Universidad de Valladolid

FACULTAD DE CIENCIAS

TRABAJO FIN DE GRADO

GRADO EN MATEMÁTICAS

CÓDIGOS CORRECTORES DE ERRORES CUÁNTICOS

Autor: Jorge Monzón de Castro
Tutor: Diego Ruano Benito
2024

Prefacio

Este trabajo de fin de grado versa sobre el procesamiento de información cuántica y la corrección de errores, analizando las diferentes técnicas de corrección de errores cuánticos y la teoría necesaria para el desarrollo de esta disciplina.

En los inicios de la computación clásica, la corrección de errores era un área fundamental, debido a que cualquier perturbación del entorno, ya fuesen campos electromagnéticos o ruido de otra naturaleza, podía cambiar el valor de un bit, produciendo una pérdida grave de coherencia en la información. A día de hoy, sin embargo, su importancia no es sino una sombra de lo que un día fue, debido a la enorme mejora de los circuitos y los sistemas de almacenamiento, que impiden cada vez más la interacción crítica de los bits con el entorno, produciendo que un error se reduzca a una posibilidad irrisoria, con una media de un bit perturbado por cada 10^{17} bits ([1]). En la mayoría de los canales de transmisión y almacenamiento de información clásica, se usan códigos con muy poca redundancia y por tanto baja capacidad de corrección de errores. De esta manera, hoy en día, para la mayoría de aplicaciones prácticas puede suponerse que los ordenadores y componentes de almacenamiento, procesamiento y transporte de información modernos están prácticamente exentos de errores. Además, como veremos en el capítulo 3, la teoría de corrección de errores cuánticos se basa en gran medida en su análogo clásico, heredando resultados, propiedades e incluso procedimientos.

Por su parte, la computación cuántica, como es de esperar en una disciplina emergente como en su día lo fue la clásica, no solo no está exenta de errores, sino que la probabilidad de que suceda un error en uno de los *qubits* (el análogo cuántico de los bits) puede llegar a ser comparable a la unidad. Esto se debe a diversos factores, entre los cuales podemos destacar la extrema influencia del entorno sobre los qubits y sobre cualquier tipo de sistema cuántico. Como veremos a lo largo de la memoria, la naturaleza de un sistema cuántico requiere que se encuentre completamente aislado del exterior para preservar la información contenida. Aislar completamente sistemas cuánticos es una tarea que se encuentra en los límites de la ciencia conocida y en la que, sin entrar en detalles, se destina una fracción no despreciable de los presupuestos de multitud de gobiernos y corporaciones, ya que el aislamiento de estos sistemas conlleva una mejor preservación de un fenómeno conocido como *entrelazamiento cuántico* y, en consecuencia, al aumento del número de qubits que pueden usarse al mismo tiempo en un ordenador cuántico, aumentando su capacidad de cálculo y almacenamiento. Por esta razón, la corrección de errores cuánticos es un campo de mucho interés que se encuentra en continuo y ágil desarrollo, con el objetivo de poner remedio a esta, en ocasiones inevitable, interacción de los sistemas cuánticos con el entorno y consiguiente corrupción de la información.

El objetivo de esta memoria es brindar una visión general de la teoría de corrección de errores cuánticos. A excepción de los últimos apartados, referidos a las últimas líneas de desarrollo actuales en este campo, se ha pretendido que esta memoria sea autocontenida, es decir, se ha construido de manera inductiva, introduciendo en riguroso orden todos los conceptos que se utilizan, de manera que cualquier alumno que acabe de terminar el grado en matemáticas pueda comprender en profundidad lo que aquí se expone, sin poseer conocimientos de física, ni mucho menos de física cuántica. Para ello, realizaremos en el capítulo 1 un repaso a los conceptos básicos de la mecánica cuántica, explicados con el formalismo matemático adecuado y haciendo hincapié en las implicaciones físicas de los resultados relevantes, para brindar contexto intuitivo en todo momento y saber exactamente qué es lo que estamos desarrollando y con qué objetivo. Esta introducción teórica a la mecánica cuántica es necesaria para entender los capítulos consecutivos de teoría de la información cuántica y desarrollo de los códigos correctores, ya que se utiliza una notación única de la disciplina de la mecánica cuántica: la notación de Dirac. Posteriormente, en el capítulo 2, introduciremos la teoría de la información cuántica, explicando el concepto fundamental de *qubit* y sus representaciones, así como una formalización del concepto de ruido y error con nociones de distancia de información, clasificando la morfología básica de errores cuánticos. Por último, en el capítulo 3 estudiaremos la teoría de corrección de errores cuánticos, analizando las bases y el comportamiento de los principales códigos correctores cuánticos

partiendo siempre de análogos clásicos, para rematar con unos breves apuntes sobre una de las líneas de investigación actual: los códigos correctores asistidos por entrelazamiento cuántico.

Índice

1. Fundamento teórico

En este capítulo nos familiarizaremos con los conceptos teóricos más relevantes utilizados en la teoría de la información cuántica, expresados en la notación habitual de este campo: la notación de Dirac, para ello, seguiremos una estructura inductiva similar a la del libro [2], con una importante carga de significado físico de los elementos desarrollados.

1.1. Contexto matemático

En mecánica cuántica, consideramos que un elemento (que puede ser, por ejemplo, una partícula) queda totalmente definido por su función de onda. Dicha función podemos englobarla dentro del subespacio $\mathscr{F}$ del espacio de Hilbert $\mathscr{L}^2(\mathbb{R}^n)$ formado por las funciones de $\mathscr{L}^2(\mathbb{R}^n)$ que son "suficientemente regulares" (definidas en todo el dominio, continuas e infinitamente diferenciables).

Observación 1.1. Por simplicidad en la notación, en los siguientes apartados trabajaremos con las coordenadas $\vec{r}$, referidas a la posición física de una partícula. No obstante, como se mencionará en la observación 1.10, podemos construir otros espacios de funciones $\mathscr{F}$ diferentes cambiando la dimensión n de $\mathbb{R}^n$, dependiendo de si nos referimos a posición, momento, spin o cualquier otra magnitud física medible. Lo fundamental es que, dependiendo de la magnitud física con la que trabajemos, deberemos operar en un espacio u otro.

A continuación, conviene recordar algunos conceptos básicos de álgebra y análisis de funciones que nos serán útiles a lo largo de la memoria.

1.1.1. Producto escalar

Definición 1.2. *Para cada par de elementos $\psi(\vec{r})$, $\varphi(\vec{r})$ de $\mathscr{F}$ asociamos un número complejo que llamaremos* ***producto escalar*** *de $\psi(\vec{r})$ y $\varphi(\vec{r})$*

$$(\psi, \varphi) = \int \varphi^*(\vec{r})\psi(\vec{r})d\vec{r}$$

Con esta definición, la norma de una función de onda es

$$\|\psi(\vec{r})\|^2 = (\psi, \psi) = \int \psi^*(\vec{r})\psi(\vec{r})d\vec{r} = \int |\psi(\vec{r})|^2 d\vec{r} \tag{1}$$

Cumpliendo las propiedades habituales.

Observación 1.3. La interpretación física de la norma de una función es probabilística. Para ilustrarlo, elegimos el caso habitual $\mathbb{R}^3$, el espacio tridimensional habitual de posiciones. Si $\psi(\vec{r})$ es la función de onda de posición de una partícula en un determinado instante, entonces la norma $\|\psi(\vec{r})\|_V = \left(\int_V |\psi(\vec{r})|^2 d\vec{r}\right)^{1/2}$ calculada en un abierto $V \subset \mathbb{R}^3$ es la probabilidad de encontrar a la partícula en dicho abierto. Con esta definición, se deduce inmediatamente que, para hablar de conceptos físicos, las funciones de onda deben estar siempre normalizadas, ya que de esta manera la norma de la función en todo su dominio, $\mathbb{R}^3$, será 1. Es decir, la probabilidad de que la posición de la partícula se manifieste dentro del espacio total es 1. Así, en cualquier abierto de $\mathbb{R}^3$, $\|\psi(\vec{r})\| \leq 1$.

1.1.2. Operadores lineales

Definición 1.4. *Un* ***operador lineal*** *A es una correspondencia lineal entre dos funciones de $\mathscr{F}$*

$$\begin{aligned} A : \mathscr{F} &\longrightarrow \mathscr{F} \\ \psi(\vec{r}) &\longmapsto \psi'(\vec{r}) \end{aligned}$$

Propiedad 1.5. El producto de operadores es a su vez un operador, que actúa con la composición habitual $(AB)\psi(\vec{r}) = A(B\psi(\vec{r}))$, generalizable a un número arbitrario de operadores.

Definición 1.6. *Sean A, B dos operadores lineales, definimos el* ***conmutador*** *de A y B como*

$$[A, B] = AB - BA$$

Si $[A, B] = 0$, diremos que los operadores A, B conmutan.

1.1.3. Bases ortonormales discretas en $\mathscr{F}$

Definición 1.7. *Consideramos una familia de funciones $\{u_i(\vec{r})\}_i$ en $\mathscr{F}$. Este conjunto será* ***ortonormal*** *si cada función está normalizada y*

$$(u_i, u_j) = \int u_i^*(\vec{r}) u_j(\vec{r}) d\vec{r} = \delta_{ij}$$

Definición 1.8. *El conjunto ortonormal anterior será* ***base*** *si cada $\psi(\vec{r}) \in \mathscr{F}$ puede expresarse en términos de dicho conjunto ortonormal como sigue:*

$$\psi(\vec{r}) = \sum_i c_i u_i(\vec{r}) \ , \qquad con \quad c_i = \langle u_i, \psi \rangle = \int u_i^*(\vec{r}) \psi(\vec{r}) d\vec{r}$$

Con esta definición de base, recordamos dos resultados básicos que usaremos en adelante:

- **Expansión del producto escalar en términos de la base**

  Consideramos $\varphi(\vec{r}), \psi(\vec{r})$ dos funciones de onda, que podemos expresar en términos de una base $\{u_i\}_i$ como:

  $$\varphi(\vec{r}) = \sum_i b_i u_i(\vec{r}), \ \ \psi(\vec{r}) = \sum_j c_j u_j(\vec{r}) \tag{2}$$

  El producto escalar será

  $$(\varphi, \psi) = \sum_{i,j} b_i^* c_j (u_i, u_j) = \sum_{i,j} b_i^* c_j \delta_{ij} = \sum_i b_i^* c_i \tag{3}$$

  En particular,

  $$\|\psi\|^2 = (\psi, \psi) = \sum_i |c_i|^2 \tag{4}$$

- **Relación de cierre**

  Sea $\{u_i\}_i$ una familia ortonormal de funciones de $\mathscr{F}$, esta familia es base de $\mathscr{F}$ si y solo si satisface la siguiente expresión, conocida como *relación de cierre*:

  $$\sum_i u_i(\vec{r}) u_i^*(\vec{r'}) = \delta(\vec{r} - \vec{r'}) \tag{5}$$

1.2. Notación de Dirac

Una vez estudiadas las propiedades del espacio $\mathscr{F}$, estamos en disposición de definir el espacio en el que trabajaremos en adelante: el *Espacio de estados*, $\mathscr{E}$. Este va a ser un espacio vectorial que va a constituir nuestro marco de trabajo. Como veremos en los postulados de la mecánica cuántica (apartado 1.4), el nombre de *espacio de estados* viene dado por la posibilidad de representar los estados de un sistema cuántico en términos de vectores de este espacio.

Definición 1.9. *A cada función $\psi(\vec{r}) \in \mathscr{F}$ le asociamos un vector que denotaremos $|\psi\rangle$. Denominando* ***espacio de estados de posición****, $\mathscr{E}_r$, al espacio vectorial formado a partir de estos vectores.*

$$\psi(\vec{r}) \in \mathscr{F} \Longleftrightarrow |\psi\rangle \in \mathscr{E}_r$$

Por definición, $\mathscr{E}_r$ es isomorfo a $\mathscr{F}$.

Nótese que la dependencia con $\vec{r}$ ya no aparece explícitamente en los vectores de $\mathscr{E}_r$, solamente aparece la letra ψ para aludir a la función de $\mathscr{F}$ a la que está asociada. En adelante, denotaremos al espacio de estados simplemente por $\mathscr{E}$, excepto cuando sea necesario especificar el sistema de coordenadas en el que trabajamos.

Observación 1.10. En física cuántica, el subíndice r del espacio de estados se refiere a la posición, dotando a $\mathscr{E}_r$ con el significado de *espacio de estados de posición*. Como hemos dicho antes, en el *espacio de estados de posición* trabaremos habitualmente con $n = 3$, identificando con $\mathbb{R}^3$ los tres grados de libertad espaciales habituales. No obstante, este espacio tan solo es un caso particular. Si queremos hablar del momento de una partícula debemos trabajar en el *espacio de estados de momento*, $\mathscr{E}_p$, donde p se refiere al momento (concepto similar a la energía cinética de una partícula). Este espacio también estará construido normalmente sobre $\mathbb{R}^3$, pero encontraremos casos diferentes, en función de los grados de libertad de la magnitud física que queramos medir. Por ejemplo, el *espacio de estados de spin*, $\mathscr{E}_s$, tiene dos grados de libertad en el caso de partículas fermiónicas (electrones, protones, neutrones, etc.) y tres grados de libertad en el caso de partículas bosónicas (fotones, gluones, fonones, etc.). La definición de estos espacios es análoga a la anterior, tan solo hay que tener en cuenta que el espacio $\mathscr{F}$ va a ser distinto y, por tanto, va a haber que cambiar el dominio de la función, que en lugar de representar posiciones con $\vec{r}$, representaremos, por ejemplo, momentos, con $\vec{p}$.

En adelante, usaremos los conceptos vistos anteriormente escritos en notación de Dirac. Por ejemplo, denotaremos una familia de vectores, o una base, por $\{|u_i\rangle\}_i$.

1.2.1. Ket y Bra

Definición 1.11. *Los vectores $|\psi\rangle$ del espacio de estados $\mathscr{E}$ se conocen como* ***"ket"*** *o estado, mientras que a los elementos $\langle\psi|$ del espacio dual $\mathscr{E}^*$ los llamaremos* ***"bra"****:*

$$\begin{aligned} \langle\psi| : \mathscr{E} &\longrightarrow \mathbb{C} \\ |\psi\rangle &\longmapsto \lambda \end{aligned}$$

Usaremos la notación $\langle\psi|\varphi\rangle$, conocida como ***"braket"*** *para expresar la acción del funcional lineal sobre el vector (del bra sobre el ket), $\langle\psi|\left(|\varphi\rangle\right) \in \mathbb{C}$.*

La existencia de un producto escalar en $\mathscr{E}$ nos permite asociar un covector $\langle\varphi|$ a cada vector $|\varphi\rangle$. El funcional lineal que podemos definir a partir de cada *ket* $|\varphi\rangle$ es el que asocia linealmente a cada *ket* $|\psi\rangle$ el número complejo que resulta del producto escalar $\left(|\varphi\rangle, |\psi\rangle\right)$. Denotando mediante el *bra* $\langle\varphi|$ a este funcional lineal, se tiene que

$$\langle\varphi|\psi\rangle = \left(|\varphi\rangle, |\psi\rangle\right)$$

Además, se cumplen las siguientes propiedades de linealidad:

Propiedades 1.12. Sean $|\psi\rangle \in \mathscr{E}$, $\lambda \in \mathbb{C}$, se tiene que

$$\begin{aligned} |\lambda\psi\rangle &= \lambda\,|\psi\rangle \\ \langle\lambda\psi| &= \lambda^*\,\langle\psi| \end{aligned}$$

Y sean $|\varphi_1\rangle$, $|\varphi_2\rangle \in \mathscr{E}$, λ_1, $\lambda_2 \in \mathbb{C}$

$$\lambda_1\,|\varphi_1\rangle + \lambda_2\,|\varphi_2\rangle = \lambda_1^*\,\langle\varphi_1| + \lambda_2^*\,\langle\varphi_2|$$

Como es habitual cuando hablamos de espacio dual, para todo *ket* existe un *bra*, mientras que la correspondencia contraria, en general, no es cierta.

