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.

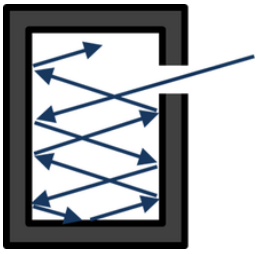

Figura 1: Ilustración del cuerpo negro

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:

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 (2):

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

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.

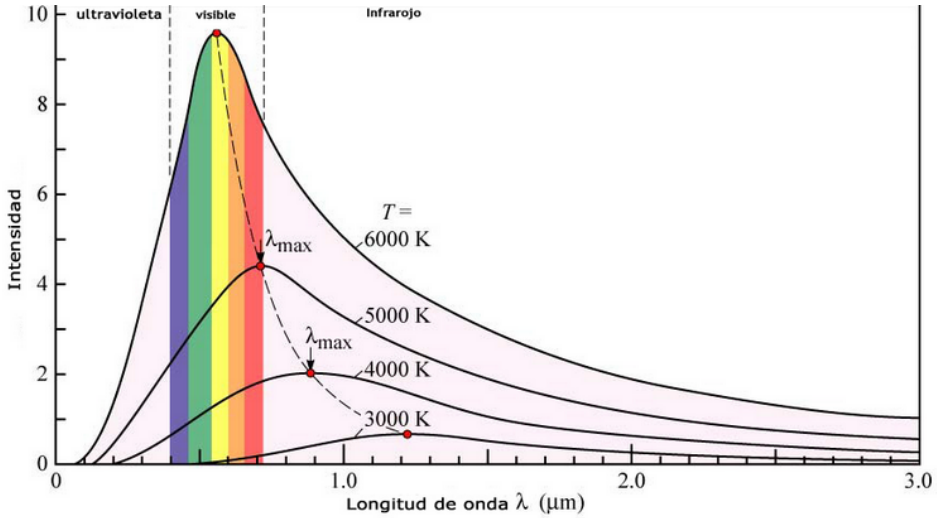

Figura 2: Catástrofe del ultravioleta

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 (1.1), 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* (1.1), además de conocer la *energía cinética* de una partícula, podemos desarrollar la expresión (1.3):

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

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.

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,

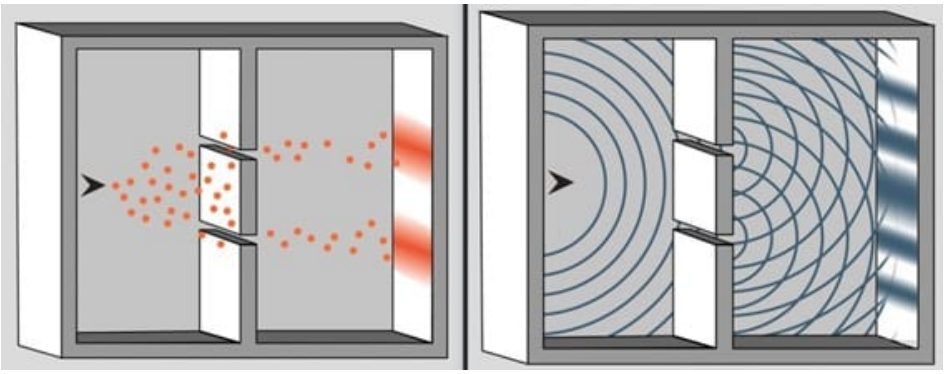

Figura 3: Experimento de la doble rendija

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 (1.8):

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

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

Ecuación de Schrödinguer

2.1. Obtención de la Ecuación de Schrödinguer

Todas las ideas vistas anteriormente, la función de onda (1.5), la superposición cuántica (1.7) y la interpretacion probabilística de la función de onda (1.8) 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 (1.5).
En primer lugar, derivamos (1.5) 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 (1.5), 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 (1.5) 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 (2.1), 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 (2.2). Para simplificar cálculos, vamos a suponer que la energía potencial $V(x)$ en (2.2) 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 (2.2) 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

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

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

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

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

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 (2.3):

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

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 (2.4) 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

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

La ecuación (2.5) 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.

