Comunicación cuántica

Seminario: Introducción a la física cuántica segundo semestre 2025–2026

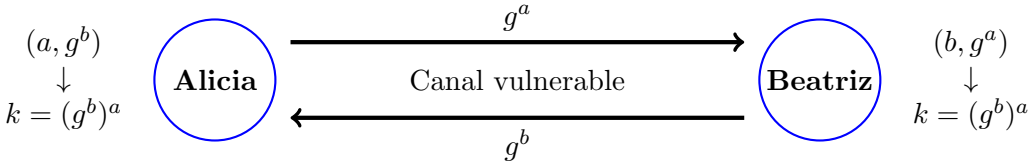
Fernando Chamizo https://matematicas.uam.es/~fernando.chamizo/

Las peculiaridades de la física cuántica permiten establecer, al menos teóricamente, métodos de comunicación impensables desde el punto de vista clásico. Por otro aparte, el inevitable efecto de las mediciones sobre los estados también impone severas restricciones.

3.1. Intercambio de claves

La criptografía de clave pública se enfrenta al reto de acordar un secreto a través de un canal vulnerable. En principio, parece un objetivo imposible. Sin embargo, con un ingenioso procedimiento elemental se alcanza a efectos prácticos bajo el supuesto de que no se desarrollen algoritmos o máquinas fuera de nuestro alcance hoy en día. El propósito de este apartado es mostrar uno de los métodos basados en la física cuántica que permiten compartir claves certificando que no se ha espiado el canal. Esta certificación tiene un fundamento teórico, es invulnerable a potenciales desarrollos técnicos futuros.

Antes de entrar en las sutilezas cuánticas, recordemos o aprendamos el *intercambio de claves de Diffie-Hellman* [5, §2.3] que es el procedimiento (no cuántico) usado extensivamente en la práctica. Consideremos el grupo $G=(\mathbb{Z}/p\mathbb{Z}-\{\bar 0\},\cdot)$ formado por las unidades de las clases módulo p con p un número primo muy grande, digamos que de cientos de dígitos binarios. Se sabe que G es cíclico. Sea g un generador de G (a efectos prácticos un elemento de orden muy grande bastaría). Dado $0<a<p$ hay algoritmos que permiten calcular g^a en un instante en cualquier ordenador moderno [5, §1.3.2]. Sin embargo, no se conocen algoritmos con los que un superordenador pueda recuperar a a partir de g^a exceptuando casos especiales. Esta situación da lugar al importante y no resuelto *problema del logaritmo discreto*: encontrar una manera eficiente de implementar $g^a\mapsto a$.



Si Alicia y Beatriz inventan por separado números secretos $0<a<p$ y $0<b<p$ y transmiten g^a y g^b, respectivamente, por un canal vulnerable que las conecta, Alicia estará en posesión de a y g^b, mientras que Beatriz conocerá b y g^a. De este modo, ambas pueden calcular fácilmente $k=(g^b)^a=(g^a)^b$ y usar k como una clave secreta común con la que

encriptar un mensaje. Lo importante es que la clave k no ha sido transmitida por el canal vulnerable. Un atacante que llegara a tener acceso a la información que circula por dicho canal, solo conseguiría g^a y g^b y los algoritmos y ordenadores conocidos no permiten recuperar en la práctica a y b.

Fantaseemos con críticas conspirativas a la expresión "los algoritmos y ordenadores conocidos". ¿Y si alguien ya ha resuelto el problema del logaritmo discreto y lo ha vendido a una empresa o gobierno que está sacando provecho? ¿Y si hay algún atajo guardado en secreto para calcular g^{ab} a partir de g^a y g^b sin resolver el problema del logaritmo discreto? ¿Y si una corporación ha creado ya un ordenador cuántico fiable a escala suficientemente grande? Se sabe que tal ordenador resolvería el problema del logaritmo discreto [9].

Existe un método para compartir claves basado en física cuántica a prueba de estas y otras conspiraciones. Tiene varias versiones y recibe el nombre genérico de *QKB* por las siglas de *Quantum Key Distribution*. Aquí solo veremos la versión más simple [6, §3.2] (véase en [1] una réplica del original).

