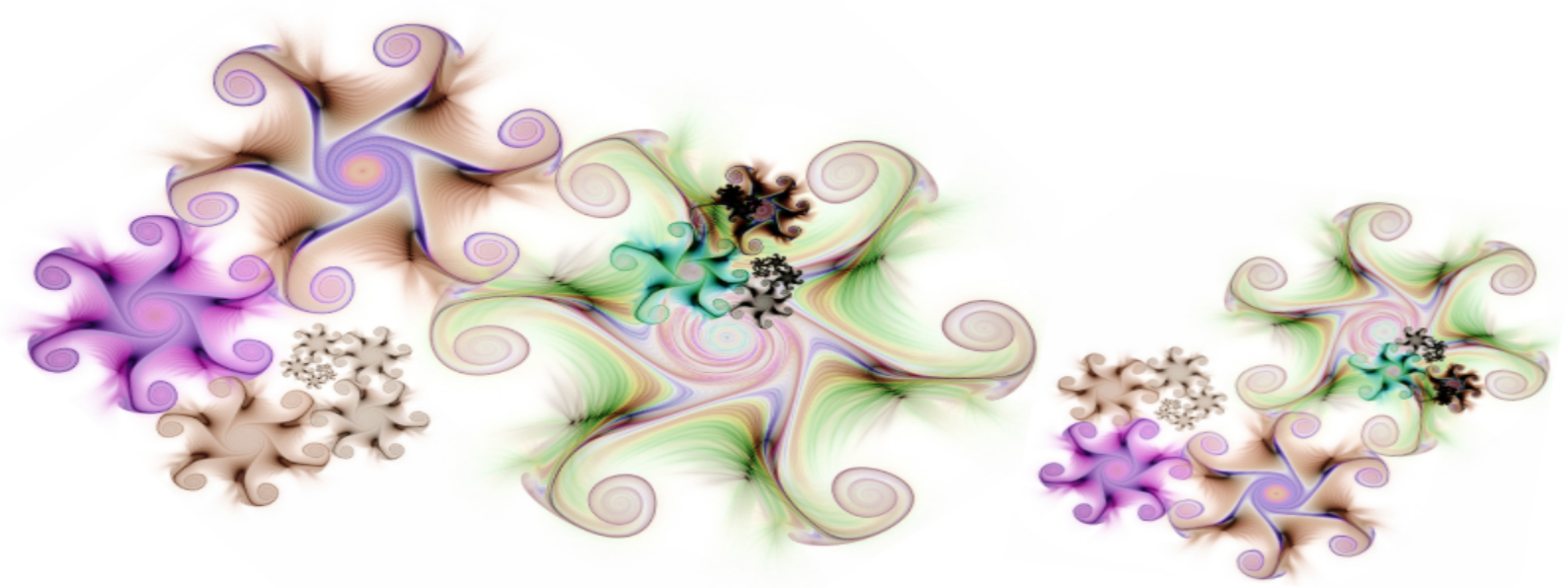
UNIVERSIDAD AUTÓNOMA METROPOLITANA
Casa abierta al tiempo
Unidad Iztapalapa

Ciencias Básicas e Ingeniería CBI

mixba'al
Revista Metropolitana de Matemáticas
www.doi.org/10.24275/uami/dcbi/mix/v16n1/bolpitcan ISSN: 2007-7874



Del Cero al Quantum: Un viaje por el mundo de los códigos

Jorge Ricardo Bolaños Servín
Yuriko Pitones Amaro
Josué Ivan Rios Cangas

7° Coloquio del Departamento de Matemáticas UAM-I

Del 27 al 31 de enero de 2025

Casa abierta al tiempo | UNIVERSIDAD AUTÓNOMA METROPOLITANA

MIXBA'AL. Vol. 16, No. 1, enero-diciembre de 2025, es una publicación anual de la Universidad Autónoma Metropolitana a través de la Unidad Iztapalapa, División de Ciencias Básicas e Ingeniería, Departamento de Matemáticas. Prolongación Canal de Miramontes 3855, Col. Ex Hacienda San Juan de Dios, Alcaldía Tlalpan, C.P. 14387, CDMX, México y Av. Ferrocarril San Rafael Atlixco, No. 186, Col. Leyes de Reforma 1a Sección, Alcaldía Iztapalapa, C.P. 09340, CDMX, México. Tel. 5804 4658. Página electrónica de la revista: http://mat.izt.uam.mx/mat/ index.php/revistamixba-al. Correos electrónicos: mixbaal2009@gmail.com, mixb@xanum.uam.mx. Coordinador Editorial Mario Pineda Ruelas. Certificado de Reserva de Derechos al Uso Exclusivo de Título No. 04-2023-07031 1572300-102, ISSN5 2007-7874, ambos otorgados por el Instituto Nacional del Derecho de Autor. Responsable de la última actualización de este número Mario Pineda Ruelas, Departamento de Matemáticas, edificio AT, oficina 318. División de Ciencias Básicas e Ingeniería, Universidad Autónoma Metropolitana-Iztapalapa. Av. Ferrocarril San Rafael Atlixco No. 186,Colonia Leyes de Reforma 1a Sección, Alcaldía Iztapalapa, C.P. 09340, CDMX, México. Fecha de última modificación 30 de agosto de 2025. Tamaño del archivo 121.3 MB.

7º COLOQUIO DEL DEPARTAMENTO DE MATEMÁTICAS

del 27 al 31 de enero del 2025, Unidad Iztapalapa de la UAM, Ciudad de México

Departamento de Matemáticas
UAM IZTAPALAPA

Posgrado de Matemáticas
UAM IZTAPALAPA

Taller 1: Análisis de datos con un enfoque bayesiano

Autor: Dr. Asael Fabian Martínez Martínez

Taller 2: Un breve recorrido por la teoría de prerradicales y sus retículas

Autores: Dr. Rogelio Fernández-Alonso, Dra. Silvia Gavito Ticozzi, Dra. Martha Lizbeth Shaid Sandoval Miranda

Taller 3: Resultados del cálculo y álgebra lineal relevantes en modelos y aplicaciones

Autor: Dr. Lorenzo Héctor Juárez

Taller 4: Análisis geométrico de superficies: una introducción elemental

Autores: Dr. Josué Melendez y M. en C. Eduardo Rodríguez Romero

Taller 5: Una introducción a los torneos y sus generalizaciones

Autores: Dr. Ilán Goldfeder Ortiz y Dra. Nahid Yelene Javier Nol

Taller 6: Del cero al quantum: un viaje por el mundo de los códigos

Autores: Dr. Jorge Bolaños Servín, Dra. Yuriko Pitones Amaro y Dr. Josué Rios Cangas

Taller 7: Introducción a la teoría de juegos epistémica

Autor: Dr. Rubén Becerril Borja

Taller 8: Cómo contar más allá del infinito y para qué sirve. Inducción transfinita y algunas aplicaciones

Autor: Dr. Rodrigo Hernández Gutiérrez

UNIVERSIDAD AUTÓNOMA METROPOLITANA
Casa abierta al tiempo
Unidad Iztapalapa

Ciencias Básicas e Ingeniería CBI

7° Coloquio del Departamento de Matemáticas UAM-I 2025
Universidad Autónoma Metropolitana, Iztapalapa CDMX.

Introducción

La teoría de códigos, tanto clásica como cuántica, busca garantizar la integridad de la información frente a errores que puedan surgir durante su transmisión, almacenamiento o procesamiento. En su forma clásica, se aplica en áreas como telecomunicaciones, almacenamiento digital y criptografía, permitiendo detectar y corregir errores causados por ruido o daños físicos. En los últimos años, la teoría cuántica ha cobrado relevancia debido a su aplicación en la computación y comunicación cuántica, donde los sistemas son especialmente sensibles al ruido y la decoherencia. Estos avances son fundamentales para el desarrollo de tecnologías emergentes, como la computación cuántica, que promete revolucionar múltiples áreas de la ciencia y la tecnología.

El objetivo de estas notas es proporcionar una introducción clara y accesible a estos campos interrelacionados, enfocándose en la conexión entre las herramientas matemáticas y los principios físicos subyacentes. Estas notas no pretenden sustituir ningún libro de texto, sino ofrecer un panorama que sirva de base para aquellos que deseen adentrarse en la teoría de códigos, con énfasis en los aspectos conceptuales esenciales.

En el primer capítulo, se presenta la teoría de códigos clásicos. Se abordan códigos de bloque, códigos lineales y herramientas fundamentales como la cota de Singleton y el enumerador de pesos. Además, se exploran códigos polinomiales relevantes, como los de Reed-Solomon y Reed-Muller, que tienen aplicaciones significativas en la informática y la criptografía.

El segundo capítulo ofrece una introducción al análisis funcional en espacios finito-dimensionales, estableciendo los cimientos necesarios para entender los códigos cuánticos. En este contexto, se presentan los espacios de Banach y Hilbert, los operadores lineales y su teoría espectral, también se introduce la notación bra-ket de Dirac, ampliamente utilizada en física cuántica. En la última sección se presenta una introducción a operadores normales, autoadjuntos, unitarios y operadores positivos.

Finalmente, en el tercer capítulo se centra en los códigos cuánticos correctores de errores. Se revisan los conceptos fundamentales de estados cuánticos, canales cuánticos y qubits, y se describe la teoría general de códigos cuánticos correctores de errores, incluyendo el teorema de Knill-Laflamme. Además, se introduce la representación de errores mediante las matrices Pauli como una base adecuada para su descripción.

Estas notas están diseñadas como complemento al taller titulado *Del cero al quantum: un viaje por el mundo de los códigos* que se ofrecerá en el 7° Coloquio del Departamento de Matemáticas de la UAM–I. Este taller está dirigido a estudiantes avanzados de licenciatura o del primer año de posgrado en matemática y áreas afines con intereses en álgebra y análisis.

Jorge Ricardo Bolaños Servín; Yuriko Pitones Amaro; Josué Ivan Rios Cangas
jrbs@xanum.uam.mx; ypitones@xanum.uam.mx; jottsmok@xanum.uam.mx
Departamento de Matemáticas, UAM-Iztapalapa

Índice general

Capítulo 1

Códigos clásicos

Este capítulo presenta una introducción de los Códigos Clásicos, el objetivo es proporcionar al lector los conceptos fundamentales y ejemplos ilustrativos de códigos lineales correctores de errores definidos sobre campos finitos. El contenido presentado se basa en las referencias [3,5,13].

Usualmente cuando hablamos de códigos (clásicos) suponemos que un emisor quiere transmitir un mensaje m a algún receptor a través de un canal. *Un canal* es un medio físico en el que el mensaje está siendo transmitido y que, debido a las interacciones con el mismo canal, puede ser alterado y convertirse en un mensaje m'. Matemáticamente lo representamos como una variable aleatoria W sobre el espacio de mensajes que podemos enviar. Con símbolos lo podemos representar de la siguiente forma:

$$m \xrightarrow{W} m'.$$

Sin embargo, a menos de que $W(m' \mid m) = 1$, no existe forma de saber si el mensaje m' es el resultado de la interacción del canal con m o con cualquier otro mensaje. La teoría de códigos se refiere al diseño de algoritmos (C, D), llamados codificación y decodificación, de tal modo que, en lugar de transmitir m, enviamos $w = C(m)$. Tras recibir el mensaje w', nos gustaría que $m' = D(w')$ sea tal que $m = m'$ o al menos podamos garantizar que este es el caso con alta probabilidad de suceder.

$$m \xrightarrow{C} w \xrightarrow{W} w' \xrightarrow{D} m'.$$

Uno de los problemas de la teoría de códigos es garantizar que $\Pr(m = m') = 1 - \varepsilon$, donde ε representa el error en la transmisión. En general existen dos perspectivas de cómo abordar este problema:

- **La perspectiva de Shannon**. Esta perspectiva se centra en la cantidad máxima de información que puede transmitirse a través de un canal de comunicación con errores, de manera confiable. Shannon definió el concepto de capacidad del canal y demostró que, mediante el uso de códigos adecuados, es posible transmitir información cerca de esta capacidad con una probabilidad de error arbitrariamente pequeña. El enfoque es probabilístico: se analiza el comportamiento promedio de los códigos y los errores, en lugar de construir códigos específicos. No se preocupa tanto por cómo diseñar códigos concretos, sino por establecer los límites teóricos de lo que es posible en la transmisión de datos.

  Se consideran las propiedades probabilísticas de W, por lo que muchas veces asumimos algún tipo de distribución sobre W, y la usamos para diseñar de forma adecuada C y D. El principal objetivo es que para cualquier m, se tenga que $\Pr(m = D(m')) = 1 - \varepsilon$.

- **La perspectiva de Hamming.** Esta perspectiva se enfoca en cómo diseñar códigos específicos que permitan detectar y corregir errores en la transmisión de información. El objetivo principal es garantizar que, incluso si se alteran ciertos bits durante la transmisión, sea posible recuperar el mensaje original. Se introducen conceptos como la distancia de Hamming, que mide el número de posiciones en las que dos cadenas de bits difieren, lo cual es crucial para determinar la capacidad de corrección de un código. Este enfoque es constructivo: se diseña y analiza la estructura matemática de códigos concretos.

  En particular se asume que no tenemos ninguna información sobre W. En este caso, también asumimos que el canal es un adversario que corrompe el mensaje arbitrariamente y que tiene una capacidad limitada para alterarlo; esto lo entenderemos habitualmente como que el adversario transforma el mensaje m no en cualquier otro mensaje, sino en subconjuntos específicos, determinados por cómo midamos esta capacidad del adversario. En este caso, nos gustaría que $D(m') = m$ sin posibilidad de errores.

Estas perspectivas no son excluyentes en la práctica: muchas veces, usamos múltiples algoritmos de codificación y decodificación durante un proceso de transmisión y en estos múltiples algoritmos, a veces asumimos una u otra perspectiva en el camino.

En estas notas, nos enfocaremos en la perspectiva de Hamming para códigos de bloque.

1.1 Códigos de bloque

Sea A un conjunto finito que llamaremos alfabeto. Supondremos que nuestro canal toma símbolos en A y los transforma en otros símbolos de A, es decir, el proceso de transmitir mensajes se da sobre el mismo alfabeto.

$$W : A \to A.$$

Los mensajes con los que representaremos nuestra información pertenecen a A^k, para alguna k.

Definición 1.1. Un código de bloque C es un subconjunto de A^n de cardinalidad $|A|^k$, y una función de codificación es una función $C : A^k \to C$. Sea $D \subseteq A^n$. Una función de decodificación sobre D es una función $D : D \to A^k$.

Decimos que la decodificación es *exitosa* si en el proceso

$$m \in A^k \xrightarrow{C} w = C(m) \in C \xrightarrow{W} w' \in D,$$

tenemos que $D(w') = m$.

Siguiendo este enfoque, nos interesa diseñar códigos C de tal modo que exista una función $D : D \to A^k$, con D lo más grande posible, tal que la decodificación sea exitosa.

Ejemplo 1.2. (Mal ejemplo) Supongamos $A = \{0, 1\}$ y $k = 1$. Sea $C = \{00000, 10000\}$. En este caso podemos mostrar que no existe (C, D) de tal modo que podamos decodificar exitosamente $w' = 10000$, a menos que W no induzca errores.

Ejemplo 1.3. (Un mejor ejemplo). Sea $A = \{0,1\}$, $k = 1$ y $C = \{000, 111\}$. En este caso podemos encontrar una función codificadora y una decodificadora tal que, para $m \in A$, si $m' \in A^3$ difiere en a lo más un símbolo de $C(m)$, entonces tenemos que la decodificación es exitosa.

Cada uso del canal tiene la posibilidad de alterar un símbolo a la vez. Entonces el efecto del canal sobre el mensaje transmitido lo podemos medir usando la *distancia de Hamming*.

Definición 1.4. Sean $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n) \in A^n$. La distancia de Hamming entre u y v es el número de posiciones en las que difieren:

$$d_H(u,v) = |\{i \in [n] : u_i \neq v_i\}|.$$

El peso (de Hamming) de un vector $w \in A^n$ es el número de entradas no nulas en w, denotado como $\mathrm{wt}(w)$. Así, $\mathrm{wt}(w) = d(w,0)$, y $d(x,y) = \mathrm{wt}(x-y)$.

La distancia de Hamming es, de hecho, una métrica sobre A^n. Utilizaremos constantemente este hecho, en particular la desigualdad del triángulo.

Cuando asumimos que W es un modelo de adversario, asumimos una capacidad limitada del adversario midiéndola como el máximo número de entradas que puede alterar por cada n usos. Esto motiva la siguiente definición.

Definición 1.5. Un canal $W : A \to A$ tiene capacidad t respecto a n si al enviar cualquier elemento $m \in A^n$, obtenemos $m' \in A^n$ tal que $d_H(m,m') \leq t$.

Típicamente asumimos que $t/n \ll 1$ y que los errores pueden aparecer arbitrariamente. Asumir cualquier otra cosa nos posicionaría en la perspectiva de Shannon, y algunas de las técnicas que aquí describiremos serían insuficientes.

Entonces, si nuestro canal tiene capacidad t respecto a n, nuestro objetivo será diseñar códigos que se puedan corregir frente a la presencia de t-errores, es decir, existe un algoritmo de decodificación tal que si $w \in C$, $y \in A^n$ y $d_H(w,y) \leq t$, entonces se puede decodificar y eficientemente.

Definición 1.6. Sea $C \subseteq A^n$. Definimos la distancia mínima de C, denotada por $d(C)$, como el mínimo de las distancias de Hamming entre dos elementos distintos de C:

$$d(C) = \min\{d_H(u,v) : u,v \in C, u \neq v\}.$$

Un algoritmo simple de decodificación es una función $D : A^n \to C$ tal que:

$$D(y) \in \arg\min_{c \in C} d(y,c) = \{c \in C : d(y,v) \geq d(y,c)\}.$$

Definición 1.7. Decimos que $e \in A^n$ de peso t es corregible si para todo $v \in C$,

$$|\arg\min_{c \in C} d(v+e,c)| = 1.$$

Decimos que $e \in A^n$ de peso t es un error detectable si para toda $v \in C$,

$$v + e \notin C.$$

Si recibimos $y \in A^n$ y asumimos que proviene de una transmisión de $v \in C$, eso es equivalente a decir que $y = v + e$ para algún $e \in A^n$, donde $\mathrm{wt}(e)$ es el número de errores que sucedieron en la transmisión. Que e sea corregible significa que, al recibir y, basta con elegir la palabra más cercana a y en C, y esa será la palabra v original. *Detectable* significa que, aun si no podemos corregir, al menos podemos saber que y es una palabra que no está en el código y, por lo tanto, no pudo haber sido la palabra original.

Con la definición de distancia mínima, analicemos con detalle el ejemplo 1.2.

Ejemplo 1.8. La distancia de Hamming entre las palabras del código C es:

$$d(C) = d_H(00000, 10000) = 1.$$

Esto significa que las palabras código están separadas por una sola posición. Por lo tanto, un único error puede transformar una palabra del código en otra palabra del código.

Supongamos los siguientes escenarios:

- Si transmitimos 00000 y ocurre un error en la primera posición, el receptor recibe:

$$w' = 10000.$$

- Si transmitimos 10000 y no hay errores, el receptor también recibe:

$$w' = 10000.$$

Esto crea una ambigüedad: la palabra recibida $w' = 10000$ puede corresponder tanto a 00000 con un error como a 10000 sin errores.

Para decodificar correctamente, necesitamos que cada palabra recibida se asocie de manera inequívoca con una palabra en C. Sin embargo, en este caso:

- $w' = 10000$ está a distancia 1 de 00000 (cuando se transmite con un error).
- $w' = 10000$ también es una palabra válida del código.

Por lo tanto, la decodificación de $w' = 10000$ no es posible sin ambigüedad.

Si asumimos que no hay errores en el canal, entonces:

$$w' = 10000 \implies \text{decodificado como } 10000.$$

Sin embargo, si el canal introduce errores, $w' = 10000$ no puede decodificarse inequívocamente porque podría haber resultado de la transformación de 00000.

En conclusión, no es posible construir un par (C, D) que permita decodificar $w' = 10000$ de manera inequívoca si el canal introduce errores. Esto se debe a que la distancia mínima del código C es $d(C) = 1$, lo que no permite distinguir entre una palabra código recibida correctamente y una palabra transformada por un error.

Para que se pueda garantizar una decodificación confiable, el código debe tener una distancia mínima $d(C) \geq 3$, lo que permitiría detectar y corregir al menos un error.

Ejemplo 1.9. Sea $C = \{000000, 111000, 000111, 111111\}$. La distancia mínima $d(C)$ se calcula como la menor distancia de Hamming entre dos palabras distintas de C. Comparando todas las parejas:

$$d_H(000000, 111000) = 3, \quad d_H(000000, 000111) = 3, \quad d_H(000000, 111111) = 6,$$

$$d_H(111000, 000111) = 6, \quad d_H(111000, 111111) = 3, \quad d_H(000111, 111111) = 3.$$

La menor de estas distancias es:

$$d(C) = 3.$$

Por lo tanto, la distancia mínima del código es $d(C) = 3$.

- ¿Cuál es el máximo número de errores s tal que siempre se puede saber cuándo hubo hasta s errores? Un código puede detectar hasta s errores si $s < d(C)$. Dado que $d(C) = 3$:

  $$s = d(C) - 1 = 3 - 1 = 2.$$

  Por lo tanto, el código puede detectar hasta $s = 2$ errores de manera confiable.

- ¿Cuál es el máximo número de errores que C puede corregir? Un código puede corregir hasta t errores, donde:

  $$t = \left\lfloor \frac{d(C) - 1}{2} \right\rfloor.$$

  Sustituyendo $d(C) = 3$:

  $$t = \left\lfloor \frac{3 - 1}{2} \right\rfloor = \left\lfloor \frac{2}{2} \right\rfloor = 1.$$

  Por lo tanto, el código puede corregir hasta $t = 1$ error.

- Si recibimos la palabra (110011) y sabemos que el canal tiene capacidad 3, ¿cuál es la palabra que originalmente enviamos? Recibimos $w' = 110011$, y el canal tiene capacidad para introducir hasta 3 errores. Calculamos la distancia de Hamming entre w' y cada palabra en C:

  $$d_H(110011, 000000) = 4, \quad d_H(110011, 111000) = 3,$$

  $$d_H(110011, 000111) = 3, \quad d_H(110011, 111111) = 2.$$

  La distancia mínima es 2, y la palabra más cercana es 111111. Por lo tanto, asumimos que la palabra originalmente enviada fue:

  $$\boxed{111111}.$$

Proposición 1.10. *Sea C un código de distancia mínima d. Pruebe que C puede detectar hasta $d-1$ errores y corregir hasta $\lfloor (d-1)/2 \rfloor$ errores.*

Demostración. Sea $v \in C$ y sea $y \in A^n$ tal que $y = v + e$ para algún e con $\mathrm{wt}(e) \leq d - 1$. Si e no fuera detectable, entonces $y \in C$ y, por lo tanto, $d(C) \leq d(y, v) = d - 1$, contradiciendo la definición de distancia mínima.

Si $\mathrm{wt}(e) \leq (d-1)/2$ y $w \in \arg\min_{c \in C} d(y,c)$, entonces

$$d(w,y) \leq \mathrm{wt}(e) \leq (d-1)/2$$

y por lo tanto

$$d(w,y) \leq d(w,y) + d(y,v) \leq (d-1)/2 + (d-1)/2 = d-1.$$

Como $w, v \in C$ y $d(C) = d$, entonces $w = v$, y por lo tanto $|\arg\min_{c \in C} d(y,c)| = 1$. □

La cantidad $d-1$ se denomina la *capacidad de detección del código*, y $t_C = \lfloor (d-1)/2 \rfloor$ se denomina la *capacidad de corrección del código*. El proceso de decodificar eligiendo la palabra más cercana en el código a la palabra recibida se denomina *decodificación del vecino más próximo*. La existencia de este decodificador está garantizada siempre por una búsqueda exhaustiva; sin embargo, la complejidad de este proceso es elevada. En la siguiente sección, exploraremos códigos con cierta estructura algebraica que permiten reducir el costo de almacenamiento, la complejidad de codificación y de decodificación.

Ejercicios de la sección

P.1.1.1 Demuestra que todo código que corrige t errores también detecta t errores, pero no necesariamente al revés.

P.1.1.2 Demuestra que para cualquier entero n, no existe un código con longitud de bloque n que pueda manejar un número arbitrario de errores.

P.1.1.3 Prueba que la distancia de Hamming es una métrica.

P.1.1.4 Sea C un código con distancia d para d par. Entonces, argumenta que C puede corregir hasta $d/2-1$ errores, pero no puede corregir $d/2$ errores. Usando esto u otro método, argumenta que si un código C corrige t errores, entonces tiene una distancia de $2t+1$ o $2t+2$.

1.2 Códigos lineales

A partir de ahora, supondremos que $A = \mathbb{F}_q$ es un campo finito de q elementos.

Definición 1.11. Un código lineal sobre $\mathbb{F}_q$ es un subespacio vectorial de $\mathbb{F}_q^n$. Los parámetros básicos de un código son: su longitud (n), dimensión (denotada k usualmente) y la distancia mínima (d). Un código con estos parámetros se denomina un $[n,k,d]_q$-código.

Proposición 1.12. *La distancia mínima de C corresponde con el peso mínimo de sus palabras no cero.*

Podemos representar a un código a través de una base y escribirla como una matriz de rango completo.

Definición 1.13. Sea C un $[n,k,d]_q$-código. Una matriz $G \in \mathbb{F}_q^{k\times n}$, cuyos renglones forman una base de C, es llamada una matriz generadora de C. Si G se puede escribir como una matriz de la forma $[I_k|A]$, donde I_k es una identidad de tamaño k, se dice que G está en forma sistemática o estándar.

Definición 1.14. Dos códigos C y D son equivalentes si existe una permutación de las coordenadas σ tal que

$$C = \{(v_{\sigma(1)}, \ldots, v_{\sigma(n)}) : v \in D\},$$

o equivalentemente, si existe una matriz de permutación P tal que

$$C = DP = \{vP : v \in D\}.$$

Una matriz monomial es una matriz invertible con renglones de peso 1. Dos códigos son isométricos si y solo si existe una matriz monomial M tal que $C = DM$.

Proposición 1.15. *Siempre existe una permutación P tal que CP tiene una matriz generadora en forma sistemática.*

Demostración. Sea G una matriz generadora de C en forma escalonada reducida y considere los índices $i_1, \ldots, i_k \in [n]$ de las columnas de G tales que $e_j = G_{i_j}$, donde G_i es la i-ésima columna de G y e_j es el j-ésimo elemento de la base canónica. Sea P una matriz cuadrada de tamaño n tal que $P_{ij} = 1$ si $i = i_j$ para $1 \leq i \leq k$.

Entonces para $1 \leq i \leq k$,

$$(GP)_{ij} = \sum_{h=1}^{n} G_{ih}P_{hj} = G_{i_j j}.$$

Es decir, la i-ésima columna de GP es la i_j-ésima columna de G, y por lo tanto las primeras k-columnas de GP forman una matriz identidad. □

Determinar la presencia de errores en la transmisión es el primer paso tras la transmisión. La linealidad del código permite realizar este proceso de manera eficiente y sencilla.

Definición 1.16. Sea C un código con matriz generadora G. Definimos el dual de C como

$$C^{\perp} = \ker(G).$$

Una matriz generadora de $C^{\perp}$ se denomina una matriz de chequeo de paridad de C.

Proposición 1.17.

$$C^{\perp} = \{v \in \mathbb{F}_q^n : \langle v, c\rangle = \sum_{i=1}^{n} v_i c_i = 0, \forall c \in C\},$$

y

$$\dim(C^{\perp}) = n - \dim(C).$$

Proposición 1.18. *Sea H una matriz de chequeo de paridad de C. Entonces $v \in C$ si y solo si*

$$Hv^{\top} = 0.$$

El dual de un código contiene información relevante del código. Muchas de las propiedades de C se pueden leer directamente sobre $C^{\perp}$, y en general, podemos estudiar la teoría de códigos desde el punto de vista del dual. Muchas veces, los códigos se definen desde la comprensión del dual en lugar de una descripción directa del código. En particular, la distancia mínima se puede describir desde el dual.

