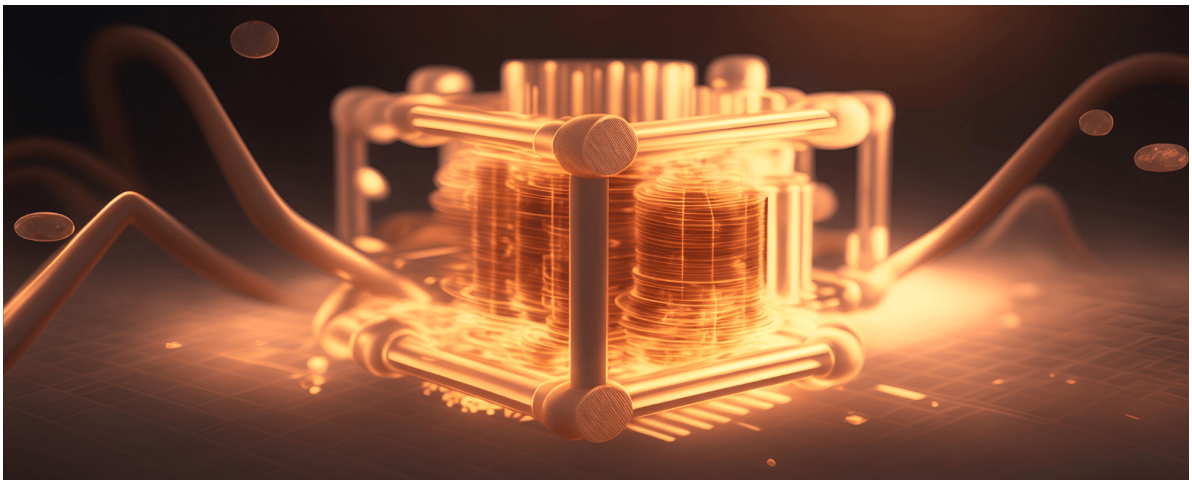
LA SEGUNDA REVOLUCIÓN CUÁNTICA

Física cuántica e información: nuevas tecnologías para el siglo XXI

Ignacio Cirac, Antonio Acín



Representación abstracta de un ordenador cuántico con partículas. Conceptualización: Luisa Quiroga

La información es un concepto clave en nuestra sociedad, que tiene un impacto muy directo en nuestro día a día: desde que nos levantamos hasta que nos metemos en la cama, se intercambian miles de mensajes por internet o las redes de datos móviles, y también se ejecutan miles de operaciones, de más o menos complejidad, en los diferentes dispositivos procesadores de información, desde supercomputadores hasta nuestros móviles mismos. La información ha modificado de tal manera la forma en que vivimos y convivimos que a menudo se conoce nuestra sociedad como la sociedad de la información. La importancia y el impacto de este concepto son fáciles de entender si se tiene en cuenta que multitud de puestos de trabajo, empresas, inversiones y decisiones políticas giran en torno a la información.

Todas las aplicaciones de información operan en bits, que no son más que su unidad básica y que pueden tomar dos valores: 0 o 1. Nuestra conexión de internet en casa o en el trabajo, la capacidad de memoria de nuestro móvil o la velocidad del procesador de nuestro portátil: todo se mide en bits. Un ordenador no es más que un dispositivo que toma información codificada en bits, realiza operaciones siguiendo los pasos descritos en un algoritmo y nos devuelve el resultado en bits. Cuando enviamos un correo electrónico a un amigo en la otra punta del planeta, la información se transmite en bits codificados en luz,

que se envían a través de una fibra óptica.

La física cuántica fue otra de las revoluciones que nos ofreció el siglo XX. Es el formalismo que explica todos los fenómenos microscópicos que nos rodean. Al tener que ver con el mundo de lo más pequeño, su impacto en nuestra sociedad no es tan evidente a simple vista. Sin embargo, esta conclusión es incorrecta, porque es superficial. Por una parte, y desde un ámbito fundamental, las predicciones de la física cuántica supusieron un cambio radical en la comprensión de la naturaleza, ya que son, en muchos aspectos, muy diferentes de las predicciones de la hasta entonces imperante física newtoniana. Por otra parte, desde un ámbito más aplicado, la física cuántica ha sido y es crucial para comprender los materiales, la química y la estructura molecular y, por lo tanto, gran parte de la ciencia y la tecnología modernas. Aplicaciones como el láser, que se utiliza desde para leer el código de barras en el supermercado hasta para complejas operaciones quirúrgicas, o el transistor, que es fundamental para el funcionamiento de cualquier ordenador, fueron sólo posibles gracias a la comprensión del mundo microscópico que proporcionó la física cuántica.

