Computación mecánico-cuántica

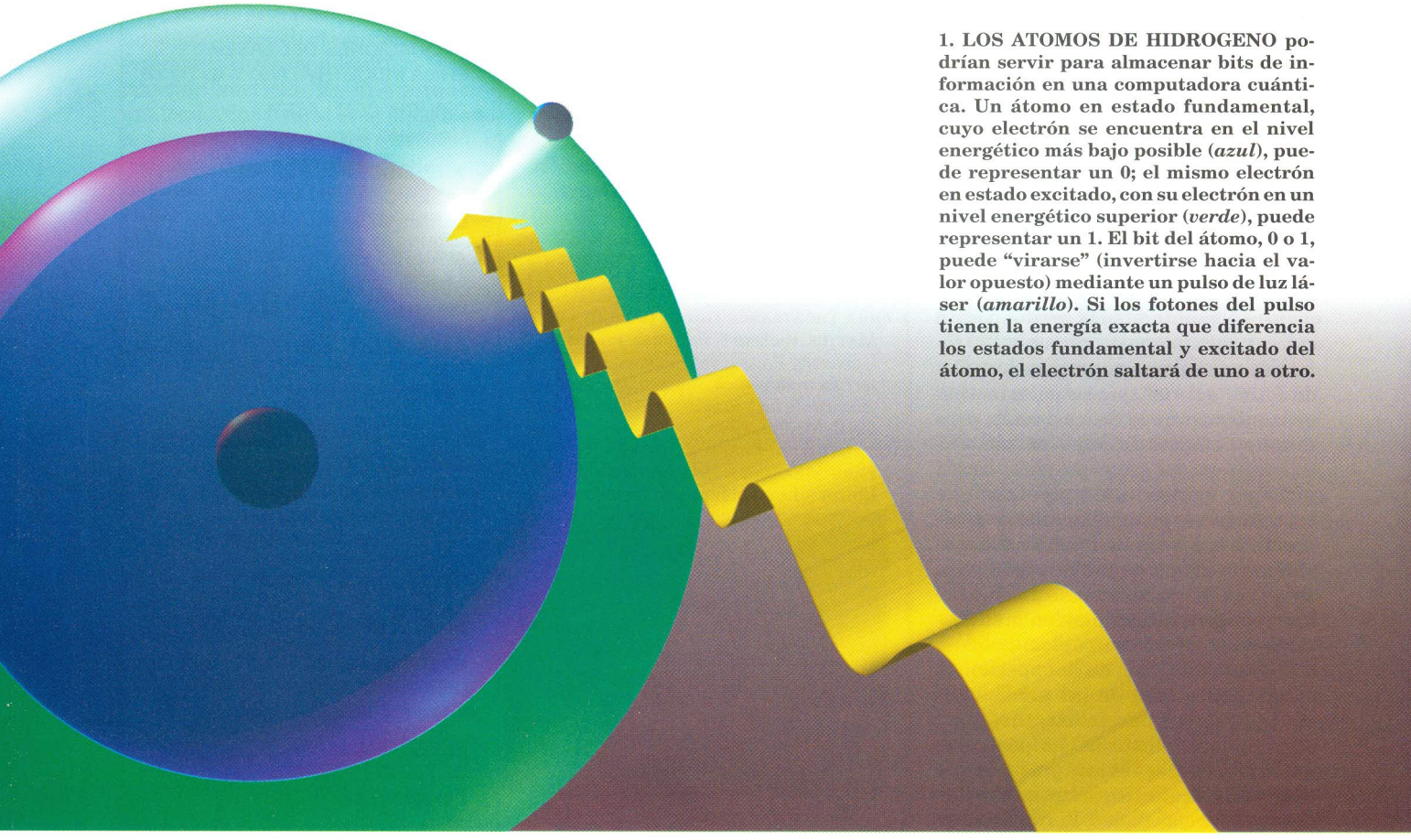
Seth Lloyd

Si algún día llegan a construirse, los ordenadores mecánico-cuánticos lograrán lo que ningún ordenador en uso puede hacer

Durante el último medio siglo, los ordenadores han ido duplicando su velocidad cada dos años, al tiempo que el tamaño de sus componentes se reducía a la mitad. Los circuitos actuales contienen transistores y líneas de conducción cuya anchura es sólo una centésima parte de la de un cabello humano. Las máquinas de nuestros días son millones de veces más potentes que sus rudimentarias antepasadas a causa de tan explosivo progreso. Pero las explosiones acaban disipándose y las técnicas de integración de microcircuitos están empezando a tropezar con sus límites.

Mediante técnicas litográficas avanzadas podrían producirse elementos cien veces menores que los hoy disponibles. Pero a tal escala, en la que la materia se presenta como una muchedumbre de átomos disgregados, los circuitos integrados apenas consiguen funcionar. Al reducir la escala diez veces más, los átomos manifiestan ya su identidad individual y basta un solo defecto para provocar una catástrofe. Por consiguiente, si se pretende que los ordenadores del futuro mengüen de tamaño, preciso habrá de ser que la técnica en uso se reemplace o suplemente con otras nuevas.

Hace ya bastantes años que Rolf Landauer y Charles H. Bennett empezaron a investigar la física de los circuitos de procesamiento de información y plantearse hacia dónde podría conducirnos la miniaturización: ¿cuál sería el tamaño mínimo de los componentes circuitales? ¿Cuánta energía es preciso utilizar en el curso de una computación? Por ser dispositivos mecánicos, el funcionamiento básico de los ordenadores está descrito por la física. La naturaleza de las cosas impone que, al hacerse muy pequeños



1. LOS ATOMOS DE HIDROGENO podrían servir para almacenar bits de información en una computadora cuántica. Un átomo en estado fundamental, cuyo electrón se encuentra en el nivel energético más bajo posible (*azul*), puede representar un 0; el mismo electrón en estado excitado, con su electrón en un nivel energético superior (*verde*), puede representar un 1. El bit del átomo, 0 o 1, puede "virarse" (invertirse hacia el valor opuesto) mediante un pulso de luz láser (*amarillo*). Si los fotones del pulso tienen la energía exacta que diferencia los estados fundamental y excitado del átomo, el electrón saltará de uno a otro.

los componentes de los circuitos de cómputo, su descripción debe dejarse en manos de la mecánica cuántica.