PROPOSICIÓN 1.19. *Sea C un código de longitud n y H una matriz de chequeo de paridad. Si $I \subseteq [n]$, denotamos por H_I la submatriz de H formada por las columnas indexadas por I. Entonces:*

$$d(C) - 1 = \max\{t : \forall I \subseteq [n], |I| = t, \det(H_I) \neq 0\}.$$

Demostración. Sea $d = d(C)$. Sea $I \subseteq [n]$ un conjunto de cardinalidad t, y sea $A = \{H_i : i \in I\}$ el conjunto de columnas de H indexadas por I. Si A es linealmente dependiente, entonces existen coeficientes no todos cero $v_i \in \mathbb{F}_q$, $i \in I$, tales que

$$\sum_{i \in I} v_i H_i = 0.$$

Definamos al vector $w \in \mathbb{F}_q^n$ tal que $w_i = v_i$ si $i \in I$ y $w_i = 0$ en otro caso. Entonces, $Hw^{\top} = 0$, y como H es una matriz de chequeo de paridad, $w \in C$. Luego, $w = 0$, lo cual contradice la linealidad de H. Así, $d \leq t$. Por lo tanto, todo conjunto linealmente dependiente de columnas de H tiene cardinalidad al menos d, y todo conjunto de columnas de tamaño $\leq d-1$ es linealmente independiente.

Para terminar, basta observar que hay al menos un conjunto linealmente dependiente de tamaño d. Sea $w \in C$ tal que $\mathrm{wt}(w) = d$, y sea $I = \{i \in [n] : w_i \neq 0\}$. Dado que

$$Hw^{\top} = \sum_{i \in I} w_i H_i = 0,$$

entonces $\{H_i : i \in I\}$ es linealmente dependiente. □

Podemos acelerar el proceso de decodificación por vecino más cercano utilizando la *decodificación por síndrome*.

DEFINICIÓN 1.20. Sea $v \in \mathbb{F}_q^n$, y sea H la matriz de chequeo de paridad de un código C de longitud n. El síndrome de v respecto a H es

$$\mathrm{syn}(v) = Hv^{\top}.$$

Para cualquier $s \in \mathbb{F}_q^{n-k}$, decimos que $e \in \mathbb{F}_q^n$ es un líder del coset definido por s si

$$\mathrm{wt}(e) = \min\{\mathrm{wt}(v) : Hv^{\top} = s\}.$$

PROPOSICIÓN 1.21. *Sea H una matriz de chequeo de paridad de un $[n,k,d]_q$-código C. Sea $s \in \mathbb{F}_q^{n-k}$. Si existe $e \in \{v \in \mathbb{F}_q^n : Hv^{\top} = s\}$ tal que $\mathrm{wt}(e) \leq (d-1)/2$, entonces e es único.*

Demostración. Sean $e, e' \in \{v \in \mathbb{F}_q^n : Hv^{\top} = s\}$ de peso mínimo. Como $He^{\top} = He'^{\top}$, entonces $e - e' \in C$, y por lo tanto, $\mathrm{wt}(e - e') \leq \mathrm{wt}(e) + \mathrm{wt}(e') \leq d - 1$. Luego, por la definición de distancia mínima, $e - e' = 0$, y por lo tanto, e es único. □

Proposición 1.22. *Sea C un código y H una matriz de chequeo de paridad. Pruebe que la decodificación por vecino más cercano y la decodificación por síndrome, definida abajo, son equivalentes.*

Decodificación por síndrome: Sea $y \in \mathbb{F}_q^n$.

1. Calcular $\text{syn}(y)$.
2. Recuperar el líder $e \in \mathbb{F}_q^n$ del coset definido por $\text{syn}(y)$.
3. Devolver $y + e$.

Ejercicios de la sección

P.1.2.1 Sea G una matriz generadora de un código lineal binario $[n,k,d]_2$. Entonces, G tiene al menos $k \cdot d$ unos en ella.

P.1.2.2 Argumenta que en cualquier código lineal binario, o bien todas las palabras código comienzan con un 0, o exactamente la mitad de las palabras código comienzan con un 0.

P.1.2.3 En este ejercicio, veremos cómo convertir códigos arbitrarios en códigos con parámetros ligeramente diferentes:

a) Demuestra que si existe un código $[n,k,d]_\Sigma$, entonces también existe un código $[n-1,k,d-1]_\Sigma$. Específicamente, muestra cómo convertir un código $[n,k,d]_\Sigma$ C en un código $[n-1,k,d-1]_\Sigma$.

b) Para d impar, demuestra que si existe un código $(n,k,d)_2$, entonces también existe un código $[n+1,k,d+1]_2$. Específicamente, muestra cómo convertir un código $[n,k,d]_2$ C en un código $[n+1,k,d+1]_2$.

P.1.2.4 Demuestra que el espacio generado por k vectores linealmente independientes sobre $\mathbb{F}_q$ tiene tamaño exactamente q^k.

P.1.2.5 Sea G una matriz generadora y H una matriz de control de paridad del mismo código lineal de dimensión k y longitud de bloque n. Entonces, $G \cdot H^T = 0$.

P.1.2.6 Sea C un código lineal $[n,k]_q$ con una matriz generadora que no contiene columnas de ceros. Entonces, para cada posición $i \in [n]$ y $\alpha \in \mathbb{F}_q$, el número de palabras código $c \in C$ tales que $c_i = \alpha$ es exactamente q^{k-1}.

P.1.2.7 Sea C un código lineal. Entonces, demuestra que $(C^\perp)^\perp = C$.

P.1.2.8 Para cualquier código lineal C, la palabra código 0 está en ambos C y $C^\perp$. Demuestra que existe un código lineal C tal que comparte una palabra código no nula con $C^\perp$.

1.3 Cota de Singleton y enumerador de pesos

Nuestro siguiente reto es diseñar códigos $[n,k,d]$ tales que:

- n sea corto, para reducir el número de usos del canal y aumentar la transmisión de información por unidad de tiempo.
- k sea grande, para transmitir la mayor cantidad de información por cada n-usos del canal.
- d sea grande, para decodificar la mayor cantidad de errores.

Sin embargo, estos parámetros no son independientes entre sí. En particular, $\mathbb{F}_q^n$ tiene distancia mínima 1, lo que lo hace un código inútil. ¿Qué tan bueno podemos hacerlo?

Teorema 1.23. *(Cota de Singleton). Sea C un $[n,k,d]_q$-código. Entonces:*

$$d-1 \leq n-k.$$

Demostración. Si H es una matriz de chequeo de paridad de C, entonces H es de rango $n-k$, por lo que el máximo tamaño de un conjunto de columnas linealmente independiente es $n-k$. Por la proposición 1.2, tenemos el resultado. □

Corolario 1.24. *Si C es un código con distancia mínima d y $C^\perp$ tiene distancia mínima $d^\perp$, entonces:*

$$d+d^\perp \leq n+2.$$

Demostración. Por la cota de Singleton:

$$d-1 \leq n-k, \quad d^\perp-1 \leq n-(n-k).$$

Sumando desigualdades, tenemos $d+d^\perp-2 \leq n$. □

Definición 1.25. Un código $[n,k,d]_q$ tal que $d=n-k+1$ se llama un código MDS (*maximum distance separable*).

Diseñar códigos MDS no es sencillo. No conocemos todos los códigos MDS existentes, ni podemos garantizar su existencia para cualquier longitud. Sin embargo, son los mejores códigos que podemos obtener. Sus propiedades estructurales los hacen uno de los objetos más estudiados tanto a nivel de ingeniería como a nivel matemático.

Proposición 1.26. *Sea C un código MDS de longitud n y dimensión k. Para cualquier conjunto $I \subseteq [n]$ de cardinalidad $n-k+1$, existe una palabra $v \in C$ tal que $v_i \neq 0$ si y solo si $i \in I$.*

Demostración. Sea H una matriz de chequeo de paridad, y sea $I \subseteq [n]$ de cardinalidad $n-k+1$. Como H es de rango $n-k$, las columnas indexadas por I son linealmente dependientes. Por lo tanto, existe una combinación lineal no trivial de ellas, o equivalente, existe un $v \in \mathbb{F}_q^n$ tal que:

$$Hv^\top = 0,$$

y si $i \notin I$, entonces $v_i = 0$, por lo que el peso de v es a lo más $n-k+1$. Como $Hv^\top = 0$, $v \in C$, y como C es MDS, todas las entradas de v indexadas por I son no nulas. □

Proposición 1.27. *Pruebe que los siguientes son equivalentes:*

1. *C es un $[n,k,d]$-código MDS.*
2. *Si H es una matriz de chequeo de paridad de C, entonces cualquier menor de H tiene rango $n-k$.*

Demostración. Si C es MDS, entonces $d-1 = n-k$. Por la proposición 1.2, cualquier conjunto de $n-k$ columnas de H es linealmente independiente. Esto prueba $1 \Rightarrow 2$. La implicación inversa es un corolario de la proposición 1.2 y la cota de Singleton. □

El dual de un código MDS también es un código MDS.

Proposición 1.28. *Si C es un $[n,k,d]$-código MDS, entonces $C^\perp$ es MDS.*

Demostración. Sea $I \subseteq [n]$ de tamaño k, $I = \{i_1, \ldots, i_k\}$. Existe una palabra $v^{(1)} \in C$ cuyas entradas forman el conjunto $I^c \cup \{i_1\}$; podemos además suponer $v^{(1)}_{i_1} = 1$. Repetimos este proceso para cada $2 \leq j \leq k$, hasta obtener $v^{(1)}, \ldots, v^{(k)}$, tal que $v^{(j)}_{i_h} = 1$ si $h = j$, y 0 en otro caso. Luego, la proyección de C en las entradas de I es igual al espacio $\mathbb{F}_q^k$. Esto implica que cualquier subconjunto de k columnas de una matriz generadora de C es linealmente independiente. Por lo tanto, usando la proposición anterior tenemos que $C^\perp$ también es MDS. □

Proposición 1.29. *Sea C un código de distancia d y longitud n, y sea $d^\perp$ la distancia de $C^\perp$. Entonces $d + d^\perp = n+2$ si y solo si C es MDS.*

Demostración. Si C es MDS, su dual también lo es, y por lo tanto, si $k = \dim(C)$, $d = n-k+1$ y $d^\perp = k+1$. La suma da la igualdad deseada.

Ahora, si $d + d^\perp = n+2$ y C no es MDS, entonces $d \leq n-k$. Por lo tanto:

$$d + d^\perp = n+2 \leq n-k+d^\perp \Rightarrow k+2 \leq d^\perp,$$

lo cual contradice la cota de Singleton. Por lo tanto, C es MDS. □

Ejemplo 1.30. Sea $\mathbb{F}_5$ un campo de 5 elementos y sea C el código generado por:

$$G = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

El código C está compuesto por todas las combinaciones lineales de las filas de G. Para $a, b \in \mathbb{F}_5$, cada palabra código tiene la forma:

$$c = a \cdot \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \end{pmatrix} + b \cdot \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Expandiendo:

$$c = \begin{pmatrix} b & a+b & 2a+b & 3a+b & 4a+b \end{pmatrix}.$$

Dado que $\dim(C) = 2$, el código tiene $q^k = 5^2 = 25$ palabras distintas.

Distancia mínima del código C

La distancia mínima $d(C)$ es el peso mínimo de las palabras código no triviales. Observamos que cualquier combinación no trivial de las filas de G genera palabras con al menos 4 posiciones no nulas. Por lo tanto:

$$d(C) = 4.$$

Además, dado que $d(C) = n - k + 1 = 5 - 2 + 1 = 4$, el código C es un código MDS. Además, si consideramos la matriz

$$H = \begin{pmatrix} 0 & 1 & 4 & 4 & 1 \\ 0 & 1 & 2 & 3 & 4 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Tenemos que:

$$G \cdot H^T = 0.$$

Esto confirma que H es una matriz de chequeo de paridad válida para C y el código $C^\perp$ generado por H tiene:

$$\dim(C^\perp) = n - \dim(C) = 5 - 2 = 3.$$

La distancia mínima de $C^\perp$ es:

$$d(C^\perp) = n - \dim(C^\perp) + 1 = 5 - 3 + 1 = 3.$$

Por lo tanto, $C^\perp$ también es un código MDS.

Nota: Si bien la distancia mínima determina el mejor desempeño para una palabra arbitraria del código, algunas palabras pueden ser detectadas incluso si el error tiene peso que supera la capacidad de detección del código.

Los errores que no pueden ser corregidos coinciden con errores que tienen el mismo síndrome y, por lo tanto, la diferencia de cualesquiera dos elementos en el coset coincide con un error no detectable. Así, si r es una palabra del código, el número de errores de peso w que no pueden ser detectados corresponde únicamente con las palabras de peso w del código. Por lo tanto, el número de palabras que no pueden detectarse es:

$$A_w = \{v \in C : \mathrm{wt}(v) = w\}.$$

Si además asumimos que la probabilidad de observar un error en cada uso de la transmisión es, en promedio, p, entonces la probabilidad de que un error de peso w no sea detectado es:

$$A_w p^w (1-p)^{n-w}.$$

Así, la probabilidad de que no detectemos un error es:

$$\sum_{w=0}^{n} A_w p^w (1-p)^{n-w}.$$

Observe que si $1 \leq w \leq d-1$, siempre podemos detectar el error. El peor caso será cuando el número de errores w induzca el mayor A_w, pues aun si sabemos cuántos errores tenemos, tendremos $|A_w|$ opciones como posibles errores.

La probabilidad de no detectar un error es un polinomio sobre p. Esto nos conduce a analizar el **enumerador de pesos**.

Definición 1.31. Sea C un código de longitud n y para cada $w \in [n]$, defina

$$A_w = \{v \in C : \mathrm{wt}(v) = w\}.$$

El polinomio enumerador de pesos de C es el polinomio:

$$W_C(x,y) = \sum_{i=0}^{n} A_i x^i y^{n-i}.$$

Calcular el enumerador de pesos es, en general, difícil. Es un invariante del código que revela mucha de la información estructural del código, pero incluso la determinación de los coeficientes es complicada. Es importante señalar que ni siquiera podemos determinar cuándo existe un código con un enumerador de pesos específico, y más aún, no podemos elegir arbitrariamente un polinomio y aspirar a que corresponda a un código.

Así, nos gustaría encontrar códigos para los cuales calcular el enumerador sea sencillo, por ejemplo, que tenga pocos coeficientes distintos de cero.

Es importante observar que la complejidad de calcular el polinomio enumerador es #P-completo (tan difícil como calcular todas las coloraciones de una gráfica) y para un código arbitrario implica realizar $q^{\dim C}$ operaciones.

A fin de reducir la complejidad de estas operaciones, nos gustaría determinar qué códigos, relacionados con C, pueden proveer información sobre esto. El código que más relación guarda con C es su dual, y si $k = \dim C$ es muy grande, entonces $n-k$ es pequeño. El reto es, entonces, averiguar si W_C y $W_{C^\perp}$ guardan alguna relación.

Teorema 1.32. *(Identidades de McWilliams). Sea C un código de longitud n. Entonces:*

$$W_{C^\perp}(x,y) = \frac{1}{|C|} W_C(y-x, y+(q-1)x).$$

Demostración. Sea $\chi : \mathbb{F}_q \to \mathbb{C}^*$ un carácter no trivial [1]. Notemos lo siguiente:

$$\sum_{v \in C} \chi(uv^\top) = \begin{cases} |C| & \text{si } u \in C^\perp, \\ 0 & \text{en otro caso.} \end{cases}$$

[1] Sea $\mathbb{F}_q$ un campo finito con $q = p^m$ elementos (donde p es un número primo y $m \geq 1$). Un carácter no trivial $\chi : \mathbb{F}_q \to \mathbb{C}^*$ es una función que es un homomorfismo multiplicativo y es no trivial.

Esto significa que el carácter funciona como una función característica de $C^\perp$ y, por lo tanto:

$$W_{C^\perp}(x,y) = \frac{1}{|C|}\sum_{u\in\mathbb{F}_q^n}\left(\sum_{v\in C}\chi(uv^\top)\right)x^{\mathrm{wt}(u)}y^{n-\mathrm{wt}(u)}$$
$$= \frac{1}{|C|}\sum_{c\in C}\left(\sum_{u\in\mathbb{F}_q^n}\chi(uv^\top)\right)x^{\mathrm{wt}(u)}y^{n-\mathrm{wt}(u)}.$$

Dado que $uv^\top = \sum_{i=1}^n u_iv_i$, y usando las propiedades del carácter tenemos:

$$\chi(uv^t) = \prod_{i=1}^n \chi(u_iv_i) \implies W_{C^\perp}(x,y) = \frac{1}{|C|}\sum_{c\in C}\left(\sum_{u\in\mathbb{F}_q^n}\prod_{i=1}^n \chi(u_iv_i)x^{\mathrm{wt}(u_i)}y^{1-\mathrm{wt}(u_i)}\right).$$

Reagrupando,

$$W_{C^\perp}(x,y) = \frac{1}{|C|}\sum_{c\in C}\prod_{i=1}^n\left(\sum_{u\in\mathbb{F}_q}\chi(uv_i)x^{\mathrm{wt}(u)}y^{1-\mathrm{wt}(u)}\right).$$

Finalmente,

$$\sum_{u\in\mathbb{F}_q}\chi(uv_i)x^{\mathrm{wt}(u)}y^{1-\mathrm{wt}(u)} = \begin{cases} y+(q-1)x & \text{si } v_i = 0,\\ y-x & \text{si } v_i \neq 0.\end{cases}$$

Sustituyendo,

$$W_{C^\perp}(x,y) = \frac{1}{|C|}\sum_{c\in C}(y+(q-1)x)^{n-\mathrm{wt}(v)}(y-x)^{\mathrm{wt}(v)}$$

y concluye la prueba. □

Ejemplo 1.33. En $\mathbb{F}_5^2$, calcule cuántas palabras de peso $2k$ hay para cada $0 \le k \le 2$.

Sabemos que si el peso de la palabra v es par, entonces $v \in (11111)^\perp$. El enumerador de pesos del código generado por (11111) es:

$$W_C(x,y) = y^5 + x^5.$$

Por lo tanto, usando McWilliams:

$$W_{C^\perp}(x,y) = \frac{1}{2}\left((y-x)^5 + (y+x)^5\right) = y^5 + 10y^3x^2 + 5yx^4.$$

Ejercicios de la sección

p.1.3.1 Sea C el código con matriz de chequeo de paridad:

$$\begin{bmatrix} 0 & 1 & a & a^2 \\ 1 & 1 & 1 & 1 \end{bmatrix},$$

donde $a \in \mathbb{F}_4 = \mathbb{F}_2[a]$ satisface $a^2 + a + 1 = 0$. La capacidad de detección de C es 2.

Supongamos que recibimos una palabra con error $e = (1110)$. Pruebe que e puede ser detectado, pero no corregido.

P.1.3.2 Demuestre que C es MDS si y solo si cualquier conjunto de k columnas en su matriz generadora es linealmente independiente.

P.1.3.3 Demuestre que C es MDS si y solo si su código dual es MDS (suponiendo que $k < n$).

1.4 Códigos polinomiales

1.4.1 Reed-Solomon

Una de las herramientas más eficientes para diseñar códigos es a través de los **códigos de evaluación**. Exploraremos la familia de códigos que quizás son los más importante de todos: los códigos Reed-Solomon.

Definición 1.34. Sean $A = \{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{F}_q$, $0 \leq k < n$ un entero y $R = \mathbb{F}_q[x]$ el anillo de polinomios, y definamos el mapeo evaluación:

$$\mathrm{ev}_A : R \to \mathbb{F}_q^n, \quad \mathrm{ev}_A(f) = (f(\alpha_1), \ldots, f(\alpha_n)).$$

El código Reed-Solomon de grado k, $0 \leq k \leq n-1$, sobre A, se define como:

$$RS(A,k) = \mathrm{ev}_A(R_{\leq k-1}),$$

donde $R_{\leq k-1}$ denota el espacio de polinomios de grado a lo más $k-1$.

Al definir cualquier código, nos interesa calcular una matriz generadora, sus parámetros básicos y su dual.

Dado que sabemos que $R_{\leq k-1}$ es generado por los monomios $1, x, \ldots, x^{k-1}$, entonces las evaluaciones de estos monomios forman una base de $RS(A,k)$. Luego

$$G = \begin{pmatrix} \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \\ \alpha_1^{k-2} & \alpha_2^{k-2} & \cdots & \alpha_n^{k-2} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ 1 & 1 & \cdots & 1 \end{pmatrix}$$

es una matriz generadora del código.

Proposición 1.35. *Cualquier código Reed-Solomon es un código MDS.*

Demostración. Sea $C = RS(A,k)$. Sea $f \in \mathbb{F}_q[x]_{\leq k-1}$. Entonces:

$$\mathrm{wt}(\mathrm{ev}(f)) = |\{\alpha \in A : f(\alpha) \neq 0\}|.$$

Esto es equivalente a:

$$\mathrm{wt}(\mathrm{ev}(f)) = |A| - |\{\alpha \in A : f(\alpha) = 0\}|.$$

Dado que $\deg(f) \leq k-1$, el número de raíces es a lo más $k-1$. Luego:

$$\mathrm{wt}(\mathrm{ev}(f)) \geq |A| - k + 1.$$

La parte derecha coincide con la cota de Singleton para la distancia mínima. Por lo tanto, se tiene que $d(C) = |A| - k + 1$, es decir, C es MDS. □

Ejemplo 1.36. Sea $f \in \mathbb{F}_5[x]$ definido por $f = x^2(x-1)$. f tiene dos raíces y al evaluar sobre $\mathbb{F}_5$, tenemos

$$\mathrm{ev}(f) = \big(f(0), f(1), f(2), f(3), f(4)\big) = (0,0,4,3,3)$$

que es de peso $3 = 5 - 2$.

Proposición 1.37. *El dual de un código RS es un código isométrico a un código RS.*

Demostración. Tome $g = \prod_{\alpha \notin A}(x - \alpha)$. Sabemos que para cualquier $s \leq q-2$, $\sum_{\alpha \in \mathbb{F}_q} \alpha^s = 0$, por lo tanto para cualquier monomio x^s, $s < k$,

$$\sum_{\alpha \in \mathbb{F}_q} (x^{d+s} g)(\alpha) = \sum_{\alpha \in A} (x^{d+s} g)(\alpha) = 0,$$

para cualquier s tal que $d + s < q$. □

Los códigos Reed-Solomon son muy eficientes, pero están limitados por el tamaño del campo. Más aún, si la conjetura MDS es cierta, el régimen donde un código Reed-Solomon existe, es también el régimen donde los códigos MDS no triviales existen.

Una de las formas tradicionales para generar códigos de mayor longitud y aprovechar las buenas propiedades de los códigos Reed-Solomon, es a través de la concatenación.

Sea $C_{\text{in}} \subseteq \mathbb{F}_q^n$ un código de dimensión k (llamado código interior) y sea $C_{\text{out}} \subseteq \mathbb{F}_{q^k}^N$ un código de dimensión K (llamado código exterior). Observemos que el alfabeto base del código exterior es de grado la dimensión del código interior. Dado que $\mathbb{F}_{q^k}$ es también un espacio vectorial sobre $\mathbb{F}_q$, podemos asociar un mapeo lineal inyectivo entre $\mathbb{F}_{q^k}$ y C_{in}, denotémoslo E_{in}.

Así, podemos crear un código C sobre $\mathbb{F}_q$ de longitud nN, dimensión kK y distancia mínima al menos $d(C_{\text{in}})d(C_{\text{out}})$ dado por

$$C = \{(E_{\text{in}}(v_1), \ldots, E_{\text{in}}(v_N)) : v \in C_{\text{out}}\}.$$

Típicamente, C_{out} es un código MDS y en general un Reed-Solomon. Para aprovechar las ventajas que tal código da, utilizaremos una doble decodificación usando el siguiente proceso.

Sea $y \in \mathbb{F}_q^N$ la palabra recibida. Para cada $0 \leq i \leq N-1$, utilizamos un decodificador de C_{in} para corregir

$$y^i = (y_{in+1}, \ldots, y_{in+n}).$$

Si la decodificación es exitosa, tomamos el resultado de la decodificación

$$v^i = (v_{in+1}, \ldots, v_{in+n}) \in C_{\text{in}},$$

de lo contrario marcamos una falla, denotándola por el símbolo e.

Tomamos $z_i = E_{\text{in}}(v^i)$ si v^i existe y si no tomamos $z_i = e$. El vector z vive en $\mathbb{F}_q^k \cup \{e\}$. Las entradas de z que no son e, son valores correctos de una palabra código en C_{out}. Nuestro objetivo es entonces averiguar cuáles eran los símbolos correctos para las posiciones iguales a e.

En el caso de un código Reed-Solomon, esto es particularmente sencillo.

Proposición 1.38. *Sea $C = RS(A,k)$ un código Reed-Solomon, con $A = \{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{F}_q$. Sea f un polinomio de grado a lo más $k-1$ y $v = ev_A(f)$ y sea f' un polinomio de grado a lo más n tal que $d(v, ev(f')) \leq n-k$. Sea $I = \{i \in [n] \mid e_i \neq 0\}$. Definamos $g = \prod_{\alpha \in A}(x-\alpha)$ y $\ell = \prod_{i \in I}(x-\alpha_i)$. Entonces*

$$f'(x) \cdot \ell(x) = q(x)g(x) + f(x)\ell(x)$$

para algún $q(x)$.

Demostración. Tenemos que $f'(x)\ell(x)$ es un polinomio tal que $f'(\alpha_i)\ell(\alpha_i) = 0$ para toda $i \in I$. Sabemos que $f'(\alpha_i) = f(\alpha_i)$ para toda $i \notin I$ y por lo tanto

$$\ell(x)\big(f'(x) - f(x)\big)$$

se anula en cualquier $\alpha \in A$. Es decir, $x - \alpha$ divide al polinomio para cualquier $\alpha \in A$ y por lo tanto

$$g(x) \big| \ell(x)\big(f'(x) - f(x)\big),$$

es decir, existe $q(x)$ tal que $g(x)q(x) = \ell(x)\big(f'(x) - f(x)\big)$ y termina la prueba. □

Utilizando la proposición anterior, podemos terminar de corregir un código concatenado si C_{out} es un Reed-Solomon.

Ejemplo 1.39. Sea $\mathbb{F}_7$, $n = 6$, $\mathbf{x} = (1,2,3,4,5,6)$ y $k = 4$. La matriz generadora de este código Reed-Solomon, con respecto a la base canónica de $R_{<4}$, es

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 2 & 4 & 1 \\ 1 & 6 & 1 & 6 & 1 & 6 \end{bmatrix}$$

y un ejemplo de codificación es

$$3 + 2x^2 + x^3 \sim (3,0,2,1)G = (6,5,6,1,3,4).$$

Ejercicios de la sección

P.1.4.1.1 Demuestre que el dual $C^\perp$ del código en el ejemplo 1.39 no es Reed-Solomon.

1.4.2 Reed-Muller y otros códigos de evaluación

Los códigos Reed-Muller son códigos fáciles de decodificar y codificar, cuya longitud puede ser mucho más grande que el alfabeto base. Sin embargo, su distancia mínima puede ser muy baja, así no estamos considerando los mejores códigos. Su flexibilidad, los han hecho unos de los códigos más importantes.

Trabajaremos sobre un anillo de polinomios de varias variables, $R = \mathbb{F}_q[x_1, \ldots, x_m]$. Para propósitos de estas notas, tomaremos códigos Reed-Muller evaluando sobre todo el espacio, es decir, escribiremos $\mathbb{F}_q^m = \{P_1, \ldots, P_N\}$ y utilizaremos el mapeo evaluación

$$ev_m(f) = \big(f(P_1), \ldots, f(P_N)\big).$$

Para $u \in \mathbb{N}_0^m$, escribimos $x^u = x_1^{u_1} \cdots x_m^{u_m}$. Diremos que el grado de x^u es la suma de las entradas de u. El grado de un polinomio $f = \sum_{u \in \mathbb{N}_0^m} a_u x^u$ es el máximo de los grados donde $a_u \neq 0$.

