Publicaciones Electrónicas
Sociedad Matemática Mexicana

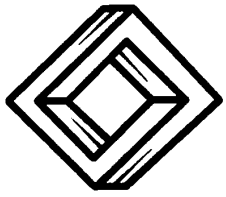
Una breve revisión de Álgebras de Clifford y Cómputo Cuántico

Curso Introductorio

Dalia Cervantes
Guillermo Morales-Luna

www.smm.org.mx

Serie: Textos. Vol. 19 (2016)



Dalia Cervantes y Guillermo Morales-Luna
Departamento de Computación, CINVESTAV-IPN, Ciudad de México, México

Una breve revisión de álgebras de Clifford y Cómputo Cuántico

– Curso introductorio –

Octubre de 2016

Cinvestav-IPN

Proemio

El presente texto es introductorio al Cómputo Cuántico y se presenta de manera rigurosa desde un punto de vista del formalismo matemático. Aunque las disciplinas de estudio en Física y en Matemáticas han sido diversas, hemos querido aquí presentar un enfoque unificado que concilie la teoría física con la práctica matemática y viceversa. Hacemos una breve revisión de las álgebras de Clifford y de sus relaciones con el Cómputo Cuántico.

1 de octubre de 2016 *Dalia Cervantes y Guillermo Morales-Luna*

Índice

Capítulo 1
Introducción

Resumen En esta Introducción exponemos las motivaciones para eleborar el presente texto y describimos someramente su estructura.

El presente texto tiene un carácter principalmente didáctico, buscando dar una visión panorámica de los principales conceptos de Física y de Algebra utilizados en el Cómputo Cuántico. Tiene pues como propósito, introducir y acercar a estudiantes de Física y de Matemáticas a un área de estudio y de desarrollo de gran potencial tecnológico: el Cómputo Cuántico. Así, hemos buscado un equilibrio en la presentación entre el formalismo matemático, la práctica y el razonamiento de tipo físico.

No reclamamos originalidad alguna en este texto, hemos incluido una larga lista de referencias bibliográficas en la esperanza de que el lector reconozca los orígenes de las ideas y las fuentes donde ha de profundizar su conocimiento en los temas aquí expuestos. Tampoco hemos pretendido hacer una recopilación exhaustiva de todas las nociones relevantes. Una tal tarea de tipo enciclopédico es colosal y va más allá de nuestras intenciones y capacidades.

Hemos querido partir de ideas de tipo físico para después desarrollarlas con abstracciones formales matemáticas.

Esta "breve revisión" habrá de estar en constante desarrollo, por lo que estimamos que en algún momento dejará de ser "breve", y seguramente, habremos también de incluir resultados propios en estos temas, por lo que ya no será una mera "revisión".

Invitamos al lector a que nos haga llegar sus comentarios y observaciones, así como señalamientos a errores u omisiones. Apreciaríamos en extremo poder enriquecer el presente texto con las observaciones de sus lectores.

Iniciamos con una presentación de algunos conceptos de la Física Clásica, como las nociones de campo y de las ecuaciones de Maxwell. Esto para ilustrar el uso de la Física Matemática y de las formas diferenciales, las cuales surgen de un álgebra alternante que a su vez está emparentada con el producto tensorial de espacios vectoriales. El Cómputo Cuántico tiene lugar en productos tensoriales de espacios de Hilbert.

Discutimos el experimento de Stern-Gerlach como una introducción a la Mecánica Cuántica y precisamos las nociones de estado y de observables. Aquí introducimos tanto estados puros como mixtos, los cuales son de hecho distribuciones de probabilidad entre estados puros.

La noción de enredamiento, acaso también denotada como entrelazamiento, es esencial de la Mecánica Cuántica. En los orígenes de ésta, el enredamiento fue presentado como una incompletitud, en el mejor de los casos, o, de plano, como una paradoja, en el peor de los casos, inherente a la Mecánica Cuántica por Einstein, Rosen y Podolski. Ciertamente el enredamiento estaba en el centro de la célebre polémica entre Bohr y Einstein. En la actualidad, el enredamiento se utiliza en protocolos de comunicación segura de tipo cuántico, y desde la década de los 60, cuando se probó experimentalmente su existencia, hasta la actual en la que se han tendido redes de comunicacón de varios kilómetros de extensión, el enredamiento ha demostrado su efectividad en las comunicaciones y en otras aplicaciones. Opuesta a la noción de enredamiento, está la de separabilidad, y diversas medidas de enredamiento han sido introducidas. Aquí nos referimos a algunas de ellas.

Los grupos de simetría han sido aplicados en diversas áreas de la Mecánica Cuántica, tanto para describir transformaciones de tipo geométrico como para caracterizar espacios de soluciones de ecuaciones diferenciales que surgen en el estudio de la Mecánica Cuántica. Un aspecto esencial del Cómputo Cuántico es la relación entre la esfera unitaria de un espacio de Hilbert y algunos grupos de simetría.

Las álgebras de Clifford incluyen a los operadores usuales en el Cómputo Cuántico, por lo que éste se reduce a transformaciones homomorfas entre álgebras de Clifford. Presentamos éstas de manera apenas suficiente (pues el tema es inmenso y excede con mucho los límites que nos hemos fijado para el presente texto) para analizar la reducción del Cómputo Cuántico a ellas.

Un aspecto sumamente relevante de esta reducción es el concepto de universalidad.

Capítulo 2
Elementos de Física Clásica

Resumen Presentamos temas propios de la Física Clásica con el fin de ilustrar la modelación de procesos físicos utilizando conceptos de grupos de simetría y de álgebras alternantes. Veremos que las ecuaciones de Maxwell pueden ser presentadas en términos de productos externos de espacios de Hilbert.

2.1 Campos dinámicos

Seguiremos aquí la presentación en [Varadarajan(2004)]. Recordamos tratamientos convencionales de Mecánica Clásica y Electrodinámica, con el fin de ilustrar el uso de conceptos propios de grupos, variedades diferenciables y formas diferenciales. En [Arnold(1989), Goldstein et al(2002)] se puede profundizar estas presentaciones.

Mecánica Clásica.

Un problema fundamental en la Mecánica Clásica consiste en determinar la correspondencia entre campos vectoriales y homomorfismos.

Sea S un conjunto de *estados* y sea S^S la colección de funciones $S \to S$. Definimos

$$\mathrm{Sim}(S) = \{f : S \to S \,|\, f \text{ es biyectiva}\},$$

el cual es un grupo con la composición de funciones y la identidad como elemento neutro. $\mathrm{Sim}(S)$ es el *grupo simétrico* correspondiente al conjunto S. Sea $c : \mathbb{R} \to \mathrm{Sim}(S)$ un homomorfismo $(\mathbb{R}, +) \to (\mathrm{Sim}(S), \circ)$, escrito como $t \mapsto c_t$. Así pues para todos $t, s \in \mathbb{R}$: $c_{t+s} = c_t \circ c_s$.

Supóngase que S es una variedad C^∞-diferenciable en $\mathbb{R}^n$ y que en $\mathrm{Sim}(S)$ se ha introducido una topología que lo hace un grupo de Lie. Sea $c : \mathbb{R} \to \mathrm{Sim}(S)$ un homomorfismo $(\mathbb{R}, +) \to (\mathrm{Sim}(S), \circ)$ diferenciable. El operador

$$V : S \to \mathbb{R}^n \ , \ s \mapsto V_s = \left. \frac{d}{dt} c_t(s) \right|_{t=0} ,$$

que en coordenadas locales ha de asumir la forma

$$V_s = (\frac{d}{dt} x_1(s)|_{t=0}, \ldots, \frac{d}{dt} x_n(s)|_{t=0}),$$

respecto a la base canónica de $\mathbb{R}^n$, se dice ser ser el *campo vectorial dinámico* determinado por c. Viceversa, dado un campo vectorial $V : S \to \mathbb{R}^n$ se busca el homomorfismo c que lo determine, cuando éste exista. Cuando c sólo está definido en un conjunto de la forma $I \times S$, con $I \subset \mathbb{R}$, entonces se dice que se tiene un *flujo local* generado por V.

Mecánica lagrangiana.

Sea X una variedad C^∞-diferenciable en $\mathbb{R}^n$. Sea x un *camino suave* en la variedad X, es decir una transformación diferenciable $x : \mathbb{R} \to X$, $t \mapsto x(t) \in X$. Si $f : X \to \mathbb{R}$ es a su vez diferenciable, la *diferencial* de $f \circ x : \mathbb{R} \to \mathbb{R}$ es, por la regla de la cadena,

$$D(f \circ x)(t) = df(x(t))(x'(t)) = \sum_{i=1}^{n} \partial_i f(x(t)) x_i'(t).$$

Así pues, para cada $t \in \mathbb{R}$, la aplicación $(x(t), x'(t)) : f \mapsto D(f \circ x)(t)$ es propiamente un elemento del espacio tangente $T_{x(t)}X$. Por tanto la colección de aplicaciones

$$\left\{ (x(t), x'(t)) |\ x \text{ camino suave y } t \in \mathbb{R} \right\}$$

es un subconjunto del *haz tangente* TX de la variedad X.

Una función *lagrangiana* $L : TX \to \mathbb{R}$ es tal que satisface las ecuaciones *de Euler y Lagrange*, también llamadas *de movimiento*:

$$\frac{\partial L}{\partial x_i} = \frac{d}{dt} \left(\frac{\partial L}{\partial x_i'} \right) \qquad \forall i \in [\![0, n-1]\!].$$

Para $t_0, t_1 \in \mathbb{R}$, con $t_0 \leq t_1$, los lagrangianos corresponden a valores extremos de operadores de la forma

$$(L, x) \mapsto \int_{t_0}^{t_1} L(x(t), x'(t))\, dt \quad \text{con } x(t_0), x(t_1) \text{ fijos.}$$

Mecánica hamiltoniana.

Recordamos que una *k-forma multilineal alternante*, o *k-forma* a secas, es una $\omega : (\mathbb{R}^n)^k \to \mathbb{R}$ que es lineal en cada componente (multilineal) y "alterna de signo"

según la paridad con la que se permute a sus componentes. Dadas k 1-formas $\omega_0,\dots,\omega_{k-1}$ su *producto exterior* es

$$\bigwedge_{\kappa=0}^{k-1}\omega_\kappa : (x_0,\dots,x_{k-1}) \mapsto \left(\bigwedge_{\kappa=0}^{k-1}\omega_\kappa\right)(x_0,\dots,x_{k-1}) = \det\left[\omega_{\kappa_0}(x_{\kappa_1})\right]_{\kappa_0,\kappa_1\in[\![0,k-1]\!]}.$$

Para cada $i \in [\![0,n-1]\!]$ sea x_i la 1-forma que toma la i-ésima proyección de cada vector. Entonces toda k-forma se escribe como una combinación lineal de monomios

$$\omega = \sum_{I\in[\![0,n-1]\!]^{(k)}} a_I \bigwedge_{i\in I} x_i.$$

El producto de un k-monomio por un ℓ-monomio es un $(k+\ell)$-monomio (definido de manera natural) y extendida esta definición por multilinealidad y alternancia se tiene el producto exterior de formas, el cual es *antisimétrico*, asociativo y distributivo.

Si $L:\mathbb{R}^m\to\mathbb{R}^n$ es lineal y ω es una k-forma definida en $\mathbb{R}^n$, $L^*\omega$ es la k-forma definida en $\mathbb{R}^m$ tal que:

$$(L^*\omega)(x_0,\dots,x_{k-1}) = \omega(Lx_0,\dots,Lx_{k-1}).$$

Sea X una variedad diferenciable en $\mathbb{R}^n$ y sea TX su haz tangente. Una 1-*forma diferencial* es una función $\omega : TX\to\mathbb{R}$, diferenciable, que es lineal en cada espacio tangente $\mathbb{R}^n_x$, con $x\in X$. ω es pues un operador en los duales de los espacios tangentes, está en los espacios cotangentes. Los operadores $dx_0,\dots,dx_{n-1}$ forman una base de estos operadores y se tiene que toda 1-forma diferencial es de la forma

$$\omega : x\mapsto\omega(x) = \sum_{i=0}^{n-1} a_i(x)\,dx_i, \quad \text{con } a_i \text{ suave } \forall i.$$

k-formas diferenciales son productos exteriores de k 1-formas diferenciables.

Sea X una variedad diferenciable en $\mathbb{R}^n$ y sea S su *haz cotangente*, es decir, $S=T^*X$. Sea $\omega=\sum_{i=0}^{n-1} y_i\,dx_i$ una 1-forma canónica definida en S. Entonces $d\omega=\sum_{i=0}^{n-1} dy_i\wedge dx_i$ la cual es no-degenerada y por tanto, S es simpléctica. La correspondencia ϕ tal que $\phi : dy_i\mapsto\frac{\partial}{\partial x_i}$ y $\phi : dx_i\mapsto -\frac{\partial}{\partial y_i}$ determina un isomorfismo que preserva haces entre los espacios cotangente y tangente en cada punto. Por lo tanto, si $H:S\to\mathbb{R}$ es un campo real en S entonces $dH:S\to\mathbb{R}^n$ es un campo vectorial en S y $\phi(dH)$ será un homomorfismo $(\mathbb{R},+)\to(S^S,\circ)$.

Es decir, la dinámica en TX generada por L se induce en la dinámica en T^*X generada por H bajo este isomorfismo (transformación de Legendre), en tal caso, se dice que H es el *hamiltoniano* del sistema dinámico $\phi(dH)$.

2.2 Electromagnetismo y las ecuaciones de Maxwell

Los campos *eléctrico* y *magnético* dependen de posiciones y del tiempo. Denotemos por $\varepsilon_1, \varepsilon_2, \varepsilon_3 : \mathbb{R} \to \mathbb{R}$ las componentes del campo eléctrico y por $\beta_1, \beta_2, \beta_3 : \mathbb{R} \to \mathbb{R}$ las del magnético. Así pues $E = (\varepsilon_1, \varepsilon_2, \varepsilon_3), B = (\beta_1, \beta_2, \beta_3)$ son los campos eléctrico y magnético. Las *ecuaciones de Maxwell en el vacío* estipulan:

$$\begin{aligned} \frac{dB}{dt} &= -\nabla \times E \quad , \quad \nabla \cdot B = 0 \\ \frac{dE}{dt} &= +\nabla \times B \quad , \quad \nabla \cdot E = 0 \end{aligned} \tag{2.1}$$

Se define la 2-forma diferencial

$$F = +\varepsilon_1 dt \wedge dx_1 + \varepsilon_2 dt \wedge dx_2 + \varepsilon_3 dt \wedge dx_3 - \beta_1 dx_2 \wedge dx_3 - \beta_2 dx_3 \wedge dx_1 - \beta_3 dx_1 \wedge dx_2$$

Al considerar la matriz

$$A = \begin{pmatrix} 0 & \varepsilon_1 & \varepsilon_2 & \varepsilon_3 \\ -\varepsilon_1 & 0 & -\beta_3 & \beta_2 \\ -\varepsilon_2 & \beta_3 & 0 & -\beta_1 \\ -\varepsilon_3 & -\beta_2 & \beta_1 & 0 \end{pmatrix}$$

se obtiene la forma bilineal (en términos del producto exterior de 1-formas)

$$\begin{aligned} dx^T A\, dx = \quad & dt \wedge (\varepsilon_1\, dx_1 + \varepsilon_2\, dx_2 + \varepsilon_3\, dx_3) + dx_1 \wedge (-\varepsilon_1\, dt - \beta_3\, dx_2 + \beta_2\, dx_3) \\ & + dx_2 \wedge (-\varepsilon_2\, dt + \beta_3\, dx_1 - \beta_1\, dx_3) + dx_3 \wedge (-\varepsilon_3\, dt - \beta_2\, dx_1 + \beta_1\, dx_2) \\ = \quad & \varepsilon_1\, dt \wedge dx_1 + \varepsilon_2\, dt \wedge dx_2 + \varepsilon_3\, dt \wedge dx_3 - \varepsilon_1\, dx_1 \wedge dt \\ & - \beta_3\, dx_1 \wedge dx_2 + \beta_2\, dx_1 \wedge dx_3 - \varepsilon_2\, dx_2 \wedge dt + \beta_3\, dx_2 \wedge dx_1 \\ & - \beta_1\, dx_2 \wedge dx_3 - \varepsilon_3\, dx_3 \wedge dt - \beta_2\, dx_3 \wedge dx_1 + \beta_1\, dx_3 \wedge dx_2 \\ = \quad & \varepsilon_1\, dt \wedge dx_1 + \varepsilon_2\, dt \wedge dx_2 + \varepsilon_3\, dt \wedge dx_3 + \varepsilon_1\, dt \wedge dx_1 \\ & - \beta_3\, dx_1 \wedge dx_2 + \beta_2\, dx_1 \wedge dx_3 + \varepsilon_2\, dt \wedge dx_2 - \beta_3\, dx_1 \wedge dx_2 \\ & - \beta_1\, dx_2 \wedge dx_3 + \varepsilon_3\, dt \wedge dx_3 + \beta_2\, dx_1 \wedge dx_3 - \beta_1\, dx_2 \wedge dx_3 \\ = \quad & 2\,(\varepsilon_1\, dt \wedge dx_1 + \varepsilon_2\, dt \wedge dx_2 + \varepsilon_3\, dt \wedge dx_3 \\ & - \beta_3\, dx_1 \wedge dx_2 - \beta_1\, dx_2 \wedge dx_3 + \beta_2\, dx_1 \wedge dx_3) \\ = \quad & 2F \end{aligned}$$

o sea

$$F = \frac{1}{2}\, dx^T A\, dx.$$

Las ecuaciones de Maxwell (2.1) equivalen a la aseveración $dF = 0$.

Esta presentación tiene sus orígenes en [Arnold(1989)], la cual es muy buena y didáctica, y en [Jackson(1999)].

Capítulo 3
Principios de Mecánica Cuántica y Cómputo Cuántico

Resumen Recordamos el célebre experimento de Stern-Gerlach para ilustrar un fenómeno de superposición cuántica. Después presentamos las nociones de estados y de observables. Los estados puros son vectores unitarios en espacios de Hilbert, y, al considerar operadores autoadjuntos en ellos, se les expresa en su descomposición espectral, lo que da una lista de posibles autovalores, los cuales vienen a ser los observables del operador. Un "procedimiento de medición" es un proceso de selección de uno de estos valores, con lo cual un estado superpuesto ha de asumir una connotación determinista. Los estados mixtos son propiamente distribuciones de probabilidad en conjuntos finitos de estados puros. Todo estado mixto puede inducir una estructura de estado mixto en un subsistema suyo, así pues, hemos de concluir este capítulo con una exposición de matrices reducidas de densidad.

Los libros clásicos de introducción a la Mecánica Cuántica son los de Landau y Lifshitz [Landau and Lifshitz(1981)] y de Ballentine [Ballentine(1998)]. A ellos remitimos a los lectores para profundizar en los temas que expondremos en el presente capítulo.

3.1 Experimento de Stern-Gerlach

Hacemos una somera exposición de este experimento. Remitimos al lector también a [Sakurai(1993)] para una presentación más detallada.

3.1.1 Descripción

Se calienta átomos de plata en un horno. Éste tiene un pequeño orificio mediante el cual escapan algunos átomos, como lo muestra la Figura 3.1. El haz de átomos escapados pasa a través de un colimador y después se le somete a un campo magnético

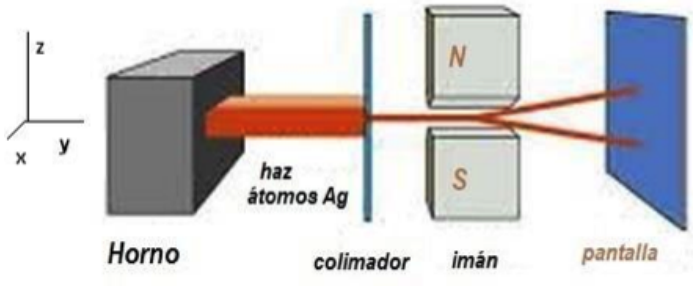


Figura 3.1 Dispositivo de Stern-Gerlach

no-homogéneo B. Considerando una versión simplificada del átomo de plata con un núcleo y 47 electrones, donde a 46 se los ve como una nube de electrones con simetría esférica y nulo momento angular neto. Así el momento angular de cada átomo de plata se realiza como el momento de espín magnético de su 47-o electrón. Es decir, el momento magnético μ de un átomo es proporcional al espín del electrón S, es decir $\mu \propto S$, donde la constante de proporcionalidad es $\frac{e}{m_e c}$, siendo $e = -1.6 \times 10^{-19} C$, $m_e = 9.1 \times 10^{-31}$ kg y $c = 2.9 \times 10^{8}$ $\frac{\text{m}}{\text{s}}$ son respectivamente la carga del electrón, su masa y la velocidad de la luz en el vacío.

El campo magnético ejerce una fuerza en el átomo (en la componente z), dada por:

$$F_z = \frac{\partial}{\partial z}(\mu \cdot B) \backsimeq \mu_z \frac{\partial B_z}{\partial z}.$$

Con el arreglo mostrado en la Figura 3.1, para $\mu_z < 0$ ($S_z > 0$), sobre el átomo se ejerce una fuerza hacia arriba, mientras que para $\mu_z > 0$ ($S_z < 0$) la fuerza se ejerce hacia abajo. El *dispositivo de Sten-Gerlach* (*SG*) "mide" la componente z del momento μ o equivalentemente la componente z de S salvo un factor de proporcionalidad.

Los átomos en el horno están orientados aleatoriamente. Si los electrones tuvieran un comportamiento clásico se esperaría tener un continuo de valores de μ_z en el intervalo $[-|\mu|, |\mu|]$, pero lo que se observa es que el dispositivo de *SG* separa el haz original en dos componentes solamente. Así entonces la componente z del espín S puede tener sólo dos valores $S_z^+ = \frac{\hbar}{2}$ y $S_z^- = -\frac{\hbar}{2}$ donde $\hbar = 1.05 \times 10^{-34}$ J·s es la *constante de Planck*.

3.1.2 Una serie de dispositivos de Stern-Gerlach

Al considerar sucesivos dispositivos SG, el haz de átomos pasa por varios dispositivos *SG*, por lo que surgen los casos siguientes:

- En el primero, un rayo que sale del horno y pasa por el dispositivo mostrado por la Figura 3.2 (a), donde SG $\hat{z}$ denota a un aparato con un campo magnético no-homogéneo en la dirección $\hat{z}$. Bloqueando la componente S_z^-, que sale de *SG* y manteniendo la componente S_z^+, la cual pasa por otro dispositivo SG $\hat{z}$, el haz resultante del segundo aparato tiene sólo una componente S_z^+.
- En el segundo ejemplo, véase la Figura 3.2 (b), el haz de átomos pasa a través de SG $\hat{z}$ y se bloquea la componente S_z-, como en el primer caso, pero ahora, el segundo aparato por el que atraviesa el haz es SG $\hat{x}$, es decir uno con un campo no-homogéneo en la dirección x. El rayo resultante tiene dos componentes S_x+ y S_x- de igual intensidad.
- En el tercer caso, Figura 3.2 (c), consideremos como antes un haz que pasa por un SG $\hat{z}$ y se obstruye la componente S_z^-, después el rayo pasa por un SG $\hat{x}$, obteniendo las componentes S_x^+ y S_x^-. Ahora se bloquea la componente S_x^- y se hace pasar el haz por un SG $\hat{z}$ obteniendo sorprendentemente la división de este haz en las dos componentes S_z^+ y S_z^-. Este ejemplo ilustra que en la mecánica cuántica no es posible determinar simultáneamente S_z y S_x. Es decir la selección de S_x^+ del rayo del segundo aparato SG $\hat{x}$ destruye completamente la información previa sobre S_z.

3.2 Estados y observables

Sea $\mathbb{H}$ un espacio de Hilbert complejo de dimensión finita n y sea $P(\mathbb{H})$ su respectivo espacio proyectivo, es decir, el espacio consistente de los subespacios de dimensión 1, o *rayos*, en $\mathbb{H}$. Una forma alternativa de realizar a $P(\mathbb{H})$ es considerando en la esfera unitaria $S_{\mathbb{H}} = \{x \in \mathbb{H} |\ \langle x|x\rangle = 1\}$ (aquí, $\langle\cdot|\cdot\rangle$ es el producto interno definido en $\mathbb{H}$), la relación de equivalencia:

$$[x \sim y \ \Leftrightarrow\ \exists c \in \mathbb{C} :\ |c| = 1 \ \&\ y = cx\ :\ x \text{ e } y \text{ difieren por un } \textit{cambio de fase}\,].$$

Entonces $P(\mathbb{H}) = S_{\mathbb{H}}/\sim$.

En la llamada *interpretación de Copenhage*, un *observable* tiene asociado un operador $A : \mathbb{H} \to \mathbb{H}$ lineal autoadjunto, es decir, $\langle x|Ay\rangle = \langle Ax|y\rangle$. Si su descomposición espectral es

$$A = \sum_{i=0}^{n-1} a_i\, \pi_{x_i} \quad , \quad \text{con } \pi_{x_i} = x_i\, x_i^H, x_i \in S_{\mathbb{H}} \tag{3.1}$$

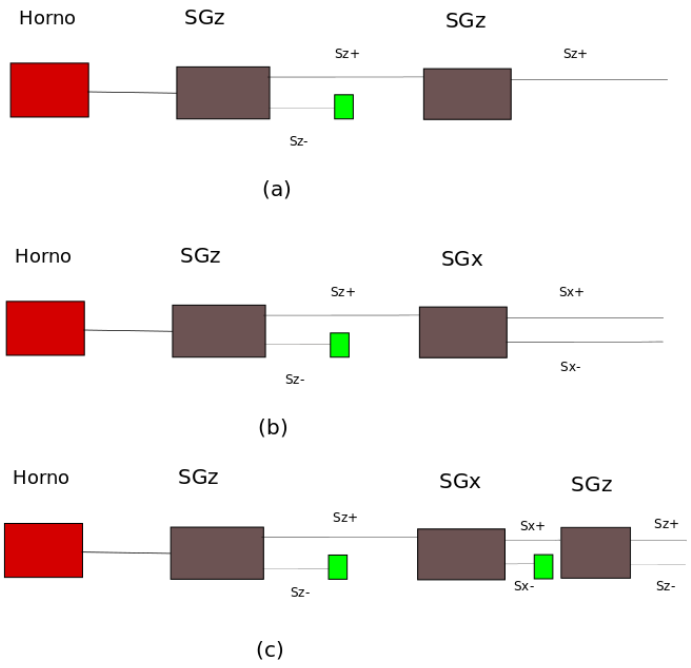


Figura 3.2 Sucesivos dispositivos de Stern-Gerlach

es decir, cada operador π_{x_i} es la proyección ortogonal sobre el rayo generado por el vector unitario $x_i \in S_{\mathbb{H}}$, cuya matriz está dada por el producto del vector "columna" x_i por el vector "renglón" x_i^H, que es el transpuesto conjugado del anterior. En estas condiciones, el conjunto $\{x_i\}_{i=0}^{n-1}$ consistente de los *eigenestados*, o *estados propios*, del operador A, es una base ortonormal de $\mathbb{H}$, es decir $\langle x_i | x_j \rangle = \delta_{ij}$, y los correspondientes *eigenvalores*, o *valores propios*, son los coeficientes $\{a_i\}_{i=0}^{n-1}$.

Señalamos en este punto que el operador A se dice *positivo* si todos sus eigenvalores lo son, lo cual equivale a la propiedad siguiente:

$$\forall x \in \mathbb{H} : \; x^H A x \geq 0. \tag{3.2}$$

Los vectores unitarios en $\mathbb{H}$, es decir, los elementos de $S_{\mathbb{H}}$ son llamados convencionalmente *estados* y, también, debido a la autodualidad de $\mathbb{H}$, *funciones de onda*, considerando cada $x \in S_{\mathbb{H}}$, como la funcional lineal $\mathbb{H} \to \mathbb{C}$, $z \mapsto \langle x | z \rangle \in \mathbb{C}$.

Entonces una *medición* $\mu(A, y)$ del operador asociado A en un *estado* $y \in S_{\mathbb{H}}$, con $y = \sum_{i=0}^{n-1} y_i x_i$, asumirá el valor numérico a_i con probabilidad $|y_i|^2$, y por consiguiente, el estado actual será x_i, es decir, $\Pr(\mu(A, y) = a_i) = |y_i|^2$.

O sea el observable ha de asumir un eigenvalor del operador lineal autoadjunto (hermitiano) en una base de eigenestados.

A este aspecto de la medición se le llama también *colapso de la función de onda*: antes de la medición el estado es de superposición y hecha ésta, tanto el eigenvalor a_i, como el estado y_i quedan completamente determinados.

Para el tipo de bases mencionadas anteriormente de un operador autoadjunto A, es posible dar una representación matricial de éste.

En efecto, observemos que

$$\forall i,j:\ \langle x_i|Ax_j\rangle = \langle x_i|a_j x_j\rangle = a_j\langle x_i|x_j\rangle = a_j\delta_{ij}. \tag{3.3}$$

Ahora, para un estado cualquiera $y=\sum_{i=0}^{n-1} y_i x_i \in S_{\mathbb{H}}$ se ha de tener

$$\begin{aligned}\langle y|Ay\rangle &= \left\langle \sum_{i=0}^{n-1} y_i x_i | A \sum_{j=0}^{n-1} y_j x_j \right\rangle \\ &= \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} \overline{y_i} y_j \langle x_i|A\,x_j\rangle \\ &= \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} \overline{y_i} y_j a_j \delta_{ij} \\ &= \sum_{j=0}^{n-1} |y_j|^2 a_j \\ &= \sum_{j=0}^{n-1} a_j \Pr\left(\mu(y)=a_j\right). \end{aligned} \tag{3.4}$$

Por lo cual, el *valor esperado* o *esperanza* del operador A con respecto a un estado $y\in S_{\mathbb{H}}$, es $\langle A\rangle = \langle y|Ay\rangle$ y, en consecuencia, se define la *dispersión* o *varianza* por $\sigma_A = \langle A^2\rangle - \langle A\rangle^2$.

De (3.3), observamos que, respecto a la base $\{x_i\}_{i=0}^{n-1}$ de eigenvectores, el operador A se representa por la matriz diagonal $D=\operatorname{diag}(a_0,\ldots,a_{n-1})$. Así pues, si para cada j, $x_j=\sum_{j=0}^{n-1} x_{ij}e_j$, donde $\{e_i\}_{i=0}^{n-1}$ es la base canónica del espacio $\mathbb{H}$, entonces $X=(x_{ij})_{i,j}$ es la matriz de cambio de base y se ha de tener la llamada *forma espectral* de A:

$$A = XDX^H.$$

De manera general, para dos bases ortonormales diferentes $\{x_i\}_{i=0}^{n-1}$ y $\{y_i\}_{i=0}^{n-1}$ del espacio $\mathbb{H}$ y un operador A, asociado a un observable, existe un *operador unitario* U, es decir tal que $U^{-1}=U^H$, por lo cual se satisface la condición $U^HU=UU^H=1$, con la propiedad de que $y_i=Ux_i$, para toda $i=0,\ldots,n-1$. En la representación matricial del operador A, el cambio de la base $\{x_i\}_{i=0}^{n-1}$ a la base $\{y_i\}_{i=0}^{n-1}$, está dado por

$$\forall i,j:\ \ \langle y_i,Ay_j\rangle = \sum_{l=1}^{n}\sum_{k=1}^{n}\langle x_i,U^Hx_l\rangle\langle x_l,Ax_k\rangle\langle x_k,Ux_j\rangle$$

es decir, por la transformación *similar* $U^H AU$. Los observables correspondientes de A y $U^H AU$ son pues *equivalentes*.

