Procesamiento cuántico de la información

La mecánica cuántica ofrece nuevas formas de procesamiento y transmisión de información. Para llevar a cabo cualquiera de estas aplicaciones, se debe combatir la decoherencia, el ruido que degrada las propiedades cuánticas de todo sistema

Antonio Acín

Supongamos que se almacena información en el estado de un átomo o de un fotón de luz, partículas cuyo comportamiento se rige por las leyes de la mecánica cuántica. ¿Implica algún cambio en el procesamiento y transmisión de la información? En los últimos años, una nueva disciplina científica pretende dar respuesta a esa pregunta: la teoría de la información cuántica. Ha emergido de la combinación de diferentes aspectos de la física teórica y aplicada con la teoría de la información y la computación. Se propone analizar qué posibilidades le ofrecen las leyes de la mecánica cuántica al procesamiento y a la transmisión de información. Gracias a este enfoque, se han encontrado espectaculares aplicaciones (como la criptografía cuántica o la teleportación cuántica) que desafían la comprensión *clásica* de la realidad. Nuestra intuición sólo está acostumbrada a razonar según dicta el entorno, donde los efectos cuánticos son imperceptibles y la mecánica clásica (o newtoniana) ofrece una descripción satisfactoria de los fenómenos que se observan. Por ejemplo, nadie se ha encontrado nunca delante del famoso gato de Schrödinger, vivo y muerto al mismo tiempo. Por ello, una de las primeras recetas que hay que seguir a la hora de afrontar y analizar las nuevas propuestas de la teoría de la información cuántica consiste en abstenerse de buscarles explicaciones *clásicas*. Se debe realizar un esfuerzo intelectual y acostumbrarse a pensar de un modo *cuántico*, aceptando e intentando explotar al máximo las nuevas reglas de juego que este formalismo nos ofrece. En mi opinión, si la teoría de la información cuántica parece un campo apasionante y siempre sorprendente, es porque nos "obliga" a renunciar a la intuición.

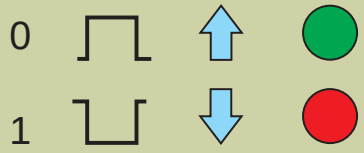
Históricamente, la mecánica cuántica fue la respuesta a una serie de problemas que aparecieron a finales del siglo XIX y principios del siglo XX, cuando la física experimental permitió la observación de fenómenos a escala atómica. Surgieron entonces nuevas preguntas que requirieron nuevas respuestas, y éstas llevaron de manera más o menos natural a la mecánica cuántica tal y como hoy la concebimos. Hacia finales de los años treinta, se había elaborado la mayor parte de la formulación teórica de la mecánica cuántica. ¿Por qué, pues, tardaron alrededor de medio siglo en aparecer los primeros resultados relativos a la información? Una primera y sencilla razón es que en aquella época no existía una formulación de la teoría de la información. Los trabajos de Shannon que establecieron las bases de la teoría de la información datan de 1949. Esta simple respuesta justifica en parte el retraso entre la finalización del desarrollo teórico de la mecánica cuántica y el nacimiento de la información cuántica. Pero no es suficiente para explicar las razones por las cuales no se pensó en la posible aplicación de las leyes cuánticas al procesamiento de la información hasta principios de los años ochenta.

A partir de entonces diversos investigadores empiezan a plantearse la siguiente situación: si el progreso técnico de los dispositivos de transmisión y procesamiento de la información prosigue en su tendencia actual, se alcanzará la escala atómica en un tiempo razonable. Para representar esta evolución se recurre a la ley de Moore. En 1965, Gordon Moore observó un comportamiento exponencial en el cambio a lo largo del tiempo del número de transistores por circuito integrado y predijo que esta tendencia continuaría.

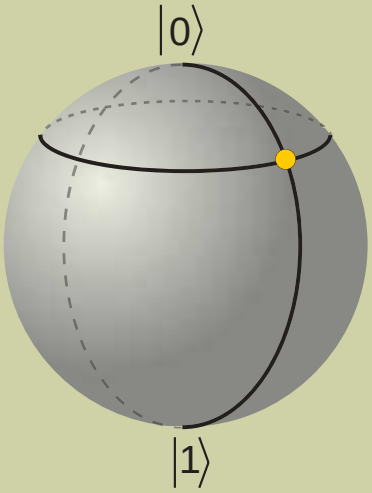
La predicción de Moore ha venido cumpliéndose hasta el día de hoy con sorprendente exactitud. Suponiendo que esta tendencia siga manteniéndose, ¡la ley muestra que la información se codificará en átomos hacia el año 2030! Parecerá demasiado optimista, pero es una indicación razonable de que la técnica alcanzará pronto el mundo microscópico, donde las leyes cuánticas gobiernan el comportamiento de los dispositivos físicos. Por lo tanto, hay que analizar el grado en que estos efectos modificarán la manera de transmitir y procesar la información. Una primera opción habría sido conservadora: evitar que las peculiaridades cuánticas modificasen los resultados ya establecidos. La opción escogida por los investigadores de la teoría de la información cuántica fue más ambiciosa: explotar las posibilidades que ofrecerá el futuro entorno cuántico para diseñar nuevas aplicaciones.

El bit cuántico

El bit clásico puede tomar dos valores posibles, el 0 y el 1 lógicos. Ejemplos de realización de un bit son:



Todas estas realizaciones codifican la misma cantidad de información: un bit.



EL BIT CUANTICO O QUBIT se puede representar como un punto en la llamada esfera de Poincaré. Los polos se asocian con los estados $|0\rangle$ y $|1\rangle$. Cualquier superposición de estos dos estados genera un punto en la esfera, único. Por tanto, el valor del bit cuántico se puede especificar por medio de dos ángulos, la longitud y la latitud.

¿Por qué decimos que la información es cuántica o clásica?