1.2.2. Operadores lineales

Definición 1.13. *Un **operador lineal** A es una correspondencia lineal que asocia un ket $|\psi\rangle \in \mathscr{E}$ con otro ket $|\psi'\rangle \in \mathscr{E}$:*

$$|\psi'\rangle = A\,|\psi\rangle$$
$$A(\lambda_1\,|\psi_1\rangle + \lambda_2\,|\psi_2\rangle) = \lambda_1 A\,|\psi_1\rangle + \lambda_2 A\,|\psi_2\rangle \qquad \lambda_1, \lambda_2 \in \mathbb{C}$$

Las propiedades de los operadores no difieren de las vistas anteriormente, siendo el producto de dos operadores:

$$(AB)\,|\psi\rangle = A(B\,|\psi\rangle) \tag{6}$$

Definición 1.14. *Sean $|\varphi\rangle$ y $|\psi\rangle$ dos kets, llamaremos el **elemento de matriz** de A entre $|\varphi\rangle$ y $|\psi\rangle$ al producto escalar*

$$\langle\varphi|(A|\psi\rangle)$$

Este nombre de elemento de matriz cobrará sentido en la sección 1.2.6, donde desarrollaremos las representaciones matriciales de *kets*, *bras* y operadores. Ahora veamos cómo actúan los operadores sobre los *bras*:

Sea $\langle\varphi|$ un *bra* definido, consideramos el conjunto de todos los *kets* $|\psi\rangle$. Para cada *ket* podemos asociar el número complejo $\langle\varphi|\,(A\,|\psi\rangle)$, que ya hemos definido en 1.14 como el elemento de matriz de A entre $|\varphi\rangle$ y $|\psi\rangle$.

Como A es lineal y el producto escalar es lineal en el *ket*, entonces el número $\langle\varphi|\,(A\,|\psi\rangle)$ depende linealmente de $|\psi\rangle$. Por tanto, para $\langle\varphi|$ y A fijos, podemos asociar a cada $|\psi\rangle$ un número que depende linealmente de $|\psi\rangle$, por lo que $(\langle\varphi|\,A)$ define un funcional lineal sobre los *ket* de $\mathscr{E}$, es decir, $(\langle\varphi|\,A) \in \mathscr{E}^*$. Con esto, concluimos que

$$(\langle\varphi|\,A)\,|\psi\rangle = \langle\varphi|(A|\psi\rangle) \tag{7}$$

Por tanto, un operador actuando sobre un *bra* nos proporciona un nuevo *bra* con una correspondencia lineal. Podemos probar la linealidad:

Consideramos el bra definido por:

$$\langle\chi| = \lambda_1\,\langle\varphi_1| + \lambda_2\,\langle\varphi_2| \tag{8}$$

Vemos cómo actúa sobre un *ket* arbitrario $|\psi\rangle$ y usamos la relación 7:

$$\begin{aligned}(\langle\chi|\,A)\,|\psi\rangle &= \langle\chi|(A|\psi\rangle)\\ &= \lambda_1\,\langle\varphi_1|\,(A\,|\psi\rangle) + \lambda_2\,\langle\varphi_2|\,(A\,|\psi\rangle)\\ &= \lambda_1(\langle\varphi_1|\,A)\,|\psi\rangle + \lambda_2(\langle\varphi_2|\,A)\,|\psi\rangle\end{aligned} \tag{9}$$

Como comentario, hemos visto que el elemento de matriz de un operador A entre $|\varphi\rangle$ y $|\psi\rangle$ definido en 1.14 puede escribirse sin paréntesis, ya que es indiferente hacer actuar el operador sobre el *bra* o sobre el *ket*.

$$\langle\varphi|(A|\psi\rangle) = \langle\varphi|A|\psi\rangle \tag{10}$$

Definición 1.15. *La **traza** de un operador A, que denotaremos por $Tr\{A\}$, es la suma de los elementos diagonales de matriz, es decir, dada una base $\{|u_i\rangle\}_i$ del espacio de estados $\mathscr{E}$ en el que está definido el operador:*

$$Tr\{A\} = \sum_i \langle u_i|A|u_i\rangle$$

Como podrá verse a lo largo del proyecto, la traza de un operador va a tener mucha relevancia en la mecánica cuántica, ya que vamos a poder dotarla de significado físico en el caso de operadores observables (definición 1.39). Esto se debe, entre otras cosas, a que no depende de la base escogida.

Proposición 1.16. *La traza de un operador es invariante frente a cambios de base.*

Demostración.
Consideramos dos bases discretas ortonormales de $\mathscr{E}$, que llamaremos $\{|u_i\rangle\}_i$ y $\{|t_k\rangle\}_k$. Se tiene que:

$$\sum_i \langle u_i|A|u_i\rangle = \sum_i \langle u_i| \left[\sum_k |t_k\rangle \langle t_k|\right] A |u_i\rangle \tag{11}$$

Donde hemos introducido la relación de cierre (concepto desarrollado en la observación 1.28) para los estados $|t_k\rangle$. El lado derecho de la ecuación podemos igualarlo a:

$$\sum_{i,k} \langle u_i|t_k\rangle \langle t_k|A|u_i\rangle = \sum_{i,k} \langle t_k|A|u_i\rangle \langle u_i|t_k\rangle \tag{12}$$

Podemos intercambiar el orden de los factores ya que los *brakets* son escalares complejos. Ahora solo hay que sustituir en la expresión resultante la relación de cierre para los estados $|u_i\rangle$ por el operador identidad (en adelante, $\mathbb{I}$) y obtenemos:

$$\sum_i \langle u_i|A|u_i\rangle = \sum_k \langle t_k|A|t_k\rangle \tag{13}$$

□

Propiedades 1.17. Sean A, B, C operadores lineales, se cumple:

$$Tr\{AB\} = Tr\{BA\}$$

$$Tr\{ABC\} = Tr\{BCA\} = Tr\{CAB\}$$

En general, la traza del producto de un número arbitrario de operadores es invariante frente a permutaciones cíclicas. Para ilustrarlo, demostramos el primer caso, con dos operadores, usando la relación de cierre:

Demostración.
Podemos proceder de manera similar a la demostración anterior, considerando una base $\{|u_i\rangle\}_i$:

$$\begin{aligned} Tr\{AB\} &= \sum_i \langle u_i|AB|u_i\rangle = \sum_{i,j} \langle u_i|A|u_j\rangle \langle u_j|B|u_i\rangle \\ &= \sum_{i,j} \langle u_j|B|u_i\rangle \langle u_i|A|u_j\rangle = \sum_i \langle u_i|BA|u_i\rangle \end{aligned}$$

□

1.2.3. Conjugación hermítica

La correspondencia que hemos estudiado entre *ket* y *bra* nos permite definir el *operador adjunto* o *conjugado hermítico* $A^\dagger$ de un operador A, considerando la **restricción biyectiva** del espacio dual en la que tomamos solamente los *bras* que tienen un *ket* asociado.

Definición 1.18. *Consideramos $|\psi\rangle$ un ket arbitrario de $\mathscr{E}$ y un operador A tal que $A|\psi\rangle = |\psi'\rangle$. Sean $\langle\psi|$ y $\langle\psi'|$ los bra asociados a $|\psi\rangle$ y $|\psi'\rangle$, respectivamente, definimos el* ***operador adjunto*** *de A, que denotaremos por $A^\dagger$, como el operador que relaciona los correspondientes bra:*

$$\langle\psi'| = \langle\psi| A^\dagger$$

Es decir,

$$|\psi'\rangle = A|\psi\rangle \iff \langle\psi'| = \langle\psi| A^\dagger$$

Nótese que el operador adjunto de un operador lineal también es lineal

Y a partir de aquí podemos definir la operación de conjugación hermítica como la operación que transforma un operador en su adjunto, tal que:

$$(A\,|\psi\rangle)^\dagger = \langle\psi|\,A^\dagger \tag{14}$$

Teniendo en cuenta una de las propiedades básicas del producto escalar,

$$\langle\psi|\varphi\rangle = \langle\varphi|\psi\rangle^* \tag{15}$$

podemos deducir

$$\langle\psi|A^\dagger|\varphi\rangle = \langle\varphi|A|\psi\rangle^* \tag{16}$$

que es una relación válida para todo $|\varphi\rangle$ y $|\psi\rangle$.

Propiedades 1.19 (del operador adjunto)**.** Sea, A, B dos operadores lineales, $\lambda \in \mathbb{C}$, se tiene que:

$$(A^\dagger)^\dagger = A$$
$$(\lambda A)^\dagger = \lambda^* A^\dagger$$
$$(A+B)^\dagger = A^\dagger + B^\dagger$$
$$(AB)^\dagger = B^\dagger A^\dagger$$

Definición 1.20. *Se dice que un operador A es **hermítico** si es igual que su adjunto,*

$$A = A^\dagger$$

Propiedades 1.21. Un operador hermítico A cumple:

$$\langle\psi|A|\varphi\rangle = \langle\varphi|A|\psi\rangle^*$$
$$\langle A\psi|\varphi\rangle = \langle\varphi|A\psi\rangle$$

Para cualquier par de *kets* $|\psi\rangle$, $|\varphi\rangle$ y sus *bras* asociados.

La operación de conjugación hermítica también puede ser aplicada a *kets* y *bras*. Se dice que un *ket* y su *bra* asociado son conjugados hermíticos entre ellos (es importante notar que esto solo se cumple con la restricción del espacio dual mencionada al principio, ya que en general no todo *bra* tiene un *ket* asociado).

Esta operación, como podemos comprobar en la expresión 14, actúa sobre los diferentes elementos como se resume a continuación:

Operador conjugación hermítica.

Se reemplazan:

$$\lambda \longrightarrow \lambda^*$$
$$|\psi\rangle \longleftrightarrow \langle\psi|$$
$$A \longrightarrow A^\dagger$$

Y se invierte el orden de los factores (la posición de las constantes no es relevante).

1.2.4. Operadores unitarios

Definición 1.22. *Un operador U es **unitario** si se cumple que*

$$U^{-1} = U^\dagger$$

Como consecuencia directa de esta definición, tenemos

$$U^\dagger U = UU^\dagger = \mathbb{I} \tag{17}$$

Observación 1.23 (Implicaciones físicas)**.** Un operador unitario es la herramienta que nos va a permitir manipular un sistema cuántico sin extraer información. No vamos a entrar en mucha profundidad en los procedimientos físicos con los que se manipulan los sistemas cuánticos, tan solo daremos unas pinceladas en el apartado 1.4.6, donde hablamos del sexto postulado de la mecánica cuántica.

Propiedad 1.24. Las transformaciones unitarias conservan el producto escalar (y, por tanto, la norma).

Demostración.
Consideramos los *kets*

$$|\psi_1'\rangle = U|\psi_1\rangle \qquad |\psi_2'\rangle = U|\psi_2\rangle$$

Y observamos que al calcular el producto escalar obtenemos el de los vectores originales:

$$\langle\psi_1'|\psi_2'\rangle = \langle\psi_1|U^\dagger U|\psi_2\rangle = \langle\psi_1|\psi_2\rangle$$

□

Propiedad 1.25. El producto de dos operadores unitarios es también unitario.

Demostración.
Consideramos U, V operadores unitarios

$$\begin{aligned}
&U^\dagger U = UU^\dagger = \mathbb{I}\\
&V^\dagger V = VV^\dagger = \mathbb{I}\\
&(UV)^\dagger(UV) = V^\dagger U^\dagger UV = V^\dagger V = \mathbb{I}\\
&(UV)(UV)^\dagger = UVV^\dagger U^\dagger = UU^\dagger = \mathbb{I}
\end{aligned}$$

□

Propiedad 1.26. Los autovalores de un operador unitario son números complejos de modulo 1.

Demostración.
Tomando los conceptos relativos a autovalores de operadores de la definición 1.31, consideramos $|\psi_u\rangle$ un autovector normalizado ($\langle\psi_u|\psi_u\rangle = 1$) del operador unitario U con autovalor u:

$$U|\psi_u\rangle = u|\psi_u\rangle$$

El cuadrado de la norma de $U|\psi_u\rangle$ resulta ser:

$$\langle\psi_u|U^\dagger U|\psi_u\rangle = u^* u\,\langle\psi_u|\psi_u\rangle = u^* u$$

Como un operador unitario conserva la norma, entonces necesariamente $u^*u = 1$, por lo que deducimos que la expresión general para el autovalor u es:

$$u = e^{i\varphi_u} \qquad \varphi_u \in \mathbb{R} \tag{18}$$

□

1.2.5. Proyectores

Definición 1.27. *Podemos reescribir el braket $\langle\varphi|\psi\rangle$ en orden inverso, $|\psi\rangle\langle\varphi|$. Esto se conoce como* ***ketbra****.*

Para ver las propiedades de este nuevo elemento, veamos cómo actúa sobre un *ket* arbitrario $|\chi\rangle$:

$$|\psi\rangle\langle\varphi|\chi\rangle \tag{19}$$

Ya sabemos que $\langle\varphi|\chi\rangle \in \mathbb{C}$, por lo que la expresión 19 es un *ket*. Deducimos que el resultado de aplicar un *ketbra* sobre un *ket* arbitrario nos proporciona otro *ket*, de manera que un *ketbra* es un operador. Con esto podemos ya entrever que en esta notación el orden de los elementos es crítico, no son operaciones conmutativas, lo único que puede cambiar de posición a placer son los escalares complejos y, por consiguiente, los *braket*.

Observación 1.28. La relación de cierre planteada en la expresión 5 toma la forma de ketbra. En el caso discreto (el habitual), se tiene que, dada una base del espacio de estados $\{|u_i\rangle\}_i$:

$$\sum_i |u_i\rangle\langle u_i| = \mathbb{I}$$

Ya que, aplicado sobre un vector $|\psi\rangle$ arbitrario del espacio de estados:

$$\sum_i |u_i\rangle\langle u_i|\psi\rangle = \sum_i c_i |u_i\rangle = |\psi\rangle$$

Donde hemos adaptado los conceptos de la definición 1.8 a notación de Dirac.

Definición 1.29. *Sea $|\psi\rangle$ un ket normalizado ($\langle\psi|\psi\rangle = 1$), el* ***proyector*** *$P_\psi$ sobre $|\psi\rangle$ es el operador*

$$P_\psi = |\psi\rangle\langle\psi|$$

Este operador, aplicado sobre un *ket* arbitrario $|\varphi\rangle$

$$P_\psi|\varphi\rangle = |\psi\rangle\langle\psi|\varphi\rangle$$

da como resultado un *ket* proporcional a $|\psi\rangle$. El coeficiente de proporcionalidad $\langle\psi|\varphi\rangle$ es el producto escalar de estos dos *ket*. El significado geométrico es inmediato, se trata del operador proyección ortogonal sobre $|\psi\rangle$ (es decir, sobre el subespacio generado por este único *ket*). De hecho, se puede comprobar inmediatamente que $P_\psi^2 = P_\psi$:

$$P_\psi^2 = P_\psi P_\psi = |\psi\rangle\langle\psi|\psi\rangle\langle\psi| = |\psi\rangle\langle\psi| = P_\psi \tag{20}$$

Donde hemos utilizado la condición de normalización $\langle\psi|\psi\rangle = 1$.

Además, este operador es hermítico.

$$P_\psi^\dagger = |\psi\rangle\langle\psi| = P_\psi \tag{21}$$

También es posible definir la proyección sobre un subespacio:

Definición 1.30. *Sean $|\varphi_1\rangle, |\varphi_2\rangle, ..., |\varphi_q\rangle$ una familia ortogonal de kets normalizados,*

$$\langle\varphi_i|\varphi_j\rangle = \delta_{ij} \quad con \;\; i,j = 1,2,...,q$$

Denotamos por $\mathscr{E}_q$ el subespacio de $\mathscr{E}$ generado por los q vectores.