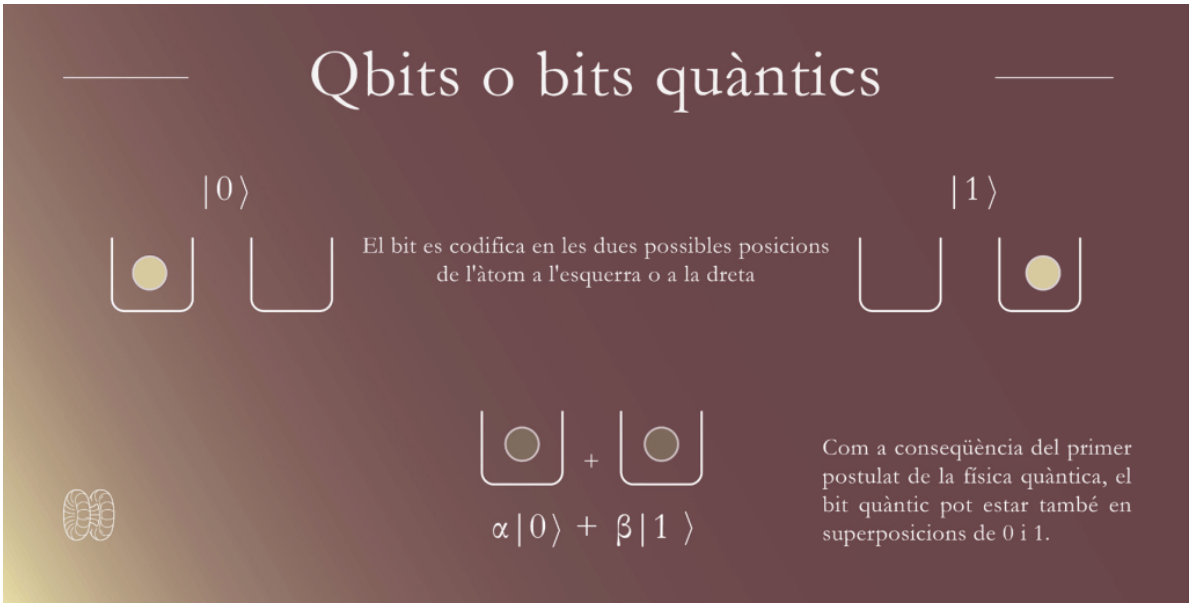
Partículas cuánticas para procesar y transmitir información: cambio de paradigma

Ya hace unas cuantas décadas, varios investigadores empezaron a plantearse qué pasaría si se combinaran la información y la física cuántica. Después de haber leído los párrafos anteriores, la pregunta puede parecer incluso sencilla y natural: ¿qué pasaría si utilizáramos partículas cuánticas, como los átomos o los fotones de luz, para transmitir y procesar información? Dicho de otra manera: ¿qué pasa si almacenamos los bits en partículas cuánticas? Pero en aquel tiempo, y aunque era una pregunta muy estimulante desde un punto de vista conceptual y teórico, era una posibilidad próxima a la ciencia-ficción, teniendo en cuenta el estado de las tecnologías. Sin embargo, las tecnologías de la información han avanzado de manera vertiginosa en las últimas décadas, e ideas que parecían más propias de la ciencia-ficción se han convertido en realidad. En particular, ya se tiene el conocimiento y las técnicas para almacenar bits en partículas cuánticas como los átomos o fotones. ¿Qué podemos esperar, entonces, de la combinación de la información y la física cuántica? Esta es la pregunta principal que la nueva disciplina de las ciencias y tecnologías de la información cuántica busca responder.

Se comprendió relativamente pronto que utilizar bits codificados en partículas cuánticas abría nuevas oportunidades para procesar y transmitir información. El mero hecho de colocar un bit en una partícula cuántica ya daba como resultado una cosa diferente de la que conocíamos. Consideramos, por ejemplo, una posible realización de un bit a través de un átomo que puede estar en dos posiciones, tal como se puede ver en la imagen: cuando está a la izquierda, el valor del bit es 0, y cuando está a la derecha, el valor es 1. Ahora abrimos cualquier libro de texto de física cuántica. No nos tenemos que asustar, ni hace falta leer mucho: hay bastante con llegar al primer postulado de la teoría, que acostumbra a aparecer en las primeras páginas. Recordamos que los postulados de una teoría no se discuten, sino que se aceptan.

