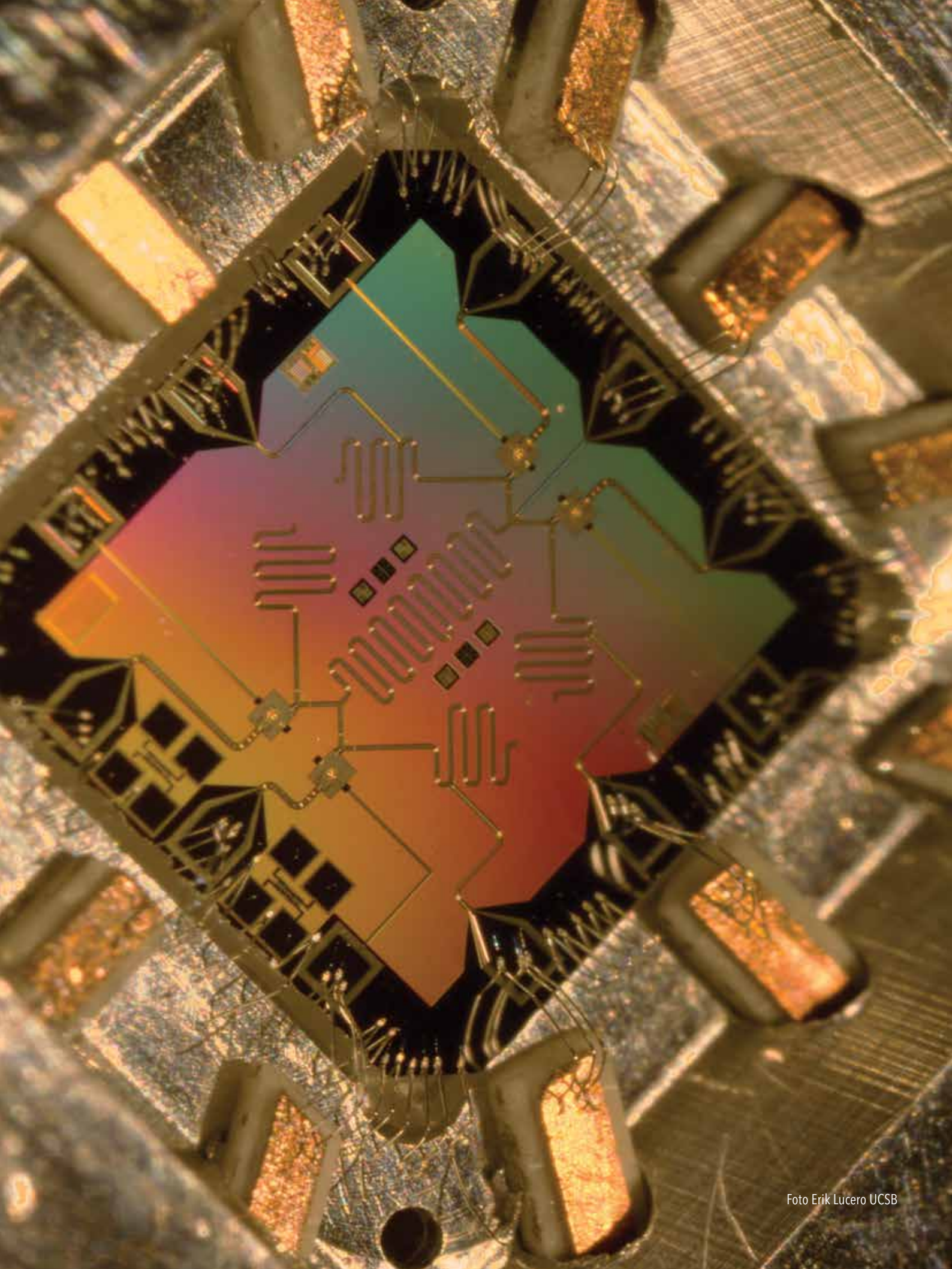

Foto Erik Lucero UCSB

Alejandro Díaz-Caro
Universidad Nacional de Quilmes

¿Qué es la computación cuántica?