El ***proyector*** *P_q* ***sobre el subespacio*** *$\mathscr{E}_q$ será el operador lineal definido por:*

$$P_q = \sum_{i=1}^{q} |\varphi_i\rangle\langle\varphi_i|$$

Siguiendo un procedimiento análogo al anterior, podemos comprobar que es idempotente:

$$P_q^2 = \sum_{i=1}^{q}\sum_{j=1}^{q} |\varphi_i\rangle \langle\varphi_i|\varphi_j\rangle \langle\varphi_j| = \sum_{i=1}^{q}\sum_{j=1}^{q} |\varphi_i\rangle \langle\varphi_j| \, \delta_{ij} = \sum_{i=1}^{q} |\varphi_i\rangle \langle\varphi_i| = P_q \tag{22}$$

Si hacemos actuar este proyector sobre un *ket* $|\psi\rangle$, podemos ver que el resultado es una combinación lineal de proyecciones de $|\psi\rangle$ sobre los *kets* $|\varphi_i\rangle$, lo cual resulta en la proyección de $|\psi\rangle$ sobre el subespacio $\mathscr{E}_q$.

$$P_q |\psi\rangle = \sum_{i=1}^{q} |\varphi_i\rangle \langle\varphi_i|\psi\rangle \tag{23}$$

1.2.6. Representación matricial

Consideramos una base $\{|u_i\rangle\}_i$ del espacio de estados $\mathscr{E}$. En esta base, un *ket* $|\psi\rangle$ puede expresarse en términos de sus componentes $c_i = \langle u_i|\psi\rangle$ (definición 1.8 con notación de Dirac). Podemos construir un vector columna con estas componentes:

$$\begin{pmatrix} \langle u_1|\psi\rangle \\ \langle u_2|\psi\rangle \\ \vdots \\ \langle u_i|\psi\rangle \\ \vdots \end{pmatrix} \tag{24}$$

Por otra parte, un *bra* $\langle\varphi|$ puede ser escrito en términos de los *bras* $\{\langle u_i|\}_i$:

$$\langle\varphi| = \langle\varphi| \sum_i |u_i\rangle \langle u_i| = \sum_i \langle\varphi|u_i\rangle \langle u_i|$$

Donde $\langle\varphi|u_i\rangle = b_i^*$ son los complejos conjugados de $b_i = \langle u_i|\varphi\rangle$. Podemos construir un vector fila con estas componentes:

$$\begin{pmatrix} \langle\varphi|u_1\rangle & \langle\varphi|u_2\rangle & \dots & \langle\varphi|u_i\rangle & \dots \end{pmatrix} \tag{25}$$

Por último, consideramos un operador A, que en la base $\{|u_i\rangle\}_i$ puede ser representado por los elementos de matriz (1.14):

$$A_{ij} = \langle u_i|A|u_j\rangle$$

Por tanto, un operador A queda representado por una matriz:

$$\begin{pmatrix} A_{11} & A_{12} & \dots & A_{1j} & \dots \\ A_{21} & A_{22} & \dots & A_{2j} & \dots \\ \vdots & \vdots & \ddots & \vdots & \\ A_{i1} & A_{i2} & \dots & A_{ij} & \dots \\ \vdots & \vdots & & \vdots & \ddots \end{pmatrix} \tag{26}$$

En conclusión, podemos sustituir *kets, bras* y operadores por sus representaciones matriciales en las expresiones, lo que nos permite realizar las operaciones correspondientes. Además, los conjugados hermíticos también son intuitivos, ya que en términos matriciales esta operación no es más que la *traspuesta conjugada*.

1.2.7. Observables

Definición 1.31. *Se dice que $|\psi\rangle$ es un autovector (o **autoket**) de un operador A con autovalor $\lambda \in \mathbb{C}$ si cumple*

$$A\,|\psi\rangle = \lambda\,|\psi\rangle$$

Las cuestiones relativas a degeneración, obtención de autovalores y conceptos similares son idénticas a las usuales.

Observación 1.32. Si realizamos la operación de conjugación hermítica a la ecuación de autovalores obtenemos

$$\langle\psi|\,A^\dagger = \lambda^*\,\langle\psi| \tag{27}$$

Es decir, si $|\psi\rangle$ es un *autoket* de A con autovalor λ, se puede decir también que $\langle\psi|$ es un *autobra* de $A^\dagger$ con autovalor λ^*

Proposición 1.33. *Los autovalores de un operador A hermítico son reales*

Demostración.
Consideramos un operador hermítico A. Su ecuación de autovalores es

$$A\,|\psi\rangle = \lambda\,|\psi\rangle$$

Realizamos el producto escalar por $|\psi\rangle$ a ambos lados:

$$\langle\psi|A|\psi\rangle = \lambda\,\langle\psi|\psi\rangle$$

Tenemos que $\langle\psi|A|\psi\rangle \in \mathbb{R}$, ya que:

$$\langle\psi|A|\psi\rangle^* = \langle\psi|A^\dagger|\psi\rangle = \langle\psi|A|\psi\rangle$$

Por tanto, como $\langle\psi|A|\psi\rangle$ y $\langle\psi|\psi\rangle$ son números reales, deducimos que λ también es real. □

Observación 1.34. Si A es hermítico, la ecuación 27 se convierte en

$$\langle\psi|\,A = \lambda\,\langle\psi|$$

Por lo que en el caso de A hermítico, $|\psi\rangle$ es un *autoket* y $\langle\psi|$ un *autobra* de A, ambos con autovalor λ.

Proposición 1.35. *Dos autovectores de un operador hermítico correspondientes a dos autovalores diferentes son ortogonales*

Demostración.
Consideramos dos autovectores $|\psi\rangle$ y $|\varphi\rangle$ de un operador hermítico A:

$$A\,|\psi\rangle = \lambda\,|\psi\rangle \tag{28}$$

$$A\,|\varphi\rangle = \mu\,|\varphi\rangle \tag{29}$$

Como A es hermítico, podemos escribir, por ejemplo, la ecuación 29 con *autobras*, como indica la observación 1.34:

$$\langle\varphi|\,A = \mu\,\langle\varphi| \tag{30}$$

Ahora, multiplicamos 28 por $\langle\varphi|$ a la izquierda y 30 por $|\psi\rangle$ a la derecha:

$$\langle\varphi|A|\psi\rangle = \lambda\,\langle\varphi|\psi\rangle \tag{31}$$

$$\langle\varphi|A|\psi\rangle = \mu\,\langle\varphi|\psi\rangle \tag{32}$$

Restando estas dos expresiones obtenemos:

$$(\lambda - \mu)\,\langle\varphi|\psi\rangle = 0$$

Por lo que si $(\lambda - \mu) \neq 0$, entonces $\langle\varphi|\psi\rangle = 0$, por lo que son ortogonales. □

Proposición 1.36 (Descomposición espectral de un operador hermítico)**.** *Sea A un operador hermítico, con autovalores λ_i y autovectores asociados $|\psi_i^j\rangle$, representando con j la posible degeneración de cada autovector, se tiene que:*

$$A = \sum_{ij} \lambda_i \, |\psi_i^j\rangle$$

Ejemplo 1.37. Consideramos, trabajando en un espacio de estados bidimensional, el operador Z (proyección del estado sobre el eje z):

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

Los autovalores de este operador son $+1$ y -1 y los autovectores asociados son, respectivamente, $\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ y $\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$. Y se cumple que:

$$Z = \sum_{i=1}^{2} \lambda_i \, |\psi_i\rangle \langle\psi_i| = (+1) \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} \right) + (-1) \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} \right)$$

Ejemplo 1.38. En el mismo espacio, también podemos considerar el operador X (proyección del estado sobre el eje x):

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

Los autovalores de este operador son $+1$ y -1 y los autovectores asociados son, respectivamente, $\frac{1}{\sqrt{2}}\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)$ y $\frac{1}{\sqrt{2}}\left(\begin{smallmatrix}1\\-1\end{smallmatrix}\right)$. Y tenemos que:

$$\begin{aligned} X &= \sum_{i=1}^{2} \lambda_i \, |\psi_i\rangle \langle\psi_i| = (+1) \left(\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \end{pmatrix} \right) + (-1) \left(\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \end{pmatrix} \right) \\ &= \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} - \begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 1/2 \end{pmatrix} \end{aligned}$$

Definición 1.39. *Se dice que un operador A es un **observable** si es hermítico y su sistema ortogonal de autovectores forma una base del espacio de estados $\mathscr{E}$.*

Ejemplo 1.40. el operador proyección P_ψ Consideramos el proyector $P_\psi = |\psi\rangle \langle\psi|$, con $\langle\psi|\psi\rangle = 1$. Ya hemos visto que es hermítico (21), ahora calculemos sus autovalores:

$$\begin{aligned} P_\psi \, |\varphi\rangle &= \lambda \, |\varphi\rangle \\ |\psi\rangle \langle\psi|\varphi\rangle &= \lambda \, |\varphi\rangle \end{aligned}$$

En vista de que $\langle\psi|\varphi\rangle$ solamente es no nulo si $|\varphi\rangle$ es colineal con $|\psi\rangle$, deducimos que los autovalores son 1 (asociado con el autovector $|\psi\rangle$) y 0 (asociado con el resto de vectores ortogonales a $|\psi\rangle$).

Consideramos un vector $|\varphi\rangle$ arbitrario del espacio de estados. Siempre podemos escribirlo en la forma

$$|\varphi\rangle = P_\psi \, |\varphi\rangle + (\mathbb{I} - P_\psi) \, |\varphi\rangle \tag{33}$$

Ahora, como $P_\psi \, |\varphi\rangle$ es proporcional a $|\psi\rangle$, entonces es un autovector de de P_ψ con autovalor 1. Podemos probarlo usando la condición de idempotencia del operador proyección (20):

$$P_\psi (P_\psi \, |\varphi\rangle) = P_\psi^2 \, |\varphi\rangle = P_\psi \, |\varphi\rangle \tag{34}$$

De hecho, $(\mathbb{I} - P_\psi) \, |\varphi\rangle$ también es autovector de P_ψ con autovalor 0, como podemos ver:

$$P_\psi (\mathbb{I} - P_\psi) \, |\varphi\rangle = (P_\psi - P_\psi^2) \, |\varphi\rangle = 0 \tag{35}$$

En conclusión, todo *ket* $|\varphi\rangle$ puede expresarse en términos de estos autovectores de P_ψ, por lo que P_ψ es un observable.

A nivel físico, un observable resulta ser precisamente una magnitud que es físicamente medible (de ahí su nombre). Ejemplos de observables son los operadores *Posición, Momento, Momento Angular, Spin, Polarización, Energía*, etc. Esto quiere decir que todas estas magnitudes físicas están caracterizadas en física cuántica por operadores hermíticos cuyo sistema de autovectores es base del espacio de estados. Las implicaciones de esta definición son muy interesantes, ya que nos indican que cualquier operador que cumpla esas características puede ser medido en un sistema cuántico, incluso si no tiene ningún "sentido" intuitivo.

Un ejemplo muy conocido de observable sin sentido intuitivo es el *spin*, El nombre de *spin* tiene motivación histórica, debido a que antes se creía que las partículas rotaban sobre sí mismas. No obstante, con el desarrollo de la mecánica cuántica se ha podido comprobar que las partículas no son esferas que rotan ni tienen nada que ver con sistemas de esferas que se orbiten unas a otras. De hecho, las partículas atómicas y subatómicas son más parecidas a "regiones del espacio que pueden presentar determinadas características con una determinada probabilidad" que a partículas (de ahí el modelo vigente de "funciones de onda" que comentábamos al inicio del capítulo). Por lo tanto, hablar de rotación sobre sí misma para una entidad como podría ser un electrón carece completamente de sentido. De este modo, al medir el observable conocido como *spin*, el sistema que estamos midiendo nos proporciona un valor del que, a priori, no conocemos ninguna manera intuitiva de interpretar, pero sin embargo existe.

Relacionados con observables, existen otros conceptos relevantes para la mecánica cuántica, como los *Conjuntos Completos de Observables Compatibles* (CCOC) que nos indican los observables que pueden ser medidos simultáneamente, refiriéndose por *compatible* a que los operadores conmuten (1.6) y por *completo* a que el sistema de autovectores conjunto sea base del espacio de estados correspondiente. El estudio de estos sistemas, aunque es interesante para entender en profundidad la mecánica cuántica, está lejos del objetivo de este proyecto. Tan solo vamos a hacer hincapié en un detalle: existen conjuntos de observables no compatibles entre ellos, observables tan típicos como pueden ser, por ejemplo, *posición* y *momento*. En un sistema clásico como un coche en movimiento, podemos conocer la posición y la velocidad al mismo tiempo y con precisión. No obstante, en mecánica cuántica estos dos operadores no conmutan, por lo que no forman un CCOC y por tanto no pueden ser medidos a la vez. De hecho, medir uno condiciona fuertemente la medida posterior del otro, de la manera que nos indica el *Principio de Indeterminación de Heisenberg*:

$$\Delta x \Delta p \geq \frac{\hbar}{2} \tag{36}$$

Siendo Δx, Δp las indeterminaciones en las medidas de los operadores posición y momento, respectivamente, y $\hbar$ la constante de Planck.

1.3. Producto tensorial

1.3.1. Producto tensorial de espacios de estados

Hasta ahora, todo lo que hemos visto es válido para sistemas que solo engloban una sola partícula y una sola variable. Para trabajar, por ejemplo, con una partícula que tenga spin, vamos a necesitar combinar el espacio de estados de posición $\mathscr{E}_r$ con el espacio de estados de spin $\mathscr{E}_s$. De la misma forma, si queremos trabajar con dos partículas que interactúan, tendremos que combinar el espacio de estados de la primera partícula $\mathscr{E}_1$ con el de la segunda $\mathscr{E}_2$. Esta acción de combinar espacios de estados la hacemos mediante el producto tensorial.

Notación: Consideramos $\mathscr{E}_1$, $\mathscr{E}_2$ dos espacios de dimensiones N_1 y N_2 (finitas o infinitas), respectivamente. Los vectores y operadores de estos espacios los representaremos mediante un índice (1) o (2), dependiendo si pertenecen al espacio $\mathscr{E}_1$ o $\mathscr{E}_2$.

Definición 1.41. *Sean $\mathscr{E}_1$, $\mathscr{E}_2$ dos espacios vectoriales de estados, definimos el* ***producto tensorial*** *$\mathscr{E}$:*

$$\mathscr{E} = \mathscr{E}_1 \otimes \mathscr{E}_2$$

como el espacio vectorial $\mathscr{E}$ que cumple que para cada par de vectores $|\varphi(1)\rangle \in \mathscr{E}_1$, $|\chi(2)\rangle \in \mathscr{E}_2$ existe un vector en $\mathscr{E}$, que denotamos $|\varphi(1)\rangle \otimes |\chi(2)\rangle$. La operación $\otimes$ satisface las siguientes condiciones:

- *Es lineal con respecto al producto por un escalar*

$$[\lambda\,|\varphi(1)\rangle] \otimes |\chi(2)\rangle = \lambda\,[|\varphi(1)\rangle \otimes |\chi(2)\rangle]$$
$$|\varphi(1)\rangle \otimes [\mu\,|\chi(2)\rangle] = \mu\,[|\varphi(1)\rangle \otimes |\chi(2)\rangle]$$

- *Es distributiva con respecto a la suma*

$$|\varphi(1)\rangle \otimes [|\chi_1(2)\rangle + |\chi_2(2)\rangle] = |\varphi(1)\rangle \otimes |\chi_1(2)\rangle + |\varphi(1)\rangle \otimes |\chi_2(2)\rangle$$
$$[|\varphi_1(1)\rangle + |\varphi_2(1)\rangle] \otimes |\chi(2)\rangle = |\varphi_1(1)\rangle \otimes |\chi(2)\rangle + |\varphi_2(1)\rangle \otimes |\chi(2)\rangle$$

- *Para cada par de bases $\{|u_i(1)\rangle\}$ de $\mathscr{E}_1$, $\{|v_j(2)\rangle\}$ de $\mathscr{E}_2$, el conjunto de vectores $|u_i(1)\rangle \otimes |v_j(2)\rangle$ constituye una base de $\mathscr{E}$. Además, si las dimensiones N_1, N_2 son finitas, entonces la dimensión de $\mathscr{E}$ es N_1N_2. En adelante, nos restringiremos al caso de dimensión finita.*

Consideramos dos bases $\{|u_i(1)\rangle\}$ de $\mathscr{E}_1$ y $\{|v_j(2)\rangle\}$ de $\mathscr{E}$. Como ya sabemos, los vectores $|\varphi(1)\rangle \in \mathscr{E}_1$ y $|\chi(2)\rangle \in \mathscr{E}_2$ pueden escribirse, con ciertos coeficientes a_i, b_j como

$$|\varphi(1)\rangle = \sum_i a_i\,|u_i(1)\rangle$$
$$|\chi(2)\rangle = \sum_j b_j\,|v_j(2)\rangle$$

De esta manera, un vector $|\varphi(1)\rangle \otimes |\chi(2)\rangle \in \mathscr{E}$ puede escribirse en la base $\{|u_i(1)\rangle \otimes |v_j(2)\rangle\}$ de $\mathscr{E}$ como:

$$|\varphi(1)\rangle \otimes |\chi(2)\rangle = \sum_{i,j} a_i b_j\,|u_i(1)\rangle \otimes |v_j(2)\rangle \tag{37}$$

No obstante, también existen vectores en $\mathscr{E}$ que no pueden escribirse en forma de producto tensorial. La forma más genérica de expresarlo, teniendo en cuenta que $\{|u_i(1)\rangle \otimes |v_j(2)\rangle\}$ es base de $\mathscr{E}$, sería

$$|\varphi(1)\rangle \otimes |\chi(2)\rangle = \sum_{i,j} c_{i,j}\,|u_i(1)\rangle \otimes |v_j(2)\rangle \tag{38}$$

Donde $c_{i,j}$ no siempre puede expresarse como producto de coeficientes asociados a las bases individuales. Sin embargo, un vector arbitrario de $\mathscr{E}$ siempre puede ser descompuesto en una combinación lineal de productos tensoriales de vectores de los espacios individuales, como refleja la expresión 38.