Uno de los resultados teóricos más espectaculares del nuevo campo de la teoría de la información cuántica es el algoritmo cuántico de Shor para la factorización en números primos. Es decir, dado un número inicial N, ¿podemos encontrar dos números primos tales que su producto sea N? La respuesta no entraña especial dificultad si N consta de un número modesto de dígitos, pero el problema se complica mucho cuando es grande, tanto, que no existe en la actualidad un algoritmo eficiente para resolverlo. Estamos por lo tanto ante un problema complejo.

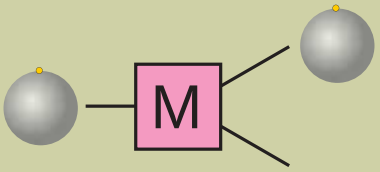
En 1994, Peter Shor propuso un algoritmo de factorización eficiente que se servía de las nuevas posibilidades ofrecidas por las leyes de la mecánica cuántica. Para hacerse una idea de la diferencia entre los dos modos de procesar, imaginemos que debe factorizarse un número de 300 dígitos. El mejor algoritmo clásico requeriría alrededor de 10^{24} pasos, mientras que el algoritmo cuántico de Shor necesitaría sólo 10^{10}. Pese a la aparente artificialidad del problema de la factorización, sobre él reposan gran parte de los métodos actuales de encriptación de información. Por lo tanto, un espía dotado de un ordenador cuántico —algo impensable con la técnica actual— podría leer muchas de las comunicaciones secretas de hoy en día.

Recuerdo que en una ocasión Rolf Tarrach, de la Universidad de Barcelona, contó que había impartido un seminario ante matemáticos acerca de este algoritmo. Reaccionaron con bastante escepticismo; estaban imbuidos de la formulación clásica de la información, donde no existe ningún método de factorización eficiente. He encontrado reacciones similares al intentar explicar la criptografía cuántica a expertos en criptografía clásica. En ciertas ocasiones me ha parecido observar en sus caras la sensación de que yo estuviera haciendo “trampas” al adoptar unas reglas que no se ajustaban a la teoría de la información matemática por ellos conocida. ¡Y, por supuesto, tienen razón! Suele creerse que la teoría de la información es abstracta y matemática

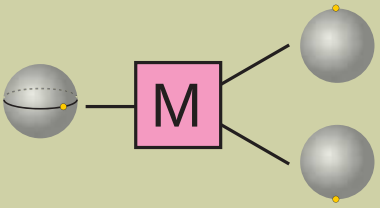
ANTONIO ACIN

Las paradojas cuánticas

El proceso de medición puede modificar el estado de un sistema. Aun habiendo preparado el sistema en un estado conocido, existen situaciones experimentales para las cuales sólo podemos dar la descripción en términos probabilísticos.

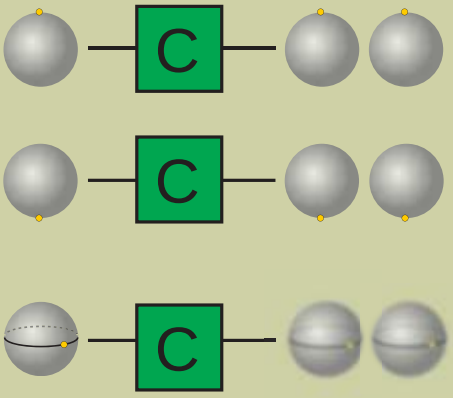


Si se prepara un estado en uno de los polos de la esfera de Poincaré y se mide según esa misma dirección, sólo un resultado es posible y la medida no afecta al sistema.



Si se prepara el bit cuántico en el ecuador de la esfera y se aplica la misma medida, se tienen dos resultados con igual probabilidad, y el estado inicial se ve modificado.

Teorema de la no-clonación: no existe una máquina capaz de clonar de manera perfecta todos los estados de un bit cuántico.



Es posible diseñar una operación cuántica que clone de manera perfecta los dos polos de la esfera de Poincaré. La misma máquina copia de manera imperfecta, con errores, estados en el ecuador de la esfera.

y está firmemente establecida. Sin embargo, al codificar la información en dispositivos físicos distintos, se tienen diferentes posibilidades y limitaciones. Como dijo Rolf Landauer, de IBM, "information is physical" (la información es un ente físico). Hablaremos, pues, de información cuántica o clásica, de bits clásicos o cuánticos, dependiendo de los dispositivos físicos con que se codifique la información. Las reglas de juego, y las posibilidades que ofrecen, cambiarán según la situación.

La coherencia cuántica: bit cuántico y entrelazamiento

La unidad básica en la teoría clásica de la información es el bit, que puede tomar dos valores: 0 y 1. Un pulso de luz o un interruptor codifican de manera sencilla un bit. Por supuesto, existen infinitos modos de codificar un bit clásico mediante un dispositivo físico; desde el punto de vista de la información clásica que poseen, todas son equivalentes.

Supongamos ahora que el bit se codifica en un sistema cuántico que puede tomar dos estados, $|0\rangle$ y $|1\rangle$. Un postulado básico de la mecánica cuántica establece que, si un sistema cuántico puede tomar dos valores distintos, también podrá tomar cualquier superposición coherente de ellos. Por ejemplo, el sistema podrá hallarse en el estado resultado de la combinación de $|0\rangle$ y $|1\rangle$ con los mismos pesos. Debe resaltarse que esta superposición es coherente; es decir, el caso anterior no equivale a declarar que el estado del sistema es igual a $|0\rangle$ o $|1\rangle$ con probabilidad un medio, sino que es mitad $|0\rangle$ y mitad $|1\rangle$, ¡al mismo tiempo! Pero ésta no es más que una de las posibles superposiciones que se pueden tener de $|0\rangle$ o $|1\rangle$. De hecho, se pueden crear múltiples combinaciones: es infinito el número de estados accesibles. Por lo tanto, el bit cuántico (o qubit), la unidad básica de información cuántica, puede ser $|0\rangle$, $|1\rangle$ o cualquier combinación de tales estados en grados distintos. Para representar gráficamente esta riqueza se acude a la esfera de Poincaré (*véase el recuadro* El bit cuántico). En esa imagen, cada bit cuántico se corresponde con un punto de la superficie de la esfera. Se puede entender la sorpresa del lector no acostumbrado al formalismo cuántico ante los estados de superposición. En nuestro entorno no existen pulsos de luz que se hallen en una superposición de apagado y encendido (o gatos vivos y muertos). Pero debemos hacer un esfuerzo y aceptar las nuevas reglas de juego, que por otra parte han sido verificadas por multitud de experimentos.