Para empezar por el principio: ¿qué es la física cuántica? Es la física de lo muy pequeño. La matemática que usa esa física permite comprender y ayuda a predecir el comportamiento de las partículas más reducidas que componen el universo, como los electrones o los fotones. La física cuántica es distinta de la física clásica, que se ocupa de objetos más grandes, como las pelotas de fútbol o los planetas. Tomemos un ejemplo: el sistema físico constituido por un futbolista que patea a un arco sin arquero. En el marco de la física clásica, los físicos pueden describir el estado inicial de ese sistema haciendo un gran número de mediciones, como la fuerza de la patada, la velocidad del viento, el ángulo del tiro, el punto en que el pie le pega a la pelota, la forma y el peso de esta, la distancia al arco y muchas más. Si pudiesen medir todas las variables –cosa irrealizable en términos prácticos–, la física clásica predeciría sin error el resultado, que solo tiene dos posiciones posibles: que el futbolista haga un gol o que no lo haga.

La física cuántica opera en un mundo muy distinto, en el que un hipotético futbolista en una situación como la anterior puede hacer el gol y también, al mismo tiempo, no hacerlo, lo que es imposible en el marco de la física clásica, además de contradecir el sentido común. La física cuántica no se aplica al futbolista ni a su pelota, pero sí a los citados fotones, las partículas sin masa que componen la luz, y ese es, justamente, su comportamiento: pueden hacer gol y también, al mismo tiempo, no hacerlo.

¿DE QUÉ SE TRATA?

Una comparación entre la computación clásica y la computación cuántica.

Para explicar esta aparente paradoja, tomemos un ejemplo equivalente al anterior en el mundo de la física cuántica: supongamos que en vez de un arco tenemos una pared con dos orificios contiguos y que encendemos una linterna de un lado de ella, a cierta distancia de los orificios, con lo que veremos a la luz emitida atravesar ambos. Pero si en vez de un haz de luz, la linterna emite una sola partícula de ella, es decir, un fotón, la física cuántica no podrá predecir por cuál orificio pasará, incluso pudiendo medir todas las variables del estado inicial del sistema. Más aún, si, emitido el fotón, registramos por donde pasó mediante un instrumento que realice la constatación del lado del muro por el que emergió el fotón, constataremos que lo hizo por los dos orificios a la vez. En otras palabras, el futbolista hizo gol y, con el mismo tiro, no lo hizo.

En el párrafo anterior razonamos pensando en la física clásica, como si el fotón fuera una pequeña pelotita, pero constatamos que se comportó como una onda, igual que el sonido o que una ola del mar, pues tiene sentido que una onda pase por ambos orificios a la vez. Pero entonces, ¿por qué se habla de partículas y no de ondas? Ello es así porque si se registra por donde pasó el fotón mediante un instrumento que realice la constatación del lado del muro en que está la linterna, por el que se puede suponer que ingresará en uno de los orificios, se constatará que, efectivamente, lo hace por uno y no por ambos. Es decir, se comporta como una partícula –como una pelotita– y no como una ola del mar. ¿Cuál de ambos comportamientos es el real? Ambos.

El mundo cuántico es así: no solo no podemos predecir con precisión lo que sucederá, sino que, además, suceden cosas que contradicen a la intuición y al sentido común. Pero a pesar de ello la física cuántica puede hacer predicciones sobre el comportamiento del mundo subatómico, y gracias a estas predicciones tenemos hoy transistores, láseres y el GPS.

Veamos algún ejemplo de lo que nos permite la física cuántica. Los vidrios polarizados dejan pasar ciertos fotones e impiden el paso de otros. Un fotón posee un atributo llamado *polarización*, que puede describirse como una extensión en un plano perpendicular a la dirección en que se desplaza. Un vidrio polarizado puede permitir que solo pasen los fotones con polarización vertical, e impedir que lo hagan los que tienen polarización horizontal. ¿Qué sucede en tal caso con un fotón polarizado a 45°? Choca contra el vidrio y, al azar, modifica su polarización para resultar polarizado horizontalmente o verticalmente, y pasar o no pasar en consecuencia. Los físicos recurren a varias teorías matemáticas para interpretar lo anterior, que no vienen al caso aquí.