Definición 1.40. El código Reed-Muller de m variables de grado s es el código dado por

$$RM_q(m,s) = ev_m(R_{\leq s}).$$

A diferencia del código Reed-Solomon, la imagen de $R_{\leq s}$ no es inyectiva bajo el mapeo evaluación. Eso implica que la dimensión no es igual al número de monomios de grado $\leq s$. Por lo que primero necesitamos entender quién es el kernel del mapeo evaluación.

Proposición 1.41. *El kernel de $ev : R \to \mathbb{F}_q^n$ es un ideal denominado el ideal anulador de $\mathbb{F}_q^m$, denotado I_m.*

Corolario 1.42. $\mathbb{F}_q^n \cong R/I_m$.

Demostración. Sea $f = \sum_{i=1}^{\infty} f_i(x_2, \ldots, x_m)(x_1 - \alpha_i)^i$. □

Proposición 1.43. $I_m = (x_i^q - x_i : 1 \leq i \leq m)$.

Demostración. Procederemos por inducción. Para el caso $m = 1$ es claro. Supongamos que es cierto para m y tomemos $f \in \mathbb{F}_q[x_1, \ldots, x_{m+1}]$. Podemos reescribir f como

$$f(x_1, \ldots, x_{m+1}) = \sum_{i=1}^{\infty} f_i(x_1, \ldots, x_m) x_i^q x_{m+1}^i.$$

Con $f_i = 0$ para casi toda i.

Podemos asumir que $\deg_{x_{m+1}} f \leq q-1$, pues

$$f - \sum_{i=0}^{q-1} x_{m+1}^i \left(\sum_j f_j : x_{m+1}^j = x_{m+1}^i \mod (x_{m+1}^q - x_{m+1}) \right) \in I_{m+1}.$$

Por lo tanto,

$$f = \sum_{i=0}^{q-1} f_i(x_1, \ldots, x_m) x_{m+1}^i.$$

Si $f_i \in I_m$ para cualquiera $0 \leq i \leq q-1$, entonces $f \in I_{m+1}$ y la prueba termina. Si existiera $0 \leq i \leq q-1$ y $P \in \mathbb{F}_q^m$ tal que $f_i(P) \neq 0$, entonces $f(P, x_{m+1})$ es un polinomio distinto de 0 que, sin embargo, se anula en todos los puntos de $\mathbb{F}_q^{m+1}$. Esto implica que su grado es al menos q, lo que es una contradicción. □

Para cualquier monomio x^u existe $x^{u'}$ tal que $x^u - x^{u'} \in I_m$ (sólo hay que hacer las reducciones en cada variable, identificando $x_i^q = x_i$). Esto implica lo siguiente.

Proposición 1.44. *Las clases de* $\Delta = \{x^u : \deg_{x_i} \leq q-1, 1 \leq i \leq m\}$ *es una base de* R/I_m.

Definición 1.45. Decimos que f es reducido si el soporte de f está contenido en Δ.

Corolario 1.46. *Si* f *es un polinomio de grado* d*, entonces existe* $f' \in Span(\Delta)$ *tal que* $f - f'$ *pertenece a* I_m*, donde el grado de* f' *es a lo más* d.

Proposición 1.47. *El código* $RM_q(m,s)$ *es un código de longitud* q^m *y dimensión*

$$|\Delta_{\leq s}| = \sum_{i=0}^{n} (-1)^i \binom{n+d-iq}{d-iq}.$$

Antes de atacar la distancia mínima, intentemos describir el dual de un código Reed-Muller. Observemos lo siguiente: sea x^u un monomio de grado a lo más $m(q-1)-1$. Notemos que

$$\sum_{\alpha \in \mathbb{F}_q^m} \alpha^u = \sum_{\alpha \in \mathbb{F}_q^m} \prod_{i=1}^{m} \alpha_i^{u_i} = \prod_{i=1}^{m} \left(\sum_{\alpha_i \in \mathbb{F}_q} \alpha_i^{u_i} \right).$$

Como $\deg x^u \leq m(q-1)-1$, entonces existe $u_i \leq q-2$ para alguna i y por lo tanto $\sum_{\alpha_i \in \mathbb{F}_q} \alpha_i^{u_i} = 0$, por lo tanto, $\sum_{\alpha \in \mathbb{F}_q^m} \alpha^u = 0$. Esto nos permite garantizar quién es el dual del RM.

Proposición 1.48. *Sea* $C = RM_q(m,d)$*. Entonces* $C^\perp = RM_q(m, m(q-1)-d-1)$.

Hasta ahora las técnicas que usamos en el caso de una variable se han podido traducir sin demasiados problemas. Sin embargo, para calcular la distancia mínima, el grado ya no es una cota sobre el número de ceros del polinomio.

Ejemplo 1.49. Sea $f = xy$ y $g = x^2 - x$ en $\mathbb{F}_3[x,y]$. Los ceros de f son $\{0,1\} \times \mathbb{F}_3 \cup \mathbb{F}_3 \times \{0\}$, es decir, 5. Los ceros de g son $\{0,1\} \times \mathbb{F}_3$, es decir, 6. No existen polinomios de menor grado que anulen a esos puntos, por lo tanto f y g son mínimos en sus respectivos ideales, pero no contienen el mismo número de ceros.

Hay, sin embargo, una cota que recupera el detalle central del teorema fundamental del álgebra: la cota de footprint. Para derivarla, primero necesitamos establecer un orden en Δ.

Definición 1.50. El orden lexicográfico $<_{\text{lex}}$ sobre Δ viene dado por las relaciones $x^u < x^v$ si $u - v$ tiene la primera entrada distinta de cero positiva.

El término líder de un polinomio f es el monomio más grande bajo el orden lexicográfico y se denota $\text{in}(f)$.

Una parte importante para poder generalizar, es entender que la relación entre conjuntos finitos de puntos e ideales, es unívoca salvo el ideal I_m. El siguiente teorema caracteriza esto.

Teorema 1.51. *(Hilbert Nullstellensatz para campos finitos). Sea $A \subset \mathbb{F}_q^m$. Supongamos que existen $f_1, \ldots, f_r \in R$ tal que $A = \{P \in \mathbb{F}_q^m : f_i(P) = 0, 1 \leq i \leq r\}$. Entonces*

$$(f \in R : f(P) = 0, \forall P \in A) = I_m + (f_1, \ldots, f_r).$$

En particular, los ceros de un polinomio f coinciden con los ceros del ideal $I_m + (f)$ y este último contiene a todos los polinomios que se desvanecen en los ceros de f. Al igual que antes, esto significa que

$$\dim R/(I_m + (f)) = |Z(f)| = |\{P \in \mathbb{F}_q^m : f(P) = 0\}|.$$

Si acotamos la dimensión de $R/(I_m + (f))$ para cualquier polinomio de grado d, entonces podemos extender el resultado que conocemos como teorema fundamental del álgebra. En particular, esta dimensión para el caso de una variable es precisamente dicho teorema. Sin embargo, acotar esta dimensión puede ser complicado, dado que necesitamos conocer un conjunto generador de $(I_m + (f))$ con propiedades específicas, pues aunque siempre podemos elegir un conjunto generador monomial en las clases de $R/(I_m + (f))$, no significa que sean linealmente independientes, a diferencia de I_m. Sin embargo, encontrando al menos este conjunto generador monomial, podemos acotar la dimensión del espacio.

La cota del footprint hace precisamente esto.

Teorema 1.52. *(Cota del footprint). Sea $f \in R$ reducido. Si $ev_m(f)$ es de peso menor a n, entonces*

$$\dim R/(I_m + (f)) \leq \dim R/(x_1^q, \ldots, x_n^q, in(f)) \leq \dim R/I_m.$$

Demostración. Denotemos por $\Delta(f) = \{x^u \in \Delta : \text{in}(f) \nmid x^u\}$. Si $h \in R$, sabemos que existe $\tilde{h}$ reducida tal que $h - \tilde{h} \in I_m$. Sea $\tilde{h}_f = \sum_{x^u \in \Delta \cap supp(\tilde{h})} \tilde{h}_u x^u$. $\tilde{h}_f$ es divisible por $\text{in}(f)$, así que definamos $g = \frac{\tilde{h}_f}{\text{in}(f)} f$.

Tenemos entonces que $h - g$ está soportado sobre $\Delta(f)$ y $h - \tilde{h} + g \in (I_m + (f))$, por lo tanto los elementos de $\Delta(f)$ forman un conjunto generador en $R/(I_m + (f))$. Notemos, por otro lado, que $\Delta(f)$ es una base de $R/(x_1^q, \ldots, x_n^q, \text{in}(f))$. La prueba termina al observar que $|\Delta(\text{in}(f))| \leq |\Delta| = \dim R/I_m$. □

En este momento quizás sea útil observar que los monomios y sus ideales están en relación con el espacio $\mathbb{Z}_0^m$. No es difícil probar que si $I = (x^{u_1}, \ldots, x^{u_r})$ es un ideal monomial, entonces

$$x^u \in I \iff u_i \leq u, \text{ para alguna } 1 \leq i \leq r.$$

Esto da intuición sobre el siguiente hecho.

Proposición 1.53. *Sea $x^u \in \Delta$ un monomio. Entonces*

$$|\Delta(x^u)| = q^m - \prod_{i=1}^{m}(q - u_i).$$

Demostración. Sea $\nabla(x^u) = \{x^v \in \Delta : x^u | x^v\}$. Cualquier elemento $v \in \mathbb{N}_0^m$ es tal que $u_i \leq v_i \leq q-1, \forall\, i \leq m$.

Equivalentemente, un v satisfaciendo estas condiciones implica que $x^v \in \nabla(x^u)$. La cantidad de tales v es

$$\prod_{i=1}^{m}(q - 1 - u_i + 1).$$

Tomando el complemento tenemos la conclusión. □

Corolario 1.54. *Para un polinomio f reducido, si $x^u = \text{in}(f)$ entonces:*

$$\text{wt}(f) \geq \prod_{i=1}^{m}(q - u_i).$$

Demostración. La cota del footprint dice que

$$n - \text{wt}(f) = \dim R/(I_m + (f)) \leq \dim R/(x_1^q, \ldots, x_m^q, \text{in}(f)) = |\Delta(\text{in}(f))|,$$

de donde se tiene el resultado. □

Definición 1.55. f un polinomio reducido con $x^u = \text{in}(f)$. Denotamos por

$$Fb(f) = \prod_{i=1}^{m}(q - u_i).$$

Si tomamos el mínimo de esos productos para cuando x^u es un monomio de grado d, tendremos una cota para la distancia mínima del código Reed-Muller. Necesitaremos los siguientes lemas.

Lema 1.56. *Sean x^u y x^v dos monomios en Δ. Si $x^u | x^v$, entonces*

$$Fb(x^u) \geq Fb(x^v).$$

Lema 1.57. *Si $x^u \in \Delta$ es tal que $1 \leq u_j \leq q-1$, entonces*

$$Fb(x^u) \geq Fb\left(\frac{x_i}{x_j}x^u\right).$$

Demostración. Observemos que

$$Fb(x^u)\frac{q-u_i-1}{q-u_i}\frac{q-u_j+1}{q-u_j}Fb\left(\frac{x_i}{x_j}x^u\right).$$

Además

$$(q-u_i)(q-u_j) \geq (q-u_i)(q-u_j)+u_j-u_i-1 = (q-u_i-1)(q-u_j+1),$$

de donde se sigue el resultado. □

Teorema 1.58. *Sea $C = RM_q(m,s)$ un código Reed-Muller. Escribamos $s = h(q-1)+l$, con $0 \leq h \leq m$ y $0 \leq l \leq q-2$. Entonces*

$$d(C) = (q-l)q^{m-h-1}.$$

Demostración. Sabemos que si f es un polinomio de grado s entonces $\mathrm{in}(f)$ es un monomio de grado a lo más s. Sea x^u un monomio de grado s tal que $x^u \in \Delta \cap (\mathrm{in}(f))$. Por el lema 1.56

$$Fb(f) \geq Fb(x^u).$$

Dado que $Fb(x^u)$ es simétrico respecto a cualquier permutación de las entradas de u, podemos asumir que $u_1 \geq u_2 \geq \cdots \geq u_m$. Aplicando varias veces el lema 1.57, sabemos que

$$Fb(x^u) \geq Fb(x_1^{q-1}x_2^{q-1}\cdots x_h^{q-1}x_{h+1}^{l}) = (q-l)q^{m-h-1}.$$

Por lo tanto,

$$\mathrm{wt}(\mathrm{ev_m}(f)) \geq (q-l)q^{m-h-1}.$$

Recorriendo sobre todos los polinomios reducidos de grado a lo más s, tenemos que

$$d(C) \geq (q-l)q^{m-h-1}.$$

Finalmente, sea $\mathbb{F}_q = \{\alpha_1,\ldots,\alpha_q\}$. El polinomio $F = \prod_{j=1}^{l}(x_{h+1}-\alpha_j)\prod_{i=h+1}^{m}(x_i^{q-1}-1)$ es de grado s y los únicos puntos donde no se anula son $\{0\}^h \times \{\alpha_j : l+1 \leq j \leq q\} \times \mathbb{F}_q^{m-h-1}$, por lo que $\mathrm{ev_m}(F)$ tiene el mínimo peso posible y se tiene la igualdad. □

Corolario 1.59. *El máximo número de ceros que un polinomio de grado s en $\mathbb{F}_q[x_1,\ldots,x_m]$ puede tener es*

$$q^m - (q-l)q^{m-h-1}$$

donde $s = h(q-1)+l$.

Para el caso $m = 1$, lo anterior es $q-(q-l) = l$, que es el grado del polinomio.

Ejercicios de la sección

P.1.4.2.1 Encuentre los parámetros y escriba todos los vectores del código Reed-Muller $RM_q(0,m)$.

P.1.4.2.2 Demuestre que $RM_2(m,m) = \mathbb{F}_2^m$, el código binario trivial de longitud 2^m.

P.1.4.2.3 ¿Cómo definiría "$RM_q(-1,m)$", que debería ser el dual de $RM_q(m,m)$?

Capítulo 2

Preliminares del análisis funcional finito-dimensional

Los siguientes temas pueden ser encontrados usualmente en libros del álgebra lineal, análisis funcional o teoría de operadores (por ejemplo, ver [6, 7, 11, 12]). Los espacios de Hilbert ocupan un lugar especial de la familia de los espacios de Banach, cuya estructura geométrica hereda múltiples propiedades de espacios euclidianos. Los espacios de Hilbert están caracterizados por tener un producto interno[1] que permite definir la ortogonalidad de los vectores, planos, proyecciones ortogonales, bases ortonormales, ángulos, entre otros.

2.1 Espacios de Banach y Hilbert

Iniciamos con espacios normados debido a que pueden provenir de espacios con producto interno y fueron desarrollados en los trabajos de S. Banach junto con otros autores. A no ser que se especifique, los espacios vectoriales que se consideran en este trabajo son de dimensión finita y sobre el campo de los números complejos $\mathbb{C}$.

Definición 2.1. Una *norma* sobre un espacio vectorial $\mathcal{L}$ es una función no negativa $\|\cdot\| : \mathcal{L} \to \mathbb{R}_{\geq 0}$ que satisface lo siguiente[2]:

1. $\|x\| = 0$ si y solo si $x = 0$,
2. $\|\alpha x\| = |\alpha| \, \|x\|$, con $\alpha \in \mathbb{C}$,
3. $\|x + y\| \leq \|x\| + \|y\|$.

Al par $(\mathcal{L}, \|\cdot\|)$ se le conoce como *espacio vectorial normado* (o simplemente espacio normado o de Banach[3]).

[1] En algunas obras, al producto interno también le llaman producto escalar o producto punto.

[2] Si se omite la primera condición, la función $\|\cdot\|$ se le conoce como *semi-norma.*

[3] En dimensión infinita se le agrega la condición de completez, i.e., si cualquier sucesión de Cauchy es convergente en $\mathcal{L}$.

Ejemplo 2.2. Para $p \in [1,\infty)$, los siguientes son ejemplos de espacios de Banach:

1. El espacio $(\mathbb{C}^n, \|\cdot\|_p)$, donde

$$\|x\|_p = \left(\sum_{j=1}^{n} |x_j|^p \right)^{1/p}, \quad x = (x_j)_{j=1}^n \in \mathbb{C}^n . \tag{2.1}$$

2. El espacio $(\mathbb{C}^n, \|\cdot\|_\infty)$, donde

$$\|x\|_\infty = \sup_{j=1,\dots,n} |x_j| , \quad x = (x_j)_{j=1}^n \in \mathbb{C}^n .$$

Definición 2.3. Un *producto interno* sobre un espacio vectorial $\mathcal{H}$ es una aplicación $\langle \cdot,\cdot \rangle \colon \mathcal{H} \times \mathcal{H} \to \mathbb{C}$ que satisface lo siguiente[4]:

$$\begin{aligned} \langle f, \alpha g + \beta h \rangle &= \alpha \langle f,g \rangle + \beta \langle f,h \rangle , \quad \alpha,\beta \in \mathbb{C} && \textit{(lineal en la } 2^a \textit{ componente)} \\ \langle f,g \rangle &= \overline{\langle g,f \rangle} , && \textit{(hermitiana)} \\ \langle f,f \rangle &> 0 , \quad f \neq 0 . && \textit{(positiva definida)} \end{aligned}$$

Al par $(\mathcal{H}, \langle \cdot,\cdot \rangle)$ se le conoce como *espacio vectorial con producto interno* (o simplemente espacio con producto interno o de Hilbert[5]).

Ejemplo 2.4. Los siguientes son ejemplos de espacios de Hilbert:

1. El espacio $(\mathbb{C}^n, \langle \cdot,\cdot \rangle)$, con

$$\langle f,g \rangle = \sum_{j=1}^{n} \overline{f}_j g_j , \quad f = (f_j)_{j=1}^n, g = (g_j)_{j=1}^n \in \mathbb{C}^n .$$

2. El espacio de matrices cuadradas con entradas en los complejos $(M_n(\mathbb{C}), \langle \cdot,\cdot \rangle)$, con

$$\langle x,y \rangle = \operatorname{tr}(x^* y) , \quad x,y \in M_n(\mathbb{C}) ,$$

donde x^* representa la traspuesta conjugada de x.

Observación 2.5. Todo producto interno $\langle \cdot,\cdot \rangle$ en $\mathcal{H}$ induce una norma dada por:

$$\|f\| = \sqrt{\langle f,f \rangle} , \quad f \in \mathcal{H} . \tag{2.2}$$

Además, se cumple lo siguiente de manera directa de (2.2);

$$\|f+g\|^2 = \|f\|^2 + \|g\|^2 + 2\operatorname{Re} \langle f,g \rangle \tag{2.3}$$

[4] Algunos autores consideran la primera propiedad del producto interno como lineal en la primera componente.

[5] En dimensión infinita se le agrega la condición de completez, i.e., si cualquier sucesión de Cauchy es convergente en $\mathcal{H}$.

Una norma se dice que proviene o es inducida por un producto interno si satisface (2.2). De ahora en adelante consideramos la norma en $\mathcal{H}$ inducida por su producto interno.

Proposición 2.6 (Desigualdad de Cauchy-Schwarz). *Para $f,g \in \mathcal{H}$, se cumple que*

$$|\langle f,g\rangle| \leq \|f\|\,\|g\|\,, \tag{2.4}$$

con igualdad si y solo si f es múltiplo escalar de g o viceversa.

Demostración. Si $\langle f,g\rangle = 0$ entonces se sigue directo (2.4), con igualdad si alguno de f,g es cero. Ahora, si $\langle f,g\rangle \neq 0$ se tiene que $f,g \neq 0$ y definiendo

$$\lambda = \frac{|\langle f,g\rangle|}{\|g\|^2} > 0\,; \qquad \alpha = \frac{|\langle f,g\rangle|}{\langle f,g\rangle} \in \mathbb{C}\,,$$

se sigue de (2.3) que

$$0 \leq \|f-\lambda\alpha g\|^2 = \|f\|^2 + \lambda^2\,|\alpha|^2\,\|g\|^2 - 2\lambda\,\mathrm{Re}(\alpha\,\langle f,g\rangle) = \|f\|^2 - \frac{|\langle f,g\rangle|^2}{\|g\|^2}\,,$$

de donde se sigue (2.4). La afirmación de la igualdad es directa. □

Para $f,g \in \mathcal{H}$, las siguientes igualdades son usuales en espacios de Hilbert:

$$\|f+g\|^2 + \|f-g\|^2 = 2\left(\|f\|^2 + \|g\|^2\right)\,; \qquad \text{(ley del paralelogramo)} \tag{2.5}$$

$$\langle f,g\rangle = \frac{1}{4}\sum_{k=0}^{3} i^k \left\|i^k f + g\right\|^2\,. \qquad \text{(identidad de polarización)} \tag{2.6}$$

No toda norma proviene de un producto interno. De hecho, lo siguiente caracteriza a las normas que provienen de productos internos.

Teorema 2.7. *Una norma proviene de un producto interno si y solo si satisface la identidad del paralelogramo* (2.5).

Demostración. Si una norma proviene de un producto interno entonces tiene la estructura de (2.2), satisface (2.3) y de manera directa cumple la ley del paralelogramo (2.5).

Inversamente, si una norma $\|\cdot\|$ en $\mathcal{H}$ satisface la ley del paralelogramo, entonces la aplicación $\langle\cdot,\cdot\rangle\colon \mathcal{H}\times\mathcal{H}\to\mathbb{C}$ dada por $\langle f,g\rangle = \frac{1}{4}\sum_{k=0}^{3} i^k \left\|i^k f+g\right\|^2$ es un producto interno para $\mathcal{H}$ (ejercicio p.2.1.5), de donde

$$\langle f,f\rangle = \frac{1}{4}\sum_{k=1}^{4} i^k \left|i^k+1\right|^2 \|f\|^2 = \frac{1}{4}\sum_{k=1}^{4} 2i^k(1+\mathrm{Re}(i^k))\,\|f\|^2 = \|f\|^2\,.$$

Por lo tanto $\|f\| = \sqrt{\langle f,f\rangle}$. □

Definición 2.8. Decimos que $\mathcal{F} \subset \mathcal{H}$ es un subespacio (denotado por $F \leq \mathcal{H}$) si es un conjunto lineal, es decir, si satisface

$$\alpha f + \beta g \in \mathcal{F}, \quad \text{para todo} \quad f, g \in \mathcal{F}, \quad \alpha, \beta \in \mathbb{C}.$$

Un subespacio es en sí un espacio de Hilbert, con el producto interno heredado de $\mathcal{H}$.

Definición 2.9. Se define el generado de un conjunto $M \subset \mathcal{H}$ como

$$\operatorname{span} M = \bigcap_{\substack{M \subset B \\ B \leq \mathcal{H}}} B,$$

el cual es el subespacio más pequeño que contiene a M. Además, se caracteriza por ser el espacio de todas las combinaciones finitas de elementos en M (ver ejercicio p.2.1.6).

Observación 2.10. Si $F \leq \mathcal{H}$ entonces $\operatorname{span} F = F$. Ciertamente, $F \subset \operatorname{span} F$ por definición y $\operatorname{span} F \subset F$ por ser el más pequeño que contiene a F.

Dos elementos $f, g \in \mathcal{H}$ son ortogonales, denotado por $f \perp g$, si $\langle f, g \rangle = 0$. Para $\mathcal{F}, \mathcal{G} \subset \mathcal{H}$, se cumple que $\mathcal{F} \perp \mathcal{G}$, si $\langle f, g \rangle = 0$ para cada $f \in \mathcal{F}$ y $g \in \mathcal{G}$.

Para $\mathcal{G} \subset \mathcal{H}$, se denota el complemento ortogonal de $\mathcal{G}$ como

$$\mathcal{G}^{\perp} := \{h \in \mathcal{H} : h \perp g, \quad \forall g \in \mathcal{G}\}.$$

Es directo verificar que $\mathcal{G}^{\perp} \leq \mathcal{H}$.

Proposición 2.11. *Para $h \in \mathcal{H}$ y $\mathcal{F}, \mathcal{G} \subset \mathcal{H}$, lo siguiente se cumple:*

(1) Si $h \perp \mathcal{G}$ entonces $h \perp \operatorname{span} \mathcal{G}$. Además, si $\operatorname{span} \mathcal{G} = \mathcal{H}$ entonces $h = 0$.

(2) Si $\mathcal{F} \subset \mathcal{G}$ entonces $G^{\perp} \subset \mathcal{F}^{\perp}$.

Demostración. (1): Si $h \perp \mathcal{G}$, entonces para $f = \sum_{j=1}^{n} \alpha_j g_j \in \operatorname{span} \mathcal{G}$, con $g_j \in \mathcal{G}$ y $\alpha_j \in \mathbb{C}$,

$$\langle h, f \rangle = \sum_{j=1}^{n} \alpha_j \langle h, g_j \rangle = 0, \tag{2.7}$$

de donde se sigue que $h \perp \operatorname{span} \mathcal{G}$. Si además $\operatorname{span} \mathcal{G} = \mathcal{H}$, haciendo $f = h$ en (2.7) se llega a $\|h\|^2 = \langle h, h \rangle = 0$, i.e., $h = 0$.

(2): Si $h \in \mathcal{G}^{\perp}$, entonces $h \perp \mathcal{G}$, o bien, $h \perp \mathcal{F}$, ya que $\mathcal{F} \subset \mathcal{G}$. Por lo tanto, $h \in \mathcal{F}^{\perp}$. □

Definición 2.12. Dos subespacios $\mathcal{F}, \mathcal{G}$ se dicen ser *linealmente independientes* (abreviado l.i.) si $\mathcal{F} \cap \mathcal{G} = \{0\}$. Además,

$$\mathcal{F} \dotplus \mathcal{G} := \{f + g : f \in \mathcal{F}, g \in \mathcal{G} \ \text{ y } \ \mathcal{F} \cap \mathcal{G} = \{0\}\}. \qquad \textit{(suma directa)}$$

$$\mathcal{F} \oplus \mathcal{G} := \mathcal{F} \dotplus \mathcal{G}, \quad \textit{tal que} \quad \mathcal{F} \subset \mathcal{G}^{\perp}. \qquad \textit{(suma ortogonal)}$$

$$\mathcal{F} \ominus \mathcal{G} := \mathcal{F} \cap \mathcal{G}^{\perp}. \qquad \textit{(diferencia directa)}$$

De aquí se verifica que $\mathcal{F}^{\perp} = \mathcal{H} \ominus \mathcal{F}$.

Un conjunto $\{f_k\}_{k=1}^n \subset \mathcal{H}$ se dice ser *linealmente independiente* (abreviado l.i.) si para $\{\alpha_k\}_{k=1}^n \subset \mathbb{C}$ tal que

$$\sum_{k=1}^{n} \alpha_k f_k = 0\,, \quad \text{implica} \quad \alpha_1 = \cdots = \alpha_n = 0\,.$$

Además, $\{f_k\}_{k=1}^n$ se dice ser *ortogonal* si sus elementos son mutuamente ortogonales. Mas aún, es *ortonormal* si es *ortogonal* y sus elementos son de norma uno.

Lo siguiente es una consecuencia directa de (2.3).

Teorema 2.13 (Teorema de Pitágoras generalizado). *Dada un conjunto $\{f_k\}_{k=1}^n \subset \mathcal{H}$ ortogonal, se tiene que*

$$\left\| \sum_{k=1}^{n} f_k \right\|^2 = \sum_{k=1}^{n} \|f_k\|^2\,. \tag{2.8}$$

Definición 2.14. Un conjunto $\{e_k\}_{k=1}^n \subset \mathcal{H}$ es una *base* para $\mathcal{H}$ si es l.i. y genera a $\mathcal{H}$, i.e., $\operatorname{span}\{e_k\}_{k=1}^n = \mathcal{H}$. Si además $\{e_k\}_{k=1}^n$ es ortonormal entonces se dice ser *base ortonormal* (abreviado b.o.n.) para $\mathcal{H}$.