A comienzos de los años ochenta Paul Benioff, partiendo de resultados obtenidos por Landauer y Bennett, demostró que, al menos en principio, un ordenador podría funcionar de modo puramente mecánico-cuántico. Poco después David Deutsch y otros comenzaron a modelizar computadoras mecánico-cuánticas para averiguar en qué divergirían de las clásicas. Se preguntaron, en particular, si cabría sacar provecho de los efectos mecánico-cuánticos para acelerar las comunicaciones o para efectuar cómputos mediante nuevos procedimientos.

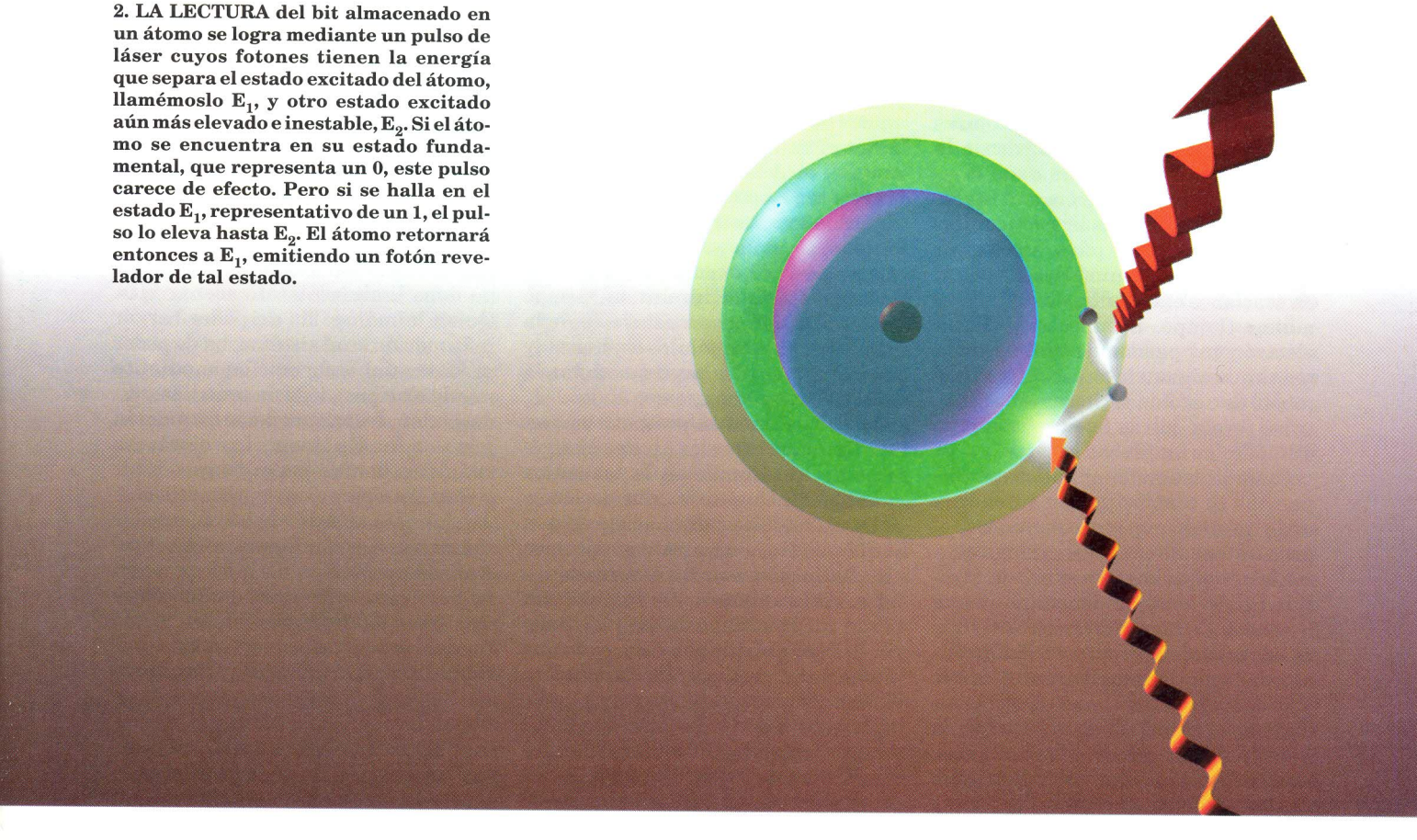
La especialidad languideció a mediados del decenio por una serie de razones. Ante todo porque, en lugar de estudiar sistemas físicos tangibles, se habían considerado las computadoras cuánticas en sentido abstracto, pecado en el que Landauer incurrió no pocas veces. Resultó también evidente que un ordenador mecánico-cuántico sería propenso a errores y que la corrección de los mismos plantearía serios problemas. Y aparte de una sugerencia de Richard P. Feynman, en el sentido de que las computadoras cuánticas podrían servir para la simulación de otros sistemas cuánticos (por ejemplo, formas de materia nuevas o inobservadas), no estaba claro que lograran resolver problemas matemáticos con mayor velocidad que sus parientes, los ordenadores clásicos.

La imagen ha cambiado en los últimos años. En 1993 describí una amplia clase de sistemas físicos, bien conocidos, que podrían actuar a modo de computadoras cuánticas, y hacerlo ahorrándome algunas de las objeciones de Landauer. Peter W. Shor demostró que podría utilizarse un ordenador cuántico para descomponer números grandes en factores primos, tarea que desborda incluso a las máquinas más potentes. En el Instituto para el Intercambio Científico de Turín se han engendrado numerosos diseños para la construcción de circuitería cuántica. En fin, los grupos de H. Jeff Kimble y de David J. Wineland han fabricado algunos de estos componentes prototípicos. Explicaré aquí de qué forma podrían ensamblarse ordenadores cuánticos y me ocuparé de algunas tareas que podrían llevar a cabo y son irrealizables por los ordenadores digitales.