Podemos ir un paso más allá en el análisis. Si el fotón del ejemplo estuviera polarizado a 45°, tendría igual probabilidad de cambiar su polarización por una horizontal que por una vertical. Pero si hubiera estado polarizado en un ángulo más cercano a una de esas dos direcciones, la probabilidad no sería de 0,5 para cada una de ellas, sino más alta para la dirección más cercana, y tanto más alta cuanto más cercana. Es decir, si un fotón tiene una polarización casi vertical, es muy probable –pero no seguro– que adopte la polarización vertical y atraviese el vidrio.

Imaginemos ahora un vidrio que deja pasar tanto los fotones polarizados horizontalmente como verticalmente. En ese caso, todos los fotones atravesarán el vidrio, porque los que tengan otra polarización, al llegar al vidrio, la modificarán para tomar sea la horizontal, sea la vertical. Los fotones que se aproximan al vidrio pueden tener, además de la polarización horizontal o la vertical, una tercera polarización, llamada de *superposición*, que viene dada por las probabilidades de tomar una y la otra para atravesar el vidrio. Esas probabilidades indican que para la física cuántica los fotones en esa situación tienen una polarización que es simultáneamente vertical y horizontal.

Lo anterior nos permite explicar unos conceptos básicos sobre la diferencia entre la computación a la que estamos acostumbrados, que llamaremos computación clásica, y la computación cuántica. Adviértase que decimos computación y no computadoras porque no nos estamos refiriendo a máquinas sino a los programas operados en ellas. De hecho, existen computadoras clásicas pero no (o si se prefiere, aún no) computadoras cuánticas de propósito general.

Las computadoras clásicas almacenan ceros y unos en sus registros para hacer con ellos todas las operaciones que son capaces. Cada dígito almacenado, es decir, cada 0 o 1, se llama *bit*, y todo bit, en un sistema binario, solo puede ser un 0 o un 1. La computación cuántica también almacena en sus registros ceros y unos, pero además a cada dígito almacenado le asigna un valor con el cual se calcula la probabilidad de ser 0 o 1 (y la probabilidad de ser lo contrario), que a su vez varía entre 0 y 1, es decir, entre imposibilidad y certeza. En este caso no se habla de bits sino de *qubits*, y cada qubit puede tomar el valor de 0, de 1, o de cualquiera de las infinitas posiciones entre ambos números que determinan dichas probabilidades. Es como si fuera, simultáneamente, 0 y 1. En consecuencia, los algoritmos para operar con los qubits son diferentes de los utilizados para hacerlo con bits, pues escapan al sistema binario. Se puede advertir la semejanza de esto con la polarización horizontal o la vertical –que podríamos equiparar a los ceros y unos de los bits de la computación clásica–, mientras que los estados de superposición serían los de los qubits de la computación cuántica.

La ejecución de cualquier programa de computadora procede por el camino de modificar los datos registrados en su memoria, que son ceros y unos. En la computación