Un espacio de Hilbert no trivial siempre admite una base y gracias al proceso de ortogonalización de Gram-Schmidt, se puede garantizar la existencia de una b.o.n. Además,

1. Todas las b.o.n.'s en un espacio de Hilbert tienen la misma cardinalidad, la cual representa la dimensión del espacio.
2. Dos espacios de Hilbert son isométricamente isomorfos si y solo si sus bases tienen la misma cardinalidad.
3. Cualquier espacio de Hilbert de dimensión n es isométricamente isomorfo a $\mathbb{C}^n$.

Proposición 2.15. *Si $\{e_k\}_{k=1}^n$ es b.o.n. para $\mathcal{H}$ y $h \in \mathcal{H}$, entonces*

$$h = \sum_{k=1}^{n} \langle e_k, h\rangle\, e_k \quad y \quad \|h\|^2 = \sum_{k=1}^{n} |\langle e_k, h\rangle|^2\,. \tag{2.9}$$

Demostración. Como $h = \sum_{k=1}^n h_k e_k$, con $\{h_k\}_{k=1}^n \subset \mathbb{C}$, se sigue que

$$\langle e_j, h\rangle = \sum_{k=1}^{n} h_k \langle e_j, e_k\rangle = h_j\,, \quad j = 1, \ldots, n\,,$$

de donde se obtiene la primera igualdad de (2.9), mientras que la segunda igualdad es consecuencia directa de (2.8). □

Los coeficientes en la primera igualdad de (2.9) son conocidos como los *coeficientes de Fourier* de h, mientras que la segunda igualdad en (2.9) se le conoce como *identidad de Parseval*.

Teorema 2.16 (Teorema de proyección). *Si $\mathcal{F} \leq \mathcal{H}$, entonces para cada $h \in \mathcal{H}$, existe una única representación $h = f + g$, donde $f \in \mathcal{F}$ y $g \in \mathcal{F}^{\perp}$. Por lo tanto,*

$$\mathcal{H} = \mathcal{F} \oplus \mathcal{F}^{\perp}.$$

Demostración. Como $\mathcal{F}$ es un espacio de Hilbert, entonces tiene una b.o.n. $\{e_k\}_{k=1}^{m}$. Para $h \in \mathcal{H}$, considera $f = \sum_{k=1}^{m} \langle e_k, h\rangle e_k \in \mathcal{F}$ y $g = h - f$. Entonces, para $j = 1, \ldots, m$,

$$\langle e_j, g\rangle = \langle e_j, h - f\rangle = \langle e_j, h\rangle - \sum_{k=1}^{m} \langle e_k, h\rangle \langle e_j, e_k\rangle = 0,$$

de donde se sigue que $g \in \mathcal{F}^{\perp}$ y $h = f + g$. Para la unicidad, si $h = f_1 + g_1$ con $f_1 \in \mathcal{F}$ y $g_1 \in \mathcal{F}^{\perp}$, entonces $0 = f - f_1 + g - g_1$ y de (2.8) se sigue que

$$0 = \|f - f_1 + g - g_1\|^2 = \|f - f_1\|^2 + \|g - g_1\|^2,$$

es decir $\|f - f_1\| = 0 = \|g - g_1\|$. Por lo tanto $f_1 = f$ y $g_1 = g$. □

Ejercicios de la sección

P.2.1.1 Muestre que $\langle 0, g\rangle = 0$ para todo $g \in \mathcal{H}$. Además, $\langle u, u\rangle = 0$ si y solo si $u = 0$.

P.2.1.2 Muestre que (2.2) en efecto es una norma para $\mathcal{H}$.

P.2.1.3 Muestre la ley del paralelogramo (2.5) e identidad de polarización (2.6).

P.2.1.4 Muestre que la norma $p \in [1, \infty)$ dada por (2.1) proviene de un producto interno si y solo si $p = 2$.

P.2.1.5 Muestre que la aplicación

$$\begin{aligned} \langle \cdot, \cdot \rangle \colon \mathcal{H} \times \mathcal{H} &\to \mathbb{C} \\ (f, g) &\mapsto \frac{1}{4} \sum_{k=0}^{3} i^k \left\| i^k f + g \right\|^2, \end{aligned}$$

define un producto interno en $\mathcal{H}$, donde $\|\cdot\|$ es una norma que satisface la ley del paralelogramo (2.5).

P.2.1.6 Para un conjunto dado $M \subset \mathcal{H}$ muestre que

a) $\operatorname{span} M = \left\{ \sum_{j=1}^{n} \alpha_j m_j \,:\, \alpha_j \in \mathbb{C}, m_j \in M, n \in \mathbb{N} \right\}$.

b) $(M^{\perp})^{\perp} = \operatorname{span} M$.

2.2 Teoría de operadores lineales

2.2.1 El álgebra de von Neumann $\mathcal{B}(\mathcal{H})$

Se estudia en esta sección algunos conceptos de operadores lineales con dominio todo el espacio $\mathcal{H}$ y rango en $\mathcal{H}$. Por simplificación estándar, escribimos Tf en vez de $T(f)$.

Definición 2.17. Decimos que una aplicación $T\colon \mathcal{H} \to \mathcal{H}$ es un *operador lineal* en $\mathcal{H}$ (o simplemente operador) si

$$T(\alpha f + g) = \alpha T f + Tg, \quad \alpha \in \mathbb{C}, f, g \in \mathcal{H},$$

donde

$$\mathcal{R}(T) := \{Tf : f \in \mathcal{H}\} \quad \text{y} \quad \mathcal{N}(T) := \{f \in \mathcal{H} : Tf = 0\},$$

representan el *rango* y *núcleo* de T, respectivamente, los cuales son subespacios en $\mathcal{H}$.

Se denota por $\mathcal{B}(\mathcal{H})$ al conjunto de todos los operadores lineales en $\mathcal{H}$. Para dos operadores $T, S \in \mathcal{B}(\mathcal{H})$ y $\alpha \in \mathbb{C}$ las operaciones $\alpha T, T+S, TS \in \mathcal{B}(\mathcal{H})$, donde

$$(\alpha T)f = \alpha T f; \quad (T+S)f = Tf + Sf; \quad (TS)f = T(Sf), \tag{2.10}$$

representan la multiplicación por escalar, suma y composición de operadores, respectivamente. El operador identidad $I \in \mathcal{B}(\mathcal{H})$ viene dado por $If = f$, mientras que el operador cero $O \in \mathcal{B}(\mathcal{H})$ como $Of = 0$. Para un operador $T \in \mathcal{B}(\mathcal{H})$ que es uno-a-uno (o equivalente a $\mathcal{N}(T) = \{0\}$, ver ejercicio p.2.2.1) su inversa está bien definida en $\mathcal{B}(\mathcal{H})$, se representa por T^{-1} y es el único operador que satisface $T^{-1}T = TT^{-1} = I$.

Observación 2.18 (Identidad de polarización). Para $T \in \mathcal{B}(\mathcal{H})$ lo siguiente se cumple:

$$\langle g, Tf \rangle = \frac{1}{4} \sum_{k=0}^{3} i^k \left\langle f + i^k g, T\left(f + i^k g\right) \right\rangle, \quad f, g \in \mathcal{H}. \tag{2.11}$$

Teorema 2.19. *Para un operador $T \in \mathcal{B}(\mathcal{H})$, los siguientes son equivalentes:*

(a) T es el operador cero.

(b) $\langle f, Tf \rangle = 0$ para todo $f \in \mathcal{H}$.

(c) $\langle g, Tf \rangle = 0$ para todo $f, g \in \mathcal{H}$.

Demostración. (a)⇒(b): Es directo. (b)⇒(c): Se sigue de (2.11). (c)⇒(a): Para $g = Tf$, se tiene que $0 = \langle Tf, Tf \rangle = \|Tf\|^2$, lo que implica $Tf = 0$, para todo $f \in \mathcal{H}$. □

Observación 2.20. El teorema 2.19 no siempre es válido si el espacio $\mathcal{H}$ es real. En efecto, para $\mathbb{R}^2$, con producto interno $\langle x,y\rangle = x_1y_1 + x_2y_2$, con $x=(x_1,x_1), y=(y_1,y_2)\in\mathbb{R}^2$,

$$\begin{aligned} T\colon \mathbb{R}^2 &\to \mathbb{R}^2 \\ (x_1,x_2) &\mapsto (-x_2,x_1) \end{aligned}$$

es un operador lineal que cumple $\langle x, Tx\rangle = 0$, para todo $x\in\mathbb{R}^2$, pero $T\neq O$.

Proposición 2.21. *Si $T\in\mathcal{B}(\mathcal{H})$ entonces existe $C\geq 0$ tal que*

$$\|Tf\| \leq C\|f\|\,, \quad \textit{para todo } f\in\mathcal{H}\,. \tag{2.12}$$

Demostración. Considere $\{e_j\}_{j=1}^n$ una b.o.n. para $\mathcal{H}$ y defina $M = \max\{\|Te_j\|\}_{j=1}^n$. De esta manera, para $f=\sum_{j=1}^n f_j e_j\in\mathcal{H}$, con $\{f_j\}_{j=1}^n\subset\mathbb{C}$, se sigue que

$$\|Tf\| \leq \sum_{j=1}^n |f_j|\,\|Te_j\| \leq M\sum_{j=1}^n |f_j| \leq Mn\|f\|\,,$$

que haciendo $C=Mn$, se llega a (2.12). □

Gracias a (2.12) uno puede definir una norma en $\mathcal{B}(\mathcal{H})$, dada por

$$\|T\| := \max_{\substack{f\in\mathcal{H}\\ \|f\|=1}} \|Tf\|\,, \quad T\in\mathcal{B}(\mathcal{H})\,, \tag{2.13}$$

la cual satisfaces la *propiedad sub-multiplicativa*

$$\|TS\| \leq \|T\|\,\|S\|\,, \quad T,S\in\mathcal{B}(\mathcal{H})\,. \tag{2.14}$$

En efecto, para T y S distintos del operador cero (en otro caso es directo),

$$\begin{aligned} \|TS\| &= \max_{\substack{f\in\mathcal{H}\\ \|f\|=1}} \|TSf\| \leq \max_{\substack{f\in\mathcal{H}\\ \|f\|=1}} \frac{\|TSf\|}{\|Sf\|}\,\|Sf\| \\ &\leq \left(\max_{\substack{g\in\mathcal{H}\\ \|g\|=1}} \|Tg\|\right)\left(\max_{\substack{f\in\mathcal{H}\\ \|f\|=1}} \|Sf\|\right) = \|T\|\,\|S\|\,. \end{aligned}$$

Definición 2.22. Definimos el *adjunto* de $T\in\mathcal{B}(\mathcal{H})$ como la aplicación $T^*\colon\mathcal{H}\to\mathcal{H}$ que satisface

$$\langle Tf, g\rangle = \langle f, T^*g\rangle\,, \quad \text{para todo } f,g\in\mathcal{H}\,.$$

Para $T,S\in\mathcal{B}(\mathcal{H})$ y $\alpha\in\mathbb{C}$, es sencillo verificar que el adjunto satisface lo siguiente:

$$\begin{aligned} T^*\in\mathcal{B}(\mathcal{H}) &\qquad (TS)^* = S^*T^*; \\ T^{**} = T; &\qquad (\alpha T+S)^* = \overline{\alpha}T^* + S^*; \\ \|T^*\| = \|T\|; &\qquad \mathcal{N}(T^*) = \mathcal{R}(T)^\perp\,. \end{aligned} \tag{2.15}$$

La última igualdad de (2.15) implica

$$\mathcal{H} = \mathcal{R}(T)\oplus\mathcal{N}(T^*)\,. \tag{2.16}$$

Teorema 2.23. *Un operador $T, T^* \in \mathcal{B}(\mathcal{H})$ son invertibles simultáneamente y*

$$(T^*)^{-1} = (T^{-1})^* . \tag{2.17}$$

Demostración. Si T es invertible entonces para $f \in \mathcal{H}$ se tiene $f = TT^{-1}f = Tg$, con $g = T^{-1}f$, de donde se sigue que $f \in \mathcal{R}(T)$, o bien, $\mathcal{H} = \mathcal{R}(T)$. Por lo tanto, de (2.16) se sigue que T^* es invertible. Por otro lado, si T^* es invertible, usando el argumento anterior se tiene que $T = T^{**}$ es invertible. Para probar (2.17), note que $I^* = I$ y de (2.15),

$$(T^{-1})^* T^* = I^* = T^*(T^{-1})^* ,$$

de donde se sigue que $(T^{-1})^* = (T^*)^{-1}$. □

Observación 2.24. Las operaciones (2.10), la norma (2.13) y la propiedad (2.14), hacen que $\mathcal{B}(\mathcal{H})$ sea un *álgebra de Banach unital*, y con la operación adjunto se torna en una *-álgebra, o bien, en una *álgebra de von Neumann*[6], que es un caso especial de C^*-álgebra.

2.2.2 Introducción a la teoría espectral

Permita introducir un poco de teoría espectral de operadores lineales en $\mathcal{B}(\mathcal{H})$.

Definición 2.25. Definimos el *espectro* de $T \in \mathcal{B}(\mathcal{H})$ como

$$\sigma(T) := \{\zeta \in \mathbb{C} : \mathcal{N}(T - \zeta I) \neq \{0\}\} .$$

A los elementos de $\sigma(T)$ se le conocen como los *autovalores* de T. Al espacio $\mathcal{N}(T - \zeta I)$ se le conoce como el *autoespacio asociado* a $\zeta \in \sigma(T)$ mientras que a sus elementos se le llaman los *autovectores* de T correspondientes al autovalor ζ. Además, el número de elementos de $\sigma(T)$ (contando su multiplicidad) coincide con la dimensión del espacio $\mathcal{H}$. Por conveniencia, los autovectores de $\mathcal{N}(T - \zeta I)$ son los elementos de alguna b.o.n. para $\mathcal{N}(T - \zeta I)$.

Corolario 2.26. *Para $T \in \mathcal{B}(\mathcal{H})$ se sigue que $\sigma(T^*)$ es el complejo conjugado de $\sigma(T)$.*

Demostración. Si $\zeta \in \sigma(T)$ entonces $T - \zeta I$ no es invertible, lo que implica del teorema 2.23 que $T^* - \overline{\zeta} I$ no sea invertible y por lo tanto $\overline{\zeta} \in \sigma(T^*)$. Ahora, si $\overline{\zeta} \in \sigma(T^*)$ entonces lo anterior y el doble adjunto implica que $\zeta \in \sigma(T)$. □

Definición 2.27. Para $\zeta \in \sigma(T)$, se denota

$$\begin{aligned} R_\zeta(T) &:= \cup_{k\in\mathbb{N}} \mathcal{N}((T - \zeta I)^k) ; && \text{(espacio raíz de } \zeta) \\ \zeta_{\text{geo}}(T) &:= \dim \mathcal{N}(T - \zeta I) ; && \text{(multiplicidad geométrica de } \zeta) \\ \zeta_{\text{alg}}(T) &:= \dim R_\zeta(T) . && \text{(multiplicidad algebraica de } \zeta) \end{aligned}$$

[6] Las álgebras de von Neumann fueron introducidas originalmente por John von Neumann en [15].

Así, $\zeta_{\text{geo}}(T) \leq \zeta_{\text{alg}}(T)$, $R_\zeta(T) \cap R_\lambda(T) = \{0\}$ y $\mathcal{N}(T-\zeta I) \cap \mathcal{N}(T-\lambda I) = \{0\}$, para $\zeta \neq \lambda$. Además, $\mathcal{N}(T-\zeta I) \subset R_\zeta(T)$ y $\cup_{\zeta\in\sigma(T)} R_\zeta(T) = \mathcal{H}$ (cf. [2, subsección 3.5.3]).

Definición 2.28. Un operador $T \in \mathcal{B}(\mathcal{H})$ se dice ser *diagonalizable* con respecto a una b.o.n $\{e_j\}_{j=1}^n \subset \mathcal{H}$ si existe $U \in \mathcal{B}(\mathcal{H})$ invertible tal que

$$T = U D_T U^{-1}, \quad \text{donde} \quad D_T e_j = \zeta_j e_j, \text{ con } \sigma(T) = \{\zeta_j\}_{j=1}^n. \tag{2.18}$$

Si U es unitario (ver definición 2.41 de sección 2.3) entonces T es *unitariamente diagonalizable*.

Observación 2.29 ([7, sección 1.3]). $T \in \mathcal{B}(\mathcal{H})$ es diagonalizable (resp. unitariamente diagonalizable) si y solo si el conjunto de todos sus autovectores forman una base (resp. b.o.n.) para $\mathcal{H}$.

Teorema 2.30. *Un operador $T \in \mathcal{B}(\mathcal{H})$ es diagonalizable si y solo si*

$$\zeta_{\text{geo}}(T) = \zeta_{\text{alg}}(T), \quad \textit{para todo } \zeta \in \sigma(T).$$

Demostración. Si T es diagonalizable entonces de la observación 2.29 el conjunto de todos sus autovectores $\{u_j\}_{j=1}^n$ forman una base para $\mathcal{H}$. Si $\zeta_{\text{geo}}(T) < \zeta_{\text{alg}}(T)$ para algún $\zeta \in \sigma(T)$, entonces existe $u \in R_\zeta(T)$ no cero tal que $u \notin \mathcal{N}(T-\lambda I)$ para todo $\lambda \in \sigma(T)$, lo que implica $u \notin \operatorname{span}\{u_j\}_{j=1}^n = \mathcal{H}$, una contradicción.

Inversamente, si $\zeta_{\text{geo}}(T) = \zeta_{\text{alg}}(T)$ para todo $\zeta \in \sigma(T)$, entonces $R_\zeta(T) = \mathcal{N}(T-\zeta I)$ y $\mathcal{H} = \cup_{\zeta\in\sigma(T)} \mathcal{N}(T-\zeta I)$, de donde se sigue que el conjunto de todos los autovalores de T son l.i. y generan a $\mathcal{H}$, i.e., es una base para $\mathcal{H}$. Así, T es diagonalizable por la observación 2.29. □

2.2.3 Notación *bra-ket* de operadores

En lo siguiente se usa el *formalismo de Dirac* [4] para operadores lineales, el cual será de gran utilidad en la secuela.

Definición 2.31 (Notación *bra-ket*). Para $u, v \in \mathcal{H}$, defina $|u\rangle\langle v| : \mathcal{H} \to \mathcal{H}$ como

$$|u\rangle\langle v|\, f = \langle v, f\rangle\, u, \quad f \in \mathcal{H}.$$

Observación 2.32. La aplicación $|u\rangle\langle v| \in \mathcal{B}(\mathcal{H})$. Ciertamente, para $f, g \in \mathcal{H}$ y $\alpha \in \mathbb{C}$,

$$\begin{aligned} |u\rangle\langle v|\,(\alpha f + g) &= \langle v, \alpha f + g\rangle\, u = \alpha\,\langle v, f\rangle\, u + \langle v, g\rangle\, u \\ &= \alpha\,|u\rangle\langle v|\, f + |u\rangle\langle v|\, g. \end{aligned}$$

Además, para $T \in \mathcal{B}(\mathcal{H})$, $u, v, w, \varphi \in \mathcal{H}$ y $\alpha \in \mathbb{C}$ lo siguiente se cumple:

$$\begin{aligned} |\alpha u + v\rangle\langle w| &= \alpha\,|u\rangle\langle w| + |v\rangle\langle w| & |u\rangle\langle \alpha v + w| &= \overline{\alpha}\,|u\rangle\langle v| + |u\rangle\langle w| \\ |u\rangle\langle v|^* &= |v\rangle\langle u| & |u\rangle\langle v|\,|w\rangle\langle \varphi| &= \langle v, w\rangle\,|u\rangle\langle \varphi| \\ \||u\rangle\langle v|\| &= \|u\|\,\|v\| & \langle w, |u\rangle\langle v|\,\varphi\rangle &= \langle w, u\rangle\,\langle v, \varphi\rangle \\ T\,|u\rangle\langle v| &= |Tu\rangle\langle v| & |u\rangle\langle v|\,T &= |u\rangle\langle T^* v| \end{aligned} \tag{2.19}$$

Teorema 2.33 (Representación matricial). *Si $\{e_j\}_{j=1}^n$ es una b.o.n. para $\mathcal{H}$ entonces $\{|e_j\rangle\langle e_k|\}_{j,k=1}^n$ es una base para el espacio $\mathcal{B}(\mathcal{H})$ y*

$$T = \sum_{j=1}^{n}\sum_{k=1}^{n} \langle e_j, Te_k\rangle\, |e_j\rangle\langle e_k|\,, \quad T \in \mathcal{B}(\mathcal{H})\,. \tag{2.20}$$

Demostración. Si $\sum_{j,k=1}^n \alpha_{jk}\,|e_j\rangle\langle e_k| = O$ (el operador cero), con $\{\alpha_{jk}\}_{j,k=1}^n \subset \mathbb{C}$, entonces

$$0 = \left\langle e_t, \sum_{j,k=1}^{n} \alpha_{jk}\,|e_j\rangle\langle e_k|\, e_s \right\rangle = \sum_{j,k=1}^{n} \alpha_{jk}\,\langle e_t, e_j\rangle\,\langle e_k, e_s\rangle = \alpha_{ts}\,, \quad t,s = 1,\ldots,n\,,$$

i.e., $\{|e_j\rangle\langle e_k|\}_{j,k=1}^n$ es l.i. en $\mathcal{B}(\mathcal{H})$. Ahora, para $T \in \mathcal{B}(\mathcal{H})$ se tiene que $Te_t = \sum_{j=1}^n \langle e_j, Te_t\rangle\, e_j$. En efecto, pues $Te_t = \sum_{j=1}^n \alpha_j e_j$, con $\{\alpha_j\}_{j=1}^n \subset \mathbb{C}$, y $\langle e_s, Te_j\rangle = \alpha_s$. De este modo,

$$\sum_{j,k=1}^{n} \langle e_j, Te_k\rangle\, |e_j\rangle\langle e_k|\, e_t = \sum_{j=1}^{n} \langle e_j, Te_t\rangle\, e_j = Te_t\,, \quad t = 1,\ldots n\,. \tag{2.21}$$

Por lo tanto, para $f = \sum_{t=1}^n f_t e_t \in \mathcal{H}$, con $\{f_j\}_{j=1}^n \subset \mathbb{C}$, se sigue de (2.21) que

$$\sum_{j,k=1}^{n} \langle e_j, Te_k\rangle\, |e_j\rangle\langle e_k|\, f = \sum_{t,j,k=1}^{n} f_t\,\langle e_j, Te_k\rangle\, |e_j\rangle\langle e_k|\, e_t = \sum_{t=1}^{n} f_t Te_t = Tf\,,$$

de donde se llega a (2.20). □

Ejercicios de la sección

P.2.2.1.1 Muestre que $T \in \mathcal{B}(\mathcal{H})$ es uno-a-uno si y solo si $\mathcal{N}(T) = \{0\}$.

P.2.2.1.2 Muestre que cada operador en $\mathcal{B}(\mathcal{H})$ es una aplicación continua.

P.2.2.1.3 Muestre que (2.13) en efecto define una norma en $\mathcal{B}(\mathcal{H})$.

P.2.2.1.4 Muestre las propiedades del adjunto (2.15).

P.2.2.1.5 Verifique las propiedades (2.19).

2.3 Operadores normales en $\mathcal{B}(\mathcal{H})$

Para efectos prácticos, primero se introduce las clases de operadores autoadjuntos y unitarios, los cuales son de gran importancia en la física-matemática que merece su investigación. Los operadores autoadjuntos y unitarios comparten propiedades análogas en muchos aspectos aunque existen distinciones esenciales.

2.3.1 Operadores autoadjuntos

Se inicia directamente con la definición de operador autoadjunto.

Definición 2.34. Decimos que $A \in \mathcal{B}(H)$ es *autoadjunto* si $A = A^*$.

Proposición 2.35. *Para $A \in \mathcal{B}(\mathcal{H})$, los siguientes son equivalentes:*

(a) A es autoadjunto.

(b) $\langle f, Af\rangle \in \mathbb{R}$, para todo $f, \in \mathcal{H}$.

(c) $\langle f, Ag\rangle = \langle Af, g\rangle$, para todo $f, g \in \mathcal{H}$.

Demostración. (a)⇒(b) Como $A = A^*$ se tiene que $\langle f, Af\rangle = \langle Af, f\rangle = \overline{\langle f, Af\rangle}$ y $\langle f, Af\rangle \in \mathbb{R}$.
(b)⇒(c): Se sigue de lo anterior y de la identidad de polarización (2.11).
(c)⇒(a): Note que $\langle f, Ag\rangle = \langle f, A^*g\rangle$, i.e., $\langle f, (A - A^*)g\rangle = 0$ y del teorema 2.19, $A = A^*$. □

El resultado anterior mostró una caracterización de operadores autoadjuntos.

Corolario 2.36. *Si $A \in \mathcal{B}(\mathcal{H})$ es autoadjunto entonces $\sigma(A) \subset \mathbb{R}$.*

Demostración. Si $\zeta \in \sigma(A)$, con autovector $f \in \mathcal{H}$, entonces de la proposición 2.35.(b),

$$\zeta = \zeta \langle f, f\rangle = \langle f, Af\rangle \in \mathbb{R},$$

como se quería. □

Los siguientes operadores se definen teniendo en cuenta teorema de proyección 2.16.

Definición 2.37. Para un subespacio $F \leq \mathcal{H}$, decimos que P_F es la *proyección ortogonal* (simplemente proyección o proyector) sobre F, si

$$P_F(f + g) = f, \text{ para todo } f \in F, g \in F^{\perp}.$$

Es claro que $P_F \in \mathcal{B}(\mathcal{H})$ y de (2.8), $\left\|P_f h\right\| \leq \|h\|$, con igualdad si $h \in F$. Por lo tanto $\|P_F\| = 1$.

Teorema 2.38. *Un operador $P \in \mathcal{B}(\mathcal{H})$ es un proyector si y solo si $P = P^* = P^2$. En este caso, $P = P_F$, donde $F = \mathcal{R}(P)$.*

Demostración. Si P es proyector, entonces existe $F \leq \mathcal{H}$ tal que $P = P_F$. Así, para $h \in \mathcal{H}$, existe $f \in F$ y $g \in F^{\perp}$, tal que $h = f + g$ y $\langle h, P(h)\rangle = \|f\|^2 \in \mathbb{R}$, que en virtud del la proposición 2.35.(b), $P = P^*$. Ahora, $P^2 h = PPh = Pf = f = Ph$, es decir, $P^2 = P$.

Inversamente, para $f \in \mathcal{R}(P), g \in \mathcal{R}(P)^{\perp}$, existe $u \in \mathcal{H}$ tal que $Pu = f$ y $Pf = PPu = Pu = f$. Además, $\|Pg\|^2 = \langle g, Pg\rangle = 0$, es decir, $Pg = 0$, de donde se sigue que $P = P_{\mathcal{R}(P)}$. □

Los dos casos triviales son $F = \{0\}, \mathcal{H}$, de donde $P_{\{0\}} = O$ y $P_{\mathcal{H}} = I$. Además, $P_{F^\perp} = I - P_F$. Se dice que una proyección P_F es no trivial si $F \neq \{0\}, \mathcal{H}$.

Observación 2.39. Si P_F es una proyección ortogonal, entonces $\sigma(P_F) \subset \{0,1\}$, con igualdad si la proyección es no trivial. Además, $\mathcal{N}(P_F - I) = \mathcal{R}(P_F)$.

Lo siguiente muestra algunas propiedades que satisfacen los proyectores. Se omite la demostración debido a que se siguen con un cálculo simple.

Proposición 2.40. *Para dos subespacios $M, N \leq \mathcal{H}$ lo siguiente se cumple:*

$$\begin{aligned} &(a)\ \text{Si } P_M P_N = P_N P_M, \quad \text{entonces} \quad P_M P_N = P_{M\cap N}\,. \\ &(b)\ \text{Si } M \leq N, \quad \text{entonces} \quad P_M P_N = P_N P_M = P_M\,. \\ &(c)\ M \perp N \quad \text{si y solo si} \quad P_M P_N = P_N P_M = O\,. \\ &(d)\ \text{Si } M \perp N, \quad \text{entonces} \quad P_{M\oplus N} = P_N + P_M\,. \end{aligned} \tag{2.22}$$

2.3.2 Operadores unitarios

A continuación se introduce la noción de operador unitario y unitario parcial, los cuales están estrechamente relacionados con la de un isomorfismo isométrico en espacios de Hilbert.

