UNIVERSIDAD ALFONSO X EL SABIO

ESCUELA POLITÉCNICA SUPERIOR

GRADO EN INGENIERÍA MATEMÁTICA

TRABAJO DE FIN DE GRADO

Computación Cuántica aplicada a la Criptografía

Rubén Nogueras González

Junio de 2025

Índice

Índice de figuras

CAPÍTULO

1

Introducción

1.1. Objetivos

- Comprender la necesidad de la mecánica cuántica en la física clásica.
- Entender los fundamentos matemáticos de la mecánica cuántica, incluyendo álgebra lineal y espacios de Hilbert.
- Aprender las diferencias, ventajas y desventajas entre un ordenador cuántico y uno tradicional.
- Analizar el papel que juegan las puertas cuánticas en la manipulación de estados, y por lo tanto en algoritmos cuánticos.
- Explicar los distintos principios básicos de la criptografía cuántica para garantizar la seguridad de los nuevos sistemas.
- Aprender el concepto de teleportación cuántica como mecanismo eficiente y seguro para la transmisión de información.

1.2. Historia de la Mecánica Cuántica

La computación cuántica es un nuevo sistema de computación, en el que nos apoyamos en las propiedades de los sistemas cuánticos para mejorar distintos paradigmas de la computación clásica. Esto lo hacemos mediante el uso del *qubit*, la unidad básica de información cuántica, a diferencia de la información clásica que se centra en el *bit* como unidad minima de información. La principal ventaja de los *qubits* es que, además de albergar información binaria (0 o 1), podemos obtener una mezcla de ambos estados (esto se conoce como el principio de superposición cuántica, que ya veremos en los próximos capítulos), de manera que podemos obtener algoritmos cuánticos que no pueden ser modelizados mediante *bits*, reduciendo en muchos casos la complejidad de algoritmos clásicos tradicionales, lo que mejora el rendimiento y eficiencia de nuestros computadores.

Para explicar esto de la mejor manera posible, nos remontamos a los orígenes de la física cuántica, a finales del siglo *XIX* y principios del siglo *XX*, cuando se pensaba que la física clásica era el foco global para explicar todos los fenómenos que suceden a nuestro alrededor, hasta que con el resultado de ciertos experimentos se comenzó a ver una relación entre el comportamiento de las ondas y las partículas, rompiendo completamente con los principios de la física clásica.

En primer lugar, vamos a comenzar explicando qué es un cuerpo negro, esto es un cuerpo que absorbe toda la radiación emitida sobre él, sin reflejar nada de lo que le llega. Esto se puede imaginar como una cavidad isotérmica con un orificio por el que se aproxima cierta radiación, de manera que permanezca en su interior. Además, suponemos que dicha cavidad se encuentra en equilibrio térmico, es decir, a una temperatura constante, de manera que la radiación que permanece dentro de ella se transforma en energía, obligando a emitir radiación hacia el exterior, sin tener nada que ver con la radiación que entra por el orificio.

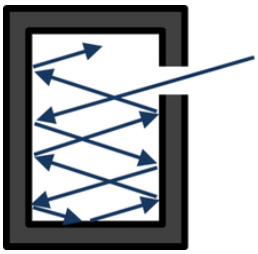


Figura 1: Ilustración del cuerpo negro. Obtenida de **?**

.

La física clásica es incapaz de explicar la radiación emitida por un cuerpo negro en función de la longitud de onda, hasta que la explicación de este fenómeno vino de la mano de *Max Planck* en el siglo *XX*, el cual establece que la energía liberada por el cuerpo negro se emite en pequeños paquetes, llamados *cuantos de energía*. Esta energía es proporcional a una pequeña constante, la constante de Planck, de manera que la energía emitida por el cuerpo negro no es continua, sino que toma un valor discreto que ha de ser múltiplo de dicha constante por su frecuencia de onda, rompiendo completamente con la física de la época y dando el nacimiento a un nuevo campo de la física, la mecánica cuántica.

$$E = h\nu \tag{1.1}$$

Siendo h la denominada *constante de Planck*, la cual alcanza un valor de $6{,}62607015 \times 10^{-34}\,\mathrm{J}\cdot\mathrm{s}$, y siendo ν la frecuencia. Esta energía o intensidad que libera el cuerpo la podemos medir, en función de su longitud de onda, obteniendo la siguiente gráfica:

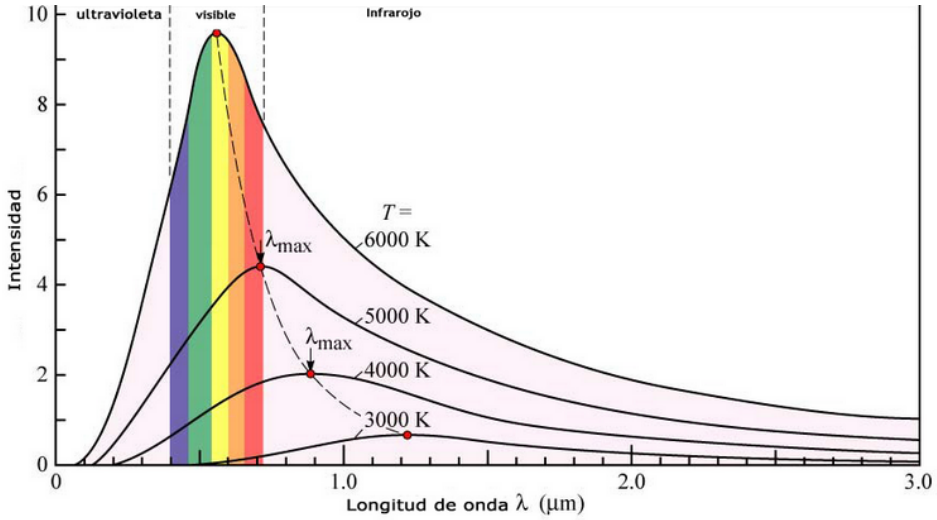


Figura 2: Catástrofe del ultravioleta. Obtenida de **?**

Podemos observar que a diferentes temperaturas (longitudes de onda) llegamos a diferentes curvas. La física clásica intentaba predecir estas curvas mediante ciertos modelos, que, aunque se ajustaban correctamente en distintas zonas de la gráfica, no se acercaban ni mucho menos a la realidad. Un ejemplo de esto es la catástrofe del ultravioleta, como resultado de no ajustarse correctamente en la zona ultravioleta, en la que la intensidad de la energía tendía a infinito como resultado de otros modelos, en lugar de tender a cero como propuso *Max Planck*, formulando una ecuación que describe perfectamente la figura (**??**):

$$B_\nu(T) = \frac{2h\nu^3}{c^2} \frac{1}{e^{\frac{h\nu}{k_B T}} - 1} \tag{1.2}$$

Donde h es la *constante de Planck*, ν la frecuencia de la radiación, c la velocidad de la luz en el vacío, k_B la *constante de Boltzmann*, T la temperatura, y e como base de los logaritmos naturales. No obstante, esta teoría cuántica fue primeramente descartada por los físicos de la época, al establecer que la energía no es un valor continuo sino discreto, hasta que con la llegada del efecto fotoeléctrico de *Albert Einstein* todo comenzó a cobrar sentido.

A finales del siglo XIX, en 1888, se presenta el efecto fotoeléctrico, definido por *Heinrich Hertz*, que consiste en la emision de electrones (fotoelectrones) al incidir luz sobre un metal, actuando como cátodo, los cuales se recogen en un ánodo, generando corriente en un circuito. Dicha luz suele ser ultravioleta, aunque en algunos casos puede ser visible.

Previamente al experimento, se plantearon varias hipótesis en base a la física clásica de la época:

- El aumento de la intensidad de la luz incrementaría la energía cinética de los fotoelectrones

emitidos.

- A mayor frecuencia mayor intensidad de corriente en el circuito.

Los resultados de dicho experimento fueron sorprendentes, ya que se observó que la energía cinetica de los electrones que poseen el cátodo no dependen de la intensidad de la luz, sino de su frecuencia, y adicionalmente se pudo ver que a mayor intensidad de luz mayor intensidad de corriente. Más tarde, en 1905, se presentó un artículo, ciertamente atrevido teniendo en cuenta los recursos de la época, que resolvía todos estos problemas.

Albert Einstein presentó su hipótesis para el efecto fotoeléctrico, basándose en los resultados del experimento de *Planck*, aclarando que la luz no se comporta como una onda, sino que está compuesta de pequeñas partículas, llamadas *fotones*, cuya energía depende de su frecuencia, como ya propuso *Max Planck* en (**??**), rompiendo de nuevo con los principios de la física clásica.

En dicha hipótesis se establece la necesidad de una frecuencia mínima, denominada frecuencia umbral, para que el efecto fotoeléctrico tenga lugar, la cual depende del material del que esté construido el cátodo. Por lo que si la frecuencia de los *fotones* emitidos por el haz de luz es menor a esta frecuencia umbral, no se produce corriente en el circuito, por muy intensa que sea la luz. De esta manera, si la frecuencia es mayor o igual a la umbral, los *fotoelectrones* se trasladarán hacia el ánodo al ser expulsados del núcleo de sus átomos, generando energía cinética y por lo tanto, intensidad de corriente en el circuito. Esto lo podemos razonar con la siguiente ecuación:

$$E_e = E_{ionizacion} + E_{cinetica} \tag{1.3}$$

Esta ecuación tiene sentido visto lo anterior, de manera que la energía de los electrones del cátodo ha de ser igual a su *energía de ionización* (o también conocido como *trabajo de extracción*), la cual es la cantidad de energía necesaria para que se produzca el efecto fotoeléctrico, sumado a su *energía cinética*. Por la explicación vista anteriormente, sabemos que dicha *energía de ionización* depende de la *frecuencia umbral* ν_0, y con la ecuación de la energía de *Planck* (**??**), además de conocer la *energía cinética* de una partícula, podemos desarrollar la expresión (**??**):

$$h\nu = h\nu_0 + \frac{1}{2}m_e v_e^2$$

Donde *h* es la *constante de Planck*, ν es la *frecuencia*, ν_0 es la *frecuencia umbral*, m_e es la masa del electrón, y v_e la velocidad del electrón, en este caso al cuadrado.

Estos son solo dos de los múltiples experimentos con soluciones extrañas para los físicos clásicos de aquella época, en los que, como hemos visto, el comportamiento de ciertos fenómenos, teóricamente

imaginados como funciones de onda, se comportan como partículas. También se da el fenómeno contrario, experimentos planteados como partículas pero que son razonados mediante funciones de onda. Esto se definió con el nombre de *dualidad onda-corpúsculo*.

Más tarde, tras estudiar a fondo las bases de la mecánica cuántica propuesta por *Max Planck* y *Albert Einstein*, *Louis de Broglie* propuso en su tesis doctoral, en *1924*, que no solo la luz tiene un carácter ondulatorio, sino que toda partícula material, como los electrones, tienen una naturaleza ondulatoria, cuya longitud de onda λ es:

$$\lambda = \frac{h}{p} \tag{1.4}$$

Donde *p* se refiere al *momento lineal* de la partícula, lo cual podemos expresar como $p = m \cdot v$, siendo *m* la masa, y *v* la velocidad de la partícula. Tras el razonamiento de *Broglie* en *1924*, surge la *función de onda* en una dimensión, la cual describe el comportamiento las partículas con carácter ondulatorio:

$$\varphi(x,t) = e^{i(px-Et)/\hbar} \tag{1.5}$$

Siendo *i* la unidad imaginaria, $\hbar$ la *constante de Planck normalizada*

$$\hbar = \frac{h}{2\pi} \tag{1.6}$$

y *x* y *t* las coordenadas de posición y tiempo de la partícula. Sin embargo, todavia no se conocia su significado fisico con total exactitud. No fue hasta que con el experimento de la doble rendija de *Clinton Davisson* y *Lester Germer* sobre electrones en *1927* (aunque *Thomas Young* lo propuso en *1801*, sobre un haz de luz, demostrando su naturaleza ondulatoria) que se confirmó la hipótesis de *De Broglie*. Como su propio nombre indica, dicho experimento consiste en una superficie opaca con dos rendijas, detrás de la cual colocamos un detector de partículas para poder percibir el comportamiento de los electrones o fotones que pasan a través de ambas rendijas. Según la física clásica, se espera que las partículas pasen a través de las rendijas en forma de línea recta, como lo haría cualquier objeto. Sin embargo, esto no sucede así en el contexto de la mecánica cuántica.

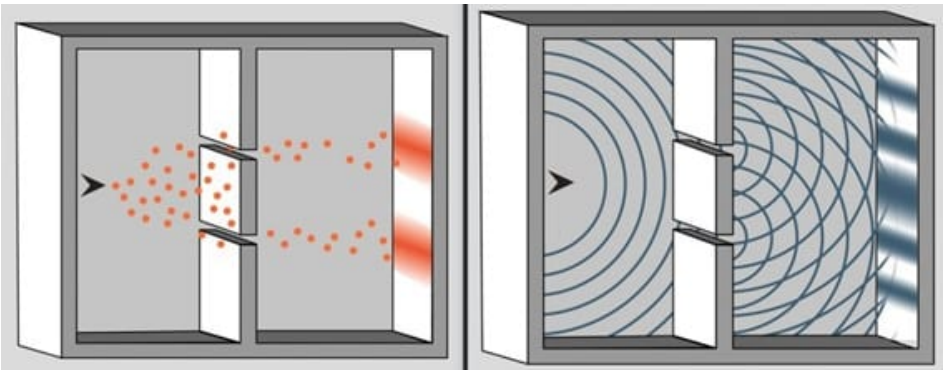


Figura 3: Experimento de la doble rendija. Obtenida de **?**

Al realizar el experimento, podemos observar un patrón de interferencias en la pantalla de detección situada detrás de las rendijas, el cual es muy similar al patrón que siguen las ondas cuando se superponen unas con otras. Efectivamente, las ondas asociadas a cada partícula se superponen unas con otras como se reveló en el experimento, no obstante, cuando observamos estas partículas mediante el detector, se comportan como una partícula clásica, cambiando su comportamiento, de manera que podemos ver por qué rendija cruzó la partícula. Este fenómeno se conoce como *colapso de función de onda*, y existen muchas teorías que intentar explicar esto, siendo la más famosa la *intepretación de Copenhage*, en la que se establece que la observación de la partícula produce un colapso de su función de onda, determinando su estado correspondiente a la medición.

Matemáticamente, podemos expresar la superposición de ondas como una superposición de estados, esto es:

$$\psi(x,t) = \psi_1(x,t) + \psi_2(x,t) + \cdots + \psi_n(x,t), \qquad \forall n \in \mathbb{N} \setminus \{0\} \tag{1.7}$$

Adicionalmente, surgieron ciertas dudas relacionadas con la naturaleza de la función de onda. Es lógico preguntarse que, si las partículas están definidas por funciones de onda, ¿Dónde están realmente las partículas? Ya que una partícula no puede estar en varios puntos a la vez, ha de estar en un único punto. Es aquí cuando entró *Max Born*, quien sugiere que $|\psi(x,t)|^2$ no es simplemente el cuadrado del módulo de la función de onda, sino que es una función de densidad de probabilidad, de manera que, para cada instante de tiempo y una región del espacio, la siguiente integral

$$\int_E |\psi(x,t)|^2 dx, \qquad \forall t \in \mathbb{R}, E \subset \Omega \tag{1.8}$$

Representa la densidad de probabilidad de encontrar una partícula para un valor de *t* en una determinada región *E* del espacio Ω, de manera que podemos deducir una condición que ha de cumplir la expresión (**??**):

$$\int_{\Omega} |\psi(x,t)|^2 dx = 1, \qquad \forall t \in \mathbb{R} \tag{1.9}$$

Esto tuvo una importancia bastante profunda en la mecánica cuántica de la época y en la física en general, ya que las únicas ideas de probabilidad estaban relacionadas a sistemas de incertidumbre, como el lanzamiento de una moneda. De esta manera se concluyó en la probabilidad como uno de los principales focos de la física y de la comprensión de las partículas subatómicas.

Esto concluye, al no poder medir con exactitud el estado de una partícula, como ocurre en la física clásica, en el *principio de incertidumbre* de *Heisenberg* en *1927*, estableciéndose que en la medición de una partícula no podemos conocer con completa exactitud la posición y el momento lineal a la vez, sino que cuanto más preciso midamos su posición exacta menos precisa será la medición del momento lineal de dicha partícula y viceversa.

CAPÍTULO

2

La Ecuación de Schrödinguer

2.1. Obtención de la Ecuación de Schrödinguer

Todas las ideas vistas anteriormente, la función de onda (**??**), la superposición cuántica (**??**) y la interpretacion probabilística de la función de onda (**??**) dieron lugar a la necesidad de decribir la evolución de la función de onda $\psi(x,t)$ en función del tiempo *t*. Es en este momento cuando aparece *Erwin Schrödinguer* en *1926*, presentando su famosa ecuación, obtenida de derivar y desarrollar la ecuación (**??**). En primer lugar, derivamos dicha expresión (**??**) con respecto al tiempo *t*:

$$\frac{\partial}{\partial t}\psi(x,t) = \frac{\partial}{\partial t}e^{i(px-Et)/\hbar}$$

$$\frac{\partial}{\partial t}\psi(x,t) = e^{i(px-Et)/\hbar}\left(-\frac{iE}{\hbar}\right)$$

Podemos observar que vuelve a aparecer la función de onda (**??**), al tratarse de una función exponencial:

$$\frac{\partial}{\partial t}\psi(x,t) = -\frac{iE}{\hbar}\psi(x,t)$$

A continuación multiplicamos ambos miembros por $i\hbar$, para eliminar los denominadores y substrayendos de la expresión:

$$i\hbar\frac{\partial}{\partial t}\psi(x,t) = E\psi(x,t) \tag{2.1}$$

Esta expresión la reservaremos para más adelante, ya que, en los siguientes cálculos, necesitaremos el producto de la energía del sistema E y la función de onda ψ. Como siguiente paso, vamos a continuar derivando la función de onda (**??**) con respecto de *x*:

$$\frac{\partial}{\partial x}\psi(x,t) = \frac{\partial}{\partial x}e^{i(px-Et)/\hbar}$$

$$\frac{\partial}{\partial x}\psi(x,t) = e^{i(px-Et)/\hbar}\left(\frac{ip}{\hbar}\right)$$

$$\frac{\partial}{\partial x}\psi(x,t) = \frac{ip}{\hbar}\psi(x,t)$$

Derivamos por segunda vez respecto de la variable espacial:

$$\frac{\partial}{\partial x^2}\psi(x,t) = \frac{\partial}{\partial x}\left(\frac{ip}{\hbar}\psi(x,t)\right)$$

$$\frac{\partial}{\partial x^2}\psi(x,t) = -\frac{p^2}{\hbar^2}\psi(x,t)$$

Multiplicamos por $(-\frac{\hbar^2}{2m})$ para obtener lo siguiente:

$$-\frac{\hbar^2}{2m}\frac{\partial}{\partial x^2}\psi(x,t) = \frac{p^2}{2m}\psi(x,t)$$

Conociéndose que la energía cinética es $E = \frac{p^2}{2m}$, obtenemos la siguiente expresión

$$-\frac{\hbar^2}{2m}\frac{\partial}{\partial x^2}\psi(x,t) = E\psi(x,t)$$

Sustituyendo el valor que acabamos de obtener $E\psi(x,t)$ en (**??**), llegamos prácticamente a la ecuación que estamos buscando:

$$i\hbar\frac{\partial}{\partial t}\psi(x,t) = -\frac{\hbar^2}{2m}\frac{\partial}{\partial x^2}\psi(x,t)$$

Para terminar, si agregamos la energía potencial y generalizamos la ecuación para más de una dimensión espacial, obtenemos la famosa ***ecuación de Schrödinguer***:

$$\boxed{i\hbar\frac{\partial}{\partial t}\psi(x,t) = (-\frac{\hbar^2}{2m}\Delta + V(x,t))\psi(x,t)} \tag{2.2}$$

Siendo Δ el operador Laplaciano en coordenadas canónicas, que se define como

$$\Delta = \frac{\partial}{\partial^2 x_1} + \cdots + \frac{\partial}{\partial^2 x_n}, \qquad \forall n \in \mathbb{N}$$

2.2. La Ecuación de Schrödinguer Independiente del Tiempo

A continuación, para obtener la *ecuación de Schrödinguer independiente del tiempo* tenemos que plantearnos obtener las soluciones de la ecuación de Schrödinguer (**??**). Para simplificar cálculos, vamos a suponer que la energía potencial $V(x)$ en (**??**) depende única y exclusivamente de la variable espacial *x*, de manera que podemos probar a encontrar soluciones por el método de *separación de variables*. Supongamos una solución como producto de dos funciones $\psi(x)$ y $\tau(t)$:

$$\Psi(x,t) = \psi(x)\tau(t)$$

Sustituyendo en (**??**) nos queda como

$$i\hbar\frac{\partial}{\partial t}\psi(x)\tau(t) = \left(-\frac{\hbar^2}{2m}\Delta + V(x)\right)\psi(x)\tau(t)$$

Podemos dividir entre $\psi(x)\tau(t)$ y ordenar ambos miembros, de manera que un miembro nos quede únicamente en función de *x* y otro en función de *t*:

$$i\hbar\frac{1}{\tau(t)}\frac{\partial}{\partial t}\tau(t) = V(x) - \frac{\hbar^2}{2m}\frac{1}{\psi(x)}\frac{\partial}{\partial x^2}\psi(x)$$

Hemos de recalcar que hemos tomado el laplaciano Δ como $\frac{\partial}{\partial x^2}$, siendo este el laplaciano en una dimensión espacial, con el fin de simplificar los cálculos. Llegados a este punto, para que se cumpla la igualdad, cada miembro de la ecuación ha de ser igual a una constante E, al demostrarse que se trata de una ecuación separable

$$\begin{cases} i\hbar\dfrac{1}{\tau(t)}\dfrac{\partial}{\partial t}\tau(t) = E \\ V(x) - \dfrac{\hbar^2}{2m}\dfrac{1}{\psi(x)}\dfrac{\partial}{\partial x^2}\psi(x) = E \end{cases} \tag{2.3}$$

Tomando como base la primera ecuación del sistema, podemos obtener una solución exponencial de la siguiente manera:

$$\frac{\partial}{\partial t}\tau(t) = \frac{E}{i\hbar}\tau(t)$$

$$\tau(t) = e^{\left(-\frac{Ei}{\hbar}\right)t}$$

Esto nos proporciona una evolución temporal del sistema en el que se encuentra la partícula. Sin embargo, para obtener la ecuación que estamos buscando, hemos de fijarnos en la segunda ecuación de (**??**):

$$V(x) - \frac{\hbar^2}{2m}\frac{1}{\psi(x)}\frac{\partial}{\partial x^2}\psi(x) = E$$

La cual podemos reescribir como

$$\left(-\frac{\hbar^2}{2m}\frac{\partial}{\partial x^2} + V(x)\right)\psi(x) = E\psi(x) \tag{2.4}$$

En muchas referencias, la ecuación (**??**) es ya la ecuación que estamos buscando. Sin embargo, nosotros la vamos a denotar en función del operador *Hamiltoniano* H, el cual representa la energía total de nuestro sistema cuando ésta permanece constante en el tiempo, que en nuestro caso sucede al establecer que $V(x,t) = V(x)$. Así, la ***ecuación de Schrödinguer independiente del tiempo*** queda como

$$\boxed{H\psi(x) = E\psi(x)} \tag{2.5}$$

Siendo $H = \left(-\frac{\hbar^2}{2m}\frac{\partial}{\partial x^2} + V(x)\right)$ el operador *Hamiltoniano*. Finalmente, podemos concluir que la solución completa queda como

$$\Psi(x,t) = e^{\left(-\frac{Ei}{\hbar}\right)t}\psi(x) \tag{2.6}$$

La ecuación (**??**) describe los estados estacionarios de una partícula en el potencial $V(x)$ y es usada en muchos sistemas físicos de vital importancia (generalmente aquellos cuyo potencial no depende del tiempo t) como átomos y moléculas en estado estacionario, siempre y cuando el sistema se encuentre en equilibrio y no haya fuerzas externas que varíen el valor de la energía potencial con respecto al tiempo, pozos de potencial infinito, osciladores armónicos, o campos eléctricos y gravitacionales constantes.

Sin embargo, hay otras muchas situaciones en las que el potencial no solo depende de la posición x, de manera que no podemos aplicar el método de separación de variables visto anteriormente, como partículas en campos magnéticos, problemas asociados a la relatividad, o sistemas caóticos. Para estos sistemas utilizamos otros métodos de resolución, como simulaciones numéricas, para alcanzar la solución del sistema.

CAPÍTULO

3

El Espacio de Hilbert

En el contexto de la mecánica cuántica, el *espacio de Hilbert*, el cual denotaremos como $\mathcal{H}$, es el marco matemático en el que nos apoyamos para explicar el estado físico de las partículas subatómicas, como ya veremos en la sección (**??**) explicando los postulados. Este *espacio de Hilbert* es simplemente una generalización de los espacios euclídeos $\mathbb{R}^n$ sobre el cuerpo de los números reales R o sobre los números complejos $\mathbb{C}$, siendo en el caso de la mecánica cuántica, como podremos imaginar, una generalización sobre $\mathbb{C}$ ya que la geometría compleja juega un papel fundamental en este campo de la física.

Una vez hemos introducido los *espacios de Hilbert*, vamos a pasar a explicar sus propiedades básicas, para poder comprender los conceptos que vendrán más adelante en los siguientes capítulos. La diferencia fundamental con respecto a los espacios euclídeos $\mathbb{R}^n$, además de que las distintas componentes de los vectores $|\psi\rangle \in \mathcal{H}$ son complejas, reside en el producto escalar, el cual para un espacio euclídeo $\mathbb{R}^n$ podemos expresar de la siguiente manera

$$\langle v, w\rangle = \sum_{i=0}^{N-1} v_i w_i, \qquad \forall\, v_i, w_i \in \mathbb{R}^n$$

Siendo N la dimensión del espacio euclídeo $\mathbb{R}^n$. La principal diferencia es que un *espacio de Hilbert* $\mathcal{H}$ cuenta con un producto escalar hermítico, el cual definiremos a continuación.

