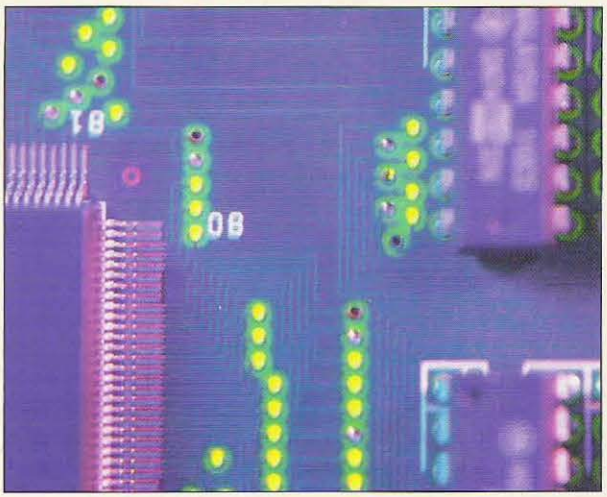
Ordenadores cuánticos

La potencia de cálculo de los ordenadores ha crecido espectacularmente en las últimas décadas, duplicándose aproximadamente cada dos años. Este crecimiento se debe a la continua miniaturización del componente básico de los ordenadores: el **transistor**. A medida que ha sido posible fabricar transistores más pequeños, mayor número de ellos han podido integrarse en un solo microchip, aumentando así la potencia de cálculo.

Sin embargo, este proceso de miniaturización no puede continuarse de modo indefinido, puesto que la mecánica cuántica impone un umbral por debajo del cual un transistor dejaría de funcionar. Los componentes actuales más avanzados tienen un tamaño de unos centenares de nanómetros (1 nm = 10^{-9} m). Si los chips pudieran miniaturizarse hasta un tamaño de unas pocas decenas de nanómetros (es decir, a escala de unos cuantos átomos), su funcionamiento se vería alterado por la aparición de fenómenos cuánticos, tales como el **efecto túnel**[1] de los electrones a través de las barreras existentes entre los hilos. Por supuesto, sería posible rediseñar los transistores para que funcionasen haciendo uso de efectos cuánticos, pero es preferible abandonar la idea del transistor a favor de un tipo de arquitectura completamente nueva que sea más adecuada a la escala de nanómetros.

No obstante, la primera generación de ordenadores con componentes que funcionen de acuerdo con la mecánica cuántica ejecutará algoritmos[2] que probablemente seguirán siendo clásicos. Pero los científicos están trabajando ya sobre otra posibilidad mucho más interesante: la mecánica cuántica podría utilizarse en algoritmos totalmente nuevos y que serían mucho más potentes que cualquier esquema clásico. Un ordenador en el que se ejecutaran tales algoritmos sería un auténtico **ordenador cuántico**.

Para entender lo que diferencia a un ordenador cuántico de uno clásico, empecemos echándole un vistazo a la unidad básica de información: un **bit**. Desde un punto de vista físico, un bit es un sistema físico que puede encontrarse en uno de dos estados diferentes que representan dos valores lógicos («sí» o «no», «verdadero» o «falso», o simplemente «1» o «0»). Por ejemplo, en los ordenadores actuales el voltaje entre las placas de un condensador representa un bit de información: un condensador cargado representa el valor 1, mientras que uno descargado representa el valor 0. Un bit de información también puede codificarse utilizando dos polarizaciones diferentes de la luz o bien dos estados electrónicos diferentes de un átomo. En este último caso, sin embargo, la Mecánica Cuántica nos dice que, aparte de los dos estados electrónicos distintos, el átomo puede también prepararse en una superposición coherente[3] de los dos estados. Esto significa que, de algún modo, el átomo está tanto en el estado 0 como en el 1.



Detalle de un circuito impreso.

En general, un sistema cuántico con dos estados posibles y que puede prepararse en una superposición de dichos estados representa un «bit cuántico» o, como suele denominarse, un **qubit**. Consideremos ahora un registro compuesto por tres bits. Un registro clásico de este tipo puede almacenar en un instante dado sólo uno de los ocho posibles números del 0 al 7 (es decir, en base binaria, 000, 001, 010, . . . , 111).

Por el contrario, un registro cuántico compuesto por tres qubits puede almacenar en un instante dado los ocho números mediante una superposición cuántica. Si añadimos más qubits al registro, aumenta su capacidad de almacenamiento exponencialmente: un registro de N qubits puede almacenar 2^N números simultáneamente (aunque, si medimos en un instante dado el contenido del registro, obtendremos sólo uno de esos números). Una vez que el registro está preparado en una superposición de números diferentes, podemos realizar operaciones sobre todos ellos. Por ejemplo, si los qubits son átomos, mediante pulsos de láser de frecuencia adecuada podríamos hacer evolucionar la superposición inicial a una nueva superposición.

Durante esa evolución, cada número de la superposición se ve afectado y, en consecuencia, generamos un cálculo masivo en paralelo en el que en un solo paso de cálculo se lleva a cabo la misma operación matemática que requeriría 2^N pasos en un procesador clásico (o un paso en 2^N procesadores diferentes trabajando en paralelo). Esto supone una ganancia enorme en tiempo y memoria que puede explotarse en ciertos tipos de cálculo gracias al fenómeno de **interferencia cuántica**.

