Entrelazamiento cuántico e información

Jeffrey Bub
Modo de citar:
Bub, Jeffrey. 2017. "Entrelazamiento cuántico e información". En Diccionario Interdisciplinar Austral, editado por Claudia E. Vanney, Ignacio Silva y Juan F. Franck.
URL=https://dia.austral.edu.ar/Entrelazamiento_cuántico_e_información

Versión española de Quantum Entanglement and Information, de la Stanford Encyclopedia of Philosophy.

Traducción: Federico Holik

Publicado por primera vez el lunes 13 de agosto de 2001; revisión substancial el sábado 7 de febrero de 2015

El entrelazamiento cuántico es un recurso físico, como la energía, asociado con las singulares correlaciones no-clásicas que son posibles entre sistemas cuánticos separados. El entrelazamiento puede ser medido, transformado y purificado. Un par de sistemas cuánticos en un estado entrelazado pueden utilizarse como un canal de información cuántica para realizar tareas computacionales y criptográficas que son imposibles para sistemas clásicos. El estudio general de las capacidades de procesamiento de la información que poseen los sistemas cuánticos es el tema principal de la teoría de la información cuántica.

1 Entrelazamiento cuántico ↑

En 1935 y 1936, Schrödinger publicó un artículo en dos partes, en el cual discutía y extendía un argumento de Einstein, Podolsky y Rosen. El argumento Einstein-Podolsky-Rosen (EPR) era, en muchos sentidos, la culminación de la crítica de Einstein a la interpretación ortodoxa de Copenhague de la mecánica cuántica, y fue diseñado para demostrar que la teoría es incompleta. (Ver "The Einstein-Podolsky-Rosen Argument in Quantum Theory" y "Copenhaguen Interpretation of Quantum Mechanics" en la SEP). En la mecánica clásica, el estado de un sistema es esencialmente una lista de las propiedades del sistema –más precisamente, es la descripción de un conjunto de parámetros a partir de los cuales la lista de propiedades puede ser reconstruida: las posiciones y momentos de todas las partículas que componen el sistema (o parámetros similares en el caso de campos). La dinámica de la teoría especifica cómo las propiedades cambian en términos de una ley de evolución para el estado. Pauli caracterizó este modo de descripción de los sistemas físicos como una idealización que involucra un "observador imparcial". Ver la carta de Pauli a Born en *The Born-Einstein's Letters* (Born 1992, 218). En la interpretación de Copenhague, esta descripción resulta inadecuada para sistemas cuánticos. En su lugar, el estado cuántico de un sistema debería entenderse como un catálogo de lo que el observador le ha hecho al sistema y lo que ha sido observado, y la importancia del estado consiste en las probabilidades que se pueden inferir (en términos de la teoría) para los resultados de posibles observaciones futuras sobre el sistema. Einstein rechazó esta visión, y propuso una serie de argumentos para mostrar que el estado cuántico es simplemente una caracterización incompleta de un sistema cuántico. Los parámetros faltantes son frecuentemente denominados "parámetros ocultos" o "variables ocultas", aunque Einstein no utilizó este término.

No debería suponerse que la noción de Einstein de una teoría completa incluía el requisito que la teoría debería ser determinista. Para ser más precisos, él exigía ciertas condiciones de separabilidad y localidad para sistemas compuestos consistentes en sistemas componentes separados: cada sistema componente por separado debería ser caracterizado por sus propiedades (su propio 'ser así', en términos de Einstein –'*So-sein*' en alemán), y debería ser imposible alterar las propiedades de un sistema distante (o las probabilidades de estas propiedades)

instantáneamente, al accionar sobre un sistema local. En análisis posteriores, especialmente en el argumento de Bell a favor de la no-localización de las correlaciones cuánticas, se tornó evidente que estas condiciones, correctamente formuladas como restricciones en las probabilidades, son equivalentes al requisito de que correlaciones estadísticas entre sistemas separados deban ser reducibles a distribuciones de probabilidad por causas comunes (deterministas o estocásticas) en el sentido de Reichenbach (Ver "Bell's Theorem" y "Reichenbach's Common Cause Principle" de la SEP.)

En el artículo EPR original, se preparan dos partículas a partir de una fuente en un determinado estado cuántico "puro" del sistema compuesto (un estado que no puede expresarse como una mezcla o distribución de probabilidad de otros estados cuánticos puros, y que no puede reducirse a un estado cuántico puro de cada partícula por separado). Una vez separadas las partículas, surgen correlaciones "combinables" tanto entre las posiciones de las dos partículas como entre sus momentos: una medición de posición o momento en una partícula determinada permitirá predecir con certeza el resultado de una medición de posición o una medición de momento, respectivamente, en la otra partícula. Estas mediciones son mutuamente excluyentes: o bien se puede realizar una medición de posición, o bien una medición de momento, pero no ambas simultáneamente. Una medición de momento subsiguiente, por ejemplo después de establecer una correlación en la posición, ya no arrojará ninguna correlación entre los momentos de las dos partículas. Es como si una medición de la posición perturbara las correlaciones entre los valores de los momentos, y viceversa. Descontando la peculiaridad de que cada correlación puede cumplirse, pero no ambas para el mismo par de partículas, las correlaciones de posición y momento para las partículas cuánticas son exactamente iguales a las correlaciones clásicas entre bolas de billar después de una colisión. Las correlaciones clásicas pueden explicarse por una causa común, o por "elementos de realidad" correlacionados. El argumento EPR afirma que la mecánica cuántica es incompleta porque estas causas comunes o elementos de realidad no están incluidos en la descripción que provee el estado cuántico.

Así es como Schrödinger describe el problema en la primera parte del artículo antes mencionado (Schrodinger 1935, 559):

"Sin embargo, al poder predecir tanto x_1 como p_1 sin interferir con el sistema nro. 1, y ya que el nro 1, como un alumno en un examen, no puede saber cuál de las dos preguntas le voy a formular primero: parece entonces que nuestro alumno está preparado para responder correctamente la *primera* pregunta que se le formule *en cualquier forma*. Por lo tanto, él debe conocer ambas respuestas: lo cual demuestra un conocimiento sorprendente; independientemente del hecho de que, después de haber dado su primera respuesta, nuestro alumno está invariablemente tan desconcertado o cansado, que todas las siguientes respuestas serán erróneas."