Notación: Para aliviar notación, escribiremos $|\varphi(1)\chi(2)\rangle$ o, en ocasiones, simplemente $|\varphi\chi\rangle$, para referirnos al producto tensorial $|\varphi(1)\rangle \otimes |\chi(2)\rangle$. Esta es la notación estándar en el campo.

Definición 1.42. *La existencia de un producto escalar en los espacios $\mathscr{E}_1$ y $\mathscr{E}_2$ nos permite definir un* ***producto escalar en*** *$\mathscr{E}$:*

$$\langle\varphi(1)\chi(2)|\varphi'(1)\chi'(2)\rangle = \langle\varphi(1)|\varphi'(1)\rangle\,\langle\chi(2)|\chi'(2)\rangle$$

Cuyas propiedades se heredan del producto escalar en los espacios de estados simples.

Observación 1.43. Consideramos dos bases $\{|u_i(1)\rangle\}_i$ de $\mathscr{E}_1$, $\{|v_j(2)\rangle\}_j$ de $\mathscr{E}_2$. La base $\{|u_i(1)v_j(2)\rangle\}_{ij}$ de $\mathscr{E}$ es ortonormal si las dos bases de los espacios simples lo son, ya que:

$$\langle u_{i'}(1)v_{j'}(2)|u_i(1)v_j(2)\rangle = \langle u_{i'}(1)|u_i(1)\rangle\,\langle v_{j'}(2)|v_j(2)\rangle = \delta_{ii'}\delta_{jj'}$$

1.3.2. Producto tensorial de operadores

Definición 1.44. *Consideramos un operador $A(1)$ definido en $\mathscr{E}_1$. La **extensión del operador** $A(1)$ a $\mathscr{E} = \mathscr{E}_1 \otimes \mathscr{E}_2$, que denotaremos por $\tilde{A}(1)$, es el operador que actúa de la siguiente forma:*

$$\tilde{A}(1)\left[|\varphi(1)\rangle \otimes |\chi(2)\rangle\right] = \left[A(1)\,|\varphi(1)\rangle \otimes |\chi(2)\rangle\right] = A(1)\,|\varphi(1)\chi(2)\rangle$$

Es decir, la extensión al espacio total de un operador que actúa sobre uno de los espacios deja invariantes los kets pertenecientes al resto de espacios.

Podemos ver la representación matricial con un ejemplo.

Ejemplo 1.45. Consideramos dos espacios de dos dimensiones $\mathscr{E}_1$, $\mathscr{E}_2$, y el operador $X(1)$ dado por la matriz

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

La matriz del operador extendido $\tilde{X}(1)$ en $\mathscr{E} = \mathscr{E}_1 \otimes \mathscr{E}_2$ será:

$$\tilde{X}(1) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Es decir, $\tilde{X}(1) = X(1) \otimes \mathbb{I}(2)$

Y, análogamente, si el operador actuara sobre el espacio $\mathscr{E}_2$, entonces tendríamos que $\tilde{X}(2) = \mathbb{I}(1) \otimes X(2)$

$$\tilde{X}(2) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Definición 1.46. *Consideramos dos operadores $A(1)$, $B(2)$, actuando respectivamente en los espacios $\mathscr{E}_1$ y $\mathscr{E}_2$. Definimos el **producto tensorial** de los dos operadores, $A(1) \otimes B(2)$ como el operador tal que:*

$$\left[A(1) \otimes B(2)\right]\left[|\varphi(1)\chi(2)\rangle\right] = \left[A(1)\,|\varphi(1)\rangle\right] \otimes \left[B(2)\,|\chi(2)\rangle\right]$$

Y su representación matricial será el producto tensorial de las matrices $A \otimes B$.

1.3.3. Autovalores en el espacio producto

Consideramos, como antes, dos espacios de estados $\mathscr{E}_1$, $\mathscr{E}_2$ y su espacio producto $\mathscr{E} = \mathscr{E}_1 \otimes \mathscr{E}_2$. Sea $A(1)$ un operador actuando en $\mathscr{E}_1$, su ecuación de autovalores en el espacio $\mathscr{E}_1$ es:

$$A(1)\,|\psi(1)\rangle = \lambda\,|\psi(1)\rangle$$

Es fácil deducir de la definición 1.44 que en el espacio total se cumplirá, para $|\varphi(2)\rangle$ arbitrario,

$$\tilde{A}(1)\left[|\psi(1)\varphi(2)\rangle\right] = \left[A(1)\,|\psi(1)\rangle\right] \otimes |\varphi(2)\rangle = \lambda\,|\psi(1)\rangle \otimes |\varphi(2)\rangle = \lambda\,|\psi(1)\varphi(2)\rangle$$

Es decir, los autovalores del operador ampliado $\tilde{A}(1)$ son los mismos que los del operador sin ampliar $A(1)$, teniendo sus autovectores degeneración $g_n \times N_2$, siendo g_n la degeneración en

el espacio individual sin realizar la extensión y N_2 la dimensión de $\mathscr{E}_2$, ya que $|\psi(1)\varphi(2)\rangle$ es autovector de $\tilde{A}(1)$ asociado al autovalor λ para cualquier $|\varphi(2)\rangle \in \mathscr{E}_2$.

El razonamiento es análogo para un operador actuando en $\mathscr{E}_2$.

Observación 1.47. También es fácil obtener expresiones para los autovalores de la suma y el producto de operadores dentro de un espacio producto tensorial, pero no será necesario en este proyecto.

1.4. Postulados de la mecánica cuántica

En este apartado vamos a ver los seis postulados en los que se basan las descripciones cuánticas de los sistemas. Esta es la formulación más extendida, pero existen otras (ver [3] y [4]). Estos postulados son la conexión entre el mundo cuántico y el formalismo matemático con el que lo describimos. La motivación de estos postulados, a primera vista, no siempre está clara, dado que surgen como resultado de muchos años de hipótesis, pruebas y errores hasta que se ha obtenido un formalismo consistente con los resultados experimentales. Es decir, tras años de experimentos en este área, acabó asentándose una forma de trabajar que formalizaron Dirac y Neumann [5] entre 1930 y 1932 en estos postulados.

1.4.1. Primer postulado

En un instante t_0, el estado de un sistema físico aislado está definido por un ket $|\psi(t_0)\rangle$ del espacio de estados $\mathscr{E}$.

1.4.2. Segundo postulado

Toda cantidad medible se describe mediante un operador A que actúa en el espacio de estados $\mathscr{E}$ y cumple las propiedades de observable.

1.4.3. Tercer postulado

Al medir una cantidad física, asociada a un observable A, los únicos resultados posibles son los autovalores del operador A.

Observación 1.48. Una medida de un observable siempre va a dar como resultado un número real, dado que los observables son, por definición, hermíticos.

Observación 1.49. Si el espectro del operador observable es discreto, los resultados de la medida están cuantizados, es decir, solo pueden tomar valores dentro de un conjunto discreto.

1.4.4. Cuarto postulado

Suponemos un sistema físico que se encuentra en un estado normalizado $|\psi\rangle$. Al medir un observable A, la probabilidad $\mathscr{P}(a_n)$ de obtener el autovalor a_n como resultado de la medida es:

$$\mathscr{P}(a_n) = \sum_{i=1}^{g_n} |\langle u_n^i | \psi \rangle|^2 \tag{39}$$

Donde g_n es el grado de degeneración de a_n y $\{|u_n^i\rangle\}_{i=1}^{g_n}$ es el conjunto ortonormal de vectores que forman una base del subespacio $\mathscr{E}_n$ asociado con el autovalor a_n de A

Observación 1.50. En caso de que el autovalor no sea degenerado, la expresión de la probabilidad se reduce a

$$\mathscr{P}(a_n) = |\langle u_n|\psi\rangle|^2 \tag{40}$$

Donde $|u_n\rangle$ es el autovector normalizado de A asociado al autovalor a_n

Proposición 1.51. *Consideramos un sistema en un estado $|\psi\rangle$. La distribución de probabilidades no cambia si el estado está alterado por un factor de fase global, $e^{i\theta}|\psi\rangle$, con $\theta \in \mathbb{R}$*

Demostración.
Consideramos dos *kets* $|\psi\rangle$, $|\psi'\rangle = e^{i\theta}|\psi\rangle$, con $\theta \in \mathbb{R}$. Empezamos comprobando que si $|\psi\rangle$ está normalizado, entonces $|\psi'\rangle$ también lo está:

$$\langle\psi'|\psi'\rangle = \langle\psi|e^{-i\theta}e^{i\theta}|\psi\rangle = \langle\psi|\psi\rangle$$

Ahora, se tiene que para cualquier autovector $|u_n^i\rangle$ asociado a un autovalor a_n:

$$|\langle u_n^i|\psi'\rangle|^2 = |e^{i\theta}\langle u_n^i|\psi\rangle|^2 = |\langle u_n^i|\psi\rangle|^2$$

Obteniendo entonces los mismos resultados de probabilidad que para el estado $|\psi\rangle$. □

Observación 1.52. Esto nos permite definir una clase de equivalencia en la que cualquier estado $|\psi'\rangle = e^{i\theta}|\psi\rangle$ con $\theta \in \mathbb{R}$ representa el mismo estado que $|\psi\rangle$.

Observación 1.53. Es necesario especificar que, aunque un factor de fase global no afecta al estado físico, sí que lo hacen los factores de fase parcial, es decir, los que se definen individualmente en cada componente de un estado de superposición, como se puede ver en el siguiente ejemplo.

Ejemplo 1.54. Consideramos un sistema en un estado $|\psi\rangle = \lambda_1|\psi_1\rangle + \lambda_2|\psi_2\rangle$, con $\lambda_1, \lambda_2 \in \mathbb{C}$. Ya sabemos que $e^{i\theta_1}|\psi_1\rangle$ representa el mismo estado que $|\psi_1\rangle$ para cualquier $\theta_1 \in \mathbb{R}$ y que $e^{i\theta_2}|\psi_2\rangle$ representa el mismo estado que $|\psi_2\rangle$ para cualquier $\theta_2 \in \mathbb{R}$. No obstante, en general, el estado:

$$|\psi'\rangle = \lambda_1 e^{i\theta_1}|\psi_1\rangle + \lambda_2 e^{i\theta_2}|\psi_2\rangle$$

No es el mismo que $|\psi\rangle$.

Estos estados son comunes, por ejemplo, en sistemas de fotones polarizados, en los que la diferencia de fase entre estados superpuestos es relevante. Además, como veremos en los apartados 2.2.4 y 2.2.7, los factores de fase parcial, más conocidos como "fases relativas" juegan un papel crucial en el área de los errores cuánticos.

Observación 1.55. Como el conjunto de autovectores $\{u_n\}_n$ de un observable, por definición, constituye una base del espacio de estados $\mathscr{E}$, un estado $|\psi\rangle$ se puede escribir en función de la base como

$$|\psi\rangle = \sum_n c_n|u_n\rangle$$

Siendo c_n los coeficientes correspondientes. De modo que la expresión de la probabilidad se reduce a

$$\mathscr{P}(a_n) = |\langle u_n|\psi\rangle|^2 = |c_n|^2 \tag{41}$$

O, en el caso de autovalores degenerados, el estado $|\psi\rangle$ se puede escribir como

$$|\psi\rangle = \sum_n \sum_{i=1}^{g_n} c_n^i|u_n^i\rangle$$

Y la probabilidad:

$$\mathscr{P}(a_n) = \sum_{i=1}^{g_n}|\langle u_n^i|\psi\rangle|^2 = \sum_{i=1}^{g_n}|c_n^i|^2 \tag{42}$$

1.4.5. Quinto postulado

Si la medida del observable A sobre un sistema en el estado $|\psi\rangle$ proporciona el resultado a_n, el estado $|\psi'\rangle$ del sistema inmediatamente después de la medida es la proyección normalizada de $|\psi\rangle$ sobre el subespacio asociado con el autovalor a_n:

$$|\psi'\rangle = \frac{P_n |\psi\rangle}{\sqrt{\langle\psi|P_n|\psi\rangle}} \tag{43}$$

Donde P_n es el proyector sobre el autovector, o subespacio de autovectores asociados con el autovalor a_n.

Observación 1.56. Este postulado refleja en qué medida afecta la medición al sistema. Establece una de las diferencias fundamentales entre la mecánica clásica y la cuántica. Clásicamente, es posible realizar mediciones de observables externamente al sistema, por ejemplo, podemos medir la posición de una pelota sin interactuar con ella. Sin embargo, en mecánica cuántica, hay que incluir el proceso de medida como una perturbación del sistema, dada por este quinto postulado. El proceso de medida pasa a formar parte del sistema. En mecánica cuántica, medir es proyectar.

Se puede poner un ejemplo para visualizarlo: Si nosotros medimos la temperatura del mar con un termómetro de mercurio, la temperatura que obtendremos será un resultado válido. En cambio, si nosotros queremos medir la temperatura de una gota de agua con el mismo procedimiento, la temperatura del termómetro afectará a la gota, proporcionándonos un resultado de la temperatura final del sistema gota-termómetro. La única manera de que la temperatura medida sea la original de la gota de agua es que el termómetro ya estuviera previamente a la misma temperatura que la gota, es decir, en el mismo "autoestado", de manera que el estado de la gota no varía. En mecánica cuántica ocurre lo mismo, dada la naturaleza nanoscópica de los sistemas, no podemos "medir" como lo haríamos en un sistema clásico, la medida consiste en aplicar un operador, es decir, perturbar el sistema con un observable, y hacer que el sistema colapse en uno de sus autoestados (autovectores), proyectándose el estado sobre dicho autovector (o autovectores) y quedando de ese modo definido el estado que previamente se encontraba indefinido (superpuesto con otros).

Por ejemplo, si medimos la velocidad de un electrón y obtenemos un determinado resultado, sabremos que esa es la velocidad que el electrón llevará a partir del momento de la medida (hasta que interactúe con algún otro sistema y su estado evolucione). No obstante, esta no es la velocidad que el electrón poseía antes de la medida, ya que esta velocidad es **indeterminada**, no tiene una velocidad concreta, sino muchas (en este caso, infinitas, un continuo) superpuestas. Al medir, el estado queda proyectado en uno de los autovalores del observable, quedando así determinada su velocidad a partir del instante de la medida.

Para más información sobre las interpretaciones físicas de este formalismo, el libro [6] es lectura recomendada.

1.4.6. Sexto postulado

La evolución temporal de un estado $|\psi(t)\rangle$ está gobernada por la ecuación de Schrödinger:

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = H(t)\,|\psi(t)\rangle \tag{44}$$

Donde H es el operador observable "Hamiltoniano" del sistema, que es el asociado a la magnitud física de la energía total del sistema.