Aceptemos de entrada que la mecánica cuántica produce desconcierto. Niels Bohr, que tanto contribuyó a su creación, confesaba: "Quien pueda contemplar la mecánica cuántica sin sensación de mareo es que no la ha comprendido adecuadamente." Por suerte o por desgracia, la mecánica cuántica predice cierto número de efectos contrarios a la intuición, pero que se han corroborado una y otra vez. Para apreciar de qué extrañas cosas son capaces los ordenadores mecánico-cuánticos, basta con abordar el fenómeno de la dualidad onda-partícula.

La dualidad onda-partícula significa que, en ciertas circunstancias, cosas normalmente consideradas partículas sólidas se comportan como si fueran ondas, mientras que cosas que describimos mediante ondas (sonido o luz) se comportan como partículas. En esencia, la teoría mecánico-cuántica establece las clases de ondas asociadas a los distintos tipos de partículas, y recíprocamente.

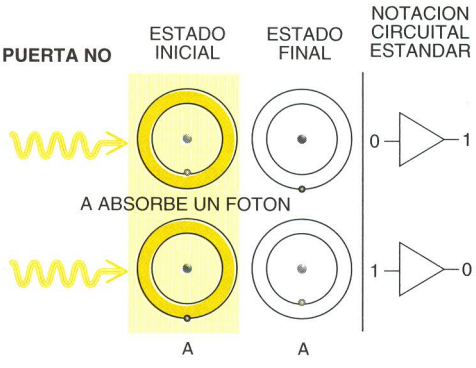
La primera y extraña consecuencia de la dualidad onda-partícula es que los sistemas físicos pequeños, como los átomos, sólo pueden existir en estados de energía discretos, bien caracterizados. Así, cuando un átomo salta de un estado energético a otro, absorbe o emite energía en cantidades exactas, llamadas fotones, que podrían considerarse partículas que componen las ondas de luz.



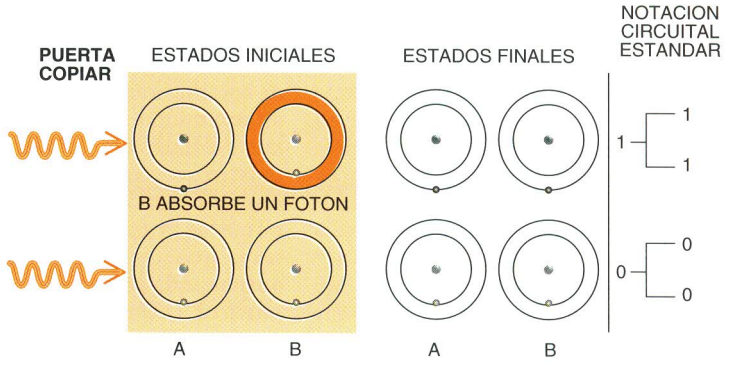
2. LA LECTURA del bit almacenado en un átomo se logra mediante un pulso de láser cuyos fotones tienen la energía que separa el estado excitado del átomo, llamémoslo E_1, y otro estado excitado aún más elevado e inestable, E_2. Si el átomo se encuentra en su estado fundamental, que representa un 0, este pulso carece de efecto. Pero si se halla en el estado E_1, representativo de un 1, el pulso lo eleva hasta E_2. El átomo retornará entonces a E_1, emitiendo un fotón revelador de tal estado.

Puertas lógico-cuánticas

Las puertas lógicas realizan operaciones elementales sobre bits de información. George Boole demostró en el siglo XIX que toda tarea lógica o aritmética, por compleja que fuese, era realizable por combinación de tres operaciones: NO, COPIAR e Y. Los átomos, o cualquier otro sistema cuántico, pueden efectuar estas operaciones.



La operación NO sólo entraña la inversión de bits, como indica la notación de la derecha: si A es 0, se convierte en 1, y viceversa. En el caso de los átomos, la negación puede efectuarse aplicando un pulso cuya energía sea igual a la diferencia entre el estado fundamental de A (su electrón se halla en el estado de mínima energía, representado por el círculo interior) y su estado excitado (el círculo exterior). Las puertas NO cuánticas, a diferencia de las ordinarias, pueden también invertir los bits sólo a medias.



COPIAR, en el mundo cuántico, se basa en la interacción entre dos átomos. Imaginemos que uno de los átomos, el A, que almacena un 0 o un 1, se encuentre junto a otro átomo, B, que se halla en su estado fundamental. La diferencia de energía entre los estados de B tendrá determinado valor si A es 0 y un valor distinto si A es 1. Apliquemos ahora un pulso luminoso cuyos fotones posean energía igual a este último valor. Si el pulso tiene la intensidad y la duración adecuadas, y si A es 1, B absorberá un fotón y cambiará de estado (*línea superior*); si A es 0, B no puede absorber un fotón del pulso y permanece invariable (*línea inferior*). Así, como vemos en el diagrama de la derecha, si A es 1, B se convierte en 1; si A es 0, B sigue siendo 0.

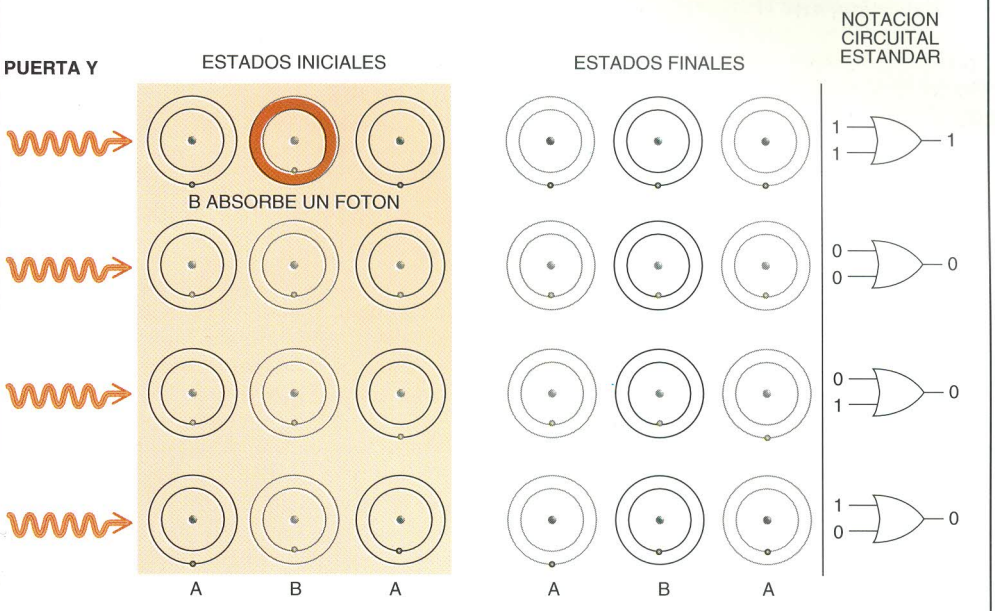
Una segunda consecuencia es que las ondas mecánico-cuánticas, como las ondas de agua, pueden superponerse, vale decir, sumarse. Tomadas individualmente, estas ondas ofrecen una descripción burda de la posición de una partícula dada. Empero, al combinar dos o más de tales ondas, la posición de la partícula se vuelve incierta. Así pues, en cierto y misterioso sentido, un electrón puede en ocasiones encontrarse aquí y allí al mismo tiempo. La ubicación de un electrón tal permanecerá incógnita hasta que alguna interacción (como el rebote de un fotón al chocar con el electrón) revele que se encuentra aquí o allí, pero no en ambos lugares.

