FACULTADE DE MATEMÁTICAS

Trabajo Fin de Grado

Fundamentos matemáticos de la computación cuántica

Ignacio Gómez Casares

2019/2020

UNIVERSIDAD DE SANTIAGO DE COMPOSTELA

GRADO EN MATEMÁTICAS

Trabajo Fin de Grado

Fundamentos matemáticos de la computación cuántica

Ignacio Gómez Casares

Julio 2020

UNIVERSIDAD DE SANTIAGO DE COMPOSTELA

Trabajo propuesto

Área de Conocimiento: Análisis matemático
Título: Fundamentos matemáticos de la computación cuántica
Breve descripción del contenido: La computación cuántica es una ciencia que aúna áreas tan diversas como las matemáticas, la ingeniería, la física, la criptografía o la filosofía. En este trabajo se pretende aportar las nociones matemáticas básicas que están tras el funcionamiento de la computación cuántica y sus algoritmos.

Resumen

Este trabajo es una pequeña introducción al mundo de la computación cuántica, a través de los espacios de Hilbert, la fibración de Hopf y los grupos de Lie; empezando por una introducción histórica de la mecánica cuántica (teoría física sobre la que se basa la computación cuántica), continuando por el concepto de qubit (la pieza clave de la computación cuántica, al igual que lo es el bit en la computación clásica) y su representación geométrica y terminando con el estudio de las puertas lógicas junto con un par de ejemplos para ilustrar su uso en los algoritmos.

Abstract

This work is a short introduction to the world of quantum computing, seen trough Hilbert spaces, the Hopf fibration and Lie groups; starting with the history of quantum mechanics (the fundamental physical theory on which quantum computing is based). Following that, the introduction of the qubit (the most important piece of quantum computing, as the bit is for classic computing), and it's geometric interpretation. And finally the study of logic gates including a couple of examples to show how they work inside an algorithm.

Índice

Introducción

La computación cuántica surge de la mecánica cuántica, una teoría física que enfoca de forma diferente la manera de ver el mundo que nos rodea, a través de espacios de Hilbert y transformaciones unitarias. Es esta formalización sorprendente la que le confiere a la computación cuántica sus diferentes propiedades, las que la hacen diferente a la computación clásica y en algunos casos incluso superior, obteniendo los mismos resultados con un número de operaciones (complejidad) inferior.

Los tres capítulos de los que se compone este Trabajo Fin de Grado pretenden introducir al lector en la disciplina de la computación cuántica, empezando desde lo más básico –los espacios de Hilbert– hasta llegar a la relación entre los grupos de Lie $SO(3)$ y $Sp(1)$.

Todo empieza con el concepto de qubit, o "quantum bit", que es la pieza clave en la computación cuántica como lo es el bit para la computación clásica. En principio es una construcción teórica, basada en los axiomas que constituyen el fundamento de la mecánica cuántica, pero sienta las bases que luego se aplican en sistemas reales.

Sobre los qubits actúan puertas lógicas similares a las existentes en la computación clásica. Estas puertas son transformaciones unitarias de un espacio de Hilbert, tal y como se recoge en los axiomas de la mecánica cuántica, y es la relación entre $SO(3)$ y $Sp(1)$ la que permite ver esas transformaciones como rotaciones de la esfera de Bloch en la que se representan los qubits.

Las diferentes puertas, tanto en las que interviene un único qubit como en las que intervienen varios, se pueden agrupar para formar circuitos cuánticos, que no son más que representaciones de la aplicación sucesiva a un conjunto de qubits de diferentes puertas lógicas. Con estos circuitos se implementan los algoritmos, entre ellos el algoritmo de Deutsch, ejemplo donde, gracias al paralelismo cuántico, se logra efectuar en una operación lo que en un ordenador convencional necesitaría por lo menos dos operaciones.

Y todo esto es simplemente una pequeña inmersión en una rama de la física inmensa, muy pujante hoy en día, y de la cual todavía se están intentando determinar sus consecuencias en los sistemas y el pensamiento que imperaban hasta ahora.

CAPÍTULO 1

Breve introducción a la mecánica cuántica

1. Origen e ideas fundamentales

Se podría calificar a la mecánica cuántica como una de las teorías físicas menos intuitivas. No es la forma natural en la que uno pensaría que se comporta el mundo, en contraposición con la mecánica clásica que, siendo más natural, no es más que una aproximación de la mecánica cuántica cuando se trata de objetos "grandes".

La idea de la mecánica cuántica surgió de la experimentación: diversos estudios mostraron resultados sorprendentes que llevaron a los físicos a replantearse las teorías existentes hasta el momento y preguntarse de qué otra forma se podría explicar el comportamiento del universo. Los primeros esbozos empezaron a fraguarse alrededor del 1900 pero la teoría no se constituyó realmente hasta 1925-1926 con los trabajos de Heisenberg, Schrödinger y Born [**4**, p. 1].

Para intentar entender en qué consiste la mecánica cuántica vamos a centrarnos en dos de los puntos más importantes de esta teoría junto con los experimentos que llevaron a estos conceptos: la dualidad onda-partícula y el comportamiento probabilístico de las partículas.

A finales del siglo XVII y principios del siglo XVIII la comunidad científica estaba dividida entre los que creían que la luz estaba formada por partículas y los que creían que era una onda. En 1804, Thomas Young publicó dos artículos donde explicaba su experimento de la doble rendija (ver Figura 1.1) que consistía en hacer pasar luz a través de unas láminas de cartón, la primera con un único agujero y la segunda con dos agujeros. Al proyectar la luz proveniente de las dos rendijas de la segunda lámina sobre una pantalla se observaban zonas más y menos iluminadas lo que llevó a Young a postular que la luz se comportaba como una onda y que las zonas oscuras se formaban debido a la interferencia entre las ondas provenientes de ambas rendijas.

En 1900, a raíz del estudio de la teoría de la radiación del cuerpo negro, Max Planck publicó un artículo donde afirmaba que la energía en el campo electromagnético a una frecuencia determinada sólo puede ser un múltiplo entero de una unidad

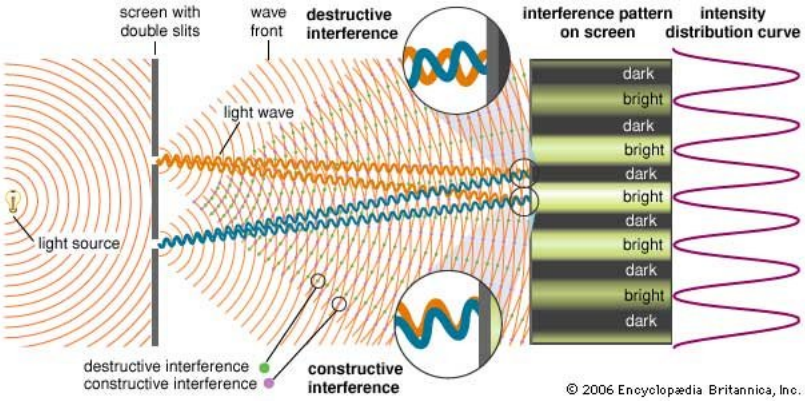

FIGURA 1.1. Experimento de la doble rendija de Thomas Young. Imagen de la Encyclopædia Britannica (`https://www.britannica.com/science/light/Youngs-double-slit-experiment#/media/1/340440/91986`).

básica determinada por la frecuencia y una constante. Esta publicación insufló nueva vida a la teoría de la luz como partícula. Otro artículo que contribuyó fue el que llevó a Einstein a ganar el Premio Nobel de física en 1921; en dicho artículo trató sobre el efecto fotoeléctrico, en el que radiación electromagnética que incide sobre un metal hace que se desprendan electrones de dicho metal. Einstein describió a la luz como un conjunto de partículas discretas, los fotones, lo que le llevó a teorizar que, al aumentar la intensidad de la luz que llegaba al metal manteniendo la frecuencia, el número de electrones emitidos aumentaba pero no la cantidad de energía que tenía cada electrón. Así, por ejemplo, al emitir luz de frecuencia baja pero intensidad alta, no se desprenderían electrones del metal al no tener cada fotón suficiente energía para arrancar un electrón. Diversos experimentos corroboraron este comportamiento, que es difícil de explicar si consideramos a la luz como una onda, mientras que es mucho más fácil al pensar en la luz como partículas.

Este fenómeno en el que la luz presenta comportamientos consistentes con la naturaleza de una onda y también con la naturaleza de una partícula se conoce hoy en día como la "dualidad onda-partícula", y es un fenómeno que ocurre en toda la materia, como propuso en 1924 el físico francés Louis-Victor de Broglie.

Alrededor de 1960 empezaron a hacerse experimentos de la doble rendija pero con electrones en vez de con fotones. Ya estaba en aquel momento perfectamente establecida y confirmada la teoría atómica, que proponía que un átomo está formado por el núcleo y una nube de electrones con carga negativa, y debido a esto, el punto de partida fue considerar a los electrones como partículas y no como una onda. Sin embargo los experimentos que se llevaron a cabo mostraron que también los electrones presentan comportamiento de onda.

Uno de los experimentos más sorprendentes fue el llevado a cabo por un equipo liderado por Akira Tonomura, que realizaron el experimento de la doble rendija pero únicamente haciendo pasar un electrón de cada vez, de forma que cada electrón incidía en la pantalla en un único punto. Los resultados obtenidos se pueden ver en

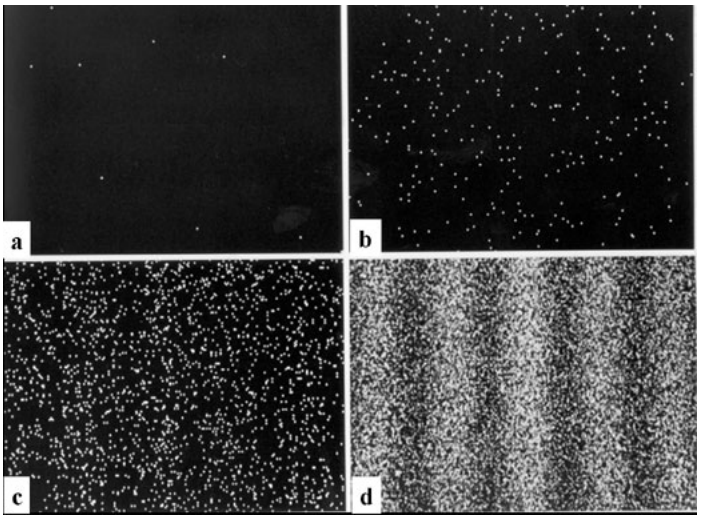

FIGURA 1.2. Experimento de la doble rendija con electrones llevado a cabo por Akira Tonomura (`https://www.hitachi.com/rd/portal/highlight/quantum/doubleslit/index.html`).

la Figura 1.2 donde claramente se observa un patrón con zonas de alta incidencia y otras donde casi ningún electrón incidía.

Entre los diferentes modelos de la mecánica cuántica publicados por Heisenberg, Born y Schrödinger se encontraba una interpretación de Born que proponía pensar en la onda de una partícula como la que determina las probabilidades de las diferentes observaciones de un sistema, y de esta forma se puede interpretar el resultado del experimento de Akira Tonomura: la onda simplemente determina la probabilidad que tiene un electrón de incidir en un punto y al hacer pasar una gran cantidad de electrones se va observando una distribución de probabilidad en la pantalla; eso es lo que produce los patrones observados en la imagen. A pesar de las fuertes críticas que recibió esta interpretación, es una de las que más se utiliza actualmente y se conoce como la interpretación de Copenhage.

Estos dos aspectos fundamentales de la mecánica cuántica –la dualidad onda-partícula y el comportamiento probabilístico de las partículas– son incorporados a la teoría de la siguiente forma: cada partícula de un sistema tiene asociada una función de onda que muestra las posibles posiciones de una partícula y evoluciona con el tiempo como si fuese la ecuación de una onda; cuando intentamos medir la posición de dicha partícula, siempre la encontramos en una posición determinada, por lo que no se observa el comportamiento de onda; la función de onda no se observa, mas determina la probabilidad de encontrar a la partícula en una posición concreta.

2. Axiomas de la mecánica cuántica

Cualquier teoría física tiene que describir en primer lugar al sistema [1] que se quiere estudiar. Para ello se utiliza el concepto de *estado* de un sistema físico. El estado de un sistema no es más un compendio de toda la información que es posible conocer sobre el sistema de forma que quede completamente determinado (es decir, se conoce todo sobre él) por el valor o los valores de dicho estado.

En el ámbito de la mecánica cuántica, el estado de un sistema va a estar representado por un vector unitario en un *espacio de Hilbert* sobre el cuerpo de los números complejos. Dicho espacio de Hilbert es lo que se conoce como el *espacio de estados* del sistema, es decir, el espacio que contiene a todos los posibles valores que puede tomar el estado del sistema. Para definirlo necesitamos primero establecer la definición de producto escalar, así como aprovechar para introducir la notación que utilizaremos a lo largo de este trabajo.

La notación utilizada habitualmente en el campo de la mecánica cuántica es la *notación bra-ket*, introducida por Paul Dirac en 1958. En nuestro caso también usaremos esta notación: un vector del espacio de Hilbert lo denotaremos $|v\rangle \in H$; el producto escalar/interior de dos vectores $|v\rangle, |w\rangle \in H$ lo denotaremos $\langle v|w\rangle$; y el conjugado de un número complejo z, lo denotaremos z^*.

Definición 1.1. Un *producto escalar* o *producto interior* sobre un espacio vectorial complejo H es una aplicación $\langle\cdot|\cdot\rangle : H \times H \to \mathbb{C}$ que satisface las siguientes propiedades.

(1) Para todo $|v\rangle, |w\rangle \in H$,

$$\langle v|w\rangle = \langle w|v\rangle^* .$$

(2) Para todo $|v\rangle \in H$, $\langle v|v\rangle$ es real y no negativo; es cero si y sólo si $|v\rangle = 0$.
(3) Para todo $|v\rangle, |w\rangle \in H$ y $c \in \mathbb{C}$,

$$\langle cv|w\rangle = c^* \langle v|w\rangle \text{ y } \langle v|cw\rangle = \langle v|w\rangle c.$$

(4) Para todo $|v_1\rangle, |v_2\rangle, |w\rangle \in H$,

$$\langle v_1 + v_2|w\rangle = \langle v_1|w\rangle + \langle v_2|w\rangle$$

y para todo $|v\rangle, |w_1\rangle, |w_2\rangle \in H$,

$$\langle v|w_1 + w_2\rangle = \langle v|w_1\rangle + \langle v|w_2\rangle .$$

Un espacio vectorial H con un producto escalar se llama *espacio prehilbertiano*.

Si consideramos una base ortonormal de un espacio prehilbertiano de dimensión finita H sobre $\mathbb{C}$, $\{|e_1\rangle, \ldots, |e_n\rangle\}$, tendremos una forma de escribir el producto

[1] Un sistema no es más que una parte del universo físico que se elige para analizar; todo lo que no se encuentra en esa parte se considera ajeno al sistema y no se consideran sus efectos.

escalar a partir de las coordenadas de los vectores en dicha base. Si tomamos $|v\rangle = \sum_{i=1}^{n} v_i |e_i\rangle$ y $|w\rangle = \sum_{j=1}^{n} w_j |e_j\rangle$ vectores de H con $v_i, w_j \in \mathbb{C}$ para todo i, j,

$$\langle v|w\rangle = \sum_{i,j} v_i^* w_j \langle e_i|e_j\rangle = \sum_i v_i^* w_i,$$

por ser $\{|e_1\rangle, \ldots, |e_n\rangle\}$ una base ortonormal.