2.3. 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 (2.4) 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

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

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

$$\|\psi\| = \sqrt{\langle \psi \mid \psi\rangle} \qquad \in \mathbb{R} \geq 0 \tag{2.7}$$

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:

$$\| \langle \phi \mid \psi \rangle \|^2 \leq \|\phi\|^2 \|\psi\|^2 \tag{2.8}$$

Al complirse esta expresión, el producto interno está bien definido, de donde obtenemos la norma como ya vimos en (2.7), 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

$$B = \{|e_j\rangle\}_{j=1}^{N} \tag{2.9}$$

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

$$\langle e_1 | e_2 \rangle = \delta_{e_1, e_2}, \qquad \forall \ |e_1\rangle, |e_2\rangle \in B \tag{2.10}$$

$$\|e_j\| = 1, \qquad \forall \ |e_j\rangle \in B \tag{2.11}$$

Donde $\delta_{n,m}$ en (2.10) es la función *delta de Kronecker*, que se define como

$$\delta_{i,j} = \begin{cases} 1, & \text{si } i = j, \\ 0, & \text{si } i \neq j \end{cases} \tag{2.12}$$

Así, el producto escalar de dos vectores de una base ortonormal siempre va a ser cero, y el producto escalar de un vector consigo mismo es la unidad

$$\langle e_1 | e_2 \rangle = 0, \qquad \forall \, e_1, e_2 \in B \tag{2.13}$$

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

$$|\psi\rangle = \sum_{j=1}^{N} c_j |e_j\rangle, \qquad \forall \ |\psi\rangle \in \mathcal{H} \quad \text{y} \quad \forall c_j \in \mathbb{C} \tag{2.14}$$

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 (1.7), 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 †:

$$(|\phi\rangle)^\dagger = \langle\phi|$$

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

$$B^* = \{\langle e_i|\}_{i=1}^N \tag{2.15}$$

mediante la que, de la misma manera que con la base B definida en (2.9) 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^*:

$$\langle\phi| = \sum_{i=1}^N d_i^* \langle e_i|, \qquad \forall\ \langle\phi| \in B^* \quad y \quad \forall\, c_i^* \in \mathbb{C} \tag{2.16}$$

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 $\mathcal{H}$

$$\langle\phi \mid \psi\rangle = |\phi\rangle \cdot |\psi\rangle = \left(\sum_{i=1}^N d_i^* \langle e_i|\right)\left(\sum_{j=1}^N c_j |e_j\rangle\right) = \sum_{i=1}^N\sum_{j=1}^N d_i^*\ c_j\ \langle e_i \mid e_j\rangle = \sum_{i=1}^N\sum_{j=1}^N d_i^*\ c_j\ \delta_{e_i,e_j} = \sum_{i=1}^N d_i^*\ c_i$$

$$\boxed{\langle\phi \mid \psi\rangle = \sum_{i=1}^N d_i^*\ c_i} \tag{2.17}$$

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

$$\|\psi\|^2 = \langle\psi|\psi\rangle = \sum_{i=1}^N d_i^* c_i = \sum_{i=1}^N \|c_i\|^2 \geq 0, \qquad \forall\psi \in \mathcal{H} \tag{2.18}$$

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

2.4. 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 (1.2). 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 (2.14) 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:

$$|\varphi\rangle = \sum_{n=1}^{N} c_n |n\rangle , \qquad \forall |\varphi\rangle \in \mathcal{H}, \quad \forall |n\rangle \in \{|e_n\rangle\}, \quad c_n \in \mathbb{C}$$

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.*

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:

$$\hat{A} |\psi\rangle = \lambda |\psi\rangle , \qquad \lambda \in \mathbb{R} \tag{2.19}$$

Y podemos verificar que $\lambda \in \mathbb{R}$, partiendo de (2.19) 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

$$\langle\psi_i|\psi_j\rangle = 0 \tag{2.20}$$

Son ortogonales. Entonces, podemos concluir que, en un espacio de Hilbert $\mathcal{H}$, un operador hermítico $\hat{A}$ tiene N autovectores ψ_i 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, por lo que hemos demostrado que un operador hermítico siempre va a ser diagonalizable.

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

$$\mathcal{P}(a_n) = \| \langle a_n|\varphi\rangle \|^2 \tag{2.21}$$

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

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

$$|\varphi\rangle \xrightarrow{a_n} \frac{P_n\,|\varphi\rangle}{\sqrt{\langle\varphi|\,P_n\,|\varphi\rangle}} \tag{2.22}$$

Donde P_n es el operador proyección sobre el subespacio asociado a a_n.

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

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = H(t)|\psi(t)\rangle, \tag{2.23}$$

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

2.4.1. El Espacio de Hilbert en Dimensión Infinita

CAPÍTULO

3

Álgebra Lineal y Puertas Cuánticas

3.1. Estados Cuánticos

3.1.1. Esfera de Bloch

3.2. Producto Escalar

3.2.1. Ortonormalidad

3.3. Puertas Cuánticas

3.4. Producto Tensorial

CAPÍTULO

4

Errores Cuánticos

4.1. Decoherencia

4.2. Shor Code

CAPÍTULO

5

Entrelazamiento Cuántico

5.1. Estados de Bell

5.2. Codificación Superdensa

CAPÍTULO

6

Teleportación Cuántica

CAPÍTULO

7

Algoritmos Cuánticos

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.