Cuando dos ondas cuánticas superpuestas se comportan como una sola onda se dice que son coherentes; el proceso por el cual dos ondas coherentes recuperan su respectiva identidad individual se denomina descoherencia. En el caso de un electrón que se encuentre en superposición de dos estados energéticos diferentes (o por decirlo sin precisión, en dos posiciones distintas en el seno de un átomo), la descoherencia puede requerir largo tiempo. Pueden transcurrir días antes de que un fotón, pongamos por caso, choque contra un electrón y revele, al hacerlo, cuál es su verdadera posición. En teoría los balones de baloncesto podrían también encontrarse a la vez aquí y allá. En la práctica, sin embargo, el tiempo que tarda un fotón en rebotar de un balón es demasiado breve para que no lo detecte el ojo o algún instrumento. El balón es, sencillamente, demasiado grande para que su posición exacta pueda permanecer indetectada durante un tiempo perceptible. En consecuencia, la regla general es que tan sólo los objetos muy pequeños y sutiles pueden exhibir la incertidumbre cuántica.

La información se presenta en piezas discretas, como los niveles energéticos de los átomos en la mecánica cuántica. El cuanto de información es el bit. Un bit de información es una simple distinción entre dos opciones alternativas: sí o no, 0 o 1, verdadero o falso. En los ordenadores digitales, un bit de información está representado por la diferencia de potencial entre las placas de un condensador: un condensador cargado representa, por ejemplo, un 1, y un condensador descargado, un 0. Un ordenador cuántico funciona asociando el conocido carácter discreto del procesamiento de información digital con el extraño carácter discreto de la mecánica cuántica.

En efecto, una ristra de átomos de hidrógeno puede alojar bits igual de bien que una serie de condensadores. Un átomo en estado fundamental electrónico podría ser la codificación de un 0, y en estado excitado, de un 1. Mas para que tal sistema cuántico pueda funcionar como un ordenador no debe limitarse a almacenar bits. Quien lo maneje ha de poder cargar información en el sistema, ha de poder procesar tal información mediante manipulaciones lógicas sencillas y ha de poder descargar la información procesada. Es decir, los sistemas cuánticos han de poder leer, escribir y efectuar operaciones aritméticas.

Isidor Isaac Rabi enseñó a escribir información en un sistema cuántico. Aplicado a átomos de hidrógeno, su método opera como sigue. Imaginemos un átomo de hidrógeno en su estado fundamental, en el que posee una cantidad de energía igual a E_0. Para escribir un bit 0 en este átomo no se hace nada. Para registrar un 1 en él, excitemos el átomo hasta un nivel energético superior, E_1. Podemos conseguirlo bañándolo en luz láser compuesta por



También la conjunción Y depende de interacciones atómicas. Imaginemos tres átomos, A, B y A, adyacentes entre sí. La diferencia de energía entre los estados fundamental y excitado de B es función de los estados de los dos A. Supongamos que B se halle en su estado fundamental. Apliquemos ahora un pulso cuya energía sea igual a la diferencia entre los dos estados de B solamente cuando los átomos A vecinos sean sendos unos. Si realmente ambos A son unos, este pulso invertirá el estado de B (*línea superior*); de no ser así, B quedará sin cambios (*todas las demás líneas*).

fotones cuya energía sea igual a la diferencia entre E_1 y E_0. Si el haz de láser posee la intensidad adecuada y se aplica durante el tiempo necesario, el átomo pasará gradualmente desde el estado fundamental hasta el estado excitado, al absorber el electrón un fotón. Si el átomo se encuentra ya en el estado excitado, el mismo pulso lumínico provocará que emita un fotón y regrese al estado fundamental. Desde el punto de vista del almacenamiento de información, el pulso le dice al átomo que invierta el estado de su bit.

¿Qué significa "gradualmente" en este contexto? Un campo eléctrico oscilante, como es el de la luz láser, conduce un electrón de un átomo desde un estado de energía inferior hacia otro de energía más elevada a la manera del adulto que, impulsando a un niño en un columpio, lo sube cada vez a mayor altura. Siempre que llega la oscilación de la onda, le da un empujoncito al electrón. Cuando los fotones del campo tienen la misma energía que la diferencia entre E_0 y E_1, estos pulsos coinciden con el "vaivén" del electrón y gradualmente convierten la onda correspondiente al electrón en una superposición de ondas que poseen diferentes energías. La amplitud de la onda asociada con el estado fundamental del electrón disminuirá conforme aumenta la de la onda asociada con el estado excitado. En el proceso, el bit registrado en el átomo "vira" desde el estado fundamental hacia el excitado. Cuando la frecuencia de los fotones no es adecuada, sus empujones no están sincronizados con el electrón y nada ocurre.