Lo que mostró Schrödinger es que si dos partículas son preparadas en un estado cuántico de EPR, donde existe una correlación de apareamiento entre dos cantidades dinámicas "canónicamente conjugadas" (cantidades como la posición y el momento, cuyos valores son suficientes para especificar todas las propiedades de un sistema clásico), hay entonces infinitas cantidades dinámicas de las dos partículas para las cuales existen correlaciones de apareamiento similares: cada función del par canónicamente conjugado de la primera partícula se aparea con la misma función del par canónicamente conjugado de la segunda partícula. Por eso (Schrödinger 1935, 559) el sistema nro 1 "no sólo sabe estas dos respuestas, sino un elevado número de otras, y esto sin ayuda mnemotécnica de ningún tipo, o al menos de ninguna de la que tengamos conocimiento."

Schrödinger acuñó el término 'entrelazamiento' para describir esta conexión peculiar entre sistemas cuánticos (Schrödinger 1935, 555):

"Cuando dos sistemas, cuyos estados conocemos a través de sus respectivos representantes, entran en una interacción física temporaria debido a fuerzas conocidas entre ellos, y cuando luego de un tiempo de influencia mutua los sistemas se separan nuevamente, por ende, ya no pueden describirse del mismo modo que antes, es decir, dotándolos a cada uno de un representante propio. Yo no llamaría a esto *un*, sino *el* rasgo característico de la mecánica cuántica, aquél que fuerza el total abandono de las líneas de pensamiento clásicas. A causa de la interacción, los dos representantes (los estados cuánticos) se entrelazaron."

Y añadió (Schrödinger 1935, 555):

“Otra forma de expresar esta situación peculiar es: el mejor conocimiento posible de una totalidad no necesariamente incluye el mejor conocimiento posible de todas sus partes, incluso aunque éstas puedan estar completamente separadas y por ello virtualmente capaces de ser “conocidas lo mejor posible”, es decir, de poseer, cada una de ellas, un representante propio.

La ausencia de conocimiento no se debe en modo alguno a que la interacción no sea suficientemente conocida –al menos, no en la forma en que posiblemente podría ser conocida de manera más completa– sino que se debe a la interacción misma.

Recientemente se ha puesto la atención en el hecho obvio pero muy desconcertante de que, incluso aunque restrinjamos las mediciones desentrelazantes a un sistema, el representante obtenido para el otro sistema no es en modo alguno independiente de la elección particular de observaciones que seleccionamos para este propósito, y que, por ende, son completamente arbitrarias. Resulta un tanto incómodo que la teoría permita que un sistema sea dirigido o pilotado hacia uno u otro tipo de estado a voluntad del experimentador a pesar de que éste no tiene acceso a él.”

En la segunda parte del artículo, Schrödinger mostró que, en general, un experimentador sofisticado puede, mediante una elección adecuada de las operaciones realizadas sobre un sistema, “dirigir” el segundo sistema hacia cualquier mezcla de estados cuánticos elegida. En otras palabras, el segundo sistema no puede ser dirigido a cualquier estado cuántico particular al antojo del experimentador, pero el experimentador puede constreñir al estado cuántico hacia el cual el segundo sistema evoluciona a encontrarse en cualquier conjunto elegido de estados, con una distribución de probabilidad fijada por el estado entrelazado. Schrödinger consideró esta conclusión lo suficientemente inquietante como para sugerir que el entrelazamiento entre dos sistemas que se están separando persistiría sólo para distancias lo suficientemente pequeñas como para que el tiempo que emplea la luz para viajar de un sistema a otro pueda ser ignorado comparado con los períodos de tiempo característicos asociados con otros cambios en el sistema compuesto. Schrödinger especulaba que, para distancias más grandes, cada uno de los dos sistemas podría de hecho estar en un estado cuántico “mezcla”, una distribución de probabilidad sobre estados puros, determinada por la forma precisa del estado entrelazado.

La mayoría de los físicos atribuyeron las desconcertantes características de los estados cuánticos entrelazados a la inapropiada visión de Einstein sobre las teorías físicas del “observador imparcial”, y consideraron la respuesta de Bohr al argumento EPR (Bohr 1935) como una justificación a la interpretación de Copenhague. Esto fue desafortunado, dado que el estudio sobre el entrelazamiento fue ignorado por treinta años hasta la reconsideración del argumento EPR por parte de John Bell (Bell 1964). Bell estudió el entrelazamiento en sistemas más simples que el caso EPR: correlaciones apareadas entre cantidades dinámicas bi-valuadas, tales como la polarización o el espín, de dos sistemas separados en un estado entrelazado. Lo que Bell demostró fue que las correlaciones estadísticas entre los resultados de las mediciones de cantidades *diferentes* correctamente elegidas sobre los dos sistemas son inconsistentes con una desigualdad derivable a partir de las hipótesis de localidad y separabilidad de Einstein –en efecto, a partir de la hipótesis de que las correlaciones tienen una causa común. Esta desigualdad se conoce como ‘desigualdad de Bell’, y varias desigualdades relacionadas pueden considerarse un indicador de correlaciones clásicas o basadas en una causa común.

La investigación de Bell generó un creciente debate sobre los fundamentos de la mecánica cuántica. Una faceta importante de este debate fue la confirmación de que el entrelazamiento puede persistir a través de grandes distancias, refutando de este modo el supuesto de Schrödinger del decaimiento espontáneo del entrelazamiento a medida que dos partículas entrelazadas se separan (el entrelazamiento de fotones en el espacio vacío ha sido confirmado en experimentos entre las Islas Canarias de La Palma y Tenerife, a una distancia de 143 km. Ver Herbst *et al* 2014, en Herramientas académicas). Pero no fue sino hasta la década de 1980 que físicos, científicos de la computación y criptógrafos comenzaron a considerar las correlaciones no-locales de estados cuánticos entrelazados como un nuevo tipo de recurso no-clásico que podría aprovecharse, en lugar de como un bochorno a ser justificado. Para una ulterior discusión acerca del entrelazamiento como recurso físico, que incluye la medición del entrelazamiento, y la manipulación y purificación del entrelazamiento mediante operaciones locales, ver “The Joy Of Entanglement” de Popescu y Rhrlich en Lo, Popescu y Spiller 1998, o Nielsen y Chuang 2000.