Observación 1.57. En esta memoria, el sexto postulado es meramente informativo. No hemos desarrollado la teoría de observables ni estados dependientes del tiempo. No obstante, nos permite introducir un concepto (desarrollado en [2]) llamado "operador evolución". Es un operador unitario que depende del Hamiltoniano del sistema y que dicta la evolución del estado cuántico de un sistema. La manera que tenemos de manipular un estado cuántico sin extraer información

es aplicando al estado una perturbación con Hamiltoniano conocido, de manera que conozcamos cómo va a ser la evolución del sistema durante la perturbación.

1.4.7. Valor medio de un operador

El cuarto postulado nos habla de probabilidad. Esto implica que, en la práctica, necesitaremos verificar las predicciones con un gran número de medidas. Para ayudar en esta tarea, conviene dar una expresión del valor medio de un observable en términos del estado.

Proposición 1.58. *El valor medio de un observable A de un sistema en un estado $|\psi\rangle$ viene dado por*

$$\langle A\rangle = \langle\psi|A|\psi\rangle$$

Demostración.
Sobre el sistema dado, consideramos un número N de medidas del observable A. Denotaremos por $\mathscr{N}(a_n)$ el número de veces que obtenemos el autovalor a_n. Con esto, tenemos que:

$$\frac{\mathscr{N}(a_n)}{N} \xrightarrow[N\longrightarrow\infty]{} \mathscr{P}(a_n) \tag{45}$$

Y además,

$$\sum_n \mathscr{N}(a_n) = N$$

El valor medio del operador A es:

$$\langle A\rangle = \frac{1}{N}\sum_n a_n \mathscr{N}(a_n)$$

Que, por la expresión 45, cuando $N \longrightarrow \infty$, este valor medio se aproxima a:

$$\langle A\rangle = \sum_n a_n \mathscr{P}(a_n)$$

Sustituimos la probabilidad por la expresión 39 del cuarto postulado y obtenemos:

$$\langle A\rangle = \sum_n a_n \sum_{i=1}^{g_n} |\langle u_n^i|\psi\rangle|^2 = \sum_n a_n \sum_{i=1}^{g_n} \langle\psi|u_n^i\rangle\langle u_n^i|\psi\rangle \tag{46}$$

Y tomando la ecuación de autovalores,

$$A\,|u_n^i\rangle = a_n\,|u_n^i\rangle$$

Podemos escribir la ecuación 46 como:

$$\sum_n \sum_{i=1}^{g_n} \langle\psi|A|u_n^i\rangle\langle u_n^i|\psi\rangle = \langle\psi|\,A\left[\sum_n \sum_{i=1}^{g_n} |u_n^i\rangle\langle u_n^i|\right]|\psi\rangle = \langle\psi|A|\psi\rangle$$

Donde hemos usado la relación de cierre. □

Además, se puede expresar la probabilidad de obtención de un autovalor como resultado de una medida como el valor medio del proyector sobre el subespacio de los autovectores asociados a dicho autovalor, como podemos observar en el siguiente resultado.

Proposición 1.59. *Sean un sistema en un estado $|\psi\rangle$ y A un observable, la probabilidad $\mathscr{P}(a_n)$ de obtener un autovalor a_n como resultado de una medida puede expresarse de la siguiente forma:*

$$\mathscr{P}(a_n) = \langle\psi|P_n|\psi\rangle$$

Siendo P_n el operador proyección sobre el subespacio generado por los autovectores asociados al autovalor a_n.

Demostración.
Consideramos $\{u_n^i\}_i$ los autovectores asociados al autovalor a_n. Tenemos que:

$$P_n = \sum_i^{g_n} |u_n^i\rangle \langle u_n^i|$$

La proyección del estado $|\psi\rangle$ sobre este subespacio será:

$$|\psi_n\rangle = P_n |\psi\rangle = \sum_i^{g_n} |u_n^i\rangle \langle u_n^i|\psi\rangle = \sum_i^{g_n} c_n^i |u_n^i\rangle$$

Por lo que, por ortonormalidad de los autovectores y usando la ecuación 42:

$$\langle\psi_n|\psi_n\rangle = \sum_i^{g_n} |c_n^i|^2 = \mathscr{P}(a_n)$$

Es decir,

$$\mathscr{P}(a_n) = \langle\psi|P_n^\dagger P_n|\psi\rangle$$

Y, como el operador proyección es hermítico e idempotente,

$$\mathscr{P}(a_n) = \langle\psi|P_n|\psi\rangle$$

□

Observación 1.60. Esta forma de expresar la probabilidad como valor medio de un proyector también prueba que, en el caso degenerado, la probabilidad es independiente de la base de autovectores que escojamos, ya que el valor $\langle\psi_n|\psi_n\rangle = \sum_i^{g_n} |c_n^i|^2$ no varía.

1.5. Formalismo del operador densidad

1.5.1. Mezcla estadística

Hasta ahora, para desarrollar la teoría, hemos considerado que conocemos el estado del sistema. Sin embargo, en la práctica, el estado no suele estar perfectamente determinado. Por ejemplo, para sistemas de varias partículas en los que queramos definir una magnitud de temperatura, deberemos conocer el promedio de la energía cinética de las partículas, pero no tendremos determinadas la energía cinética de cada una por separado.

El operador densidad es una herramienta que nos permitirá incorporar esa incompletitud de la información al formalismo que hemos trabajado hasta ahora.

En general, la información incompleta se describe en forma de mezcla estadística de estados. Es decir, el estado de un sistema puede ser $|\psi_1\rangle$, $|\psi_2\rangle$, $|\psi_3\rangle$, etc., con respectivas probabilidades p_1, p_2, p_3, etc., tales que:

$$\sum_i p_i = 1$$

Representaremos el estado $|\psi\rangle$ de un sistema en mezcla estadística como:

$$|\psi\rangle = p_1 |\psi_1\rangle + p_2 |\psi_2\rangle + p_3 |\psi_3\rangle + \dots \tag{47}$$

Este concepto de mezcla estadística no debe ser confundido con el principio de superposición cuántica. En este, un sistema cuántico está descrito por un conjunto de n estados en superposición, es decir, se encuentra en todos los estados al mismo tiempo. En el caso de una mezcla estadística, estamos contemplando posibles estados como consecuencia de una falta de información. En el caso de un estado de superposición cuántica, el estado se encuentra "perfectamente

definido". Por el aspecto del estado, puede determinarse si se trata de una superposición o una mezcla estadística, como se observa en estos dos ejemplos:

$$|\psi\rangle = \sum_{i=1}^{2} c_i |\psi_i\rangle = \frac{1}{\sqrt{2}} |\psi_1\rangle - \frac{1}{\sqrt{2}} |\psi_2\rangle \qquad \sum_i |c_i|^2 = 1 \Rightarrow \text{Superposición} \tag{48}$$

$$|\psi\rangle = \sum_{i=1}^{2} p_i |\psi_i\rangle = \frac{1}{2} |\psi_1\rangle + \frac{1}{2} |\psi_2\rangle \qquad \sum_i p_i = 1 \Rightarrow \text{Mezcla} \tag{49}$$

En un estado de superposición cuántica, sabemos que el sistema se encuentra en todos los estados posibles al mismo tiempo porque al interactuar en los experimentos aparecen términos de interferencia resultado de la interacción entre estados, que no tendrían sentido de encontrarse el sistema en un solo estado. Sin embargo, en una mezcla estadística no aparecen términos de interferencia, de manera que el sistema se encuentra en un estado concreto, pero lo desconocemos.

1.5.2. Operador densidad para estados puros

Ya hemos visto a lo largo de la sección cómo podemos describir un sistema puro a partir de un vector de estado normalizado. Esto es,

$$|\psi\rangle = \sum_n c_n |u_n\rangle$$

Donde $\{|u_n\rangle\}_n$ es la base ortonormal del espacio de estados. Y los coeficientes c_n satisfacen:

$$\sum_n |c_n|^2 = 1$$

En esta descripción, si A es un observable, sus elementos de matriz son:

$$A_{np} = \langle u_n | A | u_p \rangle \tag{50}$$

Y su valor medio es:

$$\langle A \rangle = \langle \psi | A | \psi \rangle = \sum_{n,p} c_n^* c_p A_{np}$$

En esta relación, los coeficientes $c_n^* c_p$ resultan ser los elementos de matriz del operador $|\psi\rangle \langle\psi|$:

$$\langle u_p | \psi \rangle \langle \psi | u_n \rangle = c_n^* c_p$$

Es natural, por tanto, introducir el operador densidad.

Definición 1.61. *Dado un sistema en un estado $|\psi\rangle$, definimos el* ***operador densidad para estados puros*** *como:*

$$\rho = |\psi\rangle \langle\psi|$$

Los elementos de matriz de este operador conforman la matriz densidad:

$$\rho_{pn} = \langle u_p | \rho | u_n \rangle = c_n^* c_p \tag{51}$$

Con lo que la condición de normalización del estado se traduce en:

$$\sum_n |c_n|^2 = \sum_n \rho_{nn} = Tr\{\rho\} = 1$$

Y el valor medio de un operador A, usando las ecuaciones 50 y 51, toma la forma:

$$\langle A \rangle = \sum_{n,p} c_n^* c_p A_{np} = \sum_{n,p} \langle u_p | \rho | u_n \rangle \langle u_n | A | u_p \rangle = \sum_p \langle u_p | \rho A | u_p \rangle = Tr\{\rho A\}$$

Además, la probabilidad de obtención de un autovalor, siguiendo la proposición 1.59, toma la forma:

$$\mathscr{P}(a_n) = \langle \psi | P_n | \psi \rangle = Tr\{\rho P_n\}$$

Propiedades 1.62 (del operador densidad de un estado puro)**.** El operador densidad para estados puros es hermítico, idempotente y cumple que:

$$Tr\{\rho^2\} = 1$$

1.5.3. Operador densidad para mezclas estadísticas

Consideramos un sistema en un estado bajo las condiciones descritas en el apartado 1.5.1. Si medimos un observable A, ¿Cuál será la probabilidad de obtener un autovalor a_n?

Sea $|\psi\rangle = \sum_k p_k |\psi_k\rangle$ el estado del sistema y P_n el proyector asociado al autovalor a_n, entonces la probabilidad de obtener a_n si el sistema se encuentra en el estado $|\psi_k\rangle$ será:

$$\mathscr{P}_k(a_n) = \langle\psi_k|P_n|\psi_k\rangle = Tr\{\rho_k P_n\}$$

Donde:

$$\rho_k = |\psi_k\rangle \langle\psi_k|$$

Es el operador densidad correspondiente al estado $|\psi_k\rangle$.

Por lo que la probabilidad de obtener a_n en el estado mezcla será:

$$\mathscr{P}(a_n) = \sum_k p_k \mathscr{P}_k(a_n) = \sum_k p_k Tr\{\rho_k P_n\} = Tr\left\{\sum_k p_k \rho_k P_n\right\} = Tr\{\rho P_n\}$$

Donde hemos establecido:

$$\rho = \sum_k p_k \rho_k$$

Como el operador densidad del sistema en el estado de mezcla estadística.

Como uno puede imaginarse, la utilización del operador densidad simplifica enormemente los cálculos de probabilidades en este caso, ya que la matriz densidad se reduce a la suma de matrices densidad de los posibles estados, con los pesos correspondientes.

Propiedades 1.63 (del operador densidad de un estado mezcla estadística)**.** El operador densidad para estados mezcla es hermítico, pues los valores p_k son reales y los operadores ρ_k hermíticos.

Como $Tr\{\rho_k\} = 1$, se tiene que:

$$Tr\{\rho\} = \sum_k p_k Tr\{\rho_k\} = \sum_k p_k = 1$$

Sin embargo, en general, $\rho^2 \neq \rho$ y $Tr\{\rho^2\} \neq 1$.

1.5.4. Operador densidad para espacios producto tensorial

En espacios producto tensorial, con operador de densidad global, debemos extraer un operador densidad para cada espacio del producto. Trabajaremos, por tanto, con los operadores extendidos (definición 1.44) e introduciremos el concepto de *trazas parciales*. El concepto es generalizable a más sistemas, pero en este apartado vamos a definirlo únicamente con un espacio producto tensorial de dos componentes, $\mathscr{E} = \mathscr{E}_1 \otimes \mathscr{E}_2$.

Definición 1.64. *Consideramos un sistema en un estado producto tensorial de dos componentes. Sea ρ el operador densidad del sistema, definimos la* ***traza parcial*** *de ρ con respecto a (2) como el operador $\rho(1)$, cuyos elementos de matriz son:*

$$\langle u_n(1)|\rho(1)|u_{n'}(1)\rangle) = \sum_p \langle u_n(1)v_p(2)|\,\rho\,|u_{n'}(1)v_p(2)\rangle$$

Donde $\{u_i\}_i, \{v_j\}_j$ son bases de $\mathscr{E}_1$ y $\mathscr{E}_2$, respectivamente. Y la traza parcial respecto a (1) es análoga:

$$\langle v_p(2)|\rho(2)|v_{p'}(2)\rangle) = \sum_n \langle u_n(1)v_p(2)|\,\rho\,|u_n(1)v_{p'}(2)\rangle$$

El nombre de traza parcial viene de que la traza del operador ρ es:

$$Tr\{\rho\} = \sum_n \sum_p \langle u_n(1)v_p(2)| \, \rho \, |u_n(1)v_p(2)\rangle$$

Ejemplo 1.65. Suponemos un sistema formado por dos electrones, que identificamos como (1) y (2). Trabajamos en el espacio de estados de spin, $\mathscr{E}_s = \mathscr{E}_{s1} \otimes \mathscr{E}_{s2}$. La base de $\mathscr{E}_{s1}$ y de $\mathscr{E}_{s2}$ es $\{|+\rangle, |-\rangle\}$. Por tanto, la base de $\mathscr{E}_s$ es $\{|{+}{+}\rangle, |{+}{-}\rangle, |{-}{+}\rangle, |{-}{-}\rangle\}$. Como hemos establecido en la notación del capítulo 1.3, el primer lugar de los *kets* corresponde al electrón (1), mientras que el segundo lugar corresponde al electrón (2). Consideramos una matriz densidad genérica $\rho = |\psi\rangle \langle\psi|$ correspondiente al estado $|\psi\rangle$ del sistema total para ver claro el ejemplo:

$$\rho = \begin{array}{c} \begin{array}{cccc} |{+}{+}\rangle & |{+}{-}\rangle & |{-}{+}\rangle & |{-}{-}\rangle \end{array} \\ \begin{pmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & o & q & r \end{pmatrix} \end{array} \begin{array}{l} \langle{+}{+}| \\ \langle{+}{-}| \\ \langle{-}{+}| \\ \langle{-}{-}| \end{array}$$

Vamos a calcular $\rho(1)$:

$$\begin{aligned} \langle u_n(1)|\rho(1)|u_{n'}(1)\rangle) &= \sum_p \langle u_n(1)v_p(2)| \, \rho \, |u_{n'}(1)v_p(2)\rangle \\ \langle +|\rho(1)|+\rangle &= \langle ++|\rho|++\rangle + \langle +-|\rho|+-\rangle = a+f \\ \langle +|\rho(1)|-\rangle &= \langle ++|\rho|-+\rangle + \langle +-|\rho|--\rangle = i+o \\ \langle -|\rho(1)|+\rangle &= \langle -+|\rho|++\rangle + \langle --|\rho|+-\rangle = c+h \\ \langle -|\rho(1)|-\rangle &= \langle -+|\rho|-+\rangle + \langle --|\rho|--\rangle = k+r \end{aligned}$$

$$\rho(1) = \begin{array}{c} \begin{array}{cc} |+\rangle & |-\rangle \end{array} \\ \begin{pmatrix} a+f & i+o \\ c+h & k+r \end{pmatrix} \end{array} \begin{array}{l} \langle +| \\ \langle -| \end{array}$$

Y lo mismo con $\rho(2)$:

$$\begin{aligned} \langle v_p(2)|\rho(2)|v_{p'}(2)\rangle) &= \sum_n \langle u_n(1)v_p(2)| \, \rho \, |u_n(1)v_{p'}(2)\rangle \\ \langle +|\rho(2)|+\rangle &= \langle ++|\rho|++\rangle + \langle -+|\rho|-+\rangle = a+k \\ \langle +|\rho(2)|-\rangle &= \langle ++|\rho|+-\rangle + \langle -+|\rho|--\rangle = e+q \\ \langle -|\rho(2)|+\rangle &= \langle +-|\rho|++\rangle + \langle --|\rho|-+\rangle = b+l \\ \langle -|\rho(2)|-\rangle &= \langle +-|\rho|+-\rangle + \langle --|\rho|--\rangle = f+r \end{aligned}$$

$$\rho(2) = \begin{array}{c} \begin{array}{cc} |+\rangle & |-\rangle \end{array} \\ \begin{pmatrix} a+k & e+q \\ b+l & f+r \end{pmatrix} \end{array} \begin{array}{l} \langle +| \\ \langle -| \end{array}$$

Proposición 1.66. *En las condiciones establecidas al principio del apartado, sea $A(1)$ un observable en el espacio $\mathscr{E}_1$, se tiene que:*

$$\langle A(1)\rangle = Tr\{\rho(1)A(1)\}$$

Y análogamente para un observable $B(2)$ actuando en $\mathscr{E}_2$.