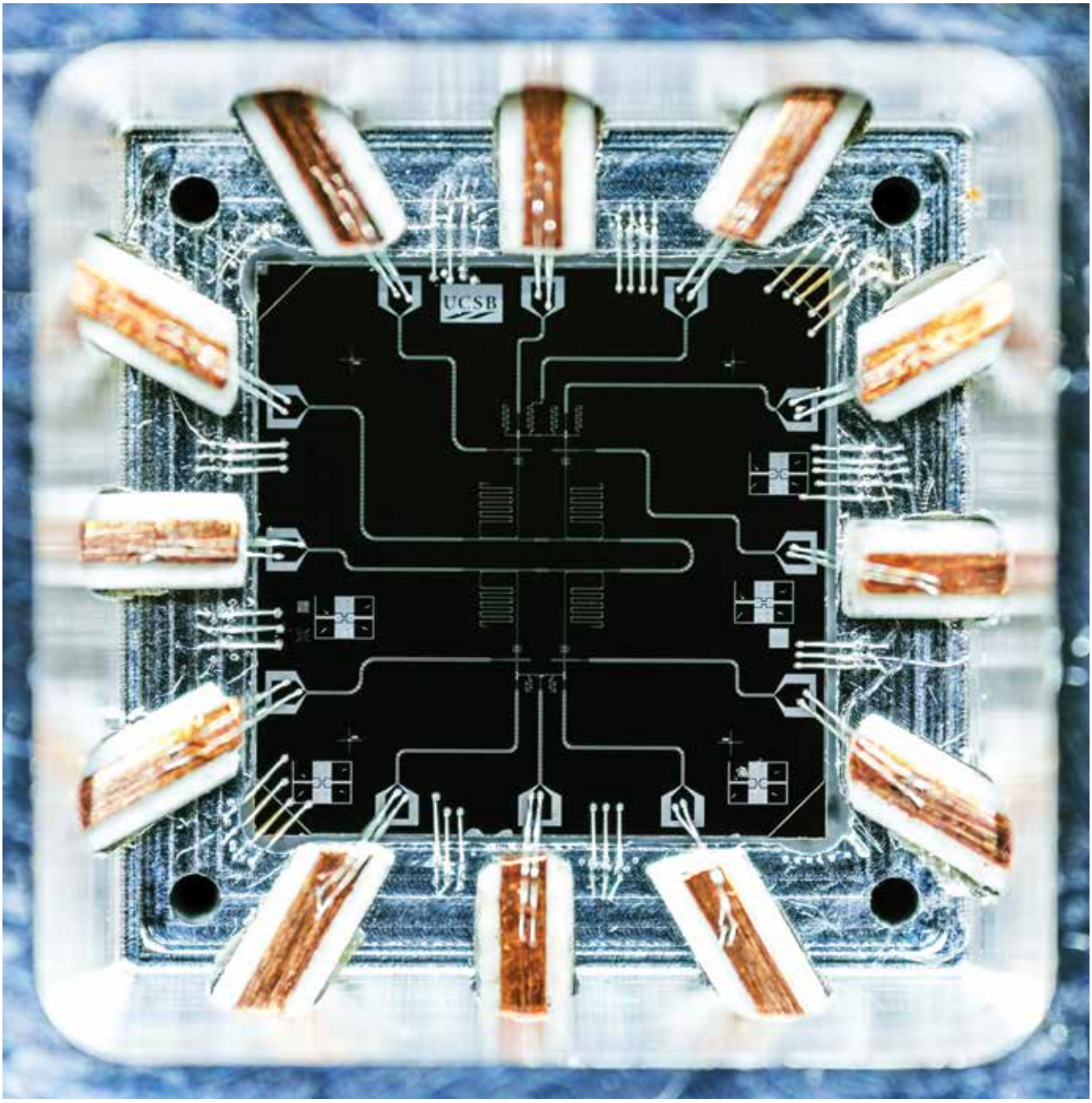

Foto Michael Fang UCSB

clásica los programas solo pueden transformar ceros en unos y unos en ceros. Pero en la computación cuántica tienen la posibilidad de modificar las probabilidades de tomar esos valores asociadas con los bits que guardan.

Volviendo al fotón y al vidrio polarizado, supongamos que disponemos de algún mecanismo que nos permita alterar la polarización del primero: si ella es horizontal, pasará a vertical y viceversa. Pero, ¿qué sucede si el fotón estaba en estado de superposición? Nuestro hipotético mecanismo se encuentra con un fotón que está simultáneamente polarizado en sentido horizontal y en sentido vertical, por lo cual actúa de las dos maneras haciendo que la probabilidad de modificarse a horizontal cuando llegue al vidrio sea ahora la de modificarse a vertical, y viceversa.

Si el hipotético mecanismo fuera un programa de computación, ejecutarlo sobre una superposición equivale a ejecutarlo simultáneamente dos veces: una sobre un fotón polarizado en sentido horizontal y otra sobre uno polarizado en sentido vertical, aunque solo arrojaría al azar uno de los resultados. La pregunta que se plantearon los especialistas en computación ante esto fue si habría cómo aprovechar esta clase de situaciones para obtener to-

dos los valores posibles encerrados en un estado de superposición con una única ejecución del programa, en lugar de obtener uno solo al azar.

En 1996, Lov Kumar Grover, un científico norteamericano nacido en la India que se desempeñaba en los laboratorios Bell, en Nueva Jersey, sugirió cómo usar este raro comportamiento cuántico para hacer la computación más eficiente, por lo menos en un caso particular. Hubo otros usos de la computación cuántica antes del que se le ocurrió a Grover, pero este es uno de los primeros programas de computación basado en la física cuántica que podrían en algún momento tener utilidad práctica (cuando exista una computadora cuántica, claro está).

