Apuntes de las clases de Física Cuántica
Juan Pablo Paz 2020

4

14 de mayo de 2020

Postulados de la mecánica cuántica

La mecánica cuántica puede formularse axiomáticamente y eso es lo que haremos en este capítulo. Como veremos, esta formulación axiomática es abstracta. Algunas de las propiedades que dieron lugar al surgimiento de la mecánica cuántica (la complementariedad, las relaciones de incertidumbre de Heisenberg, etc.) no forman parte de esos axiomas. Por el contrario, se deducen como consecuencia de ellos. Por eso, primero formularemos los axiomas (o postulados) y luego los comentaremos y, en algunos casos los generalizaremos.

4.1. Los Postulados Cinemáticos: 1-5

Postulado 1 *El estado de todo sistema físico está representado por un vector (de norma unidad) en un espacio de Hilbert $\mathcal{H}$.*

Un espacio de Hilbert es un vectorial complejo, con un producto interno hermitiano y que satisface el axioma de completitud.

La dimensión de dicho espacio es igual al número de resultados distintos que se obtienen en un análisis exhaustivo (completo) del sistema. En realidad, como veremos luego, un vector en un espacio de Hilbert representa un estado "de máxima información" (un estado "puro"). Generalizaremos esta noción más adelante.

Postulado 2 *Todas las propiedades observables de un sistema físico se representan por un operadores lineales hermíticos que actúan sobre $\mathcal{H}$.*

Denominaremos al espacio de operadores lineales hermitianos que actúan sobre el espacio de Hilbert $\mathcal{H}$ como $\mathcal{L}(\mathcal{H})$.

Todo operador hermítico $\hat{A}$ tiene una base completa de autovectores. Denotamos a los autovalores reales de $\hat{A}$ como a_n, con $n = 1,...,K$. Cada autovalor tiene asociado un subespacio (el subespacio generado por los autovectores que tienen ese autovalor). Denotaremos como P_n al proyector asociado a ese subespacio.

La descomposición espectral de $\hat{A}$ es $\hat{A} = \sum_{n=1}^{K} a_n P_n$. Si $\hat{A}$ es no degenerado, los proyectores P_n son de rango 1 y se escriben como $P_n = |\phi_n\rangle\langle\phi_n|$. En ese caso K es la dimensión del espacio de estados y los vectores $|\phi_n\rangle$ forman una base ortonormal de $\mathcal{H}$. En cambio, si el $\hat{A}$ es degenerado y g_n es la degeneración del autovalor a_n, entonces podemos escribir los proyectores P_n como $P_n = \sum_{l=1}^{g_n} |\phi_{nl}\rangle\langle\phi_{nl}|$ (donde todos los vectores $|\phi_{nl}\rangle$ satisfacen $\hat{A}|\phi_{nl}\rangle = a_n|\phi_{nl}\rangle$ para todo $l = 1,..,g_n$).

Postulado 3 *Los resultados posibles de la medición de cualquier observable $\hat{A}$ son sus autovalores a_n.*

Este postulado lleva implícita una noción sobre lo que quiere decir "medir". Si bien esta noción es intuitiva, vale la pena discutirla más extensamente (cosa que haremos más adelante). Es suficiente decir aquí que este postulado es compatible con la idea descripta en los capítulos anteriores: medir quiere decir filtrar un haz incidente (descripto por un estado cualquiera) dando lugar a un conjunto de haces, cada uno de los cuales corresponde a un autovalor distinto a_n.

Postulado 4 (Regla de Born) *Si el estado de un sistema es $|\psi\rangle$, la probabilidad de obtener el resultado a_n en la medición del observable $\hat{A}$ es siempre* $\text{Prob}(a_n||\psi\rangle) = \langle\psi|P_n|\psi\rangle$, *donde P_n es el proyector asociado al autovalor a_n.*

Si $\hat{A}$ es no degenerado entonces $P_n = |\phi_n\rangle\langle\phi_n|$ y la probabilidad resulta ser $\text{Prob}(a_n||\psi\rangle) = |\langle\phi_n|\psi\rangle|^2$. En el caso degenerado P_n tiene rango g_n y puede expresarse como la suma de los proyectores asociados a cualquier base en el subespacio de los estados con autovalor a_n:

$$\text{Prob}(a_n||\psi\rangle) = \sum_{l=1}^{g_n} |\langle\phi_{nl}|\psi\rangle|^2 \tag{4.1}$$

Antes de pasar al último postulado cinemático conviene introducir las siguientes definiciones: diremos que el valor medio del operador $\hat{A}$ en el estado $|\psi\rangle$ es

$$\langle\hat{A}\rangle = \langle\psi|\hat{A}|\psi\rangle \tag{4.2}$$

(esto también suele denominarse "valor de expectación de $\hat{A}$ en el estado $|\psi\rangle$"). El motivo del nombre se vuelve evidente si recordamos que la descomposición espectral de $\hat{A}$ es $\hat{A} = \sum_n a_n P_n$. Teniendo en cuenta el Postulado 4 y la definición de $\langle\hat{A}\rangle$, podemos escribir

$$\langle\hat{A}\rangle = \sum_n a_n \, \text{Prob}(a_n||\psi\rangle).$$

De donde se ve que la magnitud $\langle \hat{A} \rangle$ no es otra cosa que el promedio estadístico de los resultados que se obtiene al medir $\hat{A}$ muchas veces (de ahí, el nombre "valor medio"). También podemos definir la dispersión de un operador $\hat{A}$ en el estado $|\psi\rangle$ como

$$\Delta^2 \hat{A} = \langle \hat{A}^2 \rangle - \langle \hat{A} \rangle^2. \tag{4.3}$$

Usando las definiciones anteriores podemos ver que ΔA es la dispersión estadística de los resultados de la medición ya que $\Delta^2 \hat{A} = \sum_n a_n^2 \, \mathrm{Prob}(a_n \big| |\psi\rangle) - \langle \hat{A} \rangle^2$.

Con las definiciones anteriores, el Postulado 4 puede formularse equivalentemente diciendo que la probabilidad de obtener el resultado a_n es el valor medio del proyector correspondiente P_n.

Postulado 5 (Postulado de proyección o colapso) *Si el estado de un sistema es $|\psi\rangle$, medimos el observable $\hat{A}$ y detectamos el autovalor a_n, entonces el estado del sistema después de la medición $|\psi'\rangle$ se obtiene a partir de la proyección de $|\psi\rangle$ sobre el subespacio asociado al autovalor a_n.*

Si llamamos $|\psi'\rangle$ a el estado luego de la detección de a_n entonces tenemos que

$$|\psi'\rangle = \frac{P_n|\psi\rangle}{\langle \psi|P_n|\psi\rangle^{1/2}} \, . \tag{4.4}$$

Donde hemos normalizado el estado posterior a la medición.

Para el caso no degenerado, el factor de normalización se simplifica $\langle \psi|P_n|\psi\rangle^{1/2} = |\langle \phi_n|\psi\rangle|$, y por lo tanto el estado luego de la medición es $|\psi'\rangle = |\phi_n\rangle$.

Este postulado en realidad no es cinemático ya que habla sobre la evolución de un sistema cuando se realiza una medición. Es la consecuencia natural de concebir al proceso de medición como un proceso de filtrado, tal como se describió en el caso del spin. Teniendo en cuenta que más arriba dijimos que "el estado es información", este postulado nos trae aparejados problemas conceptuales serios. Al registrar el resultado a_n adquirimos información y por lo tanto tenemos que actualizar la descripción del sistema cambiando el estado. El sistema, indudablemente, cambia en el proceso de medición ya que interactúa con otro (el aparato de medición). Este cambio, en la visión que estamos presentando, es simplemente el cambio en la información de la que disponemos sobre el sistema.

En lo que sigue, haremos una serie de comentarios y generalizaciones de los postulados que describimos más arriba.

4.2. Estados Puros y Mixtos

4.2.1. Estados Puros

Los estados puros son estados de información máxima. Los estados puros son aquellos que se describen por medio de un vector en $\mathcal{H}$. De los postulados se infiere el motivo por el cual los estados puros son de máxima información. En efecto,

si el estado es $|\phi\rangle$ siempre existe un experimento cuyo resultado puede predecirse con certeza. Esto sucede para cualquier experimento que consista en la medición de un observable cuya base de autoestados contiene a $|\phi\rangle$ con autovalor no degenerado. En ese caso la mecánica cuántica predice certezas. En cualquier otro, predice probabilidades no triviales.

Los estados puros son proyectores. De los postulados enunciados, podemos deducir que todas las predicciones que hace la mecánica cuántica son las mismas si el estado es descripto por el vector $|\psi\rangle$ o por cualquier otro vector $|\psi'\rangle$ que sea de la forma $|\psi'\rangle = \exp(i\theta)|\psi\rangle$. Es decir, dos vectores que difieren en una fase describen el mismo estado o, equivalentemente, una fase global no cambia el estado. Podemos convencernos de esto estudiando los postulados. Por su construcción, el postulado 4 (regla de Born), elimina explícitamente estas fases como se verifica en la ecuación 4.1 y de su versión para operadores no degenerados $\text{Prob}(a_n \big| |\psi\rangle) = |\langle\phi_n|\psi\rangle|^2$.