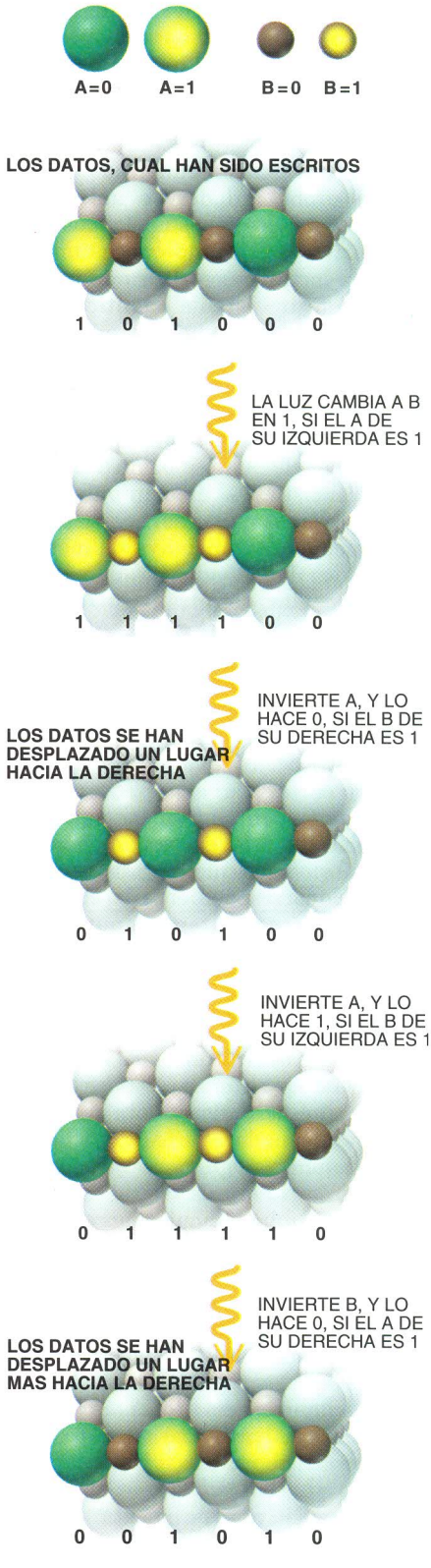
Si se aplica la luz adecuada, pero se hace durante la mitad del tiempo necesario para llevar al átomo desde el estado 0 al 1, el átomo se encuentra en un estado igual a la superposición de la onda correspondiente al 0 y de la onda correspondiente al 1, que tienen ambas iguales amplitudes. Tal bit cuántico, al que llamamos cubit, ha virado sólo a medias. Un bit clásico, por el contrario, dará siempre una lectura de 0 o de 1. En los ordenadores corrientes un condensador cargado a medias provoca errores, mientras que un cubit semivirado abre el camino a nuevas formas de computación.

La lectura de bits en un sistema cuántico procede de forma parecida. Se empuja al átomo hasta un estado energético todavía más elevado y menos estable, al que llamaremos E_2. Ello se consigue sometiendo el átomo a luz que tenga una energía igual a la diferencia entre E_1 y E_2: si el átomo se encuentra en E_1, se excitará hasta E_2, pero retornará rápidamente a E_1, emitiendo un fotón. Si el átomo se encuentra ya en el estado fundamental, nada ocurre. Si se halla en el estado "semivirado" tiene iguales probabilidades de emitir un fotón, revelando que es un 1, como de no emitirlo, indicando que es un 0. Entre la lectura y escritura de información en un sistema cuántico y la computación sólo media un breve paso.

Los circuitos electrónicos están formados por elementos lineales (conductores, resistencias y condensadores) y por elementos no lineales (diodos y transistores) que manipulan los bits de diversas maneras. Los dispositivos lineales alteran individualmente las señales de entrada. Los dispositivos no lineales, por otra parte, hacen que interactúen entre sí las señales de entrada que pasan a su través. Por ejemplo, de no ser porque nuestro equipo estereofónico contiene transistores no lineales, no podríamos cambiar el nivel de graves de la música que reproduce. Hacerlo así requiere cierta coordinación de la información procedente del lector de discos compactos y de la información que llega del ajuste del mando correspondiente del equipo.

Los circuitos realizan cómputos por iteración, a gran velocidad, de un pequeño número de tareas, tanto lineales como no lineales. Entre ellas se cuenta la inversión de un bit, que equivale a la operación lógica llamada NO: verdadero se torna en falso y falso se trueca en verdadero. Otra de ellas es la operación de COPIAR, que hace que el valor del segundo bit sea igual que el del primero. Estas dos operaciones son ambas lineales, porque en ambas la salida refleja el valor de una sola entrada. Efectuar la conjunción (la "Y") de dos bits —otra tarea útil— constituye, en cambio, una operación no lineal: si los dos bits de entrada son ambos 1, se hace que un tercer bit sea también igual a 1; en los demás casos, el tercer bit se hace igual a 0. El tercer bit depende ahora de cierta interacción entre las entradas.

Los dispositivos que ejecutan estas operaciones se denominan puertas lógicas. Si un ordenador digital posee puertas lineales, como la NO y la COPIAR, y puertas no lineales, tales como las puertas Y, entonces puede llevar a cabo cualquier tarea lógica o aritmética. Las computadoras cuánticas han de cumplir los mismos requisitos. Artur Ekert, Deutsch y Adriano Barenco, por un lado, y quien esto firma, por otro, han demostrado que



3. UN CRISTAL SALINO podría realizar cómputos actuando sobre pares de iones vecinos. Se invierte el bit almacenado en cada B si el A de su izquierda contiene un 1; seguidamente, se invierte cada A si el B a su derecha es 1. Se traslada así la información desde cada A hasta el B situado a su derecha. Ahora, utilizando la misma táctica, se traslada la información desde cada B al A de su derecha. El proceso permite que una línea de átomos actúe de "conductor" cuántico. Dado que un cristal puede realizar estas operaciones de "doble resonancia" en todas las direcciones simultáneamente con cada ion vecino, el cristal puede remedar la dinámica de cualquier sistema, actuando así de computadora cuántica analógica de uso general.

prácticamente cualquier interacción no lineal entre bits cuánticos será adecuada. A decir verdad, con tal de que un ordenador cuántico pueda invertir bits, cualquier interacción cuántica no lineal lo faculta para llevar a cabo cualquier cómputo. Para la construcción de ordenadores cuánticos podría sacarse provecho, pues, de muy distintos fenómenos físicos.