Definición 2.41. Decimos que $U \in \mathcal{B}(H)$ es *unitario* si

$$\|Uf\| = \|f\|\,, \quad \text{para todo} \quad f \in \mathcal{H}\,. \tag{2.23}$$

Decimos que U es *unitario parcial*[7] si (2.23) se cumple para $f \in \mathcal{H} \ominus \mathcal{N}(U) = \mathcal{R}(U^*)$ (ver (2.16)).

Note que un operador unitario es unitario parcial pero no al revés. De hecho, un operador unitario parcial es unitario si y solo si su núcleo es trivial.

Teorema 2.42. *Para $U \in \mathcal{B}(\mathcal{H})$, los siguientes son equivalentes:*

(a) U es unitario parcial.

(b) $\langle Uf, Ug\rangle = \langle f, g\rangle$, para todo $f, g \in \mathcal{R}(U^*)$.

(c) $U^*U = P_{\mathcal{R}(U^*)}$ (la proyección sobre $\mathcal{R}(U^*)$).

Demostración. (a)⇒(b): Se sigue de la definición y de la identidad de polarización (2.11).

(b)⇒(c): Considere $P = U^*U$ el cual cumple que $P^* = P$. Además, es claro que $\mathcal{N}(U) \subset \mathcal{N}(P)$ y para $f \in \mathcal{N}(P)$ se tiene que $U^*Uf = 0$, i.e., $0 = \langle f, U^*Uf\rangle = \|Uf\|^2$, de donde se cumple que

[7] En la literatura también se le conoce como isometría parcial

$f \in \mathcal{N}(U)$. Así, $\mathcal{N}(P) = \mathcal{N}(U)$ y $\mathcal{R}(P) = \mathcal{R}(U^*) = \mathcal{H} \ominus \mathcal{N}(U)$, en virtud de (2.16). Entonces, para $f = f_1 + f_2 \in \mathcal{H}$, con $f_1 \in \mathcal{R}(P)$ y $f_2 \in \mathcal{R}(P)^\perp = \mathcal{N}(P)$, se tiene del punto (b) que

$$\begin{aligned} \langle f, P^2 f \rangle &= \langle Pf_1, Pf_1 \rangle = \langle Uf_1, UU^*Uf_1 \rangle \\ &= \langle f_1, U^*Uf_1 \rangle = \langle f, Pf \rangle \,, \end{aligned}$$

lo que implica del teorema 2.19.(b) que $P = P^2$. Por lo tanto, del teorema 2.38 se llega a (c).

(c)⇒(a) Para $f \in \mathcal{R}(U^*)$, se sigue que $\langle Uf, Uf \rangle = \langle f, P_{\mathcal{R}(U^*)} f \rangle = \langle f, f \rangle$, i.e., $\|Uf\| = \|f\|$. Por lo tanto, U es unitario parcial. □

Una consecuencia del teorema anterior es que U y U^* son unitarios parciales simultáneamente, debido al siguiente resultado.

Corolario 2.43. *Un operador $U \in \mathcal{B}(\mathcal{H})$ es unitario parcial si y solo si U^* lo es.*

Demostración. Ses U unitario parcial y para $g \in \mathcal{R}(U)$ no cero existe $f \in \mathcal{H} \ominus \mathcal{N}(U) = \mathcal{R}(U^*)$ tal que $Uf = g$. Entonces, del teorema 2.42.(c) se tiene que

$$\langle U^*g, U^*g \rangle = \langle P_{\mathcal{R}(U^*)} f, U^*Uf \rangle = \langle f, U^*Uf \rangle = \langle g, g \rangle \,,$$

de donde se sigue que U^* es unitario parcial. El sentido inverso se sigue de lo anterior tomado el doble adjunto. □

Lo siguiente permite identificar el conjunto de donde se encuentra el espectro de un operador unitario.

Corolario 2.44. *Si $U \in \mathcal{B}(\mathcal{H})$ es unitario parcial entonces:*

(a) $\sigma(U) \subset \{\zeta \in \mathbb{C} : |\zeta| = 1\} \cup \{0\}$.

(b) $\{e_j\}_{j=1}^n$ *es b.o.n. para* $\mathcal{R}(U^*)$ *si y solo si* $\{Ue_j\}_{j=1}^n$ *es b.o.n. para* $\mathcal{R}(U)$.

Demostración. (a): Para $\zeta \in \sigma(U) \backslash \{0\}$, con autovector f, se sigue que $f \in \mathcal{H} \ominus \mathcal{N}(U)$ y

$$|\zeta| = \|\zeta f\| = \|Uf\| = \|f\| = 1 \,.$$

(b): Si $\{e_j\}_{j=1}^n$ es b.o.n. para $\mathcal{R}(U^*)$, entonces del teorema 2.42.(b),

$$\langle Ue_j, Ue_k \rangle = \langle e_j, e_k \rangle = \delta_{jk} \,,$$

siendo δ_{jk} la delta de Kronecker, de donde se sigue que $\{Ue_j\}_{j=1}^n$ es b.o.n. para $\mathcal{R}(U)$. Inversamente, si $\{Ue_j\}_{j=1}^n$ es b.o.n. para $\mathcal{R}(U)$ entonces de lo anterior y como U^* es unitario parcial (ver corolario 2.43), se tiene del teorema 2.42.(c) que $\{e_j = U^*Ue_j\}_{j=1}^n$ es b.o.n. para $\mathcal{R}(U^*)$. □

Observación 2.45. Un operador $U \in \mathcal{B}(\mathcal{H})$ es unitario si y solo si es invertible, $U^{-1} = U^*$ y $\mathcal{R}(U) = \mathcal{R}(U^*) = \mathcal{H}$. Esto como consecuencia del teorema 2.42.(c) y corolario 2.43. En este caso, del corolario 2.44 se tiene que

(a) $\sigma(U) \subset \{\zeta \in \mathbb{C} : |\zeta| = 1\}$.

(b) $\{e_j\}_{j=1}^n$ y $\{Ue_j\}_{j=1}^n$ son b.o.n.'s simultaneamente para $\mathcal{H}$.

De esta manera, la inversa de un operador unitario también es unitario. Además, si U, V son unitarios entonces también lo es UV. Así, los operadores unitarios forman un grupo con respecto a la composición.

2.3.3 Operadores normales

En lo siguiente se introduce la clase de operadores normales, lo cuales juegan un papel esencial en la teoría espectral.

Definición 2.46. Un operador $T \in \mathcal{B}(\mathcal{H})$ se dice ser *normal* si $TT^* = T^*T$. En otras palabras, un operador es normal si conmuta con su adjunto.

Ejemplo 2.47. Los operadores autoadjuntos y unitarios son caso particular de operadores normales.

Lema 2.48. *Un operador $T \in \mathcal{B}(\mathcal{H})$ es normal si y solo si*

$$\|T^* f\| = \|Tf\|, \quad \text{para todo } f \in \mathcal{H}. \tag{2.24}$$

En este caso se cumple lo siguiente:

(a) $\mathcal{N}(T - \lambda I) = \mathcal{N}(T^* - \overline{\lambda} I)$, para todo $\lambda \in \mathbb{C}$.

(b) $\mathcal{H} = \mathcal{R}(T - \lambda I) \oplus \mathcal{N}(T - \lambda I)$, para todo $\lambda \in \mathbb{C}$.

(c) $\mathcal{N}(T - \lambda I) \perp \mathcal{N}(T - \zeta I)$, para λ y ζ autovalores distintos.

Demostración. Si T es normal entonces para $f \in \mathcal{H}$,

$$\|T^* f\|^2 = \langle T^* f, T^* f\rangle = \langle TT^* f, f\rangle = \langle T^* Tf, f\rangle = \langle Tf, Tf\rangle = \|Tf\|^2,$$

de donde se sigue (2.24). Inversamente, si T cumple (2.24), entonces

$$\langle f, TT^* f\rangle = \|T^* f\|^2 = \|Tf\|^2 = \langle f, T^* Tf\rangle, \quad f \in \mathcal{H},$$

es decir, $\langle f, (TT^* - T^*T)f\rangle = 0$, para toto $f \in \mathcal{H}$. Por lo tanto, T es normal en virtud del teorema 2.19. Ahora bien:

(a): Si $f \in \mathcal{N}(T - \lambda I)$, entonces se tiene de (2.15) y (2.24) que

$$0 = \|(T - \lambda I)f\| = \left\|(T^* - \overline{\lambda} I)f\right\|,$$

de donde se sigue que $f \in \mathcal{N}(T^* - \overline{\lambda} I)$, i.e., $\mathcal{N}(T - \lambda I) \subset \mathcal{N}(T^* - \overline{\lambda} I)$. La otra contención se sigue usando lo anterior y el doble adjunto.

(b): Se sigue de (2.16) y del punto (a).

(c): Si u y v son autovectores correspondientes a λ y ζ, respectivamente, entonces del punto (a) se tiene que $T^*u = \overline{\lambda}u$ y

$$\zeta \langle u, v\rangle = \langle u, Tv\rangle = \left\langle \overline{\lambda}u, v\right\rangle = \lambda \langle u, v\rangle ,$$

o bien, $(\lambda - \zeta)\langle u, v\rangle = 0$, de donde se obtiene $\langle u, v\rangle = 0$. □

Lo siguiente muestra otra caracterización de operadores normales que es respecto a su descomposición espectral.

Teorema 2.49 (Teorema espectral). *Para $T \in \mathcal{B}(\mathcal{H})$, los siguientes enunciados son equivalentes:*

(a) T es normal.

(b) T es unitariamente diagonalizable.

(c) Existe una b.o.n. $\{u_j\}_{j=1}^n$ para $\mathcal{H}$ y $\{\zeta_j\}_{j=1}^n \subset \mathbb{C}$ tales que

$$T = \sum_{j=1}^{n} \zeta_j \left|u_j\right\rangle\!\left\langle u_j\right| . \tag{2.25}$$

Demostración. (a)⇒(b): Para $\zeta \in \sigma(T)$, si $(T - \zeta I)^2 f = 0$ y $g = (T - \zeta I)f$, entonces se cumple que $g \in \mathcal{R}(T - \zeta I) \cap \mathcal{N}(T - \zeta I)$ y por consiguiente $g = 0$, debido al lema 2.48.(b). De esta manera, $R_\zeta(T) = \mathcal{N}(T - \zeta I)$ y $\zeta_{\text{geo}}(T) = \zeta_{\text{alg}}(T)$. Por lo tanto, se tiene del teorema 2.30, juntamente con la observación 2.29 y lema 2.48.(c), que T es unitariamente diagonalizable.

(b)⇒(c): Usando (2.18), se tiene una b.o.n. $\{e_j\}_{j=1}^n$ para $\mathcal{H}$, un operador unitario $U \in \mathcal{B}(\mathcal{H})$ y el operador $D_T = \sum_{j=1}^n \zeta_j \left|e_j\right\rangle\!\left\langle e_j\right|$, con $\sigma(T) = \{\zeta_j\}_{j=1}^n$, tales que

$$T = UD_TU^* = \sum_{j=1}^{n} \zeta_j \left|Ue_j\right\rangle\!\left\langle Ue_j\right| .$$

Haciendo $u_j = Ue_j$ se llega a (2.25), ya que de la observación 2.45.(b), $\{Ue_j\}_{j=1}^n$ es b.o.n. para $\mathcal{H}$.

(c)⇒(a): Un cálculo simple muestra que $TT^* = \sum_{j=1}^n \left|\zeta_j\right|^2 \left|u_j\right\rangle\!\left\langle u_j\right| = T^*T$. □

Concluimos la sección con una consecuencia del teorema espectral.

Teorema 2.50 (Diagonalización simultánea). *Dos operadores normales $T, S \in \mathcal{B}(\mathcal{H})$ son simultáneamente diagonalizables respecto a una b.o.n. para $\mathcal{H}$ si y solo si conmutan.*

Demostración. Es directo verificar del teorema 2.49.(c) que Si T y S son simultáneamente diagonalizables respecto a una b.o.n., entonces $TS = ST$. Para el sentido inverso de la demostración, es suficiente mostrar que existe una b.o.n. de autovectores de S y T. Sea $\zeta \in \sigma(T)$ y defina el autoespacio $\mathcal{N}(T - \zeta)$ como F. Luego, para $u \in F$ se tiene que

$$TSu = STu = \zeta Su , \quad \text{es decir} \quad Su \in F . \tag{2.26}$$

Además, para $h \in \mathcal{H}$, se tiene $h = u + v$, donde $u \in F$ y $v \in F^{\perp}$ y de (2.26) se sigue que $Su \in F$ y $Sv \in F^{\perp}$, ya que el conjunto de los autovectores de T es una b.o.n. para $\mathcal{H}$. De esta manera,

$$P_F S h = P_F(Su + Sv) = Su = SP_F u = SP_F h\,,$$

donde P_F es la proyección ortogonal sobre F y se cumple que P_F y S conmutan. Ahora, sea $S_F = P_F S$ el cual es normal, ya que como S lo es,

$$S_F S_F^* = P_F S S^* P_F = P_F S^* S P_F = (P_F S)^* P_F S = S_F^* S_F\,.$$

Entonces, del teorema 2.49.(c), existe una b.o.n de autovectores de S_F, los cuales son autovectores de T, debido a que $\mathcal{R}(S_F) \subset F$. Así, para $u \in F$ autovector de S_F con autovalor λ se tiene que $Su = SP_F u = P_F S u = S_F u = \lambda u$, es decir, u es autovector de S. Por lo tanto, en F se tiene una b.o.n. de autovectores de T y S, que uniendo estás bases de cada autoespacio se tiene el resultado. □

Ejercicios de la sección

P.2.3.1 Verifique las propiedades de proyección (2.22).

P.2.3.2 Dada una b.o.n. $\{u_j\}_{j=1}^n$ para $\mathcal{H}$, muestre que para $m = 0, \ldots, n-1$,

$$U_m = \sum_{j=1}^{n-m} \zeta_j \left|u_{j+m}\right\rangle\!\left\langle u_j\right|\,, \quad \text{con } \left|\zeta_j\right| = 1\,,$$

es un operador unitario parcial.

P.2.3.3 Considere una b.o.n. $\{e_1, e_2\} \subset \mathbb{C}^2$ y defina los operadores[8] en $\mathcal{B}(\mathbb{C}^2)$,

$$\sigma_x = |e_1\rangle\langle e_2| + |e_2\rangle\langle e_1|\,; \qquad \sigma_y = i(|e_1\rangle\langle e_2| - |e_2\rangle\langle e_1|)\,;$$
$$\sigma_z = |e_1\rangle\langle e_1| - |e_2\rangle\langle e_2|\,.$$

Muestre que son tanto autoadjuntos como unitarios y calcule su espectro.

P.2.3.4 Muestre que $P \in \mathcal{B}(\mathcal{H})$ es una proyección ortogonal si y solo si

$$P = \sum_{j=1}^{m} \left|e_j\right\rangle\!\left\langle e_j\right|\,, \tag{2.27}$$

donde $\{e_j\}_{j=1}^m$ es una b.o.n. para $\mathcal{R}(P)$.

P.2.3.5 Muestre que la representación del proyector (2.27) no depende de la elección de la b.o.n.

P.2.3.6 Muestre que las siguientes condiciones son equivalentes:

a) U es unitario parcial.

b) $TT^*T = T$.

c) $T^*TT^* = T^*$.

[8] Estos operadores junto con la identidad en $\mathcal{B}(\mathbb{C}^2)$ son conocidos como las *matrices de Pauli*. Se estudiarán otras propiedades de estos operadores en la sección 3.2.2.

2.4 Operadores positivos y estados en $\mathcal{B}(\mathcal{H})$

Los operadores positivos son una parte esencial para caracterizar a los operadores de densidad o estados en $\mathcal{B}(\mathcal{H})$, debido a que cualquier sistema cuántico tiene asociado un espacio de Hilbert complejo y este sistema se describe totalmente por un estado.

2.4.1 Operadores lineales positivos

Definición 2.51. Decimos que un operador $A \in \mathcal{B}(\mathcal{H})$ es *positivo* (se escribe $A \geq 0$) si

$$\langle f, Af \rangle \geq 0\,, \quad f \in \mathcal{H}\,. \tag{2.28}$$

Se dice que A es *estrictamente positivo* ($A > 0$) si la desigualdad (2.28) es estricta, para todo $f \neq 0$.

Note que para $A \geq 0$ se tiene que $A > 0$ si y solo si es invertible. Además, se sigue de la proposición 2.35.(a) que un operador positivo es autoadjunto y por lo tanto normal. Para $A, B \in \mathcal{B}(\mathcal{H})$ autoadjuntos la expresión $A \geq B$ significa que $A - B \geq 0$.

Observación 2.52. Si $A \in \mathcal{B}(\mathcal{H})$ es positivo entonces existe una b.o.n. $\{u_j\}_{j=1}^n$ para $\mathcal{H}$ tal que

$$A = \sum_{j=1}^{n} \lambda_j \left|u_j\right\rangle\!\left\langle u_j\right|\,, \quad \lambda_j \geq 0\,. \tag{2.29}$$

Ciertamente, (2.29) se sigue del teorema 2.49.(a) y $\lambda_j = \langle u_j, \lambda_j u_j \rangle = \langle u_j, A u_j \rangle \geq 0$.

De (2.29) se tiene que $\sigma(A) = \{\lambda_j\}_{j=1}^n$ y $\{u_j\}_{j=1}^n$ son los autovectores de A. Además, $A > 0$ implica $\lambda_j > 0$, para $j = 1, \ldots, n$.

Teorema 2.53. *Un $A \in \mathcal{B}(\mathcal{H})$ es positivo si y solo si existe un único operador positivo $B \in \mathcal{B}(\mathcal{H})$ que conmuta con A y $B^2 = A$. Es este caso, $\sigma(B) = \{\sqrt{\lambda_j}\}_{j=1}^n$, donde $\sigma(A) = \{\lambda_j\}_{j=1}^n$.*

Demostración. Si A es positivo entonces satisface la descomposición (2.29). De esta manera, para

$$B = \sum_{j=1}^{n} \sqrt{\lambda_j} \left|u_j\right\rangle\!\left\langle u_j\right|\,, \quad \text{es sencillo ver que} \quad B \geq 0,\, B^2 = A \text{ y } A, B \text{ conmutan}\,. \tag{2.30}$$

Para la unicidad, si existe $T \geq 0$, tal que T conmuta con A y $T^2 = A$. Entonces, del teorema 2.50 T, A son simultáneamente diagonalizables, o bien, T, B lo son y $T = \sum_{j=1}^n t_j \left|u_j\right\rangle\!\left\langle u_j\right|$. Así,

$$\sum_{j=1}^{n} t_j^2 \left|u_j\right\rangle\!\left\langle u_j\right| = T^2 = A = \sum_{j=1}^{n} \lambda_j \left|u_j\right\rangle\!\left\langle u_j\right|\,,$$

de donde $t_j^2 = \langle u_j, T^2 u_j \rangle = \lambda_j$, i.e., $t_j = \sqrt{\lambda_j}$, para $j = 1, \ldots, n$, y por lo tanto $T = B$. El sentido inverso se sigue de manera directa. La segunda parte de la demostración se sigue de (2.30). □

Para $A \geq 0$ denote su raíz cuadrada positiva como $\sqrt{A}$. Entonces, del teorema anterior se tiene que A y $\sqrt{A}$ son simultáneamente diagonalizables y

$$\sqrt{A} = \sum_{j=1}^{n} \sqrt{\lambda_j} \, |u_j\rangle\langle u_j| \,, \quad \sigma(A) = \{\lambda_j\}_{j=1}^{n} \,. \tag{2.31}$$

Para $T \in \mathcal{B}(\mathcal{H})$ es directo calcular que $T^*T \geq 0$. Así, se puede denotar

$$|T| := \sqrt{T^*T} \geq 0 \,.$$

Observación 2.54. Para $T \in \mathcal{B}(\mathcal{H})$ se cumple que $\||T| f\| = \|Tf\|$ y $\mathcal{N}(|T|) = \mathcal{N}(T)$. En efecto, ya que si $f \in \mathcal{H}$ entonces

$$\||T| f\|^2 = \left\langle f, |T|^2 f \right\rangle = \langle Tf, Tf \rangle = \|Tf\|^2 \,. \tag{2.32}$$

Esto implica que $\||T|\| = \|T\|$ y $|T| > 0$ si y solo si T es invertible

Definición 2.55. Para $T \in \mathcal{B}(\mathcal{H})$, a elementos de $\sigma(|T|)$ se llaman los *valores singulares* de T.

Observación 2.56. Si $T \in \mathcal{B}(\mathcal{H})$ es normal, entonces sus valores singulares son los valores absolutos de sus autovalores. Ciertamente, se sigue del teorema 2.49.(c) y (2.31) que

$$|T| = \sqrt{T^*T} = \sum_{j=1}^{n} \left|\zeta_j\right| |u_j\rangle\langle u_j| \,, \quad \text{donde} \quad \sigma(T) = \{\zeta_j\}_{j=1}^{n} \,.$$

Teorema 2.57 (Descomposición polar). *Para $T \in \mathcal{B}(\mathcal{H})$ existe un operador unitario parcial $U \in \mathcal{B}(\mathcal{H})$ tal que*

$$T = U|T| \,. \tag{2.33}$$

Además, si T es invertible entonces U es único y unitario.

Demostración. Como $|T| = |T|^*$, para $f \in \mathcal{H}$ de (2.16) se tienen $f_1 \in \mathcal{R}(|T|)$ y $f_2 \in \mathcal{N}(|T|)$, tales que $f = f_1 + f_2$, o bien, $g \in \mathcal{H}$ tal que $f_1 = |T| g$ y $f = |T| g + f_2$. Defina el operado

$$Uf = Tg \,, \qquad f = |T| g + f_2 \in \mathcal{H} \quad \text{y} \quad f_2 \in \mathcal{N}(|T|) = \mathcal{N}(T) \,. \tag{2.34}$$

De esta manera, $\mathcal{N}(U) = \mathcal{N}(|T|)$ y $U|T| f = U|T| f_1 = Tf_1 = Tf$. Además, de (2.32) y (2.34),

$$\|Uf_1\| = \|Tg\| = \||T| g\| = \|f_1\| \,, \tag{2.35}$$

de donde se sigue que U es unitario parcial, ya que $\mathcal{N}(U)^\perp = \mathcal{N}(|T|)^\perp = \mathcal{R}(|T|)$. Si T es invertible, entonces lo es $|T|$. Así, $\mathcal{R}(|T|) = \mathcal{H}$ y (2.35) se cumple para todo $f_1 \in \mathcal{H}$ y por lo tanto U es unitario. La unicidad se sigue del hecho de que $|T|$ es invertible. □

Del teorema anterior, la descomposición (2.33) cumple que

$$\mathcal{R}(U) = \mathcal{R}(T) \quad \text{y} \quad \mathcal{N}(U) = \mathcal{N}(|T|) = \mathcal{N}(T)\,.$$

Corolario 2.58. *Si $T \in \mathcal{B}(\mathcal{H})$ es no cero entonces existen b.o.n.'s $\{v_j\}_{j=1}^n, \{u_j\}_{j=1}^n$ para $\mathcal{R}(T), \mathcal{R}(|T|)$, respectivamente tales que*

$$T = \sum_{j=1}^{n} \lambda_j \left|v_j\right\rangle\!\left\langle u_j\right| ,$$

donde λ_j son los valores singulares de T distinto de cero.

Demostración. Usando la representación (2.52) para $|T|$, con los valores singulares de T distinto de cero, se tiene de (2.33) que $T = U\sum_{j=1}^n \lambda_j \left|u_j\right\rangle\!\left\langle u_j\right| = \sum_{j=1}^n \lambda_j \left|v_j\right\rangle\!\left\langle u_j\right|$, donde $v_j = Uu_j$, $j = 1, \ldots, n$. Ahora, note de (2.34) que $\mathcal{R}(U) = \mathcal{R}(T)$ y $\mathcal{R}(U^*) = \mathcal{N}(U)^\perp = \mathcal{N}(|T|)^\perp = \mathcal{R}(|T|)$. Por lo tanto, del 2.44.(a) se tiene lo deseado. □

2.4.2 La traza de un operador lineal

Usualmente, se define la traza sobre una matriz cuadrada y es la suma de las entradas de su diagonal principal. Con base en la representación matricial de un operador (2.20) que se mostró en el teorema 2.33, se puede dar la siguiente definición de la traza de un operador lineal.

Definición 2.59. Definimos la transformación $\operatorname{tr}\colon \mathcal{B}(\mathcal{H}) \to \mathbb{C}$ como

$$\operatorname{tr}(T) = \sum_{j=1}^{n} \left\langle e_j, Te_j \right\rangle , \tag{2.36}$$

donde $\{e_j\}_{j=1}^n$ es una b.o.n. para $\mathcal{H}$. Al número (2.36) se le conoce como la *traza* de T.

La representación (2.36) no depende de la base. En efecto, si $\{u_j\}_{j=1}^n$ es una b.o.n. para $\mathcal{H}$, entonces $I = \sum_{k=1}^n |u_k\rangle\langle u_k| = \sum_{j=1}^n \left|e_j\right\rangle\!\left\langle e_j\right|$ (ver ejercicios p.2.2.4 y p.2.2.5) y

$$\begin{aligned}\sum_{k=1}^{n} \langle u_k, Tu_k\rangle &= \sum_{k=1}^{n}\sum_{j=1}^{n} \left\langle u_k, \left|e_j\right\rangle\!\left\langle e_j\right| Tu_k\right\rangle = \sum_{j=1}^{n}\sum_{k=1}^{n} \left\langle T^*e_j, u_k\right\rangle \left\langle u_k, e_j\right\rangle \\ &= \sum_{j=1}^{n}\sum_{k=1}^{n} \left\langle T^*e_j, |u_k\rangle\langle u_k| e_j\right\rangle = \sum_{j=1}^{n} \left\langle e_j, Te_j\right\rangle .\end{aligned}$$

Teorema 2.60. *La transformación (2.36) es un funcional lineal continuo respecto a la norma operador (2.13) y cumple las siguientes propiedades:*

(a) $\operatorname{tr}(T^*) = \overline{\operatorname{tr}(T)}$.

(b) $\operatorname{tr}(TS) = \operatorname{tr}(ST)$

(c) Si U es invertible, entonces $\operatorname{tr}\left(U^{-1}TU\right) = \operatorname{tr}(T)$.

(d) Si U unitario parcial y $\mathcal{R}(T) \subset \mathcal{R}(U)$ entonces $\operatorname{tr}(U^*TU) = \operatorname{tr}(T)$.

(e) $\operatorname{tr}(A\,|u\rangle\langle v|) = \langle v, Au\rangle$, *con* $u, v \in \mathcal{H}$.

(f) Si T es normal entonces $\operatorname{tr}(T)$ *es la suma de sus autovalores (incluyendo multiplicidades).*

Además, para $A, B \in \mathcal{B}(\mathcal{H})$ autoadjuntos:

(f) $\operatorname{tr}(A) \in \mathbb{R}$, $\operatorname{tr}(A) \geq 0$ *para* $A \geq 0$ *y* $\operatorname{tr}(A) > 0$ *para* $A > 0$.

(g) $\operatorname{tr}(A) \leq \operatorname{tr}(B)$ *si* $A \leq B$.

(h) Si $A \geq 0$, entonces $\operatorname{tr}(A) = 0$ *si y solo si* $A = O$.

Demostración. Es claro que (2.36) es un funcional lineal y de la desigualdad de Cauchy-Schwarz (2.4), para $T, S \in \mathcal{B}(\mathcal{H})$ y $\varepsilon > 0$ tal que $\|T - S\| < \varepsilon/n$ entonces

$$|\operatorname{tr}(T-S)| \leq \sum_{j=1}^{n} \left|\left\langle e_j, (T-S)e_j\right\rangle\right| \leq \|T-S\|\, n < \varepsilon\,.$$

Ahora, solo se muestran los puntos (b) y (d), ya que los demás se siguen con un cálculo simple de la definición y del teorema espectral 2.49.