Traduciendo esto en la notación bra-ket, dado un vector o "ket" $|v\rangle$, el conjugado traspuesto, dual o "bra" de dicho vector lo denotaremos por $\langle v|$ de forma que, trabajando en una base ortonormal, el que el producto escalar de $|v\rangle$ y $|w\rangle$ lo escribimos como $\langle v|w\rangle$:

$$\langle v|w\rangle = \langle v| \, |w\rangle = \begin{pmatrix} v_0^* & v_1^* & \cdots & v_n^* \end{pmatrix} \begin{pmatrix} w_0 \\ w_1 \\ \vdots \\ w_n \end{pmatrix} = v_0^* w_0 + v_1^* w_1 + \cdots + v_n^* w_n.$$

Definición 1.2. Un *espacio de Hilbert* H sobre $\mathbb{C}$ es un espacio vectorial sobre $\mathbb{C}$ con un producto interior $\langle \cdot | \cdot \rangle : H \times H \to \mathbb{C}$ tal que, con la métrica inducida por dicho producto escalar ($\mathrm{d}(u, v) := \sqrt{\langle u - v | u - v \rangle}$ para $u, v \in H$), el espacio H es un espacio métrico completo.

Esta definición es más general de lo que necesitaremos, ya que en el ámbito de la computación cuántica se utiliza el término espacio de Hilbert haciendo únicamente referencia a los espacios vectoriales de dimensión finita (que son siempre espacios de Hilbert con el producto escalar usual); y eso es lo que haremos a partir de ahora.

El primer axioma establece por tanto cómo describir al sistema que se pretende estudiar.

Axioma 1. Cualquier sistema físico aislado tiene asociado un espacio de Hilbert llamado el espacio de estados del sistema. Un sistema queda completamente determinado en cada instante por su vector de estado, que es un vector unitario en el espacio de estados del sistema.

Una posible interpretación del axioma surge al considerar a la mecánica cuántica como una generalización de la probabilidad, pero usando la norma 2 en vez de la norma 1 (que es la que constituye la probabilidad usual: la suma de las probabilidades de los posibles resultados de un experimento deben sumar 1) [**1**, p. 110-112]. Es más, entre las generalizaciones de la probabilidad, es una de las pocas opciones posibles si queremos obtener propiedades interesantes, como el tener aplicaciones "no triviales" que conserven la norma de los vectores [**1**, p. 116].

Una vez descrito un sistema físico como un espacio de Hilbert sobre $\mathbb{C}$ (a partir de ahora cuando nos refiramos a un espacio de Hilbert estará siempre definido sobre el cuerpo de los complejos), el siguiente paso es describir su evolución con el paso del tiempo, de forma que se pueda predecir su comportamiento futuro a partir del estado actual del sistema.

La descripción de la evolución temporal se lleva a cabo en este caso mediante el concepto de *transformaciones unitarias*. Para definir dicho concepto necesitamos algunos conceptos previos.

DEFINICIÓN 1.3. Dado A un endomorfismo sobre un espacio de Hilbert H, el *adjunto* o *conjugado hermitiano* de A, denotado por $A^\dagger$, es el único [**2**, p. 204] operador lineal $A^\dagger$ tal que, para todo $|v\rangle, |w\rangle \in H$,

$$\langle v|Aw\rangle = \langle A^\dagger v|w\rangle .$$

Diremos que un operador es *hermitiano* o *autoadjunto* si $A^\dagger = A$.

Dada la matriz asociada a un operador lineal, la construcción de la matriz asociada al operador adjunto se consigue conjugando sus entradas y transponiendo la matriz, i.e., $A^\dagger = (A^*)^T$. Como ya hemos visto, para un vector $|v\rangle \in H$, $|v\rangle^\dagger = \langle v|$. A partir de esta definición se define el concepto de operador unitario.

DEFINICIÓN 1.4. Un operador U sobre un espacio de Hilbert H se dice *unitario* si $U^\dagger U = I$ donde I representa la aplicación identidad.

En lo que se refiere a la representación matricial del operador, será unitario si dada una matriz asociada U se satisface que $U^\dagger U = I$ donde I es la matriz identidad. Dado un operador unitario, se satisface además una propiedad importante y es que conservan los productos escalares, i.e., si tenemos dos vectores $|v\rangle, |w\rangle \in H$ se satisface que el producto escalar de $U|v\rangle$ y $U|w\rangle$ es igual al producto escalar de $|v\rangle$ y $|w\rangle$:

$$\langle Uv|Uw\rangle = \langle v|U^\dagger Uw\rangle = \langle v|w\rangle ,$$

usando la definición de operador adjunto. Aprovechamos esta pequeña prueba para introducir un poco más de notación. Para escribir el producto escalar de $|v\rangle$ y $A|w\rangle$ (o equivalentemente de $A^\dagger|v\rangle$ y $|w\rangle$) utilizaremos la notación $\langle v|A|w\rangle$. En este caso, escribiremos de esta forma la expresión $\langle v|U^\dagger Uw\rangle$, que será igual a $\langle v|U^\dagger U|w\rangle$.

Hay otra descripción de la evolución del estado de un sistema para tiempo continuo que se conoce como la ecuación de Schrödinger [**6**, p. 82] y a partir de la cual se puede obtener la versión del postulado que hemos presentado. Sin embargo, para estudiar la computación cuántica no es necesario utilizarla por lo que no la presentaremos en este trabajo.

Así, el segundo axioma de la mecánica cuántica es el siguiente.

AXIOMA 2. La evolución de un sistema cerrado se describe mediante una transformación unitaria. Es decir, si el estado de un sistema es $|\psi\rangle$ en el tiempo t_1 y $|\psi'\rangle$ en el tiempo t_2, la relación entre ambos estados es

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

donde U es un operador unitario que solo depende de los tiempos t_1 y t_2.

El siguiente axioma introduce la acción de algo externo al sistema en el propio sistema, en concreto, el efecto que tiene una medición del sistema. Antes de presentar el axioma necesitamos probar un pequeño lema previo.

LEMA 1.5. *Dada una colección numerable de operadores* $\{M_m\}$ *actuando sobre un espacio de Hilbert* H *tales que* $\sum_m M_m^\dagger M_m = I$*, y dado* $|\psi\rangle \in H$ *un vector unitario,* $\langle\psi|M_m^\dagger M_m|\psi\rangle \in [0,1]$ *para todo* m*.*

DEMOSTRACIÓN. Tenemos en primer lugar que

$$\sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle = \langle\psi|\sum_m M_m^\dagger M_m|\psi\rangle = \langle\psi|\psi\rangle = 1.$$

Por otro lado,

$$\langle\psi|M_m^\dagger M_m|\psi\rangle = \left\langle\psi\middle|M_m^\dagger M_m\psi\right\rangle = \langle M_m\psi|M_m\psi\rangle = |M_m\psi|^2$$

para todo m usando la definición del conjugado hermitiano de un operador. Así, juntando ambas afirmaciones, tendremos que necesariamente

$$0 \leq \langle\psi|M_m^\dagger M_m|\psi\rangle \leq \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle \leq 1.$$

□

Con este pequeño lema ya estamos preparados para concretar el tercer axioma de la mecánica cuántica.

AXIOMA 3. Una medida cuántica se describe mediante una colección $\{M_m\}$ de *operadores de medida*. Estos operadores actúan sobre el espacio de estados del sistema que se está midiendo. El índice m se refiere a los posibles resultados que se pueden obtener en la medición. Si el sistema se encuentra en el estado $|\psi\rangle$ justo antes de la medición, la probabilidad de que el resultado m ocurra viene determinada por

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle,$$

que pertenece al intervalo $[0,1]$ (Lema 1.5) y el estado del sistema tras la medición será

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}.$$

Los operadores de medición satisfacen la *ecuación de completitud*

$$\sum_m M_m^\dagger M_m = I,$$

que fuerza a que las probabilidades de los diferentes resultados sumen uno:

$$\sum_m p(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle = \langle\psi|\sum_m M_m^\dagger M_m|\psi\rangle = \langle\psi|\psi\rangle = 1$$

por ser $|\psi\rangle$ unitario, es decir, $(\mathscr{M}, \mathscr{P}(M), p)$ es un espacio de probabilidad, donde $\mathscr{M} = \{M_n\}$.

El último axioma resume cómo considerar un sistema formado por varios sistemas físicos. Para ello se utiliza el *producto tensor* de espacios vectoriales.

DEFINICIÓN 1.6. Dados dos espacios vectoriales V_1 y V_2 sobre $\mathbb{C}$ un *producto tensor* de V_1 y V_2 es un espacio vectorial W sobre $\mathbb{C}$ junto con una aplicación bilineal $T : V_1 \times V_2 \to W$ que satisface la siguiente propiedad universal: si U es cualquier espacio vectorial sobre $\mathbb{C}$ y $\Phi : V_1 \times V_2 \to U$ es una aplicación bilineal, entonces existe una única aplicación lineal $\tilde{\Phi} : W \to U$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} V_1 \times V_2 & \xrightarrow{T} & W \\ & \searrow^{\Phi} & \downarrow{\scriptstyle \exists!\,\tilde{\Phi}} \\ & & U \end{array}$$

El producto tensor de dos espacios vectoriales es único [**4**, p. 527].

PROPOSICIÓN 1.7. *Dados dos espacios vectoriales V_1, V_2, existe al menos un producto tensor de V_1 y V_2 y es único salvo isomorfismo, i.e., dados dos productos tensores (W_1, T_1) y (W_2, T_2), existe una única aplicación lineal biyectiva $\Psi : W_1 \to W_2$ tal que $T_2 = \Psi \circ T_1$.*

Denotaremos al producto tensor de dos espacios vectoriales V_1 y V_2 por $V_1 \otimes V_2$, y a la aplicación bilineal asociada por $\otimes : V_1 \times V_2 \to V_1 \otimes V_2$.

Todos los elementos del producto tensor de V y W son combinación lineal de elementos de la forma $|v_1\rangle \otimes |v_2\rangle$ con $|v_1\rangle \in V_1, |v_2\rangle \in V_2$. Es más, si $\{|e_i\rangle\}$ es una base ortonormal de V_1 y $\{|e'_j\rangle\}$ una base ortonormal de V_2, la colección $\{|e_i\rangle \otimes |e'_j\rangle\}$ es una base de $V_1 \otimes V_2$.

Por la definición de espacio tensor se satisface que [**6**, p. 73]:

(1) para un escalar arbitrario z, $|v\rangle \in V_1$, $|w\rangle \in V_2$, se tiene que

$$z(|v\rangle \otimes |w\rangle) = (z\,|v\rangle) \otimes |w\rangle = |v\rangle \otimes (z\,|w\rangle);$$

(2) para $|v_1\rangle, |v_2\rangle \in V_1$ y $|w\rangle \in V_2$, se tiene que

$$(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle\,;$$

(3) para $|v\rangle \in V_1$ y $|w_1\rangle, |w_w\rangle \in V_2$, se tiene que

$$|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle\,.$$

A partir de la definición de producto tensor podemos definir el operador lineal $A \otimes B$ a partir de A un operador lineal sobre V_1 y B un operador lineal sobre V_2 de la siguiente forma:

$$(A \otimes B)\left(\sum_i a_i\,|v_i\rangle \otimes |w_i\rangle\right) = \sum_i a_i A\,|v_i\rangle \otimes B\,|w_i\rangle \tag{1}$$

donde $|v_i\rangle, |v'_j\rangle \in V$ y $a_i \in \mathbb{C}$.

Así mismo, si V_1 y V_2 son espacios de Hilbert, podemos definir un producto escalar en $V_1 \otimes V_2$ a partir de los productos escalares de V_1 y V_2:

$$\langle \tilde{v}|\tilde{w}\rangle = \sum_{i,j} a_i^* b_j \langle v_i|v'_j\rangle \langle w_i|w'_j\rangle \tag{2}$$

donde $\tilde{v} = \sum_i a_i |v_i\rangle \otimes |w_i\rangle$ y $\tilde{w} = \sum_i b_i |v'_j\rangle \otimes |w'_j\rangle$ pertenecen a $V_1 \otimes V_2$ con $|v_i\rangle, |v'_j\rangle \in V_1$, $|w_i\rangle, |w'_j\rangle \in V_2$ y $a_i \in \mathbb{C}$.

Usando estos conceptos podemos escribir el último axioma de la mecánica cuántica de la siguiente forma.

AXIOMA 4. El espacio de estados de un sistema físico compuesto es el producto tensor de los espacios de estados de las componentes del sistema. Si las componentes son los sistemas $1, \ldots, n$, y el sistema i está en el estado $|\psi_i\rangle$, el estado del sistema completo es $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$.

CAPÍTULO 2

Los fundamentos de la computación cuántica

1. El concepto de qubit

Al igual que un bit en la computación clásica, un *qubit* se puede pensar como un sistema físico con "dos" estados: $|0\rangle$ y $|1\rangle$. Como ya hemos visto, un sistema físico aislado se representa en mecánica cuántica por un espacio de Hilbert; en este caso, un espacio de Hilbert de dimensión dos, donde los estados $|0\rangle$ y $|1\rangle$ son una base ortonormal de dicho espacio. Por tanto, estos estados no son los únicos que puede tomar un qubit, sino que siguiendo el primer axioma de la mecánica cuántica, cualquier vector unitario del espacio es un estado posible del sistema físico. Así, podemos tener por ejemplo un qubit en el estado

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle .$$

En general son de la forma

$$\frac{1}{\sqrt{|x|^2 + |y|^2}}\left(x|0\rangle + y|1\rangle\right) \quad (x, y) \in \mathbb{C} \times \mathbb{C} \setminus \{(0,0)\}.$$

Los estados que son combinaciones de $|0\rangle$ y $|1\rangle$ se denominan *superposiciones* de estos dos estados. Esta particularidad de los qubits contrasta con los bits de la computación clásica, ya que en ese caso no hay más que dos estados posibles para un bit.

Otra particularidad de los qubits aparece cuando consideramos una medición de un qubit, y es que cuando intentamos medir el estado de un qubit, el aparato de medición tiene que tener dos estados "preferidos" que formen una base ortonormal del espacio de estados (i.e., dos vectores $|u\rangle$ y $|v\rangle$ tales que $\{|u\rangle, |v\rangle\}$ sea una base del espacio de Hilbert y $\langle u|v\rangle = 0$) y lo único que obtendremos al llevar a cabo la medición es $|0\rangle$ o $|1\rangle$ (si seleccionamos la base canónica) **[7**, p. 16**]**.

Es por esto por lo que, cuando se presentan los axiomas de la mecánica cuántica, se suele utilizar una versión más restrictiva del tercer axioma **[6**, p 87**]**. Esta versión utiliza las *mediciones proyectivas* que son un caso particular del axioma más general.

Antes de mostrar el tercer axioma modificado necesitamos ver qué es una proyección en un estado de Hilbert.

Si tenemos un subespacio del espacio de Hilbert, generado por una base ortonormal $\{|v_1\rangle, \ldots, |v_k\rangle\}$, la proyección de un vector $|\psi\rangle$ sobre ese subespacio se define como

$$P|\psi\rangle := \langle v_1|\psi\rangle |v_1\rangle + \cdots + \langle v_k|\psi\rangle |v_k\rangle .$$

Esto implica varias cosas.