Teniendo esto en cuenta, el primer postulado, tal como lo formulamos más arriba, es en realidad incompleto (o incorrecto). Un estado físico no se describe por un único vector sino por una familia de vectores. Todos esos vectores se relacionan entre si por vía de la multiplicación por un número complejo de módulo unidad. Esto define un rayo en el espacio de Hilbert. La descripción matemáticamente correcta del estado de máxima información sobre un sistema no es mediante un vector $|\psi\rangle$ sino mediante el proyector $\rho_\psi = |\psi\rangle\langle\psi|$. El Postulado 1 debería decir *''El estado de máxima información de un sistema físico se representa mediante un proyector de rango 1 y traza unidad sobre un espacio de Hilbert"*.

El proyector sobre el estado $|\psi\rangle$ es idéntico al proyector sobre el estado $|\psi'\rangle$ ya que en el proyector desaparece la ambiguedad en la elección de la fase. En términos de este proyector, podemos reescribir la regla de Born para calcular las probabilidades asociadas a los distintos resultados de una medición de la siguiente manera:

$$\text{Prob}(a_n \big| |\psi\rangle) = \langle\psi|P_{a_n}|\psi\rangle = \text{Tr}(\rho_\psi \; P_n).$$

En general, el valor medio de cualquier operador $\hat{A}$ se calcula entonces como

$$\langle\hat{A}\rangle = \text{Tr}(\rho_\psi \hat{A}).$$

4.2.2. Estados mixtos, la matriz densidad

En la mayoría de las situaciones de interés físico no somos capaces de preparar estados puros (que se representan por vectores, o por proyectores de rango 1). Por ejemplo, en el experimento de Stern Gerlach prepamos el estado $|0_n\rangle$ tomando las partículas que salen por la rama superior de un aparato de SG_n. Sin embargo, nunca es posible mantener la alineación del imán en una dirección inalterada. Inevitablemente, debido a que nuestra capacidad de control es finita, el eje del imán tendrá desviaciones o fluctuaciones pequeñas alrededor de una dirección principal $\vec{e}_n$.

Por simplicidad, supongamos que el imán puede estar orientado en k direcciones $\vec{e}_i$, con $i = 1, ..., k$ y que a cada una de ellas se le puede asignar una probabilidad

p_i. En una situación como esta, no obtenemos siempre el mismo estado sino que, con probabilidad p_i preparamos el estado $|0_i\rangle$. Esto es lo que se denomina un estado "mixto" que no es otra cosa que un "ensemble", un conjunto de estados puros, cada uno con una probabilidad diferente.

En general, diremos que un ensemble es un conjunto de estados con una probabilidad asociada a cada uno de ellos: $\mathcal{E} = \{|\phi_i\rangle,\ p_i,\ i = 1,...,k\}$. A diferencia de lo que sucede con un estado puro, en este caso no existe ningún experimento en el cual podamos predecir resultados con certeza. Por eso, este estado no es un estado de máxima información y lo llamamos mixto.

Los estados mixtos se describen matemáticamente mediante con el operador al que se denomina "operador densidad" o "matriz densidad" definido como

$$\rho = \sum_{i=1}^{k} p_i |\phi_i\rangle\langle\phi_i|, \tag{4.5}$$

con la condición de normalización $\sum p_i = 1$. Veamos que un operador así definido cumple con lo que esperamos de él. En primer lugar, vemos que si un $p_i = 1$ entonces el debe ser nulo y tenemos que la matriz densidad describe un estado puro. En segundo lugar queremos probar que a partir de ρ podemos calcular cualquier probabilidad $\text{Prob}(a_n\big|\ \mathcal{E})$ asociada al estado mixto. Veamos: si el estado fuera $|\phi_i\rangle$, la probabilidad de obtener el resultado a_n al medir $\hat{A}$ es $\text{Prob}(a_n\big||\phi_i\rangle) = \langle\phi_i|P_n|\phi_i\rangle$. Pero si preparamos $|\phi_i\rangle$ con probabilidad p_i, la probabilidad total de obtener a_n es

$$\begin{aligned}
\text{Prob}(a_n\big|\ \mathcal{E}) &= \sum_i p_i \text{Prob}(a_n\big|\ |\phi_i\rangle) \\
&= \sum_i p_i\ \text{Tr}(|\phi_i\rangle\langle\phi_i|\ P_n) \\
&= \text{Tr}(\sum_i p_i\ |\phi_i\rangle\langle\phi_i|\ P_n) \\
&= \text{Tr}(\rho\ P_n).
\end{aligned}$$

De donde vemos que cualquier probabilidad puede obtenerse a partir de la matriz densidad del estado. Por lo tanto, diremos que el operador ρ representa al estado del sistema.

Cabe notar que en general los estados $|\phi_i\rangle$ no necesariamente son ortogonales entre si. Esto sucede, por ejemplo, en el aparato de Stern-Gerlach para el caso de fluctuaciones en el eje del imán o el gradiente del campo magnético no fuera uniforme sobre el tamaño del haz de átomos. Si estas fluctuaciones son pequeñas, los estados $|\phi_i\rangle$ serán distintos, pero no ortogonales entre si.

El operador densidad tiene propiedades importantes:

1. Es hermítico: $\rho^\dagger = \rho$. Por lo tanto es diagonalizable y tiene autovalores reales.

2. Está normalizado: $\text{Tr}(\rho) = 1$. Por lo tanto las probabilidades suman 1 en la base que diagonaliza a ρ.

3. Es semidefinido positivo: $\langle\phi|\rho|\phi\rangle \geq 0$ para todo estado $|\phi\rangle$. Por lo tanto las probabilidades de cualquier medición son ≥ 0.

Para incluir a los estados mixtos, el Postulado 1 debe formularse de la siguiente manera: *''El estado general de un sistema físico está representado por un operador ρ (que es hermítico, de traza unidad y semi definido positivo) que actúa sobre un espacio de Hilbert"*. Los estados puros son aquellos para los cuales ρ tiene rango unidad.

Como la matriz densidad ρ es un operador hermítico es diagonalizable. Sea $B = \{|\phi_j\rangle, j = 1, ..., D\}$ la base de autovectores de ρ. En esta base ρ tiene una descomposición espectral de la forma: $\rho = \sum_j q_j |\phi_j\rangle\langle\phi_j|$, donde los autovalores q_j son números reales y positivos (ya que ρ tiene que ser positivo) cuya suma es igual a 1 (o sea, son probabilidades).

Esta expresión pone en evidencia una propiedad fundamental de los estados mixtos: existen infinitas maneras de preparar un estado mixto, o sea, un dado operador ρ puede corresponder a muchas mezclas de estados puros con distintas probabilidades.

Pureza de un estado. ¿Cómo cuantificar la "pureza"de un estado? (o, inversamente, ¿cómo cuantificamos cuán mixto es un estado dado?). Para un estado puro, el estado es un proyector de rango 1: satisface las propiedades $\rho_\psi = |\psi\rangle\langle\psi| = \rho^2$ y $\mathrm{Tr}\,\rho = \mathrm{Tr}\,\rho^2 = 1$. En cambio, cuando un estado es mixto, si bien $\mathrm{Tr}\,\rho = 1$ ya no es cierto que $\mathrm{Tr}\,\rho^2 = 1$. En efecto, escribiendo ρ en la base en la cual el estado es diagonal podemos escribir ρ^2 como $\rho^2 = \sum_j q_j^2 |\phi_j\rangle\langle\phi_j|$. Teniendo en cuenta que $q_j^2 \leq q_j$ (y que la igualdad solamente se verifica cuando estas probabilidades son iguales a cero o a uno), resulta que $\xi = \mathrm{Tr}\,\rho^2 = \sum_j q_j^2 \leq 1$. La desigualdad será estricta cuando haya más de un q_j que es no nulo). El grado de impureza es medido por ξ.

Un ejemplo interesante es el estado que llamamos de máxima ignorancia. En este estado tenemos que todas las posibilidades ocurren con igual probabilidad. En tal caso escribiremos $q_j = 1/D$ donde $D = \dim(\mathcal{H})$ y por lo tanto tenemos que $\xi = 1/D$. Este es el mínimo valor que puede tomar la pureza para un estado de dimensión D. Llamaremos a los estados de mínima pureza "máximamente mixtos". Es interesante notar que, la matriz de densidad de este estado se es proporcional a la identidad $\rho = \mathbb{1}/D$ y por lo tanto es igual en cualquier base ortonormal.

La medida que describimos lleva el nombre de *pureza*, a secas, y se define, como sugiere lo anterior, así:

$$\xi = \mathrm{Tr}\,\rho^2. \tag{4.6}$$

Existen, sin embargo, otras manera de medir la pureza de un estado que surgen de caracterizar la distribución de probabilidades q_j (la entropía de la distribución, por ejemplo).