Físicamente, un bit cuántico suele realizarse con el espín de un átomo o la polarización de un fotón. Como sucede en el caso del bit clásico, todas estas operaciones son equivalentes desde el punto de vista de la información cuántica que poseen.

Consideremos ahora un caso ligeramente más complicado, con dos bits cuánticos. Dos posibles estados del sistema serán $|00\rangle$ y $|11\rangle$. Pero del mismo modo que antes, otro estado posible será la superposición coherente de $|00\rangle$ y $|11\rangle$. En este caso, no podremos especificar las propiedades individuales de cada qubit, sino que sólo cabrá dar las propiedades de los dos bits como entidad global. Los dos bits se encuentran en un estado entrelazado, en el cual las propiedades de uno se ligan, o correlacionan, fuertemente con las del otro. Este tipo de correlaciones entre partículas cuánticas escapa a cualquier explicación clásica y constituye una de las propiedades clave de la mayoría de las aplicaciones de teoría de la información cuántica. El entrelazamiento (en inglés, *entanglement*) es un recurso básico de la información cuántica. Su importancia es capital. Como

ANTONIO ACÍN

hemos visto, el entrelazamiento no es más que una consecuencia de la posibilidad de tener superposiciones coherentes de estados en un sistema de más de una partícula.

¿Por qué nuestro entorno no es cuántico?

Hacerse una idea intuitiva de qué significa una superposición coherente de estados resulta complicado. No tenemos nada a nuestro alrededor que presente esas propiedades; efectos de ese tipo se manifiestan experimentalmente sólo cuando se desciende a la escala microscópica. Cabe preguntarse, pues, por el motivo de que las propiedades cuánticas no aparezcan a escala macroscópica y por la naturaleza de la transición entre las descripciones clásica y cuántica de la realidad.

Los sistemas macroscópicos, compuestos de un gran número de partículas, son complejos. Se produce en ellos una gran cantidad de interacciones. Aislar completamente un sistema dado es difícil. Se deben controlar tantos grados de libertad, que resulta muy complicado impedir que el sistema no interactúe con su entorno. Este proceso indeseado de interacción afecta profundamente a las propiedades cuánticas de un sistema. Los estados de superposición se transforman y pierden su coherencia. Así, un estado que sea la superposición coherente de $|0\rangle$ y $|1\rangle$ se convierte en una superposición incoherente de $|0\rangle$ y $|1\rangle$. En este caso obtenemos una descripción del sistema a la que estamos acostumbrados: su estado es $|0\rangle$ o $|1\rangle$ con probabilidad un medio. Debe tenerse muy en cuenta la irreversibilidad de este proceso. Sólo se podría recuperar la coherencia a partir del entorno. Pero, al no controlarse la interacción con éste, no hay forma de deshacer los cambios y devolver el sistema cuántico a su estado inicial.

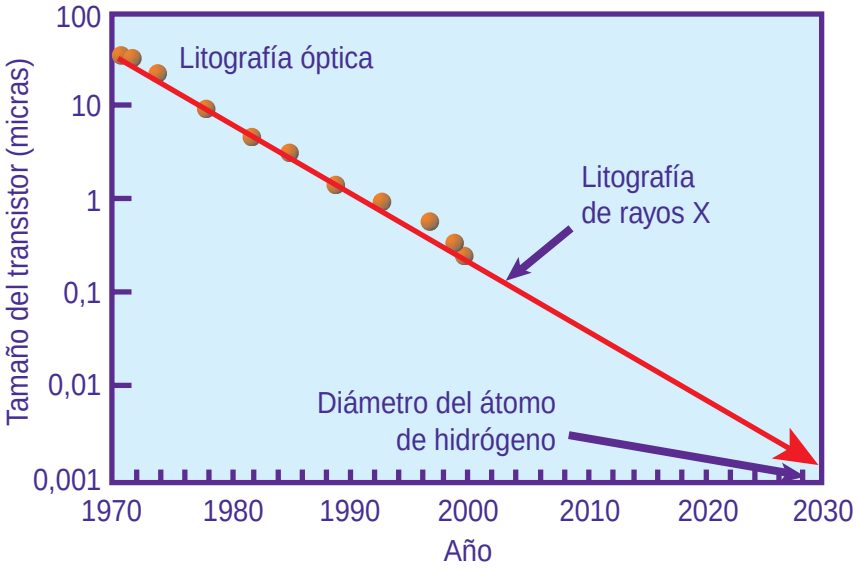
La interacción indeseada con el entorno causa, pues, la decoherencia, o pérdida de coherencia, de un sistema cuántico. En situaciones de alta decoherencia no es posible mantener estados de superposición; sus propiedades de coherencia se pierden rápidamente. Ello implica que el bit cuántico no tendrá a su disposición todas las posibilidades de la esfera de Poincaré; toda esa riqueza, la perderemos. Del mismo modo, no habrá estados entrelazados, superposiciones coherentes de $|00\rangle$ y $|11\rangle$, de importancia capital en la teoría de la información cuántica.

La decoherencia, en resumidas cuentas, hace que los dispositivos que almacenan y codifican la información pierdan sus propiedades cuánticas. Se vuelve entonces a la situación habitual hasta hace poco: la descripción de los dispositivos corresponde a la mecánica clásica (*véase el recuadro* "Superposiciones coherentes"). Todo procesamiento efectuado con ellos conducirá a los conocidos resultados de la teoría clásica de la información. Ninguna de las nuevas aplicaciones que aporta la teoría de la información cuántica podrá llevarse a cabo en situaciones de fuerte decoherencia.