Consideremos un espacio vectorial $\mathcal{H} = \{|\psi\rangle, |\phi\rangle, \cdots\}$ sobre el cuerpo de los números complejos $\mathbb{C}$, de manera que se cumplen la propiedad de la suma y la multiplicación por un escalar:

$$|\psi\rangle + |\phi\rangle \in \mathcal{H}, \qquad \forall\, |\psi\rangle, |\phi\rangle \in \mathcal{H}$$

$$\alpha\,|\psi\rangle \in \mathcal{H}, \qquad \forall\, |\psi\rangle \in \mathcal{H} \quad \text{y} \quad \forall \alpha \in \mathbb{C}$$

Además, dicho espacio vectorial $\mathcal{H}$ cuenta con un producto escalar hermítico, el cual es una aplicación

$$\begin{aligned} \mathcal{H} \times \mathcal{H} &\longrightarrow \mathbb{C} \\ |\phi\rangle, |\psi\rangle &\longrightarrow \langle \phi \mid \psi \rangle \end{aligned}$$

Que cumple con las propiedades de linealidad y hermiticidad, respectivamente:

$$\langle \phi \mid \lambda_1 \psi_1 + \lambda_2 \psi_2 \rangle = \lambda_1 \langle \phi \mid \psi_1 \rangle + \lambda_2 \langle \phi \mid \psi_2 \rangle, \qquad \forall \lambda_1, \lambda 2 \in \mathbb{C}$$

$$\langle \phi \mid \psi \rangle = \langle \psi \mid \phi \rangle^*$$

Siendo $\langle \psi \mid \phi \rangle^*$ la expresión conjugada compleja de $\langle \phi \mid \psi \rangle$. Esta aplicación ha de ser definida positiva, de manera que

$$\langle \psi \mid \psi \rangle \geq 0 \quad \text{y} \quad \langle \psi \mid \psi \rangle = 0 \Leftrightarrow |\psi\rangle = 0$$

Si $\mathcal{H}$ satisface estas propiedades, podemos concluir que $\mathcal{H}$ es un espacio de Hilbert. Con esto podemos definir la norma de un vector ψ como

$$\|\psi\| = \sqrt{\langle \psi \mid \psi \rangle} \qquad \in \mathbb{R} \geq 0 \tag{3.1}$$

Podemos observar que $\|\psi\| \in \mathbb{R} \geq 0$, ya que al tratarse de la longitud de un vector, ha de ser un número real no negativo. Con esto podemos introducir la desigualdad de Schwartz, la cual establece lo siguiente:

$$\| \langle \phi \mid \psi \rangle \|^2 \leq \|\phi\|^2 \|\psi\|^2 \tag{3.2}$$

Al complirse esta expresión, el producto interno está bien definido, de donde obtenemos la norma como ya vimos en (**??**), pasando a ser un espacio normado cuya norma cumple con la *sucesión de Cauchy*:

$$\forall \epsilon > 0, \quad \exists N \in \mathbb{N} \text{ tal que } m, n \geq N \implies \|x_n - x_m\| < \epsilon$$

Por lo que además es un espacio completo. Con esto ya podemos llegar a la conclusión de que, un espacio de Hilbert, en resumidas cuentas, es un espacio vectorial $\mathcal{H}$ con un producto escalar hermítico, y por lo tanto sobre el cuerpo de los números complejos $\mathbb{C}$. Aún así, vamos a profundizar más en la definición de *producto escalar hermítico* en $\mathcal{H}$. Para ello, vamos a trabajar sobre el concepto de *espacio dual* y *ortonormalidad* definiendo una base ortonormal de nuestro espacio vectorial $\mathcal{H}$, como

$$B = \{|e_j\rangle\}_{j=0}^{N-1} \tag{3.3}$$

Donde N es la dimensión de $\mathcal{H}$. No obstante, esto no deja de ser una base común y corriente. Para que esta base sea ortonormal, se tienen que dar las condiciones de ortonormalidad, en las que se establece que el producto escalar de dos vectores distintos de dicha base es cero, y la norma de ambos vectores ha de ser igual a la unidad. Esto lo podemos formalizar de la siguiente manera

$$\langle e_1|e_2\rangle = \delta_{e_1,e_2}, \qquad \forall\ |e_1\rangle, |e_2\rangle \in B \tag{3.4}$$

$$\|e_j\| = 1, \qquad \forall\ |e_j\rangle \in B \tag{3.5}$$

Donde $\delta_{n,m}$ en (**??**) es la función *delta de Kronecker*, que se define como

$$\delta_{i,j} = \begin{cases} 1, & \text{si } i = j, \\ 0, & \text{si } i \neq j \end{cases} \tag{3.6}$$

Así, el producto escalar de dos vectores de una base ortonormal siempre va a ser cero, y el producto escalar de un vector cualquiera $|\psi\rangle \in \mathcal{H}$ consigo mismo es la unidad

$$\langle e_1|e_2\rangle = 0, \qquad \forall\ e_1, e_2 \in B \tag{3.7}$$

$$\|\psi\| = \sqrt{\langle \psi \mid \psi \rangle} = 1, \qquad \forall\ |\psi\rangle \in \mathcal{H} \tag{3.8}$$

Entonces, podemos expresar cualquier vector de nuestro espacio vectorial $\mathcal{H}$ como una combinación lineal de los vectores de la base:

$$|\psi\rangle = \sum_{j=0}^{N-1} c_j |e_j\rangle, \qquad \forall\ |\psi\rangle \in \mathcal{H} \quad \text{y} \quad \forall c_j \in \mathbb{C} \tag{3.9}$$

Esto es muy importante ya que vamos a usar estos vectores para ver el estado en el que se encuentra nuestro sistema cuantico. Esto está directamente ligado con la superposición de la función de onda, como ya vimos en (**??**), ya que, cada uno de los posibles estados de una partícula en una superposición de funciones de onda, no son más que los vectores de una base ortonormal perteneciente a un espacio de Hilbert $\mathcal{H}$. Esto es de vital importancia y lo seguiremos viendo cuando introduzcamos los estados de un *qubit*, como ya veremos más adelante.

Ahora vamos a dar las primeras nociones del *espacio dual* $\mathcal{H}^*$ de $\mathcal{H}$. Si tenemos un espacio de Hilbert $\mathcal{H}$ sobre el cuerpo de los número complejos $\mathbb{C}$, definimos su *espacio dual* $\mathcal{H}^*$ como el conjunto de todas las aplicaciones lineales que transforman elementos de $\mathcal{H}$, es decir, *kets*, en un número complejo $\mathbb{C}$

$$\mathcal{H}^* = \{\langle\phi| : \mathcal{H} \longrightarrow \mathbb{C}\}$$

Donde $\langle\phi|$ se construye con el conjugado hermítico, el cual se define con el operador †:

$$(|\phi\rangle)^\dagger = \langle\phi| \tag{3.10}$$

Aprovechamos para explicar la notación, en la tenemos los elementos pertenecientes al espacio dual $\mathcal{H}^*$ conocidos como *bra* $\langle\phi|$, vectores pertenecientes al espacio de Hilbert $\mathcal{H}$ que son llamados como *kets* $|\psi\rangle$, y el resultado de aplicar un producto escalar hermítico sobre un *bra* y un *ket*, al que haremos referencia como *bracket* $\langle\phi \mid \psi\rangle$.

El espacio dual $\mathcal{H}^*$ tiene una base dual asociada

$$B^* = \{\langle e_i|\}_{i=0}^{N-1} \tag{3.11}$$

mediante la que, de la misma manera que con la base B definida en (**??**) sobre un espacio de Hilbert $\mathcal{H}$, podemos expresar cualquier *bra* $\langle\phi| \in \mathcal{H}^*$ como una combinación lineal de los *bra* de la base B^*:

$$\langle\phi| = \sum_{i=0}^{N-1} d_i^* \langle e_i|\,, \qquad \forall\ \langle\phi| \in B^* \quad y \quad \forall\, c_i^* \in \mathbb{C} \tag{3.12}$$

Por lo tanto, la actuación de un *bra* $\langle\phi| \in \mathcal{H}^*$ sobre un *ket* $|\psi\rangle \in \mathcal{H}$ es el producto escalar hermítico de los *kets*, y debido a la propiedad de linealidad en $\mathcal{H}$, este producto queda perfectamente definido en $\mathcal{H}$

$$\begin{aligned}\langle\phi \mid \psi\rangle = |\phi\rangle \cdot |\psi\rangle = \left(\sum_{i=0}^{N-1} d_i^* \langle e_i|\right)\left(\sum_{j=0}^{N-1} c_j |e_j\rangle\right) = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} d_i^*\, c_j\ \langle e_i \mid e_j\rangle = \\ = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} d_i^*\, c_j\, \delta_{e_i,e_j} = \sum_{i=0}^{N-1} d_i^*\, c_i \implies \boxed{\langle\phi \mid \psi\rangle = \sum_{i=0}^{N-1} d_i^*\, c_i}\end{aligned} \tag{3.13}$$

Por lo que, el producto escalar hermítico $\langle\phi \mid \psi\rangle$ es simplemente multiplicar los complejos conjugados d_i^* provenientes del *bra* $\langle\phi|$ por los distintos elementos c_i de los vectores $|\psi\rangle$ del espacio de Hilbert $\mathcal{H}$.

Encontrándonos en este punto, a partir de (**??**) podemos desarrollar la norma de un vector en $\mathcal{H}$, obteniendo que

$$\|\psi\|^2 = \langle\psi \mid \psi\rangle = \sum_{i=0}^{N-1} d_i^* c_i = \sum_{i=0}^{N-1} |c_i|^2 = 1, \qquad \forall\psi \in \mathcal{H} \tag{3.14}$$

Esto es de vital importancia y nos ayudará a comprender y explicar los *postulados de la mecánica cuántica*, como vamos a ver a continuación.

3.1. Postulados de la Mecánica Cuántica

Una vez hemos asentado las bases históricas de la mecánica cuántica, introducido las funciones de onda, la ecuación de Schrödinguer, y hemos podido apreciar la relación de este campo de la física con el álgebra lineal, por medio de los espacios de Hilbert, estamos en condiciones de enunciar y comprender los postulados de la mecánica cuántica. Estos se podrían definir, a modo de resumen, en los principios fundamentales sobre los que se basa esta nueva teoría para definir el comportamiento de las partículas subatómicas, basándose en resultados experimentales como algunos que ya vimos en la introducción histórica (**??**). Comencemos por el primer postulado:

Postulado 1: *Para un instante t_0, el estado de un sistema cuántico se puede describir mediante un vector $|\varphi(t_0)\rangle$ de un espacio de Hilbert $\mathcal{H}$.*

Efectivamente, esto es uno de los puntos clave que vimos en (**??**) tratando sobre el espacio de Hilbert $\mathcal{H}$, en el que establecíamos que cualquier vector perteneciente a $\mathcal{H}$, se puede expresar como una combinación lineal de los vectores de la base, siendo esta base ortonormal.

Postulado 2: *Toda magnitud física medible $\mathcal{A}$ se representa mediante un operador hermítico A que actúa sobre $\mathcal{H}$. Este operador es un observable.*

En mecánica cuántica, a las magnitudes se les asigna un operador en concreto, un *observable*, y este *observable* no es más que un operador lineal hermítico. Vamos a ir desglosando punto por punto para enteder todo de la mejor manera posible. Un operador es un objeto que actúa sobre los elementos de un espacio vectorial, en nuestro caso, un espacio de Hilbert $\mathcal{H}$, transformándolos en otro vector perteneciente al mismo espacio

$$\hat{A}\,|\psi\rangle \xrightarrow{\hat{A}} |\psi'\rangle\,, \qquad |\psi\rangle\,, |\psi'\rangle \in \mathcal{H} \tag{3.15}$$

Pongamos como ejemplo el producto externo $|\phi\rangle\langle\psi|$ multiplicado a un vector $|\varphi\rangle \in \mathcal{H}$, esto es:

$$(|\phi\rangle\langle\psi|)\,(|\varphi\rangle) = |\phi\rangle\langle\psi \mid \varphi\rangle = |\phi\rangle\, k = k\,|\phi\rangle\,, \qquad k \in \mathbb{C}$$

Con esto hemos probado que $|\phi\rangle\langle\psi|$ es un *operador*, ya que

$$\hat{A}\,|\varphi\rangle = k\,|\phi\rangle\,, \qquad k \in \mathbb{C} \tag{3.16}$$

Esto resulta en que un operador fruto de un producto externo se puede expresar como una combinación lineal de productos externos de vectores de la base

$$\hat{A} = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} A_{ij} \left|i\right\rangle \left\langle j\right|, \qquad \forall \ \left|i\right\rangle, \left|j\right\rangle \in B \tag{3.17}$$

Podemos ver fácilmente que estos operadores se pueden representar como matrices cuadradas de dimensión $N \times N$. Además, partiendo de la expresión anterior, existe una condición suficiente y necesaria para que un conjunto de vectores sea base. Esta condición se denomina *relación de cierre*, y se obtiene de particularizar la expresión (**??**) para el operador identidad I, el cual se define como

$$I_{ij} = \left\{ \begin{array}{ll} 1, & \text{si } i = j \\ 0, & \text{si } i \neq j \end{array} \right\} = \delta_{ij} \tag{3.18}$$

Entonces, esta relación establece que, si la suma de los *ketbras* $\left|i\right\rangle \left\langle j\right|$ de los elementos de la base es igual al operador identidad I, todos los elementos de dicha base pueden generar el espacio de Hilbert $\mathcal{H}$, de la siguiente manera

$$I = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \delta_{ij} \left|i\right\rangle \left\langle j\right| = \sum_{i=0}^{N-1} \left|i\right\rangle \left\langle i\right|$$

$$I \left|\psi\right\rangle = \sum_{i=0}^{N-1} \left|i\right\rangle \left\langle i \mid \psi\right\rangle = \sum_{i=0}^{N-1} c_i \left|i\right\rangle = \left|\psi\right\rangle$$

$$I \left|\psi\right\rangle = \psi \tag{3.19}$$

De donde hemos obtenido que $\left\langle i \mid \psi\right\rangle = c_i$. Esto lo podemos obtener a partir de (**??**), de manera que

$$\left\langle i \mid \psi\right\rangle = \sum_{j=0}^{N-1} c_j \left\langle i \mid j\right\rangle \tag{3.20}$$

$$\left\langle i \mid \psi\right\rangle = \sum_{j=0}^{N-1} c_j \delta_{ij} = c_i \tag{3.21}$$

El resultado que acabamos de obtener en (**??**), c_i, por definición, es la proyección del vector $\left|\psi\right\rangle \in \mathcal{H}$ sobre el vector $\left|i\right\rangle$ de la base. Así, podemos observar que (**??**) es efectivamente la identidad I, y que dejará al vector $\left|\psi\right\rangle$ exactamente igual, cumpliéndose así la *relación de cierre*. A continuación, el concepto de linealidad en un operador no es más que

$$\hat{A} \left(a \left|\psi\right\rangle + b \left|\phi\right\rangle\right) = a\hat{A} \left|\psi\right\rangle + b\hat{A} \left|\phi\right\rangle, \qquad \psi, \phi \in \mathcal{H} \text{ y } \forall \ a, b \in \mathbb{C} \tag{3.22}$$

Y, finalmente, nos queda definir la condición de hermiticidad en un operador, resultando en un *operador hermítico* que, como podemos imaginar, cumple con

$$\hat{A}^\dagger = \hat{A} \tag{3.23}$$

De manera que tras aplicar el operador † sobre $\hat{A}$, se vuelve a obtener $\hat{A}$. Esto conlleva a otra condición, que se obtiene como resultado de (**??**):

$$\hat{A}^\dagger = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} A_{ij}^\dagger \left(|i\rangle \langle j|\right)^\dagger = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} A_{ij}^* |j\rangle \langle i| = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} A_{ji}^* |i\rangle \langle j|$$

Entonces, como vimos en (**??**), para que un operador sea hermítico, su traspuesto conjugado $\hat{A}^\dagger$ ha de ser igual a él mismo $\hat{A}$, resultando en la siguiente condición

$$\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} A_{ji}^* |i\rangle \langle j| = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} A_{ij} |i\rangle \langle j| \tag{3.24}$$

$$A_{ji}^* = A_{ij} \tag{3.25}$$

Y esta condición (**??**) se ha de cumplir en todo observable.

Postulado 3: *Los únicos resultados posibles a obtener en una medición de la magnitud $\mathcal{A}$ son los autovalores del operador $\hat{A}$. En la definición de operador se pide que $\hat{A}$ sea hermítico, por lo que las cantidades medidas serían reales*.

Comencemos con la definición de *autovector* y *autovalor*. Imaginemos un operador $\hat{A}$ actuando sobre un vector ψ, de manera que, tras aplicar el operador, obtenemos el mismo vector ψ multiplicado por un escalar λ. Esto es el autovector ψ asociado al autovalor λ, respectivamente:

$$\hat{A} |\psi\rangle = \lambda |\psi\rangle , \qquad \lambda \in \mathbb{R} \tag{3.26}$$

Y podemos verificar que $\lambda \in \mathbb{R}$, partiendo de (**??**) y tomando el producto interno en ambos miembros, como sigue a continuación

$$\langle\psi| \hat{A} |\psi\rangle = \lambda \langle\psi|\psi\rangle$$

$$\langle\psi| \hat{A} |\psi\rangle = \langle\psi| \hat{A}^\dagger |\psi\rangle = \lambda^* \langle\psi|\psi\rangle$$

Por lor que hemos demostrado que $\lambda \in \mathbb{R}$ ya que $\lambda^* = \lambda$. Por último vamos a ver que los autovectores asociados a autovalores distintos entre sí son ortogonales, es decir, su producto escalar es igual a cero:

$$(\hat{A}\,|\psi_i\rangle)^\dagger = (\lambda_i\,|\psi_i\rangle)^\dagger$$

$$\langle\psi_i|\,\hat{A} = \lambda_i^*\,\langle\psi_i| = \lambda_i\,\langle\psi_i|$$

$$\langle\psi_i|\,\hat{A}\,|\psi_j\rangle = \lambda_i\,\langle\psi_i|\psi_j\rangle$$

Dado que $\hat{A}\,|\psi_j\rangle = \lambda_j\,|\psi_j\rangle$, obtenemos la siguiente igualdad:

$$\langle\psi_i|\,\lambda_j\,|\psi_j\rangle = \lambda_i\,\langle\psi_i|\psi_j\rangle$$

$$(\lambda_j - \lambda_i)\,\langle\psi_i|\psi_j\rangle = 0$$

Y debido a que $\lambda_j \neq \lambda_i$, obtenemos que ambos autovectores ψ_i,ψ_j

$$\langle\psi_i|\psi_j\rangle = 0 \tag{3.27}$$

Son ortogonales. Entonces, podemos concluir que, en un espacio de Hilbert $\mathcal{H}$, un operador hermítico $\hat{A}$ tiene N autovectores $|\psi_i\rangle$ asociados a los autovalores λ_i, que como hemos demostrado, pertenecen al conjunto de los números reales $\mathbb{R}$ y son ortogonales entre sí, por lo que únicamente tendríamos que normalizar dichos autovectores para obtener una base ortonormal de autovectores, cumpliendo con el *Teorema Espectral*, el cual establece que todo operador hermítico $\hat{A}$ definido en un espacio de Hilbert $\mathcal{H}$ de dimensión finita es diagonalizable, es decir, existe una base ortonormal $B_{\hat{A}} \in \mathcal{H}$ formada por los autovectores $|\psi_i\rangle$ del operador $\hat{A}$.

De esta manera no solo garantizamos que todo operador $\hat{A} \in \mathcal{H}$ sea diagonalizable, sino que podemos expresar cualquier vector $|\phi\rangle \in \mathcal{H}$ como combinación lineal de los autovectores de $\hat{A}$, por lo que los resulados de la medición son los autovalores λ_i de dicho operador, que como hemos demostrado anteriormente, $\lambda_i \in \mathbb{R}$.

Postulado 4: **Regla de Born**. *Cuando medimos la magnitud $\mathcal{A}$ en un sistema cuántico que se encuentra en el estado $|\psi\rangle$, la probabilidad $\mathcal{P}(\lambda_n)$ de obtener el autovalor no degenerado λ_n del observable A será*

$$\mathcal{P}(\lambda_n) = \|\,\langle\lambda_n \mid \psi\rangle\,\|^2 \tag{3.28}$$

donde $|\lambda_n\rangle$ es el autovector normalizado asociado al autovalor λ_n.

Como bien ya sabemos, el resultado de una medición en en mecánica cuántica se rige bajo una función de probabilidad, y esta probabilidad se define como en (**??**). En este punto puede surgirnos

una pregunta interesante, y es que la media de estas probabilidades puede darnos una pequeña orientación, con cierto riesgo, del valor esperado de dicha medición. Podemos obtener la media, al ser la suma ponderada de los posibles estados que podemos obtener al medir la magnitud $\mathcal{A}$:

$$< \hat{A} >_{|\psi\rangle} = \sum_{i=0}^{N-1} \lambda_i \mathcal{P}_i = \sum_{i=0}^{N-1} \lambda_i \| \langle \lambda_i \mid \psi \rangle \|^2 = \sum_{i=0}^{N-1} \lambda_i \langle \psi \mid \lambda_i \rangle \langle \lambda_i \mid \psi \rangle =$$

$$= \langle \psi | \left(\sum_{i=0}^{N-1} \lambda_i |\lambda_i\rangle \langle \lambda_i | \right) |\psi\rangle = \langle \psi | \hat{A} |\psi\rangle$$

Así queda que ya tenemos la media, una orientación del valor λ_n que puede tomar el resultado, pero, ¿Y el resultado, qué pasa con él?

Postulado 5: *Si en la medición de la magnitud $\mathcal{A}$ en un sistema en el estado $|\psi\rangle$ obtenemos el resultado λ_i, inmediatamente después de la medición, el estado del sistema será la proyección del estado $|\psi\rangle$ sobre el subespacio asociado a λ_i*:

$$|\psi\rangle \xrightarrow{\lambda_i} \frac{\hat{\Pi}_i |\psi\rangle}{\sqrt{\langle \psi | \hat{\Pi}_i |\psi\rangle}} \tag{3.29}$$

Donde $\hat{\Pi}_i$ es el operador proyección sobre el subespacio asociado a λ_i.

Después de medir y obtener el resultado λ_i, que, como sabemos por el tercer postulado, es un autovalor, el estado se proyecta sobre el autovector asociado al resultado λ_i. Matemáticamente, esto lo podemos expresar mediante el producto del estado de la partícula por su proyector:

$$|\psi_i\rangle = \hat{\Pi}_i |\psi\rangle \tag{3.30}$$

Definiéndose así el operador de proyección sobre un vector como el producto externo del autovector $|\lambda_i\rangle$ sobre el que queremos proyectar nuestro estado $|\psi\rangle$

$$\hat{\Pi}_i = |\lambda_i\rangle \langle \lambda_i|$$

Que, por definición, su cuadrado es igual a sí mismo, y es ortogonal al resto de proyectores

$$\hat{\Pi}_i{}^2 = |\lambda_i\rangle \langle \lambda_i \mid \lambda_i \rangle \langle \lambda_i| = |\lambda_i\rangle \langle \lambda_i| = \hat{\Pi}_i$$

$$\hat{\Pi}_i \hat{\Pi}_j = 0$$

Siguiendo en la expresión (**??**), como el módulo del estado $|\psi_i\rangle$ debe ser igual a la unidad, lo dividimos entre su módulo para normalizarlo, y desarrollando la expresión que nos queda, llegamos al autovector asociado al resultado de la medición

$$|\psi_i\rangle = \frac{\hat{\Pi}_i |\psi\rangle}{|\hat{\Pi}_i |\psi\rangle|} = \frac{|\lambda_i\rangle \langle\lambda_i \mid \psi\rangle}{\sqrt{|\,|\lambda_i\rangle \langle\lambda_i \mid \psi\rangle\,|^2}} = \frac{|\lambda_i\rangle \langle\lambda_i \mid \psi\rangle}{\sqrt{|\,\langle\psi \mid \lambda_i\rangle \langle\lambda_i \mid \lambda_i\rangle \langle\lambda_i \mid \psi\rangle\,|^2}} =$$
$$= \frac{|\lambda_i\rangle \langle\lambda_i \mid \psi\rangle}{\sqrt{|\,\langle\psi \mid \lambda_i\rangle \langle\lambda_i \mid \psi\rangle\,|^2}} = \frac{|\lambda_i\rangle \langle\lambda_i \mid \psi\rangle}{\sqrt{|\,\langle\lambda_i \mid \psi\rangle\,|^2}} = \frac{\langle\lambda_i \mid \psi\rangle}{|\,\langle\lambda_i \mid \psi\rangle\,|} |\lambda_i\rangle = e^{i\theta} |\lambda_i\rangle$$

Siendo

$$e^{i\theta} = \frac{\langle\lambda_i \mid \psi\rangle}{|\,\langle\lambda_i \mid \psi\rangle\,|} \tag{3.31}$$

La conocida como *fase global*, la cual es un número complejo de módulo igual a la unidad, de manera que si multiplicamos dicha fase por un estado cuántico, dicho estado va a corresponder al mismo estado físico. Esto se debe a que si calculamos el módulo al cuadrado del producto de dos vectores arbitrarios con una fase global $e^{i\theta}$

$$|\psi'\rangle = e^{i\theta} |\psi\rangle$$
$$|\phi'\rangle^\dagger = e^{i\rho^\dagger} |\phi\rangle^\dagger \;\rightarrow\; \langle\phi'| = e^{-i\rho} \langle\phi|$$

El resultado sigue siendo el mismo que si no la tuviera

$$|\,\langle\phi' \mid \psi'\rangle\,|^2 = |e^{i\theta} e^{-i\rho} \langle\phi \mid \psi\rangle\,|^2 = |e^{i(\theta-\rho)}|^2 \,|\,\langle\phi \mid \psi\rangle\,|^2 =$$
$$= e^{i(\theta-\rho)} e^{-i(\theta-\rho)} \,|\,\langle\phi \mid \psi\rangle\,|^2 = e^0 \,|\,\langle\phi \mid \psi\rangle\,|^2 = |\,\langle\phi \mid \psi\rangle\,|^2$$

Por lo que podemos concluir que la proyección normalizada de un estado $|\psi_i\rangle$ es su autovector λ_i:

$$|\psi_i\rangle = \frac{\hat{\Pi}_i |\psi\rangle}{\sqrt{\hat{\Pi}_i |\psi\rangle}} \equiv |\lambda_i\rangle \tag{3.32}$$

Postulado 6: *La evolución temporal del estado de un sistema $|\psi(t)\rangle$ está gobernada por la ecuación de Schrödinger*,

$$i\hbar \frac{\partial}{\partial t} |\psi(t)\rangle = H(t) |\psi(t)\rangle\,, \tag{3.33}$$

donde $H(t)$ es el observable asociado a la energía total del sistema.

Esto ya lo vimos en (**??**), en el que obtuvimos la ecuación de Schrödinger a partir de la función de onda (**??**), y la desarrollamos obteniendo además la ecuación de Schrödinguer independiente del tiempo (**??**), con la que podemos ver perfectamente que el operador hamiltoniano H representa la energía total del sistema. Por otra parte, con esta ecuación vemos claramente que el sistema cuántico

no es realmente un espacio de Hilbert de dimensión finita, sino que, al trabajar con derivadas parciales, también aparecen primitivas e integrales, dando paso a la siguiente sección, en la que describiremos un espacio de Hilbert L^2 en infinitas dimensiones.