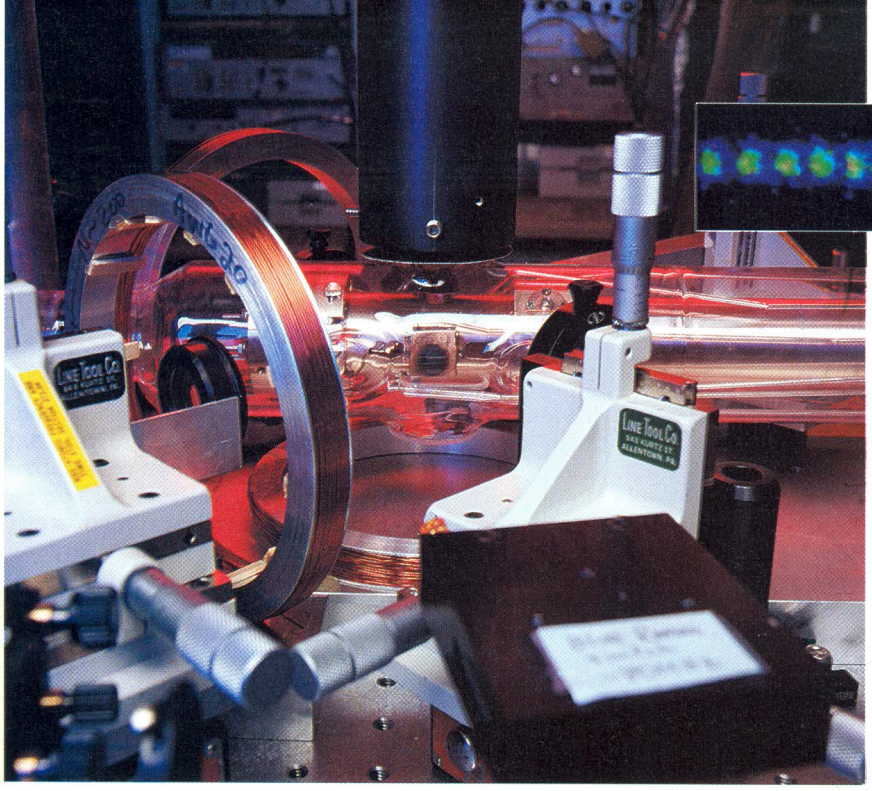
¡La verdad es que ha habido puertas lógico-cuánticas disponibles y se han usado habitualmente desde hace casi tanto tiempo como hay transistores! A finales de los años cincuenta los investigadores lograron realizar sencillas operaciones de lógica cuántica con dos bits valiéndose del espín de las partículas. Estos espines —que consisten en la orientación del movimiento de rotación de una partícula con respecto a cierto campo magnético—se encuentran, al igual que los niveles energéticos, cuantizados. Así pues, un espín en una dirección puede representar un 1, y en la otra, un 0. Se aprovechó la interacción entre el espín del electrón y el espín del protón en un átomo de hidrógeno; se puso a punto un sistema en el cual sólo se invertía el espín del protón si el espín del electrón representaba un 1. Como los investigadores no estaban pensando en lógica cuántica, bautizaron al efecto con el nombre de "doble resonancia". Aun así se valieron de ella para efectuar las operaciones lineales de negación y copia.

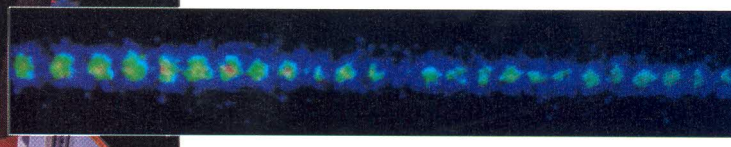
Desde entonces, Barenco, David DiVincenzo, Tycho Sleator y Harald Weinfurter han mostrado cómo, virando sólo parcialmente los espines del protón y el electrón, se puede utilizar la doble resonancia para crear también una puerta lógica Y. Tales puertas logico-cuánticas, interconectadas, podrían constituir una computadora cuántica. Inútil decir que los "conductores" cuánticos son difíciles de construir. Los conductores de un ordenador corriente pueden ser meras tirillas de metal, que transmiten sin dificultad las señales eléctricas de una puerta lógica a otra. La interconexión de puertas de doble resonancia, por el contrario, entraña una dificultad exasperante: el conductor ha de poder desensamblar átomos para trasladar protones y electrones a voluntad y luego ha de volver a ensamblarlos sin perturbar los espines de las partículas.

No hace mucho que se han ideado medios más sencillos para concatenar puertas lógico-cuánticas. Por ejemplo, fotones individuales conducidos por fibras ópticas o enviados a través del aire podrían transferir bits de información desde una puerta hasta otra. Un descubrimiento muy prometedor se ha hecho en el Instituto de Tecnología de California: concentrando fotones en un volumen diminuto junto con un solo átomo, el grupo de Kimble ha conseguido intensificar la interacción no lineal entre fotones, que por lo común es muy pequeña. El resultado es una puerta logico-cuántica: un bit de un fotón puede "virarse" parcialmente cuando otro fotón lee un 1. Un ordenador construido con puertas lógico-cuánticas de este tipo sería rápido y bastante inmune a las perturbaciones del medio que destruirían la coherencia, pero habría que superar todavía cierto número de obstáculos predichos por Landauer. El más importante es que las tolerancias en la longitud de todos los caminos ópticos del sistema tendrían que ser de una minúscula fracción de la longitud de onda utilizada.

El problema del "cableado" admite otras soluciones. J. Ignacio Cirac y Peter Zoller han propuesto un diseño que aislaría cubits en una trampa de iones, aislándolos de influencias externas indeseables. Antes de procesarlo, el bit se transferiría a un registro común, a un "bus". En concreto, la información que contuviera se representaría por un temblequeo en el que participarían todos los iones de la trampa. El grupo de Wineland ha dado ya el primer paso hacia la construcción de un tal ordenador cuántico, realizando operaciones tanto lineales como no lineales sobre bits codificados mediante iones y por el temblequeo. La construcción de computadoras capaces de operar con unas pocas decenas o centenas de bits mediante trampa iónica ofrece buenas perspectivas. Se han realizado ya operaciones binarias y el número de bits de la computadora puede aumentarse sin más que añadir iones a la trampa.