2 Cómo beneficiarse con el entrelazamiento: teleportación cuántica ↑

Consideremos nuevamente la observación de Schrödinger que sostiene que un estado entrelazado podría utilizarse para conducir a una partícula distante hacia un estado de un conjunto dado, con una cierta probabilidad. De hecho, esta posibilidad de "direccionamiento remoto" es incluso más drástica de lo que demostró Schrödinger. Supongamos que Alice y Bob comparten un estado entrelazado puro del tipo considerado por Bell, por ejemplo dos fotones en un estado entrelazado de polarización, donde Alice tiene en su poder uno de los fotones entrelazados y Bob el otro. Supongamos que Alice recibe un fotón adicional en un estado de polarización desconocido $|u\rangle$, donde la notación "|⟩" denota un estado cuántico. Para Alice es posible efectuar una operación sobre los dos fotones en su poder, que conducirá al fotón de Bob a uno de cuatro estados, dependiendo de los cuatro posibles resultados (aleatorios) de la operación de Alice: o el estado $|u\rangle$, o un estado que está vinculado con $|u\rangle$ de una forma definida. La operación de Alice entrelaza los dos fotones en su poder, y desentrelaza el fotón de Bob, direccionándolo hacia un estado $|u^*\rangle$. Luego de que Alice comunica a Bob el resultado de su operación, Bob sabe que, o bien $|u\rangle=|u^*\rangle$, o bien sabe cómo transformar $|u^*\rangle=|u\rangle$ aplicando una operación local. Este fenómeno es conocido como 'teleportación cuántica'. Luego del procedimiento de teleportación, el estado $|u\rangle$ continúa siendo desconocido tanto para Alice como para Bob.

Lo que es extraordinario acerca de este fenómeno es que Alice y Bob han logrado utilizar el estado entrelazado que comparten como un canal de comunicación cuántico para destruir el estado $|u\rangle$ de un fotón en la región del universo de Alice y recrearlo en la región del universo de Bob. Dado que el estado de polarización lineal de un fotón requiere la especificación de una dirección del espacio (el valor de un ángulo que puede variar de un modo continuo), sin la ayuda de un estado entrelazado Alice habría tenido que transmitir una cantidad infinita de información clásica a Bob para que Bob fuera capaz de reconstruir el estado $|u\rangle$ con total precisión. Según el modo en que Shannon formalizó la noción de información clásica, la cantidad de información clásica asociada con una alternativa binaria representada como 0 o 1, donde cada alternativa tiene la misma probabilidad, es un dígito binario o "bit". Especificar un ángulo arbitrario como un número decimal requiere una secuencia infinita de dígitos entre el 0 y el 9, o una secuencia infinita de ceros y unos en notación binaria. El resultado de la operación de Alice, que tiene cuatro resultados posibles con la misma probabilidad de 1\4, puede especificarse con sólo dos bits de información. En particular, Bob puede reconstruir el estado $|u\rangle$ sobre la base de sólo dos bits de información clásica comunicada por Alice, aparentemente a través del aprovechamiento del estado entrelazado como un canal de comunicación cuántica para transferir la información restante. Para una ulterior discusión sobre la teleportación cuántica, ver Nielsen y Chuang 2000, o el artículo de Richard Josza "Quantum Information and its Properties" en Lo, Popescu y Spiller 1998.

3 Información cuántica ↑

Formalmente, la cantidad de información clásica que obtenemos, en promedio, cuando adquirimos el conocimiento del valor de una variable aleatoria (o, equivalentemente, la cantidad de incerteza en el valor de una variable aleatoria antes de que sepamos su valor) se representa mediante una cantidad llamada entropía de Shannon, medida en bits (Shannon y Weaver 1949). Una variable aleatoria se define como una distribución de probabilidad sobre un conjunto de valores. En el caso de una variable aleatoria binaria, con probabilidades iguales para cada una de las dos posibilidades, la entropía de Shannon es de un bit, que representa incerteza máxima. Para todas las otras probabilidades –intuitivamente, que representan alguna información acerca de cuál alternativa es más probable– la entropía de Shannon es menor a uno. Para el caso de conocimiento maximal o incertaza cero acerca de las alternativas, donde las probabilidades son 0 y 1, la entropía de Shannon es cero. (Cabe notar que el término "bit" se utiliza para denominar la unidad básica de información clásica en términos de la entropía de Shannon, y a un sistema clásico elemental de dos estados considerado como representando los posibles estados de una fuente de información clásica elemental.)

Dado que la información siempre se materializa en el estado de un sistema físico, también podemos pensar la entropía de Shannon como cuantificador de los recursos necesarios para almacenar información clásica. Supongamos que Alice desea comunicar información clásica a Bob utilizando un canal de comunicación tal como el de una línea telefónica. Una pregunta pertinente sería hasta qué punto el mensaje puede comprimirse sin pérdida de información,

de forma tal que Bob pueda reconstruir el mensaje original exactamente a partir de la versión comprimida. De acuerdo con el teorema de Shannon de codificación de la fuente, o teorema de Shannon de codificación sin ruido (asumiendo una línea telefónica sin ruido ni pérdida de información), el recurso físico mínimo necesario para representar el mensaje (efectivamente, una cota inferior para la posibilidad de compresión) está dado por la entropía de Shannon de la fuente.

¿Qué sucede si utilizamos los estados cuánticos de sistemas físicos para almacenar la información, en lugar de estados clásicos? Resulta que la información cuántica es radicalmente diferente de la información clásica. La unidad de información cuántica es el 'qubit', que representa la cantidad de información cuántica que puede almacenarse en el estado del sistema cuántico más simple, por ejemplo, el estado de polarización de un fotón. El término se debe a Schumacher (1995), quien probó un análogo al teorema de codificación sin ruido de Shannon. (En analogía con el término "bit", el término "qubit" refiere a la unidad básica de información cuántica en términos de la entropía de von Neumann, y a un sistema cuántico elemental de dos niveles considerado como representante de los posibles estados de una fuente de información cuántica elemental). Una cantidad arbitrariamente elevada de información clásica puede codificarse en un qubit. Esta información puede ser procesada y comunicada, pero, debido a las peculiaridades de la medición cuántica, sólo es posible acceder a lo sumo a un bit. De acuerdo a un teorema de Holevo, la información accesible de una distribución de probabilidad sobre un conjunto de estados de qubits está limitada por la entropía de von Neumann, la cual es igual a la entropía de Shannon sólo cuando los estados son ortogonales en el espacio de estados cuánticos, y en los demás casos es menor que la entropía de Shannon.