LEMA 2.1. *Dado H un espacio de Hilbert y P una proyección sobre un subespacio, se satisface que $P^2 = P$.*

DEMOSTRACIÓN. Sea $|\psi\rangle \in H$ un vector. Supongamos que el subespacio está generado por una base ortonormal $\{|v_1\rangle, \ldots, |v_k\rangle\}$. Por definición,

$$P|\psi\rangle = \langle v_1|\psi\rangle |v_1\rangle + \cdots + \langle v_k|\psi\rangle |v_k\rangle$$

y, consecuentemente,

$$P^2|\psi\rangle = P(\langle v_1|\psi\rangle |v_1\rangle + \cdots + \langle v_k|\psi\rangle |v_k\rangle) = \langle v_1|\psi\rangle |v_1\rangle + \cdots + \langle v_k|\psi\rangle |v_k\rangle .$$

□

LEMA 2.2. *Dado H un espacio de Hilbert y P una proyección sobre un subespacio, se satisface que $P^\dagger = P$.*

DEMOSTRACIÓN. Sin pérdida de generalidad (el caso más general se obtiene aplicando la linealidad del producto escalar), veámoslo para el caso de un subespacio generado por un único vector $|v_1\rangle$. Usando la definición de adjunto de un operador nos basta con ver que para $|v\rangle, |w\rangle \in H$ se satisface que $\langle v|Pw\rangle = \langle Pv|w\rangle$:

$$\langle v|Pw\rangle = \langle v|\langle v_1|w\rangle v_1\rangle = \langle v_1|w\rangle \langle v|v_1\rangle = \langle v_1|w\rangle \langle v_1|v\rangle^* = \langle \langle v_1|v\rangle v_1|w\rangle = \langle Pv|w\rangle .$$

□

LEMA 2.3. *Dado H un espacio de Hilbert, y dado un operador hermitiano M, si para cada autovalor m, el operador P_m es la proyección sobre el subespacio generado por el autovector asociado al autovalor m, se satisface que $\sum_m P_m = I$.*

DEMOSTRACIÓN. Por ser M una matriz hermitiana, es diagonalizable –por lo que sus autovectores forman una base del espacio vectorial– y además la base formada por sus autovectores es una base ortogonal. Por tanto, si consideramos la base formada por los autovectores normalizados $\{|v_1\rangle, \ldots, |v_n\rangle\}$, tendremos una base ortonormal tal que $\langle v_i|v_j\rangle = \delta_{ij}$ para todo i, j. Así, dado $|\psi\rangle = \lambda_1 |v_1\rangle + \ldots \lambda_n |v_n\rangle \in H$,

$$P_i|\psi\rangle = \langle \psi|v_i\rangle |v_i\rangle = (\lambda_1 \langle v_1|v_i\rangle + \cdots + \lambda_n \langle v_n|v_i\rangle)|v_i\rangle = \lambda_i |v_i\rangle$$

y, de esta forma,

$$\left(\sum_m P_m\right)|\psi\rangle = P_1|\psi\rangle + \cdots + P_n|\psi\rangle = \langle \psi|v_1\rangle |v_1\rangle + \cdots + \langle \psi|v_n\rangle |v_n\rangle = |\psi\rangle .$$

□

Presentamos ahora el tercer axioma modificado. Una medición proyectiva se describe mediante un *observable*[1], M, un operador hermitiano en el espacio de

[1]En física, un *observable* es cualquier propiedad de un sistema determinado que se puede medir.

estados del sistema. Este operador tiene una descomposición espectral

$$M = \sum_{m \in \mathrm{sp}(M)} m P_m,$$

donde P_m es la proyección sobre el subespacio vectorial generado por el autovalor m del operador M. Esta descomposición proviene de la descomposición espectral de una matriz hermitiana. Cada uno de estos operadores P_m se puede relacionar con los operadores M_m del tercer axioma general. Así, los posibles resultados de la medición se corresponden con los autovalores del observable. Tras medir el estado $|\psi\rangle$, la probabilidad de obtener el resultado m es

$$\langle\psi|P_m^\dagger P_m|\psi\rangle = \langle\psi|P_m|\psi\rangle$$

por los Lemas 2.2 y 2.1. El estado del sistema después de la medición, suponiendo que se ha obtenido el resultado m, será

$$\frac{P_m|\psi\rangle}{\sqrt{\langle\psi|P_m|\psi\rangle}}.$$

Nótese que se satisface la condición de que $\sum_m P_m^\dagger P_m = I$:

$$\sum_m P_m^\dagger P_m = \sum_m P_m^2 = \sum_m P_m = I,$$

usando los Lemas 2.1 y 2.3.

En el desarrollo de los fundamentos de la computación cuántica nos fijaremos principalmente en el tercer axioma modificado ya que es el que realmente se corresponde con los experimentos en este ámbito.

El hecho de que un qubit pueda tener infinitos estados diferentes (en principio) nos llevaría a pensar que en ese sentido son "mejores" que los bits de la computación clásica. Sin embargo, nos encontramos con que hay estados que no se pueden distinguir [2]; por ejemplo, dos estados que no son ortogonales no se pueden distinguir.

Supongamos que es posible hacerlo si los dos estados satisfacen que $\langle\psi_1|\psi_2\rangle \neq 0$, i.e., no son ortogonales. Entonces, si el qubit se halla por ejemplo en el estado $|\psi_1\rangle$, se tendría que satisfacer que la probabilidad de obtener un resultado m en la medición tal que $f(m) = 1$ sea 1 (análogamente en caso de que el estado fuese $|\psi_2\rangle$). Definimos $E_i = \sum_{m|f(m)=i} M_m^\dagger M_m$ de forma que podemos escribir la restricción establecida antes como

$$\langle\psi_1|E_1|\psi_1\rangle = 1;\ \langle\psi_2|E_2|\psi_2\rangle = 1. \tag{3}$$

Como la colección $\{M_m\}$ es una medida cuántica, se tiene que $\sum_i E_i = I$ y por lo tanto $\sum_i \langle\psi_1|E_i|\psi_1\rangle = 1$. Como $\langle\psi_1|E_1|\psi_1\rangle = 1$, tendremos que $\langle\psi_2|E_1|\psi_2\rangle = 0$. Análogamente, $\langle\psi_1|E_2|\psi_1\rangle = 0$. Si descomponemos $|\psi_2\rangle = \alpha|\psi_1\rangle + \beta|\psi\rangle$ –donde

[2]Distinguir dos estados significa que dados dos estados $|\psi_1\rangle$ y $|\psi_2\rangle$ es posible encontrar una colección de operadores de medida $\{M_m\}$ de forma que, dependiendo del resultado obtenido en la medición, sepamos en cuál de los dos estados estaba el qubit (i.e. existe una aplicación f tal que $f(m) = i$, donde $i = 1, 2$, que indica el estado en función del resultado obtenido en la medición).

$|\psi\rangle$ es ortonormal a ψ_1, $|\alpha|^2 + |\beta|^2 = 1$ y $|\beta| < 1$ ($|\psi_1\rangle$ y $|\psi_2\rangle$ no son ortogonales)– y, usando lo anterior, tendremos que

$$\langle\psi_2|E_2|\psi_2\rangle = |\beta|^2 \langle\psi|E_2|\psi\rangle \leq |\beta|^2 < 1,$$

usando para obtener la desigualdad anterior que

$$\langle\psi|E_2|\psi\rangle \leq \sum_i \langle\psi|E_i|\psi\rangle = \langle\psi|\psi\rangle = 1.$$

Obtenemos así una contradicción con (3) que proviene de suponer que podíamos distinguir dos estados no ortogonales. Por lo tanto, si tuviésemos un sistema de medida tal que nos devolviese como resultado el estado actual del qubit, seríamos capaces de distinguir entre dos estados no ortogonales lo que supone una contradicción con el tercer axioma de la cuántica.

Sin embargo, es posible conocer la probabilidad de obtener un determinado resultado en una medición. Veamos como ejemplo lo que se conoce como la medición de un qubit en la base computacional, i.e., en la base ortonormal $\{|0\rangle, |1\rangle\}$. Para definir la medición necesitamos los operadores de medida correspondientes. En este caso son M_0 y M_1 definidos por

$$M_0 = |0\rangle\langle 0| \text{ y } M_1 = |1\rangle\langle 1|,$$

donde $|v\rangle\langle w|$ está definido de la siguiente forma.

Definición 2.4. Dados dos espacios de Hilbert V y W, y dados $|v\rangle \in V$, $|w\rangle \in W$, se define $|w\rangle\langle v| : V \to W$ como el operador lineal tal que para $|v'\rangle \in V$

$$(|w\rangle\langle v|)(|v'\rangle) = |w\rangle \langle v|v'\rangle = \langle v|v'\rangle |w\rangle.$$

Tanto M_0 como M_1 son operadores hermitianos ya que

$$M_0^\dagger = (|0\rangle\langle 0|)^\dagger = \langle 0|^\dagger |0\rangle^\dagger = |0\rangle\langle 0| = M_0,$$

(análogo para M_1), y además satisfacen que

$$M_0^2(\alpha|0\rangle + \beta|0\rangle) = (|0\rangle\langle 0|)((|0\rangle\langle 0|)(\alpha|0\rangle + \beta|0\rangle)) = (|0\rangle\langle 0|)(\alpha|0\rangle) = \alpha|0\rangle = M_0(\alpha|0\rangle + \beta|0\rangle)$$

(análogo para M_1), por lo que $M_0^2 = M_0$ y $M_1^2 = M_1$. De esta forma, la ecuación de completitud exigida por el tercer axioma se satisface:

$$M_0^\dagger M_0 + M_1^\dagger M_1 = M_0^2 + M_1^2 = M_0 + M_1 = I.$$

Así, siguiendo lo establecido por el axioma, si el estado que estamos midiendo es $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, la probabilidad de obtener el resultado 0 es

$$\langle\psi|M_0^\dagger M_0|\psi\rangle = \langle\psi|M_0|\psi\rangle = \langle\psi|M_0\psi\rangle = \alpha\langle\psi|0\rangle = |\alpha|^2$$

y, de forma similar, la probabilidad de obtener el resultado 1 es $|\beta|^2$. El estado del qubit después de la medición será en ambos casos

$$\frac{M_0|\psi\rangle}{|\alpha|} = \frac{\alpha}{|\alpha|}|0\rangle,$$

$$\text{y } \frac{M_1 |\psi\rangle}{|\beta|} = \frac{\beta}{|\beta|} |1\rangle .$$

Tanto $\frac{\alpha}{|\alpha|}$ como $\frac{\beta}{|\beta|}$ son complejos de módulo 1 y, como veremos en la siguiente sección, podemos ignorarlos, obteniendo $|0\rangle$ y $|1\rangle$ respectivamente.

Podríamos pretender entonces hacer copias del qubit, medirlo varias veces y de ahí deducir los valores α y β, o al menos su módulo. Sin embargo esto no es posible debido a que un qubit no se puede clonar, es decir, no podemos hacer una copia del qubit. Veremos el motivo en el Capítulo 3.

2. Representación geométrica de un qubit

A la hora de medir un qubit, nos encontramos con una relación de equivalencia entre sus estados. Dado un operador de medida, medir $|\psi\rangle$ o medir $\exp(i\gamma)|\psi\rangle$ con $\gamma \in \mathbb{R}$ nos lleva al mismo resultado, ya que la probabilidad de los diferentes resultados al medir $|\psi\rangle$ y al medir $\exp(i\gamma)|\psi\rangle$ es la misma:

$$\langle \exp(i\gamma)\psi | M_m^\dagger M_m | \exp(i\gamma)\psi\rangle = \langle \psi | \exp(-i\gamma) M_m^\dagger M_m \exp(i\gamma) | \psi\rangle = \langle \psi | M_m^\dagger M_m | \psi\rangle ,$$

usando la notación del tercer axioma de la mecánica cuántica y el hecho de que $(\exp(i\gamma)M_m)^\dagger = \exp(i\gamma)^* M_m^\dagger = \exp(-i\gamma)M_m^\dagger$. El factor $\exp(i\gamma)$ se llama *factor de fase global*.

Además, el recíproco también se satisface.

Lema 2.5. *Dados dos estados $|\psi\rangle$ y $|\phi\rangle$ tales que, para cualquier operador de medida las probabilidades de los diferentes resultados coinciden, ambos estados se diferencian en un factor de fase global.*

Demostración. Consideremos el operador de medida $\{M_0, M_1\}$ que introdujimos en la sección anterior. Supongamos que $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ y que $|\psi\rangle = \alpha'|0\rangle + \beta'|1\rangle$.

Por hipótesis, tendremos que

$$|\alpha|^2 = \langle \psi | M_0^\dagger M_0 | \psi\rangle = \langle \phi | M_0^\dagger M_0 | \phi\rangle = |\alpha'|^2,$$

y que

$$|\beta|^2 = \langle \psi | M_1^\dagger M_1 | \psi\rangle = \langle \phi | M_1^\dagger M_1 | \phi\rangle = |\beta'|^2.$$

Por tanto, $|\alpha| = |\alpha'|$ y $|\beta| = |\beta'|$. Podemos encontrar entonces $\gamma, \mu \in \mathbb{R}$ tales que $\alpha' = \exp(i\gamma)\alpha$ y $\beta' = \exp(i\mu)\beta$.

Consideremos ahora otro operador de medida diferente, por ejemplo el operador asociado a la medición proyectiva determinada por el observable

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Los autovalores de esta matriz son 1 y -1 con autovectores asociados $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ y $(-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ respectivamente. Así, la descomposición espectral del observable será:

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} - \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix},$$

siendo

$$P_1 \equiv \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

la proyección sobre el subespacio generado por $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ y

$$P_{-1} \equiv \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

la proyección sobre el subespacio generado por $(-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$.

De esta forma, aplicando la versión modificada del tercer axioma para una medición proyectiva, tendremos que la probabilidad de obtener el resultado asociado al autovalor -1 será, para $\alpha|0\rangle + \beta|1\rangle$,

$$\begin{aligned}\langle \alpha|0\rangle + \beta|1\rangle | P_{-1} | \alpha|0\rangle + \beta|1\rangle \rangle &= \left\langle \alpha|0\rangle + \beta|1\rangle \middle| (\frac{1}{2}\alpha - \frac{1}{2}\beta)|0\rangle + (-\frac{1}{2}\alpha + \frac{1}{2}\beta)|1\rangle \right\rangle \\ &= \frac{1}{2}\alpha^*\alpha - \frac{1}{2}\alpha\beta^* - \frac{1}{2}\alpha^*\beta + \frac{1}{2}\beta^*\beta,\end{aligned}$$

y para $\alpha'|0\rangle + \beta'|1\rangle = \exp(i\gamma)\alpha|0\rangle + \exp(i\mu)\beta|1\rangle$,

$$\begin{aligned}\langle \alpha'|0\rangle + \beta'|1\rangle | P_{-1} | \alpha'|0\rangle + \beta'|1\rangle \rangle =& \frac{1}{2}\alpha^*\alpha - \frac{1}{2}\exp(i\gamma)\exp(i\mu)^*\alpha\beta^* \\ & - \frac{1}{2}\exp(i\gamma)^*\exp(i\mu)\alpha^*\beta + \frac{1}{2}\beta^*\beta.\end{aligned}$$

Como hemos supuesto que para todo operador de medida las probabilidades de los diferentes resultados coinciden para $|\psi\rangle$ y para $|\phi\rangle$, tendremos que

$$\begin{aligned}\frac{1}{2}\alpha^*\alpha - \frac{1}{2}\alpha\beta^* - \frac{1}{2}\alpha^*\beta + \frac{1}{2}\beta^*\beta =& \frac{1}{2}\alpha^*\alpha - \frac{1}{2}\exp(i\gamma)\exp(i\mu)^*\alpha\beta^* \\ & - \frac{1}{2}\exp(i\gamma)^*\exp(i\mu)\alpha^*\beta + \frac{1}{2}\beta^*\beta,\end{aligned}$$

i.e.

$$\alpha\beta^* + \alpha^*\beta = \exp(i\gamma)\exp(i\mu)^*\alpha\beta^* + \exp(i\gamma)^*\exp(i\mu)\alpha^*\beta. \tag{4}$$

Tomemos ahora el operador de medida asociado al observable $\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$. Los autovalores de esta matriz son 1 y -1, con autovectores asociados $(-\frac{i}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ y $(\frac{i}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ respectivamente. La descomposición espectral de este observable será por tanto

$$-\begin{pmatrix} \frac{1}{2} & \frac{i}{2} \\ -\frac{i}{2} & \frac{1}{2} \end{pmatrix} + \begin{pmatrix} \frac{1}{2} & -\frac{i}{2} \\ \frac{i}{2} & \frac{1}{2} \end{pmatrix},$$

siendo

$$P'_{-1} \equiv \begin{pmatrix} \frac{1}{2} & \frac{i}{2} \\ -\frac{i}{2} & \frac{1}{2} \end{pmatrix}$$

la proyección sobre el subespacio generado por $(\frac{i}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ y

$$P'_1 \equiv \begin{pmatrix} \frac{1}{2} & -\frac{i}{2} \\ \frac{i}{2} & \frac{1}{2} \end{pmatrix}$$

la proyección sobre el subespacio generado por $(-\frac{i}{\sqrt{2}}, \frac{1}{\sqrt{2}})$.