Alicia inventa aleatoriamente dos listas (sucesiones) $\{L_n\}_{n=1}^N$ y $\{s_n\}_{n=1}^N$ con N grande. La primera es de letras, $L_n \in \{x, z\}$, y la segunda de signos, $s_n \in \{+, -\}$. Con ellas, Alicia envía a Beatriz un sistema de espín de N partículas en el estado correspondiente a

$$|\psi\rangle = |L_1 s_1\rangle \otimes |L_2 s_2\rangle \otimes \cdots \otimes |L_n s_n\rangle \,.$$

Por ejemplo, si $L_1 = z$, $L_2 = x$, $L_3 = x$, $s_1 = +$, $s_2 = +$, $s_3 = -$, entonces prepara la primera partícula en $|z+\rangle$, la segunda en $|x+\rangle$ y la tercera en $|x-\rangle$. Beatriz inventa también una lista aleatoria $\{L'_n\}_{n=1}^N$ con $L_n \in \{x, z\}$ y mide el espín de la n-ésima partícula en $|\psi\rangle$ con una máquina de Stern-Gerlach $\mathsf{SG}_{L'_n}$. El resultado será $\pm\frac{\hbar}{2}$ y de esa manera le podrá asignar un signo a cada partícula y construir una lista $\{s'_n\}_{n=1}^N$ con $s'_n \in \{+, -\}$. Si $L_n = L'_n$ entonces al medir $|L_n+\rangle$ con $\mathsf{SG}_{L'_n}$ es seguro que Beatriz obtendrá $+$ y al medir $|L_n-\rangle$ obtendrá $-$. Sin embargo, si $L_n \neq L'_n$ entonces el resultado de la medición será incierto pues $|\langle z + | x\pm\rangle|^2 = |\langle z - | x\pm\rangle|^2 = \frac{1}{2}$. Esto es,

$$L_n = L'_n \implies s_n = s'_n \qquad \text{y} \qquad L_n \neq L'_n \implies \begin{cases} s_n = s'_n & \text{con probabilidad } \frac{1}{2}, \\ s_n \neq s'_n & \text{con probabilidad } \frac{1}{2}. \end{cases}$$

Después del proceso de construcción de $\{s'_n\}_{n=1}^N$, Beatriz avisa a Alicia y ambas intercambian, por el canal vulnerable, sus listas $\{L_n\}_{n=1}^N$ y $\{L'_n\}_{n=1}^N$. Como han sido generadas al azar, se tendrá $L_{n_j} = L'_{n_j}$ para una subsucesión n_j de aproximadamente $N/2$ índices (recordemos que N se supone grande). Traduciendo los signos en bits mediante $+ \mapsto 0$, $- \mapsto 1$ Alicia y Beatriz pueden leer s_{n_j} como una clave común de aproximadamente $N/2$ bits que nunca ha sido transmitida.

La gracia de este procedimiento es que Alicia y Beatriz tienen una forma de verificar con certeza arbitrariamente grande si ha habido un espía y, en ese caso, desechar la clave como insegura. Como las listas $\{L_n\}_{n=1}^N$ y $\{L'_n\}_{n=1}^N$ solo se comparten tras la transmisión, un espía que quiera medir $|\psi\rangle$ lo tendrá que hacer sin conocer las direcciones. Con probabilidad $\frac{1}{2}$ equivocará la dirección y el estado de la n-ésima partícula colapsará a un estado erróneo. Un razonamiento elemental lleva a que cuando $L_n = L'_n$ se tiene $s_n \neq s'_n$ con probabilidad $\frac{1}{4}$. Alicia y Beatriz

pueden usar los primeros m bits de su clave común como comprobación compartiéndolos por el canal vulnerable y concluir que ha habido espionaje si hay algún caso con $s_{n_j} \neq s'_{n_j}$. En caso de espionaje,

$$\text{Prob}(s_{n_j} \neq s'_{n_j} \text{ para algún } j \leq m) = 1 - \Big(1 - \frac{1}{4}\Big)^m$$

que tiende rápidamente a uno. Así con $m = 80$ la probabilidad de que se pase por alto un ataque porque no se observa ningún caso con $s_{n_j} \neq s'_{n_j}$ es aproximadamente 10^{-10} (menor que la probabilidad de adivinar al azar una clave de 32 bits y comparable a acertar el premio gordo dos navidades seguidas). Estos m bits, como ya han sido compartidos por el canal inseguro, se eliminan de la clave común que pasa a ser la formada por el resto de los bits.

En [7, §12.6] hay una introducción sencilla y breve a los aspectos de la criptografía cuántica relacionados con QKD.