Donde los ordenadores cuánticos mostrarán más claramente su utilidad será en la aplicación de algoritmos hasta ahora considerados «lentos». Un algoritmo se dice que es lento cuando el número de pasos requerido para ejecutarlo aumenta con el tamaño de los datos de entrada de una forma más acusada que cualquier función polinómica. Un ejemplo típico de algoritmo lento es el de la factorización. Por ejemplo, supongamos que queremos hallar los números a y b tales que $a \times b = 29.083$. Con papel y lápiz, encontrar la solución podría llevarnos quizá una hora. Sin embargo, hallar la solución del problema inverso ($127 \times 229 = c$) apenas nos llevaría un minuto. Pero eso no es lo más importante, sino que, mientras que multiplicar dos números de treinta dígitos es algo tedioso pero que puede realizarse sin un enorme esfuerzo adicional, factorizar un número de treinta dígitos requiere alrededor de 10^{13} veces más de tiempo o de memoria que factorizar un número de tres dígitos.

En general, si queremos factorizar un número n con N dígitos decimales ($n \approx 10^N$), tendríamos que dividirlo por 2, 3, . . ., $\sqrt{n}$ y comprobar si el resto es cero. Por tanto, resolver el problema requiere llevar a cabo $\sqrt{n} \approx 10^{N/2}$ divisiones, es decir, el número de operaciones es una función exponencial del número de dígitos N. Supongamos un ordenador que fuera capaz de realizar 10^{10} divisiones por segundo, por lo que tardaría aproximadamente $\sqrt{n}/10^{10}$ segundos en factorizar un número n. Si ese número tiene $N = 100$ dígitos ($n \approx 10^{100}$), entonces el tiempo necesario para factorizarlo sería del orden de 10^{40} segundos, es decir, del orden de $3 \cdot 10^{32}$ años, ¡que es un tiempo muchísimo mayor que la edad estimada del universo (del orden de $12 \cdot 10^9$ años)!

Precisamente los sistemas modernos de **criptografía**[4] se basan en la enorme dificultad que supone factorizar números grandes, dificultad que está relacionada con el hecho de que el algoritmo clásico es un algoritmo lento. Ahora bien, un ordenador cuántico podría factorizar un número $n \approx 10^N$ mediante un nuevo algoritmo (propuesto por Peter Shor en 1994) que, utilizando dos registros compuestos por un cierto número de qubits, necesitaría un tiempo que es tan sólo una función cuadrática del número de dígitos N. En consecuencia, el algoritmo cuántico de factorización podría factorizar un número de 100 dígitos ¡en apenas una fracción de segundo! Otras aplicaciones de los ordenadores cuánticos incluyen la criptografía cuántica (comunicación perfectamente segura basada en el principio de incertudumbre de Heisenberg y en el «enredado» de estados cuánticos), la búsqueda de un número dado en una lista larga (mediante el algoritmo propuesto por Lov Grover en 1996) o la simulación eficiente de sistemas mecánico-cuánticos.

¿Será posible en el futuro construir ordenadores cuánticos o se quedarán para siempre en meras curiosidades teóricas? En principio, sabemos cómo construir un ordenador cuántico. Sin embargo, existen serios problemas prácticos ligados al hecho de que, cuanto mayor es el número de qubits involucrados, más difícil es mantener la interferencia cuántica. Aparte de las dificultades técnicas que conlleva trabajar a escala de un átomo y de un fotón, uno de los problemas más importantes es el de evitar que el entorno se vea afectado por las interacciones que generan las superposiciones cuánticas. A medida que aumenta el número de componentes, aumenta la posibilidad de que el proceso cuántico se extienda fuera de la unidad de cálculo y la información útil se disipe irreversiblemente al entorno.

Para evitar este proceso de deterioro de la coherencia es necesario diseñar sistemas submicroscópicos en los que los qubits interaccionen entre sí, pero no con el entorno. Algunos físicos son pesimistas sobre la posibilidad de que se alcancen progresos sustanciales en la tecnología de los ordenadores cuánticos; opinan que la pérdida de coherencia nunca podrá reducirse al extremo de poder realizar más de unos pocos pasos de cálculo cuántico consecutivos. Otros investigadores son más optimistas y creen que los ordenadores cuánticos serán una realidad en cuestión de décadas o incluso de años[5]. En realidad, no hay ningún obstáculo fundamental en el camino y el optimismo suele hacer que los deseos acaben convirtiéndose en realidad. Después de todo, ¡hubo un tiempo en que se aceptó como una «verdad científica» que ninguna máquina más pesada que el aire podría volar!

---

[1] El **efecto túnel** consiste en la posibilidad de que una partícula (por ejemplo, un electrón) pase de una región del espacio a otra, a pesar de tener una energía total menor que la altura de la barrera potencial que separa ambas regiones. Éste es un fenómeno genuinamente cuántico (es decir, imposible de explicar desde la Mecánica clásica: ¡el electrón tendría una energía cinética negativa al atravesar la barrera!) y que pone de manifiesto la naturaleza ondulatoria del comportamiento de la partícula. El efecto túnel es semejante a la propiedad de la luz de pasar de un medio transparente a otro, incluso si ambos están separados por una delgada lámina opaca.

[2] Un algoritmo es un conjunto preciso de instrucciones que pueden aplicarse mecánicamente para obtener la solución a cualquier caso particular de un problema dado.

[3] De nuevo, este fenómeno de superposición es puramente cuántico y no tiene equivalente en la Física clásica.

[4] El objetivo de la criptografía es transmitir información de tal modo que sólo pueda tener acceso a ella el receptor deseado.

[5] El lector interesado (y que pueda leer en inglés) puede ampliar información en la página web *http://www.qubit.org*.