(b): Como $I = \sum_{k=1}^{n} |e_k\rangle\langle e_k|$, se sigue que

$$\begin{aligned}\operatorname{tr}(ST) &= \sum_{j=1}^{n}\sum_{k=1}^{n} \left\langle S^*e_j, |e_k\rangle\langle e_k|\, Te_j\right\rangle = \sum_{k=1}^{n}\sum_{j=1}^{n} \left\langle T^*e_k, e_j\right\rangle \left\langle e_j, Se_k\right\rangle \\ &= \sum_{k=1}^{n}\sum_{j=1}^{n} \left\langle T^*e_k, \left|e_j\right\rangle\left\langle e_j\right| Se_k\right\rangle = \sum_{k=1}^{n} \left\langle T^*e_k, Se_k\right\rangle = \operatorname{tr}(TS)\,.\end{aligned}$$

(d): Como U es unitario parcial, del teorema 2.42.(c) y corolario 2.43, $UU^* = P_{\mathcal{R}(U)}$. Así, si $\mathcal{R}(T) \subset \mathcal{R}(U)$ entonces $P_{\mathcal{R}(U)}T = T$ y de (b), $\operatorname{tr}(U^*TU) = \operatorname{tr}\left(P_{\mathcal{R}(U)}T\right) = \operatorname{tr}(T)$. □

2.4.3 Operadores de densidad

DEFINICIÓN 2.61. Se dice que $P \in \mathcal{B}(\mathcal{H})$ es de *densidad* o *estado* si es positivo de traza uno.

En particular, $P = |u\rangle\langle u|$ es un estado llamado *estado puro*, donde $u \in \mathcal{H}$ es de norma uno. Además, un estado se dice *mezclado* si es combinación convexa de estados puros.

Es directo de la observación 2.52 y del teorema 2.60 que todo estado P mezclado y satisface

$$\sum_{j=1}^{n} \lambda_j = 1\,, \quad \text{donde} \quad \sigma(P) = \{\lambda_j\}_{j=1}^{n}\,.$$

Observación 2.62. Todo $P \in \mathcal{B}(\mathcal{H})$ positivo no cero se torna en un estado, bajo la regla $P/\operatorname{tr}(P)$.

Con el funcional traza (2.36) se pueden construir espacios de Banach dados por

$$L_1(\mathcal{H}) = (\mathcal{B}(\mathcal{H}), \|\cdot\|_1) \qquad \text{y} \qquad L_2(\mathcal{H}) = (\mathcal{B}(\mathcal{H}), \|\cdot\|_2)$$

llamados las clases de operadores *de traza* y *de Hilbert-Schmidt*, respectivamente, donde,

$$\|T\|_1 = \operatorname{tr}(|T|) \qquad \text{y} \qquad \|T\|_2 = \sqrt{\operatorname{tr}\left(|T|^2\right)}. \tag{2.37}$$

Si $\{\lambda_j\}_{j=1}^n$ son los valores singulares de T, entonces

$$\|T\|_1 = \sum_{j=1}^n \lambda_j \qquad \text{y} \qquad \|T\|_2 = \sqrt{\sum_{j=1}^n \lambda_j^2}.$$

Uno puede definir sobre $\mathcal{B}(\mathcal{H})$ la forma $\langle\cdot,\cdot\rangle_2 : \mathcal{B}(\mathcal{H}) \times \mathcal{B}(\mathcal{H}) \to \mathbb{C}$ dada por

$$\langle T, S\rangle_2 = \operatorname{tr}(T^* S), \tag{2.38}$$

la cual define un producto interno, llamado el *producto de Hilbert-Schmidt*. Además,

$$\langle T, T\rangle_2 = \operatorname{tr}(T^* T) = \operatorname{tr}\left(|T|^2\right) = \|T\|_2^2,$$

De esta manera, $\|\cdot\|_2$ es inducida por $\langle\cdot,\cdot\rangle_2$ y, por lo tanto, se ha mostrado lo siguiente.

Proposición 2.63. *El espacio $L_2(\mathcal{H})$ es de Hilbert, con $L_2(\mathcal{H}) = (\mathcal{B}(\mathcal{H}), \langle\cdot,\cdot\rangle_2)$.*

Ejercicios de la sección

P.2.4.1 Para $u \in \mathcal{H}$, muestre que $|u\rangle\langle u| \geq 0$.

P.2.4.2 Muestre que para $A, B \in \mathcal{B}(\mathcal{H})$ positivos y $\lambda \geq 0$, se cumple que $A + \lambda B \geq 0$.

P.2.4.3 Verifique $TT^*, TT^* \geq 0$, para cualquier operador $\in \mathcal{B}(\mathcal{H})$.

P.2.4.4 Sea $T = U|T|$ la descomposición polar de T. Muestre que $T^* = U^*|T^*|$ es la descomposición polar de T^* y que $T^* = |T|U^*$.

P.2.4.5 Verifique los puntos que faltan por demostrar del teorema 2.60.

P.2.4.6 Muestre que para $A \in \mathcal{B}(\mathcal{H})$ autoadjunto existe $\lambda \geq 0$ tal que $A + \lambda I \geq 0$.

P.2.4.7 Muestre que para todo $A \in \mathcal{B}(\mathcal{H})$ existen $\lambda \geq 0$ y $\beta > 0$ tales que $\beta(A + \lambda I)$ es un estado.

P.2.4.8 Muestre que (2.37) son en efecto normas en $\mathcal{B}(\mathcal{H})$.

P.2.4.9 Muestre que (2.38) es en efecto un producto interno en $\mathcal{B}(\mathcal{H})$.

2.5 Productos tensoriales de espacios de Hilbert

En esta sección se presenta el producto tensorial de espacios de Hilbert que define un nuevo espacio de Hilbert. Se muestran algunas propiedades fundamentales que serán relevantes en la teoría cuántica de varias partículas, por ejemplo para acoplar sistemas.

2.5.1 Producto tensorial de dos espacios de Hilbert

Para efectos prácticos y comodidad del lector, primero se introduce el producto tensorial de dos espacios de Hilbert y posteriormente de m espacios de Hilbert.

Definición 2.64. Para dos espacios de Hilbert $(\mathcal{H}_1, \langle\cdot,\cdot\rangle_1)$ y $(\mathcal{H}_2, \langle\cdot,\cdot\rangle_2)$ se definde su *producto tensorial algebraico* (o simplemente producto tensorial) como

$$\mathcal{H}_\otimes := \mathcal{H}_1 \otimes \mathcal{H}_2 = \text{span}\left\{u_1 \otimes u_2 : u_1 \in \mathcal{H}_1, u_2 \in \mathcal{H}_2\right\},$$

el cual es lineal en cada componente, es decir, para $u_j, v_j \in \mathcal{H}_j$, $j = 1,2$, y $\alpha, \beta \in \mathbb{C}$,

$$\begin{aligned}(u_1 + \alpha v_1) \otimes u_2 &= u_1 \otimes u_2 + \alpha v_1 \otimes u_2\,;\\ u_1 \otimes (u_2 + \beta v_2) &= u_1 \otimes u_2 + \beta u_1 \otimes v_2\,.\end{aligned}$$

Los elementos de la forma $u_1 \otimes u_2 \in \mathcal{H}_\otimes$ se les conoce como *tensores elementales*. De esta manera, cada elemento en $\mathcal{H}_\otimes$ es combinación lineal de tensores elementales.

Observación 2.65 (Elementos en $\mathcal{H}_\otimes$). Cada elemento $f \in \mathcal{H}_\otimes$ tiene la forma $f = \sum_{j=1}^m u_j \otimes v_j$. Ciertamente, se tiene de la linealidad del producto tensorial que

$$f = \sum_{j=1}^{m}\sum_{k=1}^{l} \alpha_{jk} u_j \otimes w_k = \sum_{j=1}^{m} u_j \otimes \left(\sum_{k=1}^{l} \alpha_{jk} w_k\right) = \sum_{j=1}^{m} u_j \otimes v_j\,. \qquad (\alpha_{jk} \in \mathbb{C}) \tag{2.39}$$

Además, si $\{e_h\}_{h=1}^n$, $\{\varphi_k\}_{k=1}^l$ son b.o.n. para $\mathcal{H}_1$, $\mathcal{H}_2$, respectivamente, entonces se sigue que $u_j = \sum_{h=1}^n t_{jh} e_h$ y $v_j = \sum_{k=1}^l s_{jk}\varphi_k$, con $t_{jh}, s_{jk} \in \mathbb{C}$, que sustituyendo en (2.39) se llega a

$$f = \sum_{h=1}^{n}\sum_{k=1}^{l} \gamma_{hk} e_h \otimes \varphi_k\,, \qquad \gamma_{hk} = \sum_{j=1}^{m} t_{jh} s_{jk}\,. \tag{2.40}$$

Considere la forma $\langle\cdot,\cdot\rangle_\otimes : \mathcal{H}_\otimes \times \mathcal{H}_\otimes \to \mathbb{C}$, dada por

$$\langle f, g\rangle_\otimes := \sum_{j=1}^{m}\sum_{k=1}^{n} \langle u_j, x_k\rangle \langle v_j, y_j\rangle\,, \qquad f = \sum_{j=1}^{m} u_j \otimes v_j, \quad g = \sum_{k=1}^{l} x_k \otimes y_k \in \mathcal{H}_\otimes\,, \tag{2.41}$$

el cual define un producto interno. En efecto, pues de la definición (2.3) es sencillo calcular que es lineal en la segunda componente y hermitiana. Además, usando la expresión (2.40) se tiene que

$$\langle f, f\rangle_{\otimes} = \sum_{h=1}^{n}\sum_{k=1}^{l} |\gamma_{hk}|^2 > 0 \quad \text{para } f \neq 0.$$

Por lo tanto, se ha demostrado lo siguiente.

Teorema 2.66. *El espacio $(\mathcal{H}_{\otimes}, \langle\cdot,\cdot\rangle_{\otimes})$ es un espacio de Hilbert, cuyo producto interno satisface*

$$\langle u_1 \otimes u_2, v_1 \otimes v_2\rangle_{\otimes} = \langle u_1, v_1\rangle \langle u_2, v_2\rangle \,. \tag{2.42}$$

Además, su norma inducida satisface $\|u_1 \otimes u_2\|_{\otimes} = \|u_1\|\,\|u_2\|$.

La forma (2.41) es el único producto interno en $\mathcal{H}_{\otimes}$ que satisface (2.42) sobre tensores elementales [1, lemas 2.2 y 2.3].

Corolario 2.67. *Si $\{e_h\}_{h=1}^{n}$, $\{\varphi_k\}_{k=1}^{l}$ son b.o.n. para $\mathcal{H}_1$, $\mathcal{H}_2$, respectivamente, entonces*

$$\{e_h \otimes \varphi_k\}_{h,k=1}^{n,l} \qquad \text{es b.o.n. para} \quad \mathcal{H}_{\otimes}\,.$$

Por lo tanto, $\dim \mathcal{H}_{\otimes} = \dim \mathcal{H}_1 \cdot \dim \mathcal{H}_2$.

Demostración. Se sigue de (2.40) que $\{e_h \otimes \varphi_k\}_{h,k=1}^{n,l}$ genera a $\mathcal{H}_{\otimes}$ y de (2.42),

$$\langle e_h \otimes \varphi_k, e_s \otimes \varphi_t\rangle_{\otimes} = \langle e_h, e_s\rangle \langle \varphi_k, \varphi_t\rangle = \delta_{hs}\delta_{kt}\,,$$

de donde se sigue la afirmación. □

Para dos operadores $A \in \mathcal{B}(\mathcal{H}_1)$ y $B \in \mathcal{B}(\mathcal{H}_2)$ considere $L\colon \mathcal{H}_{\otimes} \to \mathcal{H}_{\otimes}$,

$$L\left(\sum_{j=1}^{m} u_j \otimes v_j\right) = \sum_{j=1}^{m} Au_j \otimes Bv_j\,, \qquad \sum_{j=1}^{m} u_j \otimes v_j \in \mathcal{H}_{\otimes}\,. \tag{2.43}$$

Es sencillo verificar que $L \in \mathcal{B}(\mathcal{H}_{\otimes})$ y actúa sobre los tensores elementales como

$$L(u_1 \otimes u_2) = Au_1 \otimes Bu_2\,, \qquad u_1 \otimes u_2 \in \mathcal{H}_{\otimes}\,. \tag{2.44}$$

Al operador (2.43) se denota como $L = A \otimes B$ y es el único que satisface (2.44) [1, lema 3.1].

Teorema 2.68 ([1, capítulo 3] y [14, sección 7.5.2]). *Si $A, C \in \mathcal{B}(\mathcal{H}_1)$ y $B, D \in \mathcal{B}(\mathcal{H}_2)$, entonces:*

(a) $\|A \otimes I\|_{\otimes} = \|A\|$ y $\|I \otimes B\|_{\otimes} = \|B\|$.

(b) $A \otimes B = (A \otimes I)(I \otimes B) = (I \otimes B)(A \otimes I)$ y $\|A \otimes B\|_{\otimes} = \|A\|\,\|B\|$.

(c) $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$.

(d) $(A+C)\otimes(B+D) = A\otimes B + A\otimes D + C\otimes B + C\otimes D$.

(e) $A^*\otimes B^* = (A\otimes B)^*$.

(f) $A\otimes B$ *es autoadjunto, positivo o unitario de acuerdo a si* A *y* B *son autoadjuntos, positivos o unitarios, respectivamente.*

(g) $A\otimes B$ *es un proyector si* A *y* B *son proyectores. En este caso,* $\mathcal{R}(A\otimes B) = \mathcal{R}(A)\otimes\mathcal{R}(B)$.

2.5.2 Producto tensorial de m espacios de Hilbert

El método para definir el producto tensorial de dos espacios de Hilbert dado anteriormente se puede extender de manera natural para m espacios de Hilbert.

Definición 2.69. Dada una sucesión $\{(\mathcal{H}_j, \langle\cdot,\cdot\rangle_j)\}_{j=1}^m$ de espacios de Hilbert se denota su *producto tensorial* como

$$\mathcal{H}_\otimes := \bigotimes_{j=1}^m \mathcal{H}_j = \operatorname{span}\left\{u_1\otimes\cdots\otimes u_m : u_j\in\mathcal{H}_j\right\}, \tag{2.45}$$

que es lineal en cada componente, es decir, para $j = 1,\dots,m$

$$u_1\otimes\cdots\otimes(u_j+\alpha v_j)\otimes\cdots\otimes u_m = u_1\otimes\cdots\otimes u_j\otimes\cdots\otimes u_n + \alpha u_1\otimes\cdots\otimes v_j\otimes\cdots\otimes u_m\,.$$

A los elementos $u_1\otimes\cdots\otimes u_m\in\mathcal{H}_\otimes$ se les llama *tensores elementales*. De esta manera, los elemento en $\mathcal{H}_\otimes$ son combinaciones lineales de tensores elementales. Usualmente en la literatura se denota $\mathcal{H}_\otimes = \mathcal{H}^{\otimes^m}$ cuando $\mathcal{H}_1 = \cdots = \mathcal{H}_m$.

Al espacio (2.45) se equipa con el producto interno $\langle\cdot,\cdot\rangle_\otimes : \mathcal{H}_\otimes\times\mathcal{H}_\otimes\to\mathbb{C}$, que satisface

$$\langle u_1\otimes\cdots\otimes u_m, v_1\otimes\cdots\otimes v_m\rangle_\otimes = \prod_{j=1}^m \langle u_j, v_j\rangle\,. \tag{2.46}$$

Por lo tanto, $(\mathcal{H}_\otimes, \langle\cdot,\cdot\rangle_\otimes)$ es un espacio de Hilbert. La norma inducida por el producto interno (2.46) satisface

$$\|u_1\otimes\cdots\otimes u_m\|_\otimes = \prod_{j=1}^m \|u_j\|\,.$$

Al igual que en el caso de producto tensorial de dos espacios de Hilbert, la forma $\langle\cdot,\cdot\rangle_\otimes$ es el único producto interno en $\mathcal{H}_\otimes$ que satisface (2.46).

Proposición 2.70. *Para* $j = 1,\dots,m$, *si* $\{e_{jk_j}\}_{k_j=1}^{n_j}$ *es una b.o.n. para* $\mathcal{H}_j$ *entonces*

$$\left\{e_{1k_1}\otimes\cdots\otimes e_{mk_m} : k_j = 1\dots n_j,\ j = 1,\dots,m\right\} \qquad \text{es b.o.n. para} \quad \mathcal{H}_\otimes\,. \tag{2.47}$$

Por lo tanto, se cumple que $\dim\mathcal{H}_\otimes = \prod_{j=1}^m \dim\mathcal{H}_j$.

Demostración. Si $u_1 \otimes \cdots \otimes u_m \in \mathcal{H}_\otimes$, entonces $u_j = \sum_{k_j=1}^{n_j} \alpha_{jk_j} e_{jk_j}$ y

$$u_1 \otimes \cdots \otimes u_m = \sum_{k_1=1}^{n_1} \cdots \sum_{k_m=1}^{n_m} \alpha_{1k_1} \ldots \alpha_{mk_m} e_{1k_1} \otimes \cdots \otimes e_{mk_m} . \tag{2.48}$$

Como los elementos de $\mathcal{H}_\otimes$ son combinaciones lineales de elementos (2.48) se tiene que (2.47) genera a $\mathcal{H}_\otimes$. Además, se cumple de (2.46) que

$$\left\langle e_{1h_1} \otimes \cdots \otimes e_{mh_m}, e_{1k_1} \otimes \cdots \otimes e_{mk_m} \right\rangle_\otimes = \prod_{j=1}^{m} \left\langle e_{jh_j}, e_{jk_j} \right\rangle = \prod_{j=1}^{m} \delta_{h_j k_j} ,$$

de donde se sigue la afirmación. □

Análogamente al caso de dos productos tensoriales de operadores, para $A_j \in \mathcal{B}(\mathcal{H}_j)$, con $j = 1, \ldots, m$, se tiene un único operador $A_1 \otimes \cdots \otimes A_m \in \mathcal{B}(\mathcal{H}_\otimes)$ tal que sobre los tensores elementales actúa como

$$A_1 \otimes \cdots \otimes A_m (u_1 \otimes \cdots \otimes u_m) = A_1 u_1 \otimes \cdots \otimes A_m u_m , \quad u_1 \otimes \cdots \otimes u_m \in \mathcal{H}_\otimes .$$

Las propiedades del teorema 2.68 se cumplen de manera similar para productos tensoriales de m operadores lineales y solo se mencionan debido a que su demostración es análoga al caso de dos productos tensoriales de operadores.

Teorema 2.71. *Para $A_j \in \mathcal{B}(\mathcal{H}_j)$ y $B_j \in \mathcal{B}(\mathcal{H}_j)$ con $j = 1, \ldots, m$, denote $A = \bigotimes_{j=1}^m A_j$ y $B = \bigotimes_{j=1}^m B_j$ en $\mathcal{B}(\mathcal{H}_\otimes)$. Entonces:*

(a) $\|A\|_\otimes = \prod_{j=1}^m \|A_j\|$.

(b) $AB = \bigotimes_{j=1}^m A_j B_j$.

(c) $A_1 \otimes \cdots \otimes (A_j + B_j) \otimes \cdots \otimes A_m = A_1 \otimes \cdots \otimes A_j \otimes \cdots \otimes A_m + A_1 \otimes \cdots \otimes B_j \otimes \cdots \otimes A_m$.

(d) $A^* = \bigotimes_{j=1}^m A_j^*$.

(e) A es autoadjunto, positivo o unitario de acuerdo a si cada A_j es autoadjunto, positivo o unitario, respectivamente.

(f) A es un proyector si cada A_j es un proyector. En este caso, $\mathcal{R}(A) = \prod_{j=1}^m \mathcal{R}(A_j)$.

(g) Si cada $A_j = |u_j\rangle\langle v_j|$, con $u_j, v_j \in \mathcal{H}_j$, entonces

$$A = |u_1 \otimes \cdots \otimes u_m\rangle\langle v_1 \otimes \cdots \otimes v_m| .$$

Concluimos la sección mostrando una propiedad de la traza en productos tensoriales de operadores.

Teorema 2.72. *Para $A_j \in \mathcal{B}(\mathcal{H}_j)$, con $j = 1, \ldots, m$, se cumple que*

$$\operatorname{tr}_\otimes \left(\bigotimes_{j=1}^m A_j \right) = \prod_{j=1}^m \operatorname{tr}(A_j) .$$

Demostración. Si $\{e_{jk_j}\}_{k_j=1}^{n_j}$ es b.o.n. para $\mathcal{H}_j$ entonces (2.47) es b.o.n. para $\mathcal{H}_\otimes$ y

$$\begin{aligned}
\operatorname{tr}_\otimes\left(\bigotimes_{j=1}^m A_j\right) &= \sum_{k_1=1}^{n_1}\cdots\sum_{k_m=1}^{n_m}\left\langle e_{1k_1}\otimes\cdots\otimes e_{mk_m}, \bigotimes_{j=1}^m A_j(e_{1k_1}\otimes\cdots\otimes e_{mk_m})\right\rangle_\otimes \\
&= \sum_{k_1=1}^{n_1}\cdots\sum_{k_m=1}^{n_m}\left\langle e_{1k_1}\otimes\cdots\otimes e_{mk_m}, A_1e_{1k_1}\otimes\cdots\otimes A_me_{mk_m})\right\rangle_\otimes \\
&= \sum_{k_1=1}^{n_1}\cdots\sum_{k_m=1}^{n_m}\left\langle e_{1k_1}, A_1e_{1k_1}\right\rangle\ldots\left\langle e_{mk_m}, A_me_{mk_m}\right\rangle \\
&= \sum_{k_1=1}^{n_1}\left\langle e_{1k_1}, A_1e_{1k_1}\right\rangle\cdots\sum_{k_m=1}^{n_m}\left\langle e_{mk_m}, A_me_{mk_m}\right\rangle = \operatorname{tr}(A_1)\cdots\operatorname{tr}(A_m)\,,
\end{aligned}$$

como se quería. □

Ejercicios de la sección

P.2.5.1 Muestre que $\mathcal{H}_\otimes$ definido en (2.45) es un espacio vectorial.

P.2.5.2 Sea $A = U_A|A|$, $B = U_B|B|$ las descomposiciones polares de $A, B \in \mathcal{B}(\mathcal{H})$, respectivamente, y $A\otimes B = U_{A\otimes B}|A\otimes B|$ la descomposición polar de $A\otimes B \in \mathcal{B}(\mathcal{H}_\otimes)$.

a) Muestre que $U_{A\otimes B} = U_A\otimes U_B$ y $|A\otimes B| = |A|\otimes|B|$.

b) Verifique que $A\otimes B = U_A\otimes U_B|A|\otimes|B|$ es la descomposición polar de $A\otimes B$.

P.2.5.3 Muestre que si $A_j \in \mathcal{B}(\mathcal{H}_j)$ son normales, para $j = 1,\ldots,m$, entonces $\bigotimes_{j=1}^m A_j$ es normal.

P.2.5.4 Muestre que si $A_j \in \mathcal{B}(\mathcal{H}_j)$ son unitariamente diagonalizables, para $j = 1,\ldots,m$, entonces $\bigotimes_{j=1}^m A_j$ es unitariamente diagonalizables.

P.2.5.5 Muestre que si $A_j \in \mathcal{B}(\mathcal{H}_j)$ son normales, para $j = 1,\ldots,m$, entonces existen b.o.n.'s $\{u_{jk_j}\}_{k_j=1}^{n_j}$ para $\mathcal{H}_j$, respectivamente, tales que

$$\bigotimes_{j=1}^m A_j = \sum_{k_1=1}^{n_1}\cdots\sum_{k_m=1}^{n_m}\zeta_{1k_j}\cdots\zeta_{mk_j}\left|u_{1k_1}\otimes\cdots\otimes u_{mk_m}\right\rangle\left\langle u_{1k_1}\otimes\cdots\otimes u_{mk_m}\right|\,.$$

Describe los autovalores y autovectores de $\bigotimes_{j=1}^m A_j$ en relación con los autovalores y autovectores de los $A_j's$.

Capítulo 3

Códigos Cuánticos

3.1

Preliminares

Sea $\mathcal{H}$ un espacio de Hilbert complejo de dimensión N con producto interno denotado por $\langle \cdot, \cdot \rangle$. Como hemos venido haciendo en estas notas, este producto interno será conjugado lineal en la primera entrada y lineal en la segunda. En virtud de que todo operador puede representarse matricialmente respecto a una base ortonormal (teorema 2.33), de ahora en adelante utilizaremos intercambiablemente el término matriz y operador.

3.1.1

Estados cuánticos

En la mecánica cuántica, el estado de un sistema cuántico en un espacio vectorial complejo se representa mediante un operador positivo ρ y de traza uno, nos referiremos a este tipo de objetos como *estados cuánticos* o simplemente *estados*, aunque se les suele llamar también operadores o matrices de densidad. En el capítulo anterior, ver definición 2.61, se introdujeron brevemente los estados puros y mezclados. Retomaremos esa discusión como punto de partida.

Con cada vector unitario $\psi \in \mathcal{H}$ podemos asociar una proyección ortogonal sobre el subespacio que genera, i.e., $\text{span}\{\psi\}$, y podemos escribir a esta proyección en la notación de Dirac como $|\psi\rangle\langle\psi|$. Esta proyección es además un estado cuántico pues

$$\Big\langle \varphi, |\psi\rangle\langle\psi|\varphi \Big\rangle = |\langle \varphi, \psi \rangle|^2 \geq 0 \quad \text{para todo } \varphi \in \mathcal{H}, \quad \text{y} \quad \text{tr}\,(|\psi\rangle\langle\psi|) = \langle \psi, \psi \rangle = 1.$$

A un estado de esta forma se le llama *estado puro*.

Sean $|\psi_1\rangle\langle\psi_1|$ y $|\psi_2\rangle\langle\psi_2|$ dos estados puros y $p_1, p_2 \in \mathbb{C}$. La combinación lineal de dos estados puros $p_1|\psi_1\rangle\langle\psi_1| + p_2|\psi_2\rangle\langle\psi_2|$ es un estado si y solo si los escalares son reales no negativos y suman uno, i.e., si es una combinación lineal *convexa*. Una combinación lineal convexa de estados puros se llama *estado mezclado*.

De modo que un estado cuántico general es un estado mezclado. Por un lado observemos que todo estado ρ puede representarse matricialmente respecto a cualquier b.o.n. de $\mathcal{H}$ (teorema 2.33)

$$\rho = \sum_{i,j=1}^{N} \rho_{i,j} |e_i\rangle\langle e_j|.$$

Por otro lado, como consecuencia de la observación 2.52, todo estado tiene una representación matricial diagonal respecto a su b.o.n. de vectores propios $\{\psi_j\}_{j=1}^N$ de $\mathcal{H}$ y sus valores propios $\{p_j\}_{j=1}^N$, dada por

$$\rho = \sum_{j=1}^{N} p_j |\psi_j\rangle\langle\psi_j|, \quad p_j \geq 0, \quad \sum_{j=1}^{N} p_j = 1. \tag{3.1}$$

En efecto podemos verificar que

$$\rho\,\psi_k = \sum_{j=1}^{N} p_j |\psi_j\rangle\langle\psi_j|\psi_k = \sum_{j=1}^{N} p_j \delta_{j,k}\psi_j = p_k\psi_k.$$

Recordemos que una matriz autoadjunta E es una proyección ortogonal si es idempotente, es decir, $E^2 = E$. En probabilidad cuántica toda proyección ortogonal E se interpreta como un evento. Podemos calcular $P_\rho(E)$, la probabilidad de ocurrencia del evento E en el estado cuántico ρ, mediante

$$P_\rho(E) = \operatorname{tr}(\rho E) = \sum_{j=1}^{N} p_j \operatorname{tr}\left(|\psi_j\rangle\langle\psi_j|E\right) = \sum_{j=1}^{N} p_j \,\langle\psi_j, E\psi_j\rangle.$$

3.1.2 Canales cuánticos

El formalismo de canales cuánticos es una herramienta general para describir la evolución o dinámica de un sistema cuántico. Un estado ρ se transforma o evoluciona en otro al aplicarse una operación cuántica Φ obteniendo un estado final ρ' de manera

$$\rho' = \Phi(\rho).$$

El mapeo Φ es un operador lineal sobre $\mathscr{B}(\mathcal{H})$ que captura el cambio dinámico de un estado debido a un proceso físico. A los operadores lineales que representan operaciones cuánticas físicamente válidas son llamados canales cuánticos, presentamos su definición precisa a continuación.