3.2. Limitaciones cuánticas

En las comunicaciones actuales lo digital suena más avanzado que lo analógico y también está extendida la idea entre el gran público de que lo cuántico supera o superará a lo digital. Sin embargo, hay muchas limitaciones teóricas y prácticas que se aplican al mundo cuántico y no al digital. En la jerga los impedimentos teóricos reciben el nombre genérico en inglés de *no-go theorems* (este apelativo también se usa a veces fuera de la física cuántica, pero en ella es más común). Típicamente están basados en las restricciones que imponen que la evolución de un sistema tenga que venir dada mediante un operador unitario, por el Postulado 2, y que las mediciones colapsen los estados, por el Postulado 3. Hay cerca de una decena de *no-go theorems* famosos aplicables a la comunicación cuántica. Aquí veremos tres básicos estrechamente relacionados entre sí.

Es imposible entender la sociedad de la información actual sin la capacidad de copiar. Más allá de actividades tramposas o piratas, esta capacidad es la que dota de relevancia a las memorias como integrantes fundamentales de los ordenadores y, en un plano humanista, permite que tengamos un legado cultural. Pues bien, en cierto sentido matemático, es imposible duplicar estados cuánticos generales.

Veamos en primer lugar un caso particular. Supongamos una partícula con cierto estado de espín que queremos conservar y copiarlo en una segunda partícula que, para fijar ideas, suponemos inicialmente en estado $|+\rangle$. Queremos que tal proceso de copia funcione siempre, es decir, que cualquier vector inicial normalizado $|\varphi\rangle \otimes |+\rangle$ evolucione al vector $|\varphi\rangle \otimes |\varphi\rangle$. En realidad, trabajar con los estados en vez de con los vectores permite cierta libertad con los factores multiplicativos, pero no la tendremos en cuenta por ahora. Si consideramos esta copia para $|+\rangle$ y para $|\psi\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$, se tiene

$$|{+}{+}\rangle \longmapsto |{+}{+}\rangle \qquad \text{y} \qquad |\psi\rangle \otimes |+\rangle \longmapsto \frac{1}{2}\big(\,|{+}{+}\rangle + |{+}{-}\rangle + |{-}{+}\rangle + |{-}{-}\rangle\,\big).$$

El Postulado 2 implica que la evolución de un sistema debe venir dada por un operador lineal unitario. La linealidad implica

$$|{-}{+}\rangle = \sqrt{2}\,|\psi\rangle - |{+}{+}\rangle \longmapsto \Big(\frac{\sqrt{2}}{2} - 1\Big)\,|{+}{+}\rangle + \frac{\sqrt{2}}{2}\Big(\,|{+}{-}\rangle + |{-}{+}\rangle + |{-}{-}\rangle\,\Big).$$

Pero esto no es compatible con que el operador sea unitario, porque tales operadores conservan la norma y la imagen del vector normalizado $|-+\rangle$ tiene norma mayor que 1.

Siendo optimistas, quizá el proceso de copia se pueda salvar considerando sistemas más complicados con más partículas o introduciendo factores multiplicativos en los vectores, los cuales no afectan a los estados, o permitiendo un estado distinto a $|+\rangle$ en la partícula auxiliar. El siguiente resultado matemático acaba con este optimismo.

Consideramos V un espacio de Hilbert sobre $\mathbb{C}$ con $\dim V > 1$. Tendremos en mente el caso finito dimensional, de hecho el caso de sistemas de espín $V = \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$, pero el argumento es general. Dado $\vec{v}_0 \in V - \{\vec{0}\}$ no existe ningún operador lineal unitario en $V \otimes V$ tal que

$$U(\vec{v} \otimes \vec{v}_0) = \lambda(\vec{v})\vec{v} \otimes \vec{v} \qquad \text{para todo } \vec{v} \in V \text{ normalizado}$$

donde $\lambda(\vec{v}) \in \mathbb{C}$. Por lo explicado antes, este *no-go theorem* impide el proceso de copia y por eso se le llama *teorema de no clonación*.

Para la prueba podemos suponer (multiplicando λ por una constante) que $\vec{v}_0$ está normalizado. Lo que caracteriza a las transformaciones unitarias es que preservan el producto escalar, por tanto, si existiera U, para $\vec{v}, \vec{w} \in V$ normalizados

$$\langle \vec{v} \otimes \vec{v}_0 | \vec{w} \otimes \vec{v}_0 \rangle = \lambda(\vec{v})\lambda(\vec{w}) \, \langle \vec{v} \otimes \vec{v} | \vec{w} \otimes \vec{w} \rangle$$

que usando la fórmula para el producto escalar en un producto tensorial equivale a

$$\langle \vec{v} | \vec{w} \rangle = \lambda(\vec{v})\lambda(\vec{w}) \langle \vec{v} | \vec{w} \rangle^2.$$