Las paradojas cuánticas

Los estados de superposición y el entrelazamiento son fenómenos cuánticos, sin análogo clásico. Constituyen un ejemplo de lo que a veces se denominan "paradojas cuánticas", resultados del formalismo cuántico que escapan a nuestra intuición. Hay otras "paradojas cuánticas"; por ejemplo, que el proceso de medición de un sistema cuántico modifique el propio sistema o que, por mucho que se prepare un sistema cuántico de una manera perfectamente controlada, haya situaciones experimentales para las cuales sólo se podrá dar una respuesta probabilista (recordemos el "Dios no juega a los dados" de Albert Einstein). Menos conocido, pero fundamental en teoría de la información cuántica, es el teorema de la imposibilidad de la clonación. De acuerdo con el mismo, no existe una operación capaz de producir una copia idéntica de cualquier estado cuántico. Se podría diseñar, por ejemplo, una máquina que clonase los dos polos de la esfera de Poincaré, pero las copias de los estados que caen en el ecuador producidas por esa misma máquina serían imperfectas (*véase el recuadro* "Las paradojas cuánticas").

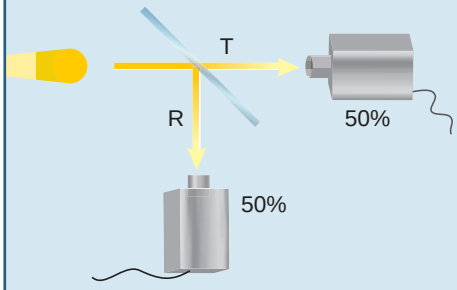
Hasta hace poco, la actitud común entre los físicos ante estos principios ha sido la de mirar hacia otro lado. Comparados con el enorme éxito de la mecánica cuántica a la hora de predecir los datos experimentales, estos resultados se han presentado con un halo negativo, que hay que aceptar y asumir, y para los que, "desgraciadamente", no existe alternativa. El enfoque de la teoría de la información cuántica es el opuesto: no sólo hay



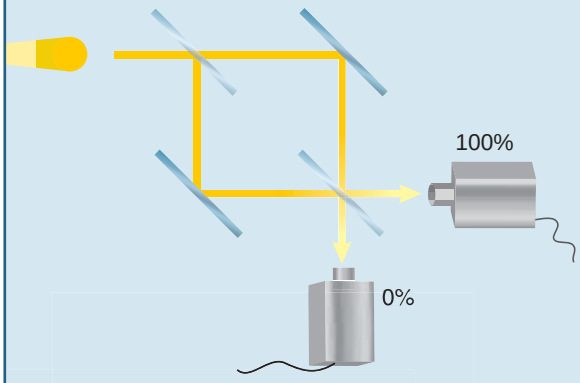
1. EN 1965, Gordon Moore, cofundador de Intel, observó un aumento exponencial con el tiempo del número de transistores por circuito integrado y predijo que este comportamiento se mantendría. En la actualidad, la "ley" de Moore ha venido cumpliéndose, de tal manera que cada 18 meses ese número se multiplica por dos. Ello implica que el tamaño de los dispositivos físicos que almacenan la información decrece de un modo exponencial. Asumiendo que esta tendencia se mantenga, se alcanzarán las escalas microscópicas, donde los efectos cuánticos son relevantes, hacia el año 2030.

ANTONIO ACIN

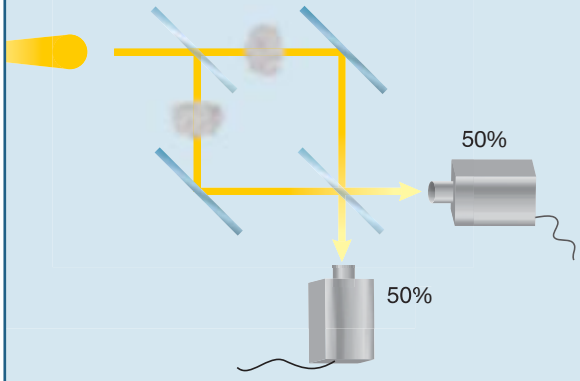
Superposiciones coherentes



1 Un fotón de luz incide sobre un espejo semitransparente, que transmite la luz con probabilidad 1/2.El fotón resultante se encuentra en un estado que llamaremos "superposición coherente" de fotón transmitido (es decir, que toma el camino T) y reflejado (que toma el camino R). Vamos a ver qué se quiere decir con esto. Si colocamos dos detectores y repetimos el experimento N veces, cada uno de los detectores medirá el fotón N/2 veces. Hasta aquí, los resultados de las medidas pueden ser también explicarse si se supone que el fotón se encuentra en una superposición "incoherente" de transmitido o reflejado, es decir, que el fotón toma uno de los dos caminos el 50% de las veces y el otro el 50% restante.



2 Supongamos que el fotón a la salida del primer espejo se encontrara en una superposición probabilística clásica, esa que hemos llamado incoherente, de T y R. Al combinar los dos caminos con espejos totalmente reflectantes sobre un segundo espejo semitransparente, se esperaría encontrar el fotón en cada uno de los detectores con probabilidad 1/2. Sin embargo, ¡existen configuraciones en las que sólo uno de los detectores mide el fotón! Es así porque las dos posibilidades se interfieren de manera constructiva para uno de los detectores, y destructiva para el otro. Por lo tanto, el estado del fotón a la salida del primer espejo no puede ser una mera combinación de T o R con probabilidad 1/2, sino que es una superposición coherente de fotón transmitido y reflejado.



3 Finalmente, supongamos que el fotón a la salida del primer espejo se ve afectado por decoherencia, o interacción incontrolada con el entorno. El estado pierde la coherencia y se transforma en una superposición incoherente de fotón transmitido o reflejado. Como consecuencia de este proceso, al repetir el montaje anterior el fotón puede encontrarse con igual probabilidad en cualquiera de los dos detectores. La interferencia constructiva/destructiva que se observaba anteriormente se ha perdido. Ahora, es de nuevo posible ofrecer una explicación del experimento suponiendo que el fotón toma cualquiera de los dos caminos posibles con igual probabilidad.