A modo de conclusión, con estos postulados y con la introducción a los espacios de Hilbert $\mathcal{H}$, hemos visto la estrecha relación entre la mecánica cuántica y el álgebra lineal, ya que, como vimos anteriormente, el sistema cuántico es un espacio de Hilbert $\mathcal{H}$, el cual es un espacio vectorial, en el que podemos expresar el estado de una partícula subatómica a través de un vector $|\psi\rangle$, y expresar dicho vector como combinación lineal de vectores de la base, realizar aplicaciones sobre dicho vector, ver como surgen conceptos básicos del álgebra lineal como autovectores y autovalores, y todas las lecciones tratadas anteriormente. Por esto es el espacio de Hilbert tan importante en la física cuántica (además de aplicarse en muchos otros campos de la ciencia), porque es el puente que conecta la mecánica de las partículas y las matemáticas.

3.2. El Espacio de Hilbert en Dimensión Infinita

En la sección anterior, explicamos los conceptos básicos de un espacio de Hilbert $\mathcal{H}$ en una dimensión finita, donde definíamos en (**??**) una base de dicho espacio vectorial de dimensión N. Esto lo hicimos para dar una mejor explicación y comprender todos los conceptos adecuadamente, aunque en la mecánica cuántica no suceda realmente así.

Sin embargo, podemos pensar que, cuando N tiende al infinito ($N \to \infty$), todo el trabajo que llevamos hasta ahora es válido, y no vamos por mal camino, simplemente hemos de hacer algunos cambios en las expresiones vistas anteriormente. Comencemos por la base, que ahora tendrá infinitas componentes:

$$B = \{|\alpha\rangle\}_{\alpha\in\mathbb{R}} \tag{3.34}$$

Entonces, tenemos que modificar la nomenclatura vista anteriormente, como cuando establecimos en la expresión (**??**) que podemos expresar todo vector perteneciente a un espacio de Hilbert, ahora tenemos que generalizar dicha expresión para un espacio de dimensión infinita, quedando que

$$|\psi\rangle = \int_{\mathbb{R}} c(\alpha)\,|\alpha\rangle\,d\alpha \tag{3.35}$$

Donde $c\,(\alpha)$ es una función compleja de variable real, siendo ahora una función continua, la cual es la contrapartida de lo que llamábamos antes c_j, que no eran más que elementos complejos de una sucesión en la que para cada valor de j obteníamos un número complejo c_j. Por otra parte, la generalización de un sumatorio en un espacio continuo es simplemente la integral sobre un cierto dominio perteneciente a $\mathbb{R}$ que ya definiremos más adelante. Con esto, hemos dado el salto de un vector perteneciente a un espacio discreto, a un vector en un espacio continuo $|\psi\rangle \in L^2$, el cual

ya veremos más adelante, de momento vamos a quedarnos con la idea de que L^2 es un espacio de Hilbert muy concreto y de dimensión infinita. De la misma manera que en (**??**), el vector dual se puede construir con la misma lógica que cuando lo definimos para una base finita en (**??**)

$$\langle\psi| = \int_{\mathbb{R}} c^*(\alpha)\,\langle\alpha|\,d\alpha \tag{3.36}$$

Sin embargo, a la hora de definir el producto escalar de dos vectores de la base α, α' hay un pequeño cambio, y esto lo podemos ver a través de la proyección $c(\alpha)$ del vector $|\psi\rangle$ sobre el vector de la base $|\alpha\rangle$:

$$\langle\alpha \mid \psi\rangle = c(\alpha)$$
$$\langle\alpha \mid \psi\rangle = \langle\alpha| \int_{\mathbb{R}} c\,(\alpha')\,|\alpha'\rangle\,d\alpha' = \int_{\mathbb{R}} c(\alpha')\,\langle\alpha \mid \alpha'\rangle\,d\alpha' = c(\alpha)$$

Para que la expresión anterior sea cierta, $\langle\alpha \mid \alpha'\rangle$ tiene que ser un función que recibe como parámetros α y α', en concreto se establece la *delta de Dirac*, de manera que

$$\int_{\mathbb{R}} c(\alpha')\,\delta(\alpha - \alpha')d\alpha' = c(\alpha)$$

La *delta de Dirac* es

$$\delta(x) = \begin{cases} 0, & \text{si} \quad x \neq 0 \\ +\infty, & \text{si} \quad x = 0 \end{cases} \tag{3.37}$$

Y esto no es una función, ya que una función asocia a cada $x \in \mathbb{R}$, otro número real, y sabemos que $+\infty \notin \mathbb{R}$. Además, como δ es cero $\forall x \in \mathbb{R}$ a excepción del punto cero, la integral debería ser cero y no la unidad. No obstante, la *delta de Dirac* aparece con mucha frecuencia en física, especialmente en mecánica ondulatoria, y no es sorpresa que aparezca en mecánica cuántica, al tener las partículas subatómicas un carácter ondulatorio como vimos en (**??**).

La *delta de Dirac* es un funcional lineal, y esto es simplemente una aplicación cuyo dominio es un espacio vectorial dado y cuyo recorrido es un conjunto numérico. En nuestro caso, estamos hablando de un funcional lineal en un espacio de Hilbert de dimensión infinita L^2 sobre el cuerpo de los números complejos $\mathbb{C}$

Entonces, una vez definida la *delta de Dirac*, podemos expresar el producto escalar de dos vectores α, α' de la base como

$$\langle\alpha \mid \alpha'\rangle = \delta(\alpha - \alpha') \tag{3.38}$$

Siendo este otro de los cambios notables al ampliar a una dimensión infinita, ya que este producto en una base finita de un espacio de Hilbert $\mathcal{H}$ era anteriormente la *delta de Kronecker* δ_{ij} (**??**). Una vez

aclarado esto, podemos expresar el producto de dos vectores $|\psi\rangle, |\phi\rangle \in L^2$ cualesquiera, obteniendo una expresión bastante similar a la que obtuvimos en (**??**) en un espacio discreto de Hilbert $\mathcal{H}$

$$\langle\phi \mid \psi\rangle = \int_{\mathbb{R}} b^*(\alpha') \langle\alpha'| \, d\alpha' \int_{\mathbb{R}} c(\alpha) |\alpha\rangle \, d\alpha = \int \int_{\mathbb{R}} b^*(\alpha') \, c(\alpha) \langle\alpha' \mid \alpha\rangle \, d\alpha' \, d\alpha =$$

$$= \int \int_{\mathbb{R}} b^*(\alpha') \, c(\alpha) \, \delta(\alpha' - \alpha) d\alpha' \, d\alpha = \int_{\mathbb{R}} b^*(\alpha) \, c(\alpha) d\alpha$$

$$\langle\phi \mid \psi\rangle = \int_{\mathbb{R}} b^*(\alpha) \, c(\alpha) d\alpha \tag{3.39}$$

Teniendo esto en cuenta, podemos obtener un caso particular de la expresión (**??**), y es que el producto escalar de un vector $|\psi\rangle \in L^2$ consigo mismo:

$$\langle\psi \mid \psi\rangle = \int_{\mathbb{R}} c^*(\alpha) \, c(\alpha) \, d\alpha = \int_{\mathbb{R}} |c(\alpha)|^2 \, d\alpha = 1 \tag{3.40}$$

Esta proyección ha de ser igual a la unidad, ya que la proyección de cualquier vector consigo mismo siempre es uno. Además, también cumplimos con la interpretación física del vector $|\psi\rangle$, ya que el resultado que acabamos de obtener ya lo vimos en (**??**), cuando *Max Born* introdujo la interpretación probabilística de la función de onda.

Al imponer la condición vista en (**??**), la función $c(\alpha)$ ha de ser parte de un espacio vectorial muy concreto, el espacio L^2, el cual es un *espacio de Lebesgue* L^p para $p = 2$, que podemos definir como sigue: Sea $f : \mathbb{R} \to \mathbb{C}$, entonces $f \in L^p(\mathbb{R})$ si

$$\int_{-\infty}^{+\infty} |f(x)|^p dx < \infty, \qquad \forall \, x \in \mathbb{R}, \quad p \geq 1 \tag{3.41}$$

Es decir, nuestra función compleja de variable real $c(\alpha)$ ha de ser de cuadrado integrable, perteneciendo así a un espacio L^2 el cual es el único *espacio de Lebesgue* L^p que es un espacio de Hilbert $\mathcal{H}$. Para un espacio L^2 se garantizan todas las propiedades vistas anteriormente para un espacio de Hilbert de dimensión infinita, aunque hemos de establecer que la expresión vista en la definición de un espacio cuyo módulo es cuadrado integrable no solo ha de ser $< \infty$, sino que ha de ser igual a la unidad, como vimos en (**??**):

$$\langle\psi \mid \psi\rangle = \int_{\mathbb{R}} |c(\alpha)|^2 \, d\alpha = 1$$

Esto es debido a la interpretación física del vector $|\psi\rangle$. De hecho, es muy importante conocer que $c(\alpha)$ es la famosa función de onda de la mecánica cuántica $\psi(x)$, sobre la cual hemos estado hablando antes de adentrarnos en los espacios de Hilbert $\mathcal{H}$. Para finalizar, también hemos de recalcar que hemos estado trabajando sobre una única dimensión espacial, para que la explicación sea más sencilla y fácil de entender, pero esto en realidad se debe hacer en las tres dimensiones espaciales del espacio, que se suele compactar con una notación vectorial

$$|\psi\rangle = \int_{\mathbb{R}^3} c(\vec{x})\,|\vec{x}\rangle\,d\vec{x}, \qquad \forall\ \vec{x} \in \mathbb{R}^3$$

CAPÍTULO

4

El Qubit

Antes de nada, es importante definir algunos conceptos. Empecemos por el ordenador cuántico, esto es una máquina que se rige por las leyes de la mecánica cuántica, como hemos estudiado anteriormente, de manera que es capaz de aprovechar todas las ventajas de las partículas a nivel subatómico como la superposición, vista en (**??**), o el entrelazamiento, el cual veremos más adelante. Estas propiedades son fundamentales para la reducción de tiempos de cómputo y complejidad de ciertas tareas, poniendo como ejemplo algoritmos de fuerza bruta o de factorización, los cuales se ven mejorados con los algoritmos cuánticos de *Grover* y *Shor*, respectivamente.

De la misma manera que los computadores cuánticos aprovechan las propiedades de la mecánica cuántica, sus predecesores, los computadores clásicos se apoyan en un cierto sistema numérico, el *sistema binario*. Este sistema se basa únicamente en dos estados, 0 y 1, que se construyen en base a la ausencia o incremento de corriente, respectivamente. Estos estados se conocen como *bits*, que por definición son la unidad de información clásica. Sin embargo, un ordenador cuántico utiliza la unidad de información cuántica, el *qubit*, que representa el estado de una partícula subatómica y que además de poder encontrarse en los estados clásicos $|0\rangle$ y $|1\rangle$, también se puede encontrar en una combinación lineal de estos estados, es decir

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \qquad \alpha, \beta \in \mathbb{C} \tag{4.1}$$

Además, la norma de este qubit $|\psi\rangle$ ya la definimos anteriormente en (**??**), por lo que podemos deducir que

$$|\alpha|^2 + |\beta|^2 = 1 \tag{4.2}$$

Con esta condición, podemos representar el estado del qubit en una esfera, la *esfera de Bloch*, esto nos ayudará a visualizar el estado del qubit de la mejor manera posible, y nos ayudará a comprender los siguientes capítulos. Para ello, podemos parametrizar el estado del qubit $|\psi\rangle$ definido en (**??**) en función de dos ángulos θ y φ, sustituyendo α y β por las siguientes funciones trigonométricas:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)|1\rangle$$

Pero ya definimos en (**??**) que $\alpha, \beta \in \mathbb{C}$, por lo que podemos multiplicar ambos coeficientes por un número complejo de módulo igual a la unidad, de manera que se cumple (**??**), y desarrollando, llegamos a que

$$|\psi\rangle = e^{i\alpha}\cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\beta}\sin\left(\frac{\theta}{2}\right)|1\rangle = e^{i\alpha}\left[\cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i(\beta-\alpha)}\sin\left(\frac{\theta}{2}\right)|1\rangle\right]$$

Esto es el estado de nuestro qubit $|\psi\rangle$ multiplicado por una fase global $e^{i\alpha}$, de manera que no cambia el estado físico del qubit, siendo su módulo al cuadrado equivalente, como vimos en el quinto postulado, de manera que podemos eliminar dicha fase global ya que no aporta significado físico a nuestro qubit. También vamos a establecer el ańgulo $\varphi = \beta - \alpha$, concluyendo en

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle, \qquad 0 \leq \theta \leq \pi, \quad 0 \leq \varphi \leq 2\pi \tag{4.3}$$

Esto nos permite representar el qubit $|\psi\rangle$ mediante la *esfera de Bloch* mencionada anteriormente

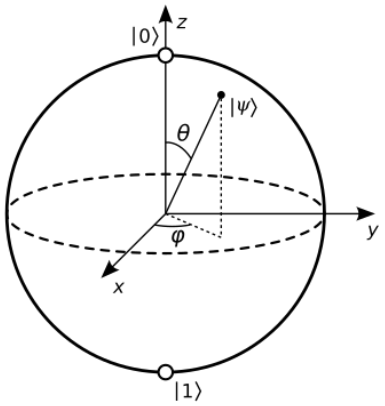


Figura 4: Esfera de Bloch. Obtenida de **?**

Pudiendo representar todos los posibles estados de un qubit $|\psi\rangle$ como un vector dentro de esta esfera. Si nos fijamos en la expresión (**??**) que acabamos de ver, vemos que hay un número complejo $e^{i\varphi}$ de módulo uno, similar a una fase global. Sin embargo, esto no es una fase global, ya que para ello ha de multiplicar a todos los posibles estados del qubit, y vemos en este caso que solo aparece en el estado $|1\rangle$, por lo que es una *fase relativa*, y a diferencia de las fases globales que no cambian el significado físico del qubit, la fase relativa sí lo modifica. Esto es debido a que, aunque los coeficientes que acompañan a $|0\rangle$ y $|1\rangle$ sigan cumpliendo que su módulo al cuadrado sea uno, el vector representado en la esfera de Bloch es diferente, ya que puede variar el ángulo φ.

Podemos pensar que aunque cambie la fase relativa no va a cambiar la probabilidad de obtener el estado $|0\rangle$ o $|1\rangle$ al medir el qubit. Esto se debe a que las mediciones se realizan normalmente sobre el eje Z y dicho vector estaría a la misma distancia de ambos polos de la esfera, manteniendo la probabilidad de obtener ambos estados $|0\rangle, |1\rangle$ invariante, ya que la probabilidad de obtener un estado viene dada por el módulo al cuadrado de los coeficientes que los acompañan, como se puede apreciar en la expresión (**??**). Pero, ¿Y si cambiamos de base?

4.1. Medición del Estado un Qubit

Antes de hacer cambios de base, tenemos que tratar sobre las mediciones, las cuales ya hemos introducido en los párrafos anteriores y en esta pequeña sección vamos a profundizar sobre este tema. Como bien sabemos, un qubit puede estar en una superposición de $|0\rangle$ y $|1\rangle$ debido a las leyes de la mecánica cuántica, pero esto también establece que cuando vamos a leer el resultado de una operación, como al finalizar un algoritmo cuántico, este qubit colapsa a un único estado, de manera que obtenemos $|0\rangle$ o bien $|1\rangle$, cada uno con una cierta probabilidad, y esa probabilidad es el módulo al cuadrado de los coeficientes que acompañan a cada posible estado, como vimos en (**??**). Estos coeficientes se denominan amplitudes, y al tratarse de una probabilidad, la suma del módulo al cuadrado de las amplitudes ha de ser igual a uno. Vamos a ver esto con un ejemplo:

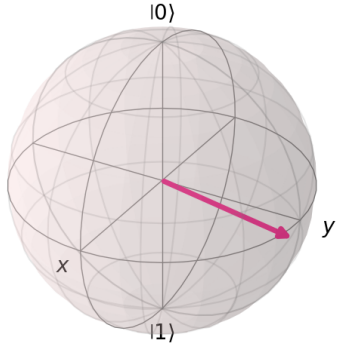


Figura 5: Medición de un Qubit.

Sea el siguiente qubit $|\psi\rangle$:

$$|\psi\rangle = \frac{1+i\sqrt{3}}{3}|0\rangle + \frac{2-i}{3}|1\rangle$$

La probabilidad de obtener el estado $|0\rangle$ y el estado $|1\rangle$ viene dada por

$$\left|\frac{1+i\sqrt{3}}{3}\right|^2 + \left|\frac{2-i}{3}\right|^2 = \left(\frac{1+i\sqrt{3}}{3}\right)\left(\frac{1-i\sqrt{3}}{3}\right) +$$
$$+\left(\frac{2-i}{3}\right)\left(\frac{2+i}{3}\right) = \frac{4}{9} + \frac{5}{9} = 1$$

Siendo la probabilidad de colapsar en $|0\rangle$ de $\frac{4}{9}$ y de $\frac{5}{9}$ en el estado $|1\rangle$. Esto lo podemos ver gráficamente si representamos el vector correspondiente al estado $|\psi\rangle$ en la esfera de Bloch, ya que si nos fijamos en (**??**) podemos ver que $|\psi\rangle$ está un poco más cercano al estado $|1\rangle$ de dicha esfera, y esto se corresponde con una probabilidad mayor de obtener dicho estado, como hemos podido apreciar en el ejemplo anterior.

Una vez definida correctamente la medición de un qubit, podemos hablar más profundamente sobre

el concepto de *colapso* de un qubit. Cuando medimos un qubit, este colapsa a un estado como hemos visto anteriormente, que puede ser $|0\rangle$ o $|1\rangle$ según el ejemplo propuesto, de manera que el estado del qubit se vuelve completamente fijo al estado que ha colapsado, por lo que el qubit deja de estar en superposición, y es forzado a tomar un bando, en este caso $|0\rangle$ o $|1\rangle$. Esto hace que el estado del qubit esté ya completamente definido, de manera que si volvemos a medir el estado de $|\psi\rangle$, obtendremos el estado al que ha colapsado con una probabilidad de 1.

Tomando el ejemplo anterior, supongamos que $|\psi\rangle$ colapsa a $|1\rangle$. La probabilidad de que $|\psi\rangle$ haya colapsado en $|1\rangle$ es de $\frac{5}{9}$ según la explicación anterior, sin embargo, si medimos el qubit una segunda vez, es decir, después de que haya colapsado, la probabilidad de obtener otra vez el mismo estado $|1\rangle$ es 1, mientras que la probabilidad de obtener $|0\rangle$ es 0. Esto es debido a que el qubit ya ha colapsado a un estado, por lo que podemos concluir que las mediciones de los qubits afectan a su estado físico, dejando de estar en superposición e influyendo el resultado de las mediciones posteriores. Es por esto que, generalmente, vamos a realizar las mediciones de los diferentes qubits al final de un algoritmo cuántico.

4.2. Cambio de Base

Generalmente, vamos a realizar las mediciones en el eje Z, ya que los polos de este eje son los estados $|0\rangle$ y $|1\rangle$, que representan la información clásica de un bit, la cual sabemos que puede ser 0 o 1, por lo que efectivamente, toda la información clásica, o mejor dicho, todo algoritmo clásico se puede realizar mediante un algoritmo cuántico, simplemente haciendo una adaptación de puertas lógicas a puertas cuánticas como ya veremos más adelante.

Ya sabemos la razón por la que vamos a medir en la mayoría de los casos sobre el eje Z, pero como podemos apreciar en la esfera de Bloch, tenemos infinitos ejes sobre los que podríamos hacer la medición, así que la única condición para escoger dos puntos como vectores base de nuestro espacio de Hilbert $\mathcal{H}$ sobre el que estudiaremos el estado de nuestro qubit $|\psi\rangle$, es que estos puntos sean completamente opuestos. Vamos a tomar como ejemplo los estados en el eje X e Y, cuyos polos son $|+\rangle, |-\rangle$ y $|i\rangle, |-i\rangle$, respectivamente

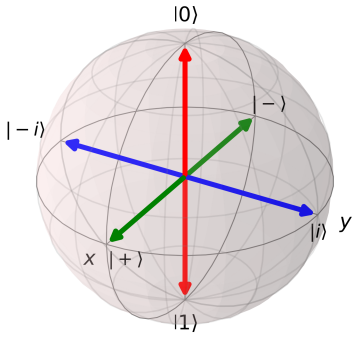


Figura 6: Estados principales de la esfera de Bloch. Obtenida de [Qiskit]

Estos estados se pueden expresar en base a $|0\rangle$ y $|1\rangle$:

$$|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \tag{4.4}$$

$$|-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \tag{4.5}$$

$$|i\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + i\,|1\rangle\right) \tag{4.6}$$

$$|-i\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - i\,|1\rangle\right) \tag{4.7}$$

Y su representación la podemos ver reflejada en (**??**). Estos estados sabemos que están en superposición ya que no se encuentran en $|0\rangle$ o $|1\rangle$, de hecho, están justamente en el punto medio entre $|0\rangle$ y $|1\rangle$, por lo que la probabilidad de obtener $|0\rangle$ o $|1\rangle$ es exactamente la misma ($\frac{1}{2}$) si nuestro qubit $|\psi\rangle$ se encuentra en uno de los estados en (**??**). No obstante, para poder realizar el cambio de base, necesitamos expresar los estados $|0\rangle$ y $|1\rangle$ en función de la base a la que queramos aplicar el cambio. Comencemos por $|+\rangle$ y $|-\rangle$:

$$|+\rangle + |-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) + \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) = \frac{2}{\sqrt{2}}\,|0\rangle = \sqrt{2}\,|0\rangle$$

$$\implies \boxed{|0\rangle = \frac{1}{\sqrt{2}}\left(|+\rangle + |-\rangle\right)} \tag{4.8}$$

$$|+\rangle - |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) - \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{2}{\sqrt{2}}|1\rangle = \sqrt{2}|1\rangle$$

$$\implies \boxed{|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)} \tag{4.9}$$

Y esto está muy relacionado con la *puerta de Hadamard*, la cual es una de las puertas cuánticas de un qubit más importantes, como veremos en la siguiente sección. Volviendo a retomar el ejemplo (**??**), vamos a aplicar el cambio a la base $B_H = \{|+\rangle, |-\rangle\}$ y ver como afecta esto al estado de nuestro qubit $|\psi\rangle$. Aplicando dicho cambio, nos queda lo siguiente

$$|\psi\rangle = \frac{1+i\sqrt{3}}{3}|0\rangle + \frac{2-i}{3}|1\rangle = \frac{1+i\sqrt{3}}{3\sqrt{2}}(|+\rangle + |-\rangle) + \frac{2-i}{3\sqrt{2}}(|+\rangle - |-$$

$$= \frac{3+\left(\sqrt{3}-1\right)i}{3\sqrt{2}}|+\rangle - \frac{1-\left(\sqrt{3}+1\right)i}{3\sqrt{2}}|-\rangle$$

Y la probabilidad de obtener $|+\rangle$ y $|-\rangle$ es

$$|+\rangle \longrightarrow \left|\frac{3+\left(\sqrt{3}-1\right)i}{3\sqrt{2}}\right|^2 = \frac{9+\left(\sqrt{3}-1\right)^2}{18} \approx 0{,}53$$

$$|-\rangle \longrightarrow \left|\frac{1-\left(\sqrt{3}+1\right)i}{3\sqrt{2}}\right|^2 = \frac{1+\left(\sqrt{3}+1\right)^2}{18} \approx 0{,}47$$

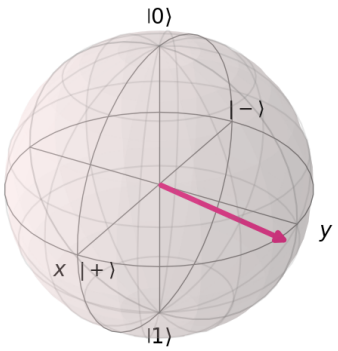


Figura 7: Cambio a la base $\{|+\rangle, |-\rangle\}$.

Podemos ver que esto tiene sentido, ya que el vector que representa el estado de $|\psi\rangle$ se encuentra ligeramente más próximo al estado $|+\rangle$ que a $|-\rangle$, por lo que es lógico obtener una probabilidad en $|+\rangle$ ligeramente mayor que en $|-\rangle$, aunque esto no quiere decir que vaya a colapsar siempre a $|+\rangle$, significa que si midiéramos varios qubits en el mismo estado que $|\psi\rangle$, por estadísitica, obtendríamos normalmente mayor número de colapsos en $|+\rangle$, aunque no siempre va a colapsar en $|+\rangle$ por tener una probabilidad mayor.

De la misma manera que en (**??**) y (**??**), podemos expresar $|0\rangle$ y $|1\rangle$ en función de $|i\rangle$ y $|-i\rangle$, obteniendo que

$$|0\rangle = \frac{1}{\sqrt{2}}(|i\rangle + |-i\rangle), \quad |1\rangle = \frac{-i}{\sqrt{2}}(|i\rangle - |-i\rangle) \tag{4.10}$$

En este caso la diferencia entre ambas probabilidades va a ser mucho mayor, ya que $|\psi\rangle$ está muy próximo a $|i\rangle$ en la esfera de Bloch, por lo que la probabilidad de obtener $|i\rangle$ será muy cercana a uno, y en caso contrario, la probabilidad de obtener $|-i\rangle$ será prácticamente nula.