Cuando $\mathbb{H}$ es de dimensión infinita, digamos $\mathbb{H} = \mathscr{L}_2(\mathbb{R}, \nu)$, el espacio de funciones de *cuadrados integrables respecto a la medida de Lebesgue* ν, la forma espectral (continua) de un operador A asociado a un observable, será de la forma $D = \int_{\mathbb{R}} a(t)\, d\nu(t)$ (aquí la *medida espectral* es ν). Para un conjunto medible $E \subset \mathbb{R}$ se tendrá que existe un operador acotado $\pi_E : \mathscr{L}_2(\mathbb{R}, \nu) \to \mathscr{L}_2(\mathbb{R}, \nu)$, tal que para todo estado $x \in S_{\mathbb{H}}$:

$$|\langle \pi_E(x)|x\rangle|^2 = \Pr(\mu(A) \in E).$$

Nótese el carácter estadístico en este caso.

3.3 Estados mixtos

Un *estado puro* x es un punto en la esfera unitaria de un espacio de Hilbert, y también puede ser representado mediante una transformación lineal $\rho_p(x)$ en el espacio de Hilbert la cual es acotada, autoadjunta, positiva, de traza 1 e idempotente, es decir $\rho_p(x)^2 = \rho_p(x)$.

Propiamente, para cada estado x, se ha de tener $\rho_p(x) = xx^H$, lo que geométricamente corresponde a la proyección ortogonal hacia el subespacio generado por x en el espacio de Hilbert. En otras palabras, $\rho_p(x)$ es la proyección sobre el rayo generado por x. La correspondencia $\rho_p : x \mapsto \rho_p(x)$, es llamada *operador de densidad*.

Un ejemplo de ensamble que da origen a un estado puro es un haz de átomos de plata saliendo de un dispositivo *SG*. Cada átomo en el rayo tiene su espín apuntando en la misma dirección, la que es determinada por el campo magnético no-homogéneo.

Un *estado mixto* es una distribución de probabilidad en un conjunto de más de un estado puro. Formalmente, es un operador de densidad ρ con las propiedades mencionadas anteriormente, excepto que no es idempotente, es decir $\rho^2 \neq \rho$. Un estado mixto es una suma convexa de operadores de densidad asociados a estados puros:

$$\rho = \sum_{k\in K} w_k x_k x_k^H = \sum_{k\in K} w_k \rho_p(x_k),$$

donde

$$\sum_{k\in K} w_k = 1 \;\&\; \forall k \in K : \; [w_k \in [0,1] \;\&\; x_k \in S_{\mathbb{H}}]$$
$$\&\; \exists k_0, k_1 \in K \; \left[k_0 \neq k_1 \;\&\; w_{k_0}, w_{k_1} > 0\right]$$

siendo K un conjunto finito de índices. Naturalmente, combinaciones convexas de estados mixtos son también estados mixtos. Por lo tanto, *la cerradura convexa del conjunto de operadores de densidad de estados puros consiste de ellos y de todos los estados mixtos*.

El espacio $\mathrm{Lin}(\mathbb{H})$ de transformaciones lineales en el espacio de Hilbert en sí mismo es a su vez un espacio de Hilbert con el producto interno

$$\langle\cdot|\cdot\rangle : (A,B) \mapsto \mathrm{Tr}\left(A^H B\right),$$

donde $\mathrm{Tr}(\cdot)$ es la *traza* de matrices. Ya que $\forall x \in S_{\mathbb{H}}$:

$$\begin{aligned}
\left\langle \rho_p(x) | \rho_p(x) \right\rangle &= \mathrm{Tr}\left(\rho_p(x)^H \rho_p(x)\right) \\
&= \mathrm{Tr}\left((xx^H)^H (xx^H)\right) \\
&= \mathrm{Tr}\left(xx^H xx^H\right) \\
&= \mathrm{Tr}\left(xx^H\right) \\
&= \langle x|x\rangle
\end{aligned}$$

se tiene que la esfera unitaria $S_{\mathbb{H}}$ se incluye isométricamente en $\mathrm{Lin}(\mathbb{H})$ mediante la función ρ_p.

Para un operador A lineal autoadjunto en $\mathbb{H}$ y un estado mixto ρ, la esperanza de A en ρ es, por linealidad y utilizando (3.4),

$$\begin{aligned}
E_A(\rho) &= \sum_{k\in K} w_k E(Ax_k) \\
&= \sum_{k\in K} w_k \langle x_k | Ax_k \rangle \\
&= \sum_{k\in K} w_k \left\langle \sum_{i=0}^{n-1} x_{ik} e_i | A \sum_{j=0}^{n-1} x_{jk} e_j \right\rangle \\
&= \sum_{k\in K} w_k \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} x_{ik} x_{jk} \left\langle e_i | A e_j \right\rangle \\
&= \sum_{i,j=0}^{n-1} \left(\sum_{k\in K} w_k x_{ik} x_{jk} \right) \left\langle e_i | A e_j \right\rangle \\
&= \sum_{i,j=0}^{n-1} \left(e_i^H \rho\, e_j\right)\left(e_i^H A e_j\right) \\
&= \mathrm{Tr}(\rho A)
\end{aligned}$$

donde $n = \dim \mathbb{H}$, $(e_i)_{i=0}^{n-1}$ es una base ortonormal de $\mathbb{H}$ y $\left(\sum_{k\in K} w_k x_{ik} x_{jk}\right)_{i,j=0}^{n-1}$ es la representación matricial de ρ, vista como una transformación lineal, respecto a la base $(e_i)_{i=0}^{n-1}$.

Los operadores asociados a observables no forman un álgebra de operadores, pero sí forman parte de la *parte real* una tal álgebra pues son combinaciones lineales, con coeficientes reales, de operadores en esa álgebra. Los operadores asociados a observables son puntos fijos bajo un operador de *involución*, a saber, el tomar adjuntos de operadores, en el álgebra compleja de operadores acotados.

Al "factorizar" el espacio de Hilbert como $\mathbb{H} = \bigotimes_{j\in J} \mathbb{H}_{n_j}$, denotemos para cada $j \in J$ como $P_j : \mathbb{H} \to \mathbb{H}_j$ a la correspondiente proyección canónica. Consideremos como *observables* sólo a aquellos operadores A que conmuten con cada proyección: $\forall j \in J, AP_j = P_j A$. Entonces, el espacio de observables es el centro de la subálgebra de operadores generada por las proyecciones $(P_j)_{j\in J}$.

3.4 Matrices de densidad reducidas

Los estados en sistemas cuáticos *compuestos*, físicamente corresponden con aquellos que muestran una estructura interna, en la que se puede distinguir dos o más subsistemas. El formalismo matemático para considerar estos estados es el de productos tensoriales de los espacios de Hilbert de los subsistemas que los componen. Es decir,

$$\mathbb{H} = \bigotimes_{i\in I} \mathbb{H}_{n_i},$$

donde $\mathbb{H}_{n_i}$ son los espacios de Hilbert correspondientes a los subsistemas e I es un conjunto finito de índices.

Un caso importante que trataremos a continuación es el de sistemas compuestos por dos subsistemas A y B. Cada estado completo es un vector unitario en el espacio de Hilbert $\mathbb{H}_{AB} = \mathbb{H}_A \otimes \mathbb{H}_B$.

Supongamos que $\dim \mathbb{H}_A = 2^m$ y que $\dim \mathbb{H}_B = 2^n$. Entonces, $\dim \mathbb{H}_{AB} = 2^{m+n}$.

Un concepto importante es el de *matriz reducida de densidad* ρ_r. Sea ρ_{AB} un estado mixto. Entonces ρ_{AB} es propiamente una matriz cuadrada compleja de orden $2^{m+n} \times 2^{m+n}$ y como tal, determina

- tanto la transformación lineal $\mathbb{H}_{AB} \to \mathbb{H}_{AB}$, $z \mapsto \rho_{AB} z$,
- cuanto la transformación sesquilineal $\mathbb{H}_{AB} \times \mathbb{H}_{AB} \to \mathbb{C}$, $(z_0, z_1) \mapsto z_0^H \rho_{AB} z_1$.

Veámosla, para fines de esta sección, como una transformación sesquilineal.

Sean $\{e_{Ai}\}_{i=0}^{2^m-1} \subset S_{\mathbb{H}_A}$, $\{e_{Bj}\}_{j=0}^{2^n-1} \subset S_{\mathbb{H}_B}$ sendas bases ortonormales de $\mathbb{H}_A$ y $\mathbb{H}_B$.

La *traza respecto a la segunda componente* de ρ_{AB} es la transformación sesquilineal $\mathrm{Tr}_B(\rho_{AB}) : \mathbb{H}_A \times \mathbb{H}_A \to \mathbb{C}$ tal que

$$\forall x_0, x_1 \in \mathbb{H}_A : \; x_0^H \,\mathrm{Tr}_B(\rho_{AB}) x_1 = \sum_{j=0}^{2^n-1} (x_0 \otimes e_{Bj})^H \rho_{AB} (x_1 \otimes e_{Bj}). \tag{3.5}$$

Escribamos $\rho_{AB} = [r_{pq}]_{(p,q)\in[\![0,2^{m+n}-1]\!]}$ como una matriz. Igualmente, para cada $j \in [\![0, 2^n - 1]\!]$,

- el estado $x_0 \otimes e_{Bj}$ es un vector de 2^{m+n} coordenadas, éstas son todas cero excepto las de índices $q_0 = 2^m i_0 + j$, con $i_0 \in [\![0, 2^m - 1]\!]$, en las que tomará como valor la i_0-ésima componente $x_{i_0 0}$ del estado $x_0 \in \mathbb{H}_A$, similarmente

- el estado $x_1 \otimes e_{Bj}$ es un vector de 2^{m+n} coordenadas, éstas son todas cero excepto las de índices $q_1 = 2^m i_1 + j$, con $i_1 \in [\![0, 2^m - 1]\!]$, en las que tomará como valor la i_1-ésima componente $x_{i_1 1}$ del estado $x_1 \in \mathbb{H}_A$.

Por lo tanto, de (3.5) se tiene que la traza respecto a la segunda componente está dada por la matriz de orden $2^m \times 2^m$ siguiente

$$\mathrm{Tr}_B(\rho_{AB}) = \left[\sum_{j=0}^{2^n-1} r_{2^m i_0 + j, 2^m i_1 + j} \right]_{(i_0, i_1) \in [\![0, 2^m - 1]\!]} . \tag{3.6}$$

De igual manera, la *traza respecto a la primera componente* de ρ_{AB} es la transformación sesquilineal $\mathrm{Tr}_A(\rho_{AB}) : \mathbb{H}_B \times \mathbb{H}_B \to \mathbb{C}$ tal que

$$\forall y_0, y_1 \in \mathbb{H}_B : \; y_0^H \, \mathrm{Tr}_A(\rho_{AB}) \, y_1 = \sum_{i=0}^{2^m-1} (e_{Ai} \otimes y_0)^H \rho_{AB} (e_{Ai} \otimes y_1). \tag{3.7}$$

Para cada $i \in [\![0, 2^n - 1]\!]$

- el estado $e_{Ai} \otimes y_0$ es un vector de 2^{m+n} coordenadas, éstas son todas cero excepto las de índices $p_0 = 2^n i + j_0$, con $j_0 \in [\![0, 2^n - 1]\!]$, en las que tomará como valor la j_0-ésima componente $y_{j_0 0}$ del estado $y_0 \in \mathbb{H}_B$, similarmente
- el estado $e_{Ai} \otimes y_1$ es un vector de 2^{m+n} coordenadas, éstas son todas cero excepto las de índices $p_1 = 2^n i + j_1$, con $j_1 \in [\![0, 2^n - 1]\!]$, en las que tomará como valor la j_1-ésima componente $y_{j_1 1}$ del estado $y_1 \in \mathbb{H}_B$.

Por lo tanto, de (3.7) se tiene que la traza respecto a la primera componente está dada por la matriz de orden $2^n \times 2^n$ siguiente

$$\mathrm{Tr}_A(\rho_{AB}) = \left[\sum_{i=0}^{2^m-1} r_{2^n i + j_0, 2^n i + j_1} \right]_{(j_0, j_1) \in [\![0, 2^n - 1]\!]} . \tag{3.8}$$

Se define entonces [Nielsen and Chuang(2011)], a las correspondientes *matrices reducidas de densidad* como

$$\rho_A = \mathrm{Tr}_B(\rho_{AB}) \;\; , \;\; \rho_B = \mathrm{Tr}_A(\rho_{AB})$$

y las respectivas esperanzas de dos operadores autoadjuntos A y B:

$$E_A(\rho_{AB}) = \mathrm{Tr}\,(\rho_A A) \;\; , \;\; E_B(\rho_{AB}) = \mathrm{Tr}\,(\rho_B B)\,.$$

Capítulo 4
Sistemas compuestos y enredamiento

Resumen La noción de enredamiento en la Mecánica Cuántica es esencial y característica de ella: la medición que se haga en una partícula en un sistema enredado ha de determinar la que dé otra partícula en ese sistema. Esto contradice propiedades de "realidad" y de "localidad" de fenómenos físicos y está en el centro de la celebre polémica entre Bohry Einstein. El enredamiento da origen a protocolos muy eficientes de comunicación y de establecimiento de claves de criptografía cuántica. Si bien el enredamiento surge en estados puros por las propiedades del producto tensorial de espacios de Hilbert, en el caso de estados mixtos podría haber varias nociones de enredamiento. Aquí asumimos la de considerar estados mixtos enredados como aquellos que no son separables, es decir, no son combinaciones convexas de estados que efectivamente son productos de subestados de menor dimensión. En este capítulo presentamos primero las nociones de separabilidad para estados puros y para estados mixtos. Posteriormente, introducimos diversos criterios para medir el nivel de enredamiento de los estados.

La noción de enredamiento es esencial en la Mecánica Cuántica y siendo característica de ésta, ha redundado en grandes beneficios en el Cómputo Cuántico. Remitimos al lector al libro de Audretsch [Audretsch(2008)] para ampliar la presente exposición, además de los materiales que referiremos en ella.

4.1 Separabilidad y enredamiento

Un estado puro, correspondiente a un sistema físico, se realiza como un punto en la esfera unitaria de un espacio de Hilbert que es a su vez el producto tensorial de espacios de Hilbert de dimensión menor, en los cuales, como se mencionó en la sección anterior, se realizan subsistemas propios del sistema original. El espacio más sencillo es el de dimensión 2 sobre los complejos.

Se dice que un estado puro es *completamente separable* si se puede expresar como el producto tensorial de estados puros de dimensión 2, cada uno, y se dice que es *separable* si se puede expresar como el producto tensorial de estados puros de

dimensión menor que la suya. Naturalmente, todo estado completamente separable es separable, pero el recíproco no es cierto. Los estados puros que no son separables se dicen estar *enredados* o poseer la propiedad de *enredamiento*[1].

Para estados puros existen criterios para reconocer los estados enredados de los separables. Pero para estados mixtos, procedimientos análogos a los aplicados a estados puros sólo aparecen en sistemas de dimensión baja.

4.1.1 Estados puros

Para estados puros x_{AB}, cuya matriz de densidad asociada $\rho_{AB} = x_{AB}x_{AB}^H$ es acotada, autoadjunta, positiva, de traza 1 e idempotente, existen principios para determinar si estos estados son separables o enredados, varios de ellos los describiremos a continuación, así como algunas nociones de medidas del enredamiento.

Teorema 4.1.1 (Descomposición de Schmidt) *Sea $x_{AB} = \sum_{ij} a_{ij}(x_i \otimes y_j) \in \mathbb{H}_{n+m}$ un estado puro en un sistema bipartito, vale decir, con dos subsistemas bien identificados, dado en términos de dos bases de eigenestados $\{x_i\}_{i=0}^{n-1}$ y $\{y_j\}_{j=0}^{m-1}$ de dos operadores A, B respectivos. Existen bases $\{\tilde{x}_\kappa\}_{\kappa=0}^{k-1}$ y $\{\tilde{y}_\kappa\}_{\kappa=0}^{k-1}$ de sendos subespacios en $\mathbb{H}_n$ y $\mathbb{H}_m$, así como una colección de números positivos $\{a_\kappa\}_{\kappa=0}^{k-1} \subset \mathbb{R}^+$ tales que*

$$x_{AB} = \sum_{\kappa=0}^{k-1} \sqrt{a_\kappa}(\tilde{x}_\kappa \otimes \tilde{y}_\kappa) \qquad , \qquad \sum_{\kappa=0}^{k-1} a_\kappa = 1. \tag{4.1}$$

Los coeficientes $\{a_\kappa\}_{\kappa=0}^{k-1}$ son llamados de Schmidt *para x_{AB}. El* número de Schmidt *k es el mínimo número de coeficientes de Schmidt diferentes de cero con los que una expresión como (4.1) es posible.*

Demostración. Considerando la descomposición espectral de la matriz reducida de densidad del primer subsistema ρ_A, que es hermitiana y positiva, se tiene una base ortonormal del espacio $\mathbb{H}_n$ consistente de eigenestados $\{\tilde{x}_i\}_{i=0}^{n-1}$, tal que $\rho_A(\tilde{x}_i) = a_i\tilde{x}_i$ donde los eigenvalores a_i, $i \in [\![0, n-1]\!]$, son reales no-negativos.

Sea $\{z_j\}_{j=0}^{m-1}$ una base ortonormal de $\mathbb{H}_m$. Existe entonces una colección de coeficientes

$$\{c_{ij}\}_{(i,j)\in[\![0,n-1]\!]\times[\![0,m-1]\!]} \subset \mathbb{C}$$

tal que

$$x_{AB} = \sum_{i,j} c_{ij}(\tilde{x}_i \otimes z_j) = \sum_i \tilde{x}_i \otimes \left(\sum_j c_{ij}z_j\right) = \sum_i \tilde{x}_i \otimes (d_i\tilde{y}_i) = \sum_i d_i(\tilde{x}_i \otimes \tilde{y}_i), \tag{4.2}$$

donde $\tilde{y}_i \in S_{\mathbb{H}_B}$ y $d_i \in \mathbb{C}$ son tales que $d_i\tilde{y}_i = \sum_j c_{ij}z_j$.

[1] Es convencional llamar a estos estados en inglés *entangled* y a la propiedad *entanglement*. En español también se usa *entrelazado* y *entrelazamiento*

Sea $\{a_\kappa\}_{\kappa=0}^{k-1}$ la colección de eigenvalores de ρ_A estrictamente positivos (reenumerando todos los eigenvalores si fuese necesario). Entonces, por un lado,

$$\mathrm{Tr}\,(A\rho_A) = \sum_i \tilde{x}_i^H A \rho_A \tilde{x}_i = \sum_\kappa a_\kappa \tilde{x}_\kappa A \tilde{x}_\kappa, \tag{4.3}$$

y por otro lado, de (4.2)

$$x_{AB}^H (A \otimes I) x_{AB} = \sum_{i,j} \overline{d}_i d_j \tilde{x}_i A \tilde{x}_j \tilde{y}_i \tilde{y}_j = \sum_{i,j} \overline{d}_i d_j \tilde{x}_i A \tilde{x}_j \tilde{y}_i \tilde{y}_j, \tag{4.4}$$

cotejando (4.3) con (4.4) se tiene que los vectores $\tilde{y}_i \in S_{\mathbb{H}_B}$ forman una base ortonormal de $\mathbb{H}_B$ y $\forall j$: $a_j = |d_j|^2$.

Se sigue entonces la expresión (4.1). □

Observación 4.1.1 *La descomposición de Schmidt, permite concluir que un estado puro en un sistema compuesto x_{AB}, es separable si y sólo si tiene un único coeficiente de Schmidt distinto de cero, en otro caso el sistema está enredado.*

Observación 4.1.2 *Además $k = 1$ si y sólo si* $\mathrm{Tr}\left(\rho_A^2\right) = \mathrm{Tr}\left(\rho_B^2\right) = 1$.

Ejemplo: (Estado de Bell) Supongamos dos operadores A, B correspondientes a sendos observables, con espacios de Hilbert respectivos $\mathbb{H}_n$ y $\mathbb{H}_m$. Definimos los estados básicos

$$x_A^+ = e_{0\cdots 0} = e_0 \otimes \cdots \otimes e_0 \qquad , \qquad x_A^- = e_{1\cdots 1} = e_1 \otimes \cdots \otimes e_1$$

donde $\{e_0, e_1\}$ es la base canónica de $\mathbb{H}_1 = \mathbb{C}^2$. Similarmente, definimos $x_B^+, x_B^- \in S_{\mathbb{H}_B}$. Consideremos el primer *estado de Bell*

$$x_{AB} = \frac{1}{\sqrt{2}}(x_A^+ \otimes x_B^+ + x_A^- \otimes x_B^-)$$

en la esfera unitaria $S_{\mathbb{H}_{AB}}$ del espacio $\mathbb{H}_{AB} = \mathbb{H}_A \otimes \mathbb{H}_B$. La matriz de densidad asociada es

$$\rho_{AB} = x_{AB} x_{AB}^H = \frac{1}{2}\Big[\; (x_A^+ \otimes x_B^+)(x_A^+ \otimes x_B^+)^H + (x_A^+ \otimes x_B^+)(x_A^- \otimes x_B^-)^H + (x_A^- \otimes x_B^-)(x_A^+ \otimes x_B^+)^H + (x_A^- \otimes x_B^-)(x_A^- \otimes x_B^-)^H \Big].$$

La matriz reducida correspondiente al primer subsistema es

$$\rho_A = \mathrm{Tr}_B \rho_{AB} = \frac{1}{2}\left[x_A^+ x_A^{+H} + x_B^- x_B^{-H}\right],$$

y por tanto $\mathrm{Tr}\left(\rho_A^2\right) = \frac{1}{2} < 1$. Así que, por la Observación 4.1.2, se tiene que x_{AB} está enredado. Más adelante se mostrará que es un estado de máximo enredamiento.

Los cuatro *estados de Bell* son los siguientes estados puros con enredamiento máximo:

$$x_{AB}^{\pm} = \frac{1}{\sqrt{2}}(x_A^+ \otimes x_B^+ \pm x_A^- \otimes x_B^-) \quad \text{y} \quad y_{AB}^{\pm} = \frac{1}{\sqrt{2}}(x_A^+ \otimes x_B^- \pm x_A^- \otimes x_B^+). \tag{4.5}$$

□

Entropía de von Neumann

Otro instrumento para reconocer el enredamiento es la *entropía de von Neumann*, S, que se puede pensar como la versión cuántica de la entropía en termodinámica $\hat{S}$.

Definición 4.1.1 *Para una matriz ρ, la* entropía de von Neumann $S(\rho)$ *es*

$$S(\rho) = -\mathrm{Tr}\,(\rho \log \rho)\,.$$

La entropía de von Neumann para las matrices de densidad de los *ensambles microcanónico, canónico* y *gran canónico*, coinciden [Chandler(1987)] con la entropía $\hat{S}$. Como la entropía en la termodinámica, la entropía de von Neumann es una medida de *información*.

En términos de los eigenvalores λ_i de la matriz de densidad ρ, la entropía de von Neumann es:

$$S(\rho) = -\sum_i \lambda_i \log \lambda_i \qquad , \qquad \sum_i \lambda_i = 1.$$

Usando la entropía, se puede establecer el siguiente criterio para identificar estados puros de los mixtos [Peres(1995)]:

$$[S(\rho) = 0 \Longrightarrow \rho \text{ describe un estado puro}] \;\; \& \\ [S(\rho) > 0 \Longrightarrow \rho \text{ describe un estado mixto}]$$

Si la dimensión del espacio de Hilbert $\mathbb{H}$ es n, el valor de la entropía no puede alcanzar un valor mayor a $\log n$, y se alcanza éste en estados completamente enredados, tales como los estados de Bell. Por otro lado, el valor mínimo para la entropía es 0, lo que corresponde a estados puros. Así pues, para toda matriz ρ, la entropía de von Neumann es tal que $S(\rho) \in [0, \log n]$.

Nota: En cómputo cuántico, se toma a los logaritmos en base 2, $\log_2$, para considerar la unidad de la entropía como la de un solo bit, véase la sección 7.1 más adelante.

Supongamos que ρ_{AB} fuese la matriz de densidad de un estado puro x_{AB}, es decir $\rho_{AB} = x_{AB} x_{AB}^H$. Por el Teorema de Descomposición de Schmidt 4.1.1 existen sendas bases ortogonales de los subsistemas componentes tales que vale la ecuación (4.1):

$$x_{AB} = \sum_{\kappa=0}^{k-1} \sqrt{a_\kappa}(\tilde{x}_\kappa \otimes \tilde{y}_\kappa) \qquad , \qquad \forall \kappa : a_\kappa \in [0,1] \qquad , \qquad \sum_{\kappa=0}^{k-1} a_\kappa = 1.$$

Entonces las matrices reducidas de densidad son

$$\rho_A = \sum_{\kappa=0}^{k-1} a_\kappa \tilde{x}_\kappa \tilde{x}_\kappa^H \qquad , \qquad \rho_B = \sum_{\kappa=0}^{k-1} a_\kappa \tilde{y}_\kappa \tilde{y}_\kappa^H$$

con entropía de von Neumann

$$S(\rho_A) = -\mathrm{Tr}\,(\rho_A \log \rho_A) = -\sum_{\kappa=0}^{k-1} a_\kappa \log a_\kappa = -\mathrm{Tr}\,(\rho_B \log \rho_B) = S(\rho_A).$$

Definición 4.1.2 *Sea ρ_{AB} la matriz de densidad de un estado puro en un sistema bipartito con matrices reducidas de densidad ρ_A para el primer subsistema y ρ_B para el segundo. Entonces se define la* entropía de enredamiento *como*

$$E(\rho_{AB}) = S(\rho_A) = S(\rho_B).$$

Observación 4.1.3 *Se tiene $E(\rho_{AB}) \in [0,1]$.*

Sea x_{AB} un estado puro en un sistema cuántico bipartito, con matriz de densidad $\rho_{AB} = x_{AB} x_{AB}^H$. Al definir $E(x_{AB}) = E(\rho_{AB})$ se tiene propiamente una *medida del enredamiento* del estado x_{AB}. Un estado en el cual $E(x_{AB}) = \log n$, cuando $\dim(\mathbb{H}) = n$ se dice estar *máximamente enredado*.

Los estados de Bell son unos tales estados.

4.1.2 Estados mixtos (revisitados)

Según se introdujo en la Sección 3.3, los estados mixtos bipartitos están dados como operadores lineales ρ_{AB} definidos en un espacio de Hilbert $\mathbb{H}_{AB} = \mathbb{H}_A \otimes \mathbb{H}_B$ determinados por sumas convexas de matrices de densidad. Son, por tanto, autoadjuntos, positivos y de traza 1.

Las nociones de separación y enredamiento para estados puros, así como algunas medidas del enredamiento, pueden extenderse de varias maneras a estados mixtos.

En lo que resta del presente texto, convendremos en identificar *productos* con *productos tensoriales*, por lo que en lo sucesivo omitiremos el adjetivo tensorial en producto.

Definición 4.1.3 *Un estado mixto de 2-subsistemas es* H-separable *si se expresa como una suma convexa de estados productos de los subsistemas individuales, i.e.,*

$$\rho_{AB} = \sum_i a_i \rho_{Ai} \otimes \rho_{Bi}, \quad \textit{donde} \quad \sum_i a_i = 1. \tag{4.6}$$

En caso que no lo sea, se dice estar H-enredado *[Donald et al(2002)].*

En otras palabras, un estado mixto es H-separable si se realiza como la suma convexa de matrices de densidad separables.

Si en (4.6) se tuviera que cada matriz ρ_{Ai} fuese la de densidad de un estado puro $x_{Ai} \in S_{\mathbb{H}_A}$, es decir, $\rho_{Ai} = x_{Ai}x_{Ai}^H$, y similarmente $\rho_{Bi} = y_{Bi}y_{Bi}^H$, entonces

$$\rho_{Ai} \otimes \rho_{Bi} = (x_{Ai}x_{Ai}^H) \otimes (y_{Bi}y_{Bi}^H) = (x_{Ai} \otimes y_{Bi})(x_{Ai} \otimes y_{Bi})^H.$$

Así pues:

Observación 4.1.4 *La matriz de densidad de una combinación convexa de estados puros separables es un estado mixto H-separable.*

Testigo del enredamiento

Una aproximación más geométrica está dada por el concepto de *testigo del enredamiento* el cual es muy amplio. En este texto no pretendemos hacer un recuento de todo el tema, tan solo recordamos el criterio que establece para reconocer estados mixtos.

En el espacio de matrices, o equivalentemente, en el de transformaciones lineales, se considera el producto interno:

$$(A,B) \mapsto \langle A|B\rangle = \mathrm{Tr}\left(A^H B\right).$$

Teorema 4.1.2 (Véase [Krammer(2008)]) *Un estado mixto ρ es H-enredado si y sólo si existe un operador hermitiano Z tal que:*

- $\forall \rho_{AB}$ *H-separable:* $\langle \rho_{AB}|Z\rangle \geq 0$*, y*
- $\langle \rho|Z\rangle < 0$.

En tal caso, Z se dice ser un testigo del enredamiento de ρ. El testigo Z se dice ser óptimo *si* $\exists \rho_{AB}$ *H-separable:* $\langle \rho_{AB}|Z\rangle = 0$.

Operadores positivos

Recordamos que un operador A en un espacio de Hilbert es positivo si satisface la propiedad (3.2).

Una noción de separabilidad, menos fuerte, es la siguiente:

Definición 4.1.4 *Un estado mixto ρ bipartito definido en $\mathbb{H}_{AB}$ es* J-separable *si para todo operador positivo T definido en $\mathbb{H}_B$ se tiene que la composición $(Id_{\mathbb{H}_A} \otimes T) \circ \rho$ es un operador positivo [Horodecki et al(2009)].*

4.2 Medidas de enredamiento

Como en la sección anterior consideramos sistemas bipartitos: los estados puros son vectores unitarios en el espacio de Hilbert $\mathbb{H}_{AB} = \mathbb{H}_A \otimes \mathbb{H}_B$ y los estados mixtos son

sumas convexas de matrices de densidad, son pues operadores lineales en el espacio $\mathbb{H}_{AB}$.

Sea ρ_{AB} un estado mixto. Si $\rho_{AB} = \sum_{\kappa=0}^{k-1} p_\kappa \rho_\kappa$, con $\rho_\kappa = x_\kappa x_\kappa^H$, $p_\kappa > 0$ y $\sum_{\kappa=0}^{k-1} p_\kappa = 1$, diremos que $R = \left((p_\kappa)_{\kappa=0}^{k-1}, (\rho_\kappa)_{\kappa=0}^{k-1}\right)$ es una *representación convexa* de ρ_{AB} y que $E(R) = \sum_{\kappa=0}^{k-1} p_\kappa S(\rho_\kappa)$ es la *entropía de la representación R*, donde S es la entropía de von Neumann según la Definición 4.1.1.