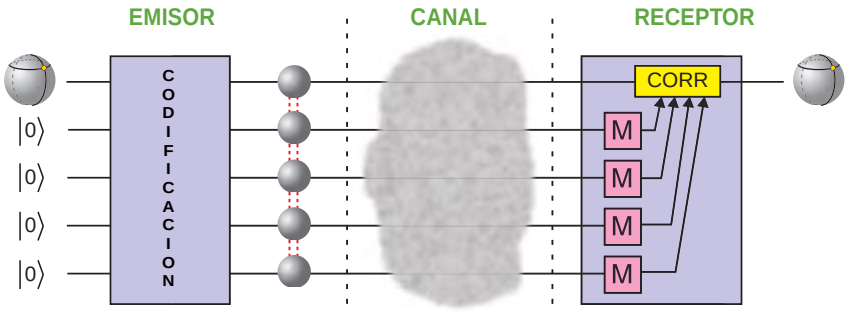
que aceptar estas paradojas, sino utilizarlas para nuestro provecho. Nos encontramos ante situaciones sin un paralelo clásico. Por lo tanto, encierran la posibilidad de dar lugar a nuevas formas de procesamiento de información. En opinión de Nicolas Gisin, de la Universidad de Ginebra, un ejemplo claro de ello es la criptografía cuántica. La medición modifica el sistema. Supongamos que un emisor envía información a un receptor codificada en un estado cuántico y que una tercera persona intenta leerla sin autorización. El efecto que esa medición causará en el estado cuántico enviado producirá errores en la transmisión. Las partes autorizadas podrán entonces detectar la presencia del espía y detener la comunicación insegura. Esta es la idea general detrás de cualquier protocolo de criptografía cuántica. Como vemos, no presenta demasiada complejidad, una vez se tienen nociones básicas de mecánica cuántica, pero sí presupone un cambio de enfoque.

Podríamos, por tanto, afirmar que, desde el punto de vista de la información cuántica, "cuanto más cuántico, mejor". Pero los efectos cuánticos de que estamos hablando aquí son imperceptibles en situaciones de gran decoherencia. Esta aparece, pues, como el enemigo del procesamiento de información en estados cuánticos. Si las condiciones experimentales no permiten una interacción controlada con el entorno, la descripción puede realizarse por medio de la mecánica clásica; no cabe esperar entonces ninguna mejora respecto a la teoría ya conocida. Es evidente que desde un punto de vista práctico es imposible contar con un sistema perfectamente aislado. El mismo proceso de observación de un sistema, la "lectura" de la información, implica una interacción

ANTONIO ACIN

con el entorno, en este caso el observador. Por lo tanto, la única solución consiste en garantizar unos niveles de decoherencia bajos y con un grado de control aceptable, y, luego, dar con un modo de procesar la información ante este tipo de situaciones. Hay que aprender a procesar y transmitir información cuántica en entornos reales con modesta decoherencia.

Detengámonos en dos de las mejores soluciones del problema: la corrección cuántica de errores y la destilación de entrelazamiento. Estas técnicas persiguen proteger la información cuántica del ruido, es decir, de las interacciones no deseadas con el entorno.



2. PARA CORREGIR ERRORES, el emisor que recibe el qubit que debe transmitirse prepara cuatro estados (cuatro bits) extra. La información se codifica en un estado entrelazado de los cinco bits cuánticos, que se envían a través del canal. Al propagarse por el canal ruidoso, esos bits cuánticos sufren decoherencia, lo que se traduce en errores. El receptor realiza medidas (M) sobre cuatro de los qubits, cuyos resultados le dan información del error que se ha producido en el canal. Esto le permite corregir (CORR) el quinto qubit y recuperar el estado de partida.

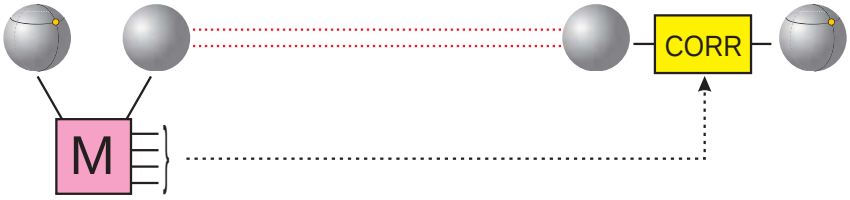
Corrección cuántica de errores

Una posible solución para combatir la decoherencia consiste en la corrección cuántica de errores. Si bien cabe ver en este método la traducción a un entorno cuántico de los protocolos clásicos de corrección de errores, éstos deben acomodarse a las nuevas propiedades cuánticas. Las soluciones deben ser más imaginativas de lo esperado a priori.

Las técnicas de corrección de errores pueden aplicarse a cualquier proceso donde se necesite un procesamiento cuántico de información que resista bien la decoherencia. Sin embargo, en aras de la simplificación e inteligibilidad, el análisis se hará para una situación de comunicación cuántica donde un emisor tiene que enviar información, codificada en un estado cuántico, a través de un canal con ruido. Supongamos que el emisor codifica un bit cuántico en la polarización de un fotón, que envía por una fibra óptica. Al propagarse por la fibra, el fotón interacciona con el material, con las moléculas que la componen; se producen efectos de decoherencia. El estado cuántico que el receptor capta es un estado ruidoso que conserva parte de la información enviada por el emisor. ¿Cómo se reconstruye la información original sin errores (es decir, con una probabilidad de error tan pequeña como se requiera)?

En este punto, vale la pena adelantar algunas ideas generales acerca del funcionamiento de los métodos de corrección de errores clásicos. Supongamos que se codifica un bit clásico en un pulso de luz que tomará dos valores, el 0 y 1 lógicos. En su propagación a través del canal, el pulso puede sufrir errores y lo que era un 0 convertirse en 1, y viceversa. Denotaremos por e la probabilidad de tener un error; la llamaremos tasa de error. Siempre podemos tomar e menor que un medio: si la probabilidad de error fuera mayor que la de que no lo hubiese, el receptor sabría que tendría que permutar el símbolo recibido para encontrarse en una situación donde $e < 1/2$.