Mientras que la información clásica puede ser copiada o clonada, el teorema de 'no clonación' cuántico (Dieks 1982; Wootters y Zurek 1982) afirma la imposibilidad de clonar un estado cuántico desconocido. Para entender por qué, consideremos cómo podríamos construir un dispositivo clásico de copiado. Una compuerta NOT es un dispositivo que toma un bit a la entrada y produce como salida un 1 si la entrada es un 0, o un 0 si la entrada es un 1. En otras palabras, una compuerta NOT es una compuerta de un bit que cambia el bit de entrada. Una compuerta NOT controlada, o compuerta CNOT, toma dos bits como entrada, un bit de control y otro de objetivo, y cambia el bit de objetivo si y sólo si el bit de control es 1, al tiempo que reproduce el bit de control. Entonces, hay dos entradas, el control y el objetivo, y dos salidas: el control, y o bien el objetivo, o bien el objetivo cambiado, dependiendo del valor del control. Una compuerta CNOT funciona como un dispositivo de copiado para el bit de control si el bit de objetivo es puesto en 0, porque la salida del bit de objetivo es entonces una copia del bit de control: la entrada 00 produce la salida 00, y la entrada 10 produce la salida 11 (aquí el primer bit es el control y el segundo es el objetivo). En la medida en que podamos pensar una medición como simplemente una operación de copiado, una compuerta CNOT es el paradigma de dispositivo de medición clásico. Imaginemos a Alice equipada con un dispositivo así, con cables de control y objetivo de entrada y salida, midiendo las propiedades de un mundo clásico. El cable de control de entrada es una prueba para la presencia o ausencia de una propiedad, representada por un 1 o un 0. El cable de objetivo funciona como un puntero, que es inicialmente preparado en 0. La salida del objetivo es 1 o 0, dependiendo de la presencia o ausencia de la propiedad.

Supongamos que intentamos utilizar una compuerta CNOT para copiar un estado desconocido de un qubit. Dado que estamos proponiendo considerar la compuerta CNOT como un dispositivo para procesar estados cuánticos, la evolución desde los estados de entrada a los estados de salida debe ser efectuada por una transformación física cuántica. Las transformaciones cuánticas son lineales en el espacio de estados lineales de qubits. La linealidad en el espacio de estados se refiere a que, para dos estados del qubit que son ortogonales en el espacio de estados del qubit –por ejemplo, $|0\rangle$ y $|1\rangle$–, existen estados del qubit que son representados por superposiciones lineales o sumas de $|0\rangle$ y $|1\rangle$, con ciertos coeficientes. Tales superposiciones –por ejemplo, una superposición con coeficientes c_0 y c_1 representada simbólicamente como $c_0|0\rangle+c_1|1\rangle$– son no ortogonales a $|0\rangle$ y a $|1\rangle$. La linealidad de la transformación requiere que una transformación transforme un estado del qubit representado por la suma de dos qubits ortogonales, a un nuevo estado del qubit que es la suma de los estados ortogonales del qubit transformados. Si la compuerta CNOT logra copiar dos qubits ortogonales, no logrará copiar una superposición lineal de estos qubits. Como la compuerta funciona linealmente, en vez de ello, debe producir un estado que es una superposición lineal de las salidas obtenidas para los dos qubits ortogonales. Es decir, el resultado de la compuerta va a estar representado por un estado cuántico que es la suma de dos términos, donde el primer término representa la salida de control y objetivo del primer qubit, y el segundo término representa la salida de control y objetivo para el segundo qubit ortogonal. Esto podría ser

expresado como $c_0|0\rangle|0\rangle+c_1|1\rangle|1\rangle$, el cual es un estado entrelazado, y no el resultado que se requeriría para una operación de copiado exitosa (donde el control y el objetivo, cada uno, arrojan el qubit superpuesto).

4 Criptografía cuántica ↑

Supongamos que Alice y Bob están separados y quieren comunicar un mensaje secreto, sin revelar ninguna información a Eve, una espía. Ellos pueden hacerlo en un mundo clásico si comparten una '*one-time pad*', es decir, una clave criptográfica representada por una secuencia de bits aleatorios al menos tan grande como el número de bits requeridos para comunicar el mensaje. De hecho, esta es la única forma segura de lograr seguridad perfecta en un mundo clásico. Para enviar un mensaje a Bob, Alice comunica qué bits en la clave debería cambiar Bob. La secuencia de bits resultante es el mensaje. Adicionalmente, necesitarían tener algún modo de codificar mensajes como secuencias de bits, representando letras del alfabeto, espacios y símbolos de puntuación como números binarios, lo cual se podría hacer con algún esquema estándar de disponibilidad pública.

El problema es que los mensajes comunicados de esta forma son secretos solamente si Alice y Bob utilizan una "one time pad" diferente para cada mensaje. Si ellos utilizan la misma para todos los mensajes, Eve podría conseguir alguna información sobre la correspondencia entre las letras del alfabeto y las subsecuencias de bits en la clave, al relacionar características estadísticas de los mensajes con la forma en la que las palabras están compuestas por letras. Para compartir una nueva clave, ellos tendrían que apoyarse en mensajeros confiables, o algún método similar para distribuir la clave. No hay forma de garantizar la seguridad del procedimiento de distribución de la clave en un mundo clásico.

Copiar la clave, sin revelar que ha sido copiada, es también un problema para la clave compartida que Alice y Bob almacenan de un modo supuestamente seguro. Pero las leyes de la física en un mundo clásico no garantizan que el procedimiento de almacenamiento sea completamente seguro, y no pueden garantizar que la ruptura de la seguridad y el copiado de la clave serán siempre detectados. Por ello, además del problema de distribución de claves, existe un problema de almacenamiento de claves.

El entrelazamiento cuántico proporciona una forma de resolver estos problemas a través de la 'monogamia' de las correlaciones en estados entrelazados: ningún tercero participante puede compartir el entrelazamiento entre Alice y Bob. Además, cualquier intento de Eve de medir los sistemas cuánticos en el estado entrelazado compartido por Alice y Bob destruirá al estado entrelazado. Alice y Bob pueden detectar esto chequeando una desigualdad de Bell.