4.3. Observables

4.3.1. Conjunto Completo de Observables que Conmutan (CCOC)

Un concepto muy importante es el de Conjunto Completo de Observables que Conmutan (CCOC). Su definición es sencilla: Se trata de un conjunto de operadores que conmutan todos entre si (y que, por lo tanto, pueden ser diagonalizados simultáneamente) que cumplen con la condición de "completitud".

El conjunto de observables que conmutan $\{\hat{A}, \hat{B}, \hat{C}, \hat{D}, ...\}$ es completo si y sólo si cada secuencia de autovalores $(a_i, b_j, c_k, d_l, ...)$ identifica a un único vector de la base ortonormal que diagonaliza a todos los operadores (o sea, que existe un único vector que es autovector de $\hat{A}$ con autovalor a_i, de $\hat{B}$ con autovalor b_j, etc). En consecuencia, la base que diagonaliza simultáneamente a todos estos operadores puede denotarse como $B = \{|a_i, b_j, c_k, d_l, ...\rangle\}$.

Esta noción tiene sentido para operadores degenerados, ya que un operador no degenerado define, por sí mismo, un CCOC.

4.3.2. Mediciones alternadas de dos operadores

Dos observables compatibles pueden ser medidos simultáneamente o, mejor dicho, el orden en el que se miden dos operadores compatibles no altera los resultados que se obtienen. Veamos que esto es así. Recordemos llamamos operadores compatibles a aquellos que conmutan: $[\hat{A}, \hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A} = 0$. Supongamos ahora que uno mide primero $\hat{A}$, registra el resultado y seguidamente mide $\hat{B}$ sobre el estado en el que quedó preparado el sistema, registrando también el resultado de la medición. Si los observables son compatibles una nueva medición de $\hat{A}$ dará el mismo resultado que en la primera medición y si a esta le sigue otra medición de $\hat{B}$ obtendremos nuevamente el mismo resultado, etc. Dejamos al lector verificar esta afirmación haciendo uso de los postulados.

En cambio, si $\hat{A}$ y $\hat{B}$ no conmutan la medición alternada de ellos no dará necesariamente siempre el mismo resultado.

Estas propiedades son consecuencias del hecho de que en la mecánica cuántica los estados se representan como vectores y los observables como operadores sobre un espacio de Hilbert. Estas propiedades extrañas tuvieron un rol primordial en el desarrollo histórico de la mecánica cuántica. Sin embargo, en esta presentación no histórica, aparecen como meras consecuencias de postulados más abstractos y generales.

4.3.3. Operadores complementarios

Veamos aquí el concepto de complementariedad, acuñado originalmente por Niels Bohr. Quien conozca la obra teatral "Copenhague", escrita por Michael Frayn, recordará las intensas discusiones entre Niels Bohr y Werner Heisenberg, que en Buenos Aires fueron interpretados magistralmente por Juan Carlos Gene y Alberto

Segado. Bohr y Heisenberg discutían sobre la complementariedad y la incertidumbre. Estos son dos de los ingredientes básicos de la mecánica cuántica que ponen de manifiesto cuán extraño es el comportamiento de la naturaleza a escala microscópica.

El *principio de complementariedad* es un verdadero atentado contra nuestra intuición. En su versión más general afirma lo siguiente: *Si preparamos un objeto de manera tal que la propiedad A toma un valor preciso, entonces siempre existe otra propiedad B cuyo valor está completamente indeterminado. En ese caso, afirmamos que las propiedades A y B son "complementarias".*

El principio se aplica a situaciones muy habituales en las que sometemos a un objeto a algún proceso de preparación tal que si posteriormente medimos repetidamente la propiedad A siempre obtenemos el mismo valor. Lo sorprendente es que el principio de complementariedad afirma que *"entonces, siempre existe otra propiedad B cuyo valor está completamente indeterminado"*. ¿Qué quiere decir esto? Simplemente significa que si preparamos el sistema en un estado en el que la propiedad A tiene un valor preciso y medimos la propiedad B entonces obtendremos resultados completamente aleatorios. Si repetimos muchas veces este procedimiento (es decir, preparamos el sistema con un valor de A y medimos la propiedad B) obtendremos resultados diferentes, distribuidos de manera totalmente azarosa. Es decir, dos operadores complementarios son totalmente máximamente incompatibles.

La demostración del principio de complementariedad es muy sencilla. Consideremos el observable $\hat{A}$ que es diagonal en la base $B_A = \{|\phi_j\rangle, j = 1, ..., D\}$. Teniendo en cuenta los postulados enunciados más arriba sabemos que si medimos $\hat{A}$ obtendremos uno de sus autovalores a_j como resultado. Si el autovalor medido no es degenerado, el estado del sistema quedará preparado en el correspondiente autoestado $|\phi_j\rangle$. Es fácil ver que siempre podemos construir un operador $\hat{B}$ que es tal que si luego de medir $\hat{A}$ medimos $\hat{B}$, la probabilidad de todos los resultados b_j será uniforme (aleatoriedad completa). Para esto, alcanza con decir cual es la base en la que $\hat{B}$ debe ser diagonal. Esta base puede elegirse como $B_B = \{|\tilde{\phi}_j\rangle, j = 1, ..., D\}$ donde los vectores $|\tilde{\phi}_j\rangle$ se definen como $|\tilde{\phi}_j\rangle = \frac{1}{\sqrt{D}} \sum_k \exp(-2\pi i\ jk/D)|\phi_k\rangle$. Es inmediato verificar que estos vectores son ortonormales $\langle\tilde{\phi}_j|\tilde{\phi}_l\rangle = \delta_{jl}$ y que puede invertirse la expresión anterior expresando los vectores de la base B_A en función de los de la base B_B. También es inmediato verificar que

$$\left|\langle\phi_j|\tilde{\phi}_l\rangle\right|^2 = \frac{1}{D}\,. \tag{4.7}$$

De dónde surge que la probabilidad de medir cualquier autovalor de $\hat{B}$ en cualquier estado de B_A es la misma y es igual a $1/D$. O sea, todos los estados son equiprobables y por lo tanto estas las propiedades A y B son complementarias.

de medición en las direcciones no ortogonales z=(Llamamos a las bases B_A y B_B de dos operadores complementarios bases "mutuamente no sezgadas". Es posible demostrar que en cualquier espacio vectorial de dimensión D existen a lo sumo $D+1$ bases que son mutuamente no sezgadas entre sí (y que ese número siempre se puede alcanzar si D es un número primo o una potencia de un número primo). En

el caso de un sistema de spin 1/2, los observables S_x, S_y y S_z son complementarios ya que, como vimos, sus bases son no sesgadas. En cambio, por ejemplo, los operadores de medición en las direcciones no ortogonales z y $\vec{n} = (0, 1, 1)/\sqrt{2}$, aunque no compatilbes, no llegan a ser complementarios.

4.3.4. Relaciones de indeterminación. Desigualdad de Heisenberg

El principio de indeterminación (o, mal llamado, principio de incertidumbre) de Heisenberg es otra de las piedras fundacionales de la mecánica cuántica. Tuvo una importancia histórica enorme. Podría tomarse como la versión cuantitativa del principio de complementariedad de Bohr. En efecto, es posible demostrar que para cualquier par de observables no compatibles hay una cota inferior al producto de la varianza en la medición de ambos observables. Por ese motivo cuando el estado es tal que la varianza (la dispersión de los resultados en la medición) de uno de los observables disminuye entonces la varianza del otro aumenta. Pese a ser una pieza clave del desarollo la mecánica cuántica hoy ha sido "relegada" a ser una consecuencia bastante trivial de los postulados que hemos visto. En particular, en su derivación, que veremos ahora, son fundamentales las propiedades del producto interno en el espacio de Hilbert y reglas elementales del álgebra de operadores.