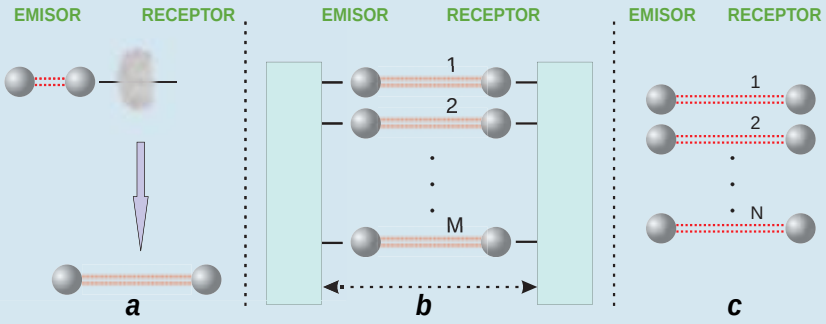
Una manera estándar de corregir los errores recurre a la redundancia: envía por el canal ruidoso varios pulsos con la misma información. En este caso, el bit lógico se codifica con más de un pulso de luz. El receptor, tras recibir y leer todos los pulsos, toma el valor más frecuente como bit enviado y prepara un nuevo estado si es necesario. Por ejemplo, supongamos que la probabilidad de error es de un 15 % y que el emisor utiliza cinco pulsos de luz para codificar el bit lógico. Si se produce un error en los pulsos, el receptor será capaz de reconstruir la información enviada, puesto que cuatro de los cinco pulsos no habrán sufrido error. En cambio, se tendrá un error en la recepción del mensaje cuando tres, cuatro o los cinco pulsos hayan experimentado un error en la propagación. La nueva probabilidad de error se verá entonces rebajada a aproximadamente un 2,66 %. No cuesta convencerse de que la probabilidad de error final puede hacerse tan pequeña como se quiera, si bien no nula, incrementando el número de pulsos que codifican un mismo bit lógico. Fijado el error final, el número de pulsos requerido dependerá de las propiedades de ruido del canal, es decir, de la tasa de error e. La redundancia constituye uno de los



3. PARA TELEPORTAR un bit cuántico, el emisor comparte con el receptor un estado máximamente entrelazado de dos bits cuánticos. El emisor realiza una medida del qubit a transmitir más la mitad que posee del estado entrelazado. Comunica el resultado obtenido (entre cuatro posibles) al receptor. El receptor, tras haber recibido la información (clásica) del resultado de la medida, realiza una operación sobre la mitad del estado entrelazado que tiene, con lo que consigue el estado que debía ser enviado sin error. Se debe notar que la partícula que contiene el estado cuántico a transmitir no se mueve del emisor, que sólo transmite el resultado de su medición. Al final del protocolo, no queda entrelazamiento entre emisor y receptor.

ANTONIO ACIN

Destilación de entrelazamiento



a. Emisor y receptor comparten un canal que produce decoherencia. El emisor prepara estados entrelazados de dos qubits y envía uno de ellos a través del canal. La transmisión es imperfecta, por lo que las dos partes tienen un estado entrelazado impuro (con ruido). El proceso se repite M veces.

b. Emisor y receptor procesan cada uno, de manera local, los estados cuánticos que poseen. Estas operaciones pueden ir acompañadas del envío de comunicación clásica en las dos direcciones, de emisor a receptor o viceversa. En este proceso, no se transmite ningún tipo de información cuántica por el canal. El objetivo es destilar entrelazamiento sin ruido.

c. Al final del proceso, se comparten $n < M$ estados entrelazados perfectos. Estos estados permiten teleportar qubits desde el emisor al receptor de manera perfecta. Por tanto, es entonces posible el envío de información cuántica sin errores.

métodos más simples de corrección de errores en la teoría clásica de la información.

Pasemos ahora a analizar la situación donde la información se codifica en sistemas cuánticos. ¿Puede aplicarse el sencillo método de corrección de errores descrito con anterioridad? La respuesta es no. Esta nueva situación sirve muy bien para ilustrar de qué modo se ve afectado el procesamiento de información por el cambio de descripción de los dispositivos físicos utilizados para la codificación. Ya sabemos que en mecánica cuántica existe el teorema de la no clonación, según el cual es imposible obtener un proceso capaz de clonar de manera perfecta cualquier estado cuántico. Excluye el uso de la redundancia para corregir errores. Más en general, parecerá que la perturbación irreversible que el proceso de medición causa en el estado cuántico de un sistema dificulta que el estado que le llega al receptor se lea de modo que no se introduzcan más errores y se pueda reconstruir la información enviada (teniendo además en cuenta que el receptor habrá de compensar los errores que se produjeron durante la transmisión).

Fueron varios los investigadores que plantearon serias dudas acerca de la viabilidad de la corrección de errores para estados cuánticos [*véase* "Reglas para un mundo cuántico complejo", por Michael A. Nielsen, INVESTIGACIÓN Y CIENCIA, enero 2003]. Sin embargo, en 1995 Andrew Steane y, de nuevo, Shor, cada uno por su parte, introdujeron los primeros métodos cuánticos de corrección de errores. La solución pasaba por saber adecuar los métodos clásicos al nuevo entorno por medio de un recurso intrínsecamente cuántico: el entrelazamiento. La idea consistía en codificar con habilidad cada bit cuántico lógico en un estado entrelazado de siete qubits físicos (en el protocolo propuesto por Steane) o nueve (en el de Shor). Esta codificación tenía más robustez bajo decoherencia y permitía una reconstrucción perfecta del estado cuántico de partida (el bit cuántico lógico) en situaciones en las que se hubiera producido un error en uno de los bits cuánticos físicos. Por tanto, el uso de estos protocolos permite el procesamiento de información cuántica en casos donde la probabilidad de tener dos errores es baja, ya que un error solo siempre se corrige.