Una forma de hacer esto es mediante un protocolo propuesto originalmente por Artur Ekert. Supongamos que Alice tiene una colección de fotones, uno para cada par entrelazado en el estado $|0\rangle|0\rangle+|1\rangle|1\rangle$ (ignorando los coeficientes iguales para mayor simplicidad), y que Bob tiene una colección de fotones de a pares. Alice mide la polarización de sus fotones aleatoriamente en direcciones 0, π/8 y 2π/8 respecto de una dirección *z* que acuerdan por adelantado, y Bob mide la polarización de sus fotones aleatoriamente en direcciones π/8, 2π/8 y 3π/8. Ellos comunican las direcciones de sus medidas de polarización públicamente, pero no los resultados, y dividen las mediciones en dos conjuntos: un conjunto en el que ambos midieron la polarización en la dirección π/8 o en el que ambos midieron la polarización en la dirección 2π/8, y otro conjunto en el que Alice midió la polarización en las direcciones 0 o 2π/8 y Bob midió las polarizaciones en las direcciones 2π/8 o 3π/8. Para el primer conjunto, cuando midieron la polarización en la misma dirección, los resultados son aleatorios pero perfectamente correlacionados en el estado entrelazado, de modo que pueden compartir estos bits aleatorios como una llave criptográfica. Y utilizan el segundo conjunto para constatar una desigualdad de Bell, cosa que revela si el estado entrelazado ha sido destruido por las mediciones de un espía o no (ver Ekert 1991).

Mientras que la diferencia entre la información clásica y la cuántica puede ser aprovechada para alcanzar una distribución de claves exitosa, existen otros protocolos criptográficos que se ven afectados por el entrelazamiento cuántico. El compromiso de bits es un protocolo criptográfico de claves que puede utilizarse como una subrutina en una variedad de tareas criptográficas importantes. En un protocolo de compromiso de bits, Alice entrega un bit

codificado a Bob.

La información disponible en la codificación debería ser insuficiente para que Bob pudiera determinar el valor del bit, pero suficiente, junto con información adicional provista por Alice en un estado subsecuente en el que se supone que ella revelará el valor del bit, para que Bob se convenza de que el protocolo no le permite a Alice hacer trampa codificando el bit en una forma que le permita a ella la posibilidad de revelar o 0 o 1 a voluntad.

Para ilustrar la idea, supongamos que Alice afirma su habilidad de predecir subas o bajas en el mercado de valores sobre una base diaria. Para dar credibilidad a su afirmación sin revelar información valiosa (quizás a Bob, un empleador potencial), ella sugiere la siguiente demostración: propone grabar su predicción, antes de que el mercado abra, escribiendo un 0 (para 'baja') o un 1 (para 'sube') en un pedazo de papel, que guardará en una caja de seguridad. La caja será enviada a Bob, pero Alice conservará la llave. Al final de las actividades comerciales del día, ella anunciará el bit que eligió y probará que de hecho se comprometió con anterioridad al entregarle la llave a Bob. Por supuesto, el protocolo de "llave y caja de seguridad" no es comprobablemente seguro para evitar que Bob haga una trampa, dado que no existe principio en la física clásica que evite que Bob abra la caja fuerte y la cierre sin dejar rastro alguno. La pregunta es, si existe un análogo cuántico de este procedimiento que sea incondicionalmente seguro: demostrablemente seguro por las leyes de la física contra cualquier mala acción de Alice o Bob. Bob puede hacer trampa si puede obtener *alguna* información sobre el compromiso de Alice antes de que ella lo revele (lo cual le daría una ventaja en repeticiones del protocolo con Alice). Alice puede hacer trampa si puede retrasar su elección de compromiso hasta la etapa final, cuando se le requiera revelar su compromiso, o si puede cambiar su compromiso en la etapa final con una probabilidad de detección muy baja.

Como resultante, el compromiso de bits incondicionalmente seguro entre dos partes, basado solamente en los principios de la mecánica clásica o cuántica (sin explotar las restricciones para señales que impone la relatividad especial, o los principios de la relatividad general o de la termodinámica) es imposible. Ver Mayers 1997, Lo and Chau 1997 y el artículo de Lo 'Quantum Cryptology' en Lo, Popescu y Spiller 1998 para una ulterior discusión. Kent (1999) ha demostrado que se puede implementar un protocolo de compromiso de bit clásico seguro utilizando condiciones de vínculo relativistas en una secuencia temporalizada de comunicaciones entre sitios verificablemente separados para Alice y Bob. En términos generales, la imposibilidad surge porque a cada paso del protocolo en el que se requiere que Alice o Bob realicen una elección determinada (realizar una medición sobre una partícula en el canal cuántico, elegir aleatoriamente y quizá condicionalmente entre un conjunto de acciones alternativas a ser implementadas en la partícula en el canal cuántico, etc.), la elección puede retrasarse entrelazando una o más partículas 'ancla' con la partícula del canal de una forma apropiada. Si se realizan las operaciones adecuadas en las anclas, la partícula del canal puede ser 'dirigida' de forma tal que la estrategia de la trampa sea indetectable. En efecto, si Bob no puede obtener información sobre el bit comprometido, entonces el entrelazamiento le permitirá a Alice 'dirigir' el bit a 0 o a 1 a voluntad.

5 Computación cuántica ↑

La información cuántica puede ser procesada, pero la accesibilidad a esta información está limitada por el límite de Holevo (mencionado en la Sección 3). David Deutsch (1985) fue el primero en mostrar cómo utilizar el entrelazamiento cuántico para realizar una tarea computacional imposible para una computadora clásica. Supongamos que tenemos una caja negra u oráculo, que evalúa una función Booleana *f*, donde los argumentos o entradas de *f* son 0 o 1 y los valores o salidas también son 0 o 1. Las salidas son o bien coincidentes para ambas entradas (en cuyo caso se dice que *f* es constante), o bien distintas para las dos entradas (en cuyo caso decimos que *f* es balanceada). Supongamos que estamos interesados en determinar si *f* es constante o balanceada. Clásicamente, la única forma de hacer esto es ejecutar pruebas de caja negra o preguntarle al oráculo dos veces, tanto para 0 como para 1, y pasar los valores (las salidas de *f*) a un circuito que determine si son iguales (para 'constantes') o diferentes (para 'balanceadas'). Deutsch mostró que si utilizamos estados cuánticos y compuertas cuánticas para almacenar y procesar la información, entonces podemos determinar si *f* es constante o balanceada en una sola evaluación de la función *f*. El truco es diseñar el circuito (la secuencia de compuertas) para producir la respuesta a una pregunta *global*

sobre la función, en un registrador de qubits de salida que pueda leerse o medirse.