Aplicando esto, al igual que antes, obtenemos que la probabilidad de obtener el resultado asociado al autovalor 1 será, para $\alpha|0\rangle + \beta|1\rangle$

$$\begin{aligned}\langle \alpha|0\rangle + \beta|1\rangle | P_1' | \alpha|0\rangle + \beta|1\rangle\rangle &= \left\langle \alpha|0\rangle + \beta|1\rangle \middle| (\frac{1}{2}\alpha - \frac{i}{2}\beta)|0\rangle + (\frac{i}{2}\alpha + \frac{1}{2}\beta)|1\rangle \right\rangle \\ &= \frac{1}{2}\alpha^*\alpha + \frac{i}{2}\alpha\beta^* - \frac{i}{2}\alpha^*\beta + \frac{1}{2}\beta^*\beta,\end{aligned}$$

y para $\alpha'|0\rangle + \beta'|1\rangle = \exp(i\gamma)\alpha|0\rangle + \exp(i\mu)\beta|1\rangle$,

$$\begin{aligned}\langle \alpha'|0\rangle + \beta'|1\rangle | P_1' | \alpha'|0\rangle + \beta'|1\rangle\rangle =& \frac{1}{2}\alpha^*\alpha + \frac{i}{2}\exp(i\gamma)\exp(i\mu)^*\alpha\beta^* \\ &- \frac{i}{2}\exp(i\gamma)^*\exp(i\mu)\alpha^*\beta + \frac{1}{2}\beta^*\beta.\end{aligned}$$

Como hemos supuesto que para todo operador de medida las probabilidades de los diferentes resultados coinciden para $|\psi\rangle$ y para $|\phi\rangle$, tendremos que

$$\begin{aligned}\frac{1}{2}\alpha^*\alpha + \frac{i}{2}\alpha\beta^* - \frac{i}{2}\alpha^*\beta + \frac{1}{2}\beta^*\beta =& \frac{1}{2}\alpha^*\alpha + \frac{i}{2}\exp(i\gamma)\exp(i\mu)^*\alpha\beta^* \\ &- \frac{i}{2}\exp(i\gamma)^*\exp(i\mu)\alpha^*\beta + \frac{1}{2}\beta^*\beta,\end{aligned}$$

i.e.

$$\alpha\beta^* - \alpha^*\beta = \exp(i\gamma)\exp(i\mu)^*\alpha\beta^* - \exp(i\gamma)^*\exp(i\mu)\alpha^*\beta. \tag{5}$$

Juntando (4) y (5) tenemos que

$$\alpha^*\beta(1-\exp(i\gamma)^*\exp(i\mu)) \overset{(5)}{=} \alpha\beta^* - \exp(i\gamma)\exp(i\mu)^*\alpha\beta^* \overset{(4)}{=} \alpha^*\beta(\exp(i\gamma)^*\exp(i\mu) - 1).$$

Consecuentemente, (suponiendo que $\alpha\beta^* \neq 0$; en caso contrario, se verifica la proposición tomando como factor de fase global el factor asociado a α ó β dependiendo de cuál de ellos sea distinto de cero),

$$1 - \exp(i\gamma)^*\exp(i\mu) = \exp(i\gamma)^*\exp(i\mu) - 1,$$

luego

$$1 = \exp(i\gamma)^*\exp(i\mu).$$

Así,

$$\exp(i\gamma)^*\exp(i\mu) = \exp(-i\gamma)\exp(i\mu) = \exp(i(\mu - \gamma)) = 1.$$

Como $1 = \exp(i2k\pi)$ para $k \in \mathbb{Z}$, tendremos que $\mu - \gamma = 2k\pi$ para $k \in \mathbb{Z}$; pero entonces $\exp(i\mu) = \exp(i\gamma)$, obteniendo lo que buscábamos.

□

Podemos por tanto establecer una relación de equivalencia que identifique los vectores que representan estado físicos iguales (i.e. estados para los que, dado un operador de medida cualquiera, las probabilidades de los diferentes resultados coinciden):

$$|\psi\rangle \sim |\psi'\rangle \iff |\psi'\rangle = \exp(i\gamma)|\psi\rangle \text{ para } \gamma \in \mathbb{R}. \tag{6}$$

Por tanto, todos los estados "diferentes" se pueden representar en el espacio cociente $\{z \in \mathbb{C}^2 \mid \|z\| = 1\}/\sim$ (el espacio de estados, como espacio de Hilbert de dimensión 2, es isomorfo a $\mathbb{C}^2$). Sin embargo, hay una representación de los qubits que nos aporta una mayor intuición, que es la representación en la *esfera de Bloch*.

Para entender la representación en la esfera de Bloch primero tenemos que definir el cuerpo de los cuaterniones y la *fibración de Hopf*.

2.1. El cuerpo de los cuaterniones. Los cuateriones surgieron de la idea de intentar extender las operaciones en $\mathbb{C}$ a más dimensiones. En 1843, Willian Rowan Hamilton publicó un artículo dónde describía cómo generalizar las operaciones de los números complejos (isomorfos a $\mathbb{R}^2$) a $\mathbb{R}^4$ **[9]**.

Podemos así definir una multiplicación en $\mathbb{R}^4$ de forma que con la suma usual tengamos un cuerpo (aunque no conmutativo). Para ello tomamos una base $\{1, i, j, k\}$ de $\mathbb{R}^4$ (normalmente la base canónica) y definimos la operación de multiplicación como

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

.

De esta manera, extendiendo la operación por linealidad, podemos multiplicar elementos de $\mathbb{R}^4$:

$$\begin{aligned}(a+bi+cj+dk)(x+yi+zj+wk) = &(ax-by-cz-dw)\\ &+(ay+bx+cw-dz)i\\ &+(az+cx+dy-bw)j\\ &+(aw+dx+bz-cy)k.\end{aligned}$$

$\mathbb{R}^4$ con esta multiplicación constituye lo que se denomina el conjunto de los *cuaterniones* (denotado por $\mathbb{H}$). Podemos incluir los números reales en los cuaterniones identificando al complejo $a+bi$ con el cuaternión $a+bi+0k+0k$. La multiplicación que hemos definido en $\mathbb{H}$ extiende la multiplicación en $\mathbb{C}$ al incluir $\mathbb{C}$ en $\mathbb{H}$ de esta forma.

Definimos el *conjugado* de un cuaternión $r = a + bi + cj + dk$ como

$$r^* = a - bi - cj - dk.$$

La *norma* de un cuaternión es la norma en $\mathbb{R}^4$ y el *inverso multiplicativo* de un cuaternión r es

$$r^{-1} = \frac{r^*}{\|r\|^2},$$

de forma que $rr^{-1} = 1$ (siendo $1 + 0i + 0j + 0k$ el neutro para la multiplicación). Para cuateriones unitarios, $r^* = r^{-1}$.

Al igual que en $\mathbb{C}$, podemos definir un producto interior en $\mathbb{H}$, utilizando el concepto de conjugado de un cuaternión que hemos definido, de manera similar al producto escalar en $\mathbb{C}$; con la particularidad de que la multiplicación no es conmutativa y por tanto

$$(\alpha\beta)^* = \beta^*\alpha^*.$$

2.2. La fibración de Hopf. Empecemos definiendo lo que se conoce como la fibración de Hopf.

DEFINICIÓN 2.6. Dadas las esferas $S^3 \subset \mathbb{R}^4$ y $S^2 \subset \mathbb{R}^3$, la *fibración de Hopf* es la aplicación $h : S^3 \to S^2$ definida por

$$h(a,b,c,d) = (a^2 + b^2 - c^2 - d^2,\, 2(ad + bc),\, 2(bd - ac)). \tag{7}$$

Es fácil comprobar que la imagen de la fibración de Hopf está contenida en la esfera S^2. Veamos ahora una interpretación geométrica de la fibración de Hopf usando los cuaterniones. En $\mathbb{R}^3$, para describir una rotación, únicamente necesitamos determinar el eje de rotación y el ángulo que queremos rotar, i.e., sólo necesitamos cuatro números reales (tres para el eje y una para el ángulo). Algebraicamente, podemos codificar esto usando los cuaterniones **[5]**.

Dado un vector $p = (x, y, z)$ de $\mathbb{R}^3$, le asociamos el cuaternión $xi + yj + zk$, al que llamaremos cuaternión *puro* por tener la parte real igual a cero. Denotaremos también a este cuaternión como p. Al hacer rpr^{-1} con $r = a+bi+cj+dk$, obtenemos

$$\begin{aligned} rpr^{-1} = &\frac{a^2x + a(2cz - 2dy) + b^2x + 2b(cy + dz) - x\left(c^2 + d^2\right)}{a^2 + b^2 + c^2 + d^2} i \\ &+ \frac{a^2y - 2abz + 2adx - b^2y + 2bcx + c^2y + 2cdz - d^2y}{a^2 + b^2 + c^2 + d^2} j \\ &+ \frac{a^2z + a(2by - 2cx) - z\left(b^2 + c^2 - d^2\right) + 2d(bx + cy)}{a^2 + b^2 + c^2 + d^2} k, \end{aligned}$$

por lo que sigue siendo un cuaternión puro y lo podemos considerar como punto de $\mathbb{R}^3$. Usando lo anterior, podemos definir una aplicación $Ad_r : \mathbb{R}^3 \to \mathbb{R}^3$ para $r \neq 0$:

$$Ad_r(x, y, z) = rpr^{-1}.$$

Se satisface que $Ad_r = Ad_{tr}$ para t un real distinto de cero. Por tanto, basta con considerar los r de norma uno para obtener todas las posibles aplicaciones Ad_r. Cada una de estas aplicaciones es lineal y determina una rotación en $\mathbb{R}^3$ con eje de rotación (b, c, d) y ángulo de rotación $\theta = 2\cos^{-1}(a) = 2\sin^{-1}(\sqrt{b^2 + c^2 + d^2})$. Comprobemos estas afirmaciones.

En primer lugar veamos que son aplicaciones lineales.

LEMA 2.7. *Dado un cuaternión unitario $0 \neq r = a + bi + cj + dk$, la aplicación $Ad_r : \mathbb{R}^3 \to \mathbb{R}^3$ definida como $Ad_r(x, y, z) = rpr^{-1}$ es una aplicación lineal.*

DEMOSTRACIÓN. Sean $(x, y, z), (x', y', z') \in \mathbb{R}^3$ y $\lambda, \lambda' \in \mathbb{R}$. Se satisface que

$$\begin{aligned} Ad_r(\lambda x, \lambda y, \lambda z) = &\lambda\left(a^2x + a(2cz - 2dy) + b^2x + 2b(cy + dz) - x\left(c^2 + d^2\right)\right) i \\ &+ \lambda\left(a^2y - 2abz + 2adx - b^2y + 2bcx + c^2y + 2cdz - d^2y\right) j \\ &+ \lambda\left(a^2z + 2aby - 2acx - b^2z + 2bdx - c^2z + 2cdy + d^2z\right) k \\ = &\lambda Ad_r(x, y, z) \end{aligned}$$

y que

$$\begin{aligned}Ad_r(x+x',y+y',z+z') =& [a^2(x+x') + 2ac(z+z') - 2ad(y+y') + b^2(x+x') \\ &+ 2b(c(y+y') + d(z+z')) - \left(c^2+d^2\right)(x+x')]i \\ &+ [a^2(y+y') - 2ab(z+z') + 2ad(x+x') - b^2(y+y') \\ &+ 2bc(x+x') + c^2(y+y') + 2cdz + 2cdz' - d^2(y+y')]j \\ &+ [a^2(z+z') + 2ab(y+y') - 2ac(x+x') - b^2(z+z') \\ &+ 2bd(x+x') - c^2(z+z') + 2cdy + 2cdy' + d^2(z+z')]k \\ =& Ad_r(x,y,z) + Ad_r(x',y',z').\end{aligned}$$

□

Tenemos ahora que la matriz asociada a la aplicación Ad_r (en las condiciones del lema anterior) sobre la base canónica de $\mathbb{R}^3$ es

$$M = \begin{pmatrix} a^2+b^2-c^2-d^2 & 2bc-2ad & 2ac+2bd \\ 2bc+2ad & a^2-b^2+c^2-d^2 & 2cd-2ab \\ 2bd-2ac & 2ab+2cd & a^2-b^2-c^2+d^2 \end{pmatrix}. \tag{8}$$

El determinante de esta matriz es 1, y la matriz es ortogonal (i.e. $MM^t = I$) por lo que efectivamente se trata de una rotación. Los autovalores son

$$\begin{aligned}\lambda_1 &= 1, \\ \lambda_2 &= a^2-b^2-c^2-d^2-2\sqrt{-a^2b^2-a^2c^2-a^2d^2}, \\ \lambda_3 &= a^2-b^2-c^2-d^2+2\sqrt{-a^2b^2-a^2c^2-a^2d^2},\end{aligned}$$

y uno de los autovectores asociado al autovalor λ_1 (que es el eje de la rotación; al ser los autovalores distintos, el subespacio asociado es una recta) es (b,c,d). Para calcular el ángulo de giro, consideremos un vector perpendicular a (b,c,d), por ejemplo $(b,c,d)\times(1,0,0) = (0,d,-c)$ (usando el producto vectorial de $\mathbb{R}^3$). El ángulo de giro θ será el ángulo que forma $w = (0,d,-c)$ con su imagen Mw. Por la definición de producto escalar en $\mathbb{R}^3$, tenemos que el coseno de este ángulo es

$$\cos\theta = \frac{w\cdot Mw}{\|w\|^2} = a^2-b^2-c^2-d^2 = 2a^2-1,$$

por lo que $a^2 = \frac{1}{2}(\cos\theta+1)$, lo que significa que $a = \cos\frac{\theta}{2}$. Así, $\theta = 2\cos^{-1}(a)$ es el ángulo de la rotación.

Una vez definidas las aplicaciones Ad_r, podemos definir la fibración de Hopf a partir de ellas. Fijamos un punto en S^2, w_0, y dado un punto $(a,b,c,d)\in S^3$ definimos

$$r \to Ad_r(w_0) = rw_0r^{-1} = rw_0r^*.$$

Para el punto $w_0 = (1,0,0)$, esta aplicación coincide con la definida en (7). Es decir, la fibración de Hopf consiste en, dado un punto de la esfera S^3, aplicar la rotación determinada por ese cuaternión sobre un punto determinado w_0 en la esfera S^2.

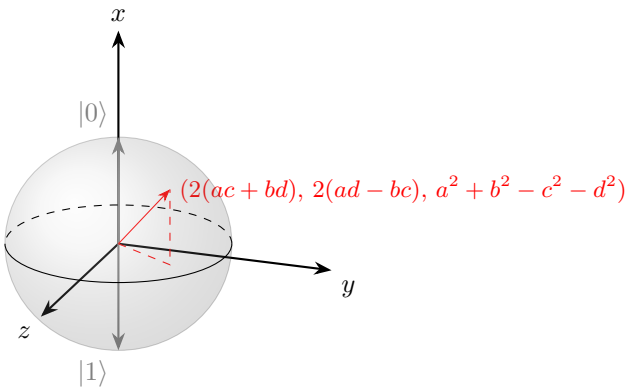

FIGURA 2.1. Fibración de Hopf.