A partir de estos primeros esquemas, aparecieron nuevos y más refinados protocolos de corrección de errores. Hoy existe una formulación general del problema. Todos esos protocolos traducen a un entorno cuántico métodos ya conocidos en la teoría clásica de la información. A grandes rasgos, un esquema de corrección de errores cuántico consta de una etapa de codificación en el emisor, que almacena el qubit lógico en un estado entrelazado de diferentes qubits físicos, y un proceso de decodificación en el receptor, donde se detecta y corrige el error que se haya producido en el canal (*véase la figura 2*). Las propiedades de cada protocolo de corrección de errores vienen descritas por tres números $[[n, k, d]]$, donde n corresponde al número de bits físicos utilizados en la codificación, k al número de bits lógicos almacenados, y d está ligado al número de errores que se pueden corregir, n_E: $d = 2n_E + 1$. Por tanto, el esquema de Steane es $[[7,1,3]]$, mientras que el de Shor es $[[9,1,3]]$. Para valores de n y k fijados, el mejor código es el que proporciona el mayor d, la mayor cantidad de errores corregibles. Sin entrar en más detalles, ejemplos de códigos conocidos son $[[8,3,3]]$, $[[21,6,5]]$, $[[23,1,7]]$ o $[[127,50,15]]$. El mínimo código capaz de corregir un error es el $[[5,1,3]]$.

Más allá de su importancia de tipo práctico, los métodos de corrección de errores supusieron un importante avance hacia la consolidación de la teoría de la información cuántica, al demostrar que se podía combatir la decoherencia. Recordemos que importantes investigadores habían expresado la posibilidad de que la codificación de información en estados cuánticos fuera demasiado delicada y sensible a la interacción con el entorno, y que ello supondría una barrera fundamental para la aplicación de la información cuántica. Los protocolos de corrección de errores demostraron que ello no era cierto: de modo parecido al caso clásico, si se tenía una cierta tasa de error inicial en el canal cuántico, podía llevarse a cabo una transmisión con probabilidad de error efectiva arbitrariamente pequeña.

ANTONIO ACIN

El problema, pues, dejaba de residir en el lado teórico (si bien las técnicas para la mejora de los códigos correctores de errores siguen siendo objeto de intenso estudio) y se trasladaba al experimental. Para cuando el avance de la técnica permita un procesamiento cuántico de la información con buena robustez bajo decoherencia, se conocerán ya métodos que reducirán el nivel de ruido cuanto se quiera.

La teleportación

Los protocolos de corrección de errores demuestran que es posible adecuar una aplicación bien establecida en teoría clásica de la información al nuevo entorno cuántico. Hay, sin embargo, un método alternativo de corrección de errores intrínsecamente cuántico; sin análogo clásico, explota las propiedades del entrelazamiento. Antes de entrar en detalles, señalemos que la idea general radica en realizar la corrección de errores antes del envío de la información, en transformar el canal ruidoso en un canal sin errores. Una vez se ha establecido este canal cuántico, se puede proceder a la transmisión perfecta de la información. La teleportación cuántica desempeña un papel clave en este método.

La teleportación cuántica es una de las aplicaciones de la información cuántica más importantes y sorprendentes. El emisor recibe una partícula que codifica un bit cuántico, desconocido para él, que debe transmitir a un receptor. Una primera opción, trivial, consiste en que el emisor envíe la partícula directamente. Sin embargo, quizá no resulte posible; por ejemplo, porque el canal produzca demasiado ruido. Supongamos que emisor y receptor comparten dos bits cuánticos en un estado máximamente entrelazado. Es decir, emisor y receptor tienen cada uno una partícula cuántica, y el estado global de las dos viene dado por una superposición coherente de pesos iguales de $|00\rangle$ y $|11\rangle$. Gracias al esquema basado en la teleportación cuántica, el receptor puede, valiéndose de ese entrelazamiento y tras recibir dos bits de información clásica del emisor, reconstruir el bit cuántico de un modo perfecto.

Importa subrayar el papel de los dos bits clásicos que el emisor debe enviar al receptor para que éste sea capaz de reconstruir el estado. Sin estos dos bits, el proceso no puede llevarse a cabo, ya que el receptor no tendrá información hasta que no los reciba. Es decir, la teleportación no permite la transmisión instantánea de información. Es más bien un método, sorprendente, de transmisión de información cuántica por medio de un estado entrelazado y bits clásicos.

Alguien pudiera inferir que la teleportación implica que un bit cuántico es equivalente a dos bits clásicos. Una deducción falsa. Si el emisor quisiera especificarle el bit cuántico al receptor por medio de información clásica, tendría que dar una dirección en la esfera de Poincaré. Para hacerlo con buena precisión, se requeriría un gran número de bits clásicos (infinitos para conseguir una imprecisión nula). Además, en la teleportación el emisor no tiene por qué conocer el bit cuántico que envía. El entrelazamiento compartido por las dos partes es el recurso esencial en que se basa la teleportación. Esta se consume una vez el receptor ha reconstruido el bit cuántico: el entrelazamiento no sobrevive tras el final del proceso. Debemos retener lo siguiente: si emisor y receptor comparten un estado de dos qubits máximamente entrelazado, será posible el envío de un qubit sin errores por medio de la teleportación. En consecuencia, se podrá considerar a ese estado un canal cuántico perfecto.

Una pregunta surge de modo natural: ¿de qué forma emisor y receptor consiguen establecer el entrelazamiento inicial requerido para la teleportación? El emisor puede, en principio, preparar el estado localmente y enviar al receptor uno de los dos bits cuánticos. Sin embargo, debe hacerlo a través del canal que poseen, que es ruidoso. Recordemos que se debe crear una superposición coherente de $|00\rangle$ y $|11\rangle$; los mecanismos generadores de decoherencia del canal repercutirán en el estado enviado; emisor y receptor acabarán compartiendo una versión ruidosa del estado deseado, que no permitirá una teleportación perfecta.