Con $\vec{v} = \vec{w}$ se deduce $|\lambda(\vec{v})| = 1$ para todo $\vec{v}$ normalizado, así que tomando módulos en la igualdad anterior $|\langle \vec{v} | \vec{w} \rangle| = |\langle \vec{v} | \vec{w} \rangle|^2$. Como $\dim V > 1$ existen $\vec{v}$ y $\vec{w}$ que no son linealmente dependientes y en ese caso la desigualdad de Cauchy-Schwarz es estricta: $|\langle \vec{v} | \vec{w} \rangle|^2 < \langle \vec{v} | \vec{v} \rangle \, \langle \vec{w} | \vec{w} \rangle = 1$. Si además escogemos $\vec{v}$ y $\vec{w}$ no ortogonales, se tiene

$$0 = |\langle \vec{v} | \vec{w} \rangle|^2 - |\langle \vec{v} | \vec{w} \rangle|^2 = |\langle \vec{v} | \vec{w} \rangle|^2 \big(1 - |\langle \vec{v} | \vec{w} \rangle|^2\big) > 0$$

que es una contradicción.

Es importante aclarar que sí se pueden clonar estados individuales, lo que no puede existir es un procedimiento, una máquina, que clone (copie) cualquier estado. Por ejemplo, con $\vec{v}_0 = |+\rangle$ el operador identidad en $\mathbb{C}^2 \otimes \mathbb{C}^2$ clona trivialmente $|+\rangle$ porque $|+\rangle \otimes |+\rangle$ se aplica en sí mismo, pero no clona $|-\rangle$ que se aplicaría en $|-+\rangle$. Por poner un ejemplo más complicado, el operador que actúa como la identidad en $|+\rangle \otimes \mathbb{C}^2$ y como $1 \otimes \sigma_1$ en $|-\rangle \otimes \mathbb{C}^2$ es unitario y permite clonar tanto $|+\rangle$ como $|-\rangle$ con $\vec{v}_0 = |+\rangle$, pero falla con otros estados.

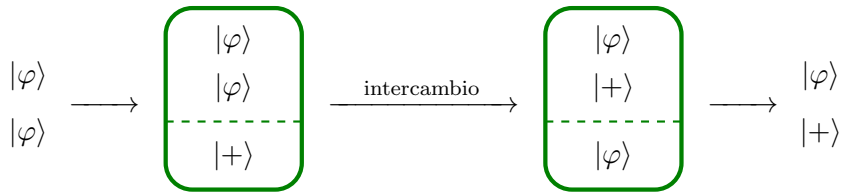
Con la misma notación que en el teorema de no clonación se tiene el *teorema de no borrado* que afirma que no existe U unitario tal que

$$U(\vec{v} \otimes \vec{v}) = \lambda(\vec{v})\vec{v} \otimes \vec{v}_0 \qquad \text{para todo } \vec{v} \in V \text{ normalizado.}$$

En realidad es un corolario del teorema de no clonación porque el inverso de un operador unitario es unitario.

Para terminar, veamos una versión más avanzada de este resultado que también recibe el nombre de teorema de no borrado, aunque la demostración es bien distinta.

A modo de motivación, imaginemos una máquina que admite dos partículas con cierto estado de espín como entrada y oculta en un "doble fondo" una tercera en el estado $|+\rangle$. La máquina actúa intercambiando la segunda partícula con la del doble fondo que seguirá oculta, mientras que muestra las otras dos como salida. En un esquema:



El intercambio define un operador unitario, por tanto, lícito. Aparentemente tenemos un contraejemplo al teorema de no borrado. El truco está está en que tal operador afecta a un sistema de tres partículas, no de dos. Desde el punto de vista matemático, estamos trabajando en $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$. La máquina no ha funcionado como una máquina común que vuelve a la situación inicial lista para volver a ser usada después de hacer su trabajo, sino que ha cambiado su estado almacenando una tercera partícula. La versión avanzada del teorema de no borrado dice intuitivamente que la única forma de que una máquina borre es que el estado presuntamente borrado se quede dentro.

Conservaremos la notación anterior e introduciremos un nuevo espacio vectorial W que representa el espacio de estados que añade la máquina. El nuevo *teorema de no borrado* afirma que dados $\vec{v}_0 \in V$ y $\vec{w}_0 \in W$ normalizados, si U es un operador unitario en $V \otimes V \otimes W$ tal que para cada $\vec{v} \in V$ normalizado existe $\vec{w} \in W$ tal que

$$U(\vec{v} \otimes \vec{v} \otimes \vec{w}_0) = \vec{v} \otimes \vec{v}_0 \otimes \vec{w}$$

entonces la aplicación $V \longrightarrow W$ dada por $\vec{v} \mapsto \vec{w}$ es una inmersión isométrica (un isomorfismo sobre su imagen conservando el producto escalar).