Partimos de la desigualdad de Schwarz establece que

$$\langle \phi|\phi\rangle \, \langle \psi|\psi\rangle \geq |\langle \phi|\psi\rangle|^2 \tag{4.8}$$

Aplicaremos esta desigualdad para dos estados particulares, obtenidos a partir de dos operadores hermíticos $\hat{A}$ y $\hat{B}$. En efecto, tomamos $|\phi\rangle = (\hat{A} - \alpha)|\xi\rangle$ y $|\psi\rangle = (\hat{B} - \beta)|\xi\rangle$ (donde α y β son dos números reales cualesquiera, que después elegiremos a nuestra conveniencia, y $|\xi\rangle$ es un vector cualquiera de norma unidad). Entonces, la desigualdad de Schwarz implica que

$$\langle \xi|(\hat{B} - \beta)^2|\xi\rangle\langle \xi|(\hat{A} - \alpha)^2|\xi\rangle \geq |\langle \xi|(\hat{B} - \beta)(\hat{A} - \alpha)|\xi\rangle|^2.$$

Si elegimos $\alpha = \langle \hat{A}\rangle$ y $\beta = \langle \hat{B}\rangle$ entonces la expresión anterior se reduce a

$$\Delta^2\hat{A} \, \Delta^2\hat{B} \geq |\langle \xi|(\hat{B}\hat{A} - \langle \hat{A}\rangle\langle \hat{B}\rangle)|\xi\rangle|^2. \tag{4.9}$$

Donde podemos reescribir el lado derecho de la desigualdad usando la identidad $BA = \frac{1}{2}\{B, A\} + \frac{1}{2}[B, A]$. Asimismo, el módulo al cuadrado que aparece en el lado derecho puede calcularse explícitamente usando dos propiedades importantes: a) el valor medio del conmutador de dos operadores hermíticos es siempre un número imaginario puro; b) el valor medio del anticonmutador es siempre real. De este modo, la desigualdad resulta ser

$$\Delta^2\hat{A} \, \Delta^2\hat{B} \geq \frac{1}{4}|\langle [A, B]\rangle|^2 + K^2(A, B), \tag{4.10}$$

donde la función de correlación $K(A,B)$ está definida como $K(A,B) = \frac{1}{2}\langle\{A,B\}\rangle - \langle\hat{A}\rangle\langle\hat{B}\rangle$. Como ambos términos de la desigualdad anterior son positivos, es evidente que de lo anterior se pueden deducir las siguientes desigualdades

$$\begin{aligned} \Delta\hat{A}\,\Delta\hat{B} &\geq \frac{1}{2}|\langle[A,B]\rangle|, \\ \Delta\hat{A}\,\Delta\hat{B} &\geq |K(A,B)|. \end{aligned}$$

La primera de estas dos desigualdades es la famosa desigualdad de Heisenberg: si la aplicamos para el caso del operador posición y momento que satisfacen $[\hat{X},\hat{P}] = i\hbar\mathbb{1}$ la desigualdad se transforma en la famosa expresión:

$$\Delta\hat{X}\Delta\hat{P} \geq \hbar/2 \tag{4.11}$$

En este caso el lado derecho de la desigualdad es independiente del estado. La segunda desigualdad, en cambio, no es relevante ya que siempre es posible encontrar estados para los cuales la función de correlación se anula (por ejemplo, para cualquier autoestado de $\hat{A}$ o $\hat{B}$ vale que $K(A,B) = 0$).

Como el producto de las dos dispersiones debe ser mayor que una cierta cantidad entonces debe cumplirse que cuanto más pequeña sea $\Delta\hat{A}$, más grande debe ser el valor de ΔB (y viceversa). Para el caso de posición y momento, la pequeñez del valor de $\hbar$ (un número con treinta y cuatro ceros detras del punto decimal) explica el motivo por el cual las consecuencias de los principios de complementariedad e incertidumbre no son perceptibles en la escala macroscópica. Por ejemplo, si preparamos una partícula de 1 gramo en un estado donde la posición está determinada con una incerteza de $\Delta X = 1\text{cm}$, entonces el principio de indeterminación establece que nunca podremos determinar la velocidad con una incerteza menor que 10^{-28}m/seg. Claramente es extremadamente difícil construir un instrumento de medición capaz de detectar una desviación tan pequeña.

No es posible dejar de sorprenderse por las implicancias de los principios de complementariedad y el de indeterminación, que fueron establecidos respectivamente por Niels Bohr y Werner Heisenberg alrededor de 1925. Ponen en evidencia cuán extraña es la mecánica cuántica y es imposible aceptarlos sin antes intentar demolerlos: Einstein, y cualquier persona en su sano juicio, preguntaría: ¿Cómo es posible que podamos preparar un objeto de modo tal que si medimos la propiedad A siempre obtenemos el mismo valor pero que sea imposible lograr que el valor de la propiedad complementaria B tenga también un valor definido? Esta pregunta *no* tiene respuesta dentro de la mecánica cuántica. Dicha teoría acepta este hecho sorprendente como una propiedad de la naturaleza y a partir de eso formula un modelo que tiene una notable capacidad predictiva. Con todo dramatismo, la mecánica cuántica se yergue hoy, a más de cien años de su nacimiento, como la única teoría compatible con los resultados experimentales modernos.

Es importante notar que en muchos libros de texto de mecánica cuántica, el principio de indeterminación se ilustra con una gran cantidad de ejemplos que muestran que cuando uno quiere medir la posición de una partícula con una precisión alta (con una incerteza pequeña ΔX) entonces inevitablemente introduce una

perturbación que afecta el valor del momento P. Por ejemplo, si queremos localizar a la partícula en un intervalo de longitud ΔX podemos intentar iluminarla con luz de longitud de onda menor que ese tamaño. En ese caso, cada fotón tendrá un momento $P_f = \hbar 2\pi/\lambda > \hbar 2\pi/\Delta X$. Al interactuar con la partícula el fotón transferirá su momento a ella y por lo tanto introducirá una incerteza en el momento del orden de $\Delta P = P_f$. Esto lleva a que $\Delta X \Delta P \geq \hbar/2$. Sin embargo, este tipo de este tipo de razonamientos son innecesarios dentro de la presente formulación de la mecánica cuántica y en muchos casos pueden inducir a equívocos. Esas discusiones sirven para motivar la mecánica cuántica mostrando que no podemos imaginar mecanismos físicos que introduzcan perturbaciones despreciables en todas las propiedades de un sistema. Sin embargo, la interpretación de las relaciones de Heisenberg no tiene nada que ver con la perturbación del valor de un observable al medirse otro complementario con el anterior. La mecánica cuántica, como dijimos varias veces, es mucho más radical. Nos obliga a aceptar que "los experimentos que no se realizan, no tienen resultados". O sea, la medición de un observable no puede perturbar el valor que toma otro ya que ese valor no existe, no pre-existe a la medición. Como vimos y veremos, si imaginamos que esos valores existen (y que de alguna manera desconocida determinan el resultado de la medición de estos observables, aún aceptando que no puedan medirse simultaneamente por algún motivo desconocido) llegamos a paradojas y contradicciones con las predicciones de la mecánica cuántica.

4.3.5. Indeterminación o Ignorancia

A lo largo del siglo XX los físicos hicieron numerosos intentos por encontrar alternativas a la mecánica cuántica y desarrollar teorías que sean mas aceptables para nuestro sentido común. La clase de modelos que naturalmente podrían competir con la mecánica cuántica incluye a aquellos en los que la complementariedad no es una propiedad fundamental sino que es fruto de nuestras limitaciones. Por ejemplo, podríamos imaginar que la naturaleza es tal que cada vez que fijamos el valor de alguna propiedad A perturbamos el objeto de manera tal que afectamos el valor de B. En un mundo como ese, la razón por la cual una medición de B da lugar a resultados aleatorios es nuestra incapacidad de controlar todas las propiedades de los objetos o, equivalentemente, nuestra ignorancia sobre detalles del mundo microscópico que todavía son inaccesibles a nuestras limitadas posibilidades experimentales. Einstein, y cualquier persona razonable, hubiera estado dispuesto a aceptar un mundo de estas características. En ese caso, la mecánica cuántica no proveería una descripción completa de la naturaleza sino solamente daría una descripción parcial. Más adelante presentaremos un famoso argumento formulado por Einstein en 1935 que intentaba demostrar precisamente esto: que la descripción del mundo provista por la mecánica cuántica es incompleta. Veremos también, cómo, sorprendentemente, los notables avances de la física de fines del siglo XX fueron capaces de demostrar la falsedad del argumento de Einstein. Es notable, pero la física ha sido capaz de demostrar que el azar no se origina en nuestra ignorancia. Sin embargo, debemos reconoce que, hasta ahora: *¡ignoramos*

4.4. Spin 1/2

Los estados

El caso de una partícula de spin 1/2 ha sido el ejemplo motivador de los postulados de la mecánica cuántica, por eso es útil e importante resumir aquí todo lo que sabemos sobre este sistema. Como vimos, hay infinitas bases que se corresponden a autoestados del observable $\hat{S}_n = \vec{e}_n \cdot \vec{S}$. A estas bases las denotamos $B_n = \{|0_n\rangle, |1_n\rangle\}$. Cualquier estado puede escribirse como combinación lineal de los elementos de alguna de estas bases. Por simplicidad, tomaremos la base B_z y escribimos un estado como

$$|\psi\rangle = \alpha|0_z\rangle + \beta|1_z\rangle$$

donde $|\alpha|^2 + |\beta|^2 = 1$ es la condición de normalización del estado. El proyector sobre este estado es

$$\begin{aligned} \rho &= |\psi\rangle\langle\psi| = |\alpha|^2|0_z\rangle\langle 0_z| + |\beta|^2|1_z\rangle\langle 1_z| + \\ &+ \alpha\beta^*|0_z\rangle\langle 1_z| + \alpha^*\beta|1_z\rangle\langle 0_z|. \end{aligned} \tag{4.12}$$

Los estados de una base bases B_n pueden escribirse como combinación lineal de los estados de cualquier otra B_m. Veremos más abajo como obtener estas expresiones de manera muy sencilla.

