$\frac{1}{\sqrt{2}}|\uparrow,\uparrow\rangle+\frac{1}{\sqrt{2}}|\downarrow,\downarrow\rangle$$

La ecuación anterior nos describe el estado de una pareja de electrones. Si medimos el espín de un electrón, encontraremos los valores "arriba" o "abajo" con igual probabilidad. Ahora bien, siempre sabremos que el otro electrón se encuentra en el mismo estado, incluso sin medirlo. Lo que podemos hacer ahora es repartir estas dos partículas entre dos puntos alejados, p.ej. Madrid y Barcelona, y emplear estas correlaciones para transmitir información de forma segura. La seguridad en este tipo de comunicación o Criptografía Cuántica viene dada por las leyes de la Física: un observador externo no puede influir la comunicación sin ser detectado, esto es, sin destruir el estado cuántico correlacionado. ⇨

La Teoría de la Información Cuántica es un campo de investigación a caballo entre la Matemática Aplicada y la Física Matemática, que se estudia cómo almacenar, procesar y distribuir información empleando las leyes de la Mecánica Cuántica. De una forma abstracta, se encuentran respuestas a preguntas como, "¿Cuánta información clásica (= binaria) se puede almacenar en un qubit?" "¿Cómo caracterizar y utilizar los estados entrelazados?" "¿Cómo corregir los errores que se producen al manipular la información con un sistema físico determinado?"... Cuestiones similares que ya se han resuelto en el desarrollo de la informática clásica.

Aparte de estos problemas fundamentales, quizás uno de los retos más interesantes sea diseñar dispositivos para el procesamiento de la I.C. Nos referimos, por ejemplo, a memorias, canales de comunicación, o incluso el equivalente de los computadores actuales. La primera pregunta que uno se hace al abordar semejante problema es qué sistemas físicos son aptos para almacenar, transmitir y procesar información cuántica. Desgraciadamente no existe una única respuesta. Por un lado, los fotones o partículas de luz se pueden emplear como qubits y transmitir a largas distancias sin errores y son el sistema ideal para comunicaciones cuánticas. Así, como mencionábamos anteriormente, las primeras aplicaciones comerciales de I.C. son sitemas criptográficos que, bien a través del aire libre o por medio de fibras ópticas, emplean luz coherente para transmitir información de manera segura.



¬ **Figura 3**: Una puerta cuántica puede operar sobre superposiciones de dos valores distintos y proporcionar ambos resultados a la vez.

Por el contrario, si lo que deseamos es almacenar y manipular la información, es posible que los átomos sean los mejores candidatos para nuestro diseño. Los átomos, al contrario que los fotones, son capaces de interaccionar entre sí, se pueden atrapar y, bajo condiciones adecuadas de aislamiento, pueden preservar su estado cuántico durante años. Todas estas propiedades los convierten en elementos ideales para memorias y computadores cuánticos.

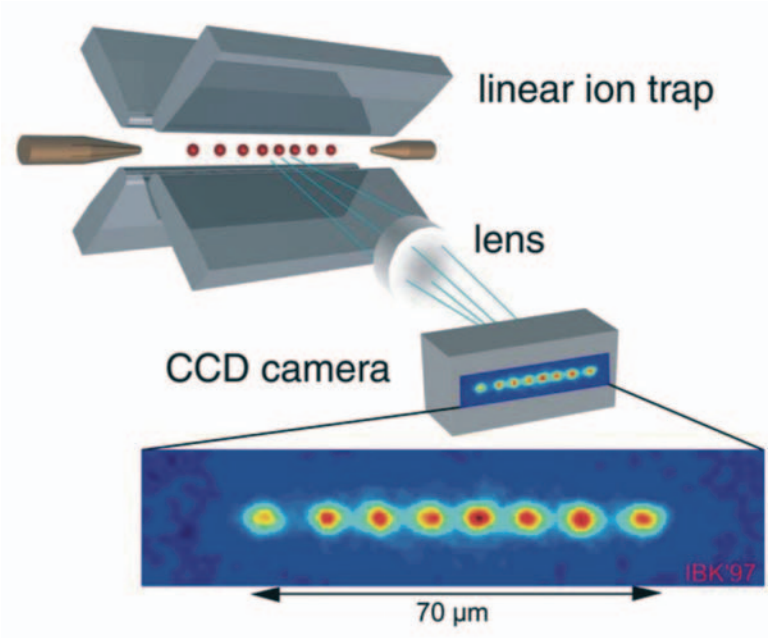
A modo de ejemplo, en la figura 2 vemos el montaje experimental empleado por el grupo del Prof. Polzik (Instituto Niels Bohr, Copenhague, Dinamarca) para crear una memoria cuántica. En este diseño, la información almacenada en la polarización de los fotones se transmite a todo una nube de átomos de cesio encerrados en celdas de cristal. Este proceso es reversible y por medio de múltiples haces de luz láser podemos leer, borrar y reescribir el estado de los átomos tantas veces como queramos. Resulta interesante pensar que, cualitativamente hablando, cada una de las celdas de vapor se comporta a todos los efectos como un qubit. Las leyes de la Mecánica Cuántica se manifiestan por tanto no sólo a nivel microscópico, sino tambien a nivel mesoscópico. Nada nos impide, por ejemplo, crear estados entrelazados entre dos o más celdas de vapor, ¡cada una con cientos de miles de átomos!