2.3. La esfera de Bloch. Una vez visto el concepto de la fibración de Hopf, lo usaremos para representar el estado de un qubit en la esfera de Bloch. Podemos representar el estado $|\psi\rangle$ de un qubit en la base $\{|0\rangle, |1\rangle\}$ como

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

con $\alpha, \beta \in \mathbb{C}$ tales que $|\alpha|^2 + |\beta|^2 = 1$. A su vez, $\alpha = a + bi$ y $\beta = c + di$ donde $a, b, c, d \in \mathbb{R}$. Que $|\alpha|^2 + |\beta|^2 = 1$ implica que $a^2 + b^2 + c^2 + d^2 = 1$. Esta ecuación describe la esfera S^3 contenida en $\mathbb{R}^4$.

La idea es construir una aplicación que relacione $\mathbb{C} \times \mathbb{C}$ con los cuaterniones, de forma que a la imagen de un estado de un qubit por esta aplicación le podamos aplicar la fibración de Hopf y obtener un punto en la esfera S^2. La aplicación que definimos (por motivos técnicos que exploraremos más adelante) es

$$\begin{array}{rcl} f : \mathbb{C} \times \mathbb{C} & \longrightarrow & \mathbb{H} \\ (\alpha, \beta) = (a + bi, c + di) & \longmapsto & (a, b, -c, d). \end{array}$$

La imagen de la composición $h \circ f$ es lo que se denomina la *esfera de Bloch*, tal y como podemos ver en la Figura 2.1. También vemos que $h(|0\rangle) = h(1, 0, 0, 0) = (1, 0, 0)$ y $h(|1\rangle) = h(0, 0, 1, 0) = (-1, 0, 0)$. Esta no es la convención utilizada habitualmente por los físicos, sino que los papeles del eje x y el eje z están intercambiados.

Al comienzo de esta sección, definimos lo que se conoce como el factor de fase global, de forma que dos estados que se diferencian únicamente en un complejo unitario $\exp(i\gamma)$ son "iguales" desde el punto de vista de las mediciones. La pregunta ahora es si esta fibración de Hopf $h \circ f$ lleva siempre dos estados "iguales" al mismo punto, es decir, si respecta la relación de equivalencia definida en (6).

LEMA 2.8. *La aplicación $h \circ f$ respeta la relación de equivalencia* (6).

DEMOSTRACIÓN. Sean $|\psi\rangle$ y $|\psi'\rangle$ tales que $|\psi\rangle \sim |\psi'\rangle$. Entonces, $|\psi'\rangle = \exp(i\gamma)\,|\psi\rangle$ para $\gamma \in \mathbb{R}$, es decir, si $|\psi\rangle = (\alpha, \beta) = (a + bi, c + di)$, tendremos

que

$$|\psi'\rangle = \exp(i\gamma)(a+bi, c+di) = (\cos(\gamma) + i\sin(\gamma))(a+bi, c+di)$$

y por tanto,

$$\begin{aligned}(h\circ f)(|\psi'\rangle) &= h(a\cos\gamma - b\sin\gamma, a\sin\gamma + b\cos\gamma, -c\cos\gamma + d\sin\gamma, c\sin\gamma + d\cos\gamma)\\ &= (a^2+b^2-c^2-d^2,\, 2(ad-bc),\, 2(bd+ac)) = h(a,b,-c,d)\\ &= (h\circ f)(a,b,c,d) = (h\circ f)(|\psi\rangle).\end{aligned}$$

□

Hemos definido así una representación del qubit en la esfera S^3. En el caso de varios qubits, no se ha podido definir todavía una representación tan simple como la esfera de Bloch en el caso de un qubit [**6**, p. 15].

En el resto del capítulo nos centraremos en estudiar las puertas lógicas, que constituyen la base de la computación cuántica, así como intentar interpretar geométricamente su efecto sobre la representación del qubit en la esfera de Bloch.

3. Transformaciones unitarias

En la Definición 1.4 introdujimos el concepto de operador unitario sobre un espacio de Hilbert. Los operadores unitarios son, según los axiomas de la mecánica cuántica, la forma de representar los cambios a lo largo del tiempo de los qubits. En esta sección los estudiaremos a fondo para después centrarnos en aquellos operadores que constituirán las puertas lógicas de la computación cuántica.

Para analizar estos operadores utilizaremos los grupos de matrices, es decir, supondremos fijada una base en el espacio de Hilbert y consideraremos las matrices asociadas a los diferentes operadores sobre esa base.

3.1. Grupo lineal general. En la Sección 2.1 de este capítulo utilizamos los cuaterniones para definir la fibración de Hopf. Tal y como dijimos en su momento, tenemos las siguientes inclusiones

$$\mathbb{R} \subset \mathbb{C} \subset \mathbb{H},$$

donde la operación de multiplicación y sus propiedades se mantiene, excepto que en $\mathbb{H}$ no es conmutativa. En lo que sigue, denotaremos por $\mathbb{K}$ a cualquiera de los tres, es decir, $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}, \mathbb{H}\}$. Por otro lado, denotaremos a las matrices cuadradas $n \times n$ con coeficientes en $\mathbb{K}$ por $M_n(\mathbb{K})$.

Cuando $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$, la aplicación

$$\det : M_n(\mathbb{K}) \longrightarrow \mathbb{K},$$

es conocida. Sin embargo, debido a las particularidades de $\mathbb{H}$, no podemos utilizar la misma definición para las matrices con coeficientes en $\mathbb{H}$ si queremos retener propiedades como que las matrices sean invertibles si y sólo si el determinante es

distinto de cero. Por ejemplo, si definiésemos el determinante con la definición habitual, al considerar la matriz

$$A = \begin{pmatrix} i & j \\ i & j \end{pmatrix} \in M_2(\mathbb{H}),$$

obtendríamos un determinante igual a $ij - ji = k - (-k) = 2k \neq 0$; sin embargo, la matriz no es invertible, ya que si existiese una matriz

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{H})$$

tal que

$$\begin{pmatrix} i & j \\ i & j \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

tendríamos que

$$\begin{aligned} ia + jc &= 1, \\ ib + jd &= 0, \\ ia + jc &= 0, \\ ib + jd &= 1, \end{aligned}$$

lo que supone una contradicción, ya que $0 \neq 1$. Más adelante definiremos una aplicación que verificará esta propiedad y que nos servirá como definición de determinante para una matriz con coeficientes cuaterniónicos.

Las particularidades de $\mathbb{H}$ también afectan a la estructura de los espacios vectoriales sobre los cuaterniones. Al no ser un cuerpo conmutativo, podemos considerar tanto espacios vectoriales por la derecha como por la izquierda.

Definición 2.9. Un *espacio vectorial por la izquierda* sobre un cuerpo no conmutativo $\mathbb{K}$ es un conjunto M junto con una suma de $M \times M$ a M (denotada por $A, B \mapsto A + B$) y una multiplicación de $\mathbb{K} \times M$ a M (denotada por $a, A \mapsto a \cdot A$) tal que M es un grupo abeliano con la suma y, para todo $a, b \in \mathbb{K}$ y todo $A, B \in M$,

(1) $a \cdot (b \cdot A) = (a \cdot b) \cdot A$,
(2) $1 \cdot A = A$,
(3) $(a + b) \cdot A = a \cdot A + b \cdot A$,
(4) $a \cdot (A + B) = a \cdot A + a \cdot B$.

Un *espacio vectorial por la derecha* sobre $\mathbb{K}$ verifica las mismas propiedades, aplicando los correspondientes cambios de notación (la multiplicación es ahora $a, A \mapsto A \cdot a$); excepto que la primera propiedad cambia con respecto a la enunciada para espacios vectoriales por la izquierda, quedando en este caso expresada como

$$(A \cdot b) \cdot a = A \cdot (b \cdot a).$$

Así, podemos considerar $M_n(\mathbb{K})$ como espacios vectoriales sobre $\mathbb{K}$, y en el caso de $\mathbb{K} = \mathbb{H}$, consideraremos $M_n(\mathbb{H})$ como un espacio vectorial por la derecha.

Esta decisión tiene también consecuencias a la hora de relacionar las matrices con las aplicaciones lineales. Y es que si consideramos $\mathbb{H}^n$ como un espacio vectorial por la derecha, tendremos que definir la aplicación asociada a una matriz $A \in M_n(\mathbb{H})$ como $L_A : \mathbb{H}^n \to \mathbb{H}^n$ tal que para $x \in \mathbb{H}^n$, $L_A(x) = A \cdot x$. En otro caso, la aplicación resultante no es lineal [**8**, p. 16].

Usando esa definición, podemos establecer el concepto de *grupo lineal general* sobre $\mathbb{K}$.

Definición 2.10. El *grupo lineal general* sobre K es:

$$GL_n(\mathbb{K}) = \{A \in M_n(\mathbb{K}) \mid \exists B \in M_n(\mathbb{K}) \text{ tal que } AB = BA = I\}.$$

La matriz B es la inversa de A y la denotamos por A^{-1}. Es decir, el grupo lineal general es el conjunto de matrices con inversa. Equivalentemente, también podemos describir al grupo lineal general como el conjunto de isomorfismos de $\mathbb{K}^n \to \mathbb{K}^n$ [**8**, p. 17].

Proposición 2.11.

$$GL_n(\mathbb{K}) = \{A \in M_n(\mathbb{K}) \mid L_A : \mathbb{K}^n \longrightarrow \mathbb{K}^n \textit{ es un isomorfismo lineal.}\}$$

Para las matrices con coeficientes reales o complejos, tener inversa es equivalente a que su determinante sea no nulo. Para poder llegar a una caracterización similar en las matrices con coeficientes cuaterniónicos, necesitamos primero escribir a las matrices de $GL_n(\mathbb{H})$ como matrices de $GL_m(\mathbb{C})$ para un cierto m. Es por ello por lo que introducimos el siguiente teorema.

Teorema 2.12.

(1) $GL_n(\mathbb{C})$ *es isomorfo a un subgrupo de* $GL_{2n}(\mathbb{R})$.
(2) $GL_n(\mathbb{H})$ *es isomorfo a un subgrupo de* $GL_{2n}(\mathbb{C})$.

Demostración. Para el primer caso, empezamos por $n = 1$. Definimos así $\rho_1 : M_1(\mathbb{C}) \to M_2(\mathbb{R})$ definida por

$$\rho_1(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Para una matriz $A \in M_n(\mathbb{C})$ con $n \geq 1$, construimos $\rho_n(A)$ a partir de los bloques 2×2 resultantes de aplicar ρ_1 a cada entrada de la matriz A. Por ejemplo

$$\rho_1 \begin{pmatrix} a+bi & c+di \\ e+fi & g+hi \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ e & f & g & h \\ -f & e & -h & g \end{pmatrix}.$$

Esta aplicación así definida, es un isomorfismo lineal con su imagen (contenida en $GL_{2n}(\mathbb{R})$) al restringirla a $GL_n(\mathbb{C})$ y además conserva la multiplicación [**8**, p. 25].

En el segundo caso, procedemos de forma similar. Empezamos por el caso $n = 1$, definiendo la aplicación $\psi_1 : M_1(\mathbb{H}) \to M_2(\mathbb{C})$ dada por

$$\psi_1(a + bi + cj + dk) = \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix}$$

y generalizamos para cualquier $n \geq 1$ igual que antes. La aplicación resultante es también un isomorfismo con su imagen (contenida en $GL_{2n}(\mathbb{C})$) al restringirla a $GL_n(\mathbb{H})$ y además conserva la multiplicación [**8**, p. 29]. □

Utilizando la aplicación ψ_n definida en la demostración inmediatamente anterior, podemos definir el determinante de una matriz cuaterniónica. Esta definición consiste únicamente en componer ψ_n con el determinante usual de $M_{2n}(\mathbb{C})$:

$$\det \circ \psi_n : M_n(\mathbb{H}) \longrightarrow \mathbb{C}.$$

Así conseguimos la propiedad esperada [**8**, p. 31].

Proposición 2.13.

$$GL_n(\mathbb{H}) = \{A \in M_n(\mathbb{H}) \mid \det(A) \neq 0\}.$$

Veamos como ejemplo el caso de una matriz 2×2. Sea A una matriz de $M_2(\mathbb{H})$

$$A = \begin{pmatrix} a_{11} + b_{11}i + c_{11}j + d_{11}k & a_{12} + b_{12}i + c_{12}j + d_{12}k \\ a_{21} + b_{21}i + c_{21}j + d_{21}k & a_{22} + b_{22}i + c_{22}j + d_{22}k \end{pmatrix},$$

tendremos que su matriz asociada en $M_4(\mathbb{C})$ será

$$\begin{pmatrix} a_{11} + b_{11}i & c_{11} + d_{11}i & a_{12} + b_{12}i & c_{12} + d_{12}i \\ -c_{11} + d_{11}i & a_{11} - b_{11}i & -c_{12} + d_{12}i & a_{12} - b_{12}i \\ a_{21} + b_{21}i & c_{21} + d_{21}i & a_{22} + b_{22}i & c_{22} + d_{22}i \\ -c_{21} + d_{21}i & a_{21} - b_{21}i & -c_{22} + d_{22}i & a_{22} - b_{22}i \end{pmatrix}.$$

Por lo tanto, el determinante de A será el determinante de esta matriz. Por ejemplo, para $\begin{pmatrix} i & j \\ i & j \end{pmatrix}$ tendremos que la matriz asociada en $M_4(\mathbb{C})$ es

$$\begin{pmatrix} i & 0 & 0 & 1 \\ 0 & -i & -1 & 0 \\ i & 0 & 0 & 1 \\ 0 & -i & -1 & 0 \end{pmatrix}$$

y por tanto que

$$\det \begin{pmatrix} i & j \\ i & j \end{pmatrix} = 0.$$

3.2. Grupos ortogonales. Introducimos ahora el concepto de *grupo ortogonal sobre* $\mathbb{K}$, utilizando para ello el producto escalar definido para $\mathbb{R}$, $\mathbb{C}$ y $\mathbb{H}$ respectivamente.

DEFINICIÓN 2.14. El *grupo ortogonal sobre* $\mathbb{K}$,

$$\mathcal{O}_n(\mathbb{K}) = \{A \in GL_n(\mathbb{K}) \mid \langle x \cdot A | y \cdot A\rangle = \langle x|y\rangle \text{ para todo } x, y \in \mathbb{K}^n\}.$$

Si $\mathbb{K} = \mathbb{R}$, este grupo se denota $O(n)$ y se denomina el *grupo ortogonal*. Si $\mathbb{K} = \mathbb{C}$, se denota $U(n)$ y se denomina el *grupo unitario*. Por último, si $\mathbb{K} = \mathbb{H}$, se denota $Sp(n)$ y se denomina *grupo simpléctico*.

La denominación del grupo $U(n)$ como grupo unitario no es casual, sino que está relacionada con el concepto de operador unitario de un espacio de Hilbert: una matriz $A \in U(n)$ es una matriz unitaria en el sentido de la Definición 1.4. Esto se puede extrapolar a los otros grupos ortogonales.

PROPOSICIÓN 2.15. *Para $A \in GL_n(\mathbb{K})$ son equivalentes*

(1) $A \in \mathcal{O}_n(\mathbb{K})$,
(2) L_A *conserva bases ortonormales; i.e., si* $\{x_1, \ldots, x_n\}$ *es una base ortonormal de* $\mathbb{K}^n$, *entonces* $\{L_A(x_1), \ldots, L_A(x_n)\}$ *lo es también,*
(3) *las columnas de A forman una base ortonormal de* $\mathbb{K}^n$ *y*
(4) $A^\dagger A = I$[3].