Los operadores

Como sabemos, todos los operadores pueden representarse como matrices de 2×2. Las matrices de Pauli σ_x, σ_y y σ_z , junto con la identidad $\mathbb{1}$ forman una base completa del espacio de los operadores que actúan sobre el espacio de estados. En efecto, el espacio de los operadores $\mathcal{L}(\mathcal{H})$ tiene la estructura de un espacio de Hilbert con un producto interno tal que $(A, B) = \mathrm{Tr}(A^\dagger B)$. Por lo tanto, cualquier operador $\hat{A}$ puede escribirse como combinación lineal de estos cuatro operadores:

$$\begin{aligned} \hat{A} &= \frac{1}{2}\Big(a_0\mathbb{1} + a_z\sigma_x + a_y\sigma_y + a_z\sigma_z\Big) \\ &= \frac{1}{2}\Big(a_0\mathbb{1} + \vec{a}\cdot\vec{\sigma}\Big) \end{aligned} \tag{4.13}$$

,donde el factor 1/2 es una mera convención que se introduce por conveniencia. Teniendo en cuenta que todos los operadores σ_j son tales que $\mathrm{Tr}\sigma_j = 0$ y que dichos operadores cumplen las relaciones $\sigma_j\sigma_k = i\epsilon_{jkl}\sigma_l$ y $\sigma_i^2 = \mathbb{1}$, podemos invertir la ecuación anterior y obtener:

$$a_0 = \mathrm{Tr}(\hat{A}), \quad a_j = \mathrm{Tr}(\hat{A}\sigma_j). \tag{4.14}$$

Si escribimos al operador $\hat{A}$ de este modo, es inmediato calcular sus auto valores. En efecto, para diagonalizar $\hat{A}$ sólo tenemos que diagonalizar el término $\vec{a}\cdot\sigma$

que, como vimos, tiene autovalores $\pm|\vec{a}|$. En consecuencia, los autovalores de $\hat{A}$ resultan ser $a_\pm = (1 \pm |\vec{a}|)2$ y sus autovectores son los auto vectores del operador $\vec{a}\cdot\vec{\sigma}$.

Los proyectores y cambios de base

Las anteriores consideraciones son válias para cualquier operador $\hat{A}$ y, por lo tanto, valen también para los proyectores. Los proyectores son operadores cuyos auto valores toman los valores 0 y 1. Entonces, para un spin 1/2, podemos escribirlos como

$$P_{n,\pm} = \frac{1}{2}(I \pm \vec{n}\cdot\vec{\sigma}), \tag{4.15}$$

donde $\vec{n}$ es un vector de norma unidad (es decir, es tal que $n_x^2+n_y^2+n_z^2 = 1$). Así construido, el operador $P_{n,\pm}$ proyectará cualquier vector sobre el auto estado de autovalor $\pm\hbar/2$ del operador $S_n = \vec{n}\cdot\vec{\sigma}\,\hbar/2$.

Estas consideraciones nos permiten escribir fácilmente los vectores de cualquier base B_n en función de los de la base B_z. Por cierto, aplicando el proyector $\hat{P}_{n,\pm}$ al estado $|0_z\rangle$ obtenemos

$$\hat{P}_{n,\pm}|0_z\rangle = (1 \pm n_z)|0_z\rangle \pm (n_z + in_y)|1_z\rangle. \tag{4.16}$$

Para obtener los estados de B_n debemos, tomar la expresión anterior y normalizarla. De este modo resulta que, por ejemplo,

$$|0_n\rangle = \frac{(1+n_z)|0_z\rangle + (n_z+in_y)|1_z\rangle}{\sqrt{2(1+n_z)}}. \tag{4.17}$$

La expresión para $|1_n\rangle$ es análoga y obtenerla queda como ejercicio para el lector. Cabe destacar, que el único caso en que estas expresión *no* pueden aplicarse directamente es aquel en el cual $n_z = \pm 1$ (caso en el cual, justamente, los vectores de partida son los de la base B_n).

La esfera de Bloch

Para los estados de un spín 1/2 es posible oftener una representación geométrica y simple para los estados. Como vimos, cualquier estado puro está representado por un proyector de la forma

$$\rho = |\psi\rangle\langle\psi| = \frac{1}{2}\left(\mathbb{1} + \vec{p}\cdot\vec{\sigma}\right) \tag{4.18}$$

donde el vector $\vec{p}$, llamado vector de polarización, tiene componentes iguales a los valores medios de las respectivas matrices de Pauli. Es decir: $p_j = \mathrm{Tr}(\rho\sigma_j) = \langle\sigma_j\rangle$. En consecuencia, hay una correspondencia directa entre vectores en el espacio de Hilbert y vectores de $\vec{p}$. Es decir que todo estado cuántico tiene un vector $\vec{p}$ asociado y todo vector $\vec{p}$ da lugar a un estado, siempre que se cumpla que $|\vec{p}| \leq 1$. Por lo tanto, estos vectores esán en la superficial o el interior de una esfera de radio unidad, que se conoce como "esfera de Bloch". Para ver el origen de esta restricción

y comprender las propiedades de la ester de Bloch conviene razonar del siguiente modo.

Usando las expresiones anteriores podemos calcular el producto escalar entre dos estados $\rho = |\psi\rangle\langle\psi|$ y $\rho' = |\psi'\rangle\langle\psi'|$:

$$|\langle\psi|\psi'\rangle|^2 = \mathrm{Tr}(\rho\rho') = \frac{1}{2}(1 + \vec{p}\cdot\vec{p}'). \tag{4.19}$$

En particular, para cualquier estado puro, que está representado por un proyector de rango 1, vale que $\mathrm{Tr}(\rho^2) = 1$ y por lo tanto los estados puros están representados por expresiones de la forma

$$\rho = \frac{1}{2}(\mathbb{1} + \vec{p}\cdot\vec{\sigma}), \tag{4.20}$$

con $\vec{p}^{\,2} = 1$. O sea, todos los estados puros pueden caracterizarse por un vector $\vec{p}$ de longitud unidad, que está ubicado sobre la superficie de la esfera de Bloch.

Veamos que cómo se representan dos estados ortogonales en la esfera de Bloch. Como el producto escalar entre estados es $\mathrm{Tr}(\rho\rho') = (1+\vec{p}\cdot\vec{p}')/2$, los estados ortogonales son los que cumplen con la propiedad $\vec{p}' = -\vec{p}$, o sea que están en los puntos antipódicos de la esfera de Bloch.

Para visualizar estados mixtos en la esfera de Bloch, se puede verificar que la pureza de ρ, como fue definida más arriba es $\xi = 1 + \vec{p}^{\,2}$. Por lo tanto la representación de estados mixtos será con vectores de norma $\vec{p}^{\,2} < 1$. Estos se encuentran dentro de la esfera de Bloch. En particular, el estado máximamente mixto es descripto por la matriz densidad $\rho = \mathbb{1}/2$ y se representa en el centro de la esfera con el vector nulo $\vec{p} = 0$

En la Figura 5.1 mostramos varios ejemplos de estados puros y mixtos representados en la esfera de Bloch.

Mediciones sucesivas de SG en direcciones arbitrarias

Por último, de todo lo anterior se deduce que si preparamos el autoestado de S_n y medimos $S_{n'}$, la probabilidad de obtener el resultado $\hbar/2$ es

$$\begin{aligned}
\mathrm{Prob}(S_{n'} = \hbar/2 \,\big|\, S_n = \hbar/2) &= \frac{1}{2}(1 + \vec{e}_n\cdot\vec{e}_{n'}) \\
&= \frac{1}{2}\big(1 + \cos(\theta_{n,n'})\big) \\
&= \cos^2\left(\frac{\theta_{n,n'}}{2}\right),
\end{aligned} \tag{4.21}$$

donde $\theta_{n,n'}$ es el ángulo que se forma entre los ejes $\vec{e}_n$ y $\vec{e}_{n'}$. Esta fórmula había sido mencionada en el capítulo 1 pero su validez no había sido demostrada explícitamente hasta ahora.