2. Introducción a la información cuántica

En esta sección, basada en el libro [1], introduciremos los conceptos que serán utilizados para comprender la teoría de errores cuánticos y desarrollar los códigos correctores adecuados. En el capítulo 1, hemos desarrollado la teoría cuántica para sistemas cerrados. No obstante, en la práctica, es virtualmente imposible aislar un sistema cuántico del exterior, debido a la naturaleza de estos sistemas. Existen métodos para minimizar ese ruido exterior, pero debemos desarrollar una teoría que nos permita incorporar el ruido como una variable más del estado.

Para empezar el capítulo, debemos definir la unidad básica de información cuántica, el *qubit*.

Definición 2.1. *Llamamos* ***qubit*** *a cualquier sistema cuántico de dos niveles:*

$$|\psi\rangle = \alpha_1 |\varphi_1\rangle + \alpha_2 |\varphi_2\rangle \qquad |\alpha_1|^2 + |\alpha_2|^2 = 1$$

Habitualmente, cuando no sea necesario especificar la base de autoestados en la que trabajamos, denotaremos estos dos niveles como $|0\rangle$ *y* $|1\rangle$*:*

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$$

Un sistema que se encuentre en este estado es capaz de almacenar información. Puede estar, por ejemplo, en el estado $|0\rangle$ o en el estado $|1\rangle$, conformando un *bit* clásico. La novedad de la computación cuántica es que ahora es posible que el *qubit* se encuentre en un estado de superposición de $|0\rangle$ y $|1\rangle$, proporcionando un plano de estados que dotan a la computación cuántica de la potencia que se le ha venido asociando durante los últimos años. No obstante, conviene hacer hincapié en que cuando el qubit es medido, obtenemos $|0\rangle$ o $|1\rangle$, con probabilidades $|\alpha_0|^2$ y $|\alpha_1|^2$, respectivamente.

Observación 2.2. Una representación que nos será útil de un qubit es la esfera de Bloch: una representación del qubit en coordenadas esféricas:

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

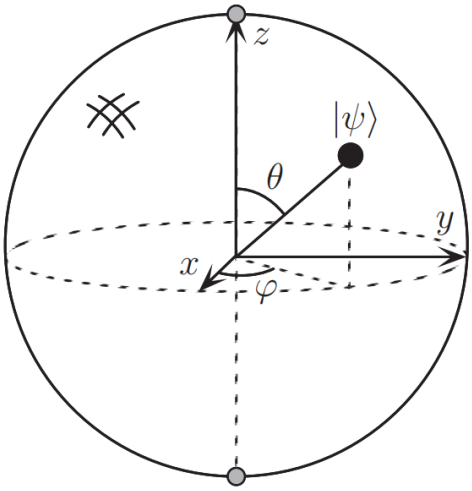

Figura 1: Representación de un qubit mediante la esfera de Bloch [1]

Siendo $cos(\theta/2)$ y $sin(\theta/2)$ los módulos de α_0 y α_1, respectivamente, y φ la diferencia de fase entre los dos coeficientes, es decir, la diferencia entre φ_1 y φ_0 al escribir los coeficientes en forma polar: $\alpha_0 = |\alpha_0|e^{i\varphi_0}$ y $\alpha_1 = |\alpha_1|e^{i\varphi_1}$.

Bajo esta representación, es fácil ver que el polo norte ($\theta = 0$) corresponde al estado $|0\rangle$ ($\alpha_1 = 0$), mientras que el polo sur ($\theta = \pi$) corresponde al estado $|1\rangle$ ($\alpha_0 = 0$).

Además, esta representación tiene la propiedad de que, al medir el qubit, el estado de colapso más probable es el correspondiente al hemisferio en el que se encuentre el estado previo a la medida.

Pongamos a continuación el ejemplo de un sistema de dos qubits para ilustrar el funcionamiento simultáneo de varios qubits.

Ejemplo 2.3. Para considerar dos qubits, debemos emplear la teoría del espacio producto tensorial: la base de ambos qubits será $\{|0\rangle, |1\rangle\}$, por lo que la base conjunta será $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, y el vector de estado del sistema:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \qquad |\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

Si medimos el sistema completo, la probabilidad de obtener uno de los cuatro estados posibles es el cuadrado del módulo del coeficiente correspondiente. Supongamos que medimos solamente el primer qubit. Según el cuarto postulado, la probabilidad de obtener el estado $|0\rangle$ es

$$\mathscr{P}(|0\rangle) = \sum_{i=1}^{g_0} |\langle u_0^i(1)|\psi\rangle|^2 = |\langle 00|\psi\rangle|^2 + |\langle 01|\psi\rangle|^2 = |\alpha_{00}|^2 + |\alpha_{01}|^2$$

Y el estado en el que el sistema pasa a estar inmediatamente después de la medida, según el postulado 5, es:

$$|\psi'\rangle = \frac{P_0|\psi\rangle}{\sqrt{\langle\psi|P_0|\psi\rangle}} = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

Donde, siguiendo la definición 1.30 del operador proyección sobre un subespacio:

$$P_0|\psi\rangle = |00\rangle\langle 00| + |01\rangle\langle 01|$$

Por lo que:

$$P_0|\psi\rangle = (|00\rangle\langle 00| + |01\rangle\langle 01|)|\psi\rangle = |00\rangle\langle 00|\psi\rangle + |01\rangle\langle 01|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle$$

Y

$$\langle\psi|P_0|\psi\rangle = \langle\psi|(\alpha_{00}|00\rangle + \alpha_{01}|01\rangle) = |\alpha_{00}|^2 + |\alpha_{01}|^2$$

No es ningún secreto que los ordenadores cuánticos que se están intentando construir a día de hoy tratan de maximizar el número de qubits, la justificación podemos encontrarla en el razonamiento siguiente: Con 1 qubit, la base de estados del sistema es $\{|0\rangle, |1\rangle\}$, por lo que el estado vendrá dado por 2 coeficientes, α_0 y α_1. Con 2 qubits, la base pasa a ser $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, por lo que el estado vendrá dado por 4 coeficientes, como en el ejemplo anterior.

Para, véase, 270 qubits, la base será:

$$\{|x_1x_2\ldots x_{270}\rangle\}_{x_i=0,1}$$

Es decir, que serán 2^{270} los coeficientes que definirán el sistema formado por esos qubits. Este número de coeficientes es del orden del número de átomos estimados del universo observable (alrededor de 10^{81}). Tratar de almacenar esta cantidad de coeficientes complejos es desorbitado para cualquier ordenador clásico, mientras que uno cuántico lo lograría con "tan solo" 270 qubits. Como comentario, para hacerse una idea de la complejidad de la naturaleza, tan solo 3 átomos de uranio interactuando entre sí contienen alrededor de 270 electrones, formando un sistema cuántico de 10^{81} variables solamente con los electrones. Más aún, en una corriente eléctrica, solamente en 1 milímetro de cable se mueven 10^{18} electrones que interactúan entre sí, formando un sistema cuántico cuyo estado consta de $2^{10^{18}}$ coeficientes.

2.1. Ruido clásico

Antes de describir el ruido cuántico, conviene tener una idea del modelo utilizado para describir el ruido clásico. Consideramos que la información está codificada en bits que pueden tomar los valores 0 o 1. La interacción de los medios de almacenamiento y transporte del bit con el exterior puede causar un *bit flip*, es decir, el bit puede cambiar al otro estado. El modelo de ruido establece que el bit tendrá una probabilidad p de sufrir un bit flip y una probabilidad $1-p$ de permanecer en el estado original. Esto puede modelarse de la siguiente manera:

Sean p_0 y p_1 las probabilidades de que el bit se encuentre inicialmente en los estados 0 y 1, respectivamente, q_0 y q_1 las probabilidades correspondientes de los estados finales (tras la acción del ruido), X el estado inicial del bit e Y el estado final de bit, la ley de probabilidad total establece que:

$$\mathscr{P}(Y=y)=\sum_x \mathscr{P}(Y=y|X=x)\mathscr{P}(X=x)$$

Las probabilidades condicionadas $\mathscr{P}(Y=y|X=x)$ se conocen como probabilidades de transición, ya que engloban los cambios que puede haber sufrido el sistema. Escribiendo estas ecuaciones explícitamente para un bit, tenemos:

$$\begin{pmatrix} q_0 \\ q_1 \end{pmatrix} = \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix} \begin{pmatrix} p_0 \\ p_1 \end{pmatrix} \tag{52}$$

No obstante, la modelización del ruido nunca va a resultar tan sencilla, ya que el bit, normalmente, va a sufrir varias transformaciones en su camino, tales como atravesar puertas lógicas o elementos similares. Podemos visualizar esto suponiendo un bit que va a sufrir dos transformaciones por alguno de estos elementos, de manera que el estado inicial del bit es $X \in \{0,1\}$, una transformación nos proporciona un estado intermedio Y y otra transformación el estado final Z. Es en las transformaciones donde el bit puede haber sufrido un cambio inesperado, la puerta lógica o el componente correspondiente podría no haber funcionado correctamente. Asumiremos para este modelo que las dos transformaciones son independientes. Los sucesivos procesos de posible ruido actúan independientemente.

Esto nos proporciona un proceso estocástico:

$$X \longrightarrow Y \longrightarrow Z \tag{53}$$

Conocido como *proceso de Markov* o *Cadena de Markov*.

En el razonamiento anterior (52), de un proceso de etapa simple, tenemos que las probabilidades finales $\vec{q}$ se relacionan con las iniciales $\vec{p}$ mediante una ecuación:

$$\vec{q} = E\vec{p}$$

Siendo E una matriz de probabilidades de transición conocida como *matriz de evolución*, que describe una relación lineal entre las dos probabilidades. Para un proceso de Markov multietapa, habría tantas matrices de evolución como etapas. En el caso de la expresión 53, tendríamos dos matrices de evolución.

Además, para que $E\vec{p}$ sea una distribución de probabilidad válida, la matriz E debe satisfacer unas determinadas propiedades: Todos los elementos de E deben ser no negativos y todas las columnas deben sumar 1. Si esto no se cumpliese, podríamos obtener probabilidades negativas, u obtener una distribución de probabilidades cuya suma no fuese la unidad. Esto es fácil de visualizar suponiendo que en la matriz E la primera columna no suma 1, y en el vector $\vec{p}$ el primer elemento es 1 y el resto nulos. Obtendríamos un vector $\vec{q}$ cuyos valores no sumarían 1, por lo que no sería una distribución de probabilidad.

2.2. Operaciones cuánticas

El formalismo de las operaciones cuánticas es una herramienta para describir la evolución de sistemas cuánticos en una amplia variedad de circunstancias, entre las que se incluyen los procesos de Markov. La formulación de estos procesos se hace de una manera similar a la descrita anteriormente para sistemas clásicos, solo que en lugar de distribuciones de probabilidad, utilizaremos operadores de densidad, que desarrollamos en el apartado 1.5.

$$\rho' = \mathcal{E}(\rho)$$

Donde $\mathcal{E}$ es una aplicación lineal que denominaremos *operación cuántica* y que transforma un operador densidad en otro.

Ejemplo 2.4. Consideramos un sistema en un estado $|\psi\rangle$, que evoluciona bajo la acción de un operador unitario U.

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

Consideramos el operador densidad del estado: $\rho = |\psi\rangle\langle\psi|$. El operador densidad asociado al estado $|\psi'\rangle = U|\psi\rangle$ será:

$$\rho' = U|\psi\rangle\langle\psi|U^\dagger$$

Ya que el *bra* asociado al *ket* ($U|\psi\rangle$) es su conjugado hermítico, ($\langle\psi|U^\dagger$).

Entonces, podemos escribir de una forma equivalente la evolución del sistema utilizando el operador densidad:

$$\rho \longrightarrow \rho' = U|\psi\rangle\langle\psi|U^\dagger = U\rho U^\dagger = \mathcal{E}(\rho)$$

Donde $\mathcal{E}$ es la operación cuántica definida en este caso por la acción de esos operadores unitarios.

2.2.1. Representación en suma de operadores

Existen 3 formas de entender y trabajar con las operaciones cuánticas (para más información, ver [1]), pero nosotros nos centraremos en su representación mediante suma de operadores.

La evolución de un sistema cuántico cerrado siempre se describe como la acción de un operador unitario. Por tanto, vamos a tratar el sistema de estudio y el entorno de manera conjunta para poder describir de esta manera su evolución. Consideramos $\{|e_k\rangle\}_k$ una base ortonormal del espacio de estados del entorno $\mathscr{E}_{env}$, siendo $|e_0\rangle$ el estado inicial del entorno. De manera que $\rho_{env} = |e_0\rangle\langle e_0|$ será el operador densidad inicial del entorno y $\rho = |\psi\rangle\langle\psi|$ el operador densidad del sistema de estudio. Sea U la transformación unitaria lineal a la que sometemos al sistema de estudio, como en el ejemplo 2.4, podemos modelar la evolución del sistema de estudio con la siguiente operación cuántica:

$$\mathcal{E}(\rho) = \sum_k \langle e_k|U\left(\rho \otimes |e_0\rangle\langle e_0|\right)U^\dagger|e_k\rangle = \sum_k E_k \rho E_k^\dagger \tag{54}$$

Donde $E_k = \langle e_k|U|e_0\rangle$ es un operador que actúa sobre el espacio de estados del sistema principal, y engloba tanto la transformación deseada de este como la acción del entorno. Estos operadores se llaman *elementos de operación* de la operación cuántica $\mathcal{E}$, y la expresión 54 es la representación en suma de operadores.

Observación 2.5. Aunque E_k sea un *braket*, que a primera vista puede parecer un elemento de matriz (definición 1.14) en realidad es un operador, ya que estamos trabajando en el espacio producto del sistema principal y el entorno. El operador unitario de evolución actúa sobre el sistema producto, de manera que al aplicarle el *braket* $\langle e_k|U|e_0\rangle$, considerando que los $\{|e_k\rangle\}_k$ son elementos de la base del sistema del entorno, obtenemos un operador que solamente actúa sobre el sistema principal. De esta manera, la representación en suma de operadores nos permite aplicar el operador U primero al entorno y después al sistema principal.

Vamos a presentar un resultado de unicidad de la representación en suma de operadores que nos será útil en el desarrollo de la teoría de corrección de errores.

Teorema 2.6. *Sean $\{E_1, \ldots, E_n\}$ y $\{F_1, \ldots, F_n\}$ dos conjuntos de elementos de operación que dan lugar a las operaciones cuánticas $\mathcal{E}$ y $\mathcal{F}$, respectivamente, entonces $\mathcal{E} = \mathcal{F}$ si, y solo si, existe una matriz unitaria compleja u_{ij} tal que*

$$E_i = \sum_j u_{ij} F_j$$

Con este formalismo, en los siguientes apartados, vamos a expresar los diferentes procesos de ruido cuántico que puede sufrir un qubit.

2.2.2. Matrices de Pauli

Las matrices de Pauli, comúnmente usadas en el campo de la mecánica cuántica, representan las tres operaciones cuánticas básicas. En el caso de un espacio de estados de dos dimensiones como es el caso de los qubits, estas matrices son:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{55}$$

Son matrices unitarias, de manera que los operadores asociados conservan la norma del estado sobre el que se aplican. En los siguientes apartados veremos qué efecto tienen estos operadores sobre los qubits, es decir, cómo se aplican sobre la información cuántica, a través del concepto de *canal ruidoso*.