Destilación de entrelazamiento

Las técnicas de destilación de entrelazamiento permiten transformar, con cierta probabilidad p, estados entrelazados ruidosos en estados máximamente entrelazados de dos bits cuánticos. Es decir, consiguen destilar el entrelazamiento impuro del estado que ha sufrido la decoherencia y transformarlo en entrelazamiento puro, sin errores. Más concretamente, existen secuencias de mediciones entre emisor y receptor, asistidas por comunicación clásica, que con probabilidad p transforman M copias de un estado ruidoso entrelazado en N copias de un estado puro máximamente entrelazado.
Emisor y receptor saben de modo exacto si el protocolo de destilación ha sido exitoso, lo que, recordemos, sucede con probabilidad p. Ahora resulta sencillo entender cómo pueden estas técnicas utilizarse para el envío de información cuántica a través de un canal ruidoso. El emisor, que ha de enviar N bits cuánticos, prepara un estado máximamente entrelazado y envía uno de los dos bits cuánticos al receptor. A causa de la decoherencia en la propagación, el estado final es impuro. Este proceso se repite M veces, por lo que emisor y receptor acaban con M copias del mismo estado. A continuación, emplean un protocolo de destilación cuántica que produce, con probabilidad p, N copias del estado máximamente entrelazado. Recordemos que estos estados son equivalentes a un canal cuántico sin ruido. El emisor puede consumir estos N estados en la transmisión sin errores de los N bits cuánticos por medio de teleportación, concluyendo así el envío de la información cuántica.

¿Es posible encontrar alguna relación entre la destilación de entrelazamiento y los métodos de corrección de errores? Se ha demostrado que si el flujo de comunicación clásica necesario en el proceso de destilación sólo cursa en una dirección, de emisor a receptor por ejemplo, se puede establecer una analogía entre ese método de destilación y un protocolo de corrección de errores. Sin embargo, esto deja de ser cierto si la destilación utiliza comunicación en las dos direcciones. Los métodos de destilación con comunicación bidireccional permiten la transmisión sin errores de información cuántica para canales cuyo nivel de ruido sea tal, que no se pueda aplicar ningún método cuántico de corrección de errores estándar. En ese sentido, los

protocolos de destilación de entrelazamiento son más potentes.

Métodos tolerantes de fallos

La discusión anterior ha servido para presentar los métodos habituales diseñados para el procesamiento cuántico de información bajo decoherencia. Por motivos de sencillez, se ha presentado en una situación de comunicación cuántica, donde se tienen dos partes separadas comunicadas por un canal ruidoso. Pero las mismas técnicas valen para la computación cuántica, donde se realizaría un procesamiento de un gran número de bits cuánticos. Si la operación es complicada y requiere un tiempo considerable, los efectos de decoherencia empiezan a adquirir importancia, ya que el sistema interacciona más de lo deseado con el entorno. Dicho de forma equivalente: no es posible garantizar que, durante todo el tiempo de ejecución, no exista ninguna parte del sistema que haya sufrido una pérdida de coherencia. De ahí se sigue que habría que alternar fases de computación y fases de corrección de errores, que emplearían los métodos descritos.

A lo largo de esta exposición hemos supuesto que las operaciones que hay que realizar para la corrección de los errores eran perfectas y no introducían más ruido. Eso no se cumple en una situación real. Resulta obligado, pues, analizar las consecuencias de habérselas con operaciones cuánticas imperfectas en los protocolos de corrección de errores. Sin entrar en más detalles, se ha demostrado que todos los métodos anteriores resisten fallos en las operaciones cuánticas que los componen. Se puede establecer un umbral de imperfección para ellas, de tal modo que aún sea posible realizar una transmisión o computación cuántica casi libre de errores. Todos estos resultados desembocan en los llamados "métodos tolerantes de fallos".

En resumen, hemos presentado las técnicas habituales para la corrección de errores en el procesamiento cuántico de información. El factor a combatir es la decoherencia, que destruye la peculiaridad cuántica del sistema: las superposiciones coherentes de estados, fundamento de cualquier protocolo de información cuántica. Durante la exposición hemos aprendido que se pueden trasladar ideas provenientes de la teoría clásica de la información al formalismo cuántico, acomodándolas a las nuevas reglas de juego. En otras ocasiones nos hemos encontrado ante situaciones intuitivamente difíciles de aceptar, debido a las peculiaridades del formalismo cuántico: estados de superposición, entrelazados o teleportación.

Los métodos que se han presentado aquí representan un primer paso, si bien crucial, de cara a explotar la gama de posibilidades que aparece al codificar la información en estados cuánticos. La mecánica cuántica ofrece multitud de situaciones sorprendentes, que desafían nuestra intuición y no tienen un análogo clásico. ¡Aprovechémoslas!

El autor

Antonio Acín Dal Maschio es ingeniero de Telecomunicaciones por la Universidad Politécnica de Cataluña (UPC), licenciado en físicas y doctor en física teórica por la Universidad de Barcelona (UB). Tras una estancia posdoctoral en el Grupo de Física Aplicada de la Universidad de Ginebra, se trasladó al Instituto de Ciencias Fotónicas (ICFO) de Barcelona, donde se encuentra en la actualidad. Su tarea investigadora se centra en los campos de la teoría de la información cuántica y de la óptica cuántica.

Bibliografía complementaria

INTRODUCTION TO QUANTUM COMPUTATION AND INFORMATION. Dirigido por H.-K. Lo, S. Popescu y T. Spiller. World Scientific; Londres, 1998.

QUANTUM COMPUTATION AND QUANTUM INFORMATION. M. A. Nielsen y I. L. Chuang. Cambridge University Press; Cambridge, 2000.

THE PHYSICS OF QUANTUM INFORMATION: QUANTUM CRYPTOGRAPHY, QUANTUM TELEPORTATION, QUANTUM COMPUTATION. Dirigido por D. Bouwmeester, A. Ekert y A. Zeilinger. Springer Verlag; Berlín, 2000.

INITIATION À LA PHYSIQUE QUANTIQUE. Valerio Scarani. Vuibert; París, 2003.