Definición 4.2.1 *Sea ρ_{AB} un estado mixto. Su* enredamiento de formación *es*

$$E_F(\rho_{AB}) = \inf\{E(R)|\ R \text{ es una representación convexa de } \rho_{AB}\}.$$

Observación 4.2.1 *Para estados puros el enredamiento de formación se reduce a la entropía de von Neumann.*

Recordamos [Vedral and Plenio(1998)] que para dos estados mixtos ρ, σ, la *entropía de ρ relativa a σ* se define como

$$S(\rho\|\sigma) = \mathrm{Tr}\,(\rho(\log\rho - \log\sigma)).$$

La función $(\rho,\sigma) \mapsto S(\rho\|\sigma)$ no es una métrica, pues ni es simétrica ni satisface una desigualdad del triángulo, pero permite estimar tanto una cierta similitud entre estados mixtos, como un grado de enredamiento.

Sea $\mathscr{S}_{AB}$ la colección de estados mixtos H-separables.

Definición 4.2.2 *Para una matriz de densidad ρ_{AB}, se define la* entropía relativa del enredamiento *de ρ_{AB}, como:*

$$E_R(\rho_{AB}) := \min\{S(\rho_{AB}\|\sigma)|\ \sigma \in \mathscr{S}_{AB}\}.$$

Observación 4.2.2 *$E_R(\rho_{AB})$ es una medida del enredamiento del estado mixto ρ_{AB}. Claramente, si ρ_{AB} fuese puro, entonces $E_R(\rho_{AB}) = 0$.*

Purificación de enredamiento

Los procedimientos de *purificación de enredamiento* quedan descritos con detalle en [Bennett et al(1996a), Bennett et al(1996b), Vedral and Plenio(1998)].

Sea $\mathbb{H}_{AB} = \mathbb{H}_A \otimes \mathbb{H}_B$ el espacio de Hilbert correspondiente a un sistema cuántico bipartito, con subsistemas en los espacios $\mathbb{H}_A$ y $\mathbb{H}_B$ de dimensiones n y m respectivamente. Sean $(x_{Ai})_{i=0}^{n-1}$ y $(y_{Bj})_{j=0}^{m-1}$ sendas bases ortonormales de $\mathbb{H}_A$ y $\mathbb{H}_B$. Entonces

$$(x_{Ai} \otimes y_{Bj})_{(i,j)\in[\![0,n-1]\!]\times[\![0,m-1]\!]}$$

es una base ortonormal de $\mathbb{H}_{AB}$.

Para un ángulo $\theta \in [-\pi,+\pi]$, escribamos $p = \cos\theta$ y $q = \mathrm{sen}\,\theta$, por lo que $p^2 + q^2 = 1$. Considérese una sucesión de estados $(z_\nu(\theta))_{\nu\in\mathbb{N}}$ tal que

$$\forall \nu:\ z_\nu(\theta) = p\,(x_{i_{0\nu}} \otimes y_{i_{0\nu}}) + q\,(x_{i_{1\nu}} \otimes y_{i_{1\nu}}) \tag{4.7}$$

donde $(i_{0\nu}(\theta))_{\nu\in\mathbb{N}}$ y $(i_{1\nu}(\theta))_{\nu\in\mathbb{N}}$ son dos sucesiones de índices en $[\![0,n-1]\!]$ y $(j_{0\nu}(\theta))_{\nu\in\mathbb{N}}$ y $(j_{1\nu}(\theta))_{\nu\in\mathbb{N}}$ son dos sucesiones de índices en $[\![0,m-1]\!]$. Hagamos:

$$\forall \mu \in \mathbb{N}:\ \ w_\mu(\theta) = \bigotimes_{\nu=0}^{\mu} z_\nu(\theta) \in \mathbb{H}_{AB}^{\otimes(\mu+1)}.$$

Al expandir, se tiene, para cada μ:

$$w_\mu(\theta) = \sum_{k=0}^{\mu} p^{\mu-k} q^k\, v_{k\mu}(\theta),$$

donde $v_{k\mu}(\theta)$ es la suma de $\binom{\mu}{k}$ productos tensoriales de estados $x_{i_{\ell\nu}} \otimes y_{i_{\ell\nu}}$, llamados *residuales*.

Cuando una de las partes, digamos, la primera, toma una medición de uno de los estados $v_{k\mu}(\theta)$, respecto al producto tensorial de los vectores en su base (en este caso $(x_{Ai})_{i=0}^{n-1}$) cada uno de los posibles valores resultantes se asumirá con probabilidad $p_{k\mu} = \binom{\mu}{k} p^{2(\mu-k)} q^{2k}$, y entonces el sistema asumirá uno de los estados residuales, digamos $u_{k\mu}(\theta)$. Puede ocurrir que el nivel de enredamiento del estado residual $u_{k\mu}(\theta)$ exceda el de los originales $v_{k\mu}(\theta)$ o $w_{k\mu}(\theta)$.

El valor esperado de la entropía será entonces:

$$E_\mu = \sum_{k=0}^{\mu} \binom{\mu}{k} p^{2(\mu-k)} q^{2k} \binom{\mu}{k} \log \binom{\mu}{k}.$$

De (4.7), observamos que el máximo enredamiento ocurre cuando $|\theta| \in \{\frac{\pi}{4}, \frac{3\pi}{4}\}$, en cuyo caso $|p| = |q| = \frac{1}{\sqrt{2}}$, y el mínimo cuando $|\theta| \in \{0, \pi\}$, en cuyo caso $(|p|,|q|) \in \{(1,0),(0,1)\}$, y aquí $E_\mu = 0$.

Ahora bien, sea ρ_{AB} un estado mixto bipartito. Sea y_{AB}^- el estado puro de Bell, de máximo enredamiento, definido en (4.5). El *grado de pureza* de ρ_{AB} está dado por

$$F = (y_{AB}^-)^H \rho_{AB} y_{AB}^-.$$

Si acaso ρ_{AB} fuese la matriz de densidad de un estado puro x_{AB} se tendría

$$F = (y_{AB}^-)^H \rho_{AB} y_{AB}^- = (y_{AB}^-)^H x_{AB} x_{AB}^H y_{AB}^- = |\left\langle x_{AB} | y_{AB}^- \right\rangle|^2.$$

Volvamos al caso general de cualquier estado mixto bipartito ρ_{AB}. Se define el estado mixto *de Wiener para* F,

$$\beta_F = F y_{AB}^-(y_{AB}^-)^H + \frac{1-F}{3}\left[y_{AB}^+(y_{AB}^+)^H + x_{AB}^-(x_{AB}^-)^H + x_{AB}^+(x_{AB}^+)^H\right]$$

(véase las relaciones (4.5)). Mediante *operaciones locales* o *elementales*, ya sean laterales o bilaterales, tales como la identidad, los operadores de Pauli, rotaciones

por ángulos rectos o negaciones, se puede transformar ρ_{AB} en el correspondiente estado de Wiener.

Dadas μ copias del estado mixto de Wiener con el mismo grado de pureza, como el producto tensorial de esas μ copias, mediante aplicaciones elementales en las componentes se busca llevarlas hacia estados puros, es decir, se busca "purificarlas". Sea m_μ el número de componentes que efectivamente son purificadas.

El enredamiento de purificación $E_D(\rho_{AB})$ es entonces:

$$E_D(\rho_{AB}) := \lim_{\mu\to+\infty} \frac{m_\mu}{\mu}.$$

Un estado mixto con componentes que pueden ser purificadas, es decir, cuando $E_D(\rho_{AB}) > 0$, es llamado *enredado libre*, en otro caso, cuando $E_D(\rho_{AB}) = 0$ se dice *enredado acotado*.

Costo de enredamiento

A diferencia de la purificación del enredamiento, el *costo del enredamiento* cuantifica a los estados puros necesarios para conformar una serie de copias del estado de Wiener con el mismo grado de pureza que un estado mixto bipartito ρ_{AB} mediante operaciones locales. Así, el *costo del enredamiento* $E_C(\rho_{AB})$ es

$$E_C(\rho_{AB}) := \lim_{\mu\to+\infty} \frac{n_\mu}{\mu},$$

donde n_μ es el número de estados máximamente enredados necesarios para formar μ copias del estado de Wiener con el mismo grado de pureza que ρ_{AB}.

Criterio de la traspuesta parcial positiva

Una matriz ρ_{AB} determina una transformación bilineal en un espacio de Hilbert $\mathbb{H}_{AB} = \mathbb{H}_A \otimes \mathbb{H}_B$ actuando sobre los vectores separables como

$$(x_{A0} \otimes y_{B0}, x_{A1} \otimes y_{B1}) \mapsto (x_{A0} \otimes y_{B0})^T \rho_{AB} (x_{A1} \otimes y_{B1})$$

(visto cada $x_{Ai} \otimes y_{Bi}$ aquí como un vector columna). La *transpuestas parciales* de ρ_{AB} son las matrices ρ_{AB}^A, ρ_{AB}^B que representan, respectivamente, a las transformaciones bilineales

$$\begin{aligned}(x_{A0} \otimes y_{B0}, x_{A1} \otimes y_{B1}) &\mapsto (x_{A1} \otimes y_{B0})^T \rho_{AB} (x_{A0} \otimes y_{B1}) \ , \\ (x_{A0} \otimes y_{B0}, x_{A1} \otimes y_{B1}) &\mapsto (x_{A0} \otimes y_{B1})^T \rho_{AB} (x_{A1} \otimes y_{B0})\end{aligned}$$

Observación 4.2.3 *Si ρ_{AB} es un estado mixto, entonces es un operador positivo, y si es H-separable, entonces sus parciales transpuestas son también positivas.*

Así pues, el que las traspuestas parciales sean positivas es una condición necesaria para tener H-separabilidad.

Por tanto, resulta, como un criterio de suficiencia:

Observación 4.2.4 *Si ρ_{AB} es un estado mixto, y alguna de sus transpuestas parciales no es positiva, entonces ρ_{AB} está H-enredado.*

Capítulo 5
Simetrías

Resumen Los grupos de simetría están conformados por transformaciones geométricas en espacios lineales que preservan algunas propiedades como inversibilidad, normas y distancias, ángulos, y orientaciones, entre otras. En espacios de Hilbert puede haber correspondencias entre los objetos del espacio, o subconjuntos de ellos, y transformaciones de simetría. Las estructuras de los grupos de simetría determinan pues la de los espacios lineales sobre los que actúan, de ahí la importancia de estos grupos en el Cómputo Cuántico. Presentamos a los grupos de simetría más usuales en la Mecánica Cuántica, las representaciones de estos grupos (en términos de generadores y relatores), así como el Teorema de Burnside que caracteriza a los grupos resolubles. Tratamos después los recubrimientos, los cuales son epimorfismos continuos de grupos topológicos, y finalmente presentamos algunas simetrías generadas por conjuntos de vectores unitarios en espacios de Hilbert.

5.1 Grupos convencionales de simetría

Los *grupos de simetría* más utilizados en el contexto de la Mecánica Cuántica son los siguientes:

$\mathrm{O}(n)$. Isometrías lineales de $\mathbb{R}^n$. Una transformación lineal $T : \mathbb{R}^n \to \mathbb{R}^n$ es *isometría* si $\forall x \in \mathbb{R}^n$: $\|Tx\|_2 = \|x\|_2$, donde $\|\cdot\|_2$ es la norma euclidiana en $\mathbb{R}^n$.

$\mathrm{SO}(n)$. Rotaciones en $\mathbb{R}^n$, es decir, transformaciones lineales isométricas que *preservan orientación*, o sea, tienen determinate 1.

Subgrupos de cristalografía. Subgrupos de los grupos anteriores, para $n = 3$, que dejan invariantes un los sólidos platónicos. Véase el ya clásico libro de Sands [Sands(1969)] o el de Alperin [Alperin and Bell(1995)].

Para un campo $\mathbb{K}$:

$\mathrm{GL}(n,\mathbb{K})$. Transformaciones lineales invertibles $\mathbb{K}^n \to \mathbb{K}^n$.

$\mathrm{SL}(n,\mathbb{K}) = \{L \in \mathrm{GL}(n,\mathbb{K}) \mid \det L = 1\}$

$\mathrm{O}(n,\mathbb{K}) = \{L \in \mathrm{GL}(n,\mathbb{K}) \mid L^T L = Id_{\mathbb{K}}\}$

$\mathrm{SO}(n,\mathbb{K}) = \{L \in \mathrm{SO}(n,\mathbb{K}) \mid \det L = 1\}$
$\mathrm{U}(n) = \{L \in \mathrm{GL}(n,\mathbb{C}) \mid \bar{L}^T L = L^H L = Id_{\mathbb{K}}\}$
$\mathrm{SU}(n) = \{L \in \mathrm{U}(n) \mid \det L = 1\}$

Para $p+q=n$ y la matriz diagonal $J_{pq} = \mathrm{diag}[1^{(p)} \ \ (-1)^{(q)}]$,
$\mathrm{O}(p,q) = \{L \in \mathrm{GL}(n,\mathbb{R}) \mid L^T J_{pq} L = J_{pq}\}$
$\mathrm{SO}(p,q) = \{L \in \mathrm{O}(p,q) \mid \det L = 1\}$

Grupo de Lorentz. $\mathrm{SO}(3,1)$: Isometrías en el espacio de Minkowski $\mathbb{R}^{3,1}$ que coincide con $\mathbb{R}^4$, dotado del producto escalar $\langle x|y\rangle = x_0y_0 + x_1y_1 + x_2y_2 - x_3y_3$ (las primeras tres componentes son de tipo *espacial* y la última *temporal*).

Un *grupo topológico* es un espacio topológico dotado de una estructura de grupo tal que las operaciones, el producto y la toma de inversos, son continuas.

Por ejemplo, para $\mathbb{K} = \mathbb{R}, \mathbb{C}$, $\mathrm{GL}(n,\mathbb{K})$ es un grupo topológico localmente compacto.

Un *grupo de Lie* es un grupo topológico que es una variedad diferenciable y en la cual las operaciones son diferenciables [Hall(2003)].

Todo grupo de Lie de dimensión n sobre los complejos puede ser realizado también como uno de dimensión $2n$ sobre los reales.

Un *grupo de Lie lineal* es un subgrupo cerrado de $\mathrm{GL}(n,\mathbb{K})$ (con su topología usual). Usualmente, al hablar de grupos de Lie, éstos se suponen lineales.

Para un conjunto M y un grupo G, se puede tener una *acción* $G \times M \to M$ la cual ha de satisfacer:

- $\forall g,h \in G\ ,\ x \in M:\ (gh)x = g(hx)$.
- $\forall x \in M:\ ex = x$, donde e es el elemento unidad del grupo G.

Entonces la relación en M: $[x \sim y \ \Leftrightarrow\ \exists g \in gx = y]$, es de equivalencia y sus clases se llaman *órbitas*.

Así, dada una acción de un grupo, el conjunto sobre el que se actúa admite una partición consistente de las órbitas de la acción.

Por ejemplo, $\mathrm{O}(2)$ actuando sobre la esfera S_2 de $\mathbb{R}^3$ determina a las paralelas de la esfera como órbitas.

Un grupo G actúa sobre sí mismo mediante la *conjugación*

$$G \times G \to G\ \ ,\ \ (g,h) \mapsto g^{-1}hg,$$

y las órbitas son entonces las *clases de conjugación*.

5.2 Representaciones

Haremos un recuento de resultados bien conocidos en la Representación de Grupos. Remitimos al lector al libro de James y Liebeck [James and Liebeck(2001)] para ver detalles.

Un *representación* de un grupo G es un espacio vectorial E de dimensión finita junto con un homomorfismo de grupos $\rho : G \to \mathrm{GL}(E)$. El espacio E es el *soporte* de la representación. Si $E = \mathbb{C}^n$, entonces ρ se dice ser una *representación matricial*.

Proposición 5.2.1 *Para cualquier representación $\rho : G \to \mathrm{GL}(E)$ existe un producto escalar $\langle \cdot | \cdot \rangle : E \times E \to \mathbb{K}$ tal que $\forall g \in G$, $\rho(g)$ es unitaria, es decir,*

$$\forall x, y \in G : \ \langle \rho(g)x | \rho(g)y \rangle = \ \langle x | y \rangle .$$

Un subespacio $F < E$ es *invariante* bajo la representación ρ si $\forall g \in G$: $\rho(g)(F) \subseteq F$.

La representación es *irreducible* si los únicos subespacios invariantes son $\{0\}$ y E mismo.

Proposición 5.2.2 *Toda representación irreducible de un grupo finito es de dimensión finita.*

Una representación es *completamente representable* si es la suma directa de representaciones irreducibles.

Proposición 5.2.3 (Maschke) *Toda representación de dimensión finita de un grupo finito es completamente representable.*

Para dos representaciones (E_0, ρ_0) y (E_1, ρ_1) de un grupo G un *operador de intercalado* ("*intertwining operator*") es una transformación lineal $T : E_0 \to E_1$ tal que $\forall g \in G$: $\rho_1(g) \circ T = T \circ \rho_0(g)$. Se dice también que T es un *G-homomorfismo*.

Las representaciones (E_0, ρ_0) y (E_1, ρ_1) son *equivalentes* si existe un G-homomorfismo bijectivo.

Proposición 5.2.4 (Lema de Schur) *Las aseveraciones siguientes son válidas:*

1. *Si (E_0, ρ_0) y (E_1, ρ_1) no son equivalentes entonces el único G-homomorfismo es 0, es decir, el homomorfismo nulo.*
2. *Si $(E_0, \rho_0) = (E_1, \rho_1)$ entonces cualquier G-homomorfismo es un producto por una constante de la identidad Id_{E_0}, es decir es meramente una homotecia.*

5.3 Caracteres

Sea G un grupo y (E, ρ) una representación sobre un espacio lineal sobre los complejos. El *carácter* de E es $\chi_E : G \to \mathbb{C}$, $g \mapsto \chi_E(g) = \mathrm{Tr}(\rho(g))$. Así pues, χ_E es constante en cada clase de conjugación.

Proposición 5.3.1 *$\forall g \in G$: $\chi_E(g)$ es la suma de $\chi_E(e)$-raíces de la unidad.*

Proposición 5.3.2 *Si (E_0, ρ_0) y (E_1, ρ_1) son dos representaciones, entonces:*

- $\chi_{E_0 \oplus E_1} = \chi_{E_0} + \chi_{E_1}$.

- $\chi_{E_0 \otimes E_1} = \chi_{E_0}\chi_{E_1}$.
- $\chi_{E_0^*} = \overline{\chi_{E_0}}$.

Mediante estas nociones se puede probar la siguiente:

Proposición 5.3.3 *El número de representaciones irreducibles de un grupo G coincide con el número de sus clases de conjugación.*

5.4 Teorema de Burnside

Recordamos que un *grupo simple G* es un grupo cuyos únicos grupos normales son los triviales: la unidad y el grupo entero.

Para un grupo G se construye la *serie derivada* $(G_i)_{i\geq 0}$ haciendo $G_0 = g$ y $G_{i+1} = Z(G_i)$, donde $Z(G_i)$ es el centralizador de G_i, es decir, el grupo de elementos que conmutan con todos los de G_i. El grupo G es *resoluble* si $\exists i$: $G_i = \{e\}$, donde e es la unidad de G.

Proposición 5.4.1 (Burnside) *Si G es un grupo de orden $p_0^{r_0} p_1^{r_1}$ donde p_0, p_1 son dos primes y r_0, r_1 enteros positivos, entonces G es resoluble.*

De aquí:

Proposición 5.4.2 *Todo grupo finito simple es de uno de los tipos siguientes:*

- *Un grupo cíclico de orden primo.*
- *Un grupo alternante de orden al menos* 5.
- *Un miembro de las* 16 *familias de grupos de Lie.*
- *Uno de los* 26 *grupos simples esporádicos.*

Proposición 5.4.3 *Si G es un grupo no-abeliano, finito y simple entonces su orden es divisible entre al menos* 3 *primos.*

5.5 Recubrimientos

Si G y H son dos grupos topológicos, se dice que G es un *recubrimiento* de H si hay un epimorfismo contínuo $\phi : G \to H$. El recubrimiento es *doble* si para cada $h \in H$, $\text{card}\left(\phi^{-1}(h)\right) = 2$.

Puede verse que existe un grupo, denotado $\text{Spin}(n, \mathbb{R})$, que es simplemente conexo y un recubrimiento doble de $\text{SO}(n)$, y, similarmente, que existe un grupo, denotado $\text{Pin}(n, \mathbb{R})$, que es simplemente conexo y un recubrimiento doble de $\text{O}(n)$. Cambiando $\mathbb{R}$ por $\mathbb{C}$ surgen los grupos $\text{Spin}(n, \mathbb{C})$ y $\text{Pin}(n, \mathbb{C})$.

Toda forma cuadrada no-degenerada $c : \mathbb{R}^n \to \mathbb{R}$ está determinada por la matriz A correspondiente un su forma bilineal y han de existir Q invertible y D diagonal, tales que $A = Q^{-1}DQ$, con p valores 1 y q valores -1 en D, siendo $p+q$ el rango de A.

Se dice entonces que la *signatura* de la forma cuadrada $c(X)$ es la pareja (p,q). Una transformación $\phi : \mathbb{R}^n \to \mathbb{R}^n$ es *ortogonal* respecto a c si $c(\phi(x)) = c(x), \forall x \in \mathbb{R}^n$. Se define correspondientes grupos $\mathrm{O}(p,q,\mathbb{R})$, $\mathrm{SO}(p,q,\mathbb{R})$, $\mathrm{Spin}(p,q,\mathbb{R})$ y $\mathrm{Pin}(p,q,\mathbb{R})$, respecto un c, en el espacio real $\mathbb{R}^n$.

En el caso de formas cuadradas en $\mathbb{C}^n$, ya que todas de un mismo rango son equivalentes, sólo se considera los grupos $\mathrm{U}(n)$, $\mathrm{SU}(n)$, $\mathrm{Spin}(n,\mathbb{C})$ y $\mathrm{Pin}(n,\mathbb{C})$.

5.6 Simetrías inducidas por operadores

Utilizaremos la notación introducida en la sección 3.2, para referirnos a espacios de Hilbert, a sus esferas unitarias y a sus espacios proyectivos.

Sea $\pi : S_{\mathbb{H}} \to P(\mathbb{H})$ la proyección natural. Se define el operador

$$p : P(\mathbb{H}) \times P(\mathbb{H}) \to \mathbb{R}^+ \ , \ (\pi(x), \pi(y)) \mapsto p(\pi(x), \pi(y)) = |\langle x|y\rangle|^2.$$

Una *isometría* es una aplicación $s : P(\mathbb{H}) \to P(\mathbb{H})$ tal que

$$\forall x, y \in S_{\mathbb{H}} : \ p(s(\pi(x)), s(\pi(y))) = p(\pi(x), \pi(y)).$$

Si $T : \mathbb{H} \to \mathbb{H}$ es un operador lineal unitario, o *antiunitario* ($T^H = -T$), entonces $T(S_{\mathbb{H}}) = S_{\mathbb{H}}$, y también la aplicación $s_T : \pi(x) \mapsto \pi(Tx)$ será una isometría en $P(\mathbb{H})$, dicha *inducida por* T.

Proposición 5.6.1 (Wigner) *Toda isometría es inducida por un operador ya sea unitario o antiunitario. Las isometrías forman un grupo, denotado por $U(\mathbb{H})$, y en él las inducidas por operadores unitarios forman un subgrupo normal de índice* 2*.*

Recordamos que un *grupo de Lie* es una variedad diferenciable G con una operación $\circ : G \times G \to G$ con la que forma un grupo de manera que tanto la operación $\circ$ como la función *inverso*, $^{-1} : G \to G$, sean suaves. Por ejemplo $\mathrm{SL}(\mathbb{R}^2)$ es un grupo de Lie, inmerso en $\mathbb{R}^4 = \mathbb{R}^{2\times 2}$, que no es conexo: en una componente están las transformaciones con determinante positivo y en la otra las de determinante negativo.

El *álgebra de Lie* de un grupo de Lie G es el espacio tangente a G en su unidad. La componente conexa, que contiene a la unidad, de G está generada por los elementos de la forma $\exp(X) = \sum_{n\geq 0} \frac{1}{n!} X^n$ con X en el álgebra de Lie. Ya que $\exp(X) = \left(\exp\left(\frac{X}{2}\right)\right)^2$, se tiene que cada operador en la componente conexa de G actúa como una isometría.

Si G es un grupo de Lie, $\mathbb{H}$ es un espacio de Hilbert y $\lambda : G \to U(\mathbb{H})$ es un homomorfismo de G en el grupo de simetrías de $\mathbb{H}$ entonces

$$\forall g \in G \ \exists L(g) : \mathbb{H} \to \mathbb{H} \text{ unitario} : \ \lambda(g) \text{ está inducido por } L(g).$$

Considérese el ejemplo siguiente:

Sea $G = \mathrm{SU}(2)$ el grupo de transformaciones unitarias en $\mathbb{C}^2$ con determinante 1. Sea

$$H = \left\{ h = \begin{bmatrix} x_2 & x_0 + i x_1 \\ x_0 - i x_1 & -x_2 \end{bmatrix} \middle| (x_0, x_1, x_2) \in \mathbb{R}^3 \right\}$$

la colección de matrices hermitianas de orden (2×2), con traza nula y diagonal real. Se tiene que H se identifica naturalmente con $\mathbb{R}^3$, digamos que mediante la aplicación $\imath : h \mapsto (x_0, x_1, x_2)$, y

$$\forall h \in H : \ \det(h) = -(x_0^2 + x_1^2 + x_2^2)$$

por lo que si $(x_0, x_1, x_2) \neq (0,0,0)$ entonces h es invertible.

El grupo G actúa en H mediante la aplicación $\alpha : (g,h) \mapsto g^H hg$ y, claramente,

$$\forall g \in G, \ h \in H : \ \det(\alpha(g,h)) = \det(h).$$

Por tanto, para cada $g \in G$, $\beta_g : (x_0, x_1, x_2) \mapsto \imath \left(\alpha(g, \imath^{-1}(x_0, x_1, x_2)) \right)$ es una isometría lineal en $\mathbb{R}^3$. Así pues, la correspondencia $\beta : g \mapsto \beta_g$ es un homomorfismo $\mathrm{SU}(2) \to \mathrm{O}(3)$ cuyo núcleo es $\{-Id_{\mathbb{C}^3}, +Id_{\mathbb{C}^3}\}$. Visto como un grupo de Lie, G es conexo y las transformaciones descritas son contínuas, por tanto la imagen de $\mathrm{SU}(2)$ bajo β está en $\mathrm{SO}(3) < \mathrm{O}(3)$, como ambos $\mathrm{SU}(2)$ y $\mathrm{SO}(3)$ son de dimensión 3, se tiene que β es suprayectiva, es decir, resulta la sucesión exacta:

$$1 \longrightarrow \{-Id_{\mathbb{C}^3}, +Id_{\mathbb{C}^3}\} \longrightarrow \mathrm{SU}(2) \longrightarrow \mathrm{SO}(3) \longrightarrow 1. \tag{5.1}$$

Capítulo 6
Álgebras de Clifford

Resumen Las álgebras de Clifford son estructuras abstractas que han sido ampliamente utilizados en diversas teorías de tipo físico y matemático,y, en particular, propician un tratamiento general de operadores involucrados en el Cómputo Cuántico. Iniciamos su exposición con una presentación en el marco de la Teoría de Categorías, luego presentamos una construcción explícita de ellas y ejemplos particulares con suma relevancia en el Cómputo Cuántico. Concluimos el capítulo con los grupos de espín.

Exposiciones más completas y detalladas de los temas que aquí presentaremos se hallan en el libro, ya clásico, de Lounesto [Lounesto(2001)] y en el de Porteous [Porteous(1995)].

6.1 Motivación

Los operadores en $\mathrm{SU}(2)$ corresponden a matrices de la forma

$$g(a,b) = \begin{bmatrix} a & b \\ -\overline{b} & \overline{a} \end{bmatrix} \text{ con } a,b \in \mathbb{C} \ , \ a\overline{a} + b\overline{b} = 1.$$

La composición de dos de ellos, es tal que

$$g(a_0,b_0) \circ g(a_1,b_1) = g(a_0a_1 - b_0\overline{b_1}, a_0b_1 + b_0\overline{a_1}).$$

Sea $i = \sqrt{-1}$ el elemento que realiza a $\mathbb{C}$ como $\mathbb{R}[i]$. Sea ahora j el segundo generador de los cuaterniones: $i^2 = j^2 = -1$ e $ij = -ji$. Considérese la aplicación $\psi : g(a,b) \mapsto a + jb$. Entonces ψ es un homomorfismo de $\mathrm{SU}(2)$ en un subálgebra del campo de los cuaterniones.

Se va a generalizar esta construcción a una similar con $\mathrm{SU}(n)$, $n > 2$.

6.2 Presentación categórica

Sea $\mathbb{K}$ un campo y sea V un espacio vectorial sobre $\mathbb{K}$ provisto de una forma cuadrada $c(X)$. Sea A una $\mathbb{K}$-álgebra asociativa, con unidad. Una inclusión (inyectiva) $\imath_A : V \to A$ se dice ser *de Clifford* si

$$\forall x \in V : \ \imath(x)^2 = -c(x)\mathbf{1}_A. \tag{6.1}$$

El *álgebra de Clifford* $\mathrm{Cl}(V, c(X))$, junto con una inclusión de Clifford $\imath_C : V \to \mathrm{Cl}(V, c(X))$, es aquella tal que satisface la siguiente *propiedad universal*:

$$\begin{array}{l} \forall A \ \mathbb{K}\text{-álgebra con inclusión de Clifford } \imath_A : V \to A \\ \exists! \phi : \mathrm{Cl}(V, c(X)) \to A \text{ homomorfismo} : \ \ \imath_A = \phi \circ \imath_C. \end{array}$$

Se sigue que, en el caso de existir, el álgebra de Clifford $\mathrm{Cl}(V, c(X))$ es única salvo imágenes isomorfas.

Para ver que existen se ha de seguir las líneas en la sección próxima (6.3) para el caso de los campos real o complejo, mediante sumas directas de potencias tensoriales, reducidas por ideales generados por las relaciones (6.2).

De hecho, se tiene que la correspondencia $(V, c(X)) \mapsto \mathrm{Cl}(V, c(X))$ es un funtor covariante de la categoría de los espacios con formas cuadradas en la categoría de las álgebras asociativas con unidad.