Definición 2.7. *Se dice que un qubit atraviesa un **canal ruidoso** si el qubit se encuentra en un contexto en el que tiene cierta probabilidad de ser afectado por una operación cuántica.*

2.2.3. Bit flip

Representada por la matriz de Pauli X, esta operación cuántica cambia el estado $|0\rangle$ de un qubit por el estado $|1\rangle$ y viceversa. Consideramos que la probabilidad de que el qubit permanezca invariable es p, mientras que la probabilidad de que el qubit vea alterado su estado será $(1-p)$. Los elementos de operación de esta operación cuántica son:

$$E_0 = \sqrt{p}\,\mathbf{I} = \sqrt{p}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad E_1 = \sqrt{1-p}\,X = \sqrt{1-p}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{56}$$

Esta operación cuántica, como todas las demás, puede ser representada mediante rotaciones, deformaciones y traslaciones en la esfera de Bloch. Para ello, consideramos el estado inicial del qubit, que tendrá la forma:

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$$

Por tanto, la matriz asociada al operador densidad será:

$$\rho = |\psi\rangle\langle\psi| = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}\begin{pmatrix} \alpha_0^* & \alpha_1^* \end{pmatrix} = \begin{pmatrix} |\alpha_0|^2 & \alpha_0\alpha_1^* \\ \alpha_1\alpha_0^* & |\alpha_1|^2 \end{pmatrix}$$

Siendo de esta manera las coordenadas cartesianas de los qubits en la esfera de Bloch en términos de los elementos del operador densidad ([7]):

$$\begin{aligned} x &= 2Re(\rho_{01}) = 2Re(\alpha_0\alpha_1^*) \\ y &= 2Im(\rho_{10}) = 2Im(\alpha_1\alpha_0^*) \\ z &= \rho_{00} - \rho_{11} = |\alpha_0|^2 - |\alpha_1|^2 \end{aligned}$$

La acción de la operación cuántica puede describirse mediante la representación de suma de operadores como:

$$\mathcal{E}(\rho) = E_0\rho E_0^\dagger + E_1\rho E_1^\dagger =$$
$$p\begin{pmatrix}1&0\\0&1\end{pmatrix}\begin{pmatrix}|\alpha_0|^2&\alpha_0\alpha_1^*\\\alpha_1\alpha_0^*&|\alpha_1|^2\end{pmatrix}\begin{pmatrix}1&0\\0&1\end{pmatrix}+(1-p)\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}|\alpha_0|^2&\alpha_0\alpha_1^*\\\alpha_1\alpha_0^*&|\alpha_1|^2\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix} =$$
$$= p\begin{pmatrix}|\alpha_0|^2&\alpha_0\alpha_1^*\\\alpha_1\alpha_0^*&|\alpha_1|^2\end{pmatrix}+(1-p)\begin{pmatrix}|\alpha_1|^2&\alpha_1\alpha_0^*\\\alpha_0\alpha_1^*&|\alpha_0|^2\end{pmatrix}$$

Por lo que las nuevas coordenadas de los qubits en la esfera de Bloch son:

$$x = 2Re(\rho_{01}) = 2Re[p(\alpha_0\alpha_1^*) + (1-p)(\alpha_1\alpha_0^*)]$$
$$y = 2Im(\rho_{10}) = 2Im[p(\alpha_1\alpha_0^*) + (1-p)(\alpha_0\alpha_1^*)]$$
$$z = \rho_{00} - \rho_{11} = p(|\alpha_0|^2 - |\alpha_1|^2) + (1-p)(|\alpha_1|^2 - |\alpha_0|^2)$$

Por ejemplo, con un parámetro $p = 0,2$, la esfera queda deformada de la siguiente manera:

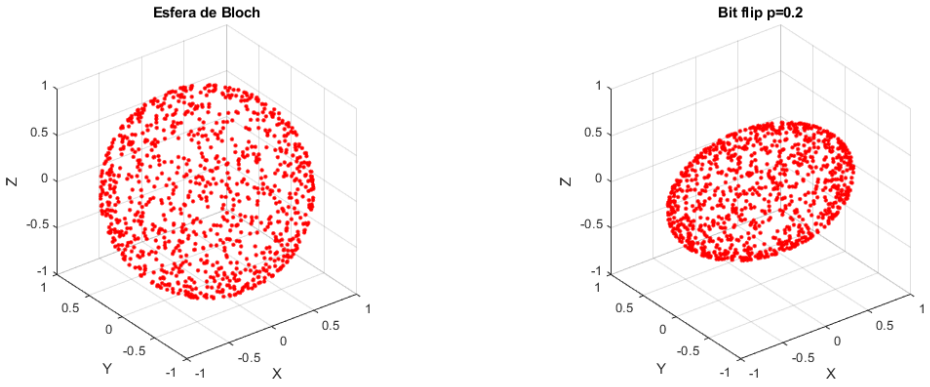

Figura 2: A la izquierda, la esfera de estados puros. A la derecha, la representación de los estados tras atravesar un canal de bit flip con p=0,2. EL eje X no varía, mientras que el plano YZ se contrae uniformemente con un factor (1-2p). Simulación realizada con el código expuesto en el anexo.

Esta representación gráfica resulta muy visual si tenemos en cuenta que:

$$Tr\{\rho^2\} = \frac{1+|r|^2}{2}$$

Donde $|r|$ es la norma del vector en la esfera de Bloch. Efectivamente, para estados puros se tiene que $Tr\{\rho^2\} = 1$. No obstante la acción del bit flip siempre reduce el valor de la traza, dejando al sistema en un estado de mezcla estadística. Recordemos de la propiedad 1.62 que para estados puros se cumple que $Tr\{\rho^2\} = 1$, mientras que para mezclas estadísticas $Tr\{\rho^2\} \neq 1$.

En el caso del bit flip, podemos observar que los únicos estados que, tras atravesar el canal, permanecen en un estado puro son $|+\rangle$ y $|-\rangle$, que corresponden a los valores extremos de la esfera en el eje X, es decir, $\varphi = 0$ y $\varphi = \pi$. Podemos comprobar que, efectivamente, al aplicar la operación de bit flip a estos dos estados permanecen invariados.

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \xrightarrow[bitflip]{} \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle) = |+\rangle$$
$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \xrightarrow[bitflip]{} \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) = e^{i\pi}|-\rangle = |-\rangle$$

Recordemos que un factor de fase global no cambia el estado cuántico (1.52). El resto de estados, tras atravesar el canal, se transforman en una mezcla estadística.

2.2.4. Phase flip

La operación de Phase flip, representada por la matriz de Pauli Z, ([8]) no tiene análogo clásico como sí que lo tenía el bit flip. Esta operación cambia la fase relativa de los estados superpuestos un valor de π. En el caso más sencillo, consideramos un qubit en el estado conocido como $|+\rangle$:

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

Los coeficientes de este estado son $\alpha_0 = \alpha_1 = 1$, o escritos en forma polar, $\alpha_0 = \alpha_1 = e^{i0}$, es decir, la fase relativa entre los dos estados superpuestos es 0. Añadir un factor de fase global no cambia el estado cuántico, por eso solamente nos centramos en la fase relativa, que será nula siempre que el argumento de los dos coeficientes coincida. Si aplicamos la operación de phase flip al estado $|+\rangle$, la fase relativa entre los dos estados superpuestos pasará de ser 0 a ser π, por lo que obtendremos el estado conocido como $|-\rangle$:

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

Los elementos de operación de esta operación cuántica son:

$$E_0 = \sqrt{p}\,\mathbb{I} = \sqrt{p}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad E_1 = \sqrt{1-p}\,Z = \sqrt{1-p}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Por lo que, siguiendo el razonamiento del apartado anterior aplicando el procedimiento de suma de operadores, obtenemos la siguiente deformación de la esfera de Bloch:

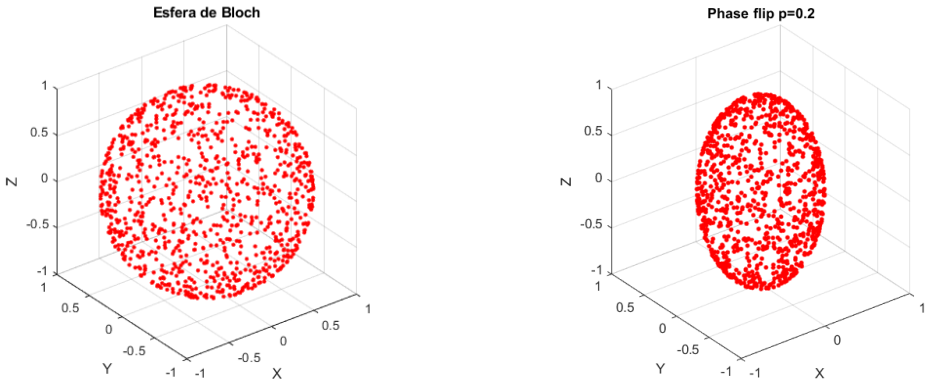

Figura 3: A la izquierda, la esfera de estados puros. A la derecha, la representación de los estados tras atravesar un canal de phase flip con p=0,2. EL eje Z no varía, mientras que el plano XY se contrae uniformemente con un factor (1-2p). Simulación realizada con el código expuesto en el anexo.

En este caso, los estados $|0\rangle$ y $|1\rangle$ (recordemos que son, respectivamente, los polos norte y sur de la esfera de Bloch) son los únicos que permanecen en un estado puro ($Tr\{\rho^2\} = 1$) tras atravesar el canal de phase flip. Todos los demás pasan a un estado de mezcla estadística ($Tr\{\rho^2\} \neq 1$). Esto se debe a que alterar las fases relativas en los estados $|0\rangle$ y $|1\rangle$ no es sino aplicar un factor de fase global, que no varía el estado, de manera que en estos dos casos conocemos los estados de los qubits tras atravesar el canal.

También pueden combinarse las dos operaciones cuánticas, en la operación bit-phase flip, cuyos elementos de operación son:

$$E_0 = \sqrt{p}\,\mathbb{I} = \sqrt{p}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad E_1 = \sqrt{1-p}\,Y = \sqrt{1-p}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

Y el efecto que tiene sobre la esfera de Bloch se ilustra en la siguiente figura:

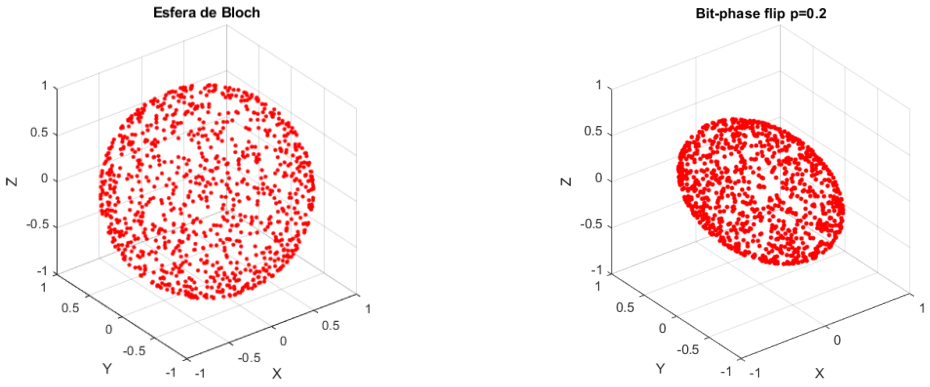

Figura 4: A la izquierda, la esfera de estados puros. A la derecha, la representación de los estados tras atravesar un canal de bit-phase flip con p=0,2. EL eje Y no varía, mientras que el plano XZ se contrae uniformemente con un factor (1-2p). Simulación realizada con el código expuesto en el anexo.

En esta esfera deformada podemos observar que los dos únicos estados que no entran en mezcla estadística tras atravesar el canal bit-phase flip son

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

que son los correspondientes a los valores extremos de la esfera en el eje Y, es decir, a $\varphi = \pi/2$ y $\varphi = -\pi/2$ (ver figura 1).

2.2.5. Depolarización

La polarización de un qubit es la relación entre los módulos de los coeficientes α_0 y α_1. Si $|\alpha_0| = 1$ y $|\alpha_1| = 0$, diremos que el qubit está totalmente polarizado en el estado $|0\rangle$ y viceversa. En cambio, si $|\alpha_0| = |\alpha_1|$, diremos que el estado está totalmente despolarizado. Este es el caso de los estados $|+\rangle$ y $|-\rangle$. Si los módulos de los coeficientes poseen otra relación, diremos que el qubit está parcialmente polarizado en el estado cuyo coeficiente sea mayor en módulo.

La operación cuántica de depolarización convierte el estado de cualquier qubit en $|+\rangle$ o $|-\rangle$, de manera que, independientemente del estado de polarización inicial del qubit, el estado final será completamente despolarizado. La matriz densidad de un estado completamente despolarizado es $\mathbb{I}/2$. Por tanto, el estado de un qubit tras atravesar un canal despolarizador es:

$$\mathcal{E}(\rho) = p\left(\frac{\mathbb{I}}{2}\right) + (1-p)\rho$$

Esta operación cuántica no está escrita con el formalismo de suma de operadores por cuestiones de simplicidad, ya que en este caso es más sencillo y directo definir de esta manera la operación. Con el formalismo de suma de operadores, esta operación cuántica se escribe como:

$$\mathcal{E}(\rho) = \frac{p}{3}\left(X\rho X + Y\rho Y + Z\rho Z\right) + (1-p)\rho$$

Y el efecto de este canal despolarizador sobre la esfera de Bloch es:

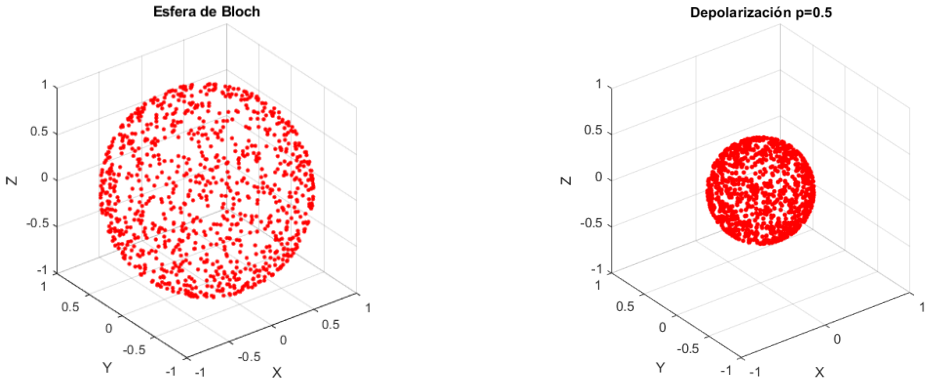

Figura 5: A la izquierda, la esfera de estados puros. A la derecha, la representación de los estados tras atravesar un canal despolarizador con p=0,5. La esfera se contrae uniformemente con factor p. Simulación realizada con el código expuesto en el anexo.

En este caso, todos los qubits entran en un estado de mezcla estadística al atravesar el canal despolarizador, ya que $Tr\{\rho^2\} \neq 1$ en ningún caso.