Al exigir la normalización de $\vec{v}_0$ y $\vec{w}_0$ es seguro que $\vec{w}$ está normalizado y se ha omitido el factor $\lambda(\vec{v})$ que aparece en los enunciados anteriores porque siempre se puede agrupar con $\vec{w}$, ya que $\lambda\vec{a} \otimes \vec{b} = \vec{a} \otimes (\lambda\vec{b})$.

En la prueba vamos a suponer $\dim V < \infty$, aunque no es estrictamente necesario, para poder trabajar con una base ortonormal finita $\mathcal{B}_V = \{\vec{v}_0, \cdots, \vec{v}_n\}$, $n \geq 1$. Siempre se puede conseguir con el proceso de Gram-Schmidt partiendo de $\vec{v}_0$. Los operadores unitarios conservan el producto escalar, por tanto definiendo $\vec{w}_j$ por medio de $U(\vec{v}_j \otimes \vec{v}_j \otimes \vec{w}_0) = \vec{v}_j \otimes \vec{v}_0 \otimes \vec{w}_j$ se tiene que $\mathcal{B}_S = \{\vec{w}_0, \cdots, \vec{w}_n\}$ es ortonormal, aunque no necesariamente una base de W sino de un subespacio $S \subset W$. Por la linealidad, escribiendo $\vec{v} = \sum_{j=0}^{n} \lambda_j \vec{v}_j$,

$$U(\vec{v} \otimes \vec{v} \otimes \vec{w}_0) = \sum_{j=0}^{n} \lambda_j^2 \vec{v}_j \otimes \vec{v}_0 \otimes \vec{w}_j + \sum_{j \neq k} \sum \lambda_j \lambda_k U(\vec{v}_j \otimes \vec{v}_k \otimes \vec{w}_0).$$

De acuerdo con la hipótesis del enunciado debe coincidir con

$$\vec{v} \otimes \vec{v}_0 \otimes \vec{w} = \sum_{j=0}^{n} \lambda_j \vec{v}_j \otimes \vec{v}_0 \otimes \vec{w}.$$

Al igualar la componente en la dirección $\vec{v}_\ell \otimes \vec{v}_0 \otimes \vec{w}_\ell$ de ambas expresiones se tiene $\lambda_\ell^2 + 0 = \lambda_\ell \mu_\ell$ con μ_ℓ la componente de $\vec{w}$ en la dirección $\vec{w}_\ell$, donde se ha usado que $\vec{v}_j \otimes \vec{v}_k \otimes \vec{w}_0 \perp \vec{v}_\ell \otimes \vec{v}_\ell \otimes \vec{w}_\ell$ para $j \neq k$ implica $U(\vec{v}_j \otimes \vec{v}_k \otimes \vec{w}_0) \perp \vec{v}_\ell \otimes \vec{v}_0 \otimes \vec{w}_\ell$. De esta forma $\mu_\ell = \lambda_\ell$, es decir, la proyección de $\vec{w}$ en S es $\sum_{j=0}^n \lambda_j \vec{w}_j$. Si $\vec{w} \in S$, la aplicación $\vec{v} \mapsto \vec{w}$ es la que envía $\sum_{j=0}^n \lambda_j \vec{v}_j$ a $\sum_{j=0}^n \lambda_j \vec{w}_j$, en particular transforma la base ortonormal $\mathcal{B}_V$ de V en la base ortonormal $\mathcal{B}_S$ de S. Por tanto, define una isometría entre ambos espacios.

El cabo suelto (que parece que se pasa por alto en la demostración original [8]) es garantizar $\vec{w} \in S$ mostrando que no tienen componente $\mu \neq 0$ en la dirección $\vec{u}$ para ningún vector unitario fijado $\vec{u} \in S^\perp$. Considerando esta vez la componente en la dirección $\vec{v}_\ell \otimes \vec{v}_0 \otimes \vec{u}$, la igualdad $U(\vec{v} \otimes \vec{v} \otimes \vec{w}_0) = \vec{v} \otimes \vec{v}_0 \otimes \vec{w}$ conduce a

$$\sum_{j \neq k} \sum a_{jk\ell} \lambda_j \lambda_k = \lambda_\ell \mu$$

con $a_{jk\ell}$ constantes. Si $\mu \neq 0$ la forma cuadrática no es idénticamente nula. Sea λ_m con $m \neq \ell$ una variable que aparece explícitamente en ella, entonces