Definición 3.1. Un operador lineal $\Phi : \mathscr{B}(\mathcal{H}) \to \mathscr{B}(\mathcal{H})$ es un canal cuántico si existen operadores $E_i \in$ tales que

1. $\Phi(\rho) = \sum_i E_i \rho E_i^*$ para todo estado ρ. (Representación de Kraus)

2. $\sum_i E_i^* E_i = \mathbb{1}$. (Relación de completez)

Ejemplo 3.2. En el espacio de Hilbert $\mathcal{H} = \mathbb{C}^2$ los siguientes son ejemplos de canales cuánticos.

$$\Phi(\rho) = E_1\rho E_1^* + E_2\rho E_2^*, \qquad \Psi(\rho) = F_1\rho F_1^* + F_2\rho F_2^*$$

donde $E_1 = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$, $E_2 = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$ y $F_1 = \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$, $F_2 = \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}$.

Los canales cuánticos del ejemplo anterior son en apariencia dos canales distintos, sin embargo después de una inspección más cuidadosa se puede ver que en realidad *representan* a la misma operación cuántica. En efecto, note que $F_1 = (E_1 + E_2)/\sqrt{2}$ y $F_2 = (E_1 - E_2)/\sqrt{2}$ de donde

$$\begin{aligned}\Psi(\rho) &= \frac{(E_1+E_2)\rho(E_1+E_2)^* + (E_1-E_2)\rho(E_1-E_2)^*}{2} \\ &= E_1\rho E_1^* + E_2\rho E_2^* \\ &= \Phi(\rho).\end{aligned}$$

Esto muestra que la representación de una operación cuántica vía un canal cuántico no es única. La demostración del siguiente teorema puede encontrarse en [9].

Teorema 3.3. *Supongamos que $\{E_1,\dots,E_m\}$ y $\{F_1,\dots,F_n\}$ son dos conjuntos de operadores que dan lugar a dos canales cuánticos Φ y Ψ respectivamente. Añadiendo operadores cero al menor de los conjuntos de modo que $m = n$, obtenemos que, $\Psi = \Phi$ si y solo si existen números $\{u_{i,j}\}_{i,j}$ tales que $E_i = \sum_j u_{i,j}F_j$ y $U = (u_{i,j})_{i,j}$ es una matriz unitaria.*

Observemos que la definición 3.1 garantiza que, si ρ es un estado válido (positivo y traza uno), entonces el estado final ρ' será un estado válido también; pues por un lado preserva la traza

$$\operatorname{tr}(\Phi(\rho)) = \sum_i \operatorname{tr}(E_i\rho E_i^*) = \operatorname{tr}\left(\sum_i E_i^* E_i \rho\right) = \operatorname{tr}(\rho),$$

y por otro lado preserva positividad. En efecto si $\rho \geq 0$ (ver definición 2.28) entonces

$$\langle\phi, \Phi(\rho)\phi\rangle = \sum_i \langle\phi, E_i\rho E_i^*\phi\rangle = \sum_i \langle E_i^*\phi, \rho E_i^*\phi\rangle \geq 0, \quad \text{para todo } \phi \in \mathcal{H}.$$

De hecho, 1. de la definición 3.1 garantiza que el operador Φ satisface una propiedad más general que solo preservar positividad llamada *positividad completa*.

Definición 3.4. Sea $k \in \mathbb{N}$. Un operador lineal $\Phi : \mathscr{B}(\mathcal{H}) \to \mathscr{B}(\mathcal{H})$ se dice

1. *k-positivo* si el operador $\mathbb{1}_k \otimes \Phi : \mathbb{M}_k(\mathbb{C}) \otimes \mathscr{B}(\mathcal{H}) \to \mathbb{M}_k(\mathbb{C}) \otimes \mathscr{B}(\mathcal{H})$ es positivo.
2. *completamente positivo* si $\mathbb{1}_k \otimes \Phi$ es k-positivo para toda $k \geq 1$.

En la definición anterior $\mathbb{1}_k$ es la matriz identidad de tamaño $k \times k$. Omitiremos el subíndice cuando sea claro del contexto. Observe que un operador positivo es 1-positivo y por lo tanto la propiedad de positividad completa es más fuerte que la positividad.

La intuición física detrás de requerir que un canal cuántico sea completamente positivo es la siguiente. Supongamos que un sistema pequeño $\mathcal{H}$ es subsistema de uno más grande $\mathcal{H}' \otimes \mathcal{H}$ donde $\dim \mathcal{H}' = k$. Supongamos también que ρ es un estado en $\mathcal{H}$. Se puede verificar que $\mathbb{1}_k \otimes \rho$ es un estado sobre $\mathcal{H}' \otimes \mathcal{H}$. Ahora, si T es un canal sobre $\mathcal{H}$, el operador $\mathbb{1}_k \otimes T$ representaría una operación trivial fuera de $\mathcal{H}$ y la operación T en $\mathcal{H}$. La positividad completa es necesario para que el resultado de la operación $(\mathbb{1}_k \otimes T) = \mathbb{1}_k \otimes T(\rho)$ sea positivo y por lo tanto un estado para todo $k \geq 1$. Ver el ejercicio p.3.1.2.1.

Ejercicios de la sección

P.3.1.2.1 Verifique que el operador de transposición $T : \mathbb{M}_2(\mathbb{C}) \to \mathbb{M}_2(\mathbb{C})$ es positivo pero no es completamente positivo. Sugerencia: Considere el mapeo $\mathbb{1} \otimes T$.

3.1.3 El Qubit

En lugar de bits en sistemas clásicos, la unidad fundamental de la información cuántica es el *qubit* o también llamado *bit cuántico*. A diferencia de un bit clásico, que puede estar exclusivamente en los estados 0 o 1 , un qubit es un objeto que puede estar en una superposición de dos estados que denotaremos por $|0\rangle$ y $|1\rangle$. La propiedad de *superposición* que es característica de la mecánica cuántica será descrita a continuación.

Frecuentemente se asocia con cada vector unitario de un espacio de Hilbert un estado puro como sigue. Al vector $\psi \in \mathcal{H}$, $\|\psi\| = 1$, se le asocia el estado puro $|\psi\rangle\langle\psi|$. Denotaremos a esta asociación utilizando el *ket*:

$$\psi \in \mathcal{H},\ \|\psi\| = 1, \quad \psi \longleftrightarrow |\psi\rangle; \quad \text{donde } |\psi\rangle := |\psi\rangle\langle\psi|.$$

Fijemos por el momento un espacio de Hilbert de dimensión dos y abusando de la notación denotemos por 0 y 1 a sus elementos básicos[1] y , i.e., $\mathcal{H} = \text{span}\{0,1\}$ Un qubit se escribe como

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \alpha,\beta \in \mathbb{C} \tag{3.2}$$

donde $|\alpha|^2 + |\beta|^2 = 1$. $|0\rangle$ y $|1\rangle$ denotan los estados puros $|0\rangle\langle 0|$ y $|1\rangle\langle 1|$ respectivamente. Por otro lado el estado puro $|\psi\rangle$ se obtiene mediante una combinación lineal convexa de $|0\rangle$ y $|1\rangle$, que sabemos es un estado también (ver definición 2.61). Lo anterior es la llamada *superposición de estados*.

La capacidad de un qubit de estar en una superposición de estados desafía nuestro sentido común del mundo físico que nos rodea. Un bit clásico es como el estado de una moneda: muestra águila o muestra sol. Por supuesto, aunque podría pensarse en el caso en que la moneda está perfectamente balanceada en su contorno, este caso es ideal y podemos descartarlo. En contraste, un qubit puede existir en un *continuo* de estados entre $|0\rangle$ y $|1\rangle$ antes de ser observado o medido. Una vez efectuada la medición el estado del qubit se colapsa ya sea a $|0\rangle$ o $|1\rangle$ con probabilidades $|\alpha|^2$ y $|\beta|^2$ respectivamente. Es decir, el qubit $|\psi\rangle$ que está en la superposición de estados $|0\rangle$ y $|1\rangle$ dado por (3.2), con α y β fijos, se tiene

$$P\big(\text{Observar } |0\rangle \text{ al medir } |\psi\rangle\big) = |\alpha|^2; \qquad P\big(\text{Observar } |1\rangle \text{ al medir } |\psi\rangle\big) = |\beta|^2.$$

Existe una representación útil de un qubit en $\mathbb{R}^3$ conocida como representación de Bloch o esfera de Bloch. Aunque en principio podría pensarse que se necesitan 4 parámetros reales para describir a un qubit, la condición $|\alpha|^2 + |\beta|^2 = 1$ implica que solo se necesitan tres. El qubit de (3.2) puede reescribirse como

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

[1] Podemos considerar una realización de $\mathcal{H}$ como $\mathbb{C}^2$ considerando a $0 = \begin{pmatrix}1\\0\end{pmatrix}$ y $1 = \begin{pmatrix}0\\1\end{pmatrix}$. Enfatizamos que esto es un abuso de notación.

donde $\theta \in [0,\pi]$ es el ángulo polar, $\phi \in [0,2\pi]$ el ángulo azimutal y $\gamma \in \mathbb{R}$ un factor de fase.

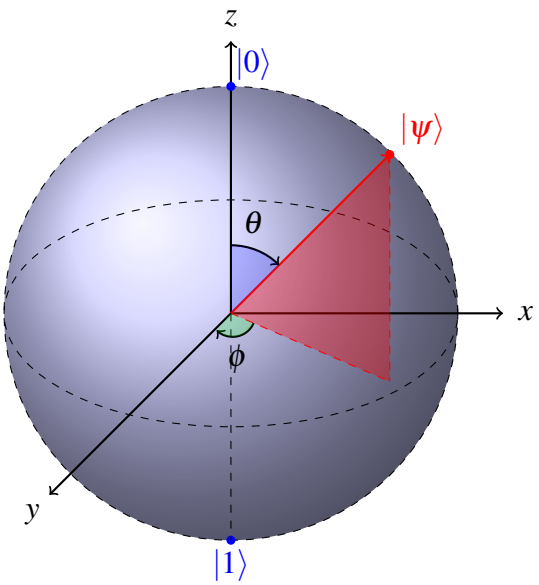


Figura 3.1: Esfera de Bloch

3.1.4 n-Qubits

Regresando al contexto clásico, dos bits pueden tomar 4 posibles estados: 00, 01, 10 y 11. De manera análoga esperaríamos que un sistema de dos qubits tendrá cuatro estados básicos *computacionales* denotados $|00\rangle$, $|01\rangle$, $|10\rangle$ y $|11\rangle$. Para obtener entonces un sistema de dos qubits debemos ejecutar el producto tensorial $\mathcal{H}\otimes\mathcal{H}$ donde $\mathcal{H} = \text{span}\{0,1\}$ es el sistema de un qubit. Para ver las propiedades principales del producto tensorial consultar la sección 2.5.

Ejemplo 3.5. El sistema de 2-qubits es el 2-producto tensorial del espacio de Hilbert asociado a un solo qubit $\mathcal{H} = \mathbb{C}^2$. Explícitamente $\mathcal{H}^{\otimes 2} = \mathcal{H}\otimes\mathcal{H}$ cuya base es

$$|00\rangle = |0\rangle\otimes|0\rangle, \quad |01\rangle = |0\rangle\otimes|1\rangle, \quad \alpha_{ij}\in\mathbb{C},$$
$$|10\rangle = |1\rangle\otimes|0\rangle, \quad |11\rangle = |1\rangle\otimes|1\rangle.$$

Por lo tanto un 2-qubit $|\psi\rangle$ general es una combinación lineal de los anteriores

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

donde $|\alpha_{00}|^2 + |\alpha_{10}|^2 + |\alpha_{01}|^2 + |\alpha_{11}|^2 = 1$.

Observemos que como $\mathcal{H}\cong\mathbb{C}^2$ entonces $\mathcal{H}\otimes\mathcal{H}\cong\mathbb{C}^{2(2)} = \mathbb{C}^4$.

De manera similar al caso de un solo qubit, la probabilidad de medir u observar algún subconjunto de los posibles estados $|00\rangle$, $|01\rangle$, $|10\rangle$ y $|11\rangle$ está dado por los coeficientes.

$$\begin{aligned} P\big(\text{Observar un } |0\rangle \text{ en el primer qubit de } |\psi\rangle\big) &= P\big(\text{Observar un } |00\rangle \text{ o } |01\rangle \text{ en } |\psi\rangle\big) \\ &= |\alpha_{00}|^2 + |\alpha_{01}|^2. \end{aligned}$$

Y en este caso el estado final después de la medición (o colapsado) será

$$|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}.$$

Ejemplo 3.6. El estado en $\mathcal{H}\otimes\mathcal{H}$ dado por

$$|\psi_B\rangle = \frac{|00\rangle + |11\rangle}{2}$$

se conoce[2] como *estado de Bell* o *par de EPR*[3]. Podemos encontrar una representación matricial explícita de este estado recordando que tiene asociado el estado puro

$$\begin{aligned}
|\psi_B\rangle\langle\psi_B| &= \left|\frac{00+11}{\sqrt{2}}\right\rangle\left\langle\frac{00+11}{\sqrt{2}}\right| = \frac{|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|}{2} \\
&= \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\
&= \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}.
\end{aligned}$$

El estado de Bell tiene la propiedad de que después de medir el primer qubit se obtienen dos posibles resultados con probabilidad $1/2$:

$$\begin{aligned}
P\big(\text{Observar un } |0\rangle \text{ en el primer qubit de } |\psi_B\rangle\big) &= P\big(\text{Observar un } |00\rangle \text{ o } |01\rangle \text{ en } |\psi_B\rangle\big) \\
&= |\alpha_{00}| = \frac{1}{2};
\end{aligned}$$

$$\begin{aligned}
P\big(\text{Observar un } |1\rangle \text{ en el primer qubit de } |\psi_B\rangle\big) &= P\big(\text{Observar un } |10\rangle \text{ o } |11\rangle \text{ en } |\psi_B\rangle\big) \\
&= |\alpha_{11}| = \frac{1}{2}.
\end{aligned}$$

Y el estado final después de la medición será $|\psi'_B\rangle = |00\rangle$ o $|\psi'_B\rangle = |11\rangle$ respectivamente. Si ahora se ejecuta una segunda medición del segundo qubit de $|\psi'_B\rangle$ se obtendrá lo que se haya obtenido en la primera medición. Podemos expresar lo anterior utilizando probabilidad condicional como sigue

$$P\left(\text{Medir un } |0\rangle \text{ en el segundo qubit de } |\psi'_B\rangle \,\middle|\, \text{Se midió un } |0\rangle \text{ en el primer qubit de } |\psi_B\rangle\right) = 1;$$

$$P\left(\text{Medir un } |0\rangle \text{ en el segundo qubit de } |\psi'_B\rangle \,\middle|\, \text{Se midió un } |1\rangle \text{ en el primer qubit de } |\psi_B\rangle\right) = 0;$$

[2] El estado de Bell no es único. Es posible construir otros estados de Bell utilizando, por ejemplo, circuitos cuánticos.

[3] Einstein–Podolsky–Rosen

$$P\left(\text{Medir un } |1\rangle \text{ en el segundo qubit de } |\psi'_B\rangle \,\middle|\, \text{Se midió un } |1\rangle \text{ en el primer qubit de } |\psi_B\rangle\right)=1;$$

$$P\left(\text{Medir un } |1\rangle \text{ en el segundo qubit de } |\psi'_B\rangle \,\middle|\, \text{Se midió un } |0\rangle \text{ en el primer qubit de } |\psi_B\rangle\right)=0.$$

Es decir, las lecturas de las mediciones están correlacionadas.

Finalmente contextualicemos la notación utilizada en el marco de productos tensoriales. Primero de manera general y después para el caso de un sistema de n-qubits.

Considere un espacio de Hilbert $\mathcal{H}$ cuya base ortonormal es indexada por un conjunto A, digamos $\{e_x : x \in A\}$. Abusamos de la notación y usamos los subíndices para referirnos a los vectores básicos $x \to e_x$ por comodidad. El conjunto de índices A juega el papel del alfabeto con el cual construiremos palabras de longitud finita. Es decir, una palabra de longitud n es un elemento de A^n, por lo tanto es una n-túpla $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in A^n$, $x_i \in A$, la cual podemos representar por un elemento $\mathbf{x} = e_{x_1} \otimes e_{x_2} \otimes \cdots \otimes e_{x_n}$ en el n-producto tensorial del espacio de Hilbert: $\mathcal{H}^{\otimes n}$.

A cada elemento (después de normalización) de un espacio de Hilbert lo podemos asociar con un estado puro. Quedando pues la asociación como sigue:

$$|\mathbf{x}\rangle\langle\mathbf{x}| = |\mathbf{x}\rangle = |x_1 x_2 \ldots x_n\rangle = |e_{x_1} \otimes e_{x_2} \otimes \cdots \otimes e_{x_n}\rangle \longleftrightarrow e_{x_1} \otimes e_{x_2} \otimes \cdots \otimes e_{x_n} \in \mathcal{H}^{\otimes n}.$$

Cuando $A = \mathbb{Z}_2$ y $n = 2$, el espacio de Hilbert $\mathcal{H}^{\otimes n}$ es el espacio de n-qubits. La siguiente discusión aclara la notación usada en el ejemplo 3.5 e ilustra el caso de 3-qubits.

Ejemplo 3.7. Para un grupo finito G se tiene el espacio de Hilbert $\mathcal{H} = \ell_2(G) = \{\alpha : G \to \mathbb{C}\}$ dotado del producto interno

$$\langle \alpha, \beta \rangle = \sum_{g \in G} \overline{\alpha(g)} \beta(g).$$

Una base ortonormal $\{e_h\}_{h \in G}$ de este espacio está dado por

$$e_h(g) = \begin{cases} 1, & \text{si } h = g \\ 0, & \text{otro.} \end{cases}.$$

Observemos que $\mathcal{H} = \mathbb{C}^{|G|}$.

Notemos que en el ejemplo anterior, si consideramos como alfabeto a $A = G = \mathbb{Z}_2$ entonces $\mathcal{H} = \ell_2(G) \cong \mathbb{C}^2$ es el espacio de un qubit.

Ejemplo 3.8. Consideremos el grupo $G = \mathbb{Z}_2^3 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ que explícitamente es el grupo

$$\{000, 001, 010, 100, 011, 101, 110, 111\}. \tag{3.3}$$

Se puede verificar que

$$\ell_2(G) = \ell_2(\mathbb{Z}_2) \otimes \ell_2(\mathbb{Z}_2) \otimes \ell_2(\mathbb{Z}_2)$$

por lo que si $\{e_0, e_1\}$ denota la base ortonormal de $\ell_2(\mathbb{Z}_2)$ entonces $\{e_i \otimes e_j \otimes e_k : i, j, k \in \mathbb{Z}_2\}$ es una base ortonormal para $\ell_2(G)$ por lo que

$$\ell_2(G) = \text{span}\,\{e_i \otimes e_j \otimes e_k : i, j, k \in \mathbb{Z}_2\} \cong \mathbb{C}^{2^3}.$$

Finalmente, por ejemplo, al vector unitario $\psi \in \ell_2(G)$ dado por

$$\psi = \tfrac{1}{\sqrt{2}}(e_0 \otimes e_0 \otimes e_1 + e_1 \otimes e_1 \otimes e_0)$$

le corresponde el estado puro

$$|\psi\rangle = \left|\frac{001+110}{\sqrt{2}}\right\rangle = \frac{|001\rangle + |110\rangle}{\sqrt{2}}$$

de forma explícita

$$\begin{aligned}|\psi\rangle\langle\psi| &= \frac{|001\rangle\langle 001| + |001\rangle\langle 110| + |110\rangle\langle 001| + |110\rangle\langle 110|}{2} \\ &= \frac{1}{2}\big(|0\rangle\langle 0| \otimes |0\rangle\langle 0| \otimes |1\rangle\langle 1| + |0\rangle\langle 1| \otimes |0\rangle\langle 1| \otimes |1\rangle\langle 0| + |1\rangle\langle 0| \otimes |1\rangle\langle 0| \otimes |0\rangle\langle 1| \\ &\quad + |1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes |0\rangle\langle 0|\big)\end{aligned}$$

y que respecto a la base ordenada como aparecen en (3.3) su representación matricial es

$$|\psi\rangle\langle\psi| = \tfrac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Del ejemplo anterior es claro que el espacio de n-qubits es isomorfo a $\mathbb{C}^{2^n}$. Una consecuencia de la superposición de estados es que en la codificación cuántica, n-qubits escalan el espacio computacional en un factor de 2^n. Esto motiva que de tener algoritmos y hardware que exploten esta ventaja, se necesitan esquemas de codificación, decodificación y correccion de errores para los qubits.

Ejercicios de la sección

P.3.1.4.1 Calcule una representación matricial de los siguientes estados de Bell

a) $\frac{|00\rangle + \langle 11|}{2}$.
b) $\frac{|01\rangle + \langle 10|}{2}$.
c) $\frac{|00\rangle - \langle 11|}{2}$.
d) $\frac{|01\rangle - \langle 10|}{2}$.

P.3.1.4.2 Verifique todos los cálculos del ejemplo 3.8.

3.2 Códigos cuánticos correctores de errores

Los canales cuánticos se utilizan para describir la evolución de un estado debido a las transformaciones que experimenta durante la transmisión de información, i.e., los canales encapsulan la dinámica

de los sistemas cuánticos en presencia de ruido y otras formas de interacción con el entorno. En la mecánica cuántica y la teoría de la información cuántica, los canales permiten modelar cómo se transforman los estados cuánticos cuando se someten a procesos físicos que pueden incluir ruido, decoherencia, pérdida de información entre otros.

Existen tres principios fundamentales que soportan la teoría matemática de transmitir información en el contexto de información cuántica.

1. Un mensaje es codificado en un estado cuántico (el estado *inicial*) y se transmite por medio de canales cuánticos.

2. El estado final podría no ser el mismo que el estado iniciar debido a la presencia de ruido en el canal.

3. Hay estados cuánticos más convenientes que otros que al ser transmitidos por un canal ruidoso lleva a estados finales de los cuales se puede recuperar el estado inicial de manera intacta o con un pequeño margen de error.

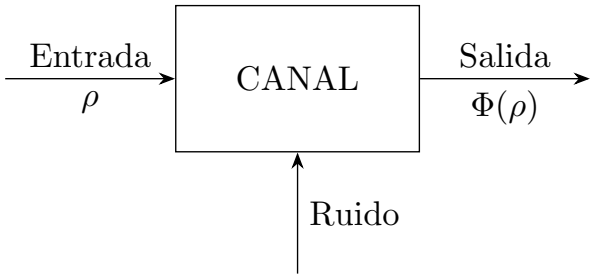


Figura 3.2: Diagrama del canal cuántico.

Si usamos un canal Φ para transmitir un estado puro inicial $|\psi\rangle\langle\psi|$, el estado final que resulta $\Phi(|\psi\rangle\langle\psi|) = \sum_i L_i|\psi\rangle\langle\psi|L_i^*$ será en general un estado mezclado. Los L_i son los elementos responsables de introducir ruido durante la transmisión, por esta razón se les suele llamar matrices de ruido o error.

En un principio nos gustaría encontrar un canal cuántico Ψ que corrigiera los errores introducidos por Φ al mandar un mensaje, en símbolos

$$\Psi(\Phi(\rho)) = \Phi(\Psi(\rho)) = \rho \quad \text{para todo estado } \rho.$$

Sin embargo es conocido [8] que esto solo puede suceder si el canal consta de un solo término unitario, i.e., $\Phi(\rho) = U\rho U^*$, para alguna matriz unitaria U.

Esto quiere decir que los únicos canales que tenemos oportunidad de corregir para todo estado son aquellos que consisten de un solo operador de Kraus unitario. Esta es una seria limitación y debemos relajar un poco nuestras expectativas.

Para poder tener oportunidad de encontrar canales que corrijan una familia de canales más amplia debemos de debilitar los requisitos que estamos considerando; sacrificaremos entonces el poder decodificar cualquier estado a solo decodificar estados que actúen *no trivialmente* en solamente cierta parte del espacio $\mathcal{H}$, más precisamente, en un subespacio propio $\mathcal{C} \subsetneq \mathcal{H}$. A este subespacio le llamamos *código cuántico*.

Definición 3.9. Un código cuántico $\mathcal{C}$ en un espacio de Hilbert $\mathcal{H}$ es un subespacio vectorial de $\mathcal{H}$.

Definición 3.10. El soporte de un estado ρ es el conjunto

$$\text{supp}\,\rho = \{\phi \in \mathcal{H} : \rho\phi \neq 0\}.$$

Si supp $\rho \subset C$ diremos que ρ está soportado en $\mathcal{C}$.

Ejemplo 3.11. Consideremos el sistema de un qubit $\mathcal{H} = \text{span}\{|0\rangle, |1\rangle\}$.

- $\mathcal{C} = \text{span}\{|0\rangle\}$ es un código cuántico pues $\mathcal{C}$ es un subespacio de $\mathcal{H}$.
- El estado $\rho = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ está soportado en $\mathcal{C}$. Para cualquier vector no nulo en $\phi \in \mathcal{C}$ vemos que $\rho\phi = \alpha\rho|0\rangle = \alpha\,|0\rangle\langle 0|\,|0\rangle = \alpha|0\rangle \neq 0$, i.e., ρ actúa no trivialmente en $\mathcal{C}$.
- Considere ahora el estado $\rho = |1\rangle\langle 1| + \rho_{0,1}\,|0\rangle\langle 1| + \overline{\rho_{0,1}}\,|1\rangle\langle 0| = \begin{pmatrix} 0 & \rho_{0,1} \\ \overline{\rho_{0,1}} & 1 \end{pmatrix}$, $\rho_{0,1} \in \mathbb{C}$.

  Vemos que

$$\begin{pmatrix} 0 & \rho_{0,1} \\ \overline{\rho_{0,1}} & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \neq 0 \Leftrightarrow \rho_{0,1} \neq 0 \text{ o } y \neq 0.$$

  Por lo tanto si $\rho_{0,1} \neq 0$ entonces supp $\rho = \mathcal{H}$ mientras que si $\rho_{0,1} = 0$ entonces

$$\text{supp}\,\rho = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} : y \neq 0 \right\}.$$

Antes de continuar precisemos la diferencia entre reversibilidad e inveritibilidad de un canal. Un canal cuántico se dice ser invertible (como función) si existe un operador lineal Ψ tal que $\Psi(\Phi(\rho)) = \Phi(\Psi(\rho)) = \rho$ para todo ρ, sin imponer restricción alguna sobre Ψ (o ρ). Sin embargo este inverso podría **no ser** un canal, como ilustra el siguiente ejemplo.

Ejemplo 3.12. Consideremos la familia de operadores en $\mathcal{H} = \mathbb{C}^2$ de la forma

$$\Phi_s(\rho) = s\rho + (1-s)\text{tr}(\rho)\,\frac{I}{2}, \quad \text{donde } s \in \mathbb{R}.$$

Notemos que Φ_s preserva la traza pero es positivo si y solo si $0 \leq s \leq 1$, i.e., solo en este caso es un canal cuántico.

Denotando por $e_{ij} = |e_i\rangle\langle e_j|$ a la base canónica ordenada $B = (e_{11}, e_{12}, e_{21}, e_{22})$ de $\mathbb{M}_2(\mathbb{C})$ obtengamos $[\Phi]_B$ la representación matricial de Φ respecto a la base ordenada B. Calculando explícitamente los elementos de matriz obtenemos

$$([\Phi]_B)_{ij,lk} = \langle e_{ij}, \Phi(e_{lk})\rangle = \text{tr}\left(e_{ji}e_{lk}\right) = s\delta_{il}\delta_{jk} + \frac{(1-s)}{2}\delta_{ij}\delta_{lk}$$

de donde concluímos que Φ_s es invertible si y solo si

$$0 = \det[\Phi_s]_B = \det \begin{bmatrix} \frac{1-s}{s} + s & 0 & 0 & \frac{1-s}{2} \\ 0 & s & 0 & 0 \\ 0 & 0 & s & 0 \\ \frac{1-s}{2} & 0 & 0 & \frac{1-s}{s} + s \end{bmatrix} = -s^3 \Leftrightarrow s = 0.$$

Se puede verificar que cuando $s \neq 0$ la inversa está dada por

$$\Phi_s^{-1}(\rho) = \frac{s-1}{s}(\mathrm{tr}\,(\rho))\frac{I}{2} + \frac{\rho}{s}. \tag{3.4}$$

Sin embargo Φ_s^{-1} no es un canal para $0 < s \leq 1$, pues falla en preservar positividad.