2.2.6. Amortiguamiento de amplitud

La amplitud de un estado cuántico está directamente relacionada con su distribución de energía. Cuando hay una disipación de energía obtenemos como consecuencia una disminución de la amplitud del estado. El amortiguamiento adopta diferentes formas, sin embargo, nos centraremos en una por su generalidad y su uso extendido: el amortiguamiento por *beam splitting* [9]. Consideramos un sistema formado por un fotón en el estado cuántico $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$, representando los *kets*, no diferentes estados del fotón, sino la propia presencia del fotón. Siendo $|0\rangle$ un estado con 0 fotones y $|1\rangle$ un estado con un fotón. Claramente, el primer estado no tiene energía, mientras que el segundo sí. Un *beam splitter* es un dispositivo que divide un haz de fotones en dos haces: reflejado y refractado. La energía del haz de fotones, en consecuencia, tiene una probabilidad de verse reducida, e incluso de "perderse" en el entorno. Los elementos de operación de la operación cuántica asociada a este fenómeno son:

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix} \qquad E_1 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}$$

Siendo $\gamma = sin^2\theta$, con θ el ángulo entre los haces reflejado y refractado, pudiendo interpretarse γ como la probabilidad de perder un fotón. Podemos ver que E_1 cambia el estado $|1\rangle$ al estado $|0\rangle$, lo que físicamente significa perder el fotón. Por su parte, E_0 deja el estado $|0\rangle$ inalterado, mientras que reduce la amplitud del estado $|1\rangle$, lo que físicamente se interpreta como una mayor probabilidad de que el fotón se encuentre en el estado $|0\rangle$. El efecto de este canal de amortiguamiento de amplitud puede ilustrarse también por la deformación que produce en la esfera de Bloch:

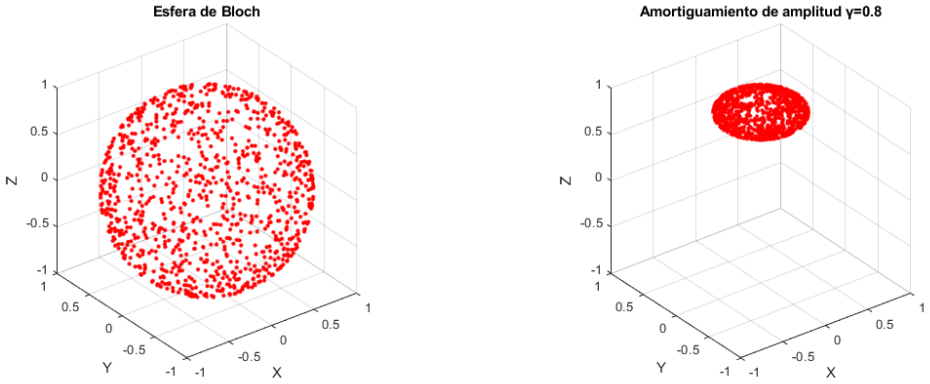

Figura 6: A la izquierda, la esfera de estados puros. A la derecha, la representación de los estados tras atravesar un canal de amortiguamiento de amplitud con $\gamma = 0,8$. Simulación realizada con el código expuesto en el anexo.

Podemos observar cómo tan solo permanece inalterado el estado $|0\rangle$, situado en el polo norte de la esfera. Todos los demás estados pasan a estar en una mezcla estadística. Efectivamente el amortiguamiento de amplitud no tiene ningún efecto en el estado cuando la amplitud es nula de partida.

2.2.7. Amortiguamiento de fase

El proceso de amortiguamiento de fase es más sutil que los anteriores. Al igual que el phase flip, es un fenómeno exclusivo de la mecánica cuántica. El amortiguamiento de fase describe la pérdida de información cuántica sin pérdida de energía. Se da cuando un sistema evoluciona durante un cierto periodo de tiempo que no se conoce con exactitud, produciendo una pérdida de información, traducida en la fase relativa de los autoestados. Puede modelizarse de una manera similar al amortiguamiento de amplitud, con un haz de fotones en un proceso de dispersión, con elementos de operación:

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{pmatrix} \qquad E_1 = \begin{pmatrix} 0 & 0 \\ 0 & \sqrt{\lambda} \end{pmatrix}$$

Donde el parámetro λ puede ser interpretado como la probabilidad de que un fotón del sistema sea dispersado sin perder energía (para más información sobre la dispersión o *scattering*, ver [10]) Cabe destacar que, en la descripción completa, λ es una función creciente con el tiempo, con asíntota en $\lambda = 1$. De los elementos de operación podemos deducir que E_0 deja el estado $|0\rangle$ inalterado, mientras que reduce la amplitud del estado $|1\rangle$, igual que en la operación de amortiguamiento de amplitud. Sin embargo, E_1 destruye el estado $|0\rangle$ y reduce la amplitud de $|1\rangle$, sin transformarlo en $|0\rangle$.

El efecto de este canal ruidoso sobre la esfera de Bloch es parecido al del canal de phase flip, pero menos "agresivo", de tal modo que con $\lambda = 0{,}8$ conseguimos un efecto similar al phase flip con p=0.2:

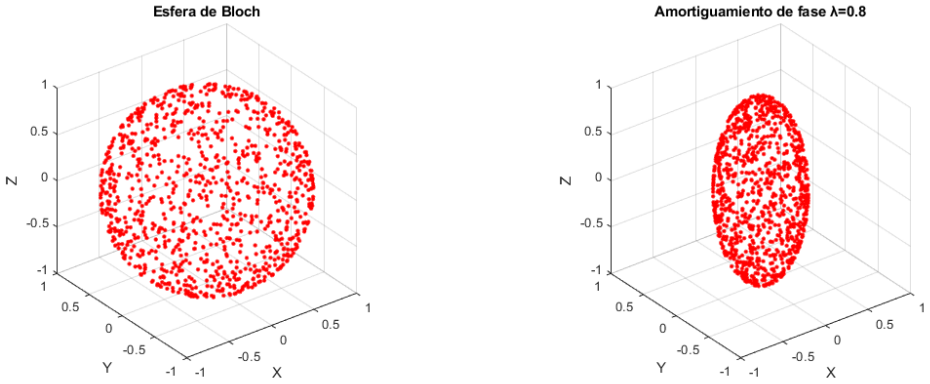

Figura 7: A la izquierda, la esfera de estados puros. A la derecha, la representación de los estados tras atravesar un canal de amortiguamiento de fase con $\lambda = 0,8$. Simulación realizada con el código expuesto en el anexo.

Podemos observar que los estados $|0\rangle$ y $|1\rangle$ permanecen inalterados, ya que al estar formados por un solo autoestado, un término de fase relativa es un factor de fase global, así que el estado no se ve alterado.

Observación 2.8. El amortiguamiento de fase ha sido objeto de gran especulación durante los últimos años. Se cree que es el fenómeno responsable de que el mundo macroscópico no exhiba propiedades cuánticas, ya que las fases de los estados de los sistemas individuales se alteran espontáneamente produciendo un sistema global incoherente y, por tanto, sin interferencias entre estados coherentes, fenómenos de superposición macroscópicos, entrelazamiento, etc. Nótese que, tomando los elementos de operación establecidos en este apartado y aplicándolos a la matriz densidad mediante el procedimiento de suma de operadores, obtenemos:

$$\mathcal{E}(\rho) = \begin{pmatrix} |\alpha_0|^2 & \sqrt{1-\lambda}\,\alpha_0\alpha_1^* \\ \sqrt{1-\lambda}\,\alpha_0^*\alpha_1 & |\alpha_1|^2 \end{pmatrix}$$

Los términos de interferencia entre estados (elementos no diagonales), considerando que λ es una función que crece rápidamente con el tiempo acercándose a $\lambda = 1$, se anulan rápidamente cuando un sistema atraviesa un canal de amortiguamiento de fase, es decir, cuando un sistema interactúa con el entorno. De este modo, si un sistema no se encuentra perfectamente aislado de su entorno, su operador de densidad pasa a ser diagonal en poco tiempo, de manera que se comporta como un sistema clásico. En la naturaleza, ningún sistema se encuentra perfectamente aislado. Si lo estuviera, ni siquiera podríamos percibirlo, ya que percibirlo implicaría interactuar con él.

2.3. Medida de distancias

Con el objetivo de desarrollar algoritmos de corrección de errores cuánticos, debemos conseguir que la secuencia final de qubits se parezca lo máximo posible a la secuencia inicial. Este parecido lo formalizaremos incorporando un concepto de distancia entre dos vectores de información.

2.3.1. Información clásica

Consideramos dos distribuciones de probabilidad sobre el mismo índice, $\{p_x\}$, $\{q_x\}$. Podemos definir dos funciones para comparar la "similitud" de las dos distribuciones.

Distancia de traza clásica

Definición 2.9. *Sean $\{p_x\}$, $\{q_x\}$ dos distribuciones de probabilidad, definimos la* ***distancia de traza*** *o distancia de Kolmogorov como:*

$$D(p_x, q_x) = \frac{1}{2}\sum_x |p_x - q_x|$$

El nombre de distancia está justificado, ya que es simétrica, cumple la propiedad triangular y no toma valores negativos, anulándose únicamente cuando las distribuciones son idénticas.

Observación 2.10. Una definición equivalente de la distancia de traza es:

$$D(p_x, q_x) = \max_S |p(S) - q(S)| = \max_S \left| \sum_{x\in S} p_x - \sum_{x\in S} q_x \right|$$

Lo que maximizamos (sobre todos los subconjuntos S del conjunto de índices $\{x\}$) en esta expresión es la diferencia entre las probabilidades de que el evento S ocurra de acuerdo con las dos distribuciones de probabilidad.

Fidelidad clásica

Definición 2.11. *Sean $\{p_x\}$, $\{q_x\}$ dos distribuciones de probabilidad, definimos la* ***fidelidad*** *entre las dos distribuciones como:*

$$F(p_x, q_x) = \sum_x \sqrt{p_x q_x}$$

Esta función no es una distancia, ya que cuando las distribuciones son idénticas el resultado es la unidad.

Estas dos definiciones nos sirven para comparar dos distribuciones de probabilidad dadas. No obstante, hay una tercera noción de distancia "dinámica" que da cuenta de la preservación de la información tras sufrir un proceso físico "ruidoso".

Medidas dinámicas

Supongamos que X es una variable aleatoria que sufre un proceso de ruido, dando como resultado otra variable aleatoria Y mediante un proceso de Markov, teniendo ambas variables aleatorias el mismo rango de valores, que podemos denotar por x. Es interesante calcular, en este caso, la probabilidad de que la variable aleatoria final no sea igual que la inicial, para tener una medida del grado de preservación de la información del proceso.

Esta medida dinámica puede entenderse como un caso particular de la distancia de traza, de la siguiente manera: Primero hacemos una copia de la variable aleatoria inicial X, creando una nueva variable $\tilde{X} = X$, después X atraviesa el proceso físico que la transforma en Y. Podemos ahora comparar las distribuciones $(\tilde{X}, X)$ y $(\tilde{X}, Y)$ usando la distancia de traza:

$$\begin{aligned}
D((\tilde{X}, X)(\tilde{X}, Y)) &= \frac{1}{2}\sum_{x,x'} |\delta_{xx'} P(X = x) - P(\tilde{X} = x, Y = x')| = \\
&= \frac{1}{2}\sum_{x\neq x'} P(\tilde{X} = x, Y = x') + \frac{1}{2}\sum_x |P(X = x) - P(\tilde{X} = x, Y = x)| = \\
&= \frac{1}{2}\sum_{x\neq x'} P(\tilde{X} = x, Y = x') + \frac{1}{2}\sum_x \Big(P(X = x) - P(\tilde{X} = x, Y = x)\Big) = \\
&= \frac{P(\tilde{X} \neq Y) + 1 - P(\tilde{X} = Y)}{2} = \\
&= \frac{P(\tilde{X} \neq Y) + P(\tilde{X} \neq Y)}{2} = \\
&= P(X \neq Y)
\end{aligned}$$

Por tanto, la probabilidad de que ocurra un cambio en la variable X es igual a la distancia de traza de las dos distribuciones de probabilidad $(\tilde{X}, X)$ y $(\tilde{X}, Y)$.

En mecánica cuántica no será posible utilizar esta definición, debido a que no pueden compararse dos distribuciones para variables que no coexisten en el tiempo, ni es posible la clonación de una variable para poder compararla posteriormente con otra (teorema 3.1). Más adelante, nos basaremos en la idea del entrelazamiento cuántico para construir una distancia dinámica para la información cuántica que dé cuenta de su evolución.

2.3.2. Información cuántica

Una vez introducidas las pautas de la teoría de la información clásica para comparar distribuciones de probabilidad, estamos en disposición de definir los conceptos análogos en la teoría de la información cuántica.

Distancia de traza cuántica

Definición 2.12. *Consideramos dos estados cuánticos determinados por sus correspondientes operadores de densidad ρ y σ. La **distancia de traza** entre ambos estados cuánticos viene dada por:*

$$D(\rho, \sigma) = \frac{1}{2} Tr \{|\rho - \sigma|\}$$

Observación 2.13. El hecho de restar dos operadores de densidad implica que ambos operadores deben encontrarse en la misma base de autoestados $\{|u_i\rangle\}_i$. Recordemos que la definición de operador densidad ρ de un estado $|\psi\rangle$ en una base $\{|u_i\rangle\}_{i\in I}$ es la siguiente:

$$\rho = |\psi\rangle \langle\psi| = \left(\sum_{i\in I} \alpha_i |u_i\rangle\right)\left(\sum_{j\in I} \alpha_j^* \langle u_j|\right) = \sum_{i,j\in I} \alpha_i \alpha_j^* |u_i\rangle \langle u_j|$$

En el caso sencillo de los qubits en estados puros, $I = \{0, 1\}$ y por tanto el operador densidad se reduce a:

$$\rho = |\alpha_0|^2 |u_0\rangle \langle u_0| + \alpha_0 \alpha_1^* |u_0\rangle \langle u_1| + \alpha_1 \alpha_0^* |u_1\rangle \langle u_0| + |\alpha_1|^2 |u_1\rangle \langle u_1|$$

Entonces, como para operar con dos operadores de densidad, ambos deben estar en la misma base (no necesariamente deben diagonalizar los dos operadores en la misma base), esto nos asegura que la distancia de traza es nula si, y solo si, los dos operadores son idénticos.

Esta definición resulta ser una generalización de su análogo clásico, que se corresponde con el caso en que los operadores de densidad conmutan. Para ver esto, debemos conocer la siguiente propiedad de los operadores que conmutan.

Propiedad 2.14 (de los operadores compatibles)**.** Si dos operadores conmutan, entonces existe una base de autovectores del espacio de estados en la que ambos operadores son diagonales.

Por tanto, si consideramos $\{|u_i\rangle\}_i$ la base en la que diagonalizan los dos operadores de densidad ρ y σ, entonces se tiene que, para $b_i, c_i \in \mathbb{R}$:

$$\rho = \sum_i b_i |u_i\rangle \langle u_i|; \qquad \sigma = \sum_i c_i |u_i\rangle \langle u_i|$$

Por lo que:

$$D(\rho, \sigma) = \frac{1}{2} Tr \left\{ \left| \sum_i (b_i - c_i) |u_i\rangle \langle u_i| \right| \right\} = D(b_i, c_i)$$

Vista la distancia de traza, también podemos definir la fidelidad entre estados cuánticos de forma análoga al caso clásico.

Fidelidad cuántica

Definición 2.15. *Consideramos dos estados cuánticos determinados por sus correspondientes operadores de densidad ρ y σ. Definimos la **fidelidad** entre estos dos operadores como:*

$$F(\rho,\sigma) = Tr\left\{\sqrt{\rho^{\frac{1}{2}}\sigma\rho^{\frac{1}{2}}}\right\}$$

Observación 2.16. En la práctica, deberemos diagonalizar el operador ρ antes de aplicarle una raíz cuadrada, y expresar σ en la misma base para realizar el producto, para posteriormente diagonalizar de nuevo el resultado y aplicar la raíz cuadrada previa a la traza.

De la misma forma que antes, podemos subrayar el caso especial en el que ρ y σ son compatibles, por lo que podremos expresar ambos en la base que los diagonaliza:

$$\rho = \sum_i b_i \left|u_i\right\rangle \left\langle u_i\right|; \qquad \sigma = \sum_i c_i \left|u_i\right\rangle \left\langle u_i\right|$$

Y, en consecuencia:

$$F(\rho,\sigma) = Tr\left\{\sqrt{\sum_i b_i c_i \left|u_i\right\rangle \left\langle u_i\right|}\right\} = Tr\left\{\sum_i \sqrt{b_i c_i}\left|u_i\right\rangle \left\langle u_i\right|\right\} = \sum_i \sqrt{b_i c_i} = F(b_i, c_i)$$

Reduciéndose de nuevo al caso clásico de la fidelidad entre dos distribuciones de autovalores.

Otro caso de interés es en el que $\rho = \left|\psi\right\rangle \left\langle\psi\right|$, siendo $\left|\psi\right\rangle$ un estado puro. En este caso, ρ es idempotente (propiedad 1.62), por lo que $\rho^{\frac{1}{2}} = \rho$. De esta manera:

$$\begin{aligned} F(\left|\psi\right\rangle, \sigma) = Tr\left\{\sqrt{