Así las cosas, los científicos pueden manejar operaciones de lógica cuántica con unos pocos bits y es muy posible que en un futuro cercano efectúen cómputos cuánticos en los que intervengan algunas decenas o centenares de bits. ¿En qué sentido puede ello





4. LA PRESENTACION del resultado de un cómputo cuántico podría ofrecer el aspecto de la banda superior. Cada lunar coloreado corresponde a la fluorescencia de un solo ion mercúrico atrapado en una trampa iónica (*izquierda*). La luz indica que cada uno de los iones se encuentra en el mismo estado, por lo que la ristra completa se lee como una serie de unos.

representar un avance sobre los ordenadores clásicos, que manejan sin dificultad miles de millones de bits? La verdad es que, incluso con un solo bit, una computadora cuántica puede realizar cosas que no están al alcance de ningún ordenador clásico. Fijémonos en lo siguiente. Tomemos un átomo en superposición de 0 y 1. Averigüemos ahora si el bit es un 0 o un 1 provocando su fluorescencia. La mitad de las veces el átomo emite un fotón y el bit es un 1. En la otra mitad no hay emisión fotónica y el bit es un 0. Es decir, el bit es un bit aleatorio, algo que ningún ordenador clásico puede crear. Los programas de números aleatorios de los ordenadores digitales generan en realidad números pseudoaleatorios, valiéndose para ello de una función cuyo resultado es tan irregular que parece producir bits por azar.

Imaginemos lo que un ordenador cuántico puede hacer con dos bits. El copiado se realiza juntando dos bits, uno con el valor a copiar y otro cuyo valor inicial es 0; al serle aplicado un pulso, el segundo bit cambia a 1 solamente en el caso de que el primer bit también sea un 1. Pero si el valor del primer bit es una superposición de 0 y 1, la aplicación del pulso crea una superposición en la que participan ambos bits, de forma tal que ambos son 1 o ambos son 0. Fijémonos en que el valor final del primer bit ya no es el mismo que inicialmente tenía; la superposición ha cambiado.

En cada componente de esta superposición el segundo bit es el mismo que el primero, pero ninguno de ellos es el mismo que el bit original. Albert Einstein hizo notar que tales estados infringirían todas las ideas intuitivas tradicionales sobre causalidad. En una tal superposición, ninguno de los bits se encuentra en un estado definido; empero, si medimos uno de ellos, situándolo en consecuencia en un estado definido, el otro bit pasa también a un estado definido. El cambio del primer bit no es la causa del cambio del segundo. Pero en virtud de la destrucción de la coherencia entre ambos, la medición del primero también despoja al segundo de su ambigüedad. Con tres cubits se pueden establecer estados imbricados todavía más complejos.

En efecto, dados tan sólo dos o tres cubits y una o dos puertas lógico-cuánticas, resulta posible la creación de estados cuánticos fascinantes. He demostrado que, con mayor número de bits, podría utilizarse una computadora cuántica para simular el comportamiento de cualquier sistema cuántico. Programada adecuadamente, la dinámica de la computadora remedaría la dinámica de cierto sistema postulado y, en particular, de la interacción del sistema con su entorno. Además el número de pasos que tal computadora tendría que dar para registrar la evolución de este sistema a lo largo del tiempo sería directamente proporcional al tamaño del sistema.

Todavía más notable es que, si una computadora cuántica tuviera arquitectura en paralelo, lo que pudiera ser factible por doble resonancia entre pares vecinos de espines en los átomos de un cristal, podría remedar en tiempo real a cualquier sistema cuántico, cualquiera que fuera su tamaño. Esta clase de computación cuántica en paralelo, de ser posible, supondría una enorme aceleración sobre los métodos al uso. Según advirtiera Feynman, para simular un sistema cuántico en un ordenador clásico se precisa, en general, un número de pasos que crece exponencialmente con el tamaño del sistema y con el lapso de tiempo invertido en rastrear sus evoluciones. La verdad es que una computadora cuántica de 40 bits podría recrear un sistema cuántico en poco más de un centenar de pasos; esta misma simulación exigiría años en un ordenador clásico provisto de un billón de bits.

¿Qué puede llegar a hacer una computadora cuántica, dotada de muchas operaciones lógicas, sobre muchos cubits? Empecemos colocando todos los bits de entrada en idéntica superposición de ceros y unos, todos iguales. La computadora se encuentra entonces en otra superposición de todas las entradas posibles. Hagamos pasar esta entrada a través de un circuito lógico que ejecute un determinado cómputo. El resultado es una superposición de todos los posibles resultados de ese cómputo. En cierto y extravagante sentido cuántico, la computadora efectúa a la vez todos los cómputos posibles. Deutsch ha denominado a este efecto "paralelismo cuántico".

Aunque el paralelismo cuántico pueda parecer extraño, pensemos por un momento en el comportamiento general de las ondas. Si las ondas mecánico-cuánticas fuesen ondas sonoras, las correspondientes a 0 y a 1 —que oscilan cada una a una sola frecuencia— constituirían tonos puros. Una onda correspondiente a una superposición de 0 y 1 sería entonces un acorde. Así como los acordes musicales suenan cualitativamente distintos de los tonos individuales que los integran, una superposición de 0 y 1 se diferencia del 0 y el 1 tomados por

COLABORADORES DE ESTE NUMERO

Traducción:

Pedro Pascual: *Teoría cuántica y realidad*; Ramón Pascual: *Realidad del mundo cuántico, Filosofía cuántica y ¿Más veloz que la luz?*; Adán Cabello: *Espín y estadística*; Juan Pedro Campos: *Teoría alternativa de Bohm a la mecánica cuántica, La dualidad en la materia y en la luz, La frontera entre lo cuántico y lo clásico* y *Visión cuántica en la obscuridad*; Luis Bou: *Criptografía cuántica y Computación mecánico-cuántica*

Portada: Prensa Científica S.A.