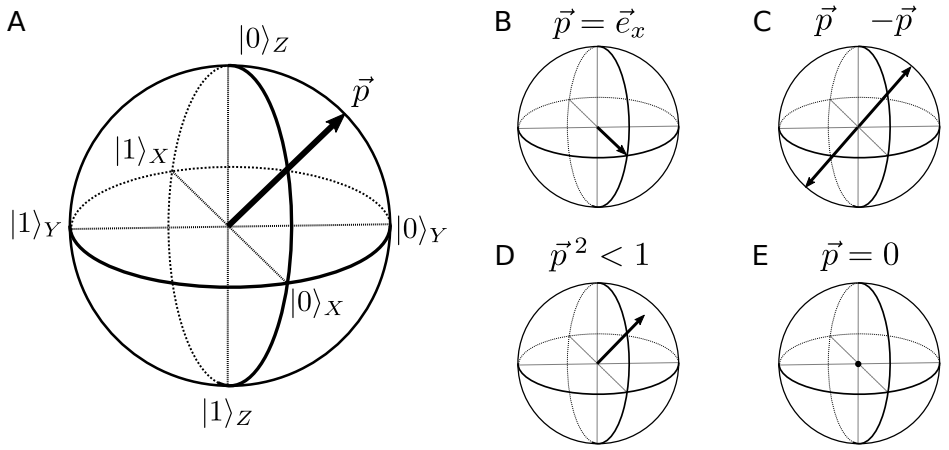

Figura 4.1: Esfera de Bloch y ejemplos de algunos estados representados. En A se muestra la esfera de Bloch, un estado con definido por el vector $\vec{p}$ y los autoestados correspondientes a las tres direcciones cartesianas x, y y z. En B se indica uno de los autoestados de σ_x: $\rho = (1+\sigma_x)/2$, representado por $\vec{p} = (1,0,0)$. En C se indican dos estados ortonormales uno representado por $\vec{p}$ y el otro por $-\vec{p}$. En D se indica un estado mixto (no puro) con $\vec{p}^{\,2} < 1$. En E se indica el estado máximamente mixto: $\rho = \mathbb{1}$ representado por $\vec{p} = 0$

Desigualdad de Heisenberg para un spín

En el caso de un sistema de spín 1/2 la desigualdad de Heisenberg adopta una forma muy simple, pero muy diferente de la conocida para el caso de los observables posición y momento. En efecto, si usamos la fórmula de la sección anterior eligiendo como observables a los operadores $\hat{A} = \sigma_x$ y $\hat{B} = \sigma_z$ es fácil reescribir la desigualdad de Heisenberg. Para eso, basta notar recordar que $\sigma_i^2 = \mathbb{1}$, por lo que la dispersión de dichos observables resulta ser

$$\Delta\hat{A}^2 = \langle\sigma_x^2\rangle - \langle\sigma_x\rangle^2 = 1 - \langle\sigma_x\rangle^2 \tag{4.22}$$

$$\Delta\hat{B}^2 = \langle\sigma_z^2\rangle - \langle\sigma_z\rangle^2 = 1 - \langle\sigma_z\rangle^2. \tag{4.23}$$

Por su parte, el lado derecho de la ecuación de Heisenberg puede escribirse utilizando que el conmutador y el anticonmutador de los operadores $\hat{A} = \sigma_x$ y $\hat{B} = \sigma_z$. Para este caso el conmutador es proporcional a σ_y mientras que el anti-conmutador es nulo. Por lo tanto, la desigualdad de Heisenberg (ecuación 4.10) en este caso resulta ser

$$\Big(1 - \langle\sigma_x\rangle^2\Big)\Big(1 - \langle\sigma_z\rangle^2\Big) \geq \Big(\langle\sigma_y\rangle^2 + \langle\sigma_x\rangle\langle\sigma_z\rangle\Big). \tag{4.24}$$

Reordenando esta expresión, la desigualdad de Heisenberg puede reescribirse como

$$1 \geq \Big(\langle\sigma_x\rangle^2 + \langle\sigma_y\rangle^2 + \langle\sigma_z\rangle^2\Big), \tag{4.25}$$

que no es otra cosa que la condición que impone que el vector polarización $\vec{p} = \langle\vec{\sigma}\rangle$ pertenezca al interior o a la superficie de la esfera unitaria (esfera de Bloch).

A diferencia de lo que sucede con la posición y el momento, el lado derecho de la desigualdad puede anularse para ciertos estados (y no está acotado por debajo por $\hbar/4$, como en ese caso). En efecto, existen estados físicos para los cuales las dispersiones de los observables σ_x o σ_z se anulan, cosa que con la posición y el momento no sucede.

4.5. Aplicación: Criptografía Cuántica

4.5.1. Complementariedad, azar y criptografía cuántica

Mostraremos aquí una de las aplicaciones más recientes de la física cuántica, que se basa en la existencia de observables complementarios. Se trata de un campo de la física y la tecnología que ha recibido muchísima atención en las últimas décadas: la "Criptografía Cuántica" que, como veremos, debemos denominar en forma más rigurosa como "Distribución Cuántica de Claves" (y que abreviaremos con la sigla DCC). En efecto, mostraremos la forma en la cual, usando uno de los aspectos más anti intuitivos de la física cuántica, dos observadores A y B (que en la literatura son habitualmente conocidos como Alice y Bob) pueden intercambiarse entre si una "clave secreta" (algo que definiremos con precisión más adelante pero que es el insumo imprescindible para que ambos puedan intercambiarse mensajes secretos sin que nadie pueda espiarlos).

La DCC surge a principios de la década de 1980, más de medio siglo después de la aparición de la mecánica cuántica. De hecho, en 1970 Stephen Wiessner y Gilles Brassard dieron los primeros pasos, que fueron completados en 1984 por Charles Bennett y el propio Brassard en un trabajo célebre que es considerado como el fundador del campo de la DCC y uno de los pioneros en lo que hoy se conoce como "Información Cuántica". El método que propusieron describe cómo Alice y Bob pueden alcanzar el objetivo de enviarse mensajes secretos usando dos ideas: primero, la posibilidad de intercambiarse sistemas cuánticos de a uno a la vez y segundo, explotar la existencia de observables complementarios.

Cabe preguntarse por qué estos trabajos fundamentales recién aparecieron más de medio siglo después de que Bohr y Heisenberg desarrollaran completamente los conceptos de *complementariedad* e *indeterminación*, en los que la DCC se basa. De hecho, ¡la DCC podría haber surgido mucho antes! En nuestra opinión, el motivo de esta demora se basa en que en el procedimiento que describiremos, los dos observadores (Alice y Bob) deben intercambiar entre si objetos cuánticos individuales, de a uno a la vez. En los albores de la cuántica esto parecía una quimera, una tarea que, según las palabras del propio Schrödinger, era comparable a la ciencia ficción y que inevitablemente conducía a resultados absurdos.

A principios de la década de 1980 la situación ya había comenzado a cambiar y la posibilidad de manipular fotones y átomos individualmente ya no parecía una tarea imposibles. Hoy, contamos con tecnologías que nos permiten generar fotones de a uno, atrapar átomos de a uno, enfriarlos y controlar su estado. Estas técnicas se realizan de manera usual en muchos laboratorios del mundo y muchas están

encontrando aplicaciones tecnológicas [1]. Este cambio de paradigma, llevó a pensar en qué se puede hacer cuándo uno puede controlar sistemas cuánticos de a uno y así surgieron ideas como la DCC y otras que veremos más adelante, incluidas las simulaciones y computación cuántica.

4.5.2. Breve introducción a la criptografía clásica: ¿Cómo enviar un mensaje secreto?

En primer lugar conviene reiterar que con la DCC alcanzaremos un objetivo necesario para transmitir información de manera absolutamente segura, pero que este procedimiento no es, en si mismo, un método para transmitir esa información. Por cierto, la DCC produce, en cambio, la materia prima para la Criptografía: una *clave secreta*. Luego, esta clave será utilizada para *encriptar* información y transmitirla en forma segura.

Para evitar confusiones, describiremos primero la forma en la cual una clave secreta puede usarse para encriptar un mensaje. Esta parte del método es *totalmente clásica* (o sea, totalmente independiente de la cuántica). Una vez hecho esto, mostraremos la forma en la que la mecánica cuántica nos permite generar esas claves secretas.

Supongamos que A escribe un mensaje y quiere enviárselo a B de manera segura. El mensaje se puede traducir siempre en una secuencia de ceros y unos (bits), y por lo tanto será una cadena de bits de la forma

$$\vec{m} = (m_1, m_2, \ldots, m_N) \tag{4.26}$$

donde cada elemento de la N-upla es $m_i = 0, 1$ y N es el número de bits del mensaje a transmitir. Para transformar un texto escrito en castellano en una secuencia de ceros y unos, se utiliza habitualmente un código (llamado código ASCII) que es públicamente conocido. Por mas que una persona común y corriente no pueda leer el texto codificado en la secuencia de bits, cualquier computadora puede traducirlo fácilmente y facilitar de ese modo la lectura.

A podría intentar esconder su mensaje, por ejemplo, utilizando un código diferente al ASCII. Estas estrategias se conocen como *alfabetos cifrados*, donde se intercambian, siguiendo alguna regla, distintas letras del alfabeto. Sin embargo, ese tipo de estrategias son muy inseguras ya que si el mensaje está escrito en castellano, por ejemplo, cualquier persona que lo intercepte no tardaría demasiado en darse cuenta de que ciertas secuencias de bits aparecen con más frecuencia que otras y a partir de esa observación, y un análisis adecuado e inteligente, podría descubrir el código utilizado y revelar el contenido del mensaje.