DEMOSTRACIÓN. La implicación (1) $\implies$ (2) se deduce de que A conserva el producto escalar. La implicación (2) $\implies$ (3) es porque las columnas de A son las imágenes de la base canónica de $\mathbb{K}^n$ (tal y como hemos definido a L_A). La implicación (3) $\implies$ (4) es debido a que

$$\begin{aligned}(A^\dagger A)_{ij} &= (\text{fila } i \text{ de } A^\dagger)(\text{columna } j \text{ de } A)\\ &= (\text{columna } i \text{ de } A^*)^T(\text{columna } j \text{ de } A)\\ &= \langle(\text{columna } i \text{ de } A)|(\text{columna } j \text{ de } A)\rangle\,.\end{aligned}$$

La implicación (4) $\implies$ (1) ya la hemos visto en la Sección 2 del Capítulo 1.

□

Esta caracterización de las matrices del grupo ortogonal sobre $\mathbb{K}$ nos permite demostrar la siguiente proposición.

PROPOSICIÓN 2.16. *Si $A \in \mathcal{O}_n(\mathbb{K})$, entonces* $|\det(A)| = 1$.

DEMOSTRACIÓN. Como $A^\dagger A = I$, tenemos que (utilizando que $\det(A^\dagger) = \det(A)^*$ [**8**, p. 39])

$$1 = \det(A^\dagger A) = \det(A^\dagger)\det(A) = \det(A)^*\det(A) = |\det(A)|^2.$$

□

[3]La definición de $A^\dagger$ para $A \in M_n(\mathbb{H})$ es la misma que para una matriz compleja, pero utilizando la definición de conjugado de un cuaternión.

Como consecuencia, es evidente que las matrices son inversibles y por tanto elementos de $GL_n(\mathbb{K})$. No solo esto, sino que además $\mathcal{O}_n(\mathbb{K})$ es un subgrupo del grupo lineal general [**8**, p. 36].

El subgrupo

$$SO(n) = \{A \in O(n) \mid \det(A) = 1\}$$

se llama el *grupo ortogonal especial*. El subgrupo

$$SU(n) = \{A \in U(n) \mid \det(A) = 1\},$$

grupo unitario especial. Ambos son subgrupos del grupo lineal general y también del *grupo lineal especial*

$$SL_n(\mathbb{K}) = \{A \in GL_n(\mathbb{K}) \mid \det(A) = 1\}.$$

3.3. Rotaciones y grupos otrogonales. El grupo $SO(3)$ constituye el grupo de las rotaciones en $\mathbb{R}^3$. Como ya hemos visto en la Sección 2.2, cada punto de la esfera S^3 se puede identificar con una rotación en $\mathbb{R}^3$, i.e., con un elemento de $SO(3)$. A pesar de que esta identificación no es un isomorfismo (ni tal isomorfismo existe [**3**, p. 64]), sí que podemos utilizarla para asociar a cada transformación unitaria de $SU(2)$ una rotación de $\mathbb{R}^3$, i.e., identificar los cambios en un qubit con rotaciones de su representación en la esfera de Bloch. Empezamos por identificar $Sp(1)$ con $SU(2)$.

Proposición 2.17. *$SU(2)$ es isomorfo a $Sp(1)$.*

Demostración. Recordemos en primer lugar la definición de la aplicación $\psi_1 : M_1(\mathbb{H}) \to M_2(\mathbb{C})$ de la demostración del Teorema 2.12:

$$\psi_1(a + bi + cj + dk) = \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix}.$$

Esta aplicación la podemos definir también como

$$\psi_1(z + wj) = \begin{pmatrix} z & w \\ -w^* & z^* \end{pmatrix},$$

ya que cualquier cuaternión $a + bi + cj + dk$ se puede expresar de la forma $z + wj$ con $z, w \in \mathbb{C}$, simplemente tomando $z = a + bi$ y $w = c + di$.

Como ya dijimos en su momento, esta aplicación es inyectiva y conserva la multiplicación. Si restringimos la aplicación a $Sp(1)$, tendremos que

$$\psi_1(Sp(1)) = \{\begin{pmatrix} z & w \\ -w^* & z^* \end{pmatrix} \mid z, w \in \mathbb{C} \text{ tales que } |z|^2 + |w|^2 = 1\}.$$

Nos queda ver que $\psi_1(Sp(1)) = SU(2)$.

Dado $r = a + bi + cj + dk \in Sp(1)$, se tiene que $\psi_1(r) = \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix}$, de forma que

$$\psi_1(r)^\dagger \psi_1(r) = \begin{pmatrix} a - bi & -c - di \\ c - di & a - bi \end{pmatrix} \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

ya que $a^2 + b^2 + c^2 + d^2 = 1$. Además, $\det(\psi_1(r)) = 1$, por lo que $\psi_1(r) \in SU(2)$.

Sea ahora $B = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SU(2)$ con $\alpha, \beta, \gamma, \delta \in \mathbb{C}$. Como B es un operador unitario, tenemos que

$$B^\dagger B = \begin{pmatrix} \alpha^* & \gamma^* \\ \beta^* & \delta^* \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Junto con la ecuación $1 = \det B = \alpha\delta - \beta\gamma$, tenemos (siendo las ecuaciones (10) y (11) equivalentes):

$$\alpha^*\alpha + \gamma^*\gamma = 1, \tag{9}$$

$$\alpha^*\beta + \gamma^*\delta = 0, \tag{10}$$

$$\beta^*\alpha + \delta^*\gamma = 0, \tag{11}$$

$$\beta^*\beta + \delta^*\delta = 1, \tag{12}$$

$$\alpha\delta - \beta\gamma = 1. \tag{13}$$

Distinguimos dos casos. El primero, suponemos que $\delta = 0$. En ese caso las ecuaciones quedarían en:

$$\alpha^*\alpha + \gamma^*\gamma = 1, \tag{14}$$

$$\alpha^*\beta = 0, \tag{15}$$

$$\beta^*\beta = 1, \tag{16}$$

$$-\beta\gamma = 1. \tag{17}$$

Las ecuaciones (15) y (16) implican en primer lugar que $\alpha^* = 0$, i.e., $\alpha = 0$. Además, la ecuación (16) implica que el inverso de β es β^*. Por último, usando esto y la ecuación (17) concluimos que $-\gamma$, que también es el inverso de β, es igual a β^*.

Si $\gamma = 0$, también podemos usar el mismo argumento para concluir que $\delta = \alpha^*$ y que $\beta = 0$.

En el segundo caso suponemos que $\delta \neq 0$ y que $\gamma \neq 0$. En ese caso, a partir de la ecuación (10), multiplicando en un primer caso por γ y después por δ^*, y usando las ecuaciones (9), (12) y (13) obtenemos:

$$\alpha^*\beta\gamma + \gamma^*\delta\gamma = 0 \implies \alpha^*\beta\gamma + (1 - \alpha^*\alpha)\delta = 0 \implies \delta = \alpha^*(\alpha\delta - \beta\gamma) = \alpha^*$$

$$\alpha^*\beta\delta^* + \gamma^*\delta\delta^* = 0 \implies \alpha^*\beta\delta^* + \gamma^*(1 - \beta^*\beta = 0 \implies \gamma^* = \beta(\beta\gamma - \alpha\delta) = -\beta$$

Por tanto, juntando ambos casos, concluimos que $\delta = \alpha^*$ y que $\gamma = -\beta^*$. Así, la matriz será de la forma

$$\begin{pmatrix} \alpha & \beta \\ -\beta^* & \alpha^* \end{pmatrix}$$

y será por tanto un elemento de $\psi_1(Sp(1))$.

□

De esta manera, al identificar cada matriz unitaria 2×2 con un elemento de la esfera S^3, podemos a su vez asociarle una rotación de $SO(3)$. La aplicación $Ad : Sp(1) \to SO(3)$ que empezamos a introducir en la Sección 2.2 es la que nos va

a permitir dicha asociación. Para estudiarla en profundidad necesitamos primero introducir una estructura topológica en los grupos de matrices con los que hemos trabajado.

Para ello, simplemente consideramos a los grupos de matrices como subespacios de un espacio topológico euclídeo, teniendo en cuenta las siguientes inclusiones. Dado G un subgrupo de $GL_n(\mathbb{K})$,

$$G \subset GL_n(\mathbb{K}) \subset M_n(\mathbb{K}) \cong \mathbb{K}^{n^2} \cong \begin{cases} \mathbb{R}^{n^2} & \text{si } \mathbb{K} = \mathbb{R}, \\ \mathbb{R}^{2n^2} & \text{si } \mathbb{K} = \mathbb{C}, \\ \mathbb{R}^{4n^2} & \text{si } \mathbb{K} = \mathbb{H}. \end{cases}$$

Una vez que tenemos una topología en $GL_n(\mathbb{K})$, introducimos la siguiente definición.

Definición 2.18. Un *grupo de matrices* es un subgrupo $G \subset GL_n(\mathbb{K})$ que es cerrado en $GL_n(\mathbb{K})$.

Todos los "grupos de matrices" definidos hasta ahora lo son en el sentido de la definición que acabamos de introducir.

Proposición 2.19. *$\mathcal{O}_n(\mathbb{K})$, $SL_n(\mathbb{K})$, $SO(n)$ y $SU(n)$ son grupos de matrices según la Definición 2.18.*

Demostración. Tenemos que probar que todos los grupos anteriores son cerrados en $GL_n(\mathbb{K})$.

Empezemos con $\mathcal{O}_n(\mathbb{K})$. Si definimos $f : M_n(\mathbb{K}) \to M_n(\mathbb{K})$ como $f(A) = AA^\dagger$, obtendremos una aplicación continua ya que cada una de sus componentes $f_{ij}(A) = (AA^\dagger)_{ij} \in \mathbb{K}$ es continua por ser un polinomio en los elementos de A (con coeficientes en $\mathbb{K}$). El conjunto $\{I\}$ es cerrado en $M_n(\mathbb{K})$, luego $\mathcal{O}_n(\mathbb{K}) = f^{-1}(\{I\}) \subset GL_n(\mathbb{K})$ es un cerrado en $M_n(\mathbb{K})$ y por tanto cerrado en $GL_n(\mathbb{K})$.

Para $SL_n(\mathbb{K})$, en vez de usar la aplicación f utilizaremos

$$\det : M_n(\mathbb{K}) \to \mathbb{R} \text{ ó } \mathbb{C}.$$

La aplicación determinante es continua porque, en el caso de $\mathbb{R}$ ó $\mathbb{C}$, es simplemente un polinomio en los elementos de A con coeficientes en el cuerpo correspondiente. En el caso de $\mathbb{H}$, tendremos que es igual a $\det(\psi_n(A))$, es decir, la composición de dos aplicaciones continuas (ψ_n es continua porque cada una de sus componentes es continua por ser proyecciones) y por tanto una aplicación continua. Como $\{1\}$ es cerrado en $\mathbb{K}$, tendremos que $SL_n(\mathbb{K}) = \det^{-1}(\{1\}) \subset GL_n(\mathbb{K})$ es cerrado en $M_n(\mathbb{K})$ y por tanto en $GL_n(\mathbb{K})$.

Por último, $SO(n) = O(n) \cap SL_n(\mathbb{R})$ y $SU(n) = U(n) \cap SL_n(\mathbb{C})$, es decir, son la intersección de dos cerrados y por tanto un cerrado.

□

Además, también se verifica que son espacios compactos, i.e., cerrados y acotados (por estar trabajando en un espacio euclídeo).

PROPOSICIÓN 2.20. *Los grupos $O(n)$, $SO(n)$, $U(n)$, $SU(n)$ y $Sp(n)$ son compactos para cada n.*

DEMOSTRACIÓN. En la Proposición 2.19 hemos visto que son cerrados. Nos falta ver que son también acotados. Utilizando la Proposición 2.15 sabemos que las columnas de cada una de las matrices de estos grupos son vectores unitarios en $\mathbb{K}^n$, luego la longitud de la matriz (como elemento $\mathbb{K}^{n^2}$) es $\sqrt{n}$, es decir, está acotada. □

Una propiedad importante de $SO(3)$ es su conexidad por caminos, de la que nos serviremos después para relacionarlo con $Sp(1)$.

LEMA 2.21. *$SO(3)$ es conexo por caminos.*

DEMOSTRACIÓN. Dada $A \in SO(3)$, podemos escribir

$$A = V \begin{pmatrix} \cos\theta & \sin\theta & 0 \\ -\sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} V^{-1},$$

donde $V \in O(n)$ **[10]**. Tomando

$$A(t) = V \begin{pmatrix} \cos t\theta & \sin t\theta & 0 \\ -\sin t\theta & \cos t\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} V^{-1} \quad 0 \leq t \leq 1,$$

obtenemos un camino entre A y la matriz identidad $I \in SO(3)$, y para todo $t \in [0,1]$, $A(t) \in SO(3)$. Por tanto, hemos encontrado una matriz en $SO(3)$ tal que podemos unir mediante un camino en $SO(3)$ cualquier otra matriz de $SO(3)$ con ella. Esto implica que $SO(3)$ es conexo por caminos. □

Habiendo demostrado este lema, estamos en condiciones de analizar la relación entre $Sp(1)$ y $SO(3)$. Como ya dijimos anteriormente, esta relación se basa en la aplicación

$$Ad : Sp(1) \longrightarrow SO(3),$$

definida de la siguiente forma: para $g \in Sp(1)$, la imagen de g es una aplicación Ad_g tal que para $v \in \mathbb{R}^3$

$$Ad_g(v) = gvg^{-1} \in \mathbb{R}^3,$$

siguiendo la convención de que un cuaternión $xi + yj + zk$ lo escribimos como $(x, y, z) \in \mathbb{R}^3$.

Definida así, esta aplicación es un homomorfismo de grupos sobreyectivo, y, cocientado por su núcleo, su dominio es isomorfo a su imagen.

LEMA 2.22. *Ad es un homomorfismo de grupos y* $\mathrm{Ker}\,(Ad) = \{1, -1\}$.

DEMOSTRACIÓN. Empecemos probando que es un homomorfismo de grupos. Si $r_1, r_2 \in Sp(1)$ y $p \in \mathbb{R}^3$, entonces

$$Ad(r_1r_2)(p) = r_1r_2p(r_1r_2)^* = r_1(r_2pr_2^*)r_1^* = Ad(r_1)(Ad(r_2)(p));$$

por tanto, Ad es un homomorfismo de grupos.

Se tiene que $Ad(1)$ y $Ad(-1)$ son la identidad en $SO(3)$, por tanto 1 y -1 pertenecen a $\mathrm{Ker}\,(Ad)$. Recíprocamente, supongamos que $Ad(q)$ es la identidad en $SO(3)$ con $q = a + bi + cj + dk$. En ese caso $Ad(q)(i) = i$ significa que

$$(a + bi + cj + dk)i(a - bi - cj - dk) = p$$

y a partir de esto obtenemos que

$$(ai-b-ck+dj)(a-bi-cj-dk) = (a^2+b^2-c^2-d^2)i+(2bc+2ad)j+(2bd-2ac)k = i.$$

Por tanto, necesariamente $a^2 + b^2 - c^2 - d^2 = 1$. Sin embargo, por hipótesis $a^2 + b^2 + c^2 + d^2 = 1$, luego $c = 0$ y $d = 0$. Aplicando un argumento similar a $Ad(q)(j) = j$ obtenemos que $b = 0$. Como $a^2 = 1$, $a \in \{1, -1\}$ por lo que $q \in \{1, -1\}$.