6.3 Construcción de álgebras de Clifford

Sea $\mathbb{K} \in \{R, \mathbb{C}\}$ uno de los campos real o complejo. Sea $c(X)$ una forma cuadrada en $\mathbb{K}^n$. Sea

$$T(\mathbb{K}^n) = \bigoplus_{m \geq 0} (\mathbb{K}^n)^{\otimes m}$$

la suma directa de todas las potencias tensoriales del espacio $\mathbb{K}^n$, la cual es una $\mathbb{K}$-álgebra. Sea $I = \left\langle \left(x \otimes x + c(x)\mathbf{1}_{T(\mathbb{K}^n)} \right)_{x \in \mathbb{K}^n} \right\rangle$ el ideal generado por los elementos de la forma $x \otimes x + c(x)\mathbf{1}_{T(\mathbb{K}^n)}$, con $x \in \mathbb{K}^n$, donde $\mathbf{1}_{T(\mathbb{K}^n)}$ es la unidad de $T(\mathbb{K}^n)$, a saber, la mónada que consta de la unidad multiplicativa $1 \in \mathbb{K}$. Se define la *álgebra de Clifford* como el cociente $\mathrm{Cl}(\mathbb{K}^n, c(X)) = T(\mathbb{K}^n)/I$. Por tanto, se ha de tener:

$$\forall x \in \mathbb{K}^n : \ x \otimes x = -c(x)\mathbf{1}_{T(\mathbb{K}^n)}, \tag{6.2}$$

o, si $b(X,Y)$ es la forma bilineal asociada a la forma $c(X)$,

$$\forall x, y \in \mathbb{K}^n : \ x \otimes y + y \otimes x = -2b(x,y)\mathbf{1}_{T(\mathbb{K}^n)}. \tag{6.3}$$

El álgebra tensorial $T(\mathbb{K}^n)$ admite naturalmente una $\mathbb{Z}$-graduación, mas como el ideal I está generado por elementos cuadrados, el álgebra de Clifford $\mathrm{Cl}(\mathbb{K}^n, c(X))$

sólo admite una $\mathbb{Z}_2$-graduación, sea ésta

$$\mathrm{Cl}(\mathbb{K}^n, c(X)) = \mathrm{Cl}_0(\mathbb{K}^n, c(X)) \oplus \mathrm{Cl}_1(\mathbb{K}^n, c(X)).$$

Observación 6.3.1 (Algebra alternante) *Si $c(X) = 0$ entonces, por (6.2), $\forall x \in \mathbb{K}^n : \ x \otimes x = 0$. En consecuencia $\mathrm{Cl}(\mathbb{K}^n, c(X)) = \mathrm{Alt}(\mathbb{K}^n)$: el álgebra alternante, o exterior, de $\mathbb{K}^n$, que es de dimensión 2^n.*

Por (6.3):

$$\forall x, y \in \mathbb{K}^n : \ [x \otimes y = -y \otimes x \iff x \perp y \text{ (respecto a la forma bilineal } b(X,Y))] .$$

Considérese $\mathbb{K} = \mathbb{R}$ y, para $n \in \mathbb{Z}^+$, que $b(X,Y) = \sum_{i=0}^{n-1} x_i y_i$ es el producto interno usual, y por tanto que la forma cuadrada es $c(X) = \sum_{i=0}^{n-1} x_i^2 = \|X\|^2$. Entonces, si $(e_i)_{i=0}^{n-1}$ es una base ortonormal de $\mathbb{R}^n$, el álgebra de Clifford $\mathrm{Cl}(\mathbb{R}^n, c(X))$ está generada por los elementos $\{1\} \cup (e_i)_{i=0}^{n-1}$ y las relaciones $e_i \oplus e_j + e_j \oplus e_i = -2\delta_{ij}$, donde δ_{ij} es la delta de Kronecker. Vale decir:

$$e_i^2 = -1 \ \ \& \ \ [i \neq j \ \Rightarrow \ e_i \oplus e_j = -e_j \oplus e_i] .$$

Observación 6.3.2 (Los números complejos) *Para $n = 1$, $\mathrm{Cl}(\mathbb{R}, c(X)) = \mathbb{C}$.*

Observación 6.3.3 (Los cuaterniones) *Para $n = 2$, $\mathrm{Cl}(\mathbb{R}^2, c(X)) = \mathbf{H}$, el álgebra de los cuaterniones.*

En efecto, si se escribe $i = e_0$, $j = e_1$, y $k = e_0 e_1$, entonces resultan las relaciones siguientes entre generadores:

$$k^2 = (ij)^2 = ijij = -i^2 j^2 = -(-1)(-1) = -1$$
$$ij = k \ , \ \ jk = jij = -ij^2 = i \ , \ \ ki = iji = -i^2 j = j.$$

Si $c(X)$ es una forma cuadrada real de signatura (p,q), se escribe

$$\mathrm{Cl}_{pq} = \mathrm{Cl}(\mathbb{R}^{p+q}, c(X)).$$

Así, por las observaciones anteriores:

$$\mathrm{Cl}_{10} = \mathbb{C} \quad , \quad \mathrm{Cl}_{20} = \mathbf{H}.$$

Al considerar la forma bilineal compleja $b(X,Y) = \sum_{i=0}^{n-1} x_i y_i$, cuya forma cuadrada es $c(X) = \sum_{i=0}^{n-1} x_i^2$ (obsérvese que el producto interno usual será entonces $\langle x|y\rangle = b(\bar{x}, y)$), se escribe $\mathrm{Cl}_n = \mathrm{Cl}(\mathbb{C}^n, c(X))$.

Los resultados siguientes aparecen en el Capítulo 1 del clásico libro de Lawson y Michelsohn [Lawson and Michelsohn(1989)].

Proposición 6.3.1 (Theorem 4.1) *Se tiene las identificaciones siguientes (módulo correspondientes isomorfismos):*

- $\mathrm{Cl}_{n0} \otimes \mathrm{Cl}_{02} \approx \mathrm{Cl}_{0,n+2}$,

- $\mathrm{Cl}_{0n} \otimes \mathrm{Cl}_{20} \approx \mathrm{Cl}_{n+2,0}$,
- $\mathrm{Cl}_{pq} \otimes \mathrm{Cl}_{11} \approx \mathrm{Cl}_{p+1,q+1}$, $\forall p,q \in \mathbb{N}$.

Proposición 6.3.2 (Proposition 4.2) *Se tiene las identificaciones siguientes (módulo correspondientes isomorfismos):*

- $\mathbb{R}^{n\times n} \otimes \mathbb{R}^{m\times m} \approx \mathbb{R}^{(nm)\times(nm)}$ *(producto tensorial de matrices),*
- $\mathbb{R}^{n\times n} \otimes_{\mathbb{R}} \mathbb{K} \approx \mathbb{K}^{n\times n}$ *, con* $\mathbb{K} \in \{\mathbb{C}, \mathbf{H}\}$,
- $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \approx \mathbb{C} \oplus \mathbb{C}$,
- $\mathbb{C} \otimes_{\mathbb{R}} \mathbf{H} \approx \mathbb{C}^{2\times 2}$,
- $\mathbf{H} \otimes_{\mathbb{R}} \mathbf{H} \approx \mathbb{R}^{4\times 4}$,

donde $\otimes_{\mathbb{R}}$ *es el producto tensorial real, es decir, con sus factores vistos como espacios vectoriales sobre* $\mathbb{R}$.

Observación 6.3.4 $\forall j \in [\![0,n]\!]$*:* $\mathrm{Cl}_n \approx \mathrm{Cl}_{n-j,j} \otimes_{\mathbb{R}} \mathbb{C}$.

Proposición 6.3.3 (Theorem 4.3) *Para cada* $n \in \mathbb{N}$ *valen las identificaciones periódicas siguientes:*

- $\mathrm{Cl}_{n+8,0} \approx \mathrm{Cl}_{n0} \otimes \mathrm{Cl}_{80}$,
- $\mathrm{Cl}_{0,n+8} \approx \mathrm{Cl}_{0n} \otimes \mathrm{Cl}_{08}$,
- $\mathrm{Cl}_{n+2} \approx \mathrm{Cl}_n \otimes \mathrm{Cl}_2$,

donde, al inicio,

$$\mathrm{Cl}_{80} \approx \mathbb{R}^{2^4\times 2^4} \quad \& \quad \mathrm{Cl}_2 \approx \mathbb{C}^{2\times 2}.$$

En consecuencia, las álgebras Cl_{n0}, Cl_{0n} *y* Cl_n *quedan determinadas por la siguiente tabla:*

n	1	2	3	4	5	6	7	8
Cl_{n0}	$\mathbb{C}$	$\mathbf{H}$	$\mathbf{H}\oplus\mathbf{H}$	$\mathbf{H}^{2\times 2}$	$\mathbb{C}^{2^2\times 2^2}$	$\mathbb{R}^{2^3\times 2^3}$	$\mathbb{R}^{2^3\times 2^3}\oplus\mathbb{R}^{2^3\times 2^3}$	$\mathbb{R}^{2^4\times 2^4}$
Cl_{0n}	$\mathbb{R}\oplus\mathbb{R}$	$\mathbb{R}^{2\times 2}$	$\mathbb{C}^{2\times 2}$	$\mathbf{H}^{2\times 2}$	$\mathbf{H}^{2\times 2}\oplus\mathbf{H}^{2\times 2}$	$\mathbf{H}^{2^2\times 2^2}$	$\mathbb{C}^{2^3\times 2^3}$	$\mathbb{R}^{2^4\times 2^4}$
Cl_n	$\mathbb{C}\oplus\mathbb{C}$	$\mathbb{C}^{2\times 2}$	$\mathbb{C}^{2\times 2}\oplus\mathbb{C}^{2\times 2}$	$\mathbb{C}^{2^2\times 2^2}$	$\mathbb{C}^{2^2\times 2^2}\oplus\mathbb{C}^{2^2\times 2^2}$	$\mathbb{C}^{2^3\times 2^3}$	$\mathbb{C}^{2^3\times 2^3}\oplus\mathbb{C}^{2^3\times 2^3}$	$\mathbb{C}^{2^4\times 2^4}$

Observación 6.3.5 $\forall p,q \in \mathbb{N}$*:* $\mathrm{Cl}_{pq} \approx \mathrm{Cl}_{p-4,q+4}$ *&* $\mathrm{Cl}_{p,q+1} \approx \mathrm{Cl}_{s,r+1}$.

Ya que $\mathrm{Cl}_{11} \approx \mathbb{R}^{2\times 2}$ resulta que las álgebras Cl_{pq} quedan determinadas por la siguiente tabla:

$p\backslash q$	0	1	2	3	4	5	6	7	8
0	$\mathbb{R}$	$\mathbb{R}^{\oplus 2}$	$\mathbb{R}^{2\times 2}$	$\mathbb{C}^{2\times 2}$	$\mathbf{H}^{2\times 2}$	$\mathrm{Cl}_{04}^{\oplus 2}$	$\mathbf{H}^{2^2\times 2^2}$	$\mathbb{C}^{2^3\times 2^3}$	$\mathbb{R}^{2^4\times 2^4}$
1	$\mathbb{C}$	Cl_{02}	$\mathrm{Cl}_{02}^{\oplus 2}$	$\mathbb{R}^{2^2\times 2^2}$	$\mathbb{C}^{2^2\times 2^2}$	Cl_{06}	$\mathrm{Cl}_{06}^{\oplus 2}$	$\mathbf{H}^{2^3\times 2^3}$	$\mathbb{C}^{2^4\times 2^4}$
2	$\mathbf{H}$	Cl_{03}	Cl_{13}	$\mathrm{Cl}_{13}^{\oplus 2}$	$\mathbb{R}^{2^3\times 2^3}$	Cl_{07}	Cl_{17}	$\mathrm{Cl}_{17}^{\oplus 2}$	$\mathbf{H}^{2^4\times 2^4}$
3	$\mathbf{H}^{\oplus 2}$	Cl_{04}	Cl_{14}	Cl_{24}	$\mathrm{Cl}_{24}^{\oplus 2}$	Cl_{08}	Cl_{18}	Cl_{28}	$\mathrm{Cl}_{28}^{\oplus 2}$
4	Cl_{04}	$\mathrm{Cl}_{04}^{\oplus 2}$	Cl_{06}	Cl_{07}	Cl_{08}	$\mathrm{Cl}_{08}^{\oplus 2}$	$\mathbb{R}^{2^5\times 2^5}$	$\mathbb{C}^{2^5\times 2^5}$	$\mathbf{H}^{2^5\times 2^5}$
5	Cl_{14}	Cl_{06}	$\mathrm{Cl}_{06}^{\oplus 2}$	Cl_{17}	Cl_{18}	Cl_{46}	$\mathrm{Cl}_{46}^{\oplus 2}$	$\mathbb{R}^{2^6\times 2^6}$	$\mathbb{C}^{2^6\times 2^6}$
6	Cl_{24}	Cl_{07}	Cl_{17}	Cl_{27}	Cl_{28}	Cl_{47}	Cl_{57}	$\mathrm{Cl}_{57}^{\oplus 2}$	$\mathbb{R}^{2^7\times 2^7}$
7	Cl_{34}	Cl_{08}	Cl_{18}	Cl_{28}	Cl_{38}	Cl_{48}	$\mathbb{C}^{2^6\times 2^6}$	Cl_{68}	$\mathrm{Cl}_{68}^{\oplus 2}$
8	Cl_{08}	Cl_{45}	Cl_{46}	Cl_{47}	Cl_{48}	$\mathrm{Cl}_{48}^{\oplus 2}$	$\mathbf{H}^{2^6\times 2^6}$	$\mathbb{C}^{2^7\times 2^7}$	$\mathbb{R}^{2^8\times 2^8}$

(aquí, si A es un álgebra, escribimos $A^{\oplus 2} = A \oplus A$).

6.4 Álgebra exterior real como álgebra de Clifford

Veamos con un mayor detenimiento la operación en el álgebra real de Clifford Cl_{n0}, correspondiente a la forma cuadrada del producto interno usual.

Para una base $E = (e_i)_{i=0}^{n-1}$ de $\mathbb{R}^n$, por la relación (6.3), se ha de tener:

$$e_i \otimes e_j = \frac{1}{2}(e_i \otimes e_j - e_j \otimes e_i) + \frac{1}{2}(e_i \otimes e_j + e_j \otimes e_i) = \frac{1}{2}[e_i, e_j] - b_{ij}\mathbf{1},$$

donde $b_{ij} = b(e_i, e_j)$, y por tanto $b_{ij} = \delta_{ij}$ si la base E es ortonormal respecto a la forma $b(X,Y)$, y

$$(x,y) \mapsto [x,y] = x \otimes y - y \otimes x \text{ (el } \textit{conmutador} \text{ de } x,y),$$

es el operador *corchete de Lie*. Se tiene pues, para dos índices $i_0, i_1 \in [\![0, n-1]\!]$:

$$e_{i_0} \otimes e_{i_1} = e_{i_0 i_1} - b_{i_0 i_1}\mathbf{1}$$

con

$$e_{i_0 i_1} = \frac{1}{2}\left(e_{i_0} \otimes e_{i_1} - e_{i_1} \otimes e_{i_0}\right) = e_{i_0} \wedge e_{i_1}.$$

De manera general, si $\{i_0, \ldots, i_{k-1}\} \subset [\![0, n-1]\!]$ es un k-subconjunto de índices, se define

$$e_{i_0 \cdots i_{k-1}} = \frac{1}{k!} \sum_{\sigma \in S_k} \mathrm{Sgn}(\sigma) e_{i_{\sigma(0)}} \otimes \cdots \otimes e_{i_{\sigma(k-1)}} \tag{6.4}$$

Entonces

$$\Phi : \bigwedge \mathbb{R}^n \to \mathrm{Cl}_{n0} \quad , \quad 1 \mapsto \mathbf{1}\ ,\ e_{i_0} \wedge \cdots \wedge e_{i_{k-1}} \mapsto e_{i_0 \cdots i_{k-1}}$$

(según se define en la relación (6.4)) es un isomorfismo de $\mathbb{R}$-espacios vectoriales, lo que concuerda con el hecho de que ambos espacios son de dimensión 2^n (véase el primer renglón en la tabla mostrada en la Proposición 6.3.3).

6.5 Algebras de Clifford y compuertas cuánticas

Como operadores unitarios, las compuertas cuánticas pueden ser formalizadas mediante álgebras de Clifford [Chappell et al(2013)].

Sea V un espacio vectorial de dimensión n sobre el campo $\mathbb{K}$. Entonces el álgebra exterior $\mathrm{Alt}(V)$ es de dimensión 2^n. Sea $q(X) = \langle X|X\rangle = X^H X$, es decir, el tensor que define la norma euclidiana en V. Puede verse, como se hizo en la sección anterior, que también en este caso, $\mathrm{Cl}(V, q(X))$ consiste de clases laterales reducidas bajo las *transformaciones lineales unitarias* en $\mathrm{Alt}(V)$.

Se escribe $\mathrm{Cl}^j(n,\mathbb{K}) = \mathrm{Cl}^j(V, q(X))$ y se dice ser el *álgebra de Clifford* con n generadores.

Si $\mathbb{K} = \mathbb{C}$ es el campo de los números complejos entonces puede verse que $\mathrm{Cl}(2n,\mathbb{K}) \approx \mathbb{C}^{2^n \times 2^n}$: el álgebra de matrices complejas de orden $2^n \times 2^n$. Los elementos unitarios en esta álgebra son las compuertas cuánticas.

6.6 Grupos de espín

Los grupos espín$(n,\mathbb{R})$ pueden construirse como los elementos invertibles en un subgrupo del álgebra de Clifford Cl_{n0}.

Sea $x \in \mathbb{R}^n - \{0\}$. De acuerdo con (6.2), en Cl_{n0}:

$$x \otimes \left(-c(x)^{-1}x\right) = -c(x)^{-1}\,(x \otimes x) = -c(x)^{-1}\,(-c(x)\mathbf{1}) = \mathbf{1},$$

por lo que $x^{-1} = -c(x)^{-1}x$. Por lo tanto, $\forall y \in \mathbb{R}^n$:

$$\begin{aligned} x\otimes y\otimes x^{-1} &= -\frac{1}{c(x)}\left((x\otimes y)\otimes x\right) \\ &\overset{(6.3)}{=} -\frac{1}{c(x)}\left(-y\otimes x-2b(x,y)\mathbf{1}\right)\otimes x \\ &= \frac{1}{c(x)}\left(y\otimes x\otimes x+2b(x,y)(\mathbf{1}\otimes x)\right) \\ &= \frac{1}{c(x)}\left(y\otimes(-c(x)\mathbf{1})+2b(x,y)x\right) \\ &= -y+2\frac{b(x,y)}{b(x,x)}x \\ &= -\left(y-2\frac{b(x,y)}{b(x,x)}x\right) \end{aligned}$$

Así pues, la transformación $\pi_x : \mathbb{R}^n \to \mathbb{R}^n$, $y \mapsto x\otimes y\otimes x^{-1}$, es la reflexión al plano perpendicular al vector x. Se define, propiamente, $\mathrm{Pin}(n,\mathbb{R})$ como el subgrupo generado por $\Pi = \{\pi_x |\ x\in\mathbb{R}^n \ \&\ c(x)=1\}$ en el grupo de automorfismos de $\mathbb{R}^n$ y $\mathrm{Spin}(n,\mathbb{R})$ es el subgrupo de $\mathrm{Pin}(n,\mathbb{R})$ de elementos que involucran un número par de transformaciones en Π. Entonces por el Teorema de Cartan-Dieudonné, se tiene que $\mathrm{Spin}(n,\mathbb{R})$ es un recubrimiento de $\mathrm{SO}(n)$.

Capítulo 7
Relación entre álgebras de Clifford con el Cómputo Cuántico

Resumen Este capítulo introduce las nociones fundamentales del Cómputo Cuántico. Inicialmente presentamos a los qubits y a los quregistros como elementos fundamentales de codificación de la información así como las compuertas cuánticas que permiten implementar algoritmos cuánticos, y la traducción de conceptos básicos de incertidumbre en la Mecánica Cuántica al Cómputo Cuántico. Presentamos de una manera abstracta las máquinas de Turing cuánticas con el fin de ilustrar el traslado del cómputo clásico al cuántico, y después hacemos una revisión minuciosa de los más ilustrativos algoritmos cuánticos, a saber el de Deutsch-Jozsa para reconocer funciones booleanas equilibradas y los de Shor para factorizar enteros y calcular logaritmos discretos. Luego presentamos a la esfera de Bloch con el propósito de describir geométricamente el espacio de los qubits. Abordamos posteriormente nociones de álgebras-C^*, de lógica cuántica y los teoremas de Gleason y de Kochen-Specker. Finalizamos introduciendo la noción de conjuntos universales de operadores cuánticos.

7.1 Qubits y quregistros

La base canónica del espacio $\mathbb{H}_1 = \mathbb{C}^2$ consta de los vectores $\mathbf{e}_0 = [1\ \ 0]^T$ y $\mathbf{e}_1 = [0\ \ 1]^T$. Si $z_0, z_1 \in \mathbb{C}$ son complejos tales que $|z_0|^2 + |z_1|^2 = 1$, entonces $z_0\mathbf{e}_0 + z_1\mathbf{e}_1$ es un *estado puro*, llamado *qubit*, apócope inglés de *bit cuántico* (*quantum bit*).

Identificamos al primer vector básico $\mathbf{e}_0$ con el valor de verdad *falso*, o *cero*, y al segundo $\mathbf{e}_1$ con el valor de verdad *verdadero*, o *uno*.

Así pues, cada qubit es una "superposición" de ambos valores cero y uno.

Se dice que un estado $\mathbf{v} = v_0\mathbf{e}_0 + v_1\mathbf{e}_1$ *produce* la *salida i* con una probabilidad $|v_i|^2 = \mathfrak{Re}v_i^2 + \mathfrak{Im}v_i^2$. Se tiene el siguiente

Postulado de Medición: Si el estado actual es $\mathbf{v} = v_0\mathbf{e}_0 + v_1\mathbf{e}_1$ entonces, para cada $i \in \{0,1\}$, con probabilidad $|v_i|^2$ se realiza lo siguiente: Se emite la respuesta i y se transita al estado $\mathbf{e}_i$; es decir este último será el estado actual en el paso siguiente.

En otras palabras, un proceso de medición consiste en suspender la superposición de un estado y hacerlo transitar a un estado determinista: falso o verdadero.

Para cada $n > 1$, definimos recursivamente $\mathbb{H}_n = \mathbb{H}_{n-1} \otimes \mathbb{H}_1$. De aquí resulta que $\dim(\mathbb{H}_n) = 2^n$ y una base de este espacio es

$$B_{\mathbb{H}_n} = \left(\mathbf{e}_{\varepsilon_{n-1}\cdots\varepsilon_1\varepsilon_0}\right)_{\varepsilon_{n-1},\ldots,\varepsilon_1,\varepsilon_0\in\{0,1\}},$$

donde, puesto de manera recursiva,

$$\mathbf{e}_{\varepsilon_{n-1}\cdots\varepsilon_1\varepsilon_0} = \mathbf{e}_{\varepsilon_{n-1}\cdots\varepsilon_1} \otimes \mathbf{e}_{\varepsilon_0}.$$

Aquí queremos llamar la atención del lector para que tome en cuenta el cambio de nuestra notación respecto a la asumida de manera convencional en el mundo de la Física y de la Computación Cuántica. En general se suele escribir

$$|\varepsilon_{n-1}\cdots\varepsilon_1\varepsilon_0\rangle := \mathbf{e}_{\varepsilon_{n-1}\cdots\varepsilon_1\varepsilon_0} = \mathbf{e}_{\varepsilon_{n-1}} \otimes \cdots \otimes \mathbf{e}_{\varepsilon_1} \otimes \mathbf{e}_{\varepsilon_0} =: |\varepsilon_{n-1}\rangle \cdots |\varepsilon_1\rangle\,|\varepsilon_0\rangle \quad (7.1)$$

Evidentemente, cada índice $i \in [\![0, 2^n - 1]\!]$ puede escribirse en binario como una cadena de bits de longitud n: $i = (\varepsilon_{n-1}\cdots\varepsilon_1\varepsilon_0)_2$. Así pues identificaremos a cada índice con la cadena que lo representa: $i \leftrightarrow \varepsilon = \varepsilon_{n-1}\cdots\varepsilon_1\varepsilon_0$. Mediante esta identificación, se ha de tener $[\![0, 2^n - 1]\!] \approx \{0,1\}^n$.

Si $\mathbf{z} \in S_{\mathbb{H}_n}$ es un vector en la esfera unitaria euclidiana en $\mathbb{H}_n$ entonces $\sum_{\varepsilon\in\{0,1\}^n} z_\varepsilon \mathbf{e}_\varepsilon$ es un estado correspondiente a una *palabra de información de longitud n*, y es también el producto tensorial de n qubits, por lo que le llamaremos *n-quregistro*.

7.2 Compuertas cuánticas

Para $n = 1$, consideraremos las siguientes *compuertas básicas*, llamadas también *operadores cuánticos*:

Identidad. $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. $I : \mathbb{H}_1 \to \mathbb{H}_1$ es el operador identidad.

Rotación. Sea $t \in [-\pi, \pi]$ un ángulo y sea $Rot_t = \begin{bmatrix} \cos(t) & -\operatorname{sen}(t) \\ \operatorname{sen}(t) & \cos(t) \end{bmatrix}$. Se tiene que Rot_t es unitaria y tiene como efecto *rotar un ángulo t* en sentido antihorario.
Si $\mathbf{x}_p = \sqrt{p}\,\mathbf{e}_0 + \sqrt{1-p}\,\mathbf{e}_1$ es el estado que elige el valor 0 con probabilidad p y el valor 1 con probabilidad $1 - p$ entonces

$$Rot_t(\mathbf{x}_p) = \left(\cos(t)\sqrt{p} - \operatorname{sen}(t)\sqrt{1-p}\right)\mathbf{e}_0 + \left(\cos(t)\sqrt{1-p} + \operatorname{sen}(t)\sqrt{p}\right)\mathbf{e}_1.$$

Ahora bien, para el ángulo $t_{0p} = \cos^{-1}(-\sqrt{p})$ se tiene

$$Rot_{t_{0p}} = \begin{bmatrix} -\sqrt{p} & -\sqrt{1-p} \\ \sqrt{1-p} & -\sqrt{p} \end{bmatrix}$$

y en consecuencia $Rot_{t_{0p}}(\mathbf{x}_p) = -\mathbf{e}_0$. Es decir, aplicando la compuerta $Rot_{t_{0p}}$ se elegirá el valor 0 con probabilidad $(-1)^2 = 1$. Similarmente, para el ángulo $t_{1p} = \cos^{-1}(\sqrt{1-p})$ se tiene

$$Rot_{t_{1p}} = \begin{bmatrix} \sqrt{1-p} & -\sqrt{p} \\ \sqrt{p} & \sqrt{1-p} \end{bmatrix}$$

y en consecuencia $Rot_{t_{1p}}(\mathbf{x}_p) = \mathbf{e}_1$. Es decir, aplicando la compuerta $Rot_{t_{1p}}$ se elegirá el valor 1 con probabilidad 1. Así pues, las rotaciones tienen el efecto de "crear interferencias" constructivas o destructivas según se prefiera un estado final.

Negación. $N = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Se tiene $N : \begin{bmatrix} z_0 \\ z_1 \end{bmatrix} \mapsto \begin{bmatrix} z_1 \\ z_0 \end{bmatrix}$. N es unitaria y tiene como función *permutar señales*, es de hecho "una reflexión a lo largo de la diagonal principal".

Hadamard. $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. Se tiene $H : \begin{bmatrix} z_0 \\ z_1 \end{bmatrix} \mapsto \frac{1}{\sqrt{2}} \begin{bmatrix} z_0 + z_1 \\ z_0 - z_1 \end{bmatrix}$. H es unitaria y tiene como función "reflejar el plano respecto al eje x y rotar luego un ángulo de $\frac{\pi}{4}$ radianes, en sentido opuesto a las manecillas del reloj".

Naturalmente, $N^{\otimes n}$ y $H^{\otimes n}$ son sendas compuertas en $\mathbb{H}_n$. Las matrices que las representan, respecto a la base producto $B_{\mathbb{H}_n}$, pueden ser calculadas mediante la relación (**??**).

Observamos aquí, primeramente, que $N^{\otimes n}$ actúa como el "complemento a $2^n - 1$", es decir, en los vectores básicos se tiene

$$N^{\otimes n}\left(\mathbf{e}_{\varepsilon_{n-1}\cdots\varepsilon_1\varepsilon_0}\right) = \mathbf{e}_{\delta_{n-1}\cdots\delta_1\delta_0} \tag{7.2}$$

donde $(\varepsilon_{n-1}\cdots\varepsilon_1\varepsilon_0)_2 + (\delta_{n-1}\cdots\delta_1\delta_0)_2 = 2^n - 1$.

Observamos también que

$$\begin{aligned} H^{\otimes 1}(\mathbf{e}_0) &= \frac{1}{\sqrt{2}}(\mathbf{e}_0 + \mathbf{e}_1) \\ H^{\otimes 2}(\mathbf{e}_{00}) &= \frac{1}{(\sqrt{2})^2}(\mathbf{e}_{00} + \mathbf{e}_{01} + \mathbf{e}_{10} + \mathbf{e}_{11}) \end{aligned}$$

y de manera general

$$H^{\otimes n}(\mathbf{e}_{0\cdots0}) = \frac{1}{(\sqrt{2})^n}\left(\sum_{\varepsilon\in\{0,1\}^n} \mathbf{e}_\varepsilon\right) \tag{7.3}$$

es decir, el operador $H^{\otimes n}$ aplicado al primer vector básico $\mathbf{e}_{0\cdots0}$ produce el estado que "promedia a todos los demás con pesos uniformes".

Negación controlada. Sea $C : \mathbb{H}_2 \to \mathbb{H}_2$ la transformación lineal que sobre los vectores básicos actúa $\mathbf{e}_x \otimes \mathbf{e}_y \mapsto \mathbf{e}_x \otimes \mathbf{e}_{x\oplus y}$ (recuerdo una vez más que $\oplus$ es la

disyunción excluyente, o más bien la adición módulo 2). Esta transformación se llama *negación controlada* debido a que en su salida, el segundo qubit es la negación del primero sólo si en la entrada el segundo qubit "estaba prendido". Esto puede verse como que el segundo qubit de entrada sirve de "control" para aplicar el operador de negación al primero, el cual hace las veces de "argumento". C no es el producto tensorial de dos transformaciones unitarias en $\mathbb{H}_1$. Se tiene que C queda representado, respecto a la base canónica de $\mathbb{H}_2$ por la matriz

$$C = \begin{bmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{bmatrix}$$

Negación controlada cambiada. Sea $D : \mathbb{H}_2 \to \mathbb{H}_2$ la transformación lineal tal que $(\mathbf{x},\mathbf{y}) \mapsto D(\mathbf{x},\mathbf{y}) = C(\mathbf{y},\mathbf{x})$ que tan sólo cambia los roles de variable de control y variable de argumento. Se tiene

$$D = \begin{bmatrix} 0&0&1&0 \\ 0&1&0&0 \\ 1&0&0&0 \\ 0&0&0&1 \end{bmatrix}$$

En el espacio de transformaciones unitarias, C y D generan un subgrupo con la operación de composición. La tabla de multiplicación del subgrupo es de la forma:

$\circ$	I	C	D	CD	DC	CDC
I	I	C	D	CD	DC	CDC
C	C	I	CD	D	CDC	DC
D	D	DC	I	CDC	C	CD
CD	CD	CDC	C	DC	I	D
DC	DC	D	CDC	I	CD	C
CDC	CDC	CD	DC	C	D	I

Alternativamente, podemos decir que este grupo queda *presentado* por su unidad I, dos generadores C,D y la relación $CDC = DCD$. De hecho este grupo es isomorfo al grupo de permutaciones de 3 elementos, S_3. En efecto, si $\rho = (1,2)$ es la *reflexión* y $\phi = (1,2,3)$ es el ciclo de orden 3, entonces se puede identificar $C \leftrightarrow \rho$, $D \leftrightarrow \rho \circ \phi$.