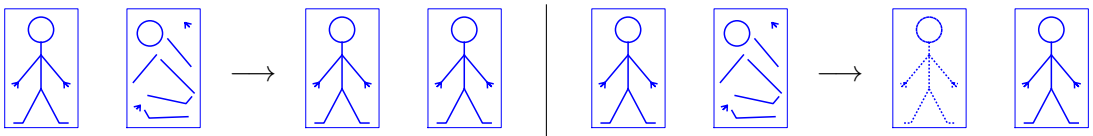
$$\sum_{j \neq k} \sum \big(\lambda_m a_{jk\ell} - \lambda_\ell a_{jkm}\big) \lambda_j \lambda_k = \lambda_m \lambda_\ell \mu - \lambda_\ell \lambda_m \mu = 0,$$

lo cual es una contradicción porque el primer miembro tiene grado dos en λ_m, ya que $j \neq k$ fuerza a que λ_m aparezca a lo más una vez en cada producto $\lambda_\ell \lambda_j \lambda_k$.

Un apunte final es que las versiones originales [10] y [4] del teorema de no clonación también incorporaban en su enunciado vectores como $\vec{w}_0$ y $\vec{w}$ que representaban el posible cambio de estado de una potencial máquina de clonar.

3.3. Teletransporte

Se podría bromear diciendo que la afirmación tan repetida de que el *teletransporte* (más conocido por el calco inglés *teleportación*) es un fenómeno puramente cuántico imposible dentro de la física clásica es un prejuicio moral porque teletransportar clásicamente a alguien requeriría un asesinato: Si queremos teletransportar a una persona P a la Luna, llevamos primero allí reservas de todos los átomos de los elementos que componen el cuerpo humano. Después examinamos la posición y el estado de cada uno de los átomos que componen P, que son del orden de 10^{28}, enviamos esos datos a los operarios de la Luna y allí colocan átomos de sus reservas en las posiciones y estados indicados. Con ello se obtiene una persona P' en la Luna idéntica a P y sólo queda eliminar a P. En suma, la física clásica permite el teletransporte como una clonación en la que se elimina el original.



Teletransporte clásico (clonación) | Teletransporte cuántico

Tras el teorema de no clonación, parece que las dificultades para teletransportar deben aparecer en el lado cuántico. Lo curioso es que hay un artificio teórico muy ingenioso (relativamente reciente [2]) que permite que una partícula adquiera el estado original de espín de otra antes de que haya sido afectada por una medición. Si las dos partículas están muy alejadas, podemos considerar que hemos teletransportado el estado de la partícula. Es como tener una fotocopiadora que solo puede hacer una copia perfecta a cambio de emborrar el original.

Es importante insistir en que el teletransporte cuántico no es el de la ciencia ficción: hay que tener previamente en el lugar de destino una partícula como la que se quiere teletransportar y hay que llamar a los operarios para darles información que permita modificar su estado. El nombre sugerente no refleja lo que el gran público entiende por teletransporte. Si llamo a alguien para explicarle una receta ¿he teletransportado el plato que hay en mi mesa? Pues el teletransporte cuántico es como si tuviera que comerme primero mi plato (destruirlo con una medición) para que otro lo pueda cocinar en otro lugar con mis indicaciones, incluso si yo no he aprendido la receta.

El argumento teórico que permite el teletransporte cuántico es más claro con una representación del operador que intercambia (los estados de espín de) dos partículas en términos de las matrices de Pauli. En términos matemáticos, tal operador de intercambio S es el operador lineal en $\mathbb{C}^2 \otimes \mathbb{C}^2$, un isomorfismo, que cumple $S(\vec{v} \otimes \vec{w}) = \vec{w} \otimes \vec{v}$. Utilizando el producto de Kronecker se tiene que en la base usual $\{|{+}{+}\rangle, |{+}{-}\rangle, |{-}{+}\rangle, |{-}{-}\rangle\}$ el operador

$$P = 1 + \sum_{j=1}^{3} \sigma_j \otimes \sigma_j \qquad \text{tiene matriz} \qquad \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

Claramente esta matriz es el doble de la de S en la base indicada (nótese que $|{+}{-}\rangle \leftrightarrow |{-}{+}\rangle$ bajo S) de lo que se deduce $P = 2S$.