□

LEMA 2.23. *$Ad : Sp(1) \to SO(3)$ es sobreyectiva.*

DEMOSTRACIÓN. Como $Sp(1)$ es compacto (Proposición 2.20), su imagen por Ad es un compacto (por ser Ad una aplicación continua: cada componente es un polinomio –ver (8)), y por tanto, es cerrado. Además, Ad es un difeomorfismo lineal, por lo que su imagen es un abierto [**8**, p. 131]. Como $SO(3)$ es conexo por caminos (Lema 2.21), concluimos que la imagen de Ad es el espacio total, i.e., $SO(3)$.

□

Concluimos así que $SO(3)$ es isomorfo a $Sp(1)/\{-1, 1\}$.

4. Puertas lógicas - un qubit

Una vez hemos visto los diferentes grupos de matrices y las relaciones entre ellos, introduciremos ahora las principales puertas lógicas que conforman los "circuitos" de la computación cuántica. Estos circuitos son únicamente una representación de los cambios que experimenta un estado cuántico y son análogos a la computación clásica en el sentido de que se fundamenta en dos elementos: un circuito formado por "cables" y "puertas" que transportan y manipulan la información cuántica.

Pero antes de introducir las puertas lógicas, necesitamos precisar las herramientas que utilizaremos para visualizar geométricamente la acción de las diferentes puertas.

4.1. Operadores unitarios equivalentes. Las puertas lógicas de la computación cuántica coinciden con los operadores unitarios del segundo axioma de la mecánica cuántica, al ser simplemente representaciones de los diferentes cambios que puede experimentar un qubit.

Sin embargo, como hemos visto en los Lemas 2.22 y 2.23, el grupo de rotaciones de $\mathbb{R}^3$, $SO(3)$, es isomorfo a $Sp(1)/\{-1,1\}$, siendo $Sp(1)$ isomorfo a las transformaciones unitarias con determinante 1, $SU(2)$. Por tanto, si queremos usar esta relación, tenemos de alguna forma que relacionar al grupo $U(2)$ con $SU(2)$ en el contexto de los qubits.

Como ya hemos visto, al multiplicar un qubit por un factor de fase global $\exp(i\gamma)$, obtenemos un qubit "idéntico" desde el punto de vista de las posibles mediciones que hagamos sobre el qubit. Por tanto, en vez de tomar un operador unitario "tal cual", simplemente lo ponemos como un operador de $SU(2)$ multiplicado por un factor de fase global.

LEMA 2.24. *Dada $U \in U(2)$, existe $\gamma \in \mathbb{R}$ y $U' \in SU(2)$ tales que*

$$U = \exp(i\gamma)U'.$$

DEMOSTRACIÓN. Por la Proposición 2.16, $|\det(U)| = 1$. Sea así $\gamma \in \mathbb{R}$ tal que $\exp(i\gamma)^2 = \det(U)$ y sea $U' = \exp(-i\gamma)U$.

Tendremos que

$$\det(U') = \det(\exp(-i\gamma)U) = \exp(-i\gamma)^2 \det(U) = \frac{1}{\det(U)} \det(U) = 1$$

y que

$$U = \exp(i\gamma)\exp(-i\gamma)U = \exp(i\gamma)U'.$$

□

Con esto, podemos ver el efecto de un operador unitario U simplemente considerando el efecto del operador U' construido en la demostración del lema, efecto que desde el punto de vista de las mediciones es exactamente el mismo: para $\gamma \in \mathbb{R}$,

$$U' |\psi\rangle = U' \exp(-i\gamma) |\psi\rangle = U |\psi\rangle .$$

4.2. De $SU(2)$ a $SO(3)$. Por último antes de presentar las diferentes puertas lógicas, tenemos que comprobar que la relación entre $SU(2)$ y $SO(3)$ que hemos definido tiene sentido al ponerla en práctica; es decir, tomando las aplicaciones $f : \mathbb{C} \times \mathbb{C} \to \mathbb{H}$ y $h : S^3 \subset \mathbb{H} \to S^2 \subset \mathbb{R}^3$ definidas en la Sección 2.2, tenemos que comprobar si $(h \circ f)(U |\psi\rangle)$ con $U \in SU(2)$ coincide con $A((h \circ f)(|\psi\rangle))$ siendo $A \in SO(3)$ la rotación que asociamos a la matriz U por las aplicaciones que hemos definido; i.e., si el siguiente diagrama (donde $W \subset \mathbb{C} \times \mathbb{C}$ es el conjunto de elementos de $\mathbb{C} \times \mathbb{C}$ que son unitarios) conmuta:

$$\begin{array}{ccc} W \subset \mathbb{C}\times\mathbb{C} & \xrightarrow{U} & W \subset \mathbb{C}\times\mathbb{C} \\ \downarrow f & & \downarrow f \\ S^3 \subset \mathbb{H} & & S^3 \subset \mathbb{H} \\ \downarrow h & & \downarrow h \\ S^2 \subset \mathbb{R}^3 & \xrightarrow{A} & S^2 \subset \mathbb{R}^3 \end{array} \tag{18}$$

La matriz A la construimos usando lo que hemos definido en la Sección 3:

$$SU(2) \xrightarrow{\psi_1^{-1}} Sp(1) \xrightarrow{Ad} SO(3)$$

Así, $A = Ad(\psi_1^{-1}(U))$. Veamos que efectivamente el diagrama conmuta.

PROPOSICIÓN 2.25. *El diagrama* (18)*, donde* $A = Ad(\psi_1^{-1}(U))$*, conmuta.*

DEMOSTRACIÓN. Sea $(a+bi, c+di) \in \mathbb{C}\times\mathbb{C}$ un vector unitario (estado de un qubit), y sea $U = \begin{pmatrix} x+yi & z+wi \\ -z+wi & x-yi \end{pmatrix}$ una matriz de $SU(2)$ (imagen recíproca de $(x,y,z,w) \in \mathbb{H}$ por ψ_1).

Tenemos que

$$\begin{aligned} (h\circ f)((U(a+bi, c+di))) =& -a^2w^2 + a^2x^2 + a^2y^2 - a^2z^2 + 4acwy + 4acxz \\ & - 4adwx + 4adyz - b^2w^2 + b^2x^2 + b^2y^2 - b^2z^2 \\ & + 4bcwx - 4bcyz + 4bdwy + 4bdxz + c^2w^2 - c^2x^2 \\ & - c^2y^2 + c^2z^2 + d^2w^2 - d^2x^2 - d^2y^2 + d^2z^2 \\ =& (x + yi + zj + wk) \\ & ((a^2 + b^2 - c^2 - d^2)i + 2(ad - bc)j + 2(bd + ac)k) \\ & (x - yi - zj - wk) \\ =& A((h\circ f)(a+bi, c+di)) \end{aligned}$$

donde $A = Ad(x, y, z, w)$.

□

4.3. Principales puertas lógicas. El primer grupo de puertas lógicas importantes son las matrices de Pauli. Estos tres operadores, junto con la matriz identidad y la multiplicación por ± 1 y $\pm i$ constituyen lo que se denomina el *grupo de Pauli*. La primera de ellas es la análoga a la puerta NOT en el caso clásico. La podemos representar en forma matricial como

$$X \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

o, usando la notación bra-ket, como $X = |0\rangle\langle 1| + |1\rangle\langle 0|$. Al actuar sobre el estado $\alpha|0\rangle + \beta|1\rangle$, que representaremos en la base $\{|0\rangle, |1\rangle\}$ como $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$, obtendremos

$\alpha\,|1\rangle + \beta\,|0\rangle$, lo que podemos escribir en forma matricial como

$$X\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}\beta\\ \alpha\end{pmatrix}.$$

También se puede denotar a esta puerta por σ_x. Nótese que X es un operador unitario y que por tanto la condición de que el vector de estado sea unitario se mantiene al aplicar el operador. En los diagramas denotaremos a esta puerta como vemos en la Figura 2.2.

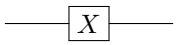

FIGURA 2.2. Representación en un diagrama de la puerta X.

La segunda puerta de este grupo es la puerta Y o también denotada por σ_y, representada matricialmente como

$$Y \equiv \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}$$

y en los diagramas como vemos en la Figura 2.3.

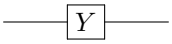

FIGURA 2.3. Representación en un diagrama de la puerta Y.

La tercera es la puerta Z, también denotada por σ_z, con representación matricial

$$Z \equiv \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}.$$

En los diagramas aparece como vemos en la Figura 2.4.

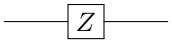

FIGURA 2.4. Representación en un diagrama de la puerta Z.

Siguiendo lo que hemos probado en el Lema 2.24, podemos tomar

$$X' = \begin{pmatrix} 0 & \exp\left(-i\frac{\pi}{2}\right) \\ \exp\left(-i\frac{\pi}{2}\right) & 0 \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix},$$
$$Y' = \begin{pmatrix} 0 & -\exp\left(-i\frac{\pi}{2}\right)i \\ \exp\left(-i\frac{\pi}{2}\right)i & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$
$$Z' = \begin{pmatrix} \exp\left(-i\frac{\pi}{2}\right) & 0 \\ 0 & -\exp\left(-i\frac{\pi}{2}\right) \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}.$$

Usando esto y la demostración de la Proposición 2.17, obtenemos que

$$X' = \psi_1(-ij) = \psi_1(-k) \quad Y' = \psi_1(-j) \quad Z' = \psi_1(-i),$$

y, aplicando el homomorfismo Ad, para X' tenemos

$$(x, y, z) \in \mathbb{R}^3 \mapsto (-k)(xi + yj + zk)k = -xi - yj + zk = (-x, -y, z) \in \mathbb{R}^3,$$

es decir, X' es una rotación de ángulo π respecto al eje z.

Para Y' tenemos,

$$(x, y, z) \in \mathbb{R}^3 \mapsto (-j)(xi + yj + zk)j = xi - yj + zk = (-x, y, -z) \in \mathbb{R}^3,$$

es decir, Y' es una rotación de ángulo π respecto al eje y.

Por último, para Z',

$$(x, y, z) \in \mathbb{R}^3 \mapsto (-i)(xi + yj + zk)i = xi - yj - zk = (x, -y, -z) \in \mathbb{R}^3,$$

es decir, Z' es una rotación de ángulo π respecto al eje x.

Estas rotaciones se aplican sobre la representación de un qubit en la esfera de Bloch, y su imagen coincide, como ya demostramos en la Proposición 2.25, con la imagen del qubit por la trasformación unitaria X', Y', Z' (ó X, Y, Z) representada en la esfera de Bloch.

El llamar a las puertas X, Y, Z hace referencia a la esfera de Bloch utilizada normalmente. Con la esfera de Bloch que usamos en este trabajo, la puerta Y hacer referencia a la rotación con respecto al eje y, mientras que las puertas X y Z lo hacen a las rotaciones con respecto a los ejes z y x respectivamente. Esto se debe a lo que comentamos al presentar la esfera de Bloch: los ejes x y z están intercambiados en nuestro caso respecto a la convención usada habitualmente.

La siguiente puerta importante es la puerta de *Hadamard*

$$H \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Usando el Lema 2.24, construimos

$$H' = \frac{1}{\sqrt{2}} \begin{pmatrix} \exp\left(-i\frac{\pi}{2}\right) & \exp\left(-i\frac{\pi}{2}\right) \\ \exp\left(-i\frac{\pi}{2}\right) & -\exp\left(-i\frac{\pi}{2}\right) \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} -i & -i \\ -i & i \end{pmatrix},$$

y, al igual que antes,

$$H' = \psi_1(-\frac{1}{\sqrt{2}}i - \frac{1}{\sqrt{2}}k).$$

Así, usando la Proposición 2.17, obtenemos en $\mathbb{R}^3$

$$(x,y,z) \mapsto (-\frac{1}{\sqrt{2}}i - \frac{1}{\sqrt{2}}k)(xi+yj+zk)(\frac{1}{\sqrt{2}}i + \frac{1}{\sqrt{2}}k) = zi - yj + xk = (z,-y,x),$$

i.e., H' es una rotación respecto al subespacio generado por $(1,0,1)$, el autovector asociado al autovalor 1. Esta puerta se denota en los circuitos como vemos en la Figura 2.5.

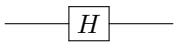

FIGURA 2.5. Representación en un diagrama de la puerta de Hadamard.

Por último, consideramos las puertas

$$S \equiv \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad \text{y} \quad T \equiv \begin{pmatrix} 1 & 0 \\ 0 & \exp(\frac{i\pi}{4}) \end{pmatrix},$$

que, aplicando los mismos pasos que antes se relacionan con

$$S' = \begin{pmatrix} \exp(-i\frac{\pi}{4}) & 0 \\ 0 & \exp(-i\frac{\pi}{4})i \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i & 0 \\ 0 & \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i \end{pmatrix}$$

y

$$T' = \begin{pmatrix} \exp(-i\frac{\pi}{8}) & 0 \\ 0 & \exp(-i\frac{\pi}{8})\exp(\frac{i\pi}{4}) \end{pmatrix} = \begin{pmatrix} \cos\frac{\pi}{8} - i\sin\frac{\pi}{8} & 0 \\ 0 & \cos\frac{\pi}{8} + i\sin\frac{\pi}{8} \end{pmatrix}.$$

De esa forma,

$$S' = \psi_1(\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i) \quad \text{y} \quad T' = \psi_1(\cos\frac{\pi}{8} - i\sin\frac{\pi}{8}),$$

y por tanto, para S', obtenemos como elemento de $SO(3)$ la aplicación

$$(x,y,z) \in \mathbb{R}^3 \mapsto (\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i)(xi+yj+zk)(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i) = xi+zj-yk = (x,z,-y) \in \mathbb{R}^3,$$

es decir, una rotación respecto al eje x de ángulo $\frac{\pi}{2}$. Para T', obtenemos

$$\begin{aligned}(x,y,z) \in \mathbb{R}^3 &\mapsto (\cos\frac{\pi}{8} - i\sin\frac{\pi}{8})(xi+yj+zk)(\cos\frac{\pi}{8} + i\sin\frac{\pi}{8}) \\ &= ((1+\frac{1}{\sqrt{2}})x, (1+\frac{1}{\sqrt{2}})z, -\frac{1}{2}(2+\sqrt{2})y) \in \mathbb{R}^3,\end{aligned}$$

es decir, una rotación respecto a eje x de ángulo $\frac{\pi}{4}$. A la puerta S se le denomina la puerta de *fase* y a T la puerta $\frac{\pi}{8}$. En los diagramas se representan como vemos en la Figura 2.6.

Otro elemento importante en los circuitos, las mediciones (que introdujimos en el tercer axioma de la mecánica cuántica), se denotan como vemos en la Figura 2.7.

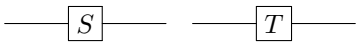

FIGURA 2.6. Representación en los diagramas de las puertas S y T.

FIGURA 2.7. Representación de una medición en un diagrama.

5. Puertas lógicas - varios qubits

Pasamos ahora a las puertas en las que intervienen varios qubits. Recordemos que el espacio de estados al tener varios qubits es el producto tensor de los espacios de estados de cada uno de los qubits. Así, si tenemos dos qubits, una base del espacio de estados será

$$\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}.$$

Sin embargo, para simplificar la notación, escribiremos

$$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}.$$

Como tenemos una base con cuatro elementos, el espacio vectorial es isomorfo a $\mathbb{R}^4$ y podemos escribir

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

Por otro lado, igual que con un único qubit, los operadores que actúan sobre el sistema son operadores unitarios. Veamos ahora que el producto de dos operadores unitarios que actúan sobre un único qubit es un operador unitario sobre dos qubits.