Reversos. Entre los elementos que aparecen en el ejemplo anterior, $R_2 = CDC$: $\mathbb{H}_2 \to \mathbb{H}_2$ queda representado, respecto a la base canónica, mediante la matriz

$$R_2 = \begin{bmatrix} 1&0&0&0 \\ 0&0&1&0 \\ 0&1&0&0 \\ 0&0&0&1 \end{bmatrix},$$

es decir, es tal que $R_2(\mathbf{e}_i \otimes \mathbf{e}_j) = \mathbf{e}_j \otimes \mathbf{e}_i$. De hecho, para cada $n \geq 2$, actuando sobre la base canónica, se tiene:

$$R_n = R_2^{\otimes n}\left(\mathbf{e}_{\varepsilon_{n-1}\cdots\varepsilon_1\varepsilon_0}\right) = \mathbf{e}_{\varepsilon_0\varepsilon_1\cdots\varepsilon_{n-1}} \tag{7.4}$$

es decir, el efecto de este operador es *revertir* el orden de la "palabra de entrada", por lo cual, R_n se dice ser el *operador reverso*.

Transformaciones de Pauli. Las *matrices de Pauli* son

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad , \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad , \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad , \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{7.5}$$

las cuales son hermitianas y unitarias, es decir, para $j = 0,1,2,3$, $\sigma_j\sigma_j = \mathbf{1}_2$ es la matriz identidad de orden 2×2. Las cuatro matrices de Pauli conforman una base de $\mathbb{C}^{2\times 2}$:

$$\forall A = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} \in \mathbb{C}^{2\times 2}\ \exists c_0,c_1,c_2,c_3 :\ A = c_0\sigma_0 + c_1\sigma_1 + c_2\sigma_2 + c_3\sigma_3 \tag{7.6}$$

de hecho $(c_0,c_1,c_2,c_3) = \frac{1}{2}\left((a_{00}+a_{11}),(a_{01}+a_{10}),i(a_{01}-a_{10}),(a_{00}-a_{11})\right)$. Se tiene también que valen las siguientes relaciones, para $1 \leq j,k \leq 3$

$$\sigma_j\sigma_k + \sigma_k\sigma_j = 2\delta_{jk}\mathbf{1}_2 \tag{7.7}$$

$$\sigma_j\sigma_k = \delta_{jk}\mathbf{1}_2 + i\sum_{\ell=1}^{3}\varepsilon_{jk\ell}\sigma_\ell \tag{7.8}$$

donde en la última expresión, $\varepsilon_{jk\ell} \in \{-1,0,1\}$, $|\varepsilon_{jk\ell}| = 1 \Leftrightarrow \{j,k,\ell\} = \{1,2,3\}$ y además $\varepsilon_{jk\ell} = 1 \Leftrightarrow (j,k,\ell)$ es una rotación horaria.

Para un qubit $\mathbf{z} = z_0\mathbf{e}_0 + z_1\mathbf{e}_1$, con $|z_0|^2 + |z_1|^2 = 1$, se tiene que $\sigma_1\mathbf{z} = z_1\mathbf{e}_0 + z_0\mathbf{e}_1$ y $\sigma_2\mathbf{z} = -iz_1\mathbf{e}_0 + iz_0\mathbf{e}_1$ corresponden a *errores de permutación de bits* (*bit-flip errors*) en $\mathbf{z}$, en tanto que $\sigma_3\mathbf{z} = z_0\mathbf{e}_0 - z_1\mathbf{e}_1$ a un *error de fase de bit* (*phase-flip error*) en $\mathbf{z}$.

Un estado en $\mathbb{H}_n$, digamos $\sigma(\mathbf{z}) = \sum_{\varepsilon\in\{0,1\}^n} z_\varepsilon\mathbf{e}_\varepsilon$ está determinado por las 2^n coordenadas del vector $\mathbf{z} \in S_{\mathbb{H}_n}$. Si $U : \mathbb{H}_n \to \mathbb{H}_n$ es una compuerta cuántica, el estado $\sigma(U\mathbf{z})$ al que arriba al aplicársele el operador U consta también de 2^n coordenadas. De esta manera, un cálculo que involucra un número exponencial de términos se hace en "un paso" de cómputo cuántico y es posible así acelerar el proceso de corrida.

7.3 Máquina de Turing cuántica

Presentaremos aquí la noción de máquinas de Turing cuánticas siguiendo los enfoques en [Bernstein and Vasirani(1993)] y [Deutsch(1985)].

7.3.1 Máquinas de Turing no-deterministas clásicas

Recordamos que una *máquina de Turing no-determinista* es un autómata

$$mTnd = (Q, A, T, q_0, F),$$

donde Q es un conjunto finito de *estados*, A es un *alfabeto* (finito), $q_0 \in Q$ es un *estado inicial*, $F \subset Q$ es un conjunto de estados *finales* y

$$T \subset (Q \times A) \times (Q \times A \times M)$$

es una relación, donde $M = \{\text{izq}, \text{der}\}$ es un conjunto de dos *movimientos*. La *mTnd* actúa sobre una cinta consistente de una sucesión (infinita) de casillas (la cinta se extiende indefinidamente hacia atrás y hacia adelante), y la acción se hace mediante una cabeza lectora que ausculta una casilla a la vez en la cinta. Si $(p, a, q, b, m) \in T$ entonces decimos que "si la *mTnd* está en el estado p y lee en la casilla auscultada el símbolo a entonces lo cambia por el símbolo b, transita al estado q y pasa a auscultar la casilla en la posición m respecto a la casilla actual".

Una *descripción instantánea*, DI, es una palabra de la forma $\sigma_i p a \sigma_d$, donde $\sigma_i, \sigma_d \in A^*$ son *palabras* en el alfabeto A y $(p, a) \in Q \times A$, y describe que la *mTnd* "está en el estado p, lee en la casilla auscultada el símbolo a, la palabra a la izquierda de la casilla auscultada es σ_i y la palabra a su derecha es σ_d". Si $\text{DI}_0 = \sigma_{i0} p_0 a_0 \sigma_{d0}$ y $\text{DI}_1 = \sigma_{i1} p_1 a_1 \sigma_{d1}$ son dos descripciones instantáneas, decimos que la *mTnd transita* de DI_0 a DI_1, y escribimos $mTnd \vdash \text{DI}_0 \to \text{DI}_1$ si para algún símbolo $b \in A$ y algún movimiento $m \in M$ se tiene $(p_0, a_0, p_1, b, m) \in T$ y

$$\begin{aligned} m = \text{izq} &\Rightarrow \sigma_{i0} = \sigma_{i1} a_1 \ \&\ \sigma_{d1} = b \sigma_{d0} \\ m = \text{der} &\Rightarrow \sigma_{i1} = \sigma_{i0} b \ \&\ \sigma_{d0} = a_1 \sigma_{d1} \end{aligned}$$

La relación $\overset{*}{\to}$ es la cerradura reflexivo transitiva de la relación $\to$:

$$\begin{aligned} mTnd \vdash \text{DI}^0 \overset{*}{\to} \text{DI}^1 \Leftrightarrow \exists \text{DI}_0, \ldots, \text{DI}_n : \ & \text{DI}_0 = \text{DI}^0 \ \&\ \text{DI}_n = \text{DI}^1 \ \& \\ & \forall j < n : mTnd \vdash \text{DI}_i \to \text{DI}_{i+1} \end{aligned}$$

Se dice que la *mTnd calcula* a la función $f : A^* \to A^*$ si para cada $\sigma \in A^*$ existe un estado final $q \in F$ tal que $mTnd \vdash q_0 \sigma \overset{*}{\to} f(\sigma) q$. Para cada pareja $(p, a) \in Q \times A$ definimos $Imagen_T(p, a) = \{(q, b, m) \in Q \times A \times M | (p, a, q, b, m) \in T\}$ como el conjunto de posibles transiciones a partir de (p, a).

7.3.2 Máquina de Turing cuántica

Una *máquina de Turing cuántica*, *mTc*, es una máquina de Turing no-determininista $mTc = (Q, A, T, q_0, F)$ *total*, es decir,

$$T = (Q \times A) \times (Q \times A \times M),$$

tal que cada quintupla en la relación de transición $(p,a,q,b,m) \in T$ tiene asociado un número complejo $z = \zeta\,(p,a,q,b,m) \in \mathbb{C}$, llamado *amplitud* de la transición, de manera que el sistema de vectores

$$\Big(\zeta(p,a) = (\zeta\,(p,a,q,b,m))_{(q,b,m)\in Q\times A\times M}\Big)_{(p,a)\in Q\times A}$$

sea *ortonormal*, es decir para cualquier estado $p \in Q$ y cualquier símbolo $a \in A$:

$$1 = \sum\{|\zeta\,(p,a,q,b,m)\,|^2 \,|\, (q,b,m) \in Q \times A \times M\}$$

y para cualesquiera dos parejas distintas $(p_0,a_0) \neq (p_1,a_1)$:

$$0 = \sum\{\overline{\zeta\,(p_0,a_0,q,b,m)}\,\zeta\,(p_1,a_1,q,b,m) \,|\, (q,b,m) \in Q \times A \times M\},$$

en otras palabras

$$\langle \zeta(p_0,a_0) | \zeta(p_1,a_1) \rangle = \delta_{(p_0,a_0)(p_1,a_1)} \tag{7.9}$$

donde δ_{xy} es la *delta de Kroenecker* y $\langle \cdot | \cdot \rangle$ es el producto interno usual de $\mathbb{C}^{2\,\mathrm{card}Q\,\mathrm{card}A}$.

Así pues, los módulos al cuadrado de las amplitudes correspondientes a una pareja actual $(p,a) \in Q \times A$ determinan una densidad de probabilidad en $Q \times A \times M$. Se interpreta que si la *mTc* está en el estado actual p y lee a en la casilla auscultada, entonces escribe b, pasa a q y realiza el movimiento m con probabilidad $|\zeta\,(p,a,q,b,m)\,|^2$, para cada $(q,b,m) \in Q \times A \times M$. Además se ha de tener que las transiciones son propiamente transformaciones lineales unitarias en el espacio de configuraciones, es decir, si $mTc \vdash \sigma_{i0} p_0 a_0 \sigma_{d0} \to \sigma_{i1} p_1 a_1 \sigma_{d1}$ entonces $\sigma_{i1} p_1 a_1 \sigma_{d1}$ es el resultado de aplicar una transformación unitaria a $\sigma_{i0} p_0 a_0 \sigma_{d0}$. Para esto es necesario introducir una estructura de espacios lineales a las configuraciones, es decir, las descripciones. Veamos cómo hacer esto.

Sin pérdida de generalidad, supondremos que el alfabeto A consta sólo de dos símbolos, $A = \{0,1\}$. Sea $m = \mathrm{card}(Q)$ el número de estados que, acaso introduciendo estados *ociosos*, supondremos una potencia de 2. Sea $\mu = \log_2(m)$. Supondremos que la *mTc* sólo ocupa una cantidad acotada de casillas en su cinta, que la cota $S(n)$ depende de la longitud n de una cadena de entrada y, acaso introduciendo casillas en blanco, supondremos también que $S(n)$ es una potencia de 2. Sea $\nu = \log_2(S(n))$ y sea $\kappa = S(n)$. Al conjunto de estados lo realizaremos como el espacio $Q = \mathbb{H}_\mu$ de dimensión m (cada dirección básica del espacio determina un estado original de la *mTc*), a las posiciones de la cabeza lectora como $H = \mathbb{H}_\nu$ de dimensión $S(n)$ (cada dirección básica de este espacio determina una posición de la cabeza lectora) y al contenido de la cinta como $C = \mathbb{H}_\kappa$ de dimensión $2^{S(n)}$ (cada dirección básica de este espacio determina una palabra sobre A de longitud $S(n)$). Así pues, el espacio de descripciones es $Q \otimes H \otimes C = \mathbb{H}_{\mu+\nu+\kappa}$. Una *descripción* $\mathbf{q} \otimes \mathbf{h} \otimes \mathbf{c}$ se interpreta como sigue:

q. La *mTc* está en una superposición de $m = 2^{\mu}$ estados (básicos) $q_0, q_1, \ldots, q_{m-1}$: $\mathbf{q} = a_0\mathbf{e}_{q_0} + a_1\mathbf{e}_{q_1} + \cdots + a_{m-1}\mathbf{e}_{q_{m-1}}$, con $1 = |a_0|^2 + |a_1|^2 + \cdots + |a_{m-1}|^2$.

h. La cabeza lectora de la *mTc* está en una superposición de $S(n) = 2^{\nu}$ índices $0, 1, \ldots, S(n)-1$: $\mathbf{h} = h_0\mathbf{e}_0 + h_1\mathbf{e}_1 + \cdots + h_{S(n)-1}\mathbf{e}_{S(n)-1}$, con $1 = |h_0|^2 + |h_1|^2 + \cdots + |h_{S(n)-1}|^2$.

c. La cinta contiene una superposición de las $2^{S(n)}$ posibles palabras sobre A de longitud $S(n)$: $\mathbf{c} = c_0\mathbf{e}_{\sigma_0} + c_1\mathbf{e}_{\sigma_1} + \cdots + c_{2^{S(n)}-1}\mathbf{e}_{\sigma_{2^{S(n)}-1}}$, con $1 = |c_0|^2 + |c_1|^2 + \cdots + |c_{2^{S(n)}-1}|^2$.

La aplicación de una transición a esta representación de la *mTc* conlleva un alto grado de paralelismo: Primero, supongamos que el "estado actual" de la máquina original es $\mathbf{e}_p$, que se lee la i-ésima posición $\mathbf{e}_i$ de la j-ésima palabra $\mathbf{e}_j$, y que ahí aparece el símbolo $a \in A$. El vector $\mathbf{e}_p \otimes \mathbf{e}_i \otimes \mathbf{e}_j$ es uno de la base canónica de $Q \otimes H \otimes C$. Sea

$$\zeta(p,a) = (\zeta(p,a,q,b,m))_{(q,b,m)\in Q\times A\times M} = \left(z_{(q,b,m)}\right)_{(q,b,m)\in Q\times A\times M} = \mathbf{z}$$

el vector de amplitudes de las transiciones correspondientes a la pareja (p,a). Entonces hacemos

$$T(\mathbf{e}_p \otimes \mathbf{e}_i \otimes \mathbf{e}_j) = \sum \left\{ z_{(q,b,m)}\mathbf{e}_q \otimes \mathbf{e}_{i_m} \otimes \mathbf{e}_{j'} \,|\, (q,b,m) \in Q \times A \times M \right\} \tag{7.10}$$

donde, en cada sumando, $i_m = i-1$ si $m =$ izq, $i_m = i+1$ si $m =$ der y j' es el índice de la palabra que coincide con la j-ésima salvo que el símbolo a en su i-ésima posición ha sido sutituído por el símbolo b. Debido a las condiciones de ortonormalidad (7.9), las imágenes de los vectores básicos forman una colección ortonormal, por lo que T podrá extenderse a una transformación unitaria.

Luego, T se extiende por (multi-)linealidad a todo el espacio $Q \otimes H \otimes C$, es decir

$$T(\mathbf{p} \otimes \mathbf{h} \otimes \mathbf{c}) = \sum \left\{ a_p h_i c_j T(\mathbf{e}_p \otimes \mathbf{e}_i \otimes \mathbf{e}_j) \,|\, q \in Q\,,\, i \le S(n)-1\,,\, j \le 2^{S(n)}-1 \right\} \tag{7.11}$$

Puede verse que T es el producto tensorial de transformaciones lineales unitarias, luego, ella misma es lineal unitaria.

Una *configuración inicial* es de la forma $\mathbf{e}_{q_0} \otimes \mathbf{e}_0 \otimes \mathbf{e}_{j_0}$ y la j_0-ésima palabra σ_{j_0} es la correspondeinte *palabra de entrada*. Una *computación* es una sucesión de configuraciones,

$$\mathbf{c}_0 = \mathbf{e}_{q_0} \otimes \mathbf{e}_0 \otimes \mathbf{e}_{j_0} \;\;,\;\; \forall t > 0 : \mathbf{c}_t = T(\mathbf{c}_{t-1})\,,$$

es decir es una sucesión $\left(T^t(\mathbf{e}_{q_0} \otimes \mathbf{e}_0 \otimes \mathbf{e}_{j_0})\right)_{t\ge 0}$. En cualquier instante de la computación se puede aplicar el postulado de medición para elegir una configuración de la forma $\mathbf{e}_q \otimes \mathbf{e}_i \otimes \mathbf{e}_j$ con la probabilidad correspondiente. La *mTc computa* la función $f : A^n \to A^{S(n)}$ si para cada $\sigma \in A^n$ a partir de la descripción inicial $\mathbf{e}_{q_0} \otimes \mathbf{e}_0 \otimes \mathbf{e}_{j_0}$ donde j_0 es el índice de la palabra $\sigma * 0^{(S(n)-n)}$, se arriba, con proba-

bilidad 1, a un estado de la forma $\mathbf{e}_q \otimes \mathbf{e}_i \otimes \mathbf{e}_j$, donde $q \in F$ es un estado final y j es el índice de la palabra $f(\sigma)$.

Observamos que toda *mTc* realiza un proceso algorítmico. De la tesis de Church deducimos que toda *mTc* es *simulable* por una *mTnd*. Por tanto, lo computable por *mTc*'s queda incluído en la clase de las funciones recursivas. Sin embargo, hay una ganancia apreciable en tiempo: las *mTc*'s realizan en una sola de sus transiciones lo que las *mTnd*'s realizarían en un número exponencial de transiciones de ellas.

Por otro lado, no toda *mTnd* es simulable por una *mTc*. Sin embargo, toda *mTnd* cuyas transiciones puedan ser ponderadas por pesos complejos que satisfagan las nociones de ortonormalidad de la ecuación (7.9) será, en efecto, simulable por una *mTc*.

7.4 Evaluación de funciones booleanas

Sea $V = \{0,1\}$ el conjunto de valores de verdad clásicos. V^n es el espacio de palabras de longitud n que constan de bits. Hay 2^n tales palabras. Una función $f : V^n \to V$ se dice ser *booleana* pues asume sólo valores booleanos, y se dice ser *equilibrada* si el número de veces que asume al valor 0 coincide con el número de veces que asume al valor 1. Obviamente hay 2^{2^n} funciones booleanas $V^n \to V$ y hay 2^{n2^n} funciones *booleanas vectoriales* $V^n \to V^n$. Cada una de las 2^n asignaciones $\varepsilon = (\varepsilon_{n-1}, \ldots, \varepsilon_1, \varepsilon_0) \in V^n$ se puede poner en correspondencia con el vector $\mathbf{e}_\varepsilon \in \mathbb{H}_n$ de la base "canónica" de $\mathbb{H}_n$.

Sea $f : V^n \to V$ una función booleana. Sea U_f una matriz permutación de orden $2^{n+1} \times 2^{n+1}$ tal que $U_f(\mathbf{e}_\varepsilon \otimes \mathbf{e}_\mathbf{0}) = (\mathbf{e}_\varepsilon \otimes \mathbf{e}_{f(\varepsilon)})$. U_f es pues unitaria. Sea $A \subset V^n$ un conjunto no-vacío de asignaciones y sea $a = \mathrm{card}(A)$ su cardinalidad. Al considerar el estado $\mathbf{u}_A = \frac{1}{\sqrt{a}} \sum_{\varepsilon \in A} \mathbf{e}_\varepsilon \otimes \mathbf{e}_\mathbf{0}$ se tiene $U_f(\mathbf{u}_A) = \frac{1}{\sqrt{a}} \sum_{\varepsilon \in A} \mathbf{e}_\varepsilon \otimes \mathbf{e}_{f(\varepsilon)}$ y así en un solo paso de cómputo se calcula a un promedio ponderado de la imagen de las asignaciones con índice en A. El proceso final de medición consiste en la selección de una pareja $\mathbf{e}_\varepsilon \otimes \mathbf{e}_{f(\varepsilon)}$, $\varepsilon \in A$, cada una con probabilidad $\frac{1}{a}$.

7.5 Algoritmo de Deutsch-Jozsa

Deutsch-Josza [Deutsch and Jozsa(1992)] propusieron el primer algoritmo en el que la Computación Cuántica proporcionó un decremento sustancial en la complejidad en tiempo. Sea $V = \{0,1\}$ el conjunto de valores de verdad clásicos. De las $2^2 = 4$ funciones booleanas $f : V \to V$ dos son constantes y las otras dos son equilibradas. Al nombrarlas

$$f_0 : \begin{matrix} 0 \mapsto 0 \\ 1 \mapsto 0 \end{matrix} \quad , \quad f_1 : \begin{matrix} 0 \mapsto 0 \\ 1 \mapsto 1 \end{matrix} \quad , \quad f_2 : \begin{matrix} 0 \mapsto 1 \\ 1 \mapsto 0 \end{matrix} \quad , \quad f_3 : \begin{matrix} 0 \mapsto 1 \\ 1 \mapsto 1 \end{matrix}$$

se tiene que las funciones constantes son f_0 y f_3, y las equilibradas son f_1 y f_2.

El propósito del algoritmo de Deutsch-Jozsa es decidir, para una f dada, si acaso es constante o equilibrada "utilizando un solo paso de cómputo".

Sea U_f una matriz permutación de orden $2^2 \times 2^2$ tal que $U_f(\mathbf{e}_x \otimes \mathbf{e}_z) = (\mathbf{e}_x \otimes \mathbf{e}_{(z+f(x)) \bmod 2})$. U_f es pues unitaria. De hecho es muy similar al funcionamiento de la compuerta "negación controlada", salvo que en aquella, la función f es propiamente la identidad. En la tabla 7.1 ilustramos la acción de U_f refiriéndonos solamente a los índices de vectores básicos.

(x,z)	$(x,(z+f(x)) \bmod 2)$
(0,0)	$(0,f(0))$
(0,1)	$(0,\overline{f(0)})$
(1,0)	$(1,f(1))$
(1,1)	$(1,\overline{f(1)})$

Table 7.1 Acción de la matriz unitaria U_f en el algoritmo de Deutsch-Jozsa.

Considerando el operador de Hadamard H, hagamos $H_2 = H \otimes H$. Primero se tiene, $H(\mathbf{e}_0) = \mathbf{x}_0 = \frac{1}{\sqrt{2}}(\mathbf{e}_0 + \mathbf{e}_1)$ y $H(\mathbf{e}_1) = \mathbf{x}_1 = \frac{1}{\sqrt{2}}(\mathbf{e}_0 - \mathbf{e}_1) \in \mathbb{H}_1$ y luego $H_2(\mathbf{e}_0 \otimes \mathbf{e}_1) = H(\mathbf{e}_0) \otimes H(\mathbf{e}_1) = \mathbf{x}_0 \otimes \mathbf{x}_1$. Claramente, $\mathbf{x}_0 \otimes \mathbf{x}_1 = \frac{1}{2}(\mathbf{e}_{00} - \mathbf{e}_{01} + \mathbf{e}_{10} - \mathbf{e}_{11}) \in \mathbb{H}_2$. Por tanto,

$$
\begin{aligned}
U_f(\mathbf{x}_0 \otimes \mathbf{x}_1) &= \frac{1}{2}(\mathbf{e}_{0,f(0)} - \mathbf{e}_{0,\overline{f(0)}} + \mathbf{e}_{1,f(1)} - \mathbf{e}_{1,\overline{f(1)}}) \\
&= \frac{1}{\sqrt{2}}\mathbf{e}_0 \otimes \left[\frac{1}{\sqrt{2}}(\mathbf{e}_{f(0)} - \mathbf{e}_{\overline{f(0)}})\right] + \frac{1}{\sqrt{2}}\mathbf{e}_1 \otimes \left[\frac{1}{\sqrt{2}}(\mathbf{e}_{f(1)} - \mathbf{e}_{\overline{f(1)}})\right] \\
&= \begin{cases} \frac{1}{\sqrt{2}}\mathbf{e}_0 \otimes \mathbf{x}_1 + \frac{1}{\sqrt{2}}\mathbf{e}_1 \otimes \mathbf{x}_1 \text{ si } f = f_0 \\ \frac{1}{\sqrt{2}}\mathbf{e}_0 \otimes \mathbf{x}_1 - \frac{1}{\sqrt{2}}\mathbf{e}_1 \otimes \mathbf{x}_1 \text{ si } f = f_1 \\ -\frac{1}{\sqrt{2}}\mathbf{e}_0 \otimes \mathbf{x}_1 + \frac{1}{\sqrt{2}}\mathbf{e}_1 \otimes \mathbf{x}_1 \text{ si } f = f_2 \\ -\frac{1}{\sqrt{2}}\mathbf{e}_0 \otimes \mathbf{x}_1 - \frac{1}{\sqrt{2}}\mathbf{e}_1 \otimes \mathbf{x}_1 \text{ si } f = f_3 \end{cases} \\
&= \begin{cases} \mathbf{x}_0 \otimes \mathbf{x}_1 \text{ si } f = f_0 \\ \mathbf{x}_1 \otimes \mathbf{x}_1 \text{ si } f = f_1 \\ -\mathbf{x}_1 \otimes \mathbf{x}_1 \text{ si } f = f_2 \\ -\mathbf{x}_0 \otimes \mathbf{x}_1 \text{ si } f = f_3 \end{cases}
\end{aligned}
$$

En consecuencia,

$$H_2U_fH_2(\mathbf{e}_0\otimes\mathbf{e}_1)=H_2U_f(\mathbf{x}_0\otimes\mathbf{x}_1)=\begin{cases}H\mathbf{x}_0\otimes H\mathbf{x}_1 \text{ si } f=f_0\\ H\mathbf{x}_1\otimes H\mathbf{x}_1 \text{ si } f=f_1\\ -H\mathbf{x}_1\otimes H\mathbf{x}_1 \text{ si } f=f_2\\ -H\mathbf{x}_0\otimes H\mathbf{x}_1 \text{ si } f=f_3\end{cases}$$
$$=\begin{cases}\mathbf{e}_0\otimes\mathbf{e}_1 \text{ si } f=f_0\\ \mathbf{e}_1\otimes\mathbf{e}_1 \text{ si } f=f_1\\ -\mathbf{e}_1\otimes\mathbf{e}_1 \text{ si } f=f_2\\ -\mathbf{e}_0\otimes\mathbf{e}_1 \text{ si } f=f_3\end{cases}$$

vale decir, al aplicar el algoritmo cuántico $H_2U_fH_2$ (nótese que utilizamos notación algebraica: los operadores se aplican de derecha a izquierda), partiendo del vector básico $\mathbf{e}_0\otimes\mathbf{e}_1$ se obtiene un vector de la forma $\varepsilon\mathbf{e}_S\otimes\mathbf{e}_1$ donde $\varepsilon\in\{-1,1\}$ es un signo y S es una señal que indica si acaso f es o no equilibrada. En otras palabras, la respuesta S coincide con $f(0)\oplus f(1)$, donde $\oplus$ es la *disyunción excluyente*, XOR. La auscultación del valor S se realiza siguiendo el postulado de medición, y su valor está apareciendo leyendo sólo el primer qubit. Al efectuar la medición se elige al vector básico $\mathbf{e}_S\otimes\mathbf{e}_1$ con probabilidad $\varepsilon^2=1$.

7.6 Algoritmo para el cálculo de la Transformada Discreta de Fourier

Sea $f:[\![0,n-1]\!]\to\mathbb{C}$ una función. La *transformada discreta de Fourier* de f es la función $\hat{f}:[\![0,n-1]\!]\to\mathbb{C}$ tal que para cada $j\in[\![0,n-1]\!]$: $\hat{f}(j)=\frac{1}{\sqrt{n}}\sum_{k=0}^{n-1}\exp\left(\frac{2\pi ijk}{n}\right)f(k)$. Aquí i es la raíz cuadrada de -1.

En $\mathbb{C}^n$ consideremos la base canónica formada por los vectores $\mathbf{e}_j=(\delta_{ij})_{i=0}^{n-1}$, $j=0,\ldots,n-1$. Para cada vector $\mathbf{f}=\sum_{j=0}^{n-1}f(j)\mathbf{e}_j\in\mathbb{C}^n$, su *transformada discreta de Fourier* es $\mathrm{TDF}(\mathbf{f})=\hat{\mathbf{f}}=\sum_{j=0}^{n-1}\hat{f}(j)\mathbf{e}_j\in\mathbb{C}^n$. Es claro que TDF es una transformación lineal y, respecto a la base canónica de $\mathbb{C}^n$, se representa por la matriz $\mathrm{TDF}=\frac{1}{\sqrt{n}}\left(\exp\left(\frac{2\pi ijk}{n}\right)\right)_{jk}$, la cual es en efecto unitaria, de hecho la matriz hermitiana de TDF, TDF^H, tiene la misma estructura que TDF salvo que los exponentes en cada entrada tienen el signo "$-$".

En particular, se tiene

$$\forall j\in[\![0,n-1]\!]:\ \mathrm{TDF}(\mathbf{e}_j)=\frac{1}{\sqrt{n}}\sum_{k=0}^{n-1}\exp\left(\frac{2\pi ijk}{n}\right)\mathbf{e}_k. \tag{7.12}$$

y, por supuesto,

$$\mathrm{TDF}(\mathbf{f})=\sum_{j=0}^{n-1}f(j)\,\mathrm{TDF}(\mathbf{e}_j). \tag{7.13}$$

Ahora, supongamos que $n = 2^\nu$ es una potencia de 2. En este caso, la TDF puede calcularse mediante el procedimiento de la llamada *transformada rápida de Fourier* TRF (o si se quiere, FFT por sus siglas en inglés: *Fast Fourier Transform*). Este procedimiento es de complejidad en tiempo $O(\nu 2^\nu) = O(n \log n)$. Mas utilizando el paralelismo inherente a la computación cuántica, se le calculará aquí en un tiempo $O(\nu)$.