> Las tecnologías de la información han avanzado de manera vertiginosa en las últimas décadas, e ideas que parecían más propias de la ciencia-ficción se han convertido en realidad. Actualmente ya se tiene el conocimiento y las técnicas para almacenar bits en partículas cuánticas como los átomos o los fotones

Pues bien, el primer postulado de la física cuántica nos dice que si una partícula cuántica puede estar en dos estados, también puede encontrarse en un estado que es la superposición de los dos estados. El concepto de superposición es difícil de asimilar, ya que las superposiciones tienen lugar en el mundo microscópico, de los átomos y las moléculas, que no vemos con los ojos, ni oímos, ni podemos tocar; en el mundo en el cual vivimos, que sí que percibimos, desaparecen. No existe, por lo tanto, una analogía que podamos utilizar para explicar la superposición: es una cosa muy especial de este mundo de lo más pequeño. Sin embargo, el hecho de que un concepto sea difícil de asimilar no significa que no sea el correcto para describir la naturaleza. Y, de hecho, el concepto de superposición cuántica es uno de los ingredientes que se utilizan para explicar los experimentos a escala microscópica. Volvemos ahora a nuestro bit codificado en la partícula cuántica: ¿qué implicaciones tiene el postulado de las superposiciones? De su aplicación se entiende que el bit cuántico, también conocido como qubit, es diferente del bit utilizado hasta ahora, el bit clásico, ya que puede estar en los dos valores habituales de 0 y 1, pero también en cualquier superposición de estos valores. La unidad básica de información cuántica, el qubit, es, por lo tanto, más rico que su análogo clásico.



Representación gráfica de los qbits o bits cuánticos.

Los ordenadores cuánticos

A partir de esta observación, vale la pena revisitar todos los usos que hacemos de la información y ver cómo se modifican bajo los fenómenos de la física cuántica, como por ejemplo las superposiciones mencionadas. ¿Cómo podemos calcular y resolver problemas cuando los codificamos en bits cuánticos? Esta pregunta lleva de manera inmediata a la idea del ordenador cuántico. ¿Qué es un ordenador cuántico? Para responder a esta pregunta, es útil recordar de nuevo qué es un ordenador clásico: una máquina que coge información codificada en bits, sobre los cuales hace una serie de transformaciones para resolver un problema, cuya solución nos devuelve de nuevo en bits. Aunque pueda parecer obvio, un ordenador cuántico no es nada más que la translación de esta idea a un entorno cuántico: una máquina que es capaz de procesar información en bits cuánticos para resolver problemas. La diferencia, sin embargo, radica en el hecho que este procesamiento se lleva a cabo utilizando los fenómenos de la física cuántica, que no tienen análogo en nuestro mundo macroscópico clásico y que, por lo tanto, son inaccesibles a nuestros ordenadores clásicos actuales. Es decir, el ordenador cuántico puede utilizar más operaciones, tiene a su disposición más herramientas para resolver problemas complejos y, en consecuencia, puede llegar a proporcionar soluciones a estos problemas de manera mucho más eficiente. A esta situación se la conoce también como ventaja cuántica (en inglés, *quantum advantage*). Este hecho no se tiene que interpretar como que todos los problemas se resolverán de manera más eficiente en un ordenador cuántico y, de hecho, existen problemas para los cuales un ordenador cuántico y uno clásico ofrecen el mismo rendimiento. Pero al mismo tiempo se conocen otros problemas para los cuales sí que se obtiene una ventaja computacional cuántica.

Siguiendo con aplicaciones de computación, un campo muy activo y de gran actualidad es el del aprendizaje automático (en inglés, *machine learning*), donde se entrenan ordenadores con muchos datos para que aprendan y nos permitan resolver problemas relevantes. ¿Cómo aprende un ordenador cuántico? Esta es, de nuevo, una pregunta fundamental con potenciales aplicaciones prácticas: es lo que busca responder el aprendizaje automático cuántico.

Criptografía cuántica

Pero sabemos que la información se utiliza para miles de aplicaciones más allá de la computación. Por ejemplo, para establecer una red de comunicaciones a escala global, internet, donde los bits son transmitidos a cualquier parte del planeta. ¿Cuál sería la estructura de un internet cuántico, donde el objetivo es transmitir bits cuánticos entre dos puntos cualesquiera? ¿Cuáles son las leyes de la comunicación cuántica? Y un aspecto clave en las comunicaciones actuales es el de la privacidad: casi tan importante como el hecho de poder enviar información de un sitio a otro es poder hacerlo de manera segura, a fin de que un posible espía o enemigo no tenga acceso a los mensajes que se envían. El campo de la criptografía nos proporciona las herramientas para diseñar métodos de transmisión

privada. En este caso, los bits cuánticos vuelven a abrir nuevas posibilidades para la encriptación de información y permiten diseñar los llamados *protocolos de criptografía cuántica,* que proporcionan un nuevo tipo de seguridad basada en las leyes de la física cuántica.