Por definición [**11**, p. 57], dados U_1, U_2 operadores en un espacio de estados de un único qubit,

$$(U_1 \otimes U_2)^\dagger = U_1^\dagger \otimes U_2^\dagger.$$

Así, tendremos que

$$(U_1 \otimes U_2)^\dagger (U_1 \otimes U_2) = (U_1^\dagger U_1) \otimes (U_2^\dagger U_2) = I \otimes I$$

ya que como ya vimos en (1), $(A \otimes B)(|\psi\rangle \otimes |\phi\rangle) = (A|\psi\rangle) \otimes (B|\phi\rangle)$.

De esta forma, a partir de las puertas que actúan sobre un único qubit, podemos construir puertas que actúan sobre varios qubits. Sin embargo, hay algunas puertas que no se pueden expresar como producto de puertas para un solo qubit [**11**, p. 57]. Entre estas puertas se encuentra la puerta $CNOT$. Esta puerta se denota en un circuito como vemos en la Figura 2.8. donde $|x_1\rangle$ es el *qubit de control* y $|x_0\rangle$ es el *qubit objetivo*. La representación y nomenclatura de esta puerta se debe al

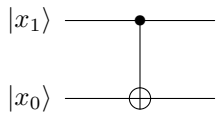

FIGURA 2.8. Representación de la puerta $CNOT$ en un diagrama.

Antes		Después	
Control	Objetivo	Control	Objetivo
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

TABLA 1. Acción de la puerta $CNOT$.

funcionamiento de la puerta: el qubit $|x_1\rangle$ no cambia mientras que el qubit $|x_0\rangle$ sí se ve afectado y el cambio depende del valor de $|x_1\rangle$, como vemos en la Figura 2.9.

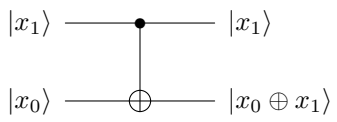

FIGURA 2.9. Representación de la puerta $CNOT$ en un diagrama.

Una forma de representar la acción de esta puerta es mediante una tabla, donde se recoge la imagen de la base del espacio de Hilbert, véase la Tabla 1.

Otra forma es representarla como una matriz actuando sobre $\mathbb{R}^4$ con la base que explicitamos antes. De esta forma, obtenemos la siguiente matriz, cuya acción coincide con la Tabla 1:

$$U_{CN} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

CAPÍTULO 3

Un par de ejemplos

En este último capítulo mostraremos un par de ejemplos que nos mostrarán en primer lugar una deficiencia de la computación cuántica, el no poder hacer una copia de un qubit, y en segundo lugar una de sus fortalezas: el paralelismo cuántico.

1. Clonación, no; teletransporte, sí

Empecemos probando que no es posible hacer una copia de un qubit [**6**, p. 532].

Supongamos en primer lugar que tenemos dos qubits, uno en un estado $|\psi\rangle$ que queremos copiar y otro qubit en un estado $|s\rangle$ que queremos que cambie al estado $|\psi\rangle$. Por tanto, el estado inicial del sistema será

$$|\psi\rangle \otimes |s\rangle \,.$$

Supongamos que una transformación unitaria U efectúa la acción de copiar el qubit, idealmente

$$|\psi\rangle \otimes |s\rangle \mapsto U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle \,.$$

Supongamos también que funciona para dos estados concretos $|\psi\rangle$ y $|\phi\rangle$. Entonces tendríamos

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle \,, \text{ y}$$
$$U(|\phi\rangle \otimes |s\rangle) = |\phi\rangle \otimes |\phi\rangle \,.$$

Si ahora hacemos el producto escalar de las dos ecuaciones, obtendremos usando (2) (ver [**11**, p. 16]) y el hecho de que los operadores unitarios conservan el producto escalar,

$$\langle\psi|\phi\rangle \langle s|s\rangle = \langle\psi|\phi\rangle = (\langle\psi|\phi\rangle)^2.$$

Pero la ecuación $x = x^2$ sólo tiene dos soluciones en $\mathbb{C}$: $x = 0$ ó $x = 1$; así, o $|\psi\rangle = |\phi\rangle$ o son ortogonales.

Por tanto, si una transformación unitaria clona a un estado, tan solo puede funcionar para ese estado y todos los estados ortogonales. Es decir, es imposible conseguir un sistema de clonación que funcione en todos los casos.

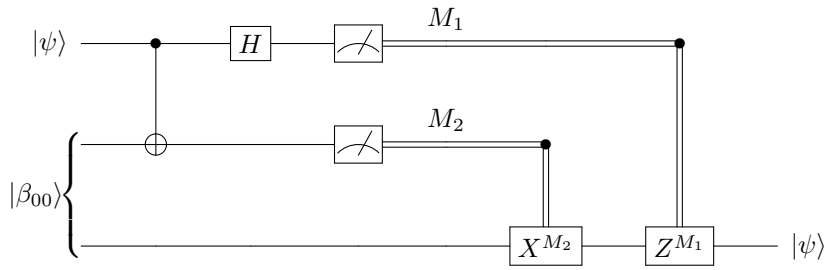

FIGURA 3.1. Circuito de teletransportación de un qubit [**6**, p. 27].

Sin embargo, sí es posible "teletransportar" un qubit de un lugar a otro mediante el envío de información clásica.

El circuito que permite hacer esto se puede ver en la Figura 3.1 que ahora analizaremos. Empecemos por explicar la situación. Supongamos que dos personas, Alice y Bob, tuvieron un encuentro pero ahora se encuentran separados. En dicho encuentro generaron un par de qubits en un *estado EPR* (también llamados *estados Bell*), i.e., en alguno de los siguientes estados

$$\begin{aligned}
|\beta_{00}\rangle &= \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \\
|\beta_{01}\rangle &= \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \\
|\beta_{10}\rangle &= \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \\
|\beta_{11}\rangle &= \frac{|01\rangle - |10\rangle}{\sqrt{2}},
\end{aligned}$$

y cada uno de ellos se llevó uno de los dos qubits. Ahora Alice quiere enviarle a Bob otro qubit $|\psi\rangle$, pero no sabe el estado en que se encuentra el qubit y tan solo puede enviar información clásica a Bob.

Supongamos que $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ y que el estado EPR que generaron era $|\beta_{00}\rangle$. Así, el estado inicial del sistema representado en la Figura 3.1 será[1]

$$|\psi_0\rangle = |\psi\rangle\,|\beta_{00}\rangle = \frac{1}{\sqrt{2}}[\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|00\rangle + |11\rangle)].$$

Alice tiene los dos primeros qubits (las dos primeras filas del diagrama) y Bob el tercero (la última fila del diagrama).

Lo primero que hace Alice es aplicar una puerta $CNOT$ a sus qubits obteniendo

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\big[\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|10\rangle + |01\rangle)\big].$$

[1]Denotamos el producto tensor $|\psi\rangle \otimes |\psi\rangle$ como $|\psi\rangle\,|\phi\rangle$ para simplificar la notación.

A continuación, envía el qubit $|\psi\rangle$, que era el qubit de control en la puerta $CNOT$, a través de una puerta de Hadamard, obteniendo

$$|\psi_2\rangle = \frac{1}{2}\big[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)\big].$$

Reescribiendo el estado obtenemos

$$\begin{aligned}|\psi_2\rangle =& \frac{1}{2}\big[\,|00\rangle\,(\alpha\,|0\rangle + \beta\,|1\rangle) + |01\rangle\,(\alpha\,|1\rangle + \beta\,|0\rangle)\\ &+ |10\rangle\,(\alpha\,|0\rangle - \beta\,|1\rangle) + |11\rangle\,(\alpha\,|1\rangle - \beta\,|0\rangle)\big].\end{aligned}$$

Una vez Alice llega a este punto, el sistema se puede encontrar en cuatro estados igualmente probables:

$$\begin{aligned}&|00\rangle\,(\alpha\,|0\rangle + \beta\,|1\rangle),\\ &|01\rangle\,(\alpha\,|1\rangle + \beta\,|0\rangle),\\ &|10\rangle\,(\alpha\,|0\rangle - \beta\,|1\rangle) \text{ y}\\ &|10\rangle\,(\alpha\,|0\rangle - \beta\,|1\rangle).\end{aligned}$$

Alice mide entonces el estado de sus dos qubits, obteniendo los resultados M_1 y M_2 respectivamente, y el sistema de tres qubits colapsa a uno de los cuatro estados posibles. De esta forma, cuando Alice envía a Bob el resultado de su medición, Bob sabe en cuál de los estados ($\alpha\,|0\rangle + \beta\,|1\rangle$, $\alpha\,|1\rangle + \beta\,|0\rangle$, $\alpha\,|0\rangle - \beta\,|1\rangle$ ó $\alpha\,|0\rangle - \beta\,|1\rangle$) se encuentra su qubit, y lo único que tiene que hacer es aplicar la puerta X M_2 veces y la puerta Z M_1 veces para transformar su qubit al mismo estado en el que estaba $|\psi\rangle$, es decir, el estado $\alpha\,|1\rangle + \beta\,|0\rangle$.

Así, logra "teletransportar" su qubit y enviárselo a Bob únicamente enviando información clásica. Esto no contradice el principio de no clonación que veíamos antes, ya que el qubit que tenía Alice colapsa al estado $|0\rangle$ o al estado $|1\rangle$.

2. El algoritmo de Deutsch

2.1. Paralelismo cuántico. El *paralelismo cuántico* es una propiedad esencial utilizada por los algoritmos de la computación cuántica. A grosso modo permite evaluar una función en diferentes puntos simultáneamente, con una única operación.

Tomemos por ejemplo una función $f(x) : \{0,1\} \to \{0,1\}$. Al introducir esta función en un algoritmo cuántico usaremos dos qubits con estado inicial $|x,y\rangle$ y mediante una sucesión adecuada de puertas lógicas transformaremos dicho estado en $|x, y \oplus f(x)\rangle$ donde $\oplus$ denota la adición módulo 2 [**6**, p. 31]. Denotaremos a esta sucesión de puertas como U_f.

Ahora bien, si partimos del estado $\frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes |0\rangle$, que podemos obtener haciendo actuar la puerta de Hadamard sobre el qubit $|0\rangle$, y aplicamos U_f (como vemos en la Figura 3.2), obtendremos el estado

$$\frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}.$$

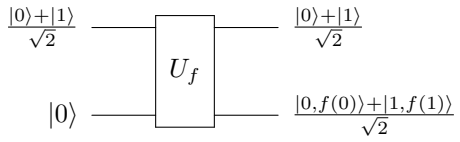

FIGURA 3.2. Ejemplo de U_f actuando sobre dos qubits.

Observamos así que, haciendo actuar únicamente una vez a U_f, obtenemos información de $f(0)$ y de $f(1)$ como si los hubiésemos evaluado simultáneamente. Esto es lo que se denomina *paralelismo cuántico*.

Podemos generalizar este proceso a un número arbitrario de qubits usando lo que se denomina la *transformada de Hadamard*. Básicamente consiste en aplicar la puerta de Hadamard simultáneamente a n qubits. Por ejemplo, si tenemos dos qubits en el estado $|0\rangle$ y hacemos la transformada de Hadamard obtendremos

$$\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)=\frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2}.$$

Podemos resumir el resultado de la transformada de Hadamard actuando sobre n qubits en estado $|0\rangle$ de la siguiente forma:

$$\frac{1}{\sqrt{2^n}}\sum_x |x\rangle,$$

donde x representa cada uno de los estados del sistema de n qubits.

Si tenemos un sistema con n qubits a los que hemos aplicado la transformada de Hadamard y otro qubit en estado $|0\rangle$, podemos aplicar algo similar a U_f y obtener así

$$\frac{1}{\sqrt{2^n}}\sum_x |x\rangle\,|f(x)\rangle,$$

habiendo en cierta forma evaluado f en todos los posibles valores del sistema de n qubits.

Ahora bien, en los dos ejemplos anteriores, obtuvimos un estado cuántico final combinación de las imágenes de los valores posibles de un qubit; pero no podemos obtener a partir de eso directamente dichos valores, porque el qubit nos dará al medirlo, por ejemplo en el primer caso, bien $|0, f(0)\rangle$ o bien $|1, f(1)\rangle$. Sin embargo, sí que es posible aprovechar esta propiedad y obtener más información que $f(0)$ o $f(1)$.

Veamos un algoritmo simple que utiliza el paralelismo cuántico para obtener en una única operación lo que en un ordenador tradicional requeriría al menos dos, mostrando así que se puede aprovechar esta propiedad y que la computación cuántica supera las posibilidades de la computación clásica.

2.2. El algoritmo de Deutsch. Retomando el circuito de la Figura 3.2, si en vez tener al segundo qubit en el estado $|0\rangle$ le aplicamos al estado $|1\rangle$ una puerta de Hadamard, obteniendo el estado inicial $\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes\frac{|0\rangle-|1\rangle}{\sqrt{2}}$, tendremos la base del algoritmo de Deutsch, representado en la Figura 3.3.

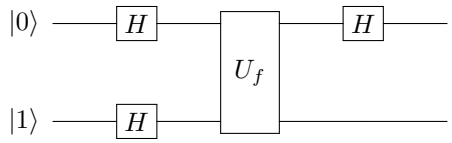

FIGURA 3.3. Circuito que ejecuta el algoritmo de Deutsch.

Dado el estado inicial $|\psi_0\rangle = |01\rangle$, obtenemos el estado

$$|\psi_1\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right).$$

Ahora, al aplicar U_f a $|\psi_1\rangle$, obtenemos una de las siguientes posibilidades [**6**, p. 33].

$$|\psi_2\rangle = \begin{cases} \pm\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & \text{si } f(0) = f(1), \\ \pm\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & \text{si } f(0) \neq f(1). \end{cases}$$

Al aplicar por último la puerta de Hadamard al primer qubit, tenemos

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & \text{si } f(0) = f(1), \\ \pm|1\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & \text{si } f(0) \neq f(1). \end{cases}$$

Llegados a este punto, nos encontramos con que $f(0) \oplus f(1)$ es 0 si $f(0) = f(1)$ y es 1 en otro caso, por lo que podemos escribir $|\psi_3\rangle$ como

$$|\psi_3\rangle = \pm|f(0) \oplus f(1)\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right),$$

de forma que al medir el primer qubit, obtendremos el valor de $f(0) \oplus f(1)$.

La importancia de este algoritmo es que obtenemos $f(0) \oplus f(1)$ evaluando f mediante U_f únicamente una vez. Y aquí es donde radica el potencial de la computación cuántica y lo que la convierte en un paradigma totalmente diferente al de la computación clásica, aportando nuevos algoritmos que permiten superar las capacidades de los ordenadores tradicionales.

Bibliografía

[1] Scott Aaronson, *Quantum computing since Democritus*, Cambridge University Press, 2013.

[2] Sheldon Axler, *Linear algebra done right*, Springer, Cham, 2015.

[3] M. L. Curtis, *Matrix groups*, Springer-Verlag New York, 1984.

[4] Brian C. Hall, *Quantum theory for mathematicians*, Springer-Verlag New York, 2013.

[5] David W. Lyons, *An elementary introduction to the Hopf fibration*, Mathematics Magazine **76** (2003Apr), no. 2, 87–98.

[6] Michael A. Nielsen and Isaac L. Chuang, *Quantum computation and quantum information*, Cambridge University Press, 2000.

[7] Eleanor Rieffel and Wolfgang Polak, *Quantum computing: A gentle introduction*, The MIT Press, 2011.

[8] Kristopher Tapp, *Matrix groups for undergraduates*, Second edition, American Mathematical Society, 2016.

[9] B. L. van der Waerden, *Hamilton's discovery of quaternions*, Mathematics Magazine **49** (1976Nov.), no. 5, 227–234.

[10] Yung-Chow Wong and Yik-Hoi Au-Yeung, *An elementary and simple proof of the connectedness of the classical groups*, The American Mathematical Monthly **74** (1967Oct.), no. 8, 964–966.

[11] Bernard Zygelman, *A first introduction to quantum computing and information*, Springer, Cham, 2018.

Índice alfabético