Sin embargo, la propuesta más arriesgada y también la que más atención atrae sobre I.C. es la posibilidad de crear ordenadores más potentes que los actuales. Tan potentes que serían capaces incluso de desencriptar códigos como los que empleados habitualmente en las transacciones bancarias o al comprar por Internet.

La idea principal es el paralelismo inherente a la Mecánica Cuántica. Para entenderlo volvamos a nuestro amigo el electrón y supongamos que identificamos los estados de espín arriba y abajo con el 0 y el 1 de un ordenador. Supongamos además que, como muestra la figura 3, tenemos una puerta lógica que realiza la operación NOT sobre este bit, esto es, invierte su valor. En un ordenador clásico, si queremos calcular esta operación ⇨

En los últimos años han surgido soluciones alternativas al problema de la información: hablamos de la Teoría de la Información Cuántica.

Juan José García Ripoll / J. Ignacio Cirac
Instituto Max-Planck de Óptica Cuántica, Garching (Alemania)



¬ **Figura 4**: Una trampa de Paul con ocho iones (Cortesía de R. Blatt, Universidad Innsbruck, Austria)

sobre el 0 y el 1 tenemos que hacerlo secuencialmente: primero introducir el 0 y luego el 1. En cambio, si la puerta lógica actua de acuerdo a las reglas de la Mecánica Cuántica podemos introducir una superposición de ambos valores: ¡La puerta calculará los dos resultados NOT(0) y NOT(1) a la vez!

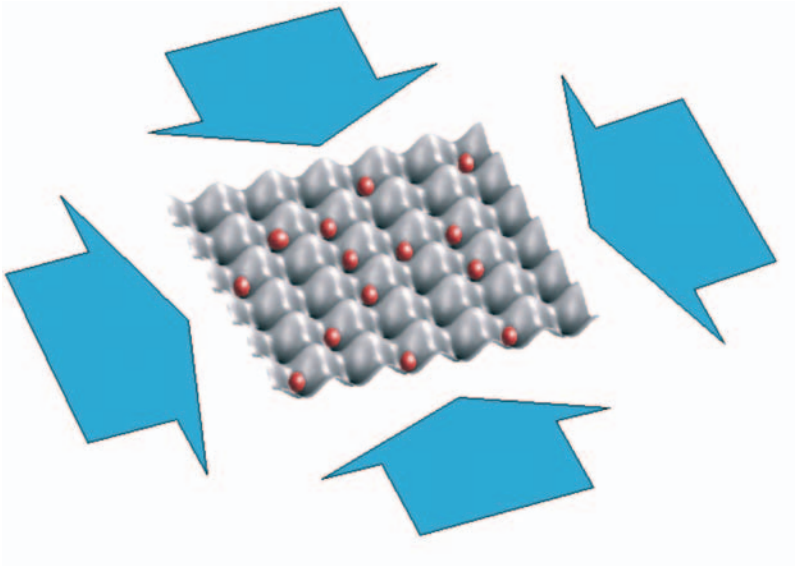
Naturalmente, no es oro todo lo que reluce y, recordando lo que decíamos anteriormente, para recuperar los dos resultados habrá que hacer por lo menos dos medidas. Sin embargo, existen ciertos algoritmos para los cuales este tipo de operación en paralelo produce una ganancia exponencial en tiempo y recursos computacionales. Algunos de estos algoritmos, como la factorización de números enteros, bastarían para romper todos los códigos de criptografía clásica conocidos.

Existen numerosas y muy diferentes ideas sobre cómo implementar un computador cuántico universal. Éntre los sistemas propuestos encontramos fotones y óptica lineal, superconductores, impurezas y defectos en semiconductores, átomos neutros atrapados con láseres, iones atrapados con trampas electromagnéticas, resonancia magnética nuclear con macromoléculas (R.M.N.),... De todos los candidatos, la R.M.N. y los iones atrapados son los dos sistemas más avanzados experimentalmente, si bien parece que sólo los diseños basados en iones son lo bastante escalables como para considerar aplicaciones realistas.