Consideremos nuevamente la compuerta CNOT cuántica, con dos qubits ortogonales |0⟩ y |1⟩ como posibles entradas para el control, y |0⟩ como la entrada para el objetivo. Se pueden pensar el qubit control de entrada y el qubit objetivo de salida, respectivamente, como el argumento y el valor asociado de una función. Esta función CNOT asocia el valor 0 con el argumento 0 y el valor 1 con el argumento 1. Para una superposición lineal de los qubits ortogonales con coeficientes iguales como entrada del control, representada como |0⟩+|1⟩ (ignorando los coeficientes, por simplicidad), y el qubit |0⟩ como la entrada del objetivo, la salida es el estado entrelazado |0⟩|0⟩+|1⟩|1⟩, una superposición lineal en la cual el primer término representa el argumento 0 y el valor asociado 0 de la función CNOT, y el segundo término representa el argumento 1 y el valor asociado 1 de la función CNOT. El estado entrelazado representa todos los posibles argumentos y valores correspondientes de la función como una superposición lineal, pero esta información no es accesible. Lo que sí puede demostrarse que es accesible, si se realiza una elección adecuada de compuertas cuánticas, es la información acerca de si la función tiene ciertas propiedades globales o no. Esta información puede obtenerse sin leer la evaluación de ningún argumento individual o valor (en efecto, acceder a la información en el estado entrelazado sobre una propiedad global de la función requerirá normalmente perder acceso a toda la información acerca de los argumentos individuales y valores).

La situación es análoga para la función *f* de Deutsch. Aquí la salida de *f* puede ser representada tanto como |0⟩|0⟩+|1⟩|0⟩ o |0⟩|1⟩+|1⟩|1⟩ (en el caso 'constante'), o como |0⟩|0⟩+|1⟩|1⟩ o |0⟩|1⟩+|1⟩|0⟩ (en el caso 'balanceado'). Los dos estados entrelazados en el caso 'constante' son ortogonales en el espacio 4-dimensional de dos qubits, y generan un plano que representa una disyunción cuántica (|0⟩|0⟩+|1⟩|0⟩ *o* |0⟩|1⟩+|1⟩|1⟩). Llamemos a éste *plano constante*. Análogamente, los dos estados cuánticos en el caso 'balanceado' generan un plano, el *plano balanceado*, que representa una disyunción cuántica alternativa (|0⟩|0⟩+|1⟩|1⟩ *o* |0⟩|1⟩+|1⟩|0⟩). Estos planos, que representan dos disyunciones cuánticas alternativas, son ortogonales en el espacio de estados de 4 dimensiones, excepto por una superposición: una recta, que representa un estado (no entrelazado) de dos qubits (un estado producto, donde cada qubit por separado está en el estado |0⟩+|0⟩). Es por lo tanto posible diseñar una medición para distinguir las dos propiedades globales o disyuntivas alternativas de *f*, 'constante' o 'balanceada', con una cierta probabilidad (de hecho, un 50%) de error, cuando la medición arroja un resultado correspondiente al estado superpuesto, que es común a los dos casos. Sin embargo, sólo se necesita una consulta a la función cuando la medición logra identificar la propiedad global. Con una elección adecuada de las compuertas cuánticas, es incluso posible diseñar un circuito cuántico que siempre logra distinguir los dos casos en una sola ejecución.

El ejemplo de Deutsch muestra cómo la información cuántica, y el entrelazamiento cuántico, pueden ser utilizados para computar una propiedad disyuntiva o global de una función en un paso, lo cual, normalmente requeriría dos pasos. Mientras que el problema de Deutsch resulta un tanto trivial, existen ahora varios algoritmos cuánticos con aplicaciones interesantes, especialmente, el algoritmo de factorización de Shor que factoriza números enteros compuestos grandes en tiempo polinomial (con aplicaciones directas a la criptografía de 'clave pública', un esquema criptográfico clásico ampliamente utilizado), y el algoritmo de búsqueda de bases de datos de Grover. El algoritmo de Shor alcanza una velocidad exponencial sobre *cualquier* algoritmo clásico *conocido*. Para algoritmos a los que se les permite acceder a oráculos (cuya estructura interna es ignorada), se puede demostrar que la velocidad es exponencial sobre *cualquier* algoritmo clásico en algunos casos, por ejemplo, el algoritmo de Simon. Ver Nielsen y Chuang 2000, el artículo de Barenco "Quantum computation: an introduction" en Lo, Popescu y Spiller 1998, Bub 2006 (Sección 6), así como la entrada "Quantum computing" de la SEP.

Cabe notar que actualmente no hay ninguna prueba de que un algoritmo cuántico pueda resolver un problema NP-completo en tiempo polinomial, y por ello la eficiencia de las computadoras cuánticas relativa a las computadoras clásicas podría resultar ilusoria. Si hay en efecto una diferencia de velocidad, parece ser debido al fenómeno del entrelazamiento. La cantidad de bits requerida para describir un estado entrelazado general de *n* qubits crece exponencialmente con *n*. El espacio de estados (espacio de Hilbert) tiene 2^n dimensiones, de modo que un estado entrelazado general es una superposición de 2^n estados de *n*-qubits. En la mecánica clásica no existen estados entrelazados: un sistema compuesto general de *n*-bits se puede describir como *n* veces la cantidad de información requerida para describir un sistema de un solo bit. Por ello, la simulación clásica de un proceso cuántico involucraría un incremento exponencial en los recursos informacionales clásicos requeridos para representar al estado cuántico,

dado que el número de qubits que se entrelazan durante la evolución crece linealmente, y habría una desaceleración exponencial correspondiente al calcular la evolución, en comparación con la computación cuántica efectiva, realizada naturalmente por el sistema.