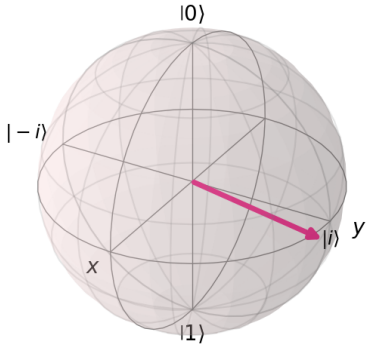


Figura 8: Cambio a la base $\{|i\rangle, |-i\rangle\}$.

$$|\psi\rangle = \frac{1+i\sqrt{3}}{3}|0\rangle + \frac{2-i}{3}|1\rangle = \frac{1+\sqrt{3}i}{3\sqrt{2}}(|i\rangle + |-i\rangle) -$$

$$-\frac{1+2i}{3\sqrt{2}}(|i\rangle - |-i\rangle) = \frac{\left(\sqrt{3}-2\right)i}{3\sqrt{2}}|i\rangle + \frac{2+\left(\sqrt{3}+2\right)i}{3\sqrt{2}}|-i\rangle$$

Y la probabilidad de obtener $|i\rangle$ y $|-i\rangle$ es

$$|i\rangle \longrightarrow \left|\frac{\left(\sqrt{3}-2\right)i}{3\sqrt{2}}\right|^2 = \frac{\left(\sqrt{3}-2\right)^2}{18} \approx 0{,}004$$

$$|-i\rangle \longrightarrow \left|\frac{2+\left(\sqrt{3}+2\right)i}{3\sqrt{2}}\right|^2 = \frac{4+\left(\sqrt{3}+2\right)^2}{18} \approx 0{,}996$$

Perfecto, vemos que el resultado es el esperado. Ahora, estamos en condiciones de explicar la fase relativa correctamente. Al final de (**??**), explicamos que una fase global no modifica el estado físico de un qubit, pero dejamos un poco abierta la fase relativa. Vamos a volver a trabajar sobre el estado de un qubit puro definido en (**??**), definiendo las probabilidades de medir $|\psi\rangle$ sobre el eje Z y posteriormente sobre el eje X, y nos vamos a dar cuenta que las probabilidades no coinciden, concluyendo en que una fase relativa sí que modifica el estado físico de un qubit, a diferencia de una fase global. Comencemos por la probabilidad de obtener $|0\rangle$ y $|1\rangle$

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

$$|0\rangle \longrightarrow \left|\cos\left(\frac{\theta}{2}\right)\right|^2 = \cos^2\left(\frac{\theta}{2}\right)$$

$$|1\rangle \longrightarrow \left|e^{i\varphi}\sin\left(\frac{\theta}{2}\right)\right|^2 = \left(\cos\left(\frac{\theta}{2}\right) + i\sin\left(\frac{\theta}{2}\right)\right)\left(\cos\left(\frac{\theta}{2}\right) - i\sin\left(\frac{\theta}{2}\right)\right)\sin^2\left(\frac{\theta}{2}\right) = \sin^2\left(\frac{\theta}{2}\right)$$

Ahora, haciendo el cambio de base a $\{|0\rangle, |1\rangle\}$

$$|\psi\rangle = \frac{1}{\sqrt{2}}\cos\left(\frac{\theta}{2}\right)(|+\rangle + |-\rangle) + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}e^{i\varphi}\sin\left(\frac{\theta}{2}\right)(|+\rangle - |-\rangle) =$$

$$= \left[\frac{1}{\sqrt{2}}\cos\left(\frac{\theta}{2}\right) + \frac{1}{\sqrt{2}}e^{i\varphi}\sin\left(\frac{\theta}{2}\right)\right]|+\rangle + \left[\frac{1}{\sqrt{2}}\cos\left(\frac{\theta}{2}\right) - \frac{1}{\sqrt{2}}e^{i\varphi}\sin\left(\frac{\theta}{2}\right)\right]|-\rangle$$

Vemos que las probabilidades no son las mismas que con la base anterior:

$$|+\rangle \longrightarrow \left|\frac{1}{\sqrt{2}}\cos\left(\frac{\theta}{2}\right)+\frac{1}{\sqrt{2}}e^{i\varphi}\sin\left(\frac{\theta}{2}\right)\right|^2=\frac{1}{2}\left[\cos\left(\frac{\theta}{2}\right)+\sin\left(\frac{\theta}{2}\right)\right]^2$$

$$|-\rangle \longrightarrow \left|\frac{1}{\sqrt{2}}\cos\left(\frac{\theta}{2}\right)-\frac{1}{\sqrt{2}}e^{i\varphi}\sin\left(\frac{\theta}{2}\right)\right|^2=\frac{1}{2}\left[\cos\left(\frac{\theta}{2}\right)-\sin\left(\frac{\theta}{2}\right)\right]^2$$

Por lo que hemos comprobado que una fase relativa no altera el estado de un qubit $|\psi\rangle$ en el eje Z, sino que lo hace en el plano azimutal, de manera que al medir el estado de $|\psi\rangle$ en otra base como $\{|+\rangle, |-\rangle\}$, la probabilidad de colapso cambia. Esto no sucede cuando aplicamos una fase global.

4.3. Puertas Cuánticas

Habiendo introducido la unidad de información cuántica y sus respectivas mediciones sobre los ejes X, Y y Z, estamos ya en condiciones de estudiar las puertas cuánticas. Así como las puertas lógicas en computación clásica son capaces de modificar la información que reside en los distintos bits, las puertas cuánticas actúan sobre el estado físico de los respectivos qubits, siguiendo las leyes de la mecánica cuántica como hemos visto hasta ahora, de manera que se consigue modificar el estado de un qubit $|\psi\rangle$ como resultado de una operación, por ejemplo, desencriptar las claves públicas y privadas de un cifrado de información, como veremos más adelante.

Estas puertas cuánticas, las podemos representar como matrices, aprovechando todo el álgebra lineal que llevamos impartido hasta ahora. Realmente, pudimos haber representado el estado de un qubit $|\psi\rangle$ en la sección anterior como un vector columna, aprovechando la representación matricial de $|0\rangle$ y $|1\rangle$ que sigue como

$$|0\rangle=\begin{pmatrix}1\\0\end{pmatrix}, \quad |1\rangle=\begin{pmatrix}0\\1\end{pmatrix} \tag{4.11}$$

Si tomamos el estado de un qubit puro que definimos en (**??**), vemos que podemos definir el estado de un qubit cualquiera $|\psi\rangle$ como un vector columna de dimensión 2^N, siendo N el número de qubits de nuestro computador cuántico, por lo que para un sistema cuántico de un único qubit tenemos el siguiente vector:

$$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle=\alpha\begin{pmatrix}1\\0\end{pmatrix}+\beta\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}\alpha\\\beta\end{pmatrix} \tag{4.12}$$

De esta manera, podemos expresar el estado de cualquier qubit como un vector columna de dimensión 2, y ya veremos la generalización de esta representación vectorial para N qubits en la siguiente

sección (**??**). Por otra parte, vamos ya a afrontar las puertas cuánticas, las cuales no son más que operadores sobre un espacio de Hilbert $\mathcal{H}$ que transforman el estado de un qubit en otro estado diferente, como vimos en (**??**):

$$\hat{A}\left|\psi\right\rangle \xrightarrow{\hat{A}} \left|\psi'\right\rangle, \qquad \left|\psi\right\rangle, \left|\psi'\right\rangle \in \mathcal{H}$$

Para estos operadores ser bautizados como puertas cuánticas, han de satisfacer unas ciertas condiciones. La primera es la condición de linealidad, la cual establece que

$$U\left(\alpha\left|0\right\rangle + \beta\left|1\right\rangle\right) = \alpha U\left|0\right\rangle + \beta U\left|1\right\rangle \tag{4.13}$$

La segunda es que la probabilidad total de los estados a obtener en una medición ha de seguir manteniéndose uno, como vimos en el capítulo anterior en (**??**)

$$|\alpha|^2 + |\beta|^2 = 1$$

Para ver qué tipo de matrices satisfacen esta propiedad, vamos a apoyarnos en el conjugado hermítico. Sea la siguiente puerta cuántica U:

$$U = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

Si la aplicamos sobre un qubit $|\psi\rangle$, nos queda como resultado un qubit diferente, el cual denotaremos como $|U\psi\rangle$

$$U\left|\psi\right\rangle = \begin{pmatrix} a & c \\ b & d \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} a\alpha + c\beta \\ b\alpha + d\beta \end{pmatrix} = \left|U\psi\right\rangle \tag{4.14}$$

Si ahora consideramos el conjugado hermítico de $|U\psi\rangle$, el cual definimos en la introducción de los espacios de Hilbert $\mathcal{H}$ en (**??**), tenemos que

$$\begin{aligned}\left\langle U\psi\right| &= \begin{pmatrix} a^*\alpha^* + c^*\beta^* & b^*\alpha^* + d^*\beta^* \end{pmatrix} = \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix}\begin{pmatrix} a^* & d^* \\ c^* & d^* \end{pmatrix} = \\ &= \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix}\begin{pmatrix} a & c \\ b & d \end{pmatrix}^\dagger = \left\langle\psi\right| U^\dagger\end{aligned} \tag{4.15}$$

Entonces, apoyándonos en las propiedades que acabamos de ver (**??**) y (**??**), obtenemos finalmente la segunda condición que estamos buscando. Esto lo hacemos viendo que el producto escalar de

$|U\psi\rangle$ sobre sí mismo, es decir, la proyección de $|U\psi\rangle$ sobre sí mismo, es igual a 1:

$$\langle U\psi \mid U\psi\rangle = 1$$

$$\langle\psi|U^\dagger U|\psi\rangle = \langle\psi \mid \psi\rangle$$

$$U^\dagger U = I \tag{4.16}$$

Y las matrices que satisfacen esta última propiedad (**??**) se conocen como *unitarias*, y podemos afirmar algo muy importante, y es que toda matriz unitaria es una puerta cuántica, y toda puerta cuántica es una matriz unitaria. Además, como hemos podido ver en (**??**), $U^\dagger$ es la matriz inversa de U, ya que el producto de estas dos matrices da como resultado la matriz identidad I, por lo que toda puerta cuántica U es reversible, y su matriz inversa es su conjugado hermítico $U^\dagger$, de manera que si aplicamos una puerta cuántica U sobre un qubit $|\psi\rangle$, podemos volver al estado original de $|\psi\rangle$ aplicando $U^\dagger$

$$U^\dagger U\,|\psi\rangle = UU^\dagger\,|\psi\rangle = I\,|\psi\rangle = |\psi\rangle$$

Esta última condición tiene mucho que ver con que las puertas cuánticas tienen que ser reversibles, es decir, siempre hemos de saber de que estado proviene el resultado. Para ver esto mejor, vamos a apoyarnos en las puertas lógicas clásicas, en este caso la puerta *NOT*, cuya tabla de verdad es

A	B
0	1
1	0

Cuadro 1: Puerta lógica NOT.

Si obtenemos el resultado $B = 1$, sabemos que el bit antes de aplicar la puerta era 0, y si obtenemos $B = 0$, no queda otra opción que el bit fuese 1, esto lo podemos representar como una matriz:

$$\left.\begin{array}{l}|0\rangle \to 1\\ |1\rangle \to 0\end{array}\right\} \quad \text{NOT} = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$

Y esta matriz vemos que es unitaria, ya que su matriz conjugada transpuesta por ella misma es la identidad I

$$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}^\dagger = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = I$$

Por lo que la puerta clásica *NOT* es una puerta cuántica perfectamente válida, la cual explicaremos en el siguiente apartado. Para ver el caso contrario, vamos a suponer la puerta clásica cuyo resultado es siempre 1:
Y podemos verificar que la matriz que representa a esta puerta no es unitaria

A	B
0	1
1	1

Cuadro 2: Puerta lógica clásica constante a 1.

$$\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}^{\dagger} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \neq I$$

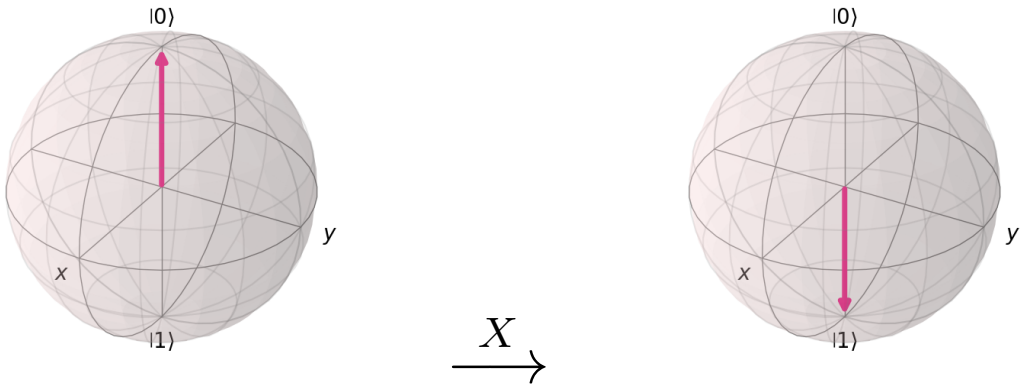
Por lo que la puerta (**??**) no es una puerta cuántica. Este pequeño nos ayuda a entender mejor que toda puerta lógica clásica reversible tiene su contrapartida en computación cuántica, y el significado físico de estas puertas cuánticas lo vamos a ver a continuación con las puertas cuánticas de 1 qubit más importantes.

4.4. Puertas Cuánticas de 1 Qubit

Una vez explicadas las condiciones que ha de cumplir una puerta cuántica, que son la condición de linealidad (**??**) y que ha de ser unitaria, como vimos en (**??**), vamos a tomar como ejemplo la puerta *NOT* clásica, que tiene su contrapartida cuántica, la cual se suele denotar como *X*, ya que cumple con los requisitos propuestos anteriormente, de manera que un qubit en el estado $|0\rangle$ pasa a $|1\rangle$ y viceversa:

$$X|\psi\rangle = \alpha X|0\rangle + \beta X|1\rangle = \alpha \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \alpha \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \beta \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \beta|0\rangle + \alpha|1\rangle$$

De esta manera, si aplicamos la puerta *X* sobre un qubit $|\psi\rangle$ que se encuentra en el estado $|0\rangle$, esta puerta rota el estado del qubit $|\psi\rangle$ al estado $|1\rangle$



(a) Estado $|0\rangle$ en la esfera de Bloch.

(b) Estado $|1\rangle$ en la esfera de Bloch.

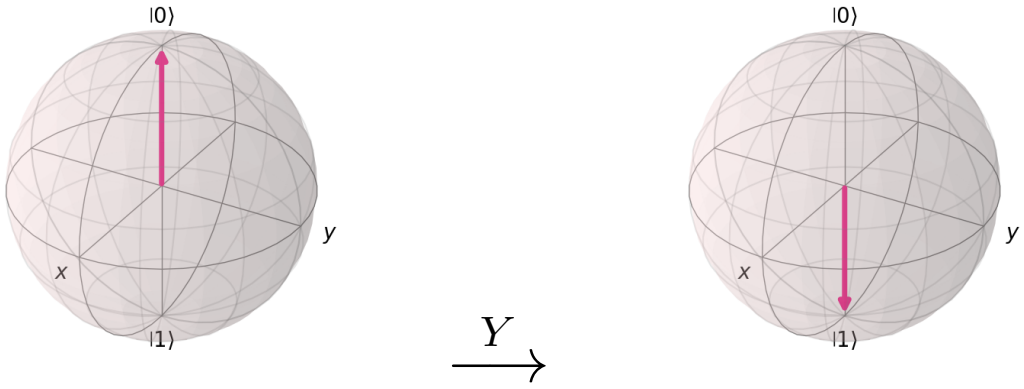
Y esto ocurre también para el caso contrario. Esta puerta *X* es una de las *puertas de Pauli*, en concreto sobre el eje X, como su propio nombre indica, y también podemos definir las puertas de Pauli para el eje *Y* y *Z* de la esfera de Bloch, de la siguiente manera

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{4.17}$$

Estas *puertas de Pauli*, y de hecho, toda puerta cuántica de un único qubit representa una rotación de $|\psi\rangle$ en la esfera de Bloch, esto es lógico ya que, como vimos anteriormente, toda puerta cuántica es un operador lineal que actúa sobre un qubit $|\psi\rangle$, de manera que cambiamos el estado de dicho qubit $|\psi\rangle$ a otro estado diferente $|\psi'\rangle$, cuya norma sigue siendo la unidad, por lo que podemos visualizar muy bien la rotación en la esfera de Bloch. Así, las puertas de Pauli que acabamos de ver en (**??**) son rotaciones de π radianes sobre uno de los ejes de la esfera de Bloch. Veamos como actúa *Y* sobre $|0\rangle$:

$$Y|\psi\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ i \end{pmatrix} = i \begin{pmatrix} 0 \\ 1 \end{pmatrix} = i|1\rangle$$

Y esto es el estado $|1\rangle$ multiplicado por una fase global, en este caso i, por lo que podemos eliminar la fase global, ya que esta no altera el significado físico de $|1\rangle$, dándose por realizada la rotación esperada sobre el eje *Y*



Vamos a tomar como último ejemplo la puerta *Z*, de manera que si la aplicamos sobre un qubit en $|0\rangle$ el estado del qubit no cambia, ya que estamos aplicando una rotación sobre el eje *Z*:

$$Z|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

Como habíamos presupuesto anteriormente. A partir de estas puertas podemos crear todas las demás puertas cuánticas de 1 qubit. Vamos definir una puerta muy importante, la cual es una rotación sobre el eje $X + Z$, que la podemos obtener únicamente sumando las puertas de Pauli *X* y *Z*

$$X + Z = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Pero si nos fijamos esta matriz no es unitaria, ya que

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{\dagger} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = 2\, I \neq I$$

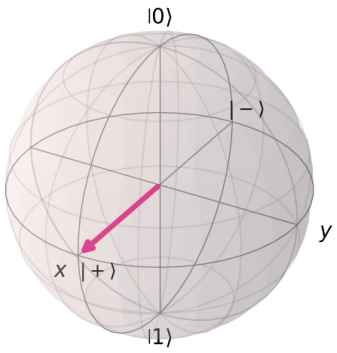
Para que sea unitaria hemos de multiplicar la matriz por $\frac{1}{\sqrt{2}}$, obteniendo así una nueva puerta cuántica, la cual suele representarse con H:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{4.18}$$

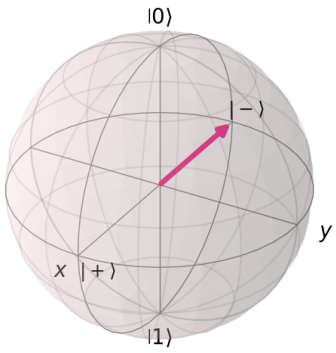
Esta es la *puerta de Hadamard H*, y es una de las puertas más importantes en computación cuántica porque nos permite colocar el estado de cualquier qubit $|\psi\rangle$ en superposición, por lo que no es de extrañar que esta puerta H se use en la gran mayoría de algoritmos cuánticos como veremos en (**??**), permitiendo así aprovechar las propiedades de la mecánica cuántica al asegurarnos por completo que el qubit $|H\psi\rangle$ se encuentra en superposición cuántica. Esto es debido a que si aplicamos la puerta H sobre $|0\rangle$ obtenemos el estado $|+\rangle$, y si la aplicamos sobre $|1\rangle$ obtenemos $|-\rangle$

$$H\,|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \left(|+\rangle + |-\rangle\right)$$

$$H\,|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} - \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \left(|+\rangle - |-\rangle\right)$$



(a) Estado $|+\rangle$ en la esfera de Bloch



(b) Estado $|-\rangle$ en la esfera de Bloch

Esto lo vimos en (**??**) cuando definimos los estados $|+\rangle$ y $|-\rangle$, y ahora hemos demostrado de donde salen. Estas son las puertas cuánticas de 1 qubit que principalmente vamos a usar, de manera que si aparece alguna otra puerta simple de 1 qubit la definiremos más adelante conforme nos vayan saliendo. Con esto damos por terminada esta sección y damos paso a la siguiente, en la que discutiremos qué sucede cuando tenemos más de 1 qubit…

CAPÍTULO

5

Múltiples Qubits

En esta sección, vamos a ver que se siguen las mismas reglas cuando tenemos más de un qubit que a la hora de tener solo uno, como vimos en la sección pasada (**??**). En este caso ya no estamos hablando de un qubit y por lo tanto, no nos encontramos en un espacio de Hilbert de dos dimensiones, sino que vamos a lograr generalizar las expresiones vistas en la sección anterior (**??**) para N qubits, llegando a las mismas expresiones que vimos en el espacio de Hilbert (**??**), y en este caso al tratarse de N qubits, tendríamos un espacio de Hilbert de 2^N dimensiones.

Para una mejor explicación, vamos a comenzar por un espacio de Hilbert de cuatro dimensiones, es decir, un sistema cuántico de dos qubits. Los estados de este sistema se pueden representar como

$$|00\rangle = |0\rangle \otimes |0\rangle = |0\rangle\,|0\rangle \tag{5.1}$$

Entonces, el resto de estados los podemos conseguir de la misma manera que sumamos números binarios, obteniendo que la base Z está formada por los siguientes estados

$$Z = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$$

De manera que el estado de un qubit de carácter genérico es una superposición de estados en el eje Z

$$|\psi\rangle = c_0\,|00\rangle + c_1\,|01\rangle + c_2\,|10\rangle + c_3\,|11\rangle \tag{5.2}$$

Y las probabilidades de obtener los distintos estados $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ al medir sobre el eje Z son $|c_0|^2$, $|c_1|^2$, $|c_2|^2$ y $|c_3|^2$, respectivamente. Hasta aquí no hay nada nuevo, pero ¿Qué sucede cuando queremos dar el paso a N qubits? Para esto necesitamos pasar los distintos estados de la base Z de binario a decimal. Suponiendo que los estados del eje Z se encuentran en la base binaria

$$|b_{N-1}\ \cdots\ b_2\ b_1\ b_0\rangle, \qquad \forall\, b_n \in \{0,1\}$$

Podemos realizar la conversión a decimal como sigue

$$|b_{N-1}\ \cdots\ b_2\ b_1\ b_0\rangle = |2^{N-1}b_{N-1} + \cdots + 2^2 b_2 + 2^1 b_1 + 2^0 b_0\rangle \tag{5.3}$$

Y esta notación nos permite desarrollar el estado en superposición de un qubit $|\psi\rangle$ que vimos en (**??**) cuando teníamos dos qubits, pero ahora teniendo N qubits

$$|\psi\rangle = \sum_{j=0}^{N-1} c_j\,|j\rangle = c_0\,|0\rangle + c_1\,|1\rangle + c_2\,|2\rangle + \cdots + c_{N-1}\,|N-1\rangle\,, \qquad j \in \mathbb{N} \tag{5.4}$$

Esta expresión nos resulta muy familiar, y es que ya la definimos anteriormente en (**??**) cuando tratábamos los espacios de Hilbert (**??**), por lo que todo encaja muy bien y nos indica que vamos por buen camino.

A continuación vamos a ver como es la representacón matricial de estos estados, y esto se hace con el denominado *producto de Kronecker*, el cual no vamos a definir formalmente, sino que vamos a ver directamente como funciona, por ejemplo, para el estado $|00\rangle$ en un sistema de dos qubits:

$$|00\rangle = |0\rangle\,|0\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\begin{pmatrix}1\\0\end{pmatrix}\\0\begin{pmatrix}1\\0\end{pmatrix}\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \tag{5.5}$$

Si esto lo aplicamos para el resto de estados que definen el eje Z en un sistema cuántico de dos qubits, obtenemos que

$$|00\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \quad |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, \quad |10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, \quad |11\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix} \tag{5.6}$$

De manera que podemos expresar el estado de un sistema cuántico de dos qubits mediante un vector columna como vimos en (**??**), ampliando la expresión para dos qubits y aplicando lo que acabamos de ver

$$|\psi\rangle = c_0\,|00\rangle + c_1\,|01\rangle + c_2\,|10\rangle + c_3\,|11\rangle = \begin{pmatrix}c_0\\c_1\\c_2\\c_3\end{pmatrix} \tag{5.7}$$

Entonces, podemos representar la expresión (**??**) como un vector columna de dimension N, siendo N el número de qubits de nuestro sistema cuántico:

$$|\psi\rangle = \sum_{j=0}^{N-1} c_j |j\rangle = c_0 |0\rangle + c_1 |1\rangle + c_2 |2\rangle + \cdots + c_{N-1} |N-1\rangle = \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{N-1} \end{pmatrix} \tag{5.8}$$

Toda esta notación funciona exactamente igual para los bra, como por ejemplo $\langle 00|$:

$$\langle 00| = \langle 0| \otimes \langle 0| = \begin{pmatrix} 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 \begin{pmatrix} 1 & 0 \end{pmatrix} & 0 \begin{pmatrix} 1 & 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}$$

Entonces, de la misma manera que acabamos de ver en (**??**) un ket generalizado para N qubits, ahora tenemos un bra generalizado para N qubits:

$$\langle \psi| = \sum_{j=0}^{N-1} c_j^* \langle j| = c_0^* \langle 0| + c_1^* \langle 1| + c_2^* \langle 2| + \cdots + c_{N-1}^* \langle N-1| = \begin{pmatrix} c_0^* & c_1^* & c_2^* & \cdots & c_{N-1}^* \end{pmatrix} \tag{5.9}$$

5.1. Puertas Cuánticas de Múltiples Qubits

De la misma manera que vimos en las puertas cuánticas de un único qubit, las puertas cuánticas aplicadas a más de un qubit siguen siendo transformaciones del estado del qubit $|\psi\rangle$ en otro $|\psi'\rangle$, solo que ahora al tener más de una unidad de información cuántica no son rotaciones en la esfera de Bloch, y esto es porque no se pueda representar algo que esté más allá de las tres dimensiones, como vimos anteriormente en los estados de Z que eran vectores columna de cuatro elementos.

Vamos a comenzar creando algunas puertas de dos qubits. Aunque esto suene tedioso, es algo bastante sencillo si tenemos en cuenta lo que hemos visto anteriormente para puertas de un qubit en (**??**), con la idea de que podemos aplicar cualquiera de estas transformaciones a los distintos qubits de $|\psi\rangle$. Tomemos como ejemplo la puerta de Hadamard *H* y la *NOT* para un qubit, podemos aplicarlas a los distintos qubits de $|\psi\rangle$, los cuales vamos a suponer que se encuentran en $|00\rangle$

$$(H \otimes X) |\psi\rangle = (H \otimes X) |00\rangle = (H \otimes X) |0\rangle \otimes |0\rangle = H |0\rangle \otimes X |0\rangle = |+\rangle \otimes |1\rangle =$$
$$= \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes |1\rangle = \frac{1}{\sqrt{2}} (|0\rangle \otimes |1\rangle + |1\rangle \otimes |1\rangle) = \frac{1}{\sqrt{2}} (|01\rangle + |11\rangle)$$

Y de esta manera podemos ver perfectamente que se ha aplicado una puerta *H* al qubit en la izquierda y una puerta *X* al qubit de la derecha. Este resultado también lo podemos obtener matricialmente ya

que $\otimes$ es el producto de Kronecker. Vamos a definir primero la matriz que representa esta puerta cuántica

$$H \otimes X = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & 1 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ 1 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & -1 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix}$$

Vemos que esta matriz es unitaria, por lo que se verifica que es una puerta cuántica perfectamente válida. Entonces, si multiplicamos esta matriz por el estado $|00\rangle$ de $|\psi\rangle$ obtenemos, como debería de ser, el mismo resultado

$$(H \otimes X)\,|00\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \left(|01\rangle + |11\rangle\right)$$

Y así podemos crear nuestras propias puertas cuánticas a nuestro gusto, según nuestras propias necesidades, asegurándonos siempre que sean puertas válidas. Volveremos a este ejemplo más adelante, ya que como veremos, aplicar puertas cuánticas simples de un qubit a un estado con múltiples qubits no puede crear el famoso entrelazamiento cuántico, el cual explicaremos detenidamente en (**??**). Sin embargo, podemos tener puertas cuánticas que cambien directamente el estado de dos qubits al mismo tiempo, al contrario de las puertas que hemos visto hasta ahora, y estas son de vital importancia ya que sí permiten crear entrelazamiento.