Observamos, por un lado, que $\mathbb{H}_\nu = \mathbb{C}^n$, y por otro lado, de la ecuación (7.12), que para los primeros valores de ν se tiene:

$\nu = 1$

$$\begin{aligned}\mathrm{TDF}(\mathbf{e}_0) &= \frac{1}{\sqrt{2}}(\mathbf{e}_0 + \mathbf{e}_1)\\ \mathrm{TDF}(\mathbf{e}_1) &= \frac{1}{\sqrt{2}}(\mathbf{e}_0 - \mathbf{e}_1)\end{aligned}$$

$\nu = 2$

$$\begin{aligned}\mathrm{TDF}(\mathbf{e}_{00}) &= \frac{1}{\sqrt{2}}(\mathbf{e}_0 + \mathbf{e}_1) \otimes \frac{1}{\sqrt{2}}(\mathbf{e}_0 + \mathbf{e}_1)\\ \mathrm{TDF}(\mathbf{e}_{01}) &= \frac{1}{\sqrt{2}}(\mathbf{e}_0 - \mathbf{e}_1) \otimes \frac{1}{\sqrt{2}}(\mathbf{e}_0 + i\mathbf{e}_1)\\ \mathrm{TDF}(\mathbf{e}_{10}) &= \frac{1}{\sqrt{2}}(\mathbf{e}_0 + \mathbf{e}_1) \otimes \frac{1}{\sqrt{2}}(\mathbf{e}_0 - \mathbf{e}_1)\\ \mathrm{TDF}(\mathbf{e}_{11}) &= \frac{1}{\sqrt{2}}(\mathbf{e}_0 - \mathbf{e}_1) \otimes \frac{1}{\sqrt{2}}(\mathbf{e}_0 - i\mathbf{e}_1)\end{aligned}$$

De manera general, a cada índice $j \in [\![0, 2^\nu - 1]\!]$ lo identificaremos con la palabra $\varepsilon_j = \varepsilon_{j,\nu-1} \cdots \varepsilon_{j,1}\varepsilon_{j,0}$ que lo representa en base 2. Así, el vector básico $\mathbf{e}_{\varepsilon_j} \in \mathbb{H}_\nu$ es el producto tensorial de los vectores básicos $\mathbf{e}_{\varepsilon_{j,k}} \in \mathbb{H}_1$. Tendremos entonces, en $\mathbb{H}_\nu$, que para cada $j = 0, \ldots, 2^\nu - 1$:

$$\begin{aligned}\mathrm{TDF}(\mathbf{e}_{\varepsilon_j}) &= \bigotimes_{k=0}^{\nu-1} \frac{1}{\sqrt{2}} \left(\mathbf{e}_0 + \exp\left(\frac{\pi i j}{2^k}\right) \mathbf{e}_1 \right)\\ &= \tfrac{1}{\sqrt{2}}\left(\mathbf{e}_0 + \exp\left(\tfrac{\pi i j}{2^0}\right)\mathbf{e}_1\right) \otimes \tfrac{1}{\sqrt{2}}\left(\mathbf{e}_0 + \exp\left(\tfrac{\pi i j}{2^1}\right)\mathbf{e}_1\right) \otimes \cdots \otimes \tfrac{1}{\sqrt{2}}\left(\mathbf{e}_0 + \exp\left(\tfrac{\pi i j}{2^{\nu-1}}\right)\mathbf{e}_1\right) \quad (7.14)\end{aligned}$$

La forma de los factores en este producto tensorial sugiere considerar los operadores $Q_k : \mathbb{H}_1 \to \mathbb{H}_1$ con representación, respecto a la base canónica, dada mediante la matriz unitaria $Q_k = \begin{bmatrix} 1 & 0 \\ 0 & \exp\left(\frac{\pi i}{2^k}\right) \end{bmatrix}$. De hecho, como en (7.14) la potencia en la exponenciación va cambiando, podemos considerar más bien un correspondiente operador "controlado": $Q^c_{kj} = \begin{bmatrix} 1 & 0 \\ 0 & \exp\left(\pi i \frac{j}{2^k}\right) \end{bmatrix}$. Así, por ejemplo, si $j = 1$ entonces $Q^c_{k1} = Q_k$ en tanto que si $j = 0$ entonces $Q^c_{k0} = I$ coincide con la identidad.

Observamos además que para $\mathbf{x}_0 = \frac{1}{\sqrt{2}}(\mathbf{e}_0 + \mathbf{e}_1) = H(\mathbf{e}_0)$ se tiene $Q^c_{kj}(\mathbf{x}_0) = \frac{1}{\sqrt{2}}\left(\mathbf{e}_0 + \exp\left(\pi i \frac{j}{2^k}\right)\mathbf{e}_1\right)$.

Ahora, a cada $j \in [\![0, 2^\nu - 1]\!]$ representémoslo en base-2 mediante la palabra ε_j. Se tiene que para cada $\ell \in [\![0, \nu-1]\!]$, $\frac{\varepsilon_{j,\ell}2^\ell}{2^k} = \frac{\varepsilon_{j,\ell}}{2^{k-\ell}}$. Por tanto, $\exp\left(\pi i \frac{j}{2^k}\right) = \exp\left(\pi i \frac{\sum_{\ell=0}^{\nu-1}\varepsilon_{j,\ell}2^\ell}{2^k}\right) = \prod_{\ell=0}^{\nu-1}\exp\left(\pi i \frac{\varepsilon_{j,\ell}}{2^{k-\ell}}\right)$ y en consecuencia, $Q^c_{kj} = Q^c_{k-\nu+1,\varepsilon_{j,\nu-1}} \circ \cdots \circ Q^c_{k-1,\varepsilon_{j,1}} \circ Q^c_{k,\varepsilon_{j,0}}$. Como k ha de variar entre 0 y $\nu-1$ vemos que se ha de disponer de $2(2\nu-1)$ compuertas de la forma $Q^c_{\kappa\varepsilon}$, $\kappa \in [\![-(\nu-1), \nu-1]\!]$, $\varepsilon \in \{0,1\}$.

Observamos también que si $j < 2^{\nu_1}$, con $\nu_1 \leq \nu$ entonces todos los dígitos, en su representación binaria, con índices entre $\nu_1 - 1$ y $\nu - 1$ son 0, y por tanto las correspondientes compuertas controladas actuarán como la identidad. Definamos pues para cada $(j,k) \in [\![0, 2^\nu - 1]\!] \times [\![0, \nu-1]\!]$,

$$P_{jk} = Q^c_{k-\nu_1+1,\varepsilon_{j,\nu_1-1}} \circ \cdots \circ Q^c_{k-1,\varepsilon_{j,1}} \circ Q^c_{k,\varepsilon_{j,0}}, \tag{7.15}$$

donde $\nu_1 = \lceil \log_2 j \rceil + 1$. Tenemos pues: $P_{jk}(\mathbf{x}_0) = \frac{1}{\sqrt{2}}\left(\mathbf{e}_0 + \exp\left(\pi i \frac{j}{2^k}\right)\mathbf{e}_1\right)$.

Fijo $j \in [\![0, 2^\nu - 1]\!]$ para $k = 0, \ldots, \nu-1$ los términos $P_{jk}(\mathbf{x}_0)$ van dando los de la derecha de la ec. (7.14) y éstos van apareciendo de izquierda a derecha según se les muestra ahí. Sin embargo, para cada $k \in [\![0, \nu-1]\!]$ observamos que en la definición (7.15) se está utilizando una notación algebraica, es decir, los operadores $Q^c_{k-\ell,\varepsilon_{j,\ell}}$ se aplican en orden inverso: de derecha a izquierda. De hecho, haciendo un poco más explícita la definición (7.15) se tiene:

$$\begin{aligned}
Q^c_{0,\varepsilon_{j,0}}(\mathbf{x}_0) &= P_{j0}(\mathbf{x}_0) \\
Q^c_{1,\varepsilon_{j,0}} \circ Q^c_{0,\varepsilon_{j,1}}(\mathbf{x}_0) &= P_{j1}(\mathbf{x}_0) \\
Q^c_{2,\varepsilon_{j,0}} \circ Q^c_{1,\varepsilon_{j,1}} \circ Q^c_{0,\varepsilon_{j,2}}(\mathbf{x}_0) &= P_{j2}(\mathbf{x}_0) \\
\vdots \quad & \quad \vdots \\
Q^c_{\nu-1,\varepsilon_{j,0}} \circ \cdots \circ Q^c_{2,\varepsilon_{j,\nu-3}} \circ Q^c_{1,\varepsilon_{j,\nu-2}} \circ Q^c_{0,\varepsilon_{j,\nu-1}}(\mathbf{x}_0) &= P_{j,\nu-1}(\mathbf{x}_0)
\end{aligned}$$

es decir, para cada $k \in [\![0, \nu-1]\!]$ se han de aplicar consecutivamente las compuertas $Q^c_{\ell,\varepsilon_{j,k-\ell}}$, con $\ell = 0, \ldots, k$, la cual selecciona a los dígitos en la representación binaria de j yendo del más significativo hacia el menos significativo.

Así pues, será necesario utilizar los operadores reverso para intercambiar el orden de los bits de cada índice $j \in [\![0, 2^\nu - 1]\!]$.

Ahora bien, cada bit ε se representa por el vector básico $\mathbf{e}_\varepsilon$. Así que cada operador controlado $Q^c_{k,\varepsilon}$, cuyo dominio es $\mathbb{H}_1$ puede identificarse con el operador $\mathbf{x} \mapsto Q^{c2}(\mathbf{x}, \mathbf{e}_\varepsilon)$ donde

$$Q^{c2} = (I \otimes Q_k) \circ C \circ (I \otimes Q_k^H) \circ C \circ (Q_k \otimes I). \tag{7.16}$$

El algoritmo para calcular la transformada de Fourier es entonces el siguiente:

Entrada. $n = 2^\nu$, $\mathbf{f} \in \mathbb{C}^n = \mathbb{H}_\nu$.
Salida. $\hat{\mathbf{f}} = \mathrm{TDF}(\mathbf{f}) \in \mathbb{H}_\nu$.
Procedimiento `TDF`$(n, \mathbf{f})$

1. Sea $\mathbf{x}_0 := H(\mathbf{e}_0)$.
2. Para cada $j \in [\![0, 2^\nu - 1]\!]$, o equivalentemente, para cada $\left(\varepsilon_{j,\nu-1} \cdots \varepsilon_{j,1}\varepsilon_{j,0}\right) \in \{0,1\}^\nu$, hágase en paralelo:
   a. Para cada $k \in [\![0, \nu - 1]\!]$ hágase en paralelo:
      i. Sea $\delta := R_k\left(\varepsilon_j\big|_k\right)$ el reverso de la cadena formada por los $(k+1)$ bits menos significativos (véase la ec. (7.4)).
      ii. Sea $\mathbf{y}_{jk} := \mathbf{x}_0$.
      iii. Para $\ell = 0$ hasta k hágase $\{\ \mathbf{y}_{jk} := Q^{c2}(\mathbf{y}_{jk}, \mathbf{e}_{\delta_{j,\ell}})$ (véase la ec. (7.16)) $\}$
   b. Sea $\mathbf{y}_j := \mathbf{y}_{j0} \otimes \cdots \otimes \mathbf{y}_{j,\nu-1}$ (véase la ec. (7.14)).
3. Dése como resultado $\hat{\mathbf{f}} = \sum_{j=0}^{2^\nu-1} f_j \mathbf{y}_j$.

El cálculo de la transformada inversa discreta de Fourier, `TIDF`$(n, \mathbf{f})$ se hace de manera similar cambiando la matriz Q_k por su hermitiana Q_k^H que sólo involucra el cambio de signo en la potencia de su elemento $(2,2)$.

7.7 Algoritmo de Shor

Este algoritmo es de tipo cuántico y tiene el propósito de factorizar a un número entero dado n como el producto de dos enteros menores, si esto es posible, o bien indicar que n es primo, en otro caso. Una presentación muy detallada puede verse en [Lavor et al(2003)]. Los artículos originales de Shor [Shor(1994), Shor(1997)] son, evidentemente, fuentes sumamente importantes de información.

7.7.1 Pequeño recordatorio de Teoría de Números

Dados dos enteros n, m, su *máximo común divisor* es $d = \mathrm{mcd}(n,m)$ tal que d divide a ambos n y m, es decir es un divisor común de n y m, y cualquier otro divisor común divide a d también. Se puede ver que d es el menor entero positivo que se puede escribir como una combinación lineal de n y m con coeficientes enteros. El *Algoritmo de Euclides* calcula, para dos enteros n y m dados, $d = \mathrm{mcd}(n,m)$ y lo expresa de la forma $d = an + bm$, con $a, b \in \mathbb{Z}$.

Los enteros n y m son *primos relativos* si $\mathrm{mcd}(n,m) = 1$, es decir, si no poseen un divisor común que no sea trivial. Sea $\Phi(n) = \{m \in [\![1,n]\!] \,|\, \mathrm{mcd}(n,m) = 1\}$ el conjunto de enteros positivos primos relativos con n, menores que n. Se tiene que el número de elementos en $\Phi(n)$ es el valor de la *función de Euler* ϕ en n. Con la multiplicación módulo n, $\Phi(n)$ es un grupo de orden $\phi(n)$. Así pues, si $m \in \Phi(n)$

entonces $m^{\phi(n)} = 1 \bmod n$. Por tanto, para cada entero $m \in \Phi(n)$ existe un mínimo elemento r, divisor de $\phi(n)$, tal que $m^r = 1 \bmod n$. Tal r se dice ser el *orden* de m en el grupo multiplicativo de residuos módulo n.

Sea n un entero para el cual se ha de buscar un factor entero no trivial. Elijamos un entero m tal que $1 < m < n$. Si $\mathrm{mcd}(n,m) = d > 1$, entonces d es un factor no-trivial de n. En otro caso, $\mathrm{mcd}(n,m) = 1$, y se tiene que m quedará en el grupo multiplicativo de residuos de n, i.e. $m \in \Phi(n)$. Si acaso m tuviera ahí un orden par r, entonces $k = m^{\frac{r}{2}}$ es tal que $k^2 = 1 \bmod n$. En consecuencia, $(k-1)(k+1) = 0 \bmod n$, es decir n divide al producto de dos números menores que él. Por tanto, los factores primos de n han de aparecer como factores de esos números. Así pues al calcular $\mathrm{mcd}(n,k-1)$ y $\mathrm{mcd}(n,k+1)$ obtendremos factores no-triviales de n.

Un primer problema en este procedimiento de decisión consiste entonces en encontrar un elemento de orden par en el grupo multiplicativo de residuos módulo n. Si se elige m al azar, la probabilidad de que m sea de orden par es $1 - \frac{1}{2^\ell}$ donde ℓ es el número de factores primos en n. Así pues, la probabilidad de que al cabo de k intentos no se haya localizado un tal m es $2^{-k\ell}$ y obviamente esto tiende a cero muy rápidamente al incrementar k. Así pues, bien vale la pena repetir pruebas arbitrarias de selección de un elemento (impar) menor que n para localizar uno de orden par en el grupo multiplicativo de residuos módulo n.

Sin embargo, desde el punto de vista computacional, el mayor problema que presenta el algoritmo descrito radica en el cálculo del orden del elemento actual m en $\Phi(n)$: el número de potencias de m a calcular es del orden de $\phi(n)$ que a su vez es de orden n.

Sea $\nu = \lceil \log_2 n \rceil$ el número de bits necesarios para escribir a n, es decir, sea ν el *tamaño* de n. Resulta claro que $O(n) = O(2^\nu)$ lo cual indica que el procedimiento anterior es de complejidad exponencial respecto al tamaño de la entrada. El algoritmo de Shor se fundamenta en un procedimiento polinomial en ν para realizar la tarea de calcular el orden de un elemento.

7.7.2 Algoritmo cuántico para el cálculo de órdenes

Supongamos dado $n \in \mathbb{N}$. Sea $\nu = \lceil \log_2 n \rceil$ su tamaño. Sea κ tal que $n^2 \leq 2^\kappa < 2n^2$, es decir, $\kappa = \lceil 2\log_2 n \rceil$. Se considerará $\kappa + \nu$ qubits y se trabajará en el espacio $\mathbb{H}_{\kappa+\nu} = \mathbb{H}_\kappa \otimes \mathbb{H}_\nu$, de dimensión $2^{\kappa+\nu} = 2^\kappa \cdot 2^\nu$.

Para cada $m \in \Phi(n)$ definimos un operador lineal unitario $V_m : \mathbb{H}_{\kappa+\nu} \to \mathbb{H}_{\kappa+\nu}$ haciéndolo actuar en los vectores básicos como

$$V_m : \mathbf{e}_{\varepsilon_j} \otimes \mathbf{e}_{\varepsilon_i} \mapsto \mathbf{e}_{\varepsilon_j} \otimes \mathbf{e}_{\varepsilon_{f(i,j,m)}} \tag{7.17}$$

donde $f(i,j,m) = (j + m^i) \bmod n$.

Elementos con orden potencia de 2

Supongamos dado $m \in \Phi(n)$ y que éste es tal que su orden r es una potencia de 2.

Sea $P_1 = H^{\otimes\kappa} \otimes I^{\otimes\nu}$ donde $H, I : \mathbb{H}_1 \to \mathbb{H}_1$ son los operadores de Hadamard e identidad respectivamente. Por la ec. (7.3) se tiene $P_1(\mathbf{e_0} \otimes \mathbf{e_0}) = \frac{1}{\sqrt{2^\kappa}} \sum_{\varepsilon \in \{0,1\}^\kappa} \mathbf{e}_\varepsilon \otimes \mathbf{e_0}$. Escribamos $\mathbf{s}_1 = P_1(\mathbf{e_0} \otimes \mathbf{e_0})$. Ahora, aplicando el operador V_m, resulta $V_m(\mathbf{s}_1) = \frac{1}{\sqrt{2^\kappa}} \sum_{i=0}^{2^\kappa - 1} \mathbf{e}_{\varepsilon_i} \otimes \mathbf{e}_{\varepsilon_{f(i,0,m)}}$. Escribamos $\mathbf{s}_2 = V_m(\mathbf{s}_1)$.

Ya que $f(i,0,m) = m^i \bmod n$, f es una función periódica de período r respecto a i. Sea $J_j = \{i | 0 \le i \le 2^\kappa - 1 : i = j \bmod r\}$ la clase de índices que dejan residuo j al dividírseles entre r. Claramente $[\![0, 2^\kappa - 1]\!] = \bigcup_{j=0}^{r-1} J_j$, y la cardinalidad de cada conjunto J_j es $s = \frac{2^\kappa}{r}$, el cual número, para este caso, es entero. Por tanto, es posible reescribir

$$\mathbf{s}_2 = \frac{1}{\sqrt{2^\kappa}} \sum_{j=0}^{r-1} \left(\sum_{i \in J_j} \mathbf{e}_{\varepsilon_i} \right) \otimes \mathbf{e}_{\varepsilon_{m^j}}. \tag{7.18}$$

Si aquí se aplica el postulado de medición, entonces se elegirá a un vector de la forma $\mathbf{e}_{\varepsilon_i} \otimes \mathbf{e}_{\varepsilon_{m^{j_0}}}$, $i \in J_{j_0}$, para una potencia fija $j_0 \le r$, con probabilidad $\frac{r}{2^\kappa}$. El estado correspondiente a esta situación es de la forma

$$\mathbf{s}_3 = \sum_{i=0}^{2^\kappa - 1} g(i) \mathbf{e}_{\varepsilon_i} \otimes \mathbf{e}_{\varepsilon_{m^{j_0}}}. \tag{7.19}$$

donde $g : i \mapsto \begin{cases} \sqrt{\frac{r}{2^\kappa}} & \text{si } i \in J_{j_0} \\ 0 & \text{si } i \notin J_{j_0} \end{cases}$

La función g también es periódica, de período r. Ahora, se tiene que la transformada de Fourier de g, $\hat{g}$ será también periódica pero de período proporcional a $\frac{1}{r}$.

Calculemos la transformada inversa discreta de Fourier de $\mathbf{s}_3$:

$$\check{\mathbf{s}_3} = \mathrm{TDF}^H(\mathbf{s}_3) = \sqrt{\frac{r}{2^\kappa}} \sum_{k=0}^{s-1} \left(\frac{1}{\sqrt{2^\kappa}} \sum_{\ell=0}^{2^\kappa - 1} \exp\left(-\frac{2\pi i \ell}{2^\kappa} (kr + j_0) \right) \mathbf{e}_\ell \right) \otimes \mathbf{e}_{\varepsilon_{m^{j_0}}},$$

y al intercambiar el orden de las sumatorias se obtiene:

$$\mathbf{s}_4 = \check{\mathbf{s}_3} = \frac{1}{\sqrt{r}} \left(\sum_{\ell=0}^{2^\kappa - 1} \left(\frac{1}{s} \sum_{k=0}^{s-1} \exp\left(-\frac{2\pi i \ell k}{s} \right) \right) \exp\left(-\frac{2\pi i \ell j_0}{2^\kappa} \right) \mathbf{e}_\ell \right) \otimes \mathbf{e}_{\varepsilon_{m^{j_0}}}. \tag{7.20}$$

Ya que $\exp\left(-\frac{2\pi i \ell}{s}\right)$ es una raíz s-ésima de la unidad, se tiene $\frac{1}{s} \sum_{k=0}^{s-1} \exp\left(-\frac{2\pi i \ell k}{s}\right)$ será 1 o 0 en función de que ℓ sea o no un múltiplo entero de s, es decir un número de la forma $\ell = ts$, con $t = 0, \ldots, r-1$. Aquí es esencial el hecho de que s es entero. Así pues, de (7.20),

$$\mathbf{s}_4 = \frac{1}{\sqrt{r}} \left(\sum_{t=0}^{r-1} \exp\left(-\frac{2\pi i t j_0}{r} \right) \mathbf{e}_{\frac{2\kappa_t}{r}} \right) \otimes \mathbf{e}_{\varepsilon_{m^{j_0}}}. \tag{7.21}$$

Las relaciones (7.19) y (7.21), que expresan a $\mathbf{s}_3$ y $\mathbf{s}_4 = \check{\mathbf{s}}_3$, involucran ambas al orden r. Pero hay una diferencia esencial entre ellas: En (7.19) los índices i, en el primer qubit, correspondientes a coeficientes no-nulos dependen de la potencia "aleatoria" j_0, en tanto que en (7.21) no dependen de ésa, e involucran sin embargo, a r.

Si ahora se aplica el postulado de medición se obtendrá un valor de la forma $\frac{2^\kappa t_0}{r}$, con $t_0 \in [\![0, r-1]\!]$, cada uno con probabilidad r^{-1}. Si $t_0 = 0$, entonces no es posible obtener ninguna información acerca de r y se ha de repetir el procedimiento otra vez. En otro caso, al dividir entre 2^κ se tiene el valor racional $\frac{r_0}{r_1} = \frac{t_0}{r}$. Se conoce a r_0 y r_1 mas aún no se conoce t_0 ni r. Sin embargo, necesariamente r_1 divide a r. Así pues, se puede aplicar de nuevo el algoritmo cuántico a partir de $m_1 = m^{r_1}$. Procediendo recursivamente se obtiene una factorización $r = r_1 r_2 \cdots r_p$ conteniendo a lo más $\log_2 r$ factores.

En resumen, el algoritmo para localizar divisores de órdenes de elementos es el siguiente:

Entrada. $n \in \mathbb{N}$, $m \in \Phi(n)$ de orden potencia de 2.
Salida. r tal que $r | o(m)$.
Procedimiento `DivisorOrdenPotencia2`(n,m)

1. Sea $\nu := \lceil \log_2 n \rceil$, $\kappa := 2\nu$.
2. Defínase $V_m : \mathbb{H}_{\kappa+\nu} \to \mathbb{H}_{\kappa+\nu}$ como en la ec. (7.17).
3. Sea $\mathbf{s}_1 := (H^{\otimes\kappa} \otimes I^{\otimes\nu})(\mathbf{e_0} \otimes \mathbf{e_0})$.
4. Sea $\mathbf{s}_2 := V_m(\mathbf{s}_1)$.
5. Sea $\mathbf{s}_3 := \sum_{i=0}^{2^\kappa - 1} g(i) \mathbf{e}_{\varepsilon_i} \otimes \mathbf{e}_{\varepsilon_{m^{j_0}}}$ el estado equivalente a "tomar una medición" en $\mathbf{s}_2$. Entonces g queda determinada como en la ec. (7.19).
6. Sea $\mathbf{s}_4 := \texttt{TIDF}(2^\kappa, \mathbf{s}_3)$ la transformada inversa discreta de Fourier de $\mathbf{s}_3$.
7. Sea $\mathbf{e}_{\varepsilon_k} \otimes \mathbf{e}_{\varepsilon_{m^{j_0}}}$ una medición de $\mathbf{s}_4$.
8. Si $k == 0$ repítase desde el paso 3. En otro caso sea $\frac{r_0}{r_1} = \frac{k}{2^\kappa}$ y dése como resultado r_1.

El algoritmo para calcular órdenes de elementos es el siguiente:

Entrada. $n \in \mathbb{N}$, $m \in \Phi(n)$ de orden potencia de 2.
Salida. r tal que $r = o(m)$.
Procedimiento `OrdenPotencia2`(n,m)

1. Sean inicialmente $r := 1$ y $m_1 := m$.
2. Repítase
   a. sea $r_1 := \texttt{DivisorOrdenPotencia2}(n, m_1)$;
   b. actualícese $r := r \cdot r_1$;
   c. actualícese $m_1 := m_1^{r_1} \bmod n$.
   hasta tener $r_1 == 1$.
3. Dése como resultado r.

Elementos con orden arbitrario

Dejemos de suponer que el orden r de m sea una potencia de 2 en $\Phi(n)$. Siguiendo la misma línea que en el caso anterior, sea V_m definido como en la ec. (7.17). Sea $\mathbf{s}_1 = (H^{\otimes\kappa} \otimes I^{\otimes\nu})(\mathbf{e_0} \otimes \mathbf{e_0})$ y $\mathbf{s}_2 = V_m(\mathbf{s}_1)$. Reagrupando los términos según se hizo en la ec. (7.18) se puede escribir

$$\mathbf{s}_2 = \frac{1}{\sqrt{2^\kappa}} \sum_{j=0}^{r-1} \left(\sum_{i \in J_j} \mathbf{e}_{\varepsilon_i} \right) \otimes \mathbf{e}_{\varepsilon_{mj}}. \tag{7.22}$$

donde los conjuntos J_j son clases de equivalencia, congruentes con j, módulo r, pero ahora no son de la misma cardinalidad. Si $u = 2^\kappa \bmod r$ y $s = (2^\kappa - u)/r$ entonces u clases tendrán $s+1$ elementos y las restantes tendrán s elementos. Definamos $s_j = s+1$ para $j = 1, \ldots, u$ y $s_j = s$ para $j = u+1, \ldots, r-1, 0$. Entonces el estado que representa el tomar una medición, como en la ec. (7.19), es, para algún $j_0 \in [\![0, r-1]\!]$:

$$\mathbf{s}_3 = \sum_{i=0}^{2^\kappa - 1} g(i) \mathbf{e}_{\varepsilon_i} \otimes \mathbf{e}_{\varepsilon_{mj_0}}. \tag{7.23}$$

donde $g : i \mapsto \begin{cases} \frac{1}{\sqrt{s_{j_0}}} & \text{si } i \in J_{j_0} \\ 0 & \text{si } i \notin J_{j_0} \end{cases}$

Calculando la transformada inversa discreta de Fourier y reagrupando términos, como en la ec. (7.20), se obtiene

$$\mathbf{s}_4 = \check{\mathbf{s}_3} = \frac{1}{\sqrt{2^\kappa}} \left(\sum_{\ell=0}^{2^\kappa - 1} \left(\frac{1}{\sqrt{s_{j_0}}} \sum_{k=0}^{s_{j_0}-1} \exp\left(-\frac{2\pi i \ell k r}{2^\kappa} \right) \right) \exp\left(-\frac{2\pi i \ell j_0}{2^\kappa} \right) \mathbf{e}_\ell \right) \otimes \mathbf{e}_{\varepsilon_{mj_0}}. \tag{7.24}$$

pero en este caso el coeficiente que involucra a la suma interior nunca se anula (como r no necesariamente divide a 2^κ, aquí no se está sumando un "juego completo" de raices s_{j_0}-ésimas de la unidad). Al tomar una medición del primer qubit, la probabilidad de que se elija a $\mathbf{e}_\ell \otimes \mathbf{e}_{\varepsilon_{mj_0}}$ es entonces

$$P(\ell) = \frac{1}{\sqrt{2^\kappa s_{j_0}}} \left| \sum_{k=0}^{s_{j_0}-1} \exp\left(-\frac{2\pi i \ell k r}{2^\kappa} \right) \right|^2$$

y los máximos de esos valores corresponden a enteros $\ell = \texttt{EnteroMásPróximo}\left(\frac{k2^\kappa}{r}\right)$, $k = 0, \ldots, r-1$. Supongamos que tras una medición se haya elegido $\mathbf{e}_{\ell_k} \otimes \mathbf{e}_{\varepsilon_{mj_0}}$, con $\ell_k = \texttt{EnteroMásPróximo}\left(\frac{k2^\kappa}{r}\right)$. Entonces, al dividir ese índice entre 2^κ se obtiene $\frac{\ell_k}{2^\kappa} \sim \frac{k}{r}$, y de aquí se quiere conocer r. Para esto hay que recordar la noción de *fracciones continuadas*.

Si $\frac{p}{q}$ es un número racional no-negativo, su *fracción continuada* es

$$\frac{p}{q} = a_0 + \frac{1}{a_1 + \frac{1}{\cdots + \frac{1}{a_v}}} = [a_0, a_1, \ldots, a_v] \tag{7.25}$$

donde $a_0, a_1, \ldots, a_v$ son enteros no-negativos. Para cada $w \leq v$, la fracción continuada $[a_0, a_1, \ldots, a_w]$ se dice ser el *w-ésimo convergente* de $\frac{p}{q}$, y, en efecto, cada convergente es una aproximación racional a $\frac{p}{q}$. El algoritmo para calcular fracciones continuadas es directo:

Entrada. $\frac{p}{q} \in \mathbb{Q}$.
Salida. $[a_0, a_1, \ldots, a_v]$: fracción continuada que representa a $\frac{p}{q} \in \mathbb{Q}$.
Procedimiento `FracciónContinuada`$(\frac{p}{q})$

1. Sean inicialmente $lst := []$ (la lista vacía) y $xact := \frac{p}{q}$.
2. Mientras el denominador de $xact$ sea mayor que 1 hágase
   a. sea $i :=$ `ParteEntera`$(xact)$;
   b. escríbase $\frac{p_1}{q_1} = xact$;
   c. actualícese $xact := \frac{q_1}{p_1 - iq_1}$;
   d. actualícese $lst := lst * [i]$.
3. Actualícese $lst := lst * [xact]$.
4. Dése como resultado lst.

Así pues, luego de haber realizado una medición y haber obtenido el valor $\frac{\ell_k}{2^\kappa} < 1$, se calcula su fracción continuada $[a_0, a_1, \ldots, a_v]$ ($a_0 = 0$) y los correspondientes convergentes $[c_0, c_1, \ldots, c_v]$ (también $c_0 = 0$), y entre éstos se selecciona a aquellos cuyos denominadores r_j sean menores que n, los cuales han de ser divisores del orden r de m.

En resumen, esta vez el algoritmo para localizar divisores de órdenes de elementos es el siguiente:

Entrada. $n \in \mathbb{N}$, $m \in \Phi(n)$.
Salida. r tal que $r | o(m)$.
Procedimiento `DivisorOrden`(n, m)

1. Sea $\nu := \lceil \log_2 n \rceil$, $\kappa = \lceil 2 \log_2 n \rceil$.
2. Defínase $V_m : \mathbb{H}_{\kappa+\nu} \to \mathbb{H}_{\kappa+\nu}$ como en la ec. (7.17).
3. Sea $\mathbf{s}_1 := (H^{\otimes\kappa} \otimes I^{\otimes\nu})(\mathbf{e_0} \otimes \mathbf{e_0})$.
4. Sea $\mathbf{s}_2 := V_m(\mathbf{s}_1)$.
5. Sea $\mathbf{s}_3 := \sum_{i=0}^{2^\kappa - 1} g(i) \mathbf{e}_{\varepsilon_i} \otimes \mathbf{e}_{\varepsilon_{m^{j_0}}}$ el estado equivalente a "tomar una medición" en $\mathbf{s}_2$. Entonces g queda determinada como en la ec. (7.23).
6. Sea $\mathbf{s}_4 :=$ `TIDF`$(2^\kappa, \mathbf{s}_3)$ la transformada inversa discreta de Fourier de $\mathbf{s}_3$.
7. Sea $\mathbf{e}_{\varepsilon_{\ell_k}} \otimes \mathbf{e}_{\varepsilon_{m^{j_0}}}$ una medición de $\mathbf{s}_4$.
8. Si $\ell_k == 0$ repítase desde el paso 3. En otro caso
   a. sea $[a_0, a_1, \ldots, a_v] :=$ `FracciónContinuada` $\left(\frac{\ell_k}{2^\kappa}\right)$;
   b. sea $[c_0, c_1, \ldots, c_v]$ la lista de convergentes; y
   c. dése como resultado la lista de denominadores, de los convergentes, que sean menores que n.