6 Observaciones interpretacionales ↑

Deutsch ha argumentado que la aceleración exponencial en la computación cuántica, y en general la forma en la que un sistema cuántico procesa información, sólo puede ser propiamente entendida en el marco de la interpretación de 'muchos mundos' de Everett (ver "Everett's Relative-State Formulation of Quantum Mechanics" y "Many Worlds Interpretation of Quantum Mechanics" en la SEP). La idea, a grandes rasgos, es que un estado entrelazado del tipo que aparece en la computación cuántica de una función, que representa una superposición lineal sobre todos los posibles argumentos y correspondientes valores de la función, debería entenderse como una computación clásica masivamente en paralelo, para todos los valores posibles de la función, en mundos paralelos. Para una crítica profunda de esta idea de 'paralelismo cuántico' como explicativa, ver Steane 2003.

Una visión alternativa, no muy discutida en la bibliografía respecto de esta cuestión, es la del abordaje lógico cuántico, que enfatiza la estructura no Booleana de las propiedades de los sistemas cuánticos. Las propiedades de un sistema clásico forman un álgebra Boole, básicamente la caracterización abstracta de una estructura conjuntista. Esto se fleja en el carácter Booleano de la lógica clásica y las compuertas Booleanas en una computadora clásica. Desde esta perspectiva, la imagen es completamente diferente. En lugar de 'computar todos los valores de una función al mismo tiempo', un algoritmo cuántico alcanza una velocidad exponencial por encima de un algoritmo clásico por computar la respuesta a una pregunta disyuntiva o global sobre una función (por ejemplo, si una función Booleana es constante o balanceada) sin computar información redundante (por ejemplo, los valores de la función para los distintos argumentos). Una diferencia fundamental entre la información cuántica y la clásica es la posibilidad de seleccionar una disyunción excluyente, que representa una propiedad global de una función, entre disyunciones alternativas posibles –por ejemplo, la disyunción 'constante', que afirma que el valor de la función (para ambos argumentos) es 0 o 1, o la disyunción 'balanceada', que afirma que el valor de la función (para ambos argumentos) es el mismo que el argumento *o* diferente del argumento– sin determinar los valores de verdad de los elementos de la disyunción.

Clásicamente, una disyunción es verdadera si y sólo si uno de sus elementos componentes es verdadero. El circuito cuántico de Deutsch logra su aceleración aprovechando la estructura no Booleana de las propiedades cuánticas para distinguir eficientemente entre dos propiedades disyuntivas, sin determinar los valores de verdad de los elementos relevantes de la disyunción (que representan la asociación entre argumentos individuales de la función y sus correspondientes valores). La clave del procedimiento es evitar la evaluación de la función para argumentos específicos en la determinación de la propiedad global, y es esta característica –imposible en la lógica Booleana de la computación clásica– la que conduce al aumento de la velocidad en comparación a los algoritmos clásicos (para una discusión sobre la lógica cuántica no específicamente en relación con la computación cuántica, ver la entrada "Quantum Logic and Quantum Probability" de la SEP).

Algunos investigadores en información cuántica y computación cuántica han argumentado en favor de una interpretación informacional de la mecánica cuántica. En su artículo sobre computación cuántica, Andrew Steane (1998, 119) realiza la siguiente observación:

"Históricamente, gran parte de la física fundamental se ha ocupado de descubrir las partículas elementales de la naturaleza y las ecuaciones que describen sus movimientos e interacciones. Ahora parece que un programa diferente podría ser igualmente importante: descubrir las formas en las que la naturaleza permite, y evita, que la *información* sea procesada y manipulada, en lugar de que las partículas se muevan."

Steane concluye su artículo con la siguiente propuesta radical:

"Para concluir, me gustaría proponer una tarea teórica de más largo alcance: elaborar un conjunto de principios como los de conservación de la energía y del momento, pero que se apliquen a la información, y a partir de los cuales la

mecánica cuántica pueda ser derivada. Dos pruebas de tales ideas serían si las correlaciones de Bell-EPR por ende se esclarecieran, y si ellas tornaran obvio el uso adecuado de términos tales como 'medición' y 'conocimiento'."

Existen extensos estudios en el marco de las así llamadas 'teorías de probabilidad generalizada' o de la teoría '*Boxworld',* acerca del problema de qué condiciones teorético-informacionales en la clase de las teorías 'sin señal' caracterizarían a las teorías cuánticas. Ver Brassard 2005, van Dam 2005, Skrzypczyk, Brunner y Popescu 2009, Pawlowski *et al*. 2009, Allcock *et al*. 2009, Navascues y Wunderlich 2009), Al-Safi y Short 2013 (ver en Herramientas académicas) y Ramanathan *et al*. para resultados interesantes en esta línea. Ver Fuchs 2014 para una perspectiva teorético-informacional radical.

7 Bibliografía ↑

Alcock, J., N. Brunner, M. Pawlowski y V. Scarani. 2009. "Recovering Part of the Quantum Boundary from Information Causality". *Physical Review A* 80: 040103.

Aspect, A., P. Grangier y G. Roger. 1982. "Experimental Tests of Bell's Inequalities Using Time-Varying Analyzers". *Physical Review Letters* 49: 1804-1807.

Barrett, J. 2007. "Information Processing in Generalized Probabilistic Theories". *Physical Review A* 75: 032304.

Barrett, J., L. Hardy y A. Kent. 2005. "No signaling and Quantum Key Distribution". *Physical Review Letters* 95: 010503.

Bell, J.S. 1964. "On the Einstein-Podolsky-Rosen Paradox". *Physics* 1: 195-200.

Bennett, C.H. y B.D. DiVicenzo. 2000. "Quantum Information and Computation". *Nature* 404: 247-255.

Bohr, N. 1935. "Can Quantum-Mechanical Description of Physical Reality be Considered Complete?". *Physical Review* 38: 696-702.

Born, M., ed. 1992. *The Born-Einstein Letters*. Dordrecht: Reidel.

Brassard, G. 2005. "Is Information the Key?". *Nature Physics* 1: 2-4.

Bub, J. 2006. "Quantum Information and Computation". En *Philosophy of Physics (Handbook of Philosophy of Science)*, editado por John Earman y Jeremy Butterfield, 555-660. Amsterdam: North Holland. [disponible online].