5.1.1. La Puerta CNOT

Vamos a ver únicamente dos ejemplos de puertas cuánticas que actúan directamente sobre más de un qubit ya que estas son las más importantes. No obstante, de la misma manera que para las puertas de un único qubit, si en algún otro momento necesitamos definir más puertas cuánticas con algún fin, las definiremos sin problema. Dicho esto, la primera puerta es la famosa *CNOT* (o *controlled-NOT*), la cual actúa sobre un estado de dos qubits como sigue

$$\begin{aligned} \textit{CNOT}\,|00\rangle &= |00\rangle \\ \textit{CNOT}\,|01\rangle &= |01\rangle \\ \textit{CNOT}\,|10\rangle &= |11\rangle \\ \textit{CNOT}\,|11\rangle &= |10\rangle \end{aligned}$$

Podemos ver que en efecto esta puerta es una puerta *NOT* con un qubit de control, de ahí su nombre *CNOT*. Por defecto el qubit de control es el izquierdo, de manera que si dicho qubit es $|0\rangle$, el estado permanece igual tras aplicar la puerta. Sin embargo si el qubit de control es $|1\rangle$, se aplica una puerta *NOT* sobre el qubit derecho, de manera que se invierte el estado del qubit. La representación matricial de esta puerta es muy sencilla, ya que al aplicar esta puerta a los estados $|00\rangle$ y $|01\rangle$ estos permanecen igual, y si la aplicamos sobre $|10\rangle$ obtenemos 11 y viceversa. Esto se traduce en que la última y penúltima columna de la matriz identidad I están cambiadas, obteniendo la matriz de la puerta *CNOT*

$$\textit{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{5.10}$$

Y esta puerta tiene su representación en un circuito cuántico, la cual es la siguiente

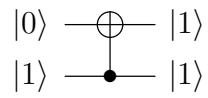


Figura 12: Puerta *CNOT* en un circuito cuántico

De manera que hemos indicado q_1 como el qubit de control y q_0 como el resultado de aplicar la puerta *NOT* en los casos que corresponda. También puede darse un segundo caso cuando ambos qubits están intercambiados, por lo que q_0 sería el qubit de control en este caso. Esto en un circuito cuántico no tiene mayor complejidad que intercambiar q_0 con q_1

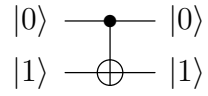


Figura 13: Puerta $\textit{CNOT}_{01}$ en un circuito cuántico

Y esto se denota como $\textit{CNOT}_{01}$, cuya representación matricial lógicamente cambia:

$$\textit{CNOT}_{01} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \tag{5.11}$$

Actuando sobre los estados de dos qubits como sigue

$$\textit{CNOT}_{01}\,|00\rangle = |00\rangle$$
$$\textit{CNOT}_{01}\,|01\rangle = |11\rangle$$
$$\textit{CNOT}_{01}\,|10\rangle = |10\rangle$$
$$\textit{CNOT}_{01}\,|11\rangle = |01\rangle$$

Esta es una de las puertas más importantes que vamos a ver ya que permite entrelazar dos qubits. De momento, vamos a definir informalmente el entrelazamiento como una conexión que se establece entre ambos, de manera que si el estado de uno de los qubits cambia, también se verá afectado el estado del otro qubit entrelazado. Esto se traduce como que el estado de ambos qubits dependen el uno con el otro, y será el principio fundamental para enviar información cuántica. Todo esto ya lo veremos mucho más detenidamente en (**??**), pero ahora vamos a continuar con la segunda puerta cuántica de múltiples qubits que vamos a ver.

5.1.2. La Puerta de Toffoli

Esta puerta es muy similar a la *CNOT* que acabamos de ver, con la diferencia de que esta puerta actúa sobre tres qubits, siendo dos qubits de control. Esto quiere decir que solo se aplica una puerta *NOT* sobre el qubit que no es de control en el caso que estos sean ambos $|1\rangle$, lo que se suele definir como:

$$\text{Toffoli}\,|a\rangle\,|b\rangle\,|c\rangle = |a\rangle\,|b\rangle\,|ab \oplus c\rangle$$

Al actuar sobre tres qubits, la matriz que representa esta puerta es una matriz cuadrada de dimensión 2^3, lo que resulta en una matriz con ocho filas y columnas:

$$\text{Toffoli} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \tag{5.12}$$

Que se puede comprobar que cumple con las condiciones para ser una puerta cuántica, como vimos en (**??**). En un circuito cuántico esto se representa simplemente añadiendo un tercer qubit de control a una puerta *CNOT*

Este resultado lo verificar operando directamente con matrices como sigue

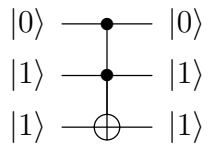
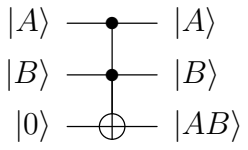


Figura 14: Caso de ejemplo de la puerta de Toffoli

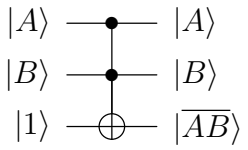
$$\text{Toffoli}\,|011\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |011\rangle$$

Y vemos que se corresponde a lo previamente explicado. Sin embargo, esto no es todo. Dependiendo del resultado que queramos obtener, vamos a establecer el qubit objetivo (aquel que no es de control) como $|0\rangle$ o $|1\rangle$ según la operación que corresponda. Esto es debido a que en la puerta de Toffoli se encuentran intrínsecas muchas de las operaciones que utilizan los ordenadores convencionales, por no decir todas y cada una de ellas.

Para ver esto mejor, vamos a definir los qubits de control como A y B para introducir un caso genérico, y vamos a analizar el comportamiento de esta puerta, que depende del qubit objetivo, que puede ser $|0\rangle$ o $|1\rangle$ como hemos mencionado anteriormente



(a) Puerta AND cuántica



(b) Puerta NAND cuántica

Figura 15: Puerta de Toffoli

Estas son, en efecto, las puertas *AND* y *NAND* de la computación clásica. Sin quitarle importancia a la puerta *AND*, la puerta *NAND* tiene una pequeña particularidad, y es que con el conjunto de puertas *NAND* podemos obtener todo el resto de puertas lógicas, y por lo tanto, podríamos obtener un ordenador clásico que utilice únicamente esta puerta. Esto se conoce como un conjunto universal de puertas lógicas, ya que a partir de este conjunto (aunque sea una sola puerta) podemos obtener las demás.

Vamos a ver que esto es realmente así con algunos ejemplos. En la práctica, para que un conjunto sea universal, tenemos que ser capaces de expresar cada puerta lógica (*AND*, *NOT*, *XOR*) mediante

puertas que estén dentro del conjunto universal. Para esto vamos a apoyarnos en el *Álgebra de Boole*, el cual nos va a ayudar a explicar el funcionamiento de las puertas lógicas a través de operaciones booleanas. Comencemos por la puerta *NOT*, la cual se representa como $\overline{A}$

$$\overline{A} = \overline{AA}$$

Este resultado es muy intuitivo ya que si tenemos un bit A, el cual puede ser 0 o 1, el resultado de multiplicar A consigo mismo, es decir, aplicar una puerta *AND*, siempre va a ser igual a A ya que $A = AA$. El segundo caso va ser la puerta *AND*, la cual podemos expresar en términos de varias *NAND* como sigue

$$AB = \overline{\overline{AB} \cdot \overline{AB}}$$

Este caso puede parecer menos intuitivo que el anterior, pero sigue siendo muy sencillo. Si aplicamos dos puertas *NOT* sobre un bit A obtenemos el mismo bit, $A = \overline{\overline{A}}$, entonces, aplicando también el principio anterior obtenemos que $\overline{\overline{AB} \cdot \overline{AB}} = \overline{\overline{AB}} = AB$, como queríamos demostrar. El último caso que vamos a ver va a ser la puerta *OR* de la computación clásica

$$A + B = \overline{\overline{AA} \cdot \overline{BB}}$$

La cual vemos que también está compuesta por varias puertas *NAND*. Esto lo hemos logrado aplicando la primera demostración, $\overline{A} = \overline{AA}$, y posteriormente una de las famosas *Leyes de De Morgan*, la cual establece que $A + B = \overline{\overline{A} \cdot \overline{B}}$. Estos son únicamente algunos de los ejemplos que se han decidido incluir para darnos cuenta que podemos expresar cualquier puerta clásica a partir de puertas de Toffoli, las cuales son la contrapartida cuántica de la puerta *NAND* que forma un conjunto universal, verificando así que toda información clásica puede ser también descrita mediante un ordenador cuántico.

Sin embargo, no vamos a utilizar únicamente puertas de Toffoli para describir información clásica. Esto lo hemos hecho para demostrar la hipótesis anterior, pero en la realidad no se usan únicamente puertas de Toffoli, ya que nos interesa tener el mínimo de puertas lógicas en un algoritmo o proceso cuántico, para reducir su complejidad al mínimo y mejorar al máximo su rendimiento. Tomando como ejemplo uno de los vistos anteriormente, podemos expresar una puerta *AND* clásica utilizando tres puertas de Toffoli con el qubit objetivo en $|1\rangle$. Sin embargo, nos interesa mucho más expresar dicha puerta mediante una única puerta de Toffoli, esta vez con el qubit objetivo en $|0\rangle$, de manera que hemos utilizado una única puerta cuántica en lugar de tres, minimizando el número de puertas como acabamos de explicar.

Con esto damos paso a la siguiente sección, en la que trataremos el entrelazamiento cuántico, el cual es uno de los pilares fundamentales de la computación cuántica y puede crearse a partir de puertas cuánticas que actúan sobre múltiples qubits a la vez, como la *CNOT* vista anteriormente en (**??**).

CAPÍTULO

6

Entrelazamiento Cuántico

En esta sección vamos a introducirnos mucho más detalladamente en el *entrelazamiento cuántico*, el cual es uno de los fenómenos más importantes de esta revolución cuántica. Ya dimos al definir la puerta *CNOT* en (**??**) una definición muy informal de entrelazamiento cuántico, en la que decíamos que si tenemos dos qubits entrelazados entre sí, un cambio en el estado de uno de ellos afectaba al otro y viceversa. Esto es una propiedad muy potente, ya que nos permite enviar información cuántica, lo cual veremos al final de este capítulo, o en el ámbito de la criptografía generar claves que sean indescifrables, además de otras muchas explotaciones que podemos conseguir con este fenómeno. Para entender mucho mejor esto, vamos a partir de un estado de dos qubits como ya vimos en (**??**)

$$|\psi\rangle = c_0 |00\rangle + c_1 |01\rangle + c_2 |10\rangle + c_3 |11\rangle$$

Ya vimos que la probabilidad de obtener $|00\rangle$ en la medición de $|\psi\rangle$ es $|c_0|^2$, midiendo $|01\rangle$ sería $|c_1|^2$, y así sucesivamente, siendo la suma del módulo cuadrado de estos coeficientes igual a la unidad. Ahora viene lo nuevo, y es que podemos medir uno de los qubits de $|\psi\rangle$ individualmente. Si medimos por ejemplo el qubit izquierdo, obtendremos los estados $|0\rangle$ o $|1\rangle$ con una cierta probabilidad, las cuales son, en el caso de obtener $|0\rangle$

$$|c_0|^2 + |c_1|^2$$

En definitiva, la probabilidad de obtener $|0\rangle$ es igual a la suma del módulo cuadrado de los coeficientes que tienen el qubit que estamos midiendo en $|0\rangle$. Esto se aplica de la misma manera si medimos $|1\rangle$, siendo la probabilidad de

$$|c_2|^2 + |c_3|^2$$

Pero ahora nos puede surgir una duda, ¿A qué estado colapsa $|\psi\rangle$? Simplemente colapsa a la superposición de estados cuyo qubit izquierdo es $|0\rangle$. En nuestro caso, si al medir el qubit de la

izquierda este ha colpasado a $|0\rangle$, nos quedamos con los estados cuyo qubit izquierdo es $|0\rangle$ y sus respectivos coeficientes, por lo que obtendríamos

$$|\psi\rangle = A\left(c_0\,|00\rangle + c_1\,|01\rangle\right)$$

Siendo *A* una constante de normalización, para que el producto escalar de $|\psi\rangle$ consigo mismo sea la unidad $\langle\psi \mid \psi\rangle = 1$, como debería de ser. Esto aplica de igual manera en el caso de obtener $|1\rangle$ como resultado de la medición, colapsando $|\psi\rangle$ en

$$|\psi\rangle = B\left(c_2\,|10\rangle + c_3\,|11\rangle\right)$$

Calculando estas constantes, obtenemos ambos estados normalizados

$$\frac{c_0\,|00\rangle + c_1\,|01\rangle}{\sqrt{|c_0|^2 + |c_1|^2}}, \qquad \frac{c_2\,|10\rangle + c_3\,|11\rangle}{\sqrt{|c_2|^2 + |c_3|^2}} \tag{6.1}$$

Pero, ¿Qué ocurre si vamos un paso más allá? Efectivamente, ahora vamos a medir el qubit derecho, partiendo de uno de los estados que acabamos de ver en (**??**), demostrando así que podemos medir los qubits secuencialmente, uno después del otro, y esto se puede aplicar para un sistema de *N* qubits, pero de momento vamos a seguir con nuestro ejemplo de dos qubits para simplificar cálculos.

Vamos a demostrar que si ahora medimos $|\psi\rangle$, obtenemos las mismas probabilidades de colapsar en $|00\rangle$, $|01\rangle$, $|10\rangle$ o $|11\rangle$. Hemos de tener en cuenta para este cálculo que primero hemos obtenido un estado con una cierta probabilidad, por lo que la probabilidad total será el producto de la probabilidad de haber obtenido la primera medición por la segunda, quedando

$$|00\rangle \to \left(|c_0|^2 + |c_1|^2\right) \frac{|c_0|^2}{\left(\sqrt{|c_0|^2 + |c_1|^2}\right)^2} = |c_0|^2$$

$$|01\rangle \to \left(|c_0|^2 + |c_1|^2\right) \frac{|c_1|^2}{\left(\sqrt{|c_0|^2 + |c_1|^2}\right)^2} = |c_1|^2$$

$$|10\rangle \to \left(|c_2|^2 + |c_3|^2\right) \frac{|c_2|^2}{\left(\sqrt{|c_2|^2 + |c_3|^2}\right)^2} = |c_2|^2$$

$$|11\rangle \to \left(|c_2|^2 + |c_3|^2\right) \frac{|c_3|^2}{\left(\sqrt{|c_2|^2 + |c_3|^2}\right)^2} = |c_3|^2$$

Y vemos que en efecto estas son las probabilidades iniciales, por lo que acabamos de demostrar que medir el estado de una partícula $|\psi\rangle$ es lo mismo que medir cada uno de sus qubits secuencialmente,

o al menos eso es lo que parece. Esto generalmente es cierto para cualquier $|\psi\rangle$ siempre y cuando sus qubits no estén entrelazados, ya que si realmente lo están, esto cambia completamente. Supongamos el siguiente estado

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

La probabilidad de obtener $|0\rangle$ o $|1\rangle$ en la medición del primer qubit es de $\frac{1}{2}$, siendo la misma probabilidad para ambos estados. Siguiendo (**??**), si obtenemos $|0\rangle$, el estado $|\psi\rangle$ colapsa a

$$|\psi\rangle = A\left(\frac{1}{\sqrt{2}}|00\rangle\right)$$

De donde sabemos que la constante de normalización *A* es

$$A = \frac{1}{\sqrt{|c_0|^2}} = \frac{1}{c_0} = \sqrt{2}$$

Por lo tanto el estado de nuestro sistema es

$$|\psi\rangle = |00\rangle$$

Y la segunda medición es trivial, ya que hemos obtenido directamente el estado $|00\rangle$. Aplicando lo mismo pero en este caso suponiendo que hemos obtenido $|1\rangle$ tras la primera medición, tenemos de manera análoga que

$$|\psi\rangle = |11\rangle$$

Y esto es nuestro primer caso de entrelazamiento, ya que hemos medido el estado de uno de los qubits de $|\Phi^+\rangle$, y el resultado de la primera medición afecta directamente a la anterior. En este caso, decimos que $|\Phi^+\rangle$ es un *estado máximo entrelazado*, ya que tras la primera medición obtenemos directamente el resultado final con una probabilidad de 1. Esto no siempre tiene por qué ser así, como veremos más adelante, un estado parcialmente entrelazado es muy parecido a esto que acabamos de ver, simplemente que la probabilidad después de la primera medición no es 1, sino que obtendremos unas probabilidades de medición para distintos estados que, por supuesto, al tratarse de qubits entrelazados, estas probabilidades se encuentran condicionadas por el resultado de la medición anterior.

6.1. Estados de Bell

Para crear entrelazamiento, necesitamos una puerta cuántica que actúe sobre más de un qubit al mismo tiempo. Esto no es posible con las puertas cuánticas de un único qubit, vistas en (**??**), ya que

al aplicar estas puertas el qubit se transforma pero de una manera independiente del resto, al contrario de las puertas que actúan sobre múltiples qubits, cuyas transformaciones generan en algunos casos una relación de dependencia entre pares de qubits, lo que conocemos como entrelazamiento.

Un ejemplo que puede crear entrelazamiento y que ya vimos anteriormente es la puerta *CNOT*, y podemos obtener el estado $|\Phi^+\rangle$ que ya demostramos en la sección anterior (**??**) que es uno de los cuatro estados máximos entrelazados, aplicando una puerta *CNOT* sobre $|+\rangle$ y $|0\rangle$:

$$\textit{CNOT}\,|+\rangle\,|0\rangle = \textit{CNOT}\frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right) = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) = |\Phi^+\rangle$$

Esto ocurre para todas las combinaciones entre la base sobre el eje $X = \{|+\rangle, |-\rangle\}$ y sobre el eje $Z = \{|0\rangle, |1\rangle\}$, obteniendo los cuatro estados máximos entrelazados, conocidos como *Estados de Bell*:

$$\textit{CNOT}\,|+\rangle\,|0\rangle = \textit{CNOT}\frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right) = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) = |\Phi^+\rangle\,, \tag{6.2}$$

$$\textit{CNOT}\,|-\rangle\,|0\rangle = \textit{CNOT}\frac{1}{\sqrt{2}}\left(|00\rangle - |10\rangle\right) = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right) = |\Phi^-\rangle\,, \tag{6.3}$$

$$\textit{CNOT}\,|+\rangle\,|1\rangle = \textit{CNOT}\frac{1}{\sqrt{2}}\left(|01\rangle + |11\rangle\right) = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) = |\Psi^+\rangle\,, \tag{6.4}$$

$$\textit{CNOT}\,|-\rangle\,|1\rangle = \textit{CNOT}\frac{1}{\sqrt{2}}\left(|01\rangle - |11\rangle\right) = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right) = |\Psi^-\rangle\,. \tag{6.5}$$

Y podemos demostrar de manera análoga a la vista para $|\Phi^+\rangle$ que si medimos uno de los dos qubits y secuencialmente medimos el otro, el estado que obtenemos al medir por segunda vez esta directamente relacionado con la medición anterior, confirmando que estos estados son estados máximamente entrelazados. Otra propiedad de un estado entrelazado es que no se pueden expresar como un producto de otros estados. Para ello vamos a tomar como ejemplo el estado de Bell $|\Phi^+\rangle$ y lo vamos a intentar expresar en función del producto de dos estados $|\psi_1\rangle\,|\psi_0\rangle$:

$$|\psi_1\rangle\,|\psi_0\rangle = \left(\alpha_1\,|0\rangle\,\beta_1\,|0\rangle\right)\left(\alpha_1\,|0\rangle\,\beta_1\,|0\rangle\right) = \alpha_1\alpha_0\,|00\rangle + \alpha_1\beta_0\,|01\rangle + \beta_1\alpha_0\,|10\rangle + \beta_1\beta_0\,|11\rangle \tag{6.6}$$

Y aplicando esto a $|\Psi^+\rangle$ llegamos a

$$\alpha_1\alpha_0 = \frac{1}{\sqrt{2}}, \quad \alpha_1\beta_0 = 0, \quad \beta_1\alpha_0 = 0, \quad \beta_1\beta_0 = \frac{1}{\sqrt{2}}$$

Y vemos que estas soluciones son muy inconsistentes y se contradicen unas con otras. Esto tambíen nos indica que $|\Psi^+\rangle$ no se puede expresar como un producto de estados $|\psi_1\rangle\,|\psi_0\rangle$ y que por lo tanto, es un estado en entrelazamiento. De manera análoga podemos demostrar que cada uno de los distintos

estados de Bell son efectivamente estados entrelazados. A continuación vamos a ver estados que se encuentran parcialmente en entrelazamiento, ya que en esta sección hemos visto únicamente los estados de Bell que son todos estados máximos entrelazados, de esta manera tendremos una visión mucho más clara de como funciona este fenómeno de la computación cuántica y posteriormente veremos algunas de las aplicaciones más importantes que tienen.

6.1.1. Estados Parcialmente Entrelazados

Como hemos introducido anteriormente, no todos los estados en entrelazamiento nos garantizan con total certeza el estado de la siguiente medición secuencial como hemos estado viendo hasta ahora con los estados de Bell, existen otros muchos estados en entrelazamiento (la gran mayoría) que se denominan estados parcialmente entrelazados, y esto en definitiva es, que no se garantiza el estado de la siguiente medición secuencial al medir qubits entrelazados. Para ver esto, vamos a considerar el siguiente estado:

$$|\psi\rangle = \frac{\sqrt{3}}{2\sqrt{2}}|00\rangle + \frac{\sqrt{3}}{2\sqrt{2}}|01\rangle + \frac{\sqrt{3}}{4}|10\rangle + \frac{1}{4}|11\rangle$$

Si medimos el qubit izquierdo, obtenemos $|0\rangle$ con una probabilidad de $\frac{3}{4}$ ya que

$$\left|\frac{\sqrt{3}}{2\sqrt{2}}\right|^2 + \left|\frac{\sqrt{3}}{2\sqrt{2}}\right|^2 = 2\,\frac{3}{8} = \frac{3}{4}$$

Y el estado colapsa a

$$|\psi\rangle = A\left(\frac{\sqrt{3}}{2\sqrt{2}}|00\rangle + \frac{\sqrt{3}}{2\sqrt{2}}|01\rangle\right)$$

Y la constante de normalización *A* la podemos obtener de múltiples maneras. La más intuitiva es sabiendo que la probabilidad total ha de ser igual a 1, obteniendo el valor de *A*

$$\left|A\,\frac{\sqrt{3}}{2\sqrt{2}}\right|^2 + \left|A\,\frac{\sqrt{3}}{2\sqrt{2}}\right|^2 = 1 \quad \rightarrow \quad A^2\,\frac{3}{4} = 1 \quad \rightarrow \quad A = \frac{2}{\sqrt{3}}$$

Y por lo tanto el estado de nuestro qubit colapsa a

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |01\rangle\right)$$

Con probabilidades de $\frac{1}{2}$ de obtener $|00\rangle$ y $|01\rangle$ al medir el segundo qubit. Como podemos observar esto no se trata de un estado máximo entrelazado, ya que la medición del primer qubit no determina

instantáneamente el resultado del segundo, sino que obtenemos una probabilidad perfectamente equiparable de $\frac{1}{2}$, aunque estas probabilidades pueden tener cualquier valor. Para ver esto, vamos a ver el segundo caso, en el que la primera medición da como resultado $|1\rangle$ con $\frac{1}{4}$ de probabilidad, colapsando en

$$|\psi\rangle = \frac{\sqrt{3}}{2}|10\rangle + \frac{1}{2}|11\rangle$$

Cuya constante de normalización ya ha sido calculada de la misma manera que en el caso anterior. Esto nos muestra que la probabilidad de obtener $|10\rangle$ es ahora de $\frac{3}{4}$ y la de obtener $|11\rangle$ de $\frac{1}{4}$, probando así que los resultados de las mediciones no son los mismos, ya que estamos ante un caso parcialmente entrelazado, ya que el estado de la segunda medición secuencial de $|\psi\rangle$ depende del resultado de la primera medición, pero no sabemos el resultado tras la primera medición con total certeza, ya que no estamos ante un caso de entrelazamiento de máximo nivel.

Todo esto nos ayudará a entender mucho mejor las aplicaciones de este fenómeno, como lo es el caso de la teleportación cuántica, en el que nos apoyaremos en los estados de Bell vistos en (**??**) para enviar información cuántica desde un emisor, el cual recibirá el nombre de Alice, y un receptor, que llamaremos Bob. Todo esto lo vamos a ver a continuación.

6.2. Teleportación Cuántica

En esta sección vamos a explicar la teleportación cuántica, el cual es un fenómeno muy importante que surge a partir del entrelazamiento cuántico visto anteriormente en (**??**). Este es un proceso en el que utilizaremos bits para enviar información cuántica, y con esto nos referimos al estado de un qubit en superposición $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ de un punto a otro, en el que pondremos nombre propio al emisor, Alice, y también al receptor, comúnmente conocido como Bob.

Llegados a este punto puede surgirnos una duda, ¿Por qué no enviamos la información cuántica directamente desde Alice hasta Bob? De esta manera nos ahorraríamos el uso de bits, sin embargo, esto no es posible, y para explicar esto nos vamos a basar en dos principios básicos que impiden esto, el *Teorema de no-clonación* y la *decoherencia*. Comencemos por el *Teorema de no-clonación*.

6.2.1. Teorema de No-Clonación

Supongamos que tengamos una partícula $|\psi\rangle$ cuyo estado es conocido, como por ejemplo $|+\rangle$. Esto nos permite clonar el estado de $|\psi\rangle$ simplemente aplicando una puerta de Hadamard sobre $|0\rangle$, creando tantas copias de $|\psi\rangle$ como queramos:

$$|+\rangle|0\rangle \xrightarrow{I\otimes H} |+\rangle|+\rangle$$

De manera que clonar el estado de un qubit conocido no es problema, el problema viene cuando no es conocido, como en el caso que acabamos de ver de enviar el estado de un qubit en superposición de Alice a Bob

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{6.7}$$

Para conseguir duplicar el estado de $|\psi\rangle$ necesitamos una puerta cuántica que satisfaga

$$|\psi\rangle\,|0\rangle \xrightarrow{U} |\psi\rangle\,|\psi\rangle$$

Esta puerta cuántica la vamos a denotar como *U*, de unitario, una de las propiedades que han de cumplir estas puertas y que ya vimos en (**??**). Entonces, se ha de satisfacer lo siguiente:

$$U\,|\psi\rangle\,|0\rangle = |\psi\rangle\,|\psi\rangle$$

Y apoyándonos en el álgebra lineal, podemos obtener un sistema de ecuaciones que satisfaga la condición anterior:

$$\begin{pmatrix} U_{11} & U_{12} & U_{13} & U_{14} \\ U_{21} & U_{22} & U_{23} & U_{24} \\ U_{31} & U_{32} & U_{33} & U_{34} \\ U_{41} & U_{42} & U_{43} & U_{44} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$\begin{pmatrix} U_{11} & U_{12} & U_{13} & U_{14} \\ U_{21} & U_{22} & U_{23} & U_{24} \\ U_{31} & U_{32} & U_{33} & U_{34} \\ U_{41} & U_{42} & U_{43} & U_{44} \end{pmatrix} \begin{pmatrix} \alpha \\ 0 \\ \beta 0 \end{pmatrix} = \begin{pmatrix} \alpha^2 \\ \alpha\beta \\ \alpha\beta \\ \beta^2 \end{pmatrix}$$

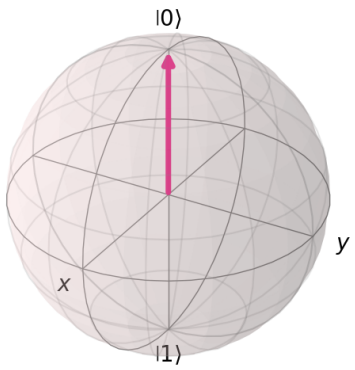
$$\begin{pmatrix} U_{11}\alpha + U_{13}\beta \\ U_{21}\alpha + U_{23}\beta \\ U_{31}\alpha + U_{33}\beta \\ U_{41}\alpha + U_{43}\beta \end{pmatrix} = \begin{pmatrix} \alpha^2 \\ \alpha\beta \\ \alpha\beta \\ \beta^2 \end{pmatrix}$$

Y con esto podemos ver perfectamente que las soluciones de este sistema dependen de α y β, por lo que acabamos de demostrar que no podemos clonar ningún estado desconocido, ya que para ello necesitamos saber el valor de α y de β.