Para enviar un mensaje de manera totalmente segura, A tiene una sola posibilidad: debe encriptarlo usando una *clave secreta y aleatoria*. Al igual que el mensaje,

[1] Algunos de estos a nivel nacional son el Laboratorio de Iones y Átomos Fríos (LIAF) de la UBA, dónde se atrapan y manipulan iones fríos y el Laboratorio de Óptica Cuántica CITEDEF, donde se generan y manipulan fotones individuales y se trabaja en DCC.

la clave es también una secuencia de ceros y unos de la forma $\vec{k} = (k_1, k_2, \ldots, k_N)$. Para que la encriptación sea totalmente segura se debe cumplir que:

1. la clave debe ser secreta (sólo conocida por A y por B),
2. la clave debe ser aleatoria (es decir, la frecuencia de aparición de bits y de secuencias debe estar uniformemente distribuida),
3. la clave debe ser tan larga como el mensaje (ambos deben tener N bits) y
4. la clave solamente debe utilizarse una única vez.

El cuarto punto, da nombre al método: "libreta de un solo uso" (o *one-time pad*, en inglés). Ya que la clave secreta no debe usarse más de una vez, y originalmente estas claves se anotaban en libretas que A y B confeccionaban. Pero, ¿cómo confeccionar y repartir estas libretas de manera secreta?. Dejando de lado la dificultad de generar secuencias realmente aleatorias (un tema bien complejo) el problema más grave es mantener el secreto de las claves logrando que sólo A y B las conozcan. Para eso, A y B podrían encontrarse y distribuirse estas claves grabadas, originalmente en una libreta, hoy en algún soporte digital y luego utilizarlas para sus comunicaciones. Pero, naturalmente, el problema aparece cuando las claves se agotan. En ese caso A y B deberían reunirse nuevamente, lo cual podría ser algo bien complicado. Por ejemplo, podríamos imaginar que Alice está en una nave espacial orbitando alrededor de la tierra y Bob permanece en el centro de comando de la nave: ¿cómo podrían distribuirse claves en esas condiciones? Eso, precisamente es lo que logra la mecánica cuántica.

Antes de pasar a describir la DCC, veamos en detalle cómo funciona el protocolo de encriptación por libreta de un solo uso.

1. Alice toma su mensaje $\vec{m}$ y lo encripta utilizando la clave $\vec{k}$ de genera de la siguiente manera:

$$\vec{m}' = \vec{m} \oplus \vec{k}, \tag{4.27}$$

   donde $\vec{m}'$ es el mensaje encriptado y el símbolo "$\oplus$" denota a la suma "módulo 2"(que se corresponde a la operación lógica "o-exclusivo", es decir: $0 \oplus 0 = 1 \oplus 1 = 0$ y $0 \oplus 1 = 1 \oplus 0 = 1$). Para N-uplas "$\oplus$" denota la operación elemento por elemento, es decir $\vec{m} \oplus \vec{k} = (m_1 \oplus k_1, \ldots, m_N \oplus k_N)$. Un ejemplo del uso de la suma módulo 2 para encriptar un mensaje se muestra en la figura 4.2.

2. Alice transmite a Bob el mensaje encriptado $\vec{m}'$ por un canal público.

   El mensaje encriptado $\vec{m}'$ es aleatorio, condición que hereda de la aleatoriedad de la clave $\vec{k}$. Por eso, aunque $\vec{m}'$ sea interceptado, no será posible utilizar los métodos basados en el estudio de la frecuencia de aparición de secuencias para decodificarlo. Por el contrario, para revertir el proceso de encripción (lo que se denomina des-encripción, es necesario utilizar nuevamente la clave. Efectivamente, un espía que intercepta el mensaje encriptado $\vec{m}'$ no tiene forma de saber si un 0 que observa en $\vec{m}'$ es el resultado de tener tanto el bit del

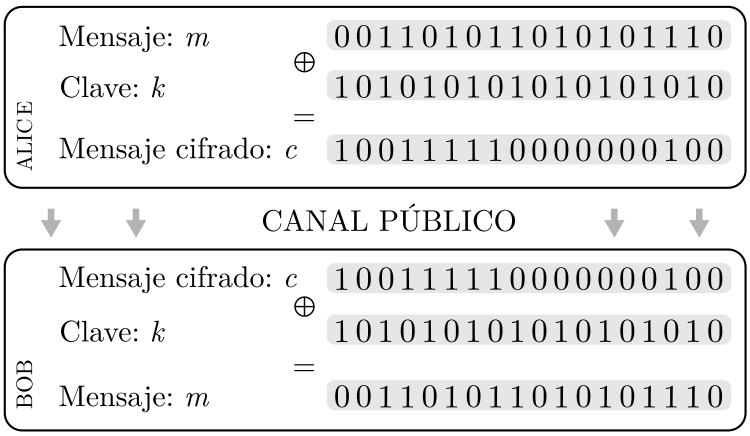

Figura 4.2: Ejemplo de uso del protocolo *one-time-pad* para mandar un mensaje encriptado de forma segura.

mensaje como el de la clave en 0 o si por el contario ambos son 1 (y análogamente si el espía ve un 1 esto es el resultado se sumar un 0 con un 1 pero no tiene forma de saber cuál es el del mensaje y cuál el de la clave).

3. Bob decodifica el mensaje aplicando el mismo método usado por Alice para encriptar:

$$\begin{aligned} \vec{m}'' &= \vec{m}' \oplus \vec{k} = \vec{m} \oplus \vec{k} \oplus \vec{k} \\ \vec{m}'' &= \vec{m} \end{aligned} \tag{4.28}$$

Esta propiedad que se deduce del hecho de que $\vec{k} \oplus \vec{k} = 0$, para cualquier valor de $\vec{k}$, como se puede ver explícitamente en acción en el ejemplo de la figura 4.2. Así vemos que, si A y B comparten una clave $\vec{k}$ podrán enviar de manera secreta un mensaje tan largo como la propia clave.

Es importante notar que, una vez utilizada, la clave debe ser desechada. Por cierto, si A utilizara la clave dos veces encriptando con la secuencia $\vec{k}$ al mensaje $\vec{m}$ y también al mensaje $\vec{n}$, entonces el método se volvería inseguro. En efecto, si alguien interceptara los mensajes codificados con la misma clave, que denominamos $\vec{m}'$ y $\vec{n}'$ entonces podría extraer información útil sobre ellos notando que el método antes descripto es tal que $\vec{m}' \oplus \vec{n}' = \vec{m} \oplus \vec{n}$. Esta secuencia, obtenida comparando dos mensajes codificados con la misma clave pierde su carácter aleatorio y, por lo tanto, es vulnerable a los métodos de análisis basados en el estudio de las frecuencias de aparición de secuencias de bits, que dependen del lenguaje utilizado, etc. Es decir, un espía suficientemente inteligente que intercepta varios mensajes codificados con la misma clave, podría finalmente leer su contenido (o extraer alguna información parcial).

En conclusión, teniendo en cuenta los cuidados descriptos, el método de encriptación por libreta de un solo uso nos provee de seguridad incondicional. Cla-

ramente, el problema radica en tener a disposición una clave $\vec{k}$ secreta ya precompartida entre Alice y Bob. La "solución" a este problema clásico es lo que se conoce como la generación pública de llaves (*public key exchange* en inglés), y es el método utilizado cotidianamente cuando con su navegador web se conecta al sitio de su banco, etc. Lo que se busca es que Alice y Bob intercambien entre sí mensajes de forma pública y puedan así establecer una clave secreta. Claramente, eso parace imposible, si un espía intercepta todos los mensajes, cómo es que no puede también conocer la clave? En efecto, clásicamente esta tarea es imposible. Sin emabrgo, sí es posible diseñar protocolos tales que, la función que tiene que aplicar el espía sobre los mensajes interceptados para poder así derivar $\vec{k}$, es muy difícil de calcular (tardando por ejmplo quizás un siglo en poder calcularla). De esta forma se tiene "seguridad" condicionada al hecho que un espía para poder saber $\vec{k}$ tiene que poder realizar una tarea muy difícil. Claramente, qué es difícil es relativo y, en efecto, problemas que eran computacionalmente díficiles hace unas décadas ya no lo son más. Sin embargo, clásicamente esto es lo mejor que podemos hacer y con lo que nos tenemos que acontentar. A continuación veremos que, por lo contrario, la mecánica cuántica nos provee de un método para generar la clave $\vec{k}$ de forma segura.

4.5.3. La Distribución Cuántica de Claves

La mecánica cuántica permite que Alice y Bob generen una clave aleatoria $\vec{k}$ sin necesidad de encontrarse y de modo tal que puedan estar seguros de que nadie más la conoce. Los ingredientes básicos que utilizaremos para esto son: (a) en la cuántica hay una fuente de azar intrínseco y (b) en la cuántica el acto de observación nunca es inocuo y, por lo tanto, deja una huella que siempre puede ser descubierta. Como veremos, Alice y Bbob utilizarán este último aspecto para revelar la presencia de un espía, en cuyo caso deberán desechar la clave generada y comenzar el procedimiento nuevamente.