Digamos que Alicia tiene un partícula con estado de espín correspondiente a $|\varphi\rangle$ que desea teletransportar al lugar donde está Beatriz. Para ello crean un sistema auxiliar de dos partículas entrelazadas en el estado de Bell $|\Phi_0\rangle$. Si consideramos que estas son las partículas 1 y 3 mientras que la inicial es la 2, el estado conjunto del sistema es

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\big(\,|{+}\rangle \otimes |\varphi\rangle \otimes |{+}\rangle + |{-}\rangle \otimes |\varphi\rangle \otimes |{-}\rangle\,\big).$$

Suponemos que Alicia guarda las partículas 1 y 2 y Beatriz la 3. El objetivo es pasar el estado de la 2 a la 3. La relación $P = 2S$ permite escribir

$$|\Psi\rangle = \frac{1}{2\sqrt{2}}\big(\,|{+}\rangle \otimes P(|{+}\rangle \otimes |\varphi\rangle) + |{-}\rangle \otimes P(|{-}\rangle \otimes |\varphi\rangle)\big).$$

Al recordar las definiciones de P y de la base de Bell, esta expresión se simplifica a

$$|\Psi\rangle = \frac{1}{2}\sum_{j=0}^{3} |\Phi_j\rangle \otimes \sigma_j\,|\varphi\rangle \qquad \text{bajo el convenio } \sigma_0 = 1.$$

Como la base de Bell es una base ortonormal, las proyecciones sobre sus elementos están en las hipótesis del Postulado 3. Si Alicia las utiliza para medir el estado de las dos partículas en su poder obtendrá en su aparato de medición un resultado $0 \leq j \leq 3$ y $|\Psi\rangle$ colapsará a $|\Phi_j\rangle \otimes \sigma_j |\varphi\rangle$. Esto significa que el estado de la partícula que tiene Beatriz se ha transformado en $\sigma_j |\varphi\rangle$. Al ser σ_j una matriz unitaria, el Postulado 2 sugiere que existe una "ecuación de Schrödinger" tal que al dejar evolucionar el tiempo $\sigma_j |\varphi\rangle$ pasa a ser $\sigma_j^2 |\varphi\rangle = |\varphi\rangle$, en suma, el estado se ha teletransportado de la partícula original de Alicia a la de Beatriz. Por ser más concretos sobre la aplicación de σ_j, en teoría con un campo magnético se puede "girar" el espín de un electrón[1] a través de un operador de rotación $R_{\vec{u}}(\alpha)$ y si $\vec{u} = \vec{e}_j$, $\alpha = \pi$ se obtiene $-i\sigma_j$ que da lugar al mismo estado que σ_j.

Estado inicial		Medición de Alicia		Operador unitario de Beatriz
$\|\Psi\rangle$	$\longrightarrow$	$\|\Phi_j\rangle \otimes \sigma_j \|\varphi\rangle$	$\xrightarrow{j}$	$\|\Phi_j\rangle \otimes \|\varphi\rangle$

No hay que perder de vista que Alicia le debe comunicar a Beatriz el j que ha obtenido. A pesar de que el Postulado 3 propugna un colapso instantáneo, hasta que Beatriz no reciba la información del valor de j por un canal convencional (¿una llamada de teléfono?) no podrá aplicar σ_j y estar segura de que su partícula ha adquirido el estado de $|\varphi\rangle$. Esta aplicación de σ_j corresponde a una evolución de la partícula (por ejemplo, bajo un campo magnético) y no entraña ninguna medición que destruiría el estado.

El teletransporte está estrechamente ligado al entrelazamiento y, como este, ha sido verificado experimentalmente, comenzando con [3], y se han alcanzado distancias bastante largas. Esto no significa que las comunicaciones cuánticas, sobre todo con sus implicaciones criptográficas, estén cerca de competir a corto plazo con las clásicas que a día de hoy son más sencillas, más baratas y mucho más fiables.

Ejercicios de la sección 3

Ejercicio 1. Supongamos que en un intercambio de claves QKD Alicia usa las listas de letras y signos $zxxzzz$ y $+-+---$. Si Beatriz emplea la lista de letras $zzxzxz$, halla las posibilidades para su lista de signos y las probabilidades con las que aparecen. Con la traducción en bits $+ \mapsto 0$, $- \mapsto 1$, ¿qué clave acordarían?

Ejercicio 2. Explica con detalle por qué al compartir claves con el procedimiento QKD descrito se cumple $\text{Prob}(s_{n_j} \neq s'_{n_j} \text{ para algún } j \leq m) = 1 - 3^m/4^m$ en caso de que haya habido espionaje.