Página	Fuente
5-12	Scientific American, Inc.
14-26	Jerome Kuhl
29	Roger Gérard, Instituto de Optica Teórica y Aplicada
30-35	Gabor Kiss
36-37	Andrew Christie
38-40	Boris Starosta
41-43	Robert Prochnow
44	John Pinderhughes
47	Archivo Bettmann
48-49	Patricia J. Wynne
50-54	Boris Starosta
56	*Nature*
58	Dan Wagner
60-61	Michael Goodman
62	UPI/Bettmann
63	Michael Goodman
64	Mark Edwards/Still Pictures
66	Adán Cabello
68-69	Michael Crawford
70-73	Michael Goodman
76	Robert Prochnow
77	Cortesía de David Kahn, ©1983 Macmillan Publishing Company
78-83	Michael Goodman
84-85	Composición digital de Jeff Brice, cortesía de Matthias Freyberger, Universidad de Ulm
86	Jared Schneidman Design
87	Michael Noel y Carlos Stroud, Universidad de Rochester
88-89	Jared Schneidman Design
91	Michael Goodman
92-97	Jared Schneidman Design; Michael Reck, Universidad de Innsbruck (*fotografía*)
98-99	Boris Starosta
100-101	Michael Goodman
102	Michael Goodman
103	Geoffrey Wheeler (*izquierda*); Instituto Nacional de Pesos y Medidas (*derecha*)

separado: en ambos casos, las ondas combinadas se interfieren entre sí.

Una computadora cuántica que realice un cómputo ordinario, en el que no haya superposición de bits, genera una secuencia de ondas análogas al sonido de un "cambio de repique" de los campanarios, en que las campanas se tañen una por vez. La secuencia de sonidos se atiene a reglas matemáticas estrictas. Un cómputo realizado en modo cuántico paralelo viene a ser como una sinfonía: su "sonido" corresponde a una multitud de ondas que se interfieren entre sí.

Shor demostró que el efecto sinfónico del paralelismo cuántico podría servir para descomponer muy rápidamente números grandes en factores primos, cosa que los ordenadores clásicos e incluso los superordenadores no siempre logran. Puso de manifiesto cómo orquestar una computación cuántica de forma que los posibles factores destaquen en la superposición, al igual que, en una sinfonía, una melodía tocada por los cellos, las violas y los violines con separación de una octava destacaría sobre el sonido de fondo creado por los demás instrumentos. Su algoritmo haría que la factorización resultase tarea sencilla para una computadora cuántica, de poder construirse. Dado que la mayoría de los sistemas criptográficos de clave pública —como los de protección de las cuentas bancarias electrónicas— se basan en que los ordenadores clásicos no pueden hallar factores primos que tengan, sea por caso, más de 100 dígitos, los merodeadores informático-cuánticos podrían darle motivo de preocupación a mucha gente.

La cuestión de si llegará a haber computadoras cuánticas (y sus correspondientes merodeadores) es cuestión debatida con ardor. Recordemos que la naturaleza cuántica de una superposición subsiste tan sólo mientras el entorno se abstiene de revelar el estado del sistema. Habida cuenta de que las computadoras cuánticas podrían consistir en miles o millones de átomos y de que para lesionar la coherencia cuántica basta la perturbación de uno solo de ellos, no está claro cuánto tiempo pueden durar en auténtica superposición los sistemas cuánticos interactuantes. Las pruebas experimentales inducen a pensar que ciertos sistemas pueden mantener superposiciones cuánticas durante varias horas. Shor y sus colaboradores han demostrado que su algoritmo sigue funcionando incluso con niveles modestos de descoherencia.

Otro de los problemas a que se enfrenta la computación cuántica es la corrección de errores. Los distintos sistemas que podrían utilizarse para el registro y procesamiento de información son sensibles al ruido, que puede invertir bits de modo aleatorio. Los métodos clásicos de corrección de errores entrañan la medición de bits para ver si son erróneos, lo que en una computadora cuántica provocaría la descoherencia. Los grupos de Ekert y de Deutsch han mostrado que la corrección de errores es posible en teoría, pero muy costosa de llevar a la práctica. Así pues, aun cuando puedan construirse computadoras cuánticas, tal vez no sean capaces de realizar cómputos con muchos bits durante períodos largos.

Para sobrepasar la capacidad de factorización de los superordenadores actuales, las computadoras cuánticas que utilizasen el algoritmo de Shor podrían tener que seguir la pista de centenares de bits durante millares de pasos, manteniendo en todo momento la coherencia cuántica. Por culpa de los problemas técnicos de que hablaba ya Landauer, entre los que se cuentan la descoherencia, las variaciones incontrolables en los pulsos de láser y la carencia de una corrección de errores eficaz, es muy verosímil que la construcción de un ordenador capaz de efectuar semejante cómputo resulte difícil. Sin embargo, para superar las simulaciones clásicas de los sistemas cuánticos bastaría con seguir la pista a unas decenas de bits durante algunas decenas de pasos, objetivo mucho más alcanzable. Y la utilización de lógica cuántica para la creación y exploración de las propiedades de extraños estados cuánticos con multitud de partículas es meta que ya se encuentra en el horizonte.

BIBLIOGRAFIA COMPLEMENTARIA

QUANTUM THEORY: THE CHURCH-TURING PRINCIPLE AND THE UNIVERSAL QUANTUM COMPUTER. David Deutsch en *Proceedings of the Royal Society of London*, serie A, vol. 400, n.º 1818, páginas 97-117; 1985.

A POTENTIALLY REALIZABLE QUANTUM COMPUTER. Seth Lloyd en *Science*, vol. 261, páginas 1569-1571; 17 de septiembre de 1993.

ALGORITHMS FOR QUANTUM COMPUTATION: DISCRETE LOGARITHMS AND FACTORING. Peter W. Shor en *35th Annual Symposium on Foundations of Computer Science: Proceedings*. Recopilación de Shafi Goldwasser. IEEE Computer Society Press, 1994.

QUANTUM COMPUTATIONS WITH COLD RAPPED IONS. J. I. Cirac y P. Zoller en *Physical Review Letters*, volumen 74, n.º 20, páginas 4091-4094; 15 de mayo de 1995.