Para generar la clave, Alice y Bob ejecutan un protocolo que tiene varios pasos. Durante ellos, se intercambiarán un sistema cuántico. Alice lo preparará en algún estado y Bob medirá alguna propiedad observable. Los pasos son los siguientes:

Paso 1 *Alice prepara un sistema en un estado eligiéndolo aleatoriamente entre autoestados de dos operadores complementarios y guarda en un cuadreno sus decisiones.*

Llamemos a los observadores complementarios O_1 y O_2 y supongamos que ambos son de dimensión 2 y tienen autovalores 0 y 1. Estos podrían ser, por ejemplo, para un un spín 1/2: $O_1 = \sigma_z$ y $O_2 = \sigma_x$. Si bien el procedimiento no se restringe al caso de spín 1/2 conviene restringirnos a ese caso para una primera exposición. En este ejemplo, el primer paso consiste en que Alice elige al azar preparar alguno de los siguientes estados $|0_z\rangle, |1_z\rangle, |0_x\rangle$ o $|1_x\rangle$.

Una vez preparado el estado, Alice confecciona una tabla con dos filas. En la primera anota el observable que eligió (O_1 u O_2) y en la segunda anota el estado que preparó (0 ó 1, independientemente de la base).

Alice	Observable elegido	O_1	O_2	O_2	O_1	O_2	O_1	O_1	O_2
	Estado preparado	0	1	0	0	1	0	1	0
Bob	Observable medido	O_1	O_1	O_2	O_2	O_1	O_2	O_1	O_2
	Estado medido	0	1	0	0	0	1	1	0
Coincidencia de observables		✓	×	✓	×	×	×	✓	✓
	Bits clave	0		0				1	0

Figura 4.3: Ejemplo de posibles resultados de las distintas rondas del protocolo BB84 para generar una clave secreta entre Alice y Bob.

Paso 2 *Alice envía al sistema a Bob.*

Esto implica enviar físicamente la partícula en cuestión de Alice a Bob; transportarla, dispararla, encausarla en un canal, en definitiva: llevarla de un lugar a otro. Esto se realiza más fácilmente con fotones que con partículas masivas ya que viajan a la velocidad de la luz y pueden ser enviados por aire o fibras ópticas sin que interactúen demasiado con su entorno.

Paso 3 *Bob recibe la partícula enviada por Alice y realiza una medición eligiendo aleatoriamente si mide el observable O_1 o si, en cambio, mide O_2 y registra sus resultados.*

Bob anota sus resultados en una tabla con dos filas, en la primera identifica cuál es el observable que midió y en la segunda anota el resultado obtenido.

Paso 4 *Alice y Bob repiten muchas veces estos tres pasos y, en cada repetición registran sus mediciones en una columna distinta de la tabla. Después de K repeticiones, cada uno de ellos tendrá una tabla con K columnas y 2 filas tal como se indica en la Figura 4.3.*

Es interesante comparar estas dos tablas. La primer fila de la tabla de Alice es totalmente independiente de la primera fila de la tabla de Bob. En efecto, esto se debe a que la elección del observable que Bob mide es totalmente independiente de la elección del observable elegido por Alice. Ambas filas tienen una distribución aleatoria de observables: O_1 y O_2 aparecen en ambas columnas de forma totalmente azaroza y no hay correlación alguna entre ellas. En cambio, la segunda fila de ambas tablas tiene un comportamiento diferente. *Si el observable elegido por Alice coincide con el elegido por Bob (lo que sucede, en promedio, la mitad de las veces) entonces los valores registrados en la segunda fila coinciden*. Esto se debe a que en esos casos Alice preparó un autoestado del observable que después Bob decidió medir. Obviamente, en esos casos el resultado registrado por Alice y Bob será idéntico. En cambio, en la otra mitad de los casos, cuando Alice elige un observable diferente del que Bob mide, los valores registrados en la segunda fila están totalmente

descorrelacionados. Esto se debe, precisamente, al carácter complementario de los observables O_1 y O_2: cuando Alice prepara un autoestado de O_1 y Bob mide O_2, la probabilidad de que los valores registrados por ambos sean diferentes es exactamente igual a 1/2.

De acuerdo a lo antedicho, Alice y Bob están a punto de alcanzar su objetivo que, recordemos, no es otra cosa que compartir una secuencia aleatoria de bits. En efecto, si se restringen a considerar solamente la segunda columna de sus tablas en aquellos casos en los que el contenido de la primera columna coincide, entonces tienen una secuencia aleatoria compartida por ambos. Para eso, deben completar el siguiente paso del protocolo que es:

Paso 5 *Alice y Bob hacen pública la primera fila de sus tablas. Se quedan con los resultados en los que sus valores coinciden y descartan el resto.*

En efecto, esta acción revela la secuencia de observables preparados por Alice y la secuencia de mediciones realizadas por Bob, pero en ningún caso revela el resultados registrados por ambos en la segunda fila.

Seguidamente, Alice y Bob descartan todas las columnas en las que los observables que aparecen en la primera fila de la tabla de Alice difiere de lo que aparece en la primera fila de la tabla de Bob. De este modo, ambos comparten una secuencia aleatoria de bits, formada por la segunda fila de sus tablas.

Hasta aquí, hemos demostrado que Alice y Bob pueden generar una secuencia aleatoria de bits compartida por ambos. ¡Pero en modo alguno hemos demostrado que esta secuencia sea secreta! Es decir, no hemos demostrado que este método de distribución de claves sea realmente seguro.

La seguridad del método se origina, precisamente, en la complementariedad. Supongamos que un tercer observador, al que llamaremos Eve (E, por espía o más fuerte, por *evesdropper* en inglés) intenta espiar lo que hacen Alice y Bob. Si Eve no tiene acceso a lo que sucede dentro de los laboratorios de Alice y Bob, su única opción es interceptar el sistema cuántico que Alice le envía a Bob. Al interceptarlo tiene la opción de realizar alguna medición sobre ese sistema para luego re enviarlo y que Bob lo reciba. En ese caso, Bob recibirá el sistema en el estado "preparado" por Eve. Cabe aquí destacar que los cuatro estados preparados por Alice no son todos ortogonales entre sí (pues efectivamente tenemos autoestados de operadores complementarios). Por lo tanto, como ya hemos discutido, no hay ninguna medición que pueda realizar Eve que le permita con certeza distinguir entre estos cuatro estados.

Veamos ahora en detalles cómo influye la acción de Eve. Si la primer fila de la tabla de Alice es realmente aleatoria y desconocida, Eva no sabe cual es el observable elegido por Alice y no tiene otra opción mas que elegir al azar algún observable para medir. Si Eve elige el mismo observable elegido por Alice, su medición no altera en modo alguno el estado del sistema. Pero en cambio, si Eve elige un observable diferente al elegido por Alice (lo que en promedio sucederá la mitad de las veces) obtendrá un resultado aleatorio y le enviará a Bob un sistema preparado

en un estado diferente al enviado por Alice. En esos casos, la medición posterior de Bob ya no estará correlacionada con la registrada por Alice sino que, la mitad de las veces, los resultados registrados en la segunda fila de las tablas de Alice y Bob obtenidas después del Paso 4 antes descripto, serán distintos. Es decir, la presencia de un espía deja una huella que se manifiesta en que las secuencias de bits de Alice y Bob obtenidas después del Paso 4 ya no son idénticas sino que están descorrelacionadas. Para revelar esa huella Alice y Bob ejecutan el último paso de su protocolo:

Paso 6 *Alice y Bob revelan algunos de los bits de la secuencia (digamos, uno de cada diez, por ejemplo) y comparan los resultados para detectar la presencia de un espía.*

Si los resultados difieren, han detectado la presencia de un espía (o bien, han detectado un mal funcionamiento de sus aparators, es decir ruido). En ese caso descartan la secuencia y comienzan de nuevo. En realidad, Alice y Bob no estarán completamente seguros de que no hay un tercero espiando si la secuencia revelada es la misma para ambos. Pero con un poco de esfuerzo matemático, pueden encontrar cual es la cantidad de bits que deben revelar para que la probabilidad de que no haya nadie en el medio sea tan baja como quieran (para entrar en detalle sobre este asunto, que puede encontrarse en la literatura del tema, es necesario un poco de matemática rigurosa, con ϵ's y δ's, que aquí omitiremos).

De este modo, la cuántica provee un método seguro para distribuir claves secretas en el cual la seguridad reside, precisamente, en las propias leyes de la naturaleza. Cabe mencionar que en las últimas décadas hay una variedad de dispositivos comerciales que usan variantes de este protocolo (que se conoce con el nombre de BB84) y que la distribución cuántica de claves ha sido implementada, inclusive, para alimentar de claves secretas a un satélite que órbita alrededor de la tierra.