Habiendo obtenido divisores de órdenes, se puede proceder a obtener los órdenes de manera similar a como se bosquejó en el procedimiento `OrdenPotencia2`, mas en este caso hay que llevar un recuento de las varias posibilidades de divisores que arroja el procedimiento `DivisorOrden` descrito arriba.

7.8 Esfera de Bloch

7.8.1 Construcción geométrica

Se define la *esfera real* $S_{n-1}(\mathbb{R})$, como el conjunto:

$$S_{n-1}(\mathbb{R}) = \{(x_0,\ldots,x_{n-1}) \in \mathbb{R}^n \mid \sum_{i=0}^{n-1} |x_i|^2 = 1\},$$

cuando $n = 1$, $S_0(\mathbb{R})$ es el conjunto (disconexo) que consta de los dos puntos $-1,+1$, para $n = 2$, $S_1(\mathbb{R})$ es el círculo unitario en el espacio $\mathbb{R}^2$, cuando $n = 3$, $S_2(\mathbb{R})$ es la esfera unitaria en el espacio $\mathbb{R}^3$ y para $n = 4$, $S_3(\mathbb{R})$ es la *hiperesfera*, la cual es un subespacio topológico de $\mathbb{R}^4$.

Análogamente, se define la *esfera compleja* $S_{n-1}(\mathbb{C})$, como el conjunto:

$$S_{n-1}(\mathbb{C}) = \{(z_0,\ldots,z_{n-1}) \in \mathbb{C}^n \mid \sum_{i=0}^{n-1} |z_i|^2 = 1\},$$

para $n = 1$, $S_0(\mathbb{C})$ es el círculo unitario en el plano complejo $\mathbb{C} \cong \mathbb{R}^2$ y cuando $n = 2$,

$$S_1(\mathbb{C}) = \{(z_0,z_1) \in \mathbb{C}^2 \mid |z_0|^2 + |z_1|^2 = 1\},$$

es la esfera unitaria del espacio de Hilbert $\mathbb{H}_1 = \mathbb{C}^2$, vale escribir $S_1(\mathbb{C}) = S_{\mathbb{H}_1}$: la esfera de los qubits.

Las esferas $S_{n-1}(\mathbb{R})$ y $S_{n-1}(\mathbb{C})$ son variedades diferenciables con las topologías inducidas por los espacios reales y complejos $\mathbb{R}^n$ y $\mathbb{C}^n$ respectivamente.

$S_2(\mathbb{R})$ es la llamada *esfera de Bloch* y es la esfera unitaria en $\mathbb{R}^3$.

Naturalmente, existe una biyección entre las variedades $S_1(\mathbb{C})$ y $S_3(\mathbb{R})$,

$$I : S_1(\mathbb{C}) \to S_3(\mathbb{R}) \subset \mathbb{R}^4 \ , \ (z_0,z_1) \mapsto I(z_0,z_1) = (\mathfrak{Re}(z_0),\mathfrak{Im}(z_0),\mathfrak{Re}(z_1),\mathfrak{Im}(z_1)),$$

la cual es, de hecho, un homeomorfismo diferenciable.

Ahora, sea D el intervalo $[0,\pi] \times [0,2\pi] \subset \mathbb{R}^2$, consideremos,

$$J : D \to S_1(\mathbb{C}) \ \ , \ \ (\theta,\varphi) \mapsto J(\theta,\varphi) = \begin{bmatrix} \cos\frac{\theta}{2} \\ e^{i\varphi}\,\mathrm{sen}\,\frac{\theta}{2} \end{bmatrix}, \tag{7.26}$$

J no es inyectiva,

$$\forall \varphi \in [0,2\pi]: \;\; J(0,\varphi) = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \mathbf{e}_0 \in S_1(\mathbb{C}),$$
$$J(\pi,\varphi) = \begin{bmatrix} 0 \\ e^{i\varphi} \end{bmatrix} = e^{i\varphi}\mathbf{e}_1 \in S_1(\mathbb{C}),$$

donde $\{\mathbf{e}_0, \mathbf{e}_1\}$ es la base canónica de $\mathbb{C}^2$, y tampoco es suprayectiva, pues:

$$\begin{bmatrix} z_0 \\ z_1 \end{bmatrix} \in J(D) \iff z_0 \in \mathbb{R}. \tag{7.27}$$

Ahora, en el espacio real $\mathbb{R}^3$ de dimensión 3, denotemos por $\{\mathbf{f}_0, \mathbf{f}_1, \mathbf{f}_2\}$ a su base canónica, cuyos elementos son también puntos en la esfera de Bloch $S_2(\mathbb{R})$. De manera convencional,

- $\mathbf{f}_2$ es el *polo norte*,
- $-\mathbf{f}_2$ es el *polo sur*, y
- $[\mathbf{f}_0, \mathbf{f}_1, -\mathbf{f}_0, -\mathbf{f}_1]$ es una trayectoria antihoraria sobre el *ecuador*.

Sea $K : D \to S_2(\mathbb{R})$, la función

$$K : (\theta,\varphi) \mapsto K(\theta,\varphi) = \begin{bmatrix} \operatorname{sen}\theta\cos\varphi \\ \operatorname{sen}\theta\operatorname{sen}\varphi \\ \cos\theta \end{bmatrix}. \tag{7.28}$$

Para cada $(\theta,\varphi) \in D$, $K(\theta,\varphi)$ es el correspondiente *vector de Bloch*. En la Figura 7.1 mostramos el vector de Bloch correspondiente a una pareja de ángulos. Se tiene

$$\begin{aligned} \forall \varphi \in [0,2\pi]: \;\; K(0,\varphi) &= \mathbf{f}_2: \;\; \text{polo norte} \\ K(\pi,\varphi) &= -\mathbf{f}_2: \;\; \text{polo sur} \end{aligned}$$

Para cada $\theta \in [0,\pi]$, sea $V_\theta = \{\theta\} \times [0,2\pi] \subset D$ la *recta vertical* de abscisa θ en D. Entonces al escribir $u = \operatorname{sen}\theta$ y $v = \cos\theta$,

$$K(V_\theta) = \left\{ \begin{bmatrix} u\cos\varphi \\ u\operatorname{sen}\varphi \\ v \end{bmatrix} \mid 0 \le \varphi \le 2\pi \right\}$$

es el *paralelo de latitud* $\frac{\pi}{2} - \theta$, el cual es un círculo inscrito en la esfera de Bloch, de radio $|u|$, paralelo al ecuador. Por tanto, para $\theta \in \{0,\pi\}$, ese paralelo se colapsa en el polo correspondiente, en tanto que $K(V_{\frac{\pi}{2}})$ es el ecuador.

Para cada $\varphi \in [0,2\pi]$, sea $H_\varphi = [0,\pi] \times \{\varphi\} \subset D$ la *recta horizontal* de ordenada φ en D. La imagen de cada recta horizontal H_φ bajo K es el *meridiano de longitud* φ, recorrido de norte a sur al variar θ de 0 a π. Entonces al escribir $u = \operatorname{sen}\varphi$ y $v = \cos\varphi$,

$$K(H_\varphi) = \left\{ \begin{bmatrix} v\operatorname{sen}\theta \\ u\operatorname{sen}\theta \\ \cos\theta \end{bmatrix} \mid 0 \le \theta \le \pi \right\}.$$

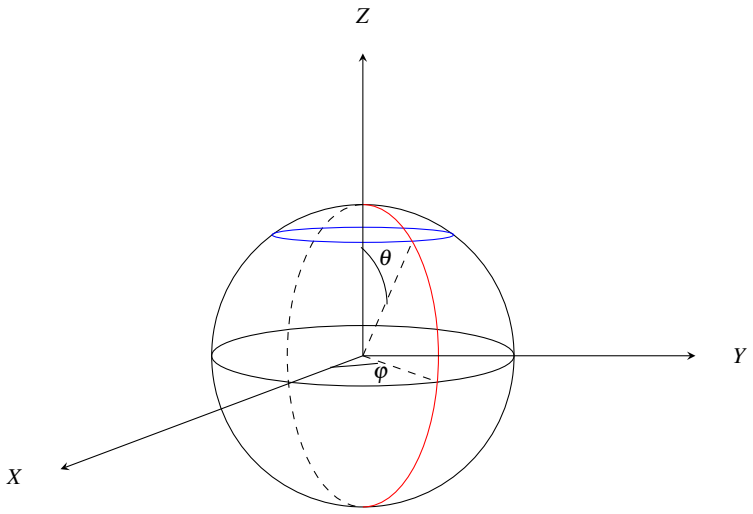


Figura 7.1 Ilustración de la función $K : D \to S_2(\mathbb{R})$. Dada una pareja de ángulos $(\theta, \varphi) \in D$, se muestra el vector de Bloch correspondiente.

En particular,

$$K(H_0) = \left\{ \begin{bmatrix} \operatorname{sen}\theta \\ 0 \\ \cos\theta \end{bmatrix} \mid 0 \leq \theta \leq \pi \right\} : \text{meridiano en el plano } Y = 0,$$

$$K(H_{\frac{\pi}{2}}) = \left\{ \begin{bmatrix} 0 \\ \operatorname{sen}\theta \\ \cos\theta \end{bmatrix} \mid 0 \leq \theta \leq \pi \right\} : \text{meridiano en el plano } X = 0.$$

De aquí se sigue

$$K(\tfrac{\pi}{2},0) = \mathbf{f}_0 \qquad K(\tfrac{\pi}{2},\pi) = -\mathbf{f}_0$$
$$K(\tfrac{\pi}{2},\tfrac{\pi}{2}) = \mathbf{f}_1 \; K(\tfrac{\pi}{2},\tfrac{\pi}{2}+\pi) = -\mathbf{f}_1$$

Observamos también, de manera general, que para cada $\varphi \in [0,\pi]$, los meridianos $K(H_\varphi)$ y $K(H_{\pi+\varphi})$ son *complementarios* en el sentido de que juntos forman una geodésica que pasa por los polos.

De manera similar, podríamos describir la acción geométrica de la aplicación $J : D \to S_1(\mathbb{C})$ definida por (7.26). Consideremos, más bien $I \circ J : D \to S_3(\mathbb{R})$, o sea, identifiquemos $S_1(\mathbb{C})$ con $S_3(\mathbb{R}) \subset \mathbb{R}^4$ mediante la biyección I.

$\mathbb{R}^4 = \mathbb{R}^2 \times \mathbb{R}^2$ es el producto cartesiano de dos planos euclidianos. De hecho, si nombramos a los rayos generados por los vectores canónicos en $\mathbb{R}^4$ como *eje X, eje Y, eje Z* y *eje W* respectivamente, entonces el espacio real de dimensión 4, $\mathbb{R}^4$, es el producto de los planos *X*-*Y* y *Z*-*W*. Así, una *curva*

$$\gamma = (\gamma_X, \gamma_Y, \gamma_Z, \gamma_W) : [a,b] \to \mathbb{R}^4,$$

vale decir, una función continua de un intervalo $[a,b]$ con $a,b \in \mathbb{R}$, $a \leq b$, en $\mathbb{R}^4$, determina dos *trazas*

$$\gamma_0 = (\gamma_X, \gamma_Y)\ ,\ \gamma_1 = (\gamma_Y, \gamma_Z) : [a,b] \to \mathbb{R}^2.$$

Pues bien, para cada $\theta \in [0,\pi]$, la transformación $I \circ J$ restringida a la recta vertical V_θ determina una curva

$$\gamma^\theta : [0,2\pi] \to S_3(\mathbb{R})\ ,\ \varphi \mapsto \gamma^\theta(\varphi) = (u, 0, v\cos\varphi, v\,\mathrm{sen}\,\varphi),$$

con $u = \cos\frac{\theta}{2}$ y $v = \mathrm{sen}\,\frac{\theta}{2}$. Por tanto, su primera traza γ_0^θ es constante y se restringe al punto $(u,0)$, en tanto que la segunda, γ_1^θ, es el círculo centrado en el origen, de radio $|v|$, en el plano Z-W. La imagen de V_θ bajo J es pues un círculo (o, si se quiere, el producto de un punto por un círculo).

Análogamente, para cada $\varphi \in [0,2\pi]$, la transformación $I \circ J$ restringida a la recta horizontal H_φ determina una curva

$$\gamma_{(\varphi)} : [0,\pi] \to S_3(\mathbb{R})\ ,\ \theta \mapsto \gamma_{(\varphi)}\theta = (\cos\frac{\theta}{2}, 0, u\cos\frac{\theta}{2}, v\,\mathrm{sen}\,\frac{\theta}{2}),$$

con $u = \cos\varphi$ y $v = \mathrm{sen}\,\varphi$. Por tanto, su primera traza $\gamma_{(\varphi)_0}$ es una línea recta, en el eje X del plano X-Y, que va del origen $(0,0)$ al punto $(1,0)$, en tanto que la segunda, $\gamma_{(\varphi)_1}$, es (la cuarta parte de) la elipse centrada en el origen, de semiejes $|u|$, $|v|$, en el plano Z-W. La imagen de H_φ bajo J es pues una curva en el producto de un segmento por una elipse (o, si se quiere, en un cilindro de base elíptica).

Ahora bien, definamos una función $B : S_2(\mathbb{R}) \to S_1(\mathbb{C})$ mediante la relación siguiente:

$$B(\mathbf{x}) = \mathbf{z} \iff \exists(\theta,\varphi) \in D :\ K(\theta,\varphi) = \mathbf{x}\ \&\ J(\theta,\varphi) = \mathbf{z} \tag{7.29}$$

B queda bien definido y hace conmutativo el diagrama siguiente:

$$\begin{array}{ccccc} D & & & & \\ & \searrow^{J} & & & \\ \downarrow{\scriptstyle K} & & S_1(\mathbb{C}) & \xrightarrow{\ I\ } & S_3(\mathbb{R}) \\ & \nearrow_{B} & & & \\ S_2(\mathbb{R}) & & & & \end{array} \tag{7.30}$$

La aplicación B se llama *función de Bloch*. De la relación (7.29) se tiene que la imagen de B es

$$B(S_2(\mathbb{R})) = J(D) \subsetneq S_1(\mathbb{C})$$

y está caracterizada por la relación (7.27). De las relaciones (7.26) y (7.28) se tiene

$$B(\mathbf{f}_0) = \frac{1}{\sqrt{2}}(\mathbf{e}_0 + \mathbf{e}_1) \ , \ B(-\mathbf{f}_0) = \frac{1}{\sqrt{2}}(-\mathbf{e}_0 + \mathbf{e}_1) \tag{7.31}$$

$$B(\mathbf{f}_1) = \frac{1}{\sqrt{2}}(\mathbf{e}_0 + i\mathbf{e}_1) \ , \ B(-\mathbf{f}_1) = \frac{1}{\sqrt{2}}(-\mathbf{e}_0 + i\mathbf{e}_1) \tag{7.32}$$

$$B(\mathbf{f}_2) = \mathbf{e}_0 \ , \ B(-\mathbf{f}_2) = \mathbf{e}_1 \tag{7.33}$$

donde $i = \sqrt{-1}$. Se ve pues, de las relaciones (7.31)-(7.33), que parejas de puntos antipodales en $S_2(\mathbb{R})$ se aplican en parejas de vectores ortogonales en $S_1(\mathbb{C})$, por lo tanto, B no es una función conforme: no preserva ni ángulos ni distancias.

La esfera y la aplicación de Bloch, $(S_2(\mathbb{R}), B)$, proporcionan una visión geométrica del subconjunto de qubits $B(S_2(\mathbb{R})) \subsetneq S_1(\mathbb{C})$. La imagen de la función de Bloch es, de acuerdo con (7.27):

$$B(S_2(\mathbb{R}) = \{z_0\mathbf{e}_0 + z_1\mathbf{e}_1 \in S_1(\mathbb{C}) |\ z_0 \in \mathbb{R}\},$$

el cual es un subconjunto propio de $S_1(\mathbb{C})$. Se tiene que $I(B(S_2(\mathbb{R}))$ es la traza de la esfera unitaria $S_3(\mathbb{R})$ con el hiperplano $Y = 0$ en $\mathbb{R}^4$.

Sea $c = e^{i\gamma} \in S_0(\mathbb{C})$ un número complejo unitario, y sea $\mathbf{z} = J(\theta, \varphi) \in S_1(\mathbb{C})$, con $(\theta, \varphi) \in D$. Al mutiplicar $\mathbf{z}$ por el escalar c se tiene

$$c\,\mathbf{z} = \begin{bmatrix} e^{i\gamma}\cos\frac{\theta}{2} \\ e^{i(\gamma+\varphi)}\,\text{sen}\,\frac{\theta}{2} \end{bmatrix},$$

entonces

$$I(c\,\mathbf{z}) = \begin{bmatrix} \cos\gamma\cos\frac{\theta}{2} \\ \text{sen}\,\gamma\cos\frac{\theta}{2} \\ \cos(\gamma+\varphi)\,\text{sen}\,\frac{\theta}{2} \\ \text{sen}\,(\gamma+\varphi)\,\text{sen}\,\frac{\theta}{2} \end{bmatrix} \in S_3(\mathbb{R}).$$

De esta manera, la transformación

$$N : D \times [0, 2\pi] \to S_1(\mathbb{C}) \ , \ (\theta, \varphi, \gamma) \mapsto N(\theta, \varphi, \gamma) = e^{i\gamma} J(\theta, \varphi),$$

es suprayectiva, es decir, N es una parametrización de la esfera de los qubits, $S_1(\mathbb{C})$, con el conjunto $D \times [0, 2\pi]$.

Sean $\mathbf{x} \in S_2(\mathbb{R})$ y $\mathbf{z} \in S_1(\mathbb{C})$ tales que $B(\mathbf{x}) = \mathbf{z}$. Entonces, $\mathbf{x}$ *representa* al qubit $\mathbf{z}$, el cual es un estado puro, con matriz de densidad $\pi_{\mathbf{z}} = \mathbf{z}\mathbf{z}^H$. Mediante la inclusión B, cada punto en la esfera de Bloch *es* pues un estado puro.

Un estado mixto ρ (véase la sección 3.3) es una combinación convexa de matrices de densidad, es decir, de estados puros. Dada una sucesión de estados puros, la colección de combinaciones convexas de ellos es el poliedro que tiene como vértices a esos estados puros. Naturalmente, un poliedro cuyos vértices están en la esfera de Bloch está incluido en el interior de la esfera. Por lo tanto, se conviene en que:

- los puntos sobre la esfera de Bloch representan estados puros, y

- los puntos en el interior de la esfera de Bloch, al cual llamamos la *bola de Bloch*, representan estados mixtos.

Otra manera de representar a los estados mixtos es la siguiente:

Sea $\mathbf{z} \in S_1(\mathbb{C})$ tal que existe $(\theta,\varphi) \in D$ de manera que $\mathbf{z} = J(\theta,\varphi)$. Entonces su matriz de densidad es

$$\begin{aligned}\rho_{\mathbf{z}} &= \mathbf{z}\mathbf{z}^H \\ &= \frac{1}{2}\begin{bmatrix} 1+\cos\theta & e^{i\varphi}\operatorname{sen}\theta \\ e^{i\varphi}\operatorname{sen}\theta & 1-\cos\theta \end{bmatrix} \\ &= \frac{1}{2}(\sigma_0 + x\sigma_1 + y\sigma_2 + z\sigma_3), \end{aligned} \tag{7.34}$$

donde $(x,y,z) = K(\theta,\varphi)$ son las coordenadas del vector de Bloch correspondiente a la pareja (θ,φ) y $\sigma_0,\sigma_1,\sigma_2,\sigma_3$ son los *operadores de Pauli* definidos en la relación (7.5).

Los estados mixtos serán entonces combinaciones convexas de expresiones de la forma (7.34). De hecho, la expresión (7.34) caracteriza a los estados puros:

Observación 7.8.1 *Un estado $\rho \in \mathbb{C}^{2\times 2}$ es puro si y sólo si existe $\mathbf{x} \in S_2(\mathbb{R})$ tal que*

$$\rho = \frac{1}{2}(\sigma_0 + x\sigma_1 + y\sigma_2 + z\sigma_3).$$

Puede verse que si $\mathbf{x}_0 = K(\theta_0,\varphi_0)$ y $\mathbf{x}_1 = K(\theta_1,\varphi_1)$ son dos vectores de Bloch de los respectivos estados puros $\mathbf{z}_0 = J(\theta_0,\varphi_0)$ y $\mathbf{z}_1 = J(\theta_1,\varphi_1)$, cuyas matrices de densidad son ρ_0 y ρ_1, entonces:

$$\operatorname{Tr}(\rho_1\rho_2) = \frac{1}{2}(1 + \langle \mathbf{x}_0 | \mathbf{x}_1 \rangle). \tag{7.35}$$

En efecto, se tiene

- $\forall i \in \{0,1,2,3\}:\ \sigma_i^2 = \sigma_0$,
- $\forall i,j \in \{1,2,3\}:\ [i \neq j \implies \sigma_i\sigma_j = \sigma_k \text{ con } \{i,j,k\} = \{1,2,3\}]$,
- $\operatorname{Tr}(\sigma_0) = 1$ & $\forall i \in \{1,2,3\}:\ \operatorname{Tr}(\sigma_i) = 0$.

Si, de acuerdo con (7.34),

$$\begin{aligned}\rho_0 &= \frac{1}{2}(\sigma_0 + x_0\sigma_1 + y_0\sigma_2 + z_0\sigma_3) \\ \rho_1 &= \frac{1}{2}(\sigma_0 + x_1\sigma_1 + y_1\sigma_2 + z_1\sigma_3)\end{aligned}$$

al realizar el producto y tomar en cuenta las relaciones anteriores, así como el hecho de que el operador "traza" es lineal, resulta (7.35).

7.8.2 Producto por complejos unitarios

Utilizaremos la notación introducida en la sección 7.8.1 anterior.

Al definir la operación producto en $S_1(\mathbb{C})$, $\star : S_1(\mathbb{C}) \times S_1(\mathbb{C}) \to S_1(\mathbb{C})$, como

$$(\mathbf{z}, \mathbf{w}) = (\begin{bmatrix} z_0 \\ z_1 \end{bmatrix}, \begin{bmatrix} w_0 \\ w_1 \end{bmatrix}) \mapsto \mathbf{z} \star \mathbf{w} = (\begin{bmatrix} z_0\, w_0 - z_1\, w_1 \\ z_1\, w_0 + z_0\, w_1 \end{bmatrix}$$

se tiene que

$$\left(S_1(\mathbb{C}), \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \star \right)$$

es un grupo. Así pues, la colección de qubits adquiere una estructura de grupo.

Para un número complejo unitario $c = e^{i\gamma} = \cos\gamma + i \operatorname{sen}\gamma \in S_0(\mathbb{C})$ definamos

$$L(c) = (\cos\gamma)\, \mathbf{e}_0 + (\operatorname{sen}\gamma)\, \mathbf{e}_1 \in S_1(\mathbb{C}) \subset \mathbb{C}^2.$$

Entonces $L : S_0(\mathbb{C}) \to S_1(\mathbb{C})$ es propiamente una inclusión del círculo (real) $S_0(\mathbb{C}) \cong S_1(\mathbb{R})$ en el círculo (complejo) $S_1(\mathbb{C})$.

Sea $\mathbf{z} = J(\theta, \varphi) \in S_1(\mathbb{C})$ un qubit, o sea, un estado puro, con $(\theta, \varphi) \in D$. Entonces, se ha de tener

$$L(c) \star \mathbf{z} = \begin{bmatrix} \cos\gamma \cos\frac{\theta}{2} - e^{i\varphi} \operatorname{sen}\gamma \operatorname{sen}\frac{\theta}{2} \\ \operatorname{sen}\gamma \cos\frac{\theta}{2} + e^{i\varphi} \cos\gamma \operatorname{sen}\frac{\theta}{2} \end{bmatrix}, \tag{7.36}$$

Definamos ahora

$$M(c) = \begin{bmatrix} \cos\gamma & -\operatorname{sen}\gamma \\ \operatorname{sen}\gamma & \cos\gamma \end{bmatrix} \in U(2).$$

Entonces $M : S_0(\mathbb{C}) \to U(2)$ es una inclusión del círculo (real) $S_0(\mathbb{C}) \cong S_1(\mathbb{R})$ en el grupo de simetría $U(2)$. Naturalmente, $\mu : U(2) \times S_1(\mathbb{C}) \to S_1(\mathbb{C})$, $(A, \mathbf{z}) \mapsto \mu(A, \mathbf{z}) = A\mathbf{z}$, es una acción del grupo $U(2)$ sobre el círculo (complejo) $S_1(\mathbb{C})$. Pues bien, se tiene

$$\mu(M(c), \mathbf{z}) = L(c) \star \mathbf{z}.$$

Así pues, el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} S_0(\mathbb{C}) \times S_1(\mathbb{C}) & \xrightarrow{(L, Id_2)} & S_1(\mathbb{C}) \times S_1(\mathbb{C}) \\ \Big\downarrow{\scriptstyle (M, Id_2)} & & \Big\downarrow{\scriptstyle \star} \\ U(2) \times S_1(\mathbb{C}) & \xrightarrow[\mu]{} & S_1(\mathbb{C}) \end{array} \tag{7.37}$$

Puesto de manera muy sintética, se podría decir que "$S_1(\mathbb{C})$ como grupo es una extensión de la acción de $U(2)$ sobre él".

7.8.3 Enfoque mediante cuaterniones

Los cuaterniones $\mathbf{H}$, véase la observación 6.3.3, también tienen una representación, llamada, *forma polar*, en donde, para cualquier cuaternión $\mathbf{q} = q_0 + q_1 i + q_2 j + q_3 k$, con $q_m \in \mathbb{R}$, para $m = 0,1,2,3$, siendo i, j, k los generadores de $\mathbf{H}$, se tiene

$$\mathbf{q} = q(\cos\alpha + \mathbf{u}\,\mathrm{sen}\,\alpha), \tag{7.38}$$

donde

$$\begin{aligned} q = |\mathbf{q}|^2 &= \sqrt{q_0^2 + q_1^2 + q_2^2 + q_3^2}, \\ \mathbf{u} &= \pm\frac{1}{\sqrt{q_1^2 + q_2^2 + q_3^2}}(q_1 i + q_2 j + q_3 k) \quad \text{es un cuaternión unitario,} \\ \cos\alpha &= \frac{q_0}{q}, \\ \mathrm{sen}\,\alpha &= \pm\frac{1}{q}\sqrt{q_1^2 + q_2^2 + q_3^2}. \end{aligned}$$

En el caso en que $q = 1$, se tiene un cuaternión unitario, al conjunto de éstos se denotará por $S_{\mathbf{H}}$. Los elementos en $S_{\mathbf{H}}$ están en correspondencia biyectiva con los puntos de la esfera unitaria $S_3(\mathbb{R})$ mediante la identificación natural

$$P : S_{\mathbf{H}} \to S_3(\mathbb{R}) \ , \ q_0 + q_1 i + q_2 j + q_3 k \mapsto (q_0, q_1, q_2, q_3)$$

y, en consecuencia

$$S_{\mathbf{H}} \cong S_3(\mathbb{R}) \cong S_1(\mathbb{C}).$$

Es bien sabido y puede verificarse directamente que la aplicación $R : \mathbf{H} \to \mathrm{GL}(3,\mathbb{R})$ tal que

$$\mathbf{q} = q_0 + q_1 i + q_2 j + q_3 k \mapsto R(\mathbf{q}) = \begin{bmatrix} 1 - 2q_2^2 - 2q_3^2 & 2(q_1 q_2 - q_3 q_0) & 2(q_1 q_3 + q_2 q_0) \\ 2(q_1 q_2 + q_3 q_0) & 1 - 2q_1^2 - 2q_3^2 & 2(q_2 q_3 - q_1 q_0) \\ 2(q_1 q_3 - q_2 q_0) & 2(q_1 q_3 + q_1 q_0) & 1 - 2q_1^2 - 2q_2^2 \end{bmatrix},$$

es un homomorfismo entre la estructura multiplicativa de $\mathbf{H}$ y la canónica de $\mathrm{GL}(3,\mathbb{R})$ (a saber, la multiplicación de matrices). En particular, su restricción a la esfera $S_{\mathbf{H}}$ es un homomorfismo $R : S_{\mathbf{H}} \to \mathrm{SO}(3,\mathbb{R})$. Se tiene que,

$$\forall \mathbf{q} \in S_{\mathbf{H}} : \ R(\mathbf{q}) = R(-\mathbf{q}),$$

por lo que se dice que R proporciona un *recubrimiento dos-a-uno* (o *doble recubrimiento*) de $\mathrm{SO}(3,\mathbb{R})$ con $S_{\mathbf{H}}$.

También se tiene de la sucesión exacta (5.1), que $\mathrm{SU}(2)$ es un doble recubrimiento de $\mathrm{SO}(3,\mathbb{R})$.

Ahora bien, recordamos que un cuaternión $\mathbf{q} = q_0 + q_1 i + q_2 j + q_3 k$ se dice ser *real* si $q_1 = q_2 = q_3 = 0$, y *puro* si $q_0 = 0$. Sea

$$T_{\mathbf{H}} = \{q_0 + q_1 i + q_2 j + q_3 k \in S_{\mathbf{H}} |\ q_0 = 0\}$$

la colección de cuaterniones unitarios puros.

Para un tal cuaternión $\mathbf{q} = q_1 i + q_2 j + q_3 k \in T_{\mathbf{H}}$, éste está en su forma polar, según la relación (7.38), con $\alpha \in \left\{\frac{\pi}{2}, \frac{3\pi}{2}\right\}$.

Mediante la aplicación

$$Q : S_2(\mathbb{R}) \to T_{\mathbf{H}}\ ,\ (x,y,z) \mapsto Q(x,y,z) = x\,i + y\,j + z\,k$$

la esfera de Bloch $S_2(\mathbb{R})$ se identifica con la colección de cuaterniones puros unitarios $T_{\mathbf{H}}$. Se tiene entonces el siguiente diagrama conmutativo:

$$\begin{array}{ccccc} S_2(\mathbb{R}) & & \xrightarrow{\quad B \quad} & & S_1(\mathbb{C}) \\ \Big\downarrow{\scriptstyle Q} & & & & \Big\downarrow{\scriptstyle I} \\ T_{\mathbf{H}} & \xrightarrow[Id_{\mathbf{H}}]{} & S_{\mathbf{H}} & \xrightarrow[P]{} & S_3(\mathbb{R}) \end{array} \tag{7.39}$$

donde aparecen operadores definidos en el diagrama (7.30).

7.9 Observables e incertidumbre

Sea $\mathbb{H}$ un espacio de Hilbert sobre $\mathbb{C}$ y sea $S_{\mathbb{H}}$ su esfera unitaria. Una función lineal $U : \mathbb{H} \to \mathbb{H}$ es *auto-adjunta* si $\forall \mathbf{x}, \mathbf{y} \in \mathbb{H}\ \ \langle \mathbf{x} | U\mathbf{y} \rangle = \langle U\mathbf{x} | \mathbf{y} \rangle$, o equivalentemente, si está representada por una matriz hermitiana: $U^H = U$. Una transformación auto-adjunta se dice ser también un *observable*.

Si $U, V : \mathbb{H} \to \mathbb{H}$ son observables, $U + V$ es también un observable, pero el producto UV lo es sólo si U y V conmutan. Sin embargo, $UV + VU$ y $i(UV - VU)$ siempre son observables.

Para un observable $U : \mathbb{H} \to \mathbb{H}$ existe una base ortonormal de $\mathbb{H}$ que consiste de eigenvectores de U. Por tanto, si $\lambda_0, \ldots, \lambda_{k-1}$ son los eigenvalores de U y $L_0, \ldots, L_k$ son los correspondientes eigenespacios rige la implicación siguiente:

$$\mathbf{x} \in L_\kappa \implies U(\mathbf{x}) = \lambda_\kappa \mathbf{x}.$$

Consecuentemente, U está representada como

$$U = \sum_{\kappa=0}^{k-1} \lambda_\kappa \pi_{L_\kappa},$$

donde para cada espacio $L < \mathbb{H}$, $\pi_L : \mathbb{H} \to L$ es la *proyección ortogonal* sobre L. Si $\{\mathbf{v}_0, \ldots, \mathbf{v}_{m-1}\}$ es una base ortonormal de L y $\mathbf{L}$ es la matriz cuyas columnas son estos vectores entonces π_L queda representada por $\mathbf{L} \cdot \mathbf{L}^H$. Ya que π_{L_κ} es una proyección ortogonal, para cada $\mathbf{x} \in \mathbb{H}$, $\langle \mathbf{x} - \pi_{L_\kappa}(\mathbf{x}) | \pi_{L_\kappa}(\mathbf{x}) \rangle = 0$, por lo que

$$\langle \mathbf{x} | \pi_{L_\kappa}(\mathbf{x}) \rangle = \langle \pi_{L_\kappa}(\mathbf{x}) | \pi_{L_\kappa}(\mathbf{x}) \rangle = \| \pi_{L_\kappa}(\mathbf{x}) \|^2.$$

Principio extendido de medición. Para cualquier observable U, al *medir* un n-registro $\mathbf{x} \in \mathbb{H}$, la *respuesta* es un eigenvalor λ_κ y el estado actual será la proyección normalizada $\frac{\pi_{L_\kappa}(\mathbf{x})}{\|\pi_{L_\kappa}(\mathbf{x})\|}$. Para cada eigenvalor λ_κ, la probabilidad de que sea la respuesta es

$$\Pr(\lambda_\kappa) = \langle \mathbf{x} | \pi_{L_\kappa}(\mathbf{x}) \rangle . \tag{7.40}$$

Evidentemente, $\sum_{\kappa=0}^{k-1} \Pr(\lambda_\kappa) = \sum_{\kappa=0}^{k-1} \|\pi_{L_\kappa}(\mathbf{x})\|^2 = \|\mathbf{x}\|^2 = 1$.

Para cualquier observable U, sea $(\mathbf{v}_j)_j$ una base ortonormal de $\mathbb{H}$ que consista de eigenvectores de U y sea λ_j el correspondiente eigenvalor $\mathbf{v}_j$. Entonces cualquier vector unitario $\mathbf{z} \in S_{\mathbb{H}}$ puede ser escrito como $\mathbf{z} = \sum_i a_i \mathbf{v}_i$, donde $\sum_i |a_i|^2 = 1$. Y

$$\begin{aligned} \langle \mathbf{z} | U\mathbf{z} \rangle &= \left\langle \sum_i a_i \mathbf{v}_i | U \left(\sum_j a_j \mathbf{v}_j \right) \right\rangle \\ &= \left\langle \sum_i a_i \mathbf{v}_i | \sum_j a_j \lambda_j \mathbf{v}_j \right\rangle \\ &= \sum_i \lambda_i |a_i|^2 = E(\lambda_i) \end{aligned}$$

Por tanto, $\langle \mathbf{z} | U\mathbf{z} \rangle$ es el *valor observado esperado* del registro cuántico $\mathbf{z}$ bajo el observable U.

La *desviación estándar* de U es el operador

$$\triangle U : \mathbb{H} \to \mathbb{R} \ , \ \mathbf{x} \mapsto \triangle U(\mathbf{x}) = \sqrt{\langle U^2 \mathbf{x} | \mathbf{x} \rangle - \langle U\mathbf{x} | \mathbf{x} \rangle^2}.$$

Sean $U_1, U_2 : \mathbb{H} \to \mathbb{H}$ dos observables. Entonces $\forall \mathbf{x} \in \mathbb{H}$:

$$\langle U_2 \circ U_1 \mathbf{x} | \mathbf{x} \rangle \langle \mathbf{x} | U_2 \circ U_1 \mathbf{x} \rangle = |\langle U_1 \mathbf{x} | U_2 \mathbf{x} \rangle|^2 = \langle U_1 \circ U_2 \mathbf{x} | \mathbf{x} \rangle \langle \mathbf{x} | U_1 \circ U_2 \mathbf{x} \rangle,$$

y, de la desigualdad de Schwartz, $|\langle U_1 \mathbf{x} | U_2 \mathbf{x} \rangle|^2 \leq \|U_1 \mathbf{x}\|^2 \|U_2 \mathbf{x}\|^2$, por lo que valen

Desigualdad de Robertson-Schrödinger.

$$\frac{1}{4} |\langle (U_1 \circ U_2 - U_2 \circ U_1) \mathbf{x} | \mathbf{x} \rangle|^2 \leq \|U_1 \mathbf{x}\|^2 \|U_2 \mathbf{x}\|^2. \tag{7.41}$$

El *conmutador* de los dos observables es $[U_1, U_2] = U_1 \circ U_2 - U_2 \circ U_1$.

Los observables U_1, U_2 son *compatibles* si $[U_1, U_2] = 0$, es decir si ellos conmutan: $U_1 \circ U_2 = U_2 \circ U_1$.

Principio de Incertidumbre de Heisenberg. Para cualesquiera dos observables U_1, U_2 y cualquier vector unitario $\mathbf{z} \in S_{\mathbb{H}}$,

$$|\triangle U_1(\mathbf{z})|^2 |\triangle U_2(\mathbf{z})|^2 \geq \frac{1}{4} |\langle \mathbf{z}| [U_1, U_2] \mathbf{z}\rangle|^2 . \tag{7.42}$$

Así, si los observables son incompatibles, toda vez que U_1 sea medido con una mayor precisión, U_2 será medido con menor precisión, y recíprocamente.

7.10 C^*-algebra de observables

Para cualquier *sistema cuántico* Σ, que consista propiamente de una colección de observables definidos sobre un espacio complejo de Hilbert $\mathbb{H}$ de dimensión finita, sea $\mathbb{A}_\Sigma = \mathscr{L}(\Sigma)$ la C^*-algebra generada por Σ. Un funcional lineal $f : \mathbb{A}_\Sigma \to \mathbb{C}$ es *positivo* si

$$\forall U \in \mathbb{A}_\Sigma : \ \langle f | U^* U \rangle \geq 0.$$

La transformación identidad $\mathbf{1}$ es una unidad en la C^*-algebra $\mathbb{A}_\Sigma$. Se tiene que *cada funcional lineal positivo* $f : \mathbb{A}_\Sigma \to \mathbb{C}$ *posee norma* $\|f\| = \langle f | \mathbf{1} \rangle$. Un *estado* sobre $\mathbb{A}_\Sigma$ es un funcional lineal positivo *normalizado*. El conjunto de estados es convexo

$$f_0, f_1 \text{ estados} \implies \forall t \in [0,1] : \ (1-t) f_0 + t f_1 \text{ estado.}$$

Cada punto $\mathbf{x}$ en la esfera unitaria $S_{\mathbb{H}}$ puede ser identificado como un estado

$$\mathbf{x} : U \mapsto \langle \mathbf{x} | U \mathbf{x} \rangle \ : \text{el valor esperado de } \mathbf{x} \text{ bajo } U .$$

Recordamos el Teorema de Banach-Alaoglu: *En la topología-débil***, la bola unitaria es compacta*. Por tanto, se tiene que el conjunto de estados es compacto en la topología-débil*.

Para cualquier observable $U \in \mathbb{A}_\Sigma$, el valor $E_z(U) = \langle z | U \rangle$ es el *valor esperado de* U en el estado $z \in \mathbb{A}_\Sigma^*$. El *espectro* de U es $\Lambda(U) = \{\lambda \in \mathbb{C} | U - \mathbf{1}$ no es invertible en $\mathbb{A}_\Sigma\}$. La *incertidumbre* es la variancia de U en z:

$$\mathrm{Var}_z(U) = E_z \left(U - E_z(U)\mathbf{1}\right)^2 = E_z\left(U^2\right) - E_z(U)^2 \geq 0.$$

El *Principio de Incertidumbre de Heisenberg* reza en este contexto:

$$\mathrm{Var}_z(A)\mathrm{Var}_z(B) \geq \frac{1}{2} |AB - BA| .$$

7.11 Lógica cuántica

Un *proposición* es cualquier observable con eigenvalores $0,1$, es decir, sus mediciones sólo dan respuestas "sí" o "no". Cada proposición es pues un operador auto-adjunto idempotente, $A^2 = A$. Las proposiciones son proyecciones, y por tanto cada proposición corresponde a un subespacio en el espacio de Hilbert $\mathbb{H}$.

El valor "tautológico" 1 corresponde a todo el espacio $\mathbb{H}$, el valor "inconsistente" al espacio nulo $\{\mathbf{0}\}$, la "conjunción" a intersección, la "disyunción" a la "suma directa" o "unión lineal", y la "negación" a la complementariedad ortogonal.

Si $A_1, A_2 \in \mathbb{A}_\Sigma$ son proposiciones entonces

$$\begin{aligned} \neg A_1 &= \mathbf{1} - A \\ A_1 \wedge A_2 &= \lim_{n\to+\infty} (A_1 A_2)^n \\ A_1 \vee A_2 &= \neg(\neg A_1 \wedge \neg A_2) = \mathbf{1} - \lim_{n\to+\infty} ((\mathbf{1}-A_1)(\mathbf{1}-A_2))^n \end{aligned}$$

El *Teorema Espectral* (*todo operador auto-adjunto puede ser expresado como la suma directa de sus eigenespacios*) entraña que *todo observable es la unión lineal de proposiciones que son compatibles a pares y compatibles con el observable dado*.

7.12 Teorema de Gleason

Sea $\mathbb{H}$ un espacio de Hilbert, sobre cualquiera de los campos real, complejo o de los cuaterniones, ya sea de dimensión finita o de dimensión infinita, y sea

$$\mathscr{V}(\mathbb{H}) = \{L < \mathbb{H} | \, L \text{ es un espacio lineal cerrado en } \mathbb{H}\},$$

donde la noción de "cerrado" se refiere al sentido topológico (en consecuencia, en dimensión finita es redundante). $\mathscr{V}(\mathbb{H})$ es de hecho un *retículo ortomodular completo* (*complete orthomodular lattice*).

Si $\{L_k\}_{k\in K} \subset \mathscr{V}(\mathbb{H})$ es una colección de subespacios, $\bigoplus_{k\in K} L_\kappa$ es su supremo. Si $\{\mathbf{v}_\iota\}_{\iota\in I} \subset \mathbb{H}$ son vectores, $\mathscr{L}\{\mathbf{v}_\iota\}_{\iota\in I} \in \mathscr{V}(\mathbb{H})$ es el espacio lineal generado por ellos.

Una *medida* es una aplicación $m : \mathscr{V}(\mathbb{H}) \to \mathbb{R}$ tal que

$$m(\mathbb{H}) = 1$$

$$\{L_k\}_{k\in K} \text{ ortogonales a pares } \implies m\left(\bigoplus_{k\in K} L_\kappa\right) = \sum_{k\in K} m(L_\kappa)$$

Por ejemplo, para cualquier $\mathbf{x} \in S_\mathbb{H}$, $m_x : L \mapsto \langle \mathbf{x} | \pi_L \mathbf{x} \rangle$ es una medida.

Teorema 7.12.1 (Gleason, 1957) *Sea $\mathbb{H}$ un espacio separable de Hilbert de dimensión al menos 3.*

Para cada medida m existe un operador positivo hermitiano T_m tal que

$$\forall L \in \mathscr{V}(\mathbb{H}): \quad m(L) = \mathrm{Tr}(T_m \pi_L),$$

donde Tr *es el operador* traza.

Además la aplicación $m \leftrightarrow T_m$ es una biyección entre medidas y operadores positivos hermitianos.

Ya que la esfera unitaria $S_{\mathbb{H}}$ es conexa y la aplicación $L \mapsto \mathrm{Tr}(T_m \pi_L)$ es contínua (en la topología bien definida en $\mathscr{V}(\mathbb{H})$) entonces del teorema de Gleason se sigue que no hay medidas-("sí","no") en el espacio de proposiciones. La lógica cuántica no puede ser booleana.

Además, por ser $S_{\mathbb{H}}$ compacto débil-*, existe una colección finita de subespacios en $\mathscr{V}(\mathbb{H})$ en la que no se puede definir una medida de dos valores. Un ejemplo de la construcción la da el teorema de Kochen-Specker.

7.13 Teorema de Kochen-Specker

7.13.1 Enunciado del teorema

Sea $\mathbb{H}$ un espacio complejo de Hilbert separable y sea Σ una colección de observables. Sea $\mu : \Sigma \to \mathbb{R}$ una aplicación que asocia a cada observable un valor definido (por ejemplo, a cada estado, la esperanza del observable en ese estado). En la colección de tales μ, consideremos dos propiedades:

Proposición 7.13.1 (Valores bien definidos (VD)) *En cualquier tiempo, la aplicación μ es total: Los valores asumidos por observables están bien determinados en todo momento.*

Proposición 7.13.2 *La aplicación μ satisface las dos reglas siguientes:*

Regla de la Suma *Si $U_0, U_1, U_2 \in \Sigma$ son compatibles entonces:*

$$[U_2 = U_0 + U_1 \implies \mu(U_2) = \mu(U_0) + \mu(U_1)].$$

Regla del Producto *Si $U_0, U_1, U_2 \in \Sigma$ son compatibles entonces:*

$$[U_2 = U_0 U_1 \implies \mu(U_2) = \mu(U_0)\mu(U_1)].$$

Así, si μ fuese una asignación-("sí","no") y $(L_i)_i$ un conjunto finito de proposiciones (sus proyecciones ortogonales π_{l_i} poseen eigenvalores 0,1), la regla de la suma implica:

$$1 = \mu\left(\pi_{\oplus_i L_i}\right) = \sum_i \mu\left(\pi_{L_i}\right).$$

Por tanto ha de valer la implicación:

(VC) $\left[\mu\left(\pi_{L_i}\right)=1 \implies \mu\left(\pi_{L_j}\right)=0\ \forall j\neq i\right].$

Por otro lado, la regla del producto implica:

(VE) $\left[L<L_0\oplus L_1 \implies \mu\left(\pi_L\right)\mu\left(\pi_{L_0\oplus L_1}\right)=\mu\left(\pi_L\right)\right].$

Asóciese el color *rojo* a las proposiciones tales que $\mu\left(\pi_{L_i}\right)=1$ y el color *verde* a las proposiciones tales que $\mu\left(\pi_{L_i}\right)=0$.

La regla de la suma y la condición **(VC)** implican que en cualquier sistema ortonormal finito de vectores exactamente un vector es rojo y los demás verdes.

La condición **(VE)** por su lado implica que cualquier proposición en el espacio generado por dos proposiciones verdes ha de ser verde.

Teorema 7.13.1 (Kochen-Specker (KSThm, 1967)) *Sea $\mathbb{H}$ un espacio de Hilbert separable de dimensión al menos 3. Entonces existe una colección de observables Σ tal que no pueden valer simultáneamente la* **Propiedad 7.13.1** *y la* **Propiedad 7.13.2**.

Teorema 7.13.2 (Kochen-Specker: Caso geométrico tridimensional real) *En $\mathbb{R}^3$ existe una colección de rayos Σ tal que en ninguna coloración rojiverde valen simultáneamente las condiciones siguientes:*

1. *En cualquier tripleta de rayos ortogonales exactamente uno es rojo.*
2. *Cualquier rayo en el plano generado por dos rayos verdes es verde.*

Motivación geométrica.

Sea $\mathbf{x}=(\cos\theta\cos\varphi,\operatorname{sen}\theta\cos\varphi,\operatorname{sen}\varphi)$ un punto en la esfera unitaria de $\mathbb{R}^3$. El ángulo θ es la *longitud* y ϕ es la *latitud*. Un punto en el equador ortogonal a $\mathbf{x}$ es $\mathbf{x}_E=(-\operatorname{sen}\theta,\cos\theta,0)$ (su longitud es la de $\mathbf{x}$ corrido por un ángulo de $\pi/2$ radianes). Sea

$$\mathbf{x}^{\perp}=\mathbf{x}\times\mathbf{x}_E=(-\cos\theta\operatorname{sen}\varphi,-\operatorname{sen}\theta\operatorname{sen}\varphi,\cos\varphi).$$

La tripleta $\left\{\mathbf{x},\mathbf{x}_E,\mathbf{x}^{\perp}\right\}$ es una base ortogonal de $\mathbb{R}^3$ orientada en sentido positivo. Supongamos que $\mathbf{x}$ está en el hemisferio norte pero no es el Polo Norte. Cambiando la dirección de $\mathbf{x}_E$ si fuera necesario, se puede suponer que $\mathbf{x}^{\perp}$ también está en el hemisferio norte. El círculo con centro en el origen que pasa sobre $\mathbf{x}$ y $\mathbf{x}_E$ es el *círculo descendiente* de $\mathbf{x}$.

Una *sucesión de descenso* $\{\mathbf{x}_i\}_{i=0}^{k}$ se construye como sigue: $\mathbf{x}_0$ es un punto en el hemisferio norte pero no es el Polo Norte. Para cualquier $i\geq 0$, $\mathbf{x}_{i+1}$ es un punto elegido en el círculo descendiente de $\mathbf{x}_i$ (hacia el sur de $\mathbf{x}_i$).

Lema 7.13.1 *Dados dos puntos en el hemisferio norte con latitudes diferentes, hay una sucesión de descenso que va del punto al norte al punto al sur.*

La prueba es directa utilizando la proyección $\mathbf{x}\mapsto\frac{1}{x_3}\mathbf{x}$ que a cada punto en el hemisferio norte lo aplica en el cruce de su rayo con el plano paralelo al plano-x,y

que pasa por el Polo Norte. Círculos paralelos corresponden a unas misma latitudes y los círculos de descendientes son tangentes a éstos.

Bosquejo de la prueba del teorema 7.13.2. Sea inicialmente $\Sigma = \{\mathbf{e}_0, \mathbf{e}_1, \mathbf{e}_2\}$ la colección de los tres vectores en la base canónica. Supongamos que el Polo Norte $\mathbf{e}_2 = (0,0,1)$ está pintado de rojo. Sea $\mathbf{x}$ un vector de latitud $\frac{2}{3}\pi$. Entonces $\mathbf{x}_E$ está en el ecuador, por tanto pintado de verde, y $\mathbf{x}^\perp$ tiene latitud $\frac{1}{3}\pi$. Se sigue que $\mathbf{x}$ y $\mathbf{x}^\perp$ tienen colores opuestos.

Si $\mathbf{x}$ es verde entonces, por un lado, $\mathbf{x}^\perp$ es rojo, y, por otro lado, cualquier rayo en el círculo de descendiente de $\mathbf{x}$ es verde. Así, cualquier rayo al que se llega mediante una sucesión de descenso a partir de $\mathbf{x}$ debe ser verde, en particular ha de serlo $\mathbf{x}^\perp$ lo cual es una contradicción.

De otra manera, cualquier rayo a un ángulo de $\frac{1}{3}\pi$ del Polo Norte, debe ser rojo, como el Polo. De hecho cualquier rayo en el cono de ángulo $\frac{1}{3}\pi$ de un rayo rojo debe ser rojo. Entonces hay es un arco de tres rayos rojos desde el Polo Norte al Ecuador, otro arco de tres rayos rojos a lo largo del Ecuador, y otro arco de tres rayos rojos desde el Ecuador al Polo Norte. Las tres esquinas en este circuito son rojas, pero ellas forman un sistema ortogonal. Esto es una contradicción.

7.13.2 Algunas implicaciones

Puesto de manera tosca, el teorema de Kochen-Specker (TeoKS) implica que la Mecánica Cuántica (QM) no es consistent con las siguientes dos propiedades:

Valores bien definidos (VD) Todos los observables poseen valores bien definidos en todo momento.

No-Contextualidad (NC) Si un observable adquiere un valor, lo hace independientemente de cualquier contexto de medida.

En símbolos:

$$\text{TeoKS: } QM \not\models VD + NC$$

Consecuentemente, la aceptación de QM entraña el rechazo de bien VD o bien de NC.

VD es el origen de cualquier *programa de variables ocultas*.

NC es la motivación de la noción de *realismo*.

Es un problema importante desarrollar una version de QM que contenga VD pero no NC.

7.14 Universalidad en las álgebras de Clifford

Hacemos una presentación basada en las monografías de Vlasov [Vlasov(1999), Vlasov(2001)].

Como se introdujo en la sección 6.5, el álgebra de Clifford $\mathrm{Cl}(2n,\mathbb{C})$ es isomorfa al álgebra de matrices $\mathbb{C}^{2^n\times 2^n}$, y las matrices unitarias en esta última son precisamente las compuertas cuánticas.

Una colección de matrices unitarias $\mathscr{U} = (U_\kappa)_{\kappa\in K} \subset \mathrm{Cl}(2n,\mathbb{C})$ se dice ser *universal* si para cada operador unitario $U \in \mathrm{U}(2^n)$ existe una lista (finita) de índices $\kappa_0 \cdots \kappa_{\ell-1} \in K^*$ tal que

$$U = U_{\kappa_0} \cdots U_{\kappa_{\ell-1}}.$$

Sean $\sigma_0,\sigma_1,\sigma_2,\sigma_3 \in \mathrm{Cl}(1,\mathbb{C})$ los operadores de Pauli definidos en la relación (7.5).

Para cada $k = 0,\ldots,n-1$ sean

$$U_{n,2k} = i\,\sigma_0^{\otimes(n-k-1)} \otimes \sigma_1 \otimes \sigma_3^{\otimes k} \;\;,\;\; U_{n,2k+1} = i\,\sigma_0^{\otimes(n-k-1)} \otimes \sigma_2 \otimes \sigma_3^{\otimes k},$$

con $i = \sqrt{-1} \in \mathbb{C}$. Entonces la colección $\mathscr{U} = (U_\kappa)_{\kappa=0}^{2n-1} \subset \mathrm{Cl}(2n,\mathbb{C})$ consta de $2n$ operadores en $\mathrm{U}(2^n)$, todos ellos antihermitianos: $\forall U \in \mathscr{U},\, U^H = -U$.

Se tiene la siguiente relación de *conmutatividad*:

$$\forall \kappa,\lambda:\;\; \{U_\kappa, U_\lambda\} = U_\kappa U_\lambda + U_\lambda U_\kappa = -2\delta_{\kappa\lambda} Id_{2^n}.$$

Sea $\mathscr{U}^*$ la colección de productos de operadores en $\mathscr{U}$. Puesto recursivamente,

$$\mathscr{U} \subset \mathscr{U}^* \;\&\; [U \in \mathscr{U}, V \in \mathscr{U}^* \;\Rightarrow UV \in \mathscr{U}^*].$$

Sea

$$\mathscr{L}_{\mathbb{K}}(\mathscr{U}) = \{\sum_J a_j V_j |\; J \text{ es finito } \;\&\; \forall j \in J\,[V_j \in \mathscr{U}^* \;\&\; a_j \in \mathbb{K}]\}$$

el espacio de operadores generado por $\mathscr{U}^*$ con coeficientes en el campo $\mathbb{K}$, el cual puede ser el de los reales $\mathbb{R}$ o el de los complejos $\mathbb{C}$.

Se tiene que, tomando coeficientes complejos, $\mathscr{L}_{\mathbb{C}}(\mathscr{U}) = \mathrm{Cl}(2n,\mathbb{C})$.

Por otra parte, tomando coeficientes reales, $\mathscr{L}_{\mathbb{R}}(\mathscr{U}) \cap \mathrm{U}(2^n)$ es un subgrupo de dimensión $n(2n+1)$ de $\mathrm{U}(2^n)$, el cual coincide con $\mathrm{Spin}(2n+1)$.

Así pues, el conjunto $\mathscr{U}$ de operadores no es universal.

Sin embargo, al incorporarse a él cualquiera de los siguientes dos operadores

$$iU_0U_1U_2 \quad \text{o} \quad iU_0U_1U_2U_3$$

entonces el conjunto resultante sí será universal.

Referencias

[Alperin and Bell(1995)] Alperin J, Bell R (1995) Groups and Representations. Graduate Texts in Mathematics, Springer New York, URL https://books.google.com.mx/books?id=fYWkPNiK0wwC

[Arnold(1989)] Arnold V (1989) Mathematical methods of classical mechanics, vol 60. Springer

[Audretsch(2008)] Audretsch J (2008) Entangled Systems: New Directions in Quantum Physics. Wiley, URL https://books.google.com.mx/books?id=4vDqYvg2aV0C

[Ballentine(1998)] Ballentine L (1998) Quantum Mechanics: A Modern Development. World Scientific, URL https://books.google.com.mx/books?id=sHJRFHz1rYsC

[Bennett et al(1996a)] Bennett CH, Bernstein HJ, Popescu S, Schumacher B (1996a) Concentrating partial entanglement by local operations. Phys Rev A 53:2046–2052, DOI 10.1103/PhysRevA.53.2046, URL http://link.aps.org/doi/10.1103/PhysRevA.53.2046

[Bennett et al(1996b)] Bennett CH, Brassard G, Popescu S, Schumacher B, Smolin JA, Wootters WK (1996b) Purification of noisy entanglement and faithful teleportation via noisy channels. Phys Rev Lett 76:722–725, DOI 10.1103/PhysRevLett.76.722, URL http://link.aps.org/doi/10.1103/PhysRevLett.76.722

[Bernstein and Vasirani(1993)] Bernstein E, Vasirani U (1993) Quantum complexity theory. In: Proc. of the 25-th Annual ACM Symposium on Theory of Computing, Association of Computing Machinery, AIP Conference Proceedings

[Chandler(1987)] Chandler D (1987) Introduction to modern statistical mechanics. Oxford University Press, New York, Oxford, URL http://opac.inria.fr/record=b1081336

[Chappell et al(2013)] Chappell JM, Iqbal A, Lohe MA, Smekal L, Abbott D (2013) An improved formalism for quantum computation based on geometric algebra–case study: Grover's search algorithm. Quantum Information Processing 12(4):1719–1735, DOI 10.1007/s11128-012-0483-7, URL http://dx.doi.org/10.1007/s11128-012-0483-7

[Deutsch(1985)] Deutsch D (1985) Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer 400:96–117

[Deutsch and Jozsa(1992)] Deutsch D, Jozsa R (1992) Rapid solution of problems by quantum computation 439:553–558

[Donald et al(2002)] Donald MJ, Horodecki M, Rudolph O (2002) The uniqueness theorem for entanglement measures, quant-ph/0105017

[Goldstein et al(2002)] Goldstein H, Poole C, Safko J (2002) Classical Mechanics. Addison Wesley, URL https://books.google.com.mx/books?id=tJCuQgAACAAJ

[Hall(2003)] Hall B (2003) Lie Groups, Lie Algebras, and Representations: An Elementary Introduction. Graduate Texts in Mathematics, Springer, URL https://books.google.com.mx/books?id=m1VQi8HmEwcC

[Horodecki et al(2009)] Horodecki R, Horodecki P, Horodecki M, Horodecki K (2009) Quantum entanglement. Rev Mod Phys 81:865–942, DOI 10.1103/RevModPhys.81.865, URL http://link.aps.org/doi/10.1103/RevModPhys.81.865

[Jackson(1999)] Jackson JD (1999) Classical electrodynamics, 3rd edn. Wiley, New York, NY, URL http://cdsweb.cern.ch/record/490457

[James and Liebeck(2001)] James G, Liebeck M (2001) Representations and Characters of Groups. Cambridge mathematical textbooks, Cambridge University Press, URL https://books.google.com.mx/books?id=PiJMr6kZP44C

[Krammer(2008)] Krammer P (2008) Characterizing entanglement with geometric entanglement witnesses, quant-ph/0807.4830

[Landau and Lifshitz(1981)] Landau LD, Lifshitz LM (1981) Quantum Mechanics Non-Relativistic Theory, Third Edition: Volume 3, 3rd edn. Butterworth-Heinemann, URL http://www.worldcat.org/isbn/0750635398

[Lavor et al(2003)] Lavor C, Manssur L, Portugal R (2003) Shor's algorithm for factoring large integers URL arXiv:quant-ph/0303175v1

[Lawson and Michelsohn(1989)] Lawson H, Michelsohn M (1989) Spin Geometry. Princeton mathematical series, Princeton University Press, URL https://books.google.com.mx/books?id=3d9JkN8w3X8C

[Lounesto(2001)] Lounesto P (2001) Clifford algebras and spinors. London Mathematical Society lecture note series, Cambridge University Press, Cambridge, New York, URL http://opac.inria.fr/record=b1135669

[Nielsen and Chuang(2011)] Nielsen MA, Chuang IL (2011) Quantum Computation and Quantum Information: 10th Anniversary Edition, 10th edn. Cambridge University Press, New York, NY, USA

[Peres(1995)] Peres A (1995) Quantum Theory: Concepts and Methods. Fundamental Theories of Physics, Springer, URL https://books.google.com.mx/books?id=rMGqMyFBcL8C

[Porteous(1995)] Porteous I (1995) Clifford Algebras and the Classical Groups. Cambridge Studies in Advanced Mathematics, Cambridge University Press, URL https://books.google.com.mx/books?id=pivcVR3d_lEC

[Sakurai(1993)] Sakurai JJ (1993) Modern Quantum Mechanics (Revised Edition), revised edn. Addison Wesley, URL http://www.amazon.com/exec/obidos/redirect?tag=citeulike07-20&path=ASIN/0201539292

[Sands(1969)] Sands D (1969) Introduction to Crystallography. Dover Books on Chemistry Series, Dover, URL https://books.google.com.mx/books?id=h_A5u5sczJoC

[Shor(1994)] Shor PW (1994) Algorithms for quantum computation: Discrete logarithms and factoring. In: IEEE Symposium on Foundations of Computer Science, IEEE, pp 124–134

[Shor(1997)] Shor PW (1997) Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing 26:1484–1509

[Varadarajan(2004)] Varadarajan V (2004) Supersymmetry for Mathematicians: An Introduction. American Mathematical Society, URL https://books.google.com.mx/books?id=sZ1-G4hQgIIC

[Vedral and Plenio(1998)] Vedral V, Plenio MB (1998) Entanglement Measures and Purification Procedures. Phys Rev A 57(quant-ph/9707035. 3):1619, URL https://cds.cern.ch/record/330751

[Vlasov(1999)] Vlasov AY (1999) Quantum gates and Clifford algebras, quant-ph/9907079

[Vlasov(2001)] Vlasov AY (2001) Clifford algebras and universal sets of quantum gates, quant-ph/0109010

Índice temático