Podemos seguir enumerando todos los posibles usos de la información en nuestra sociedad e intentar entender cómo se ven afectados por las leyes de la física cuántica. No lo haremos en esta introducción, porque no es su objetivo, y porque el resto del monográfico de la revista IDEES presenta diferentes artículos que analizan muchas de estas posibles aplicaciones. Algunas, como los ordenadores o la comunicación cuántica, son muy naturales; otras son más especulativas. Por ejemplo, los ordenadores se utilizan actualmente para componer música, por lo cual podemos plantearnos cómo generar música utilizando efectos cuánticos. Las contribuciones de este monográfico de la revista IDEES sirven, por lo tanto, para presentar una visión más detallada y completa del campo.



Conclusiones

Nos gustaría concluir esta introducción con dos mensajes. El primero tendría que ser claro: la información es un concepto crucial en nuestra sociedad y la física cuántica nos proporciona nuevas herramientas para su procesamiento y transmisión. Este mensaje ya ha sido asimilado a escala mundial y se están llevando a cabo importantes iniciativas e inversiones por parte de grandes y pequeñas empresas, o entidades gubernamentales. En nuestro entorno local, la Comisión Europea lanzó ya hace unos años el buque insignia cuántico Quantum Flagship, una iniciativa paneuropea en tecnologías cuánticas. Estamos en un momento muy interesante, de gran actividad, en el cual todos los actores relevantes trabajan de manera conjunta para entender cómo pueden explotar todo el potencial de las tecnologías cuánticas.

No obstante, existe una gran complejidad a la hora de operar con superposiciones cuánticas: cualquier aplicación de información cuántica, como por ejemplo un ordenador cuántico, hace operaciones en bits cuánticos. Para obtener una ventaja es necesario, si bien no suficiente, que estos bits estén en estados de superposición. Sin embargo, en la práctica, mantener las superposiciones es complicado, ya que cualquier interacción no controlada con el entorno las puede destruir. Esta fragilidad de los efectos cuánticos explica por qué el desarrollo de las tecnologías de la información cuántica todavía tiene que resolver importantes desafíos.

> Casi tan importante como el hecho de poder enviar información de un sitio a otro es poder hacerlo de manera segura. La criptografía cuántica abre nuevas posibilidades para la encriptación de información y permite diseñar protocolos que proporcionan un nuevo tipo de seguridad

El segundo mensaje es una llamada a un optimismo prudente o a una prudencia optimista. Preparar, manipular, almacenar y transmitir qubits es mucho más complicado que en el caso de los bits clásicos. Si el bit cuántico deja de estar en una superposición, se convierte en un bit clásico que sólo toma los valores de 0 o 1, y se pierde cualquier ventaja cuántica. Pero mantener las superposiciones es una tarea compleja, ya que el ruido y las interacciones no controladas con el entorno las destruyen. Es necesario, por lo tanto, preparar y procesar los qubits en un entorno aislado del exterior, por ejemplo, a muy baja temperatura, y que podamos manipular de manera controlada. Aquí radica el gran desafío tecnológico. Eso explica por qué, a pesar de años de esfuerzo, los ordenadores cuánticos o esquemas de comunicación cuántica existentes presenten todavía importantes desafíos que limitan la implementación práctica. El camino no es sencillo y está lleno de obstáculos. Pero la motivación y el objetivo final están claros, y existen diferentes resultados que demuestran que las tecnologías de la información cuántica permitirán resolver problemas que en la actualidad limitan nuestro progreso y bienestar como sociedad.



Ignacio Cirac

Juan Ignacio Cirac Sasturáin es director de la División Teórica del Instituto Max Planck de Óptica Cuántica de Garching (Alemania) y profesor honorario de la Universidad Técnica de Múnic. Doctor en Ciencias Físicas por la Universidad Complutense de Madrid, es especialista en tecnologías cuánticas y uno de los expertos con mayor reconocimiento mundial en el ámbito de la computación cuántica. Es miembro de las academias de ciencias española, alemana y bávara. Ha recibido numerosos premios y reconocimientos, entre ellos el Premio Príncipe de Asturias, las medallas Benjamin Franklin, Max Planck y Niels Bohr, el Premio BBVA Fronteras del Conocimiento, el galardón en Computación Cuántica de la Fundación Micius y el Premio Wolf, considerado como la antesala del Nobel. Sus investigaciones han sido cruciales para avanzar en la teoría que sustenta el desarrollo de los ordenadores cuánticos.



Antonio Acín

Antonio Acín Dal Maschio es profesor ICREA en el Instituto de Ciencias Fotónicas (ICFO), donde dirige el grupo de Teoría de la Información Cuántica. Doctor en Ciencias Físicas por la Universidad de Barcelona, es especialista en tecnologías cuánticas. Su trabajo de investigación ha sido reconocido por cuatro becas del Consejo Europeo de Investigación (European Research Council, ERC). Desde 2016, dirige la Cátedra AXA en Ciencias de la Información Cuántica.