El caso particular que atrajo la atención de Grover se puede ejemplificar con la situación de buscar a quién pertenece un número de teléfono y solo tener una guía impresa. Para encontrar el número se debe recorrer la guía completa buscándolo, actividad que se detendrá cuando se dé con él. En el peor caso, habrá que recorrer toda la guía y el último número será el buscado; en el mejor caso, será el primero que se vea. Digamos que, en el promedio, se recorrerá la mitad de la guía.

Grover aplicó el sistema de los fotones para hacer la búsqueda y probó que la cantidad de números que resulta necesario recorrer no crece como el promedio de los números incluidos en la guía sino como su raíz cuadrada, lo que arroja un resultado mucho menor. O sea, si hay 10.000 números de teléfono en la guía, con el sistema de la computación clásica se deberá recorrer 5000, en promedio, antes de encontrar el buscado; con el algoritmo de Grover alcanza con 100.

Dos años antes de que Grover ideara su algoritmo, otro estadounidense, Peter Shor, profesor del Instituto de Tecnología de Massachusetts, publicó uno usando computación cuántica que proporciona una ventaja aún más pronunciada. Se refiere a la factorización de números, es decir, al cálculo de cómo expresarlos en la forma de un producto de números primos. Es una operación matemática de enorme importancia porque está en la base de todos los sistemas criptográficos avanzados en uso actual.

Para números muy grandes, el procedimiento tradicional requiere realizar una desmedida cantidad de operaciones: en 2009, factorizar un número de 232 dígitos llevó dos años a un equipo de matemáticos, con la participación de cientos de computadoras. Shor demostró que con una hipotética computadora cuántica se podría hacer lo mismo en una cantidad de pasos exponencialmente menor. En otras palabras, si existiese una computadora cuántica que pudiese manipular la cantidad necesaria de qubits, se podría descifrar casi todos los sistemas de criptografía usados en estos momentos. Como contrapartida, la computación cuántica abre la posibilidad de acceder a otras maneras de encriptar, en principio seguras de los ataques de otras computadoras cuánticas, y de hecho imposibles de romper con ningún método, garantizadas por propiedades intrínsecas de la física cuántica (por lo menos si esos métodos se aplicaran de forma ideal).

En lo anterior hemos descripto el proceso con fotones como una serie de operaciones que conforman un programa, pero podríamos haberlo presentado como un experimento de laboratorio, del que señalamos los pasos a seguir y predecimos lo que sucederá en cada paso. Estaríamos concibiendo a un programa cuántico como la descripción de un experimento, y a la computación cuántica como una forma de describir experimentos físicos de manera estructurada, de suerte que ponga en evidencia la lógica de la física cuántica.

En el marco de la matemática, el concepto de lógica indica el conjunto de reglas que permiten demostrar matemáticamente la corrección de un razonamiento. Una deducción ajustada a dichas reglas arroja resultados con sentido, o, en lenguaje sencillo, conclusiones lógicas, por las que se puede confiar en la certeza matemática de las predicciones formuladas. En computación y en matemáticas existen muchos sistemas lógicos diferentes, cada uno de los cuales se aplica a construcciones conceptuales de distinto propósito. Así, hay una lógica detrás de cada lenguaje de programación. Una línea de investigación es descubrir la lógica detrás de la computación cuántica y, por extensión, detrás de la física cuántica. Esto va más allá de las ventajas de procedimiento que ofrece la computación cuántica, pues la convierte en nueva herramienta para razonar sobre el mundo tan poco intuitivo de las partículas elementales de nuestro universo. CH

LECTURAS SUGERIDAS

DUNN JM, MOSS LS & WNG Z, 2013, 'The third life of quantum logic. Quantum logic inspired by quantum computing', *Journal of Philosophical Logic*, 42, 3: 443-459, accesible en *http://arxiv.org/abs/1302.3465*.

GROVER LK, 1999, 'Quantum Computing', *The Sciences*, pp. 24-30, julio/agosto, accesible en *http://cryptome.org/qc-grover.htm*.

NIELSEN M & CHUANG I, 2000, *Quantum Computation and Quantum Information*, Cambridge University Press.

Alejandro Díaz-Caro

Doctor en ciencias de la computación, Universidad de Grenoble.

Investigador asistente del Conicet.

Profesor adjunto, Universidad Nacional de Quilmes.

alejandro@diaz-caro.info