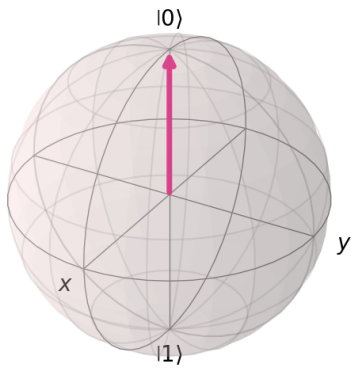
6.2.2. Decoherencia

El otro fenómeno que hace imposible duplicar el estado de $|\psi\rangle$ se conoce como decoherencia. La decoherencia es un fenómeno que sucede cuando un sistema cuántico interactúa con las propiedades del entorno, y como resultado podemos perder información, ya que lo que sucede es que el estado

nuestro sistema cuántico $|\psi\rangle$ se ve alterado, por lo que si tenemos un qubit en $|0\rangle$, este puede verse ligeramente afectado por la decoherencia, cambiando su valor, como podemos ver en el siguiente ejemplo:



(a) Estado $|0\rangle$



(b) Estado alterado por la decoherencia

Y esto puede ocurrir en múltiples escenarios, por ejemplo en casos de ruido térmico, ya que en este suceso las partículas tienen un cierto ruido térmico, siendo esto una de las principales causas de las alteraciones del estado de los qubits (decoherencia). Es por esto que los ordenadores cuánticos actuales se enfrían los máximo posible, hasta temperaturas del cero absoluto para evitar esta decoherencia producida por el ruido térmico. Otros hechos que pueden provocar decoherencia son la interferencia electromagnética, producida por ejemplo por ondas de microondas, o simplemente defectos en la fabricación de un ordenador cuántico.

Es por esto que los ordenadores cuánticos son realmente especiales y han de ser tratados con mucha delicadeza, y tenemos que mantenerlos alejados de cualquier interacción que puedan tener con su entorno. Incluso la medición de un qubit puede causar decoherencia, lo que nos ha llevado a la necesidad de métodos y sistemas de corrección de errores cuánticos, causados por estos problemas.

6.2.3. Teleportación Cuántica

Una vez ya hemos aclarado por qué no podemos enviar información cuántica directamente y la razón por la que tenemos que apoyarnos en información clásica (bits), vamos a entrar de lleno en la teleportación cuántica. Como ya introdujimos anteriormente en (**??**), vamos enviar el estado de un qubit cuántico $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ de Alice a Bob, apoyándonos en información clásica y en el entrelazamiento, aplicando todas las propiedades que el entrelazamiento tiene sobre $|\psi\rangle$.

Como no conocemos el estado de $|\psi\rangle$, Alice no puede duplicarlo sobre un qubit de Bob, como ya vimos en el *Teorema de no-clonación* (**??**), por lo que no podemos comunicarle directamente a Bob el estado de $|\psi\rangle$. Es este caso uno de los muchos usos del entrelazamiento, en el que le podremos

decir a Bob el estado de $|\psi\rangle$ utilizando únicamente dos bits. Imaginemos que Alice y Bob comparten dos qubits entrelazados en el estado $|\Phi^+\rangle$, de manera que Alice posee dos qubits, $|\psi\rangle$ el cual es el que queremos transmitir a Bob, y uno de los dos qubits de $|\Phi^+\rangle$, mientras que Bob posee el otro qubit de $|\Phi^+\rangle$, quedando los tres qubits en

$$|\psi\rangle\,|\Phi^+\rangle = \alpha\,|0\rangle\,|\Phi^+\rangle + \beta\,|1\rangle\,|\Phi^+\rangle = \alpha\,|0\rangle\,\frac{1}{\sqrt{2}}\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,\frac{1}{\sqrt{2}}\,(|00\rangle + |11\rangle) =$$

$$= \frac{1}{\sqrt{2}}\,[\alpha\,(|000\rangle + |011\rangle) + \beta\,(|100\rangle + |111\rangle)]$$

Entonces, el objetivo que tenemos ahora es expresar el estado del qubit de Bob en función de α y β, y debido a que se encuentra entrelazado con uno de los qubits de Alice, Bob va a poder saber el estado de $|\psi\rangle$ antes de la medición, ya que tendremos que medir el qubit entrelazado de Alice, lo cual afectará directamente al qubit entrelazado de Bob al encontrarse ambos en un estado máximo de entrelazamiento, y Bob podrá conocer de esta manera el estado de $|\psi\rangle$. Comencemos aplicando una puerta *CNOT* sobre los dos qubits de Alice, los cuales son el qubit izquierdo y el central, obteniendo el siguiente resultado:

$$\frac{1}{\sqrt{2}}\,[\alpha\,(|000\rangle + |011\rangle) + \beta\,(|100\rangle + |111\rangle)] \xrightarrow{CNOT} \frac{1}{\sqrt{2}}\,[\alpha\,(|000\rangle + |011\rangle) + \beta\,(|110\rangle + |101\rangle)]$$

Y a continuación aplicamos una puerta de Hadamard sobre el qubit izquierdo de Alice, y operando obtenemos el siguiente resultado:

$$\frac{1}{\sqrt{2}}\,[\alpha\,(|000\rangle + |011\rangle) + \beta\,(|110\rangle + |101\rangle)] \xrightarrow{H} \frac{1}{\sqrt{2}}\,[\alpha\,(|+00\rangle + |+11\rangle) + \beta\,(|-10\rangle + |-01\rangle)] =$$

$$= \frac{1}{2}\,[\alpha\,(|0\rangle + |1\rangle)\,(|00\rangle + |11\rangle) + \beta\,(|0\rangle - |1\rangle)\,(|10\rangle + |01\rangle)] =$$

$$= \frac{1}{2}\,[|00\rangle\,(\alpha\,|0\rangle + \beta\,|1\rangle) + |01\rangle\,(\beta\,|0\rangle + \alpha\,|1\rangle) + |10\rangle\,(\alpha\,|0\rangle - \beta\,|1\rangle) + |11\rangle\,(-\beta\,|0\rangle + \alpha\,|1\rangle)]$$

En esto se resume, a falta del procedimiento a seguir tras la medición, la teleportación cuántica, cuyo circuito viene recogido de la siguiente manera:

Ahora es cuando viene el momento de la medición. Si Alice mide sus dos qubits, estos colapsarán a uno de los siguientes estados con una probabilidad equiparable de $\frac{1}{4}$:

$$|00\rangle\,(\alpha\,|0\rangle + \beta\,|1\rangle) \tag{6.8}$$

$$|01\rangle\,(\beta\,|0\rangle + \alpha\,|1\rangle) \tag{6.9}$$

$$|10\rangle\,(\alpha\,|0\rangle - \beta\,|1\rangle) \tag{6.10}$$

$$|11\rangle\,(-\beta\,|0\rangle + \alpha\,|1\rangle) \tag{6.11}$$

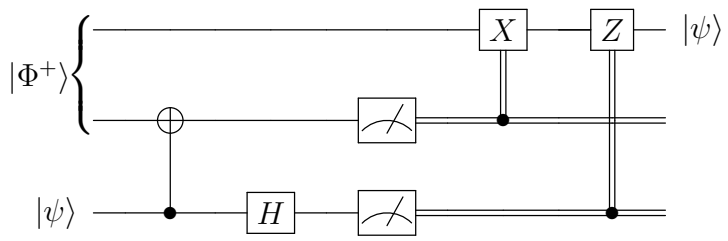


Figura 17: Teleportación cuántica. Circuito cuántico

Y aquí ya tenemos los qubits de Alice, los cuales ya vemos que han colapsado a $|00\rangle$, $|01\rangle$, $|10\rangle$ o $|11\rangle$, y tenemos también el qubit de Bob expresado en función de α y β, de manera que Alice solo tiene que comunicarle a Bob el resultado de la medición de sus dos qubits, y dependiendo del resultado, Bob tendrá que aplicar una determinada puerta cuántica a su qubit, obteniendo finalmente $|\psi\rangle$:

- Si la medición colapsó a $|00\rangle$ (**??**), Bob ya tiene directamente su qubit en el mismo que estado que $|\psi\rangle$, por lo que no tendríamos que aplicar ninguna puerta cuántica.
- Si tras la medición obtenemos $|01\rangle$ (**??**), Bob aplicará una puerta *NOT* (o puerta *X*) para obtener $|\psi\rangle$.
- Si obtenemos $|10\rangle$ (**??**) tras la medición, simplemente Bob aplica una puerta *Z* a su qubit, llegando finalmente a $|\psi\rangle$.
- Y si por último Alice obtiene $|11\rangle$ (**??**) tras la medición, Bob aplicaría una puerta *X* seguida de una *Z* para obtener $|\psi\rangle$.

Y esta es la magia de la teleportación cuántica, la cual surge ante el problema de no poder enviar físicamente información cuántica debido a problemas como el teorema de no-clonación o la decoherencia. Es por esto que aprovechamos las propiedades del entrelazamiento cuántico para asentar las bases que nos permiten describir el estado de un qubit de un emisor, en este caso Alice, a un receptor, Bob, tomando de la mano el uso de puertas cuánticas vistas en (**??**) como la *CNOT* y la puerta de Hadamard *H*.

6.3. Encriptación Cuántica. BB84

Digamos ahora que Alice y Bob quieren mandar un mensaje, pero de manera segura, ya que la información enviada entre ambos pueden ser datos confidenciales, contraseñas, etc. Es por esto que

ciertas personas nos van a intentar robar esta información, y nos solemos referir a estas personas en el abito de la criptografía cuántica como Eve, y de la misma manera que en la computación clásica se estableceremos una clave pública y privada para que Bob descifre la información enviada por Alice. Es en esto en lo que se basa el protocolo que vamos a ver en este capítulo, BB84.

Aunque es cierto que BB84 no necesita entrelazamiento, nos servirá para asentar las bases de un sistema de encriptación más complejo, como EPR (**??**) o E91 (**??**), los cuales sí usan entrelazamiento y son protocolos más seguros. Estos son solo algunos ejemplos de QKD (Quantum Key Distribution), métodos o protocolos en el que por medio de una encriptación cuántica aseguramos la la seguridad e integridad de la información transmitida. Comencemos por el primer paso de BB84, en el que el emisor, en este caso Alice, selecciona un conjunto de bits, y para cada bit se escoge aleatoriamente una base, que puede ser la base en el eje Z $\{|0\rangle, |1\rangle\}$ o en el eje X $\{|+\rangle, |-\rangle\}$, como se puede ver recogido en la siguiente tabla:

Bits de Alice	1	0	0	1	0	0	0	1	1
Bases de Alice	X	Z	Z	X	X	Z	X	Z	Z

Figura 18: Primer paso de BB84.

El siguiente paso es muy sencillo, y es que dependiendo del bit inicial y la base escogida, Alice va a enviar un estado u otro. Comenzando por la base Z, si el bit inicial es 0, Alice le enviará a Bob el estado $|0\rangle$, y si inicialmente se escogió 1, se envía $|1\rangle$. Esto aplica de la misma manera para la base en el eje X, en el que enviaremos $|+\rangle$ o $|-\rangle$ dependiendo si inicialmente se escogió 0 o 1, respectivamente, como podemos ver en la siguiente tabla:

Bits de Alice	1	0	0	1	0	0	0	1	1
Base	X	Z	Z	X	X	Z	X	Z	Z
Se envía	$\|+\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|1\rangle$

Figura 19: Segundo paso de BB84.

A continuación Bob recibe la información enviada por Alice, y Bob mide el resultado que Alice le acaba de enviar en una de las dos bases que estamos utilizando, Z o X, de manera que si la base elegida por Bob coincide con la escogida por Alice, el resultado será el mismo que Alice, ya que la información que estamos enviando se encuentra en los polos de los ejes con los que estamos trabajando, por lo que no tenemos ninguna incertidumbre en la medición y sabemos el resultado. Por el contrario, si la base es distinta, tendremos $\frac{1}{2}$ de probabilidad de acertar el resultado o de errarlo, siendo el resultado de Bob completamente aleatorio ya que la probabilidad es la misma, quedando en

Bits de Alice	1	0	0	1	0	0	0	1	1
Base	X	Z	Z	X	X	Z	X	Z	Z
Se envía	$\|+\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|1\rangle$
Base de Bob	Z	Z	X	X	X	Z	Z	X	X
Medición	$\|0\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$
Bit final	0	0	1	0	1	1	1	1	0

Figura 20: Obtención del bit final BB84.

En este momento es cuando determinamos la clave privada para comunicarnos con total seguridad, aunque siempre puede existir una pequeña probabilidad de que nos intercepten la clave, por muy pequeña que sea, lo cual veremos muy proximamente. Para establecer la clave, Alice y Bob revelan públicamente las bases que ambos han usado, y si ambas bases coinciden, saben perfectamente que su resultado es el mismo, obteniendo así los bits de la clave privada:

Bits de Alice	1	0	0	1	0	0	0	1	1
Base	X	Z	Z	X	X	Z	X	Z	Z
Se envía	$\|+\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|1\rangle$
Base de Bob	Z	Z	X	X	X	Z	Z	X	X
Medición	$\|0\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$
Bit final	0	0	1	0	1	1	1	1	0
Clave Privada		0		0	1	1			

Figura 21: Obtención de la clave privada mediante BB84.

Por lo que la clave es 0011. Sin embargo, podemos tener un problema, y es que haya una tercera partida, Eve, que esté intentando robarnos los datos. Supongamos que Alice selecciona la base *Z* y envía $|0\rangle$ a Bob, pero Eve intercepta el estado $|0\rangle$. Ahora Eve tiene dos opciones, seleccionar la base *Z* por lo que al medir el resultado seguiría siendo $|0\rangle$, o el caso contrario, en el que escoja una base distinta de Alice. En este caso, sería la base *X*, por lo que al medir $|0\rangle$ podría obtener o bien $|0\rangle$ o $|1\rangle$, y en caso de medir $|1\rangle$, Alice y Bob se darían cuenta que hay una tercera persona robando los datos, ya que los casos que nos interesan son en el que las bases de Alice y Bob coinciden, estableciendo así la clave. En definitiva, la probabilidad de detectar a Eve en un único qubit es de $\frac{1}{4}$, y entonces, la probabilidad de que Eve pase desapercibido es $\frac{3}{4}$. Esto lo podemos generalizar para *n* bits, siendo la probabilidad de detectar a Eve de

$$\text{Probabilidad de detectar a Eve} = 1 - \left(\frac{3}{4}\right)^n$$

Siendo esta probabilidad de 0.99999943 para 50 bits, por lo que la probabilidad de que Eve acceda a la información sin ser detectada es prácticamente nula. No obstante, al medir Eve los qubits enviados de Alice, el estado de estos puede colapasar a un estado que no es el que teníamos previsto, alterando la información. Para solucionar este problema simplemente añadimos unos bits de prueba a nuestra cadena de bits original, y de esta manera primero comprobaríamos si hay algún fallo al obtener la clave de la cadena de bits de prueba, la cual no es una parte de nuestra clave real, es una pequeña comprobación para verificar que todo va en orden.

6.4. El Protocolo E91

El protocolo BB84 (**??**) es una de las principales bases de la encriptación cuántica, ya que la mayoría de protocolos de este ámbito se basan en él, y el protocolo que vamos a ver a continuación, *E91*, cuyas siglas hacen referencia a su autor, *Artur Ekert* en 1991 **?**, no va a ser menos. La principal diferencia es que este sistema sí utiliza qubits entrelazados, añadiendo así una capa de seguridad adicional contra Eve.

Una vez se reparten los pares de qubits entrelazados q_j, q'_j entre Alice y Bob, cada uno eligen una base con la que medir sus qubits entrelazados, $\{\vec{a_1}, \vec{a_2}, \vec{a_3}\}$ y $\{\vec{b_1}, \vec{b_2}, \vec{b_3}\}$ respectivamente, y estas bases tienen que cumplir unas ciertas condiciones que veremos más adelante. Estas bases usadas para medir cada uno de los qubits se mantienen en secreto hasta que se cumple con todas las mediciones. Posteriormente Alice y Bob comparten públicamente las bases que han utilizado para cada qubit, de manera que si estas bases coinciden, el resultado de ambos será el mismo ya que los qubits se encuentran máximamente entrelazados en el estado de Bell $|\Phi^+\rangle$, determinando así la clave privada, y los casos en los que las bases no coincidan, serán reservados para averiguar si la comunicación ha sido interceptada por Eve, o si por el contrario ha habido algún problema de ruido o decoherencia, dificultando así la comunicación.

En primer lugar, supongamos que una tercera persona proporciona a Alice y Bob pares de qubits entrelazados entre sí, enviando uno de los qubits entrelazados a Alice y el otro a Bob, los cuales se encuentran en uno de los estados de Bell $|\Phi^+\rangle$:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right)$$

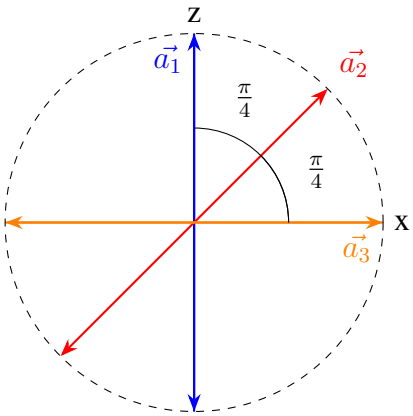
Una vez han recibido correctamente cada uno de sus qubits entrelazados y están listos para la comunicación, ambos eligen una base entre las dos posibles opciones con la que medir el qubit. Las bases que vamos a usar las vamos a denotar como $\{\vec{a_1}, \vec{a_2}, \vec{a_3}\}$ para Alice y $\{\vec{b_1}, \vec{b_2}, \vec{b_3}\}$ en el caso de Bob, para hacer un postprocesamiento de los resultados obtenidos con el fin de detectar a Eve o un excesivo ruido cuántico. En definitiva, estas bases son

$$\vec{a_1} = Z, \qquad \vec{b_1} = \frac{1}{\sqrt{2}}(X + Z)$$

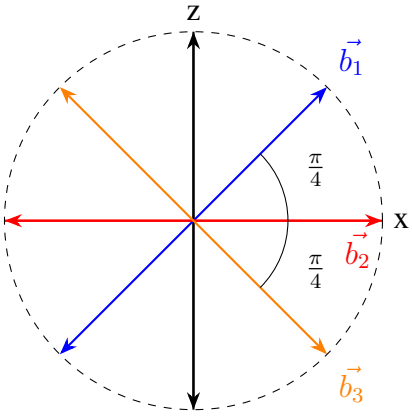
$$\vec{a_2} = \frac{1}{\sqrt{2}}(X + Z), \qquad \vec{b_2} = X$$

$$\vec{a_3} = X, \qquad \vec{b_3} = \frac{1}{\sqrt{2}}(X - Z)$$

Esto lo podemos ver gráficamente con los siguientes ángulos en el plano *XZ*:



(a) Bases de Alice relativas al plano XZ



(b) Bases de Bob relativas al plano XZ

Estas bases en concreto están escogidas para satisfacer la *desigualdad CHSH*, con la que detectaremos a Eve, la cual veremos más adelante. Una vez escogidas las bases, Alice y Bob miden sus respectivos qubits, y como se encuentran entrelazados en el estado $|\Phi^+\rangle$, el resultado siempre va a ser el mismo en el caso que coincidan sus bases escogidas. Este proceso es relativamente similar a *BB84*, ya que Alice y Bob comparten públicamente la base que usaron para su medición, y si la base coincide, nos quedamos con dicho qubit para hacer la clave de cifrado, suponiendo que todo este proceso ha funcionado correctamente.

Qubit entrelazado de Alice	q_1	q_2	q_3	q_4	q_5	q_6	q_7	q_8	q_9
Base de Alice $\vec{a_j}$	$\vec{a_1}$	$\vec{a_2}$	$\vec{a_3}$	$\vec{a_3}$	$\vec{a_1}$	$\vec{a_2}$	$\vec{a_2}$	$\vec{a_1}$	$\vec{a_3}$
Medición de Alice	$\|1\rangle$	$\|a_2^+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|0\rangle$	$\|a_2^-\rangle$	$\|a_2^+\rangle$	$\|1\rangle$	$\|+\rangle$
Valor Final de Alice	-1	1	-1	-1	1	-1	1	-1	1
Qubit entrelazado de Bob	q'_1	q'_2	q'_3	q'_4	q'_5	q'_6	q'_7	q'_8	q'_9
Base de Bob $\vec{b_j}$	$\vec{b_1}$	$\vec{b_3}$	$\vec{b_2}$	$\vec{b_1}$	$\vec{b_2}$	$\vec{b_3}$	$\vec{b_1}$	$\vec{b_2}$	$\vec{b_3}$
Medición de Bob	$\|b_1^+\rangle$	$\|b_3^-\rangle$	$\|-\rangle$	$\|b_1^+\rangle$	$\|+\rangle$	$\|b_3^-\rangle$	$\|b_1^+\rangle$	$\|-\rangle$	$\|b_3^+\rangle$
Valor Final de Bob	1	-1	-1	1	1	-1	1	-1	1
¿Clave secreta?			✓				✓		
¿Usado para calcular S?	✓			✓					✓

Figura 23: Ejemplo del Protocolo E91.

Donde los valores obtenidos son 1 si el resultado final es $|0\rangle$, $|+\rangle$ o contiene $+$, o -1 si el resultado final es $|1\rangle$, $|-\rangle$ o contiene $-$, esto es simplemente un formalismo para cumplir con los autovalores del operador de medición $\hat{O}$ (**??**). Posteriormente, los valores obtenidos como 1 pasarán a ser 0 en la clave de cifrado, y de la misma manera sucede con -1, el cual pasará a ser 1.

Entonces, con esta tabla (**??**) podemos ver que la clave privada que obtenemos está formada por los qubits q_3 y q_7, y esta es el número binario 10. Sin embargo,si comparamos este método frente a *BB84*, vemos que no tenemos ninguna ventaja aparente, ya que hemos conseguido la clave privada partiendo de coincidencias en las bases utilizadas. De hecho, este protocolo es bastante más ineficiente que *BB84*, ya que con el mismo número de 9 unidades de información, obtenemos una clave de 2 bits frente a la clave de 4 bits obtenida en (**??**), por lo que necesitaríamos un ordenador cuántico mucho más potente para obtener una clave privada utilizando este método, lo cual es una desventaja.

6.4.1. La Desigualdad de Bell CHSH

La gran ventaja de *E91* viene a la hora de detectar a Eve. Como sabemos, se puede dar el caso de tener a una tercera persona interceptando nuestros qubits y realizando mediciones sobre ellos, y es aquí la gran diferencia con respecto a *BB84*, ya que si Eve mide los qubits durante el proceso de este protocolo, el entrelazamiento entre los qubits de Alice y Bob se rompe, y esto lo podemos calcular gracias al parámetro *S* **?** de la desigualdad de Bell *CHSH*.

Para hacer el cálculo de *S*, primero necesitamos explicar el concepto de correlación $E(a, b)$. La correlación $E(a, b)$ de dos bases a y b, cuantifica la relación entre los resultados obtenidos de medir en la base a, la cual en nuestro caso será la base de Alice, con los resultados de medir en la base b (base de Bob) en un par entrelazado de qubits. De esta manera, si la base a y b resulta ser la misma,

obtendremos un valor de $E(a,b) = 1$, lo cual sucede para las bases $\vec{a_2}$ y $\vec{b_1}$, además de $\vec{a_3}$ y $\vec{b_2}$, ya que estas bases son idénticas, como se puede ver en (**??**), y se obtiene el mismo resultado en caso de coincidir (**??**), creando así la clave de cifrado.