Bub, J. 2007. "Quantum Computation from a Quantum Logical Perspective". *Quantum Information and Computation* 7: 281-296.

Bub, J. 2008. "Quantum Computation and Pseudotelepathic Games". *Philosophy of Science* 75: 458-472.

Bub, J. 2015. *Bananaworld: Quantum Mechanics for Primates*. Oxford: Oxford University Press.

Deutsch, D. 1985. "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer". *Proceedings of the Royal Society (London)* A400: 97-117.

Deutsch, D. 1997. *The Fabric of Reality*. London: Penguin.

Dieks, D. 1982. "Communication by EPR Devices". *Physics Leters A* 92: 271-272.

Einstein, A., B. Podolsky y N. Rosen. 1935. "Can Quantum-Mechanical Description of Physical Reality be Considered Complete?". *Physical Review* 47: 777-780.

Ekert, A. 1991. "Quantum Cryptography Based on Bell's Theorem". *Physical Review Letters* 67: 661-663.

Ekert, A. y R. Renner. 2014. “The Ultimate Physical Limits of Privacy”. *Nature* 507: 443-447.

Everett, H. 1957. “'Relative State' Formulation of Quantum Mechanics”. *Reviews of Modern Physics* 29: 454-462.

Feynman, R. 1996. *Feynman Lectures on Computation*. Editado por J.G. Hey y R.W. Allen. Reading, MA: Addison-Wesley Publishing Company.

Fuchs, C.A. 2014. “An Introduction to QBism with an Application to the Locality of Quantum Mechanics”. *American Journal of Physics* 82: 749-754.

Holevo, A.S. 1973. “Statistical Problems in Quantum Physics”. En *Proceedings of the Second Japan-USSR Symposium on Probability Theory, editado por* G. Murayama y J.V. Prokhorov, 104-109. Berlin: Springer.

Kent, A. 1999. “Unconditionally Secure Bit Commitment”. *Physical Review Letters* 83: 1447-1450.

Kent, A. 2012. “Unconditionally Secure Bit Commitment by Transmitting Measurement Outcomes”. *Physical Review Letters* 109: 130501.

Lo, H.-K. y H. F. Chau. 1997. “Is Quantum Bit Commitment Really Possible?”. *Physical Review Letters* 78: 3410-3413.

Lo, H.-K., S. Popescu y T. Spiller. 1998. *Introduction to Quantum Computation and Information*. Singapore: World Scientific.

Mayers, D. 1997. “Unconditionally Secure Quantum Bit Commitment is Impossible”. *Physical Review Letters* 78: 3414-3417.

Navascues, M. y H. Wunderlich. 2009. “A Glance Beyond the Quantum Model”. *Proceedings of the Royal Society A* 466: 881-890 [disponible online].

Nielsen, M.A. y I.L. Chuang. 2000. *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press.

Pawlowski, M., T. Patarek, D. Kaszlikowski, V. Scarani, A. Winter y M. Zukowski. 2009. “A New Physical Principle: Informaiton Causality”. *Nature* 461: 1101.

Ramanathan, R., T. Patarek, A. Kay, P. Kurzynski y D. Kaszkilowski. 2010. “Local Realism of Macroscopic Correlations”. *Physical Review Letters* 107: 060405.

Schrödinger, E. 1935. “Discussion of Probability Relations Between Separated Systems”. *Proceedings of the Cambridge Philosophical Society* 31: 555-563; 32 (1936): 446-451.

Schumacher, B. 1995. “Quantum Coding”. *Physical Review A* 51: 2738-2747.

Shannon, C. E. y W. Weaver. 1949. *The Mathematical Theory of Communication*. Urbana: University of Illinois Press.

Skrzypczyk, P., N. Brunner y S. Popescu. 2009. “Emergence of Quantum Correlations from Nonlocality Swapping”. *Physical Review Letterrs* 102: 110402.

Steane, A. M. 1998. “Quantum Computing”. *Reports on Progress in Physics* 61: 117-173.

Steane, A. M. 2003. “A Quantum Computer Needs Only One Universe”. *Studies in History and Philosophy of Modern Physics* 34B: 469-478 [disponible online].

Timpson, C. G. 2013. *Quantum Information Theory and the Foundations of Quantum Mechanics*. Oxford: Oxford University Press.

van Dam, W. 2013. “Implausible consequences of superstrong nonlocality”. *Natural Computing* 12(1): 9-12.

van Fraassen, B. 1982. “The Charybdis of Realism: Epistemological Implications of Bell's Inequality”. *Synthese* 52: 25-38.

Wootters, W. K. y W. H. Zurek. 1982. “A Single Quantum Cannot be Cloned”. *Nature* 299: 802-803.

8 Cómo Citar ↑

Bub, Jeffrey. 2017. "Entrelazamiento cuántico e información". En Diccionario Interdisciplinar Austral, editado por Claudia E. Vanney, Ignacio Silva y Juan F. Franck.
URL=http://dia.austral.edu.ar/Entrelazamiento_cuántico_e_información

9 Derechos de autor ↑

ISSN: 2524-941X

10 Herramientas académicas ↑

Otros recursos en internet

Al-Safi, S.W., Short, A.J., 2013. “Reversible Dynamics in Strongly Non Local Boxworld Systems”, en PDF, manuscrito en ArXiv.org, arxiv.org/abs/1312.3931.

Herbst, T., Scheidl, T., Fink, M., Handsteiner, J., Wittmann, B., Ursin, R., Zeilinger, A., 2014. “Teleportation of Entanglement over 143 km”, en PDF, manuscrito en ArXiv.org, arxiv.org/abs/1403.0009.

arXiv E-print Archive for Quantum Physics.

Todd Brun's Lecture Notes in Quantum Information Processing.

John Preskill's Course on Quantum Information and Computation.

Quantum Information Processing at Oxford University.

Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences.

Group of Applied Physics, University of Geneva.

Centre for Quantum Technologies, University of Singapore.

Joint Quantum Institute, University of Maryland.

The Dream Machine. New Yorker article on quantum computing, 2011.

New Quantum Theory Could Explain the Flow of Time. Article in *Wired*, 2014, reprinted from *Quanta Magazine*.

Spooky Actions at a Distance? David Mermin's Openheimer Lecture.