Como muestra la figura 4, un computador cuántico basado en iones consiste esencialmente en una distribución de átomos cargados (p.ej. berilio, calcio, etc), confinados por medio de una matriz de campos electromagnéticos oscilantes. Cada ión tiene dos o más estados internos con una vida media extremadamente larga (segundos en el peor de los casos, años en otros), que podemos denotar como "arriba" y "abajo", ó "0" y "1". Utilizando una técnica conocida como enfriamiento "side-band", es posible dejar a los iones casi en reposo –tanto como lo permiten las leyes de la Mecánica Cuántica–. Gracias a ésto y a que la repulsión electrostática mantiene a los átomos bastante separados, podemos leer y escribir en cada uno de ellos al menos un qubit de información cuántica, que se guarda en el estado interno del átomo. Sin embargo, para realizar computaciones cuánticas hace falta algo más: necesitamos poder crear estados entrelazados de dos o más átomos. Ésto se consigue manipulando las interacciones entre iones mediante láseres y campos magnéticos.

Todos los elementos necesarios para la computación cuántica con iones, esto es, el atrapamiento y enfriamiento, la lectura y la escritura de los iones, así como el control de las interacciones, han sido realizados experimentalmente en los grupos de D. Wineland (NIST, Boulder, USA) y R. Blatt (Univ. de Innsbruck, Austria). Sin embargo, los experimentos actuales son muy aparatosos y se ven limitados a un número pequeño de átomos y de ⇨

La Teoría de la Información Cuántica permite crear ordenadores de tal potencia que serían capaces de desencriptar códigos como los que actualmente se utilizan en las transacciones bancarias por Internet.



¬ **Figura 5**: En una red óptica, haces de luz coherente crean una onda estacionaria que confina átomos individuales en los mínimos de intensidad.

operaciones. El siguiente reto es principalmente tecnológico y consiste en desarrollar trampas microfabricadas, capaces de acoger muchos más iones y de trabajar en paralelo para incrementar el poder de computación.

Por decirlo de otra forma, nos encontramos en la actualidad a un nivel comparable a cuando Shockley, Bardeen y Brattain desarrollaron el primer transistor, mientras que nuestro objetivo es construir algo comparable a las calculadoras actuales, compuestas de miles de transistores. Hay pues un largo camino por recorrer, pero entre medias hay tambien objetivos más modestos y aplicaciones interesantes aún por descubrir, a la vez que se está avanzando a pasos agigantados en el control de los sistemas cuánticos, llámense éstos fotones, electrones o átomos.

Precisamente una de esas aplicaciones interesantes es el desarrollo de un "simulador cuántico". Anteriormente mencionamos que algunos problemas se resolverían más fácilmente en un computador cuántico. Uno de esos problemas consiste en simular otros sistemas cuánticos. Se trata, además, de un tema importante: hay muchos problemas físicos, como el doblado de proteínas, la superconductividad de alta temperatura o los sistemas aleatorios, que involucran modelos matemáticos extremadamente complicados, intratables con las técnicas analíticas o recursos computacionales existentes. Sin embargo sería relativamente fácil, de tener un ordenador cuántico, obtener información sobre el estado fundamental y las propiedades de estos sistemas. Para simular muchos de estos problemas físicos no necesitamos los requerimientos de precisión y control exigidos por un computador cuántico universal. En muchos casos nos basta con unas decenas de átomos y una serie de trampas electromagnéticas y láseres para controlar sus interacciones.

Un ejemplo paradigmático de simulación cuántica lo encontramos en las redes ópticas. Se trata de un conjunto de haces láser que dan lugar a una onda estacionaria de luz, atrapando átomos neutros en los máximos o mínimos de intensidad. Como la figura 5 muestra, el efecto es similar a un "cartón de huevos", donde cada hueco contiene muy pocos átomos. Gracias a que el espaciado entre celdas es muy pequeño (700 nanómetros), las leyes de la Mecánica Cuántica permiten a los átomos saltar de un sitio a otro, de forma similar a como los electrones se mueven en algunos sólidos. De hecho, colocando el tipo preciso y la cantidad adecuada de átomos en la red, será posible simular desde materiales magnéticos hasta superconductores. Experimentalmente, el desarrollo de las redes ópticas está muy avanzado, siendo liderado por los grupos de I. Bloch (Mainz, Alemania), T. Esslinger (Zurich, Suiza) y R. Grimm (Innsbruck, Austria), y habiéndose simulado ya algunos problemas sencillos con Hamiltonianos de Hubbard bosónicos y fermiónicos.

Si bien en este breve artículo hemos hecho énfasis en conceptos muy básicos y en algunos avances experimentales, la Teoría de la Información Cuántica es un campo que genera y precisa importantes desarrollos teóricos. En el grupo de Física Teórica en Garching, por ejemplo, aparte de los temas ya mencionados, hay gente que trabaja en caracterización del "entrelazado" y en cómo aparece en numerosos sistemas de materia condensada; en aplicar las ideas de T.I.C. al desarrollo de nuevos algoritmos numéricos para simular sistemas cuánticos; en el diseño de computadores cuánticos basados en dispositivos de estado sólido; en simuladores cuánticos con iones atrapados... En definitiva, en todo un rango de temas interdisciplinares que surgen de la imbricación entre la T.I.C., la Materia Condensada y la Óptica Cuántica. ■