Según la definición teórica de $E(a,b)$, este valor varía según los ángulos θ_A de la base de Alice y θ_B de la base de Bob, como el coseno de la diferencia de los ángulos θ_A y θ_B, y se define según el operador de medición $\hat{O}$ sobre los ángulos θ_A y θ_B

$$E(a,b) = \langle \Phi^+ \, | \hat{O}_{\theta_A} \otimes \hat{O}_{\theta_A} | \, \Phi^+ \rangle \tag{6.12}$$

Para demostrar este valor, hemos de definir el operador de medición $\hat{O}$ en una base rotada sobre el eje *Z* por un cierto ángulo θ:

$$\hat{O}_\theta = \cos(\theta) Z + \sin(\theta) X, \qquad \theta \in [0, 2\pi] \tag{6.13}$$

Donde *Z* y *X* son las matrices de Pauli, las cuales definimos en (**??**). Entonces, el operador $\hat{O}_\theta$ se puede expresar como

$$\hat{O}_\theta = \cos(\theta) \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} + \sin(\theta) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \cos(\theta) & 0 \\ 0 & -\cos(\theta) \end{pmatrix} + \begin{pmatrix} 0 & \sin(\theta) \\ \sin(\theta) & 0 \end{pmatrix} =$$
$$= \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix}$$

Entonces, aplicando el producto de Kronecker $\otimes$ (**??**) nos queda lo siguiente:

$$O_{\theta_A} \otimes O_{\theta_B} = \begin{pmatrix} \cos(\theta_A) \begin{pmatrix} \cos(\theta_B) & \sin(\theta_B) \\ \sin(\theta_B) & -\cos(\theta_B) \end{pmatrix} & \sin(\theta_A) \begin{pmatrix} \cos(\theta_B) & \sin(\theta_B) \\ \sin(\theta_B) & -\cos(\theta_B) \end{pmatrix} \\ \sin(\theta_A) \begin{pmatrix} \cos(\theta_B) & \sin(\theta_B) \\ \sin(\theta_B) & -\cos(\theta_B) \end{pmatrix} & -\cos(\theta_A) \begin{pmatrix} \cos(\theta_B) & \sin(\theta_B) \\ \sin(\theta_B) & -\cos(\theta_B) \end{pmatrix} \end{pmatrix}$$

$$= \begin{pmatrix} \cos(\theta_A)\cos(\theta_B) & \cos(\theta_A)\sin(\theta_B) & \sin(\theta_A)\cos(\theta_B) & \sin(\theta_A)\sin(\theta_B) \\ \cos(\theta_A)\sin(\theta_B) & -\cos(\theta_A)\cos(\theta_B) & \sin(\theta_A)\sin(\theta_B) & -\sin(\theta_A)\cos(\theta_B) \\ \sin(\theta_A)\cos(\theta_B) & \sin(\theta_A)\sin(\theta_B) & -\cos(\theta_A)\cos(\theta_B) & -\cos(\theta_A)\sin(\theta_B) \\ \sin(\theta_A)\sin(\theta_B) & -\sin(\theta_A)\cos(\theta_B) & -\cos(\theta_A)\sin(\theta_B) & \cos(\theta_A)\cos(\theta_B) \end{pmatrix}$$

Si sustituimos esto en la expresión (**??**), obtenemos la expresión trigonométrica que estábamos buscando:

$$E(a,b) = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0 & 0 & 1\end{pmatrix}\begin{pmatrix}\cos(\theta_A)\cos(\theta_B) & \cdots & \cdots & \sin(\theta_A)\sin(\theta_B)\\ \vdots & \ddots & \ddots & \vdots\\ \vdots & \ddots & \ddots & \vdots\\ \sin(\theta_A)\sin(\theta_B) & \cdots & \cdots & \cos(\theta_A)\cos(\theta_B)\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix} =$$

$$= \frac{1}{2}\begin{pmatrix}1 & 0 & 0 & 1\end{pmatrix}\begin{pmatrix}\cos(\theta_A)\cos(\theta_B)+\sin(\theta_A)\sin(\theta_B)\\ \cdots\\ \cdots\\ \sin(\theta_A)\sin(\theta_B)+\cos(\theta_A)\cos(\theta_B)\end{pmatrix} =$$

$$= \frac{1}{2}\left(\cos(\theta_A)\cos(\theta_B)+\sin(\theta_A)\sin(\theta_B)+\sin(\theta_A)\sin(\theta_B)+\cos(\theta_A)\cos(\theta_B)\right) =$$

$$= \frac{1}{2}\left(2\left(\cos(\theta_A)\cos(\theta_B)\right)+2\left(\sin(\theta_A)\sin(\theta_B)\right)\right) = \left(\cos(\theta_A)\cos(\theta_B)\right)+\left(\sin(\theta_A)\sin(\theta_B)\right)$$

$$\boxed{E(a,b) = \cos(\theta_A - \theta_B)} \tag{6.14}$$

Es en este punto cuando podemos definir *S*. Para un par de bases de Alice A_1, A_2 y otro par de bases de Bob B_1, B_2, se define *S* como

$$S = E(A1, B1) - E(A1, B2) + E(A2, B1) + E(A2, B2) \leq 2$$

Y, en definitiva, si obtenemos un valor de $S \leq 2$ significa que los qubits medidos en las bases de Alice y Bob no están realmente entrelazados. Es por esto que queremos violar esta desigualdad, demostrando así que los pares de qubits de Alice y Bob se encontraban en entrelazamiento antes de realizar sus respectivas mediciones. Si escogemos las bases adecuadas, S puede alcanzar un límite teórico de $2\sqrt{2}$, y esto lo podemos lograr con las bases $\vec{a_1}, \vec{a_3}$ de Alice y las bases $\vec{b_1}, \vec{b_3}$ de Bob (**??**):

$$S = E(\vec{a_1}, \vec{b_1}) - E(\vec{a_1}, \vec{b_3}) + E(\vec{a_3}, \vec{b_1}) + E(\vec{a_3}, \vec{b_3}) \tag{6.15}$$

$$S = \cos\left(\frac{\pi}{2} - \frac{\pi}{4}\right) - \cos\left(\frac{\pi}{2} - \left(-\frac{\pi}{4}\right)\right) + \cos\left(0 - \frac{\pi}{4}\right) + \cos\left(0 - \left(-\frac{\pi}{4}\right)\right) =$$

$$S = \frac{\sqrt{2}}{2} - \left(-\frac{\sqrt{2}}{2}\right) + \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}$$

$$S = 2\sqrt{2} \tag{6.16}$$

Y este es el valor que deberíamos obtener si no hay presencia de Eve en un escenario completamente ideal. En la práctica, este resultado exacto no se suele conseguir debido al ruido cuántico del sistema,

aunque se debería obtener un resultado basante similar. Es más, en una simulación real no podemos aplicar la expresión vista en (**??**) ya que $E(a, b)$ no varía según los resultados de Alice y Bob, y es esto en lo que nos hemos fijar para detectar a Eve. Para ello tenemos que calcular la correlación $E(a, b)$ en función de los resultados experimentales, de la siguiente manera:

$$E(a,b) = P_{++}(a,b) - P_{+-}(a,b) - P_{-+}(a,b) + P_{--}(a,b), \qquad E(a,b) \in [-1,1] \tag{6.17}$$

Donde $P_{++}(a, b)$ es la probabilidad de que Alice obtenga 1 en la base *a* y Bob obtenga 1 en su respectiva base *b*. De la misma manera aplica para $P_{+-}(a, b)$, donde el símbolo $+$ representa la obtención del factor 1 en la base de Alice y $-$ el factor -1 en la base de Bob. Esta idea se aplica al resto de miembros $P_{-+}(a, b)$ y $P_{--}(a, b)$. Generalizando esta notación, se obtiene que

$$P_{XY}(a,b) = \frac{\text{Nº resultados XY}}{\text{Nº total de pares medidos en las bases a, b}}$$

Entonces, cuanto mayor sea el número de mediciones mejor será la aproximación de *S* a su valor teórico (**??**). Esto no lo podemos hacer con los resultados obtenidos en la tabla de ejemplo (**??**) ya que no tenemos un número suficiente de qubits. Sin embargo, podemos realizar una simulación en un escenario cuántico real y analizar su comportamiento.

6.4.2. Simulación de E91

CAPÍTULO

7

Algoritmos Cuánticos

En este punto llegamos a una de las últimas secciones de este trabajo, en el que vamos a explicar y desarrollar por qué los ordenadores cuánticos son tan importantes. Todo se reduce a los algoritmos cuánticos, y es que, aprovechando las propiedades que ya sabemos como la superposición (**??**) o entrelazamiento (**??**) podemos mejorar la eficiencia de ciertos algoritmos, optimizándolos lo máximo posible, de manera que obtenemos algoritmos que en muchos casos son infinitamente más rápidos que la versión tradicional de estos procesos.

Cabe destacar que no todo algoritmo cuántico por ser cuántico, valga la redundancia, es más rápido, esto no siempre sucede así, pero como vimos anteriormente, toda información clásica se puede representar mediante un ordenador cuántico, por lo que únicamente tendríamos que clonar dichos procesos. En esta sección vamos a centrarnos en dos algoritmos: El algoritmo de Grover y el de Shor, los cuales mejoran la búsqueda por fuerza bruta y se optimiza de exponencial manera el problema de factorización, rompiendo con las claves públicas y privadas de ciertos cifrados como veremos próximamente.

7.1. Oráculos Cuánticos

Antes de comenzar por los oráculos, tenemos que explicar un par de conceptos. El primero es el de *complejidad de circuitos*, ya que no todos los circuitos son iguales, podemos encontrar circuitos más o menos complejos que otros, y esto se mide contando el número mínimo de puertas cuánticas, tomando como referenca un conjunto de puertas cuánticas universales, como explicamos anteriormente al final de (**??**). Tomando como ejemplo el sumador cuántico require $32n - 14$ puertas cuánticas, siendo *n* el número de qubits que represetan a cada sumando en el sumador, y esto al depender de *n*, decimos que tiene una complejidad lineal *O(N)*.

Esto es lo que buscamos, ya que para que un algoritmo cuántico sea considerado eficiente ha de tener esta complejidad *O(n)*. Sin embargo, hallar la complejidad de circuitos es una tarea muy difícil en muchos casos, y es por esto que se usan otros métodos, como el uso de *oráculos cuánticos*. Esto es un método basado en la *complejidad de consultas* (query complexity), de manera que tendremos una función, $f(x)$ a la cual llamaremos un cierto número de veces, determinando así la complejidad *O(N)*.

Pongamos como ejemplo uno de los algoritmos que veremos a continuación, el *algoritmo de Grover*. Este algoritmo mejora el problema de búsqueda por fuerza bruta de los computadores tradicionales, ya que en un computador clásico tenemos que explorar cada elemento uno a uno, y vemos si cumple con nuestros criterios. Si es el elemento que estamos buscando, el oráculo será $f(x) = 1$, y de lo contrario, si el oráculo es $f(x) = 0$ significa que no es el objeto que deseamos encontrar y que por lo tanto hemos de seguir buscando, siendo x el elemento consultado. Esto significa que, como hemos de consultar cada elemento uno a uno, tendremos una complejidad de *O(N)* ya que en el peor de los casos tendremos que consultar la función oráculo *N* veces, siendo *N* el número total de elementos. Veremos posteriormente en (**??**) como reducimos la complejidad hasta *O($\sqrt{N}$)*.

Esta idea aparece y se aplica en otros muchos otros algoritmos cuánticos, por lo que podemos asentar este concepto. Un oráculo cuántico no es más que una función booleana, es decir, su valor solo puede ser 0 o 1, lo que significa que puede definirse por medio de puertas lógicas convencionales. Si queremos tener un oráculo cuántico, tenemos que convertir este oráculo, el cual es un conjunto de puertas lógicas, en una puerta cuántica, y para ello debemos hacerla reversible como vimos en (**??**). Esto se traduce a hacer que el oráculo sea reversible, y esto lo podemos hacer muy fácilmente, apoyándonos en una de las puertas lógicas más importantes, la puerta *XOR*, cuya tabla de verdad es la siguiente:

A	B	A $\oplus$ B
0	0	0
0	1	1
1	0	1
1	1	0

Figura 24: Tabla de verdad de la puerta XOR

En definitiva, si añadimos un bit adicional *y*, además del bit *x* del oráculo, y pasamos ambos bits por una *XOR*, obtendremos un resultado reversible que es lo que buscamos para que esto sea una puerta cuántica. Este nuevo oráculo reversible, lo hemos denotado como U_f en el siguiente circuito:

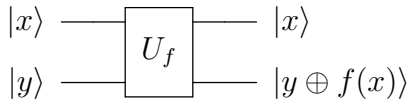


Figura 25: Oráculo cuántico

Actuando sobre $|x\rangle$ y $|y\rangle$ como sigue

$$|x\rangle |y\rangle \xrightarrow{U_f} |x\rangle |y \otimes f(x)\rangle \tag{7.1}$$

Y este oráculo lo utilizaremos posteriormente en el algoritmo de Shor (**??**).

7.2. Oráculo de Fase

Lo siguiente que vamos a ver es el oráculo de fase, y está muy ligado a los oráculos cuánticos que acabamos de ver. Si nos fijamos en el oráculo de la sección anterior en (**??**), $|x\rangle$ permanece intacto mientras que $|y\rangle$ queda como $|y \otimes f(x)\rangle$. En este caso queremos que el qubit que quede intacto sea $|y\rangle$, quedando $|x\rangle$ multiplicado por una fase, de ahí el nombre, oráculo de fase. Esto lo podemos lograr transformando $|y\rangle$ en $|-\rangle$, que lo podemos hacer inicializando $|y\rangle$ en $|0\rangle$, aplicando una puerta *X*, es decir una puerta *NOT*, y finalmente aplicando una puerta de Hadamard como sigue

$$|x\rangle |0\rangle \xrightarrow{I\otimes X} |x\rangle |1\rangle \xrightarrow{I\otimes H} |x\rangle |-\rangle$$

Entonces, si aplicamos el oráculo obtenemos lo que estábamos buscando, una fase multiplicando a $|x\rangle$ y $|-\rangle$ que permanece igual:

$$\begin{aligned}
|x\rangle |-\rangle &= \frac{1}{\sqrt{2}} \left(|x\rangle |0\rangle - |x\rangle |1\rangle\right) \xrightarrow{U_f} \frac{1}{\sqrt{2}} \left(|x\rangle |0 \oplus f(x)\rangle - |x\rangle |1 \oplus f(x)\rangle\right) = \\
&= \begin{cases} \frac{1}{\sqrt{2}} \left(|x\rangle |0\rangle - |x\rangle |1\rangle\right), & f(x) = 0 \\ \frac{1}{\sqrt{2}} \left(|x\rangle |1\rangle - |x\rangle |0\rangle\right), & f(x) = 1 \end{cases} \\
&= \begin{cases} |x\rangle |-\rangle, & f(x) = 0 \\ - |x\rangle |-\rangle, & f(x) = 1 \end{cases} \\
&= (-1)^{f(x)} |x\rangle |-\rangle
\end{aligned} \tag{7.2}$$

Y aquí tenemos el oráculo de fase en la expresión (**??**), en el que vemos que $|x\rangle$ se encuentra multiplicado por la fase $(-1)^{f(x)}$, la cual vemos que depende de $f(x)$, mientras que el segundo qubit

$|-\rangle$ permanece igual. Esto lo vamos a usar en el siguiente apartado, en el que comenzaremos ya a explicar los algoritmos cuánticos que vamos a ver y su relación con la criptografía.

7.3. Algoritmo de Grover

El primer ámbito de la criptografía que vamos a recorrer son los ataques mediante el uso de fuerza bruta. Esto ya lo explicamos anteriormente cuando definimos los oráculos cuánticos en (**??**) y básicamente se resume en que, según el algoritmo clásico, hemos de ir comprobando registro a registro si la información contenida es la que buscamos. Esto tiene una complejidad de *O(N)* ya que, en el peor de los casos, la información que estamos buscando se encuentra en el último registro. Sin embargo, con el *algoritmo de Grover* **?** vamos a lograr reducir dicha complejidad hasta *O($\sqrt{N}$)*.

Este algoritmo consta de *n* qubits en el estado $|+\rangle$, lo cual denotaremos por $|+\rangle^{\otimes n}$, y el qubit $|y\rangle$ para poder aplicar el oráculo de fase, el cual se encontrará inicialmente en $|-\rangle$. Vamos a comenzar denotando todos estos estos qubits en $|+\rangle^{\otimes n}$ como $|s\rangle$:

$$|0\rangle^{\otimes n} \xrightarrow{H\otimes n} |+\rangle^{\otimes n}$$

$$|s\rangle = |+\rangle^{\otimes n} = \left(\frac{1}{\sqrt{2}}\right)^n (|0\rangle + |1\rangle)^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle$$

Y 2^n es el número total de registros que vamos a tener en nuestra base de datos, ya que *n* es el número de bits que tienen nuestras cadenas de datos. Es por esto que vamos a denotar $2^n = N$, quedando

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^n} |x\rangle \tag{7.3}$$

Entonces, el dato que estamos buscando será una de las posibles cadenas que estamos consultando. A este dato el cual es nuestro objetivo ya que es el que queremos encontrar, lo vamos a denotar como $|w\rangle$, y al resto de cadenas que son irrelevantes, $|i\rangle$. Esto lo podemos llevar a (**??**), y desarrollando la expresión, llegamos a

$$\begin{aligned} |s\rangle &= \frac{1}{\sqrt{N}} \left(|w\rangle + \sum_{i\neq w} |i\rangle \right) = \frac{1}{\sqrt{N}} |w\rangle + \frac{1}{\sqrt{N}} \sum_{i\neq w} |i\rangle = \\ &= \frac{1}{\sqrt{N}} |w\rangle + \sqrt{\frac{N-1}{N}} \frac{1}{\sqrt{N-1}} \sum_{i\neq w} |i\rangle = \frac{1}{\sqrt{N}} |w\rangle + \sqrt{\frac{N-1}{N}} |r\rangle \end{aligned} \tag{7.4}$$

De donde

$$|r\rangle = \frac{1}{\sqrt{N-1}} \sum_{i \neq w} |i\rangle$$

Siendo $|r\rangle$ una superposición de todos los estados $|i\rangle$ que no son la solución que estamos buscando. Además $|r\rangle$ es una superposición que está normalizada, ya que hemos dividido entre $\sqrt{N-1}$ al haber $N-1$ términos en el sumatorio. Sin embargo podemos desarollar la expresión (**??**) aún un poquito más, y es que si nos fijamos dicha expresión es muy similar a la descomposición de un vector en componentes ortogonales, las cuales son $|w\rangle$ y $|r\rangle$. Es por esto que podemos extrapolar dicha expresión a un plano de coordenadas en función de un ángulo θ, donde los ejes son $|w\rangle$ y $|r\rangle$:

$$|s\rangle = \frac{1}{\sqrt{N}} |w\rangle + \sqrt{\frac{N-1}{N}} |r\rangle = \sin\theta\, |w\rangle + \cos\theta\, |r\rangle \tag{7.5}$$

Con θ definido como

$$\sin\theta = \frac{1}{\sqrt{N}}, \qquad \cos\theta = \sqrt{\frac{N-1}{N}}$$

Lo cual es consistente con las entidades trigonométricas:

$$\sin^2\theta + \cos^2\theta = 1$$

$$\left(\frac{1}{\sqrt{N}}\right)^2 + \left(\sqrt{\frac{N-1}{N}}\right)^2 = \frac{1+N-1}{N} = 1$$

Entonces, podemos llevarnos todo esto al plano que acabamos de definir en función de $|w\rangle$ y $|r\rangle$:

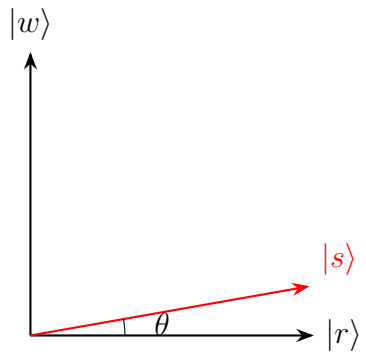


Figura 26: Representación de $|s\rangle$ en el plano

Ahora es cuando viene el momento de aplicar el oráculo de fase. Para ello necesitamos el qubit $|y\rangle$, el cual asumiremos que se encuentra directamente en $|-\rangle$. Entonces, aplicando el oráculo, obtenemos:

$$|s\rangle |-\rangle \xrightarrow{U_f} \left[(-1)^{f(x)} |s\rangle\right] |-\rangle = \left[(-1)^{f(x)} (\sin\theta |w\rangle + \cos\theta |r\rangle)\right] |-\rangle = \\ = \left((-1)^{f(x)} \sin\theta |w\rangle + (-1)^{f(x)} \cos\theta |r\rangle\right) |-\rangle$$

Y el valor de $f(x)$ sabemos que es un valor binario al ser una función booleana, y su valor es 1 cuando verificamos que el dato que estamos analizando es la solución que estamos buscando $|x\rangle = |w\rangle$, y 0 en caso contrario. Sabiendo esto, llegamos a

$$\left((-1)^1 \sin\theta |w\rangle + (-1)^0 \cos\theta |r\rangle\right) |-\rangle = (-\sin\theta |w\rangle + \cos\theta |r\rangle) |-\rangle$$

De donde $|s\rangle$ tras aplicar el oráculo de fase es

$$U_f |s\rangle = -\sin\theta |w\rangle + \cos\theta |r\rangle \tag{7.6}$$

Y esto en definitiva es una reflexión $U_f |s\rangle$ de $|s\rangle$ sobre $|r\rangle$:

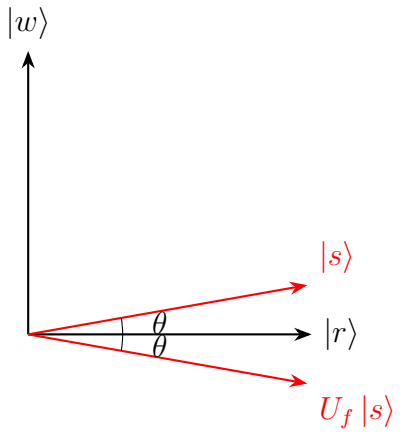


Figura 27: Reflexión $U_f |s\rangle$ en el plano

Ahora viene una parte muy interesante de este algoritmo. Para poder explicarla correctamente vamos a definir el operador de reflexión sobre $|s\rangle$, el cual es una puerta cuántica R_s que tiene la siguiente forma:

$$R_s = 2 |s\rangle \langle s| - I \tag{7.7}$$

Esta es la reflexión sobre $|s\rangle$. Para iluminarnos un poco más, si aplicamos esta puerta cuántica sobre $|s\rangle$ nos debería dar como resultado el propio estado $|s\rangle$

$$R_s \left|s\right\rangle = (2 \left|s\right\rangle \left\langle s\right| - I) \left|s\right\rangle = 2 \left|s\right\rangle \left\langle s|s\right\rangle - \left|s\right\rangle = 2 \left|s\right\rangle - \left|s\right\rangle = \left|s\right\rangle$$

Donde $\langle s|s\rangle = 1$, como vimos en (**??**). De la misma manera si aplicamos R_s sobre un vector un vector ortogonal a $|s\rangle$, $|s^\perp\rangle$, el resultado debería ser el mismo vector ortogonal $|s^\perp\rangle$ cambiado de signo, es decir $-|s^\perp\rangle$

$$R_s \left|s^\perp\right\rangle = (2 \left|s\right\rangle \left\langle s\right| - I) \left|s^\perp\right\rangle = 2 \left|s\right\rangle \left\langle s|s^\perp\right\rangle - \left|s^\perp\right\rangle = - \left|s^\perp\right\rangle$$

Por lo que ya podemos deducir de una manera intuitiva que efectivamente R_s es un operador de reflexión sobre $|s\rangle$. Nos queda demostrar que se trata de una puerta cuántica, y para ello vamos a ver que es una matriz unitaria, definiendo en primer lugar que el conjugado hermítico $R_s^\dagger$ es igual a R_s:

$$R_s^\dagger = (2 \left|s\right\rangle \left\langle s\right| - I)^\dagger = 2 \left|s\right\rangle \left\langle s\right| - I = R_s$$

Entonces ya podemos aplicar la expresión vista en (**??**), en la que vamos a ver que $R_s^\dagger R_s$ es la matriz identidad:

$$\begin{aligned} R_s^\dagger R_s = R_s R_s = (2 \left|s\right\rangle \left\langle s\right| - I) (2 \left|s\right\rangle \left\langle s\right| - I) = 4 \left|s\right\rangle \left\langle s|s\right\rangle \left\langle s\right| - 4 \left|s\right\rangle \left\langle s\right| + I = \\ = 4 \left|s\right\rangle \left\langle s\right| - 4 \left|s\right\rangle \left\langle s\right| + I = I \end{aligned}$$

Por lo que R_s es una puerta cuántica, como queríamos demostrar. Siguiendo con el algoritmo, vamos a aplicar el operador de reflexión R_s (**??**) sobre $U_f \left|s\right\rangle$, lo cual podemos ver el plano de la siguiente manera, denotado como $R_s U_f \left|s\right\rangle$:

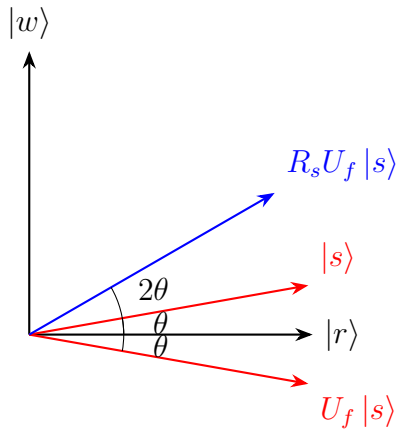


Figura 28: Reflexión $R_s U_f \left|s\right\rangle$ en el plano

Y si vamos aplicando el oráculo U_f y la reflexión R_s, seguimos rotando con un ángulo de 2θ hasta converger a la solución $|w\rangle$

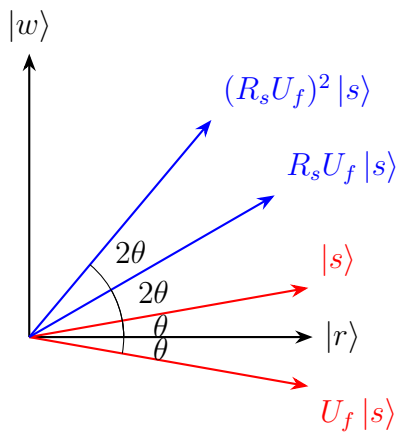


Figura 29: Segunda reflexión $(R_sU_f)^2\,|s\rangle$ en el plano

Vamos a suponer que tenemos que aplicar esta reflexión un total de t veces, podemos hallar este valor t en función de θ, de la siguiente manera, sabiendo que el ángulo definido entre $|w\rangle$ y $|r\rangle$ es $\frac{\pi}{2}$:

$$\theta + t\,(2\theta) = \frac{\pi}{2}$$

$$t\,(2\theta) = \frac{\pi}{2} - \theta$$

$$t = \frac{\pi}{4\theta} - \frac{1}{2}$$

Y a su vez θ depende del número total de registros *N* a los que estamos aplicando este algoritmo de fuerza bruta:

$$\theta = \sin^{-1}\left(\frac{1}{\sqrt{N}}\right) \approx \frac{1}{\sqrt{N}}$$

Esto lo hemos obtenido de (**??**), y hemos asumido que *N* es grande, obteniendo el resultado, que aunque sea una aproximación, es bastante firme y que no necesita depender de un valor tan elevado de *N*. Entonces, podemos concluir que el número de iteraciones o llamadas sobre el oráculo de fases es:

$$t \approx \frac{\pi}{4}\sqrt{N} - \frac{1}{2} \approx \frac{\pi}{4}\sqrt{N} \tag{7.8}$$

Lo cual es lo que estábamos buscando, determinándose una complejidad de $O(\sqrt{N})$ para este algoritmo ya que precisamos de un número dependiente de $\sqrt{N}$ llamadas al oráculo de fases, hasta converger en $|w\rangle$. Es con este algoritmo que conseguimos reducir la complejidad del algoritmo

de fuerza bruta clásico, y el salto de *N* a $\sqrt{N}$ llamadas al oráculo se denomina como *aceleración cuadrática*, y esto es posible gracias a un proceso iterativo, en el vamos aplicando el operador de reflexión R_s, con el que conseguimos una rotación en el espacio de Hilbert $\mathcal{H}$ hasta converger a la solución $|w\rangle$, lo cual es posible gracias a un oráculo muy eficiente y con el que aprovechamos las propiedades de la mecánica cuántica.

7.4. El Algoritmo de Shor

7.4.1. RSA

Clásicamente, el sistema que se suele seguir para encriptar y desencriptar mensajes se basa en claves públicas y privadas, con las que encriptamos y desencriptamos la información, respectivamente. Hay muchos sistemas basados en este principio, aunque nos vamos a centrar en el criptosistema *RSA*, el cual surgió en 1977 y se aprovecha de este enfoque.

Este sistema se basa en la factorización de números muy grandes, ya que este es uno de los problemas de los computadores convencionales al ser una tarea computacionalmente bastante costosa, resultando prácticamente imposible la factorización de ciertos números para un ordenador clásico. Este es un protocolo de vital importancia y que se usa hoy día, sin embargo, con el *algoritmo de Shor* (**??**) veremos que esta tarea, para un ordenador cuántico, es mucho menos costosa.