CAPÍTULO

9

Bibliografía

TFG Silvia Rodriguez
https://matematicas.uam.es/~fernando.chamizo/supervision/TFG/past/memoirs/TFG_silvia_rodriguez.pdf

Investigacion Computacion Cuantica –>Seguridad informatica, redes informaticas, IA, etc.
https://rua.ua.es/dspace/bitstream/10045/124691/1/Estudio_de_la_computacion_cuantica_en_los_diferent_Claramunt_Carriles_Sergio.pdf

Universidad de Murcia –>Schrodinguer, Hamiltoniano, Oscilador armonico, Atomo de Hidrogeno
https://webs.um.es/gustavo.garrigos/tfg/MarinMunoz_Diego_TFG_julio2021.pdf

TFG Pablo –>Algoritmo de Grover y otros algoritmos
https://rodin.uca.es/bitstream/handle/10498/27218/tfg_pablo.pdf?sequence=1&isAllowed=y

TFM –>Schrodinguer e interpretacion probabilistica de la funcion de onda
https://repositorioinstitucional.buap.mx/server/api/core/bitstreams/fb9bfe95-7945-404d-a3c5content

Universidad Autonoma de Madrid –>Interpretacion probabilistica de la funcion de onda e introduccion al atomo de hidrogeno
https://matematicas.uam.es/~fernando.chamizo/supervision/TFG/past/memoirs/TFG_luis_sanchez.pdf

TFG –>Espacios de Hilbert y su relacion con la mecanica cuantica
https://idus.us.es/server/api/core/bitstreams/4c49766a-cdfc-4d72-9acf-f62761db63fb/content

Claudia Mielgo –>El sistema cuantico es un espacio de Hilbert, y funciones de onda
https://matematicas.uam.es/~fernando.chamizo/supervision/TFG/past/memoirs/TFG_claudia_mielgo.pdf

Algebra Lineal –>Algebra lineal, espacios de Hilbert y criptografia cuantica
https://repositorio.ual.es/bitstream/handle/10835/9810/VILLASANA%20ALCARAZ%2C%20MARIA%20DEL%20MAR.pdf

Roberto Gonzalez –>Sistema Bineario e introduccion a los qubits
https://oa.upm.es/69234/1/TFG_ROBERTO_GONZALEZ_RIVAS.pdf

Por que un ordenador cuantico?
https://zaguan.unizar.es/record/76803/files/TAZ-TFG-2018-3072.pdf

Radiacion del cuerpo negro
https://www.fisicacuantica.es/la-radiacion-del-cuerpo-negro/

https://weblab.deusto.es/olarex/cd/kaernten/BBR_ES_new_27.09.2013/distribucin_de_la_energa.html

https://www.quimicafisica.com/teoria-cuantica/la-radiacion-del-cuerpo-negro.html

Efecto Fotoeléctrico
https://es.khanacademy.org/science/ap-chemistry/electronic-structure-of-atoms-ap/bohr-model-hydrogen-ap/a/photoelectric-effect

https://www.quimicafisica.com/teoria-cuantica/el-efecto-fotoelectrico.html

Experimento de la Doble Rendija
https://www.fisicalab.com/apartado/cantidad-movimiento#google_vignette

https://www.dciencia.es/fisica-cuantica-el-experimento-de-la-doble-rendija/

https://mecanicosvalencia.es/max-born-mecanica-cuantica/

Espacios de Hilbert. El concepto de espacio de Hilbert es una generalización del concepto de espacio euclídeo.
https://uvadoc.uva.es/bitstream/handle/10324/57982/TFG-G5986.pdf?sequence=1

https://ecfm.usac.edu.gt/sites/default/files/2021-06/Joel%20Armando%20Ju%C3%A1rez.pdf

https://repositorio.ual.es/bitstream/handle/10835/9810/VILLASANA%20ALCARAZ%2C%20MARIA%20DEL%20MAR.pdf

Videos espacios de Hilbert
https://www.youtube.com/watch?v=ZfZ39YpHZE0

https://www.youtube.com/watch?v=sZ5lwXuD5mA&t=1057s

https://campusvirtual.ull.es/ocw/file.php/26/tema1/1-ehilbert.pdf

Majorana
https://news.microsoft.com/source/latam/noticias-de-microsoft/microsoft-presenta-majorana-

Postulados
https://uvadoc.uva.es/bitstream/handle/10324/70993/TFG-G6793.pdf

https://idus.us.es/server/api/core/bitstreams/e6e34b3a-fc74-4043-98ae-8244902b96e4/content