Ejercicio 3. En la prueba del teorema de no clonación se usa que en un espacio de Hilbert V sobre $\mathbb{C}$ con $\dim V > 1$ siempre existen $\vec{v}, \vec{w} \in V$ unitarios que no son ni ortogonales ni linealmente dependientes. ¿Sabrías dar una prueba rigurosa y breve? ¿Qué ocurre en los teoremas de no clonación y de no borrado si se permite $\dim V = 1$?

[1] En la práctica, trabajar de esta forma sería técnicamente complicadísimo debido a que la carga eléctrica del electrón induce efectos añadidos.

Ejercicio 4. Sea $T = \frac{1}{2}(1+\sigma_1)\otimes 1 + \frac{1}{2}(1-\sigma_1)\otimes\sigma_3$. Halla la matriz de T en la base usual $\{|{+}{+}\rangle, |{+}{-}\rangle, |{-}{+}\rangle, |{-}{-}\rangle\}$. Comprueba que T define un operador unitario y que clona tanto $|x{+}\rangle$ como $|x{-}\rangle$ tomando $\vec{v}_0 = |x{+}\rangle$. Encuentra también un estado que no sea clonado por T.

Ejercicio 5. Halla el máximo número de estados de la forma $|\varphi\rangle\otimes|{+}\rangle$ en $\mathbb{C}^2\otimes\mathbb{C}^2$ tales que existe un operador unitario que los aplica en $|\varphi\rangle\otimes|\varphi\rangle$. Generaliza el resultado a $\mathbb{C}^2\otimes\overset{2N\text{ veces}}{\cdots\cdots}\otimes\mathbb{C}^2$. Indicación: Revisa la demostración del teorema de no clonación y nota que se cuentan estados, no de vectores, por tanto, los factores escalares no cambian el resultado.

Ejercicio 6. Sea $|\varphi_0\rangle = \alpha\,|{+}\rangle + \beta\,|{-}\rangle$ normalizado, $|\alpha|^2 + |\beta|^2 = 1$. Encuentra un operador unitario en $\mathbb{C}^2\otimes\mathbb{C}^2$ que borre $|{+}{+}\rangle$ y $|{-}{-}\rangle$ usando $|\varphi_0\rangle$ como vector de borrado, es decir, que los aplique respectivamente en $\lambda_1\,|{+}\rangle\otimes|\varphi_0\rangle$ y $\lambda_2\,|{-}\rangle\otimes|\varphi_0\rangle$ con algunos $\lambda_1, \lambda_2 \in \mathbb{C}$.

Ejercicio 7. Escribe la matriz de $P = 1 + \sum_{j=1}^{3}\sigma_j\otimes\sigma_j$ en la base de Bell.

Ejercicio 8. Al aplicar el esquema de teletransporte, calcula la probabilidad de que el estado se haya teletransportado tras la medición de Alicia. Es decir, de que Beatriz no tenga que aplicar ningún operador unitario.

Ejercicio 9. Demuestra que el operador C que permuta cíclicamente tres partículas con un estado de espín, esto es, el operador $C(\vec{u}_1\otimes\vec{u}_2\otimes\vec{u}_3) = \vec{u}_3\otimes\vec{u}_1\otimes\vec{u}_2$ en $\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^2$, es igual a $\frac{1}{4}\sum_{j,k=0}^{3}\sigma_j\otimes(\sigma_j\sigma_k)\otimes\sigma_k$, donde se usa el convenio $\sigma_0 = 1$. Encuentra una expresión similar para su inverso que aplica $\vec{u}_1\otimes\vec{u}_2\otimes\vec{u}_3$ en $\vec{u}_2\otimes\vec{u}_3\otimes\vec{u}_1$. Indicación: ¿Cómo se puede expresar C en términos del operador que intercambia dos partículas?

Referencias

[1] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. arXiv:2003.06557 [quant-ph], 2020.

[2] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, Mar 1993.

[3] D. Boschi, S. Branca, F. de Martini, L. Hardy, and S. Popescu. Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 80(6):1121–1125, feb 1998.

[4] D. Dieks. Communication by EPR devices. *Physics Letters A*, 92(6):271–272, 1982.

[5] J. Hoffstein, J. Pipher, and J. H. Silverman. *An introduction to mathematical cryptography.* Undergraduate Texts in Mathematics. Springer, New York, 2008.

[6] M. Nakahara and T. Ohmi. *Quantum computing.* CRC Press, Boca Raton, FL, 2008. From linear algebra to physical realizations.

[7] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, Cambridge, 2000.

[8] A. K. Pati and S. L. Braunstein. Quantum no-deleting principle and some of its implications. arXiv:quant-ph/0007121, 2000.

[9] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.*, 41(2):303–332, 1999.

[10] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, Oct 1982.