Aunque esto no es un algoritmo cuántico, está incluido en esta sección para explicar y comprender de una mejor manera el algoritmo de Shor, el cual veremos posteriormente. Imaginemos un emisor, Alice, que quiere enviar un mensaje a un receptor Bob. Para ello, Bob prepara una clave pública, la cual será accesible para todo el mundo y que permitirá a cualquier emisor enviarle un mensaje, y de la misma manera, Bob crea una clave privada, la cual es accesible únicamente por Bob, para desencriptar los mensajes de Alice.

El primer paso es escoger dos números primos, *p* y *q*, los cuales han de seguir ciertas condiciones, entre las cuales vamos a resumir que han de ser dos números primos con aproximadamente 1024 bits en lenguaje binario. Esto es, para que al multiplicarlos entre ellos, obtengamos un resultado *n* de 2048 bits, el cual será la primera de las dos claves públicas de Bob. Esto se rige en base al estándar RSA actual, en el cual se establece que para que nuestra información sea completamente segura, el producto de los dos números primos escogidos por Bob ha de tener 2048 bits en binario, para que sea un sistema inquebrantable por un ordenador clásico, aunque deje bastante que desear para un computador cuántico.

$$n = pq \tag{7.9}$$

A continuación vamos a establecer la segunda clave pública. Para ello calculamos

$$\phi = (p-1)(q-1) \tag{7.10}$$

Y posteriormente hemos de encontrar un entero *e* cuyo máximo común divisor con ϕ sea igual a 1, sto significa que *e* y ϕ son coprimos:

$$\gcd(e, \phi) = 1, \qquad e \in \mathbb{Z} \tag{7.11}$$

Hay muchos métodos que nos permiten obtener un valor de *e*, como el algoritmo de euclides. En definitiva, *e* es la segunda clave pública de Bob. Continuando con este protocolo, vamos a hallar la clave privada de Bob, la cual es

$$e \cdot d \equiv 1 \bmod \phi \tag{7.12}$$

Esta será nuestra clave privada *d*, cual multiplicada por una de las claves públicas *e*, da como resultado la unidad módulo ϕ. Esta clave *d* permitirá a Bob desencriptar cualquier mensaje encriptado por Alice, y será una clave muy segura ya que para hallar *d* hemos de conocer el valor de ϕ, el cual se estableció en (**??**) y que depende de dos números primos *p* y *q*, por lo que si queremos conocer el valor de *d*, es necesario aplicar un algoritmo de factorización, y los ordenadores clásicos en esta tarea son muy ineficientes.

Es ahora el momento en el que Alice envía un mensaje a Bob, el cual denotaremos como *M* y será un mensaje binario menor que la primera clave pública de Bob, *N*, por lo que $0 < M < n$. Para enviar el mensaje cifrado a Bob, utiliza sus claves públicas *n* y *e* de manera que el mensaje codificado *C* queda como

$$C = M^e \bmod n$$

Y, una vez el mensaje es enviado cifrado a Bob, este solo tiene que desencriptarlo utilizando su clave privada *d*, a través del siguiente proceso:

$$C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n = M^1 \bmod n = M$$

Por lo que Bob ha recibido el mensaje de Alice correctamente. Este protocolo nos ayuda a entender de una mejor manera por qué un algoritmo de factorización eficiente es tan importante, ya que podríamos hallar el valor de ϕ muy rápidamente, y por lo tanto, tendríamos la clave privada *d* en nuestro poder, descifrando cualquier información enviada a Bob. Vamos a ver una forma de romper esta factorización con el algoritmo de Shor (**??**), el cual vamos a ver a continuación en el siguiente apartado.

7.4.2. Algoritmo de Shor

En 1994 llegó una revolución para la criptografía cuántica. Fue gracias a *Peter Shor* y a su revolucionario algoritmo cuántico **?** con el que se rompen las bases de la criptografía pública y privada mediante la mejora del algoritmo de factorización por números primos clásico. Es por esto que ciertos sistemas, como el protocolo *RSA* (**??**), ya no son tan robustos frente a un ordenador cuántico. Para comenzar con el algoritmo, se parte de la tarea de factorizar el entero N.

Para este algoritmo se van a aplicar muchas de las condiciones vistas en otros métodos de cifrado clásicos, como *RSA* (**??**) en el que se explicó el máximo común divisor *gcd*, expresiones modulares, y se estudió con un leve nivel de detalle las propiedades de la teoría de números aplicadas a los números coprimos. Es en esto, y con la ayuda de ciertos algoritmos cuánticos, en lo que se basa el algoritmo de Shor para factorizar un $N \in \mathbb{Z}$ en dos números primos *p* y *q*. Según el libro escrito por *Thomas G. Wong* **?**, este proceso puede dividirse en tres partes:

1. Escogemos un número $a \in \mathbb{Z}$ tal que $1 < a < N$, siendo N el número que deseamos factorizar. A continuación calculamos el máximo común divisor entre *a* y *N* y, si $gcd(a, N) \neq 1$, esto quiere decir que *a* y *N* comparten un divisor no trivial, por lo que uno de los factores que estamos buscando es $p = gcd(a, N)$, y el otro lo podemos obtener en base a este factor, ya que este es $q = N/p$, y finalizaría el algoritmo. Si por el contrario $gcd(a, N) = 1$ quiere decir que *a* y *N* son coprimos, por lo que no comparten ningún divisor en común. En este caso no podemos encontrar los factores directamente y hemos de proceder con el siguiente paso del algoritmo.

   En definitiva el objetivo de este primer paso es inicializar *a* y ver si se da la casualidad de que este número comparta algún divisor no trivial con *N*, lo cual no suele ser algo común ya que se asume que *N* es un número muy grande, y por tanto no podemos aplicar ningún método clásico para obtener *a* de manera que $gcd(a, N) \neq 1$. Lo más normal es que tengamos que recurrir al siguiente paso.

2. Encontrar el periodo modular *r* de a^x mod N. Supongamos que *a* tiene un valor de 7, y *N* = *15*. La variable *x* toma valores $x \in \{0, 1, 2, \cdots\}$ de manera que

$$7^0 \text{ mod} 15 = 1 \text{ mod } 15 = 1$$

$$7^1 \text{ mod} 15 = 7 \text{ mod } 15 = 7$$

$$7^2 \text{ mod} 15 = 49 \text{ mod } 15 = 4$$

$$7^3 \text{ mod} 15 = 354 \text{ mod } 15 = 13$$

$$7^4 \text{ mod} 15 = 2401 \text{ mod } 15 = 1$$

Y si seguimos incrementando el valor de *x*, este ciclo se repite, ya que 7 y 15 son coprimos. El periodo *r* es el menor entero positivo (mayor que cero) con el que se verifica esta secuencia, por lo que en este caso, el periodo es *r = 4* como podemos ver. Esta operación resulta ser muy ineficiente para un ordenador clásico, pero bastante más eficiente para un ordenador que se apoye en las leyes de la mecánica cuántica, y el algoritmo cuántico que resuelve esta operación necesita estimar el autovalor de ciertos autovectores, lo cual cubrimos en (**??**).

Una vez hemos averiguado el valor de *r*, este ha de cumplir una serie de condiciones. La primera es que *r* ha de ser un número par, y la segunda es $a^{r/2} \bmod N \neq N - 1$. En el caso incumplirse alguna de estas restricciones, volvemos al primer paso, escogemos un valor distinto para *a* y repetimos el proceso desde el principio.

3. A continuación explicamos el último paso, con el cual vamos a obtener los factores primos *p* y *q* de *N*. En primer lugar, necesitamos expresar *r* en función de un múltiplo de *N*, esto lo podemos conseguir muy fácilmente

$$a^r = 1 \bmod N$$
$$a^r - 1 = 0 \bmod N$$
$$a^r - 1 = kN$$

Donde $k \in \mathbb{Z}$ es un múltiplo de *N*. No obstante el objetivo de este problema es hallar *p* y *q*, por lo que expresamos *N* en función de ellos, y además, podemos factorizar el término $a^r - 1$ como sigue

$$\left(a^{r/2} + 1\right)\left(a^{r/2} - 1\right) = kpq$$

Esto lo podemos hacer porque hemos definido anteriormente en el segundo paso que *r* ha de ser un número par, para que los factores $a^{r/2} + 1$ y $a^{r/2} - 1$ sean números enteros, ya que si no pertenecen a este conjunto, sería mucho más difícil, por no decir imposible, esta factorización. Llegados a este punto, *p* o *q* deben estar incluidos en al menos uno de los términos $a^{r/2} + 1$ o $a^{r/2} - 1$, lo que nos conduce a estas tres posibilidades:

$$\begin{aligned}
\underbrace{\left(a^{r/2}+1\right)}_{c}\underbrace{\left(a^{r/2}-1\right)}_{dpq} &= kpq \\
\underbrace{\left(a^{r/2}+1\right)}_{cp}\underbrace{\left(a^{r/2}-1\right)}_{dq} &= kpq \\
\underbrace{\left(a^{r/2}+1\right)}_{cpq}\underbrace{\left(a^{r/2}-1\right)}_{d} &= kpq
\end{aligned} \tag{7.13}$$

Donde $k = cd$. Sin embargo, el primer y el tercer caso son imposibles ya que $a^{r/2}+1$ y $a^{r/2}-1$ no son en ningún caso múltiplos de *N*. Esto es posible gracias a las condiciones definidas en el segundo paso, con las cuales obtenemos que $a^{r/2} \neq N-1 \bmod N$ además de $a^{r/2} \neq 1 \bmod N$ gracias a la definición del periodo *r*. Es por esto que descartamos la primera y tercera opción, quedándonos únicamente con (**??**):

$$\underbrace{\left(a^{r/2}+1\right)}_{cp}\underbrace{\left(a^{r/2}-1\right)}_{dq} = kpq$$

Entonces, ambos términos $a^{r/2}+1$ y $a^{r/2}-1$ contienen un factor no trivial de *N*, y los podemos calcular con el máximo común divisor (*gcd*):

$$\begin{aligned}
p &= \gcd(a^{r/2}+1, N) \\
q &= \gcd(a^{r/2}+1, N)
\end{aligned}$$

Obteniendo así la descomposición de *N* en los factores primos *p* y *q*. Este algoritmo es posible gracias a la obtención del periodo *r*, ya que este proceso es exponencialmente más rápido mediante un ordenador cuántico que con un computador clásico, lo que muestra muy claramente el poder de la computación cuántica en la rama de la seguridad informática, surgiendo la necesidad de nuevos protocolos de seguridad para este campo.

7.4.3. Estimación de Autovalores

Una de las partes clave del algoritmo de Shor es determinar el periodo de una expresión modular (**??**), y para ello necesitamos obtener los autovalores, los cuales tienen la forma $e^{2\pi i s/r}$, de un determinado operador el cual denotaremos *U* ya que en efecto se trata de una puerta cuántica.

Ya se estableció la definición de autovector y autovalor en el tercer postulado (**??**), en el que se observa que si aplicamos un operador $\hat{A}$ sobre un cierto estado $|\psi\rangle$, el resultado es el mismo estado $|\psi\rangle$ multiplicado por un escalar $\lambda \in \mathbb{R}$. A diferencia de esto, *U* es una puerta cuántica, lo que quiere decir que es unitario (**??**) y por lo tanto sus autovalores son complejos de módulo 1:

$$U|\nu\rangle = e^{i\theta}|\nu\rangle, \qquad \theta \in \mathbb{R} \tag{7.14}$$

Donde el autovector $|\nu\rangle$ es un vector columna de dimensión $N = 2^n$, ya que se asume que estamos en un sistema de *n* qubits, donde de la misma manera *U* tiene dimensión $N \times N$. Adicionalmente, vamos a tener *m* qubits inicializados en el estado $|0\rangle$, por lo que partimos del siguiente estado:

$$|0\rangle^{\otimes m}|\nu\rangle$$

Donde vamos a denotar $|0\rangle^{\otimes m}$ como *registro de autovalores*, que finalmente será una aproximación de *m* bits del autovalor asociado al autovector, y $|\nu\rangle$ como *registro de autoestados*. Para obtener esta aproximación en primer lugar aplicamos una puerta de Hadamard *H* sobre el registro de autovalores:

$$\begin{aligned}
|0\rangle^{\otimes m}|\nu\rangle = |000\cdots 0\rangle|\nu\rangle = |+++\cdots+\rangle|\nu\rangle = \\
= \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\cdots\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|\nu\rangle = \\
= \frac{1}{\sqrt{2^m}}(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)\cdots(|0\rangle+|1\rangle)|\nu\rangle
\end{aligned}$$

A continuación aplicamos una puerta *U* controlada (*controlled-U*) sobre el primer estado del registro de autovalores, esto se resume en la aplicación de la puerta *U*, definida en (**??**), sobre este primer estado, adquiriendo una fase de $e^{i\theta}$ cuando el qubit de control es $|1\rangle$:

$$\frac{1}{\sqrt{2^m}}(|0\rangle+|1\rangle)\cdots(|0\rangle+|1\rangle)\left(|0\rangle+e^{i\theta}|1\rangle\right)|\nu\rangle$$

Y seguiríamos aplicando la puerta U^2 controlada sobre el segundo qubit del registro de autovalores, por lo que este adquiere una fase de $e^{2i\theta}$, y sucesivamente seguiríamos hasta llegar al último estado del registro de autovalores, para el cual aplicamos U^{2m-1}:

$$\frac{1}{\sqrt{2^m}}\left(|0\rangle+e^{(2^{m-1})i\theta}|1\rangle\right)\cdots\left(|0\rangle+e^{2i\theta}|1\rangle\right)\left(|0\rangle+e^{i\theta}|1\rangle\right)|\nu\rangle$$

Ahora vamos a modificar esta expresión buscando la *transformada cuántica de Fourier* (QFT). Para ello, hacemos el cambio de variable $\theta = 2\pi j$ en el estado anterior, obteniendo

$$\frac{1}{\sqrt{2^m}}\left(|0\rangle+e^{2\pi i 2^{m-1}j}|1\rangle\right)\cdots\left(|0\rangle+e^{2\pi i 4j}|1\rangle\right)\left(|0\rangle+e^{2\pi i j}|1\rangle\right)|\nu\rangle$$

Con $0 \leq j < 1$, ya que $0 \leq \theta < 2\pi$. Como $j < 1$, vamos a expresarlo como una cadena binaria de dimensión *m* cuya forma es $0, j_1 j_2 \cdots j_m$, y aplicándolo a nuestro estado, queda lo siguiente:

$$\frac{1}{\sqrt{2^m}} \left(|0\rangle + e^{2\pi i(j_1 j_2 \cdots j_{m-1}, j_m)} |1\rangle\right) \cdots \left(|0\rangle + e^{2\pi i(j_1, j_2 \cdots j_m)} |1\rangle\right) \left(|0\rangle + e^{2\pi i(0, j_1 \cdots j_m)} |1\rangle\right) |\nu\rangle \quad (7.15)$$

Y los términos a la izquierda de la coma los podemos ignorar, ya que $e^{2\pi i} = 1$. Por ejemplo, supongamos que *j* tiene un valor de $j = 2, 1$. Aplicando las propiedades de las potencias tenemos que

$$e^{2\pi i(2,1)} = e^{2\pi i(1+1+0,1)} = e^{2\pi i} e^{2\pi i} e^{2\pi i(0,1)} = e^{2\pi i(0,1)}$$

Entonces, la expresión (**??**) queda de la siguiente manera:

$$\frac{1}{\sqrt{2^m}} \left(|0\rangle + e^{2\pi i(0, j_m)} |1\rangle\right) \cdots \left(|0\rangle + e^{2\pi i(0, j_2 \cdots j_m)} |1\rangle\right) \left(|0\rangle + e^{2\pi i(0, j_1 \cdots j_m)} |1\rangle\right) |\nu\rangle \quad (7.16)$$

Esto es exactamente la *transformada cuántica de Fourier* de $|j_1 j_2 \cdots j_m\rangle$, y podemos hallar el término $|j_1 j_2 \cdots j_m\rangle$ aplicando la *transformada de Fourier inversa* sobre el registro de autovalores, obteniendo el siguiente resultado:

$$|j_1 j_2 \cdots j_m\rangle |\nu\rangle$$

Y a continuación medimos los distintos qubits, obteniendo $j_1 j_2 \cdots j_m$. Entonces, el valor de *j* es

$$j = 0, j_1 j_2 \cdots j_m = \frac{j_1}{2} + \frac{j_2}{4} + \cdots + \frac{j_m}{2^m}$$

Lo cual simplemente es un proceso clásico para pasar de la base binaria a la base decimal. Con esto ya sabemos el valor de *j* y por lo tanto de θ ya que $\theta = 2\pi j$, por lo que hemos hallado el autovalor final $e^{i\theta}$ con *m* bits de precisión, para lo cual hemos precisado de *m* puertas de Hadamard *H* y *m* puertas U^p controladas, además de la transformada de Fourier inversa. Esto hace que la complejidad de este algoritmo sea de $O(m^2)$, ya que aplicar las puertas de Hadamard tiene una complejidad lineal a la misma vez que al aplicar las puertas U^p controladas, sin embargo, la transformada de fourier inversa es cuadŕatica $O(m^2)$, por lo que la complejidad total de este algoritmo es también cuadrática $O(m^2)$. Esto es un gran avance sobre el algoritmo clásico, cuya complejidad es de $O(N)$, lo cual es una complejidad exponencial al ser $N = 2^n$.

7.4.4. El Periodo de una Expresión Modular

CAPÍTULO

8

Estado del Arte

La empresa líder en computación cuántica es, hasta la fecha y sin duda alguna, IBM, la cual ofrece a nuestra disposición distintas páginas web en las que podemos ejecutar circuitos cuánticos y ver su comportamiento de la manera más real posible. El desarrollo del circuito se hace a través de *Python* mediante su librería destinada a la computación cuántica *Qiskit*, y una vez lo hemos completado, tenemos distintas opciones de configuración para la ejecución del circuito.

Por otra parte, si la programación en *Python* no es nuestro punto fuerte, tenemos a nuestra disposición la interfaz gráfica para el desarrollo de circuitos cuánticos de IBM, Quantum Composer. Con esta herramiento web podemos crear circuitos cuánticos con el sistema *drag and drop* sobre puertas cuánticas o qubits, de manera que se genera el correspondiente código equivalente al circuito cuántico creado y se ejecuta en un emulador o sistema cuántico, además de que podemos visualizar el estado y la fase correspondiente en la *esfera de Bloch*, y un histograma con las probabilidades de los estados a los que puede colapsar el circuito.

De la misma manera que IBM, Amazon ha desarrollado su propia plataforma para la ejecución de circuitos cuánticos, la cual está basada nuevamente en *Python*, con la diferencia de que usamos la librería relacionada con su propio producto, *Braket*. Este producto incluye ciertas ventajas sobre el producto de IBM, como que permite la combinación de computación cuántica y clásica, aunque como vimos anteriormente, todo circuito clásico se puede expresar como un circuito cuántico. Tambień podemos encontrar productos de otras empresas para la simulación y ejecución de circuitos cuánticos, como Google o Azure, pero no dejan de ser, junto con el producto de Amazon, competidores de la solución presentada por IBM, la cual fue la primera en salir públicamente al mercado con su plataforma IBM Quantum Experience, lanzada en *2016*.

No obstante, la computación cuántica tiene muchos problemas, relacionados precisamente con la naturaleza de las partículas subatómicas, las cuales son muy sensibles al ruido causado por el exterior, lo que hace que se produzcan muchos fallos en los circuitos y que, por lo tanto, los computadores

cuánticos actuales no sean tolerantes a fallos (*fault-tolerant*), de manera que los errores se acumulan muy rápidamente y sin la capacidad de ser revertidos con la tecnología cuántica hasta el momento. Sin embargo, Microsoft ha hecho un hallazgo que puede convertirse en la revolución del siglo, mucho más allá que el desarrollo de la inteligencia artificial en estos últimos años.

Microsoft ha anunciado el lanzamiento de *Majorana 1*, la primera unidad de procesamiento cuántico (QPU) con qubits topológicos, qubits que almacenan informacion cuántica de manera más estable y robusta, de manera que es mucho menos susceptible a errores cuánticos, que es uno de los principales problemas de este campo de la física y la tecnología, siendo una de las principales motivaciones para Microsoft construir el primer ordenador cuántico con tolerancia a fallos en los próximos años.

La clave de este gran avance ha sido el desarrollo de materiales topoconductores, los cuales permiten la superconductividad topológica, un estado de la materia que hasta este descubrimiento solo existía en la teoría. Este tipo de materiales se crean con arseniuro de indio y aluminio, de manera que cuando se enfrían prácticamente al cero aboluto y se sintonizan con campos magnéticos, se forman nanocables superconductores topológicos con modos cero de Majorana (MZM) en sus extremos, de manera que aumentan la estabilidad y se reducen los errores en comparación con los qubits tradicionales.

Así es como se ha desarrollado el primer qubit topológico del mundo, y se plantea tener un chip cuántico con más de un millón de qubits y tolerante a fallos en unos años, y no en unas décadas como se planteaba anteriormente, dando un gran paso en la computación cuántica práctica y probablemente uno de los mayores hitos de este campo.

Bibliografía

"La radiación del cuerpo negro." Física Cuántica, 2014. [En línea]. Disponible: https://www.fisicacuantica.es/la-radiacion-del-cuerpo-negro/.

"Distribución de la energía." WebLab Deusto, 2013. [En línea]. Disponible: https://weblab.deusto.es/olarex/cd/kaernten/BBR_ES_new_27.09.2013/distribucin_de_la_energa.html.

J. Pastor, "Física cuántica: El experimento de la doble rendija." DCIencia. [En línea]. Disponible: https://www.dciencia.es/fisica-cuantica-el-experimento-de-la-doble-rendija/.

Wikipedia contributors, "Esfera de bloch," 2023. [En línea]. Disponible: https://es.wikipedia.org/wiki/Esfera_de_Bloch.

A. K. Ekert, "Quantum cryptography based on bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug 1991.

A. S. Galante, "Desigualdades de bell: Influencia de la decoherencia y experimentos de prueba de concepto." Universidad de Valladolid, 2023. Disponible: https://uvadoc.uva.es/handle/10324/63238.

L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," *Phys. Rev. Lett.*, vol. 79, pp. 325–328, Jul 1997.

P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pp. 124–134, 1994.

T. G. Wong, *Introduction to Classical and Quantum Computing*. Rooted Grove, 2022.

S. R. de Munck, "Trabajo fin de grado en matemáticas." Universidad Autónoma de Madrid, Jun 2017. Disponible: https://matematicas.uam.es/~fernando.chamizo/supervision/TFG/past/memoirs/TFG_silvia_rodriguez.pdf.

S. C. Carriles, "Investigación sobre la computación cuántica." Universidad de Alicante, May 2022. Disponible: https://rua.ua.es/dspace/handle/10045/124691.

D. A. M. Muñoz, "La ecuación de schrödinger." Universidad de Murcia, 2021. Disponible: https://webs.um.es/gustavo.garrigos/tfg/MarinMunoz_Diego_TFG_julio2021.pdf.

P. R. Puertas, "Introducción a la computación cuántica y sus aplicaciones." Universidad de Cádiz, Jun 2021. Disponible: https://rodin.uca.es/bitstream/handle/10498/27218/tfg_pablo.pdf.

L. S. Polo, "El hamiltoniano de la estructura fina." Universidad Autónoma de Madrid, 2022. Disponible: https://matematicas.uam.es/~fernando.chamizo/supervision/TFG/past/memoirs/TFG_luis_sanchez.pdf.

M. P. de Paz, "Operadores no acotados en espacios de hilbert y su relación con la mecánica cuántica." Universidad de Sevilla, Jun 2020. Disponible: https://idus.us.es/server/api/core/bitstreams/4c49766a-cdfc-4d72-9acf-f62761db63fb/content.

C. Mielgo, "Computación cuántica básica con Álgebra lineal." Universidad Autónoma de Madrid, 2024. Disponible: https://matematicas.uam.es/~fernando.chamizo/supervision/TFG/past/memoirs/TFG_claudia_mielgo.pdf.

M. del Mar Villasana Alcaraz, "Introducción a la computación cuántica." Universidad de Almería, Jul 2020. Disponible: https://repositorio.ual.es/bitstream/handle/10835/9810/VILLASANA%20ALCARAZ%2C%20MARIA%20DEL%20MAR.pdf.

R. G. Rivas, "Computación cuántica: Implementación y análisis teórico de los experimentos chsh y hidden matching para probar la potencia de los ordenadores cuánticos." Universidad Politécnica de Madrid, 2021. Disponible: https://oa.upm.es/69234/1/TFG_ROBERTO_GONZALEZ_RIVAS.pdf.

D. L. E. Córdoba, "Algoritmos cuánticos." Universidad de Zaragoza, 2018. Disponible: https://zaguan.unizar.es/record/76803/files/TAZ-TFG-2018-3072.pdf.

G. Fernández, "Teoría cuántica. radiación del cuerpo negro. la hipótesis de planck." Química Física, 2015. [En línea]. Disponible: https://www.quimicafisica.com/teoria-cuantica/la-radiacion-del-cuerpo-negro.html.

G. Fernández, "Teoría cuántica. el efecto fotoeléctrico." Química Física, 2015. [En línea]. Disponible: https://www.quimicafisica.com/teoria-cuantica/el-efecto-fotoelectrico.html.

"Momento lineal." FísicaLab. [En línea]. Disponible: https://www.fisicalab.com/apartado/cantidad-movimiento#google_vignette.

I. G. Sevillano, "Frames en espacios de hilbert." Universidad de Valladolid, Jun 2022. Disponible: https://uvadoc.uva.es/bitstream/handle/10324/57982/TFG-G5986.pdf?sequence=1.

J. A. J. Martínez, "Geometría de un espacio de hilbert aplicada a las series de tiempo." Universidad de San Carlos de Guatemala, 2020. Disponible: https://ecfm.usac.edu.gt/sites/default/files/2021-06/Joel%20Armando%20Ju%C3%A1rez.pdf.

C. Nayak, "Microsoft presenta majorana 1, el primer procesador cuántico del mundo impulsado por qubits topológicos." Microsoft News, 2025. Disponible: https://news.microsoft.com/source/latam/noticias-de-microsoft/microsoft-presenta-majorana-1-el-primer-procesador-cuantico-del-mundo-impulsado-por-qubits-topologicos/.

A. M. Ruiz, "Una demostración de la regla de born desde la interpretación de muchos mundos." Universidad de Valladolid, 2024. Disponible: https://uvadoc.uva.es/bitstream/handle/10324/70993/TFG-G6793.pdf.

C. G. Serván, "Introducción a la mecánica cuántica." Universidad de Sevilla, 2017. Disponible: https://idus.us.es/server/api/core/bitstreams/e6e34b3a-fc74-4043-98ae-8244902b96e4/content.

S. Laverde S. N. González Estudio comparativo y evaluación de utilidad de protocolos de transmisión de datos usando criptografía cuántica. [online]. Available in: http://hdl.handle.net/10554/21443 https://www.academia.edu/102791510/Análisis_de_algoritmos_criptográficos_clásicos_vs_algoritmos_cuánticos