3.2.1 Teorema de Knill-Laflamme

Supongamos que dado un código $\mathcal{C} \subsetneq \mathcal{H}$ y un canal Φ existe un número finito de matrices $\{R_j\}$ satisfaciendo $\sum_i R_i^* R_i = I$ tales que, si $\rho = \Phi(|\psi\rangle\langle\psi|)$ es el estado final de aplicar Φ al estado puro con $\psi \in \mathcal{C}$, explícitamente

$$\rho = \sum_i L_i |\psi\rangle\langle\psi| L_i^*, \quad \psi \in \mathcal{C},$$

se cumple que

$$\sum_j R_j \rho R_j^* = \sum_j R_j \Phi(|\psi\rangle\langle\psi|) R_j^* = \sum_j \sum_i R_j L_i |\psi\rangle\langle\psi| L_i^* R_j^* = |\psi\rangle\langle\psi|.$$

Es decir, el canal construido a partir $\{R_j\}$ puede *invertir* a Φ si nos restringimos a estados soportados en $\mathcal{C}$. En este caso diremos que la familia $\{R_j\}$ es una familia de operadores de recuperación o decodificación mediante la cual podemos corregir los errores inducidos por Φ (o equivalentemente, inducidos por los operadores de error $\{L_i\}$) al usar el código $\mathcal{C}$.

En la siguiente definición se generaliza esta idea.

Definición 3.13. Sea $\mathcal{A}$ una familia de operadores en $\mathcal{H}$. Un subespacio $\mathcal{C} \subsetneq \mathcal{H}$ es un $\mathcal{A}$-código cuántico corrector de errores (QECC) si existen $\{R_j\}$ tales que para todo estado ρ soportado en $\mathcal{C}$ y toda colección finita de $\{L_i\} \subset \mathcal{A}$ que cumple $\sum_i L_i^* L_i = I$, se tiene que

$$\sum_j \sum_i R_j L_i \rho L_i^* R_j^* = \rho.$$

La siguiente proposición nos da condiciones equivalentes que los operadores de recuperación deben de satisfacer sobre el código $\mathcal{C}$.

Proposición 3.14. *$\mathcal{C} \subsetneq \mathcal{H}$ es un $\mathcal{A}$-QECC si y solo si existen $\{R_j\}$ tales que*

i) $\sum_j R_j^* R_j = I$

ii) $R_j L P_{\mathcal{C}} = \lambda_j(L) P_{\mathcal{C}}$, $\lambda(L) \in \mathbb{C}$ *para toda* $L \in \mathcal{A}$.

donde $P_{\mathcal{C}}$ es la proyección ortogonal sobre el subespacio $\mathcal{C}$.

Demostración. Supongamos que $\mathcal{C}$ es un $\mathcal{A}-$QECC con operadores de recuperación $\{R_i\}$. Sea $L \in \mathcal{A}$ arbitrario, y $\{L_i\}$ una familia de operadores de error en $\mathcal{A}$ tales que $L \in \{L_i\}$ y $\sum_i L_i^* L_i = I$. Entonces si $u \in \mathcal{C}$, $\|u\| = 1$ se satisface

$$\sum_j \sum_i R_j L_i |u\rangle\langle u| L_i^* R_j^* = |u\rangle\langle u|,$$

de donde, si $v \in \{u\}^{\perp}$, entonces

$$\sum_{j,i} |\langle v, R_j L_i u\rangle|^2 = \sum_{j,i} \langle v, R_j L_i u\rangle \langle R_j L_i u, v\rangle = \left\langle v, \sum_{j,i} R_j L_i |u\rangle\langle u| L_i^* R_j^* v \right\rangle = \left\langle v, |u\rangle\langle u| v \right\rangle = 0$$

y por lo tanto $\langle v, R_j L_i u\rangle = 0$ para todo j,i. Es decir, $R_j L_i u = \lambda(u) u$, para algún $\lambda(u) \in \mathbb{C}$ y en particular $R_j L P_{\mathcal{C}} = \lambda_j(L) P_{\mathcal{C}}$.

Por otro lado si $\{R_j\}$ cumple *i)* y *ii)*, dados $\{L_i\} \subset \mathcal{A}$ con $\sum_i L_i^* L_i = I$ se tiene que la traza se conserva y si $u \in \mathcal{C}$,

$$\sum_{j,i} |\lambda_j(L_i)|^2 \mathrm{tr}\,(|u\rangle\langle u|) = \mathrm{tr}\left(\sum_{j,i} R_j L_i |u\rangle\langle u| L_i^* R_j^* \right) = \mathrm{tr}\,(|u\rangle\langle u|) \Rightarrow \sum_{j,i} |\lambda_j(L_i)|^2 = 1,$$

de donde se sigue que, si $\|u\| = 1$, por *ii)* tenemos que

$$\sum_{j,i} R_j L_i |u\rangle\langle u| L_i^* R_j^* = \sum_{j,i} |\lambda_j(L_j)|^2 |u\rangle\langle u| = |u\rangle\langle u|,$$

i.e., $\{R_j\}$ decodifica estados puros soportados en $\mathcal{C}$. Usando linealidad obtenemos que $\{R_j\}$ decodifica cualquier estado (es decir estados mezclados) soportados en $\mathcal{C}$. □

Observemos que la proposición pasada caracteriza a las familias $\{R_j\}$ que son decodificadoras de un subespacio $\mathcal{C}$ y una familia $\mathcal{A}$ dadas.

Sin embargo el siguiente teorema da condiciones para la existencia de $\{R_j\}$ que solo dependen del $\mathcal{C}$ y $\mathcal{A}$.

Teorema 3.15 (Knill-Laflamme 1997). *Sea $\mathcal{C} \subsetneq \mathcal{H}$ un subespacio con base ortonormal $\psi_1, \ldots, \psi_d$, y $\mathcal{A}$ una familia de operadores sobre $\mathcal{H}$. Entonces existe una familia de operadores $\{R_j\}$ tales que $\mathcal{A}(\mathcal{C}, \{R_j\})$ es un QECC si y solo si*

a) $\langle \psi_p, L_1^* L_2 \psi_q\rangle = 0$, para toda $L_1, L_2 \in \mathcal{A}$ y $p \neq q$, $p,q = 1, \ldots, d$.

b) $\langle \psi_p, L_1^* L_2 \psi_p\rangle$ no depende de $p = 1, \ldots, d$.

Demostración. Si $\mathcal{A}(\mathcal{C}, \{R_j\})$ es un QECC entonces por la proposición anterior

$$\begin{aligned} \langle \psi_p, L_1^* L_2 \psi_q\rangle &= \langle \psi_p, L_1^* \sum_j R_j^* R_j L_2 \psi_q\rangle = \sum_j \lambda_j(L_2)\overline{\lambda_j(L_1)} \langle \psi_p, \psi_q\rangle \\ &= \begin{cases} \sum_j \lambda_j(L_2)\overline{\lambda_j(L_1)}, & \text{si } p = q \\ 0, & \text{si } p \neq q \end{cases}. \end{aligned}$$

Para el recíproco consideremos los d subespacios $\mathcal{A}\psi_i = \{L\psi_i : L \in \mathcal{A}\}$ y sean $\varphi_i^1, \varphi_i^2, \ldots, \varphi_i^{l_i}$ bases ortonormales de cada uno de ellos donde $\dim \mathcal{A}\psi_i = l_i$.

ψ_1	ψ_2	$\cdots$	ψ_j	$\cdots$	ψ_d
$\mathcal{A}\psi_1$	$\mathcal{A}\psi_2$	$\cdots$	$\mathcal{A}\psi_j$	$\cdots$	$\mathcal{A}\psi_d$

$$\begin{array}{|cccccc|}\hline \varphi_1^1 & \varphi_2^1 & \cdots & \varphi_j^1 & \cdots & \varphi_d^1 \\ \vdots & \vdots & \cdots & \vdots & \cdots & \vdots \\ \varphi_1^i & \varphi_2^i & \cdots & \varphi_j^i & \cdots & \varphi_d^i \\ \vdots & \vdots & \cdots & \vdots & \cdots & \vdots \\ \varphi_1^l & \varphi_2^l & \cdots & \varphi_j^l & \cdots & \varphi_d^l \\ \hline \end{array}$$

Sea $U_{ij} : \mathcal{A}\psi_i \to \mathcal{A}\psi_j$ el operador lineal definido por $L\psi_i \mapsto L\psi_j, L \in \mathcal{A}$. Este es unitario pues es suprayectivo y si $x, y \in \mathcal{A}\psi_i$ entonces

$$\langle U_{ij}x, U_{ij}y\rangle = \langle U_{ij}L\psi_i, U_{ij}L'\psi_i\rangle = \langle \psi_j, LL'\psi_j\rangle = \langle \psi_i, LL'\psi_i\rangle = \langle x, y\rangle,$$

en donde en la penúltima igualdad usamos *b)*. Esto implica que todos los subespacios tienen la misma dimensión l. Sea entonces U_j el operador unitario que manda la base de $\mathcal{A}\psi_1$ en la base de $\mathcal{A}\psi_j$, i.e., $U_j\varphi_1^i = \varphi_j^i$. Además por la condición *a)* los subespacios son mutuamente ortogonales $\mathcal{A}\psi_p \perp \mathcal{A}\psi_q$ si $p \neq q$. Sea $E_i = \sum_k |\varphi_i^k\rangle\langle\varphi_i^k|$ la proyección ortogonal sobre el subespacio generado por el i-ésimo renglón, y $V^{(i)}$ el operador sobre ese subespacio tal que $V^{(i)}\varphi_j^i = \psi_j$ para $i = 1, 2, \ldots, l$, el cual cumple que

$$\langle V^{(i)}\varphi_j^i, V^{(i)}\varphi_k^i\rangle = \langle \psi_j, \psi_k\rangle = \delta_{jk} = \langle \varphi_j^i, \varphi_k^i\rangle,$$

que nuevamente es suprayectivo y por lo tanto unitario. Definamos $R_i = V^{(i)}E_i$ para $i = 1, \ldots, l$ y R la proyección ortogonal sobre el complemento ortogonal del recuadro, i.e., sobre

$$\square^\perp = \{\varphi_j^i : 1 \leq j \leq d, 1 \leq i \leq l\}^\perp.$$

Mostraremos que $\{R_i\} \cup \{R\}$ es la familia decodificadora que buscamos.

i) Si $x = x_\square + x_\square^\perp \in \mathcal{H}$ es la descomposición ortogonal en $\square$ y $\square^\perp$ entonces

$$\Big(\sum_i R_i^* R_i + R^* R\Big)x = \sum_i R_i^* R_i x_\square + R^* R x_\square^\perp = x_\square + x_\square^\perp = x.$$

pues $R_i^* R_i x_\square = E_i V^{(i)*} V^{(i)} E_i x_\square = x_\square$. De donde $\Big(\sum_i R_i^* R_i + R^* R\Big) = I$.

ii) Sea $\psi \in \mathcal{C}$, entonces existen $c_j \in \mathbb{C}$ tales que

$$L\psi = c_1 L\psi_1 + c_2 L\psi_2 + \cdots + c_d L\psi_d = c_1 L\psi_1 + c_2 U_2 L\psi_1 + \cdots + c_d U_d L\psi_1$$

Pero como $L\psi_1$ es un elemento de $\mathcal{A}\psi_1$, expandiendolo en términos de la base ortonormal tenemos que $L\psi_1 = \lambda_1(L)\varphi_1^1 + \lambda_2(L)\varphi_1^2 + \cdots + \lambda_l(L)\varphi_1^l,\ \alpha_i(L) \in \mathbb{C}$. De donde

$$\begin{aligned} U_j L\psi_1 &= \lambda_1(L)\varphi_j^1 + \lambda_2(L)\varphi_j^2 + \cdots + \lambda_l(L)\varphi_j^l \\ &\Rightarrow E_i U_j L\psi_1 = \lambda_1(L)\varphi_j^i \\ &\Rightarrow R_i U_j L\psi_1 = V^{(i)} E_i U_j L\psi_1 = \alpha_i(L)\psi_j, \quad i = 1, \ldots, l. \end{aligned}$$

Y por otro lado $RU_j L\psi = 0$. Juntando lo anterior para toda $i = 1, \ldots, l$

$$\begin{aligned} R_i L\psi &= c_1 R_i L\psi_1 + c_2 R_i U_2 L\psi_1 + \ldots + c_d R_i U_d L\psi_d \\ &= c_1\lambda_i(L)\psi_1 + c_2\lambda_i(L)\psi_2 + \cdots + c_d\alpha_i(L)\psi_d \\ &= \lambda_i(L)\psi, \end{aligned}$$

y $RL\psi = 0$. Esto muestra que $\{R_i\} \cup \{R\}$ satisface las condiciones de la proposición 3.14.

Esto concluye la demostración. □

Antes de ilustrar el teorema anterior con algunos ejemplos incluimos sin demostración otro resultado que da condiciones necesarias y suficientes para la existencia de operadores de recuperación.

LEMA 3.16. *Sea $\mathcal{C}$ un código cuántico de $\mathcal{H}$ y $P_{\mathcal{C}}$ la proyección ortogonal sobre él. Sea Φ un canal cuántico con operadores de error $\{L_i\}$. Existe una familia de operadores de recuperación $\{R_j\}$ para Φ en $\mathcal{C}$ si y solo si existen escalares $\alpha_{i,j} \in \mathbb{C}$ tales que*

$$P_{\mathcal{C}} L_i^* L_j P_{\mathcal{C}} = \alpha_{i,j} P_{\mathcal{C}}$$

donde la matriz $(\alpha_{i,j})_{i,j}$ es autoadjunta.

Una prueba de el lema anterior puede encontrarse en [9].

EJEMPLO 3.17. Consideremos el espacio de Hilbert presentado en el ejemplo 3.7 para un G un grupo finito arbitrario, $\mathcal{H} = \ell_2(G) = \{\alpha : G \to \mathbb{C}\} \cong \mathbb{C}^{|G|}$.

Consideremos $g \mapsto U_g$ la representación regular izquierda unitaria de G en $\mathscr{B}(\mathcal{H})$, esta actúa en la base como $U_g e_h = e_{gh}$ y que puede escribirse explícitamente usando la notación de Dirac como

$$U_g = \sum_{h \in G} |e_h\rangle\langle e_{g^{-1}h}|.$$

Llamemos a un subconjunto $E \subset G$ conjunto de errores y a un subconjunto $C \subset G$ conjunto de código. Definamos

$$\mathcal{A} = \operatorname{span}\{U_g : g \in E\} \quad \text{y} \quad \mathscr{C} = \operatorname{span}\{e_g : g \in C\}.$$

Verifiquemos las condiciones de Knill-Laflamme para estos conjuntos.

Por un lado si $r \neq s$ entonces

$$\langle e_r, U_g^* U_h e_s\rangle = \langle e_r, e_{g^{-1}hs}\rangle = \delta_{r,g^{-1}hs} = 0 \quad \text{si} \quad r \neq g^{-1}hs,$$

que es equivalente a $g^{-1}h \neq rs^{-1}$ o $E^{-1}E \cap CC^{-1} = \{e\}$.

Por otro lado $\langle e_r, U_g^* U_h e_r\rangle = \delta_{r,g^{-1}hr} = \begin{cases} 1, & \text{si } r = s \\ 0, & \text{otro,} \end{cases}$.

Lo anterior muestra que el subespacio $\mathcal{C}$ es un $\mathcal{A}$-QECC si se satisface la condición

$$E^{-1}E \cap CC^{-1} = \{e\}.$$

EJEMPLO 3.18. Retomemos ahora el ejemplo 3.8, donde $G = \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2$. Consideremos los subconjuntos

$$E = \{000, 110, 011, 101\} \quad \text{y} \quad C = \{000, 111\},$$

en este caso $E^{-1}E = E - E = \{000, 110, 011, 101\}$ y $CC^{-1} = C - C = \{000, 111\}$ por lo que se cumplen las condiciones de Knill-Laflamme vistas en el ejemplo anterior, debido a que $E^{-1}E \cap CC^{-1} = \{000\}$.

Observemos por otro lado que podemos descomponer a la representación regular izquierda U_{ijk} de G en términos de las representación regular en cada factor $\mathbb{Z}_2$ como sigue.

Sean $0 \mapsto U_0$ y $1 \mapsto U_1$ la representación regular de $\mathbb{Z}_2$ en el espacio $\ell_2(\mathbb{Z}_2)$. Entonces se tiene que $U_{ijk} = U_i \otimes U_j \otimes U_k$, $i, j, k \in \mathbb{Z}_2$.

Por ejemplo,

$$U_{000} = U_0 \otimes U_0 \otimes U_0 = \mathbb{1}_8,$$

$$U_{110} = U_1 \otimes U_1 \otimes U_0 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Por un lado un estado soportado en $\mathcal{C} = \text{span}\{e000, e_{111}\} = \text{span}\{e_0 \otimes e_0 \otimes e_0, e_1 \otimes e_1 \otimes e_1\}$ es de la forma

$$\rho = \alpha\,|000\rangle + \beta\,|111\rangle, \quad \text{con } |\alpha|^2 + |\beta|^2 = 1.$$

El teorema de Knill-Laflamme nos dice que existen operadores de recuperación $\{R_j\}$ tales que

$$\sum_j R_j \Phi(\rho) R_j^* = \rho, \quad \rho \text{ soportado en } \mathcal{C} \tag{3.5}$$

para cualquier canal Φ cuyos operadores de error sean combinaciones lineales de $\{U_{ijk} : ijk \in E\}$. Sin embargo para encontrar explícitamente $\{R_j\}$ hay que seguir la demostración constructiva del teorema. Se queda como ejercicio al lector encontrar la forma explícita de los operadores de recuperación dados por el teorema.

En el esquema que hemos presentado podemos observar que el grupo finito no tiene por qué ser abeliano. Veamos el siguiente ejemplo para el grupo finito no abeliano más simple.

Ejemplo 3.19. Consideremos ahora el grupo simétrico $S_3 = \{e, g_1, g_2, g_3, g_4, g_5\}$ donde etiquetamos a los elementos de acuerdo a

$$e = \text{Identidad},\ g_1 = (1,2),\ g_2 = (2,3),\ g_3 = (1,3),\ g_4 = (1,2,3),\ \text{and } g_5 = (1,3,2).$$

y escogemos $E = \{g_1, g_4\}$ y $C = \{g_2, g_5, g_3\}$. De modo que

$$\mathcal{A} = \text{span}\{U_{g_1}, U_{g_4}\} \ \text{ y } \ \mathcal{C} = \text{span}\{e_{g_2}, e_{g_3}, e_{g_5}\}.$$

Se puede verificar (ejercicio!) que se cumple $E^{-1}E \cap CC^{-1} = \{e\}$.

Observe que los mapeos

$$\Phi_t(\rho) = tU_{g_1}\rho U_{g_1}^* + (1-t)U_{g_4}\rho U_{g_4}^*$$

son canales cuánticos para $1 \leq t \leq t$ y cuyos operadores de error están tomados de la familia $\mathcal{A}$.

El teorema de Knill-Laflamme asegura la existencia de operadores decodificadores o de recuperación $\{R_j\}$ y mediante la prueba constructiva se puede obtener que son

$$R_1 = |g_2\rangle\langle g_4| + |g_3\rangle\langle g_5| + |g_5\rangle\langle g_2|; \quad R_2 = |g_2\rangle\langle g_1| + |g_3\rangle\langle g_2| + |g_5\rangle\langle g_0|.$$

Verifique que estos operadores de recuperación efectivamente satisfacen (3.5).

Ejercicios de la sección

P.3.2.1 Muestre que en el ejemplo 3.12 el operador dado por (3.4) es el inverso de Φ_s para $s \neq 0$.

P.3.2.2 Verifique que Φ_s^{-1} en el ejemplo 3.12 no preserva positividad si $0 \leq s \leq 1$.

P.3.2.3 Verifique que en el ejemplo 3.19, los operadores $\{R_j\}$ dados decodifican cualquier estado soportado en $\mathcal{C}$ para la familia de canales Φ_t.

Sugerencia: Primero verifiquelo para estados puros $|g\rangle\langle g|$ con $g \in C$, i.e., muestre que

$$R_1\Phi_t(|g\rangle\langle g|)R_1^* + R_2\Phi_t(|g\rangle\langle g|)R_2^* = |g\rangle\langle g|.$$

y después extienda mediante un argumento de linealidad.

P.3.2.4 En el mismo ejemplo 3.19, ¿los operadores $\{R_j\}$ decodifican a cualquier canal con operadores de error tomados de $\mathcal{A}$?

3.2.2 Matrices de Pauli

Sabemos que cuando $\mathcal{H}$ es el espacio de un qubit, un operador de error L (que compone, por ejemplo, a un canal cuántico) se identifica con una matriz en $\mathbb{M}_2(\mathbb{C})$. Veremos que podemos encontrar una base del espacio $\mathbb{M}_2(\mathbb{C})$ de modo que la corrección de los elementos de esta base permitirían la corrección de cualquier error.

Las matrices de Pauli son tres matrices complejas 2×2 que son fundamentales en la mecánica cuántica. Fueron introducidas por el físico Wolfgang Pauli y se utilizan para describir, por ejemplo, el espín de partículas cuánticas como los electrones. Las matrices de Pauli son

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}; \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Puede verse que estas matrices son hermitianas y unitarias (ver ejercicios de la sección 2.3), siendo de utilidad para describir las operaciones de rotación y reflexión en el espacio de Hilbert. Además satisfacen las peculiares relaciones

- $\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = \mathbb{1}$
- $[\sigma_i, \sigma_j] = 2i\varepsilon_{ijk}\sigma_k$, donde ε_{ijk} denota el símbolo de Levi-Civita[4].

Estas matrices junto con la identidad $\mathbb{1}$ resultan ser linealmente independientes y forman una base de $\mathbb{M}_2(\mathbb{C})$ pues

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \frac{a+d}{2}\,\mathbb{1} + \frac{c+b}{2}\,\sigma_x - i\frac{c-b}{2}\,\sigma_y + \frac{a-d}{2}\,\sigma_z.$$

Aún más se puede mostrar el siguiente teorema.

[4] $\varepsilon_{ijk} = \begin{cases} +1 & \text{si } (i,j,k) \text{ es } (1,2,3),(2,3,1) \text{ o } (3,1,2) \\ -1 & \text{si } (i,j,k) \text{ es } (3,2,1),(1,3,2) \text{ o } (2,1,3) \\ 0 & \text{de otro modo } i=j \text{ o } j=k \text{ o } k=i \end{cases}$

Teorema 3.20. *1. Toda matriz de $\mathbb{M}_2(\mathbb{C})$ puede ser escrita de manera única como una combinación lineal de las matrices de Pauli y la identidad con coeficientes* ***complejos****.*

2. Cada matriz autoadjunta *de $\mathbb{M}_2(\mathbb{C})$ puede ser escrita de manera única como una combinación lineal de las matrices de Pauli y la identidad con coeficientes* ***reales****, y viceversa, cada combinación lineal de las matrices de Pauli y la identidad con coeficientes* ***reales*** *es una matriz autoadjunta.*

En el contexto de códigos cuánticos, a las matrices σ_x y σ_y de Pauli se les llaman errores de Pauli se les identifican por su subíndice X, Y, o Z respectivamente. En particular veremos que cada una de ellas están asociadas a un tipo específico de error al actuar en un qubit.

1. Error de tipo X o *bit-flip*

   Notando que
   $$X = |0\rangle\langle 1| + |1\rangle\langle 0|$$
   y haciendolo actuar en un qubit arbitrario vemos que
   $$X|\psi\rangle = \alpha X|0\rangle + \beta X|1\rangle = \alpha|1\rangle + \beta|0\rangle.$$
   Es decir, el efecto de X fue el intercambiar $|0\rangle$ por $|1\rangle$ y viceversa. El nombre dado viene en alusión al tipo de error clásico de intercambio de bits. Este tipo de error es el único posible en el contexto clásico.

2. Error de tipo Z o *phase-flip*

   Notando que
   $$Z = |0\rangle\langle 0| - |1\rangle\langle 1|$$
   y haciendolo actuar en un qubit arbitrario observamos que
   $$Z|\psi\rangle = \alpha Z|0\rangle + \beta Z|1\rangle = \alpha|0\rangle - \beta|1\rangle.$$
   Este tipo de error no tiene análogo clásico.

3. Error de tipo Y

   Estos errores son combinaciones de los dos anteriores pues $Y = iXZ$.

Ejercicios de la sección

P.3.2.2.1 Muestre que las matrices de Pauli junto con la matriz identidad forman una base de $\mathbb{M}_2(\mathbb{C})$.

P.3.2.2.2 Verifique el teorema 3.20.

P.3.2.2.3 Muestre las relaciones

- $\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = \mathbb{1}$
- $[\sigma_i, \sigma_j] = 2i\varepsilon_{ijk}\sigma_k$, donde ε_{ijk} denota el símbolo de Levi-Civita[4].

Bibliografía

[1] Asao Arai, *Analysis on Fock spaces and mathematical theory of quantum fields—an introduction to mathematical analysis of quantum fields*, second ed., World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2025. MR 4812858.

[2] M. Sh. Birman and M. Z. Solomjak, *Spectral theory of selfadjoint operators in Hilbert space*, Mathematics and its Applications (Soviet Series), D. Reidel Publishing Co., Dordrecht, 1987, Translated from the 1980 Russian original by S. Khrushchëv and V. Peller. MR 1192782 (93g:47001).

[3] E. Camps-Moreno, *Teoría de códigos*, Notas de la Escuela otoñal de códigos y aplicaciones UAMI, 2024.

[4] P. A. M. Dirac, *A new notation for quantum mechanics*, Proc. Cambridge Philos. Soc. **35** (1939), 416–418. MR 896.

[5] V. Guruswami, A. Rudra, and M. Sudan, *Essential coding theory*, 2019. Draft available at http://cse.buffalo.edu/faculty/atri/courses/coding-theory/book.

[6] Roger A. Horn and Charles R. Johnson, *Topics in matrix analysis*, Cambridge University Press, Cambridge, 1994, Corrected reprint of the 1991 original. MR 1288752.

[7] ———, *Matrix analysis*, second ed., Cambridge University Press, Cambridge, 2013. MR 2978290.

[8] Ashwin Nayak and Pranab Sen, *Invertible quantum operations and perfect encryption of quantum states*, Quantum Info. Comput., vol. 7, 2007, pp. 103–110.

[9] Michael A. Nielsen and Isaac L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, Cambridge University Press, 2011. ISBN: 9781107002173.

[10] K. R. Parthasarathy, *Lectures on Quantum computation, quantum error correcting codes and information theory*, New Delhi, India : Narosa Pub., c2006.

[11] Walter Rudin, *Real and complex analysis*, third ed., McGraw-Hill Book Co., New York, 1987. MR 924157 (88k:00002).

[12] ———, *Functional analysis*, second ed., International Series in Pure and Applied Mathematics, McGraw-Hill, Inc., New York, 1991. MR 1157815 (92k:46001).

[13] R. M. Roth, *Introduction to coding theory*, IET Communications, 47, 2006, pp. 18–19.

[14] Konrad Schmüdgen, *Unbounded self-adjoint operators on Hilbert space*, Graduate Texts in Mathematics, vol. 265, Springer, Dordrecht, 2012. MR 2953553.

[15] J. v. Neumann, *Zur Algebra der Funktionaloperationen und Theorie der normalen Operatoren*, Math. Ann. **102** (1930), no. 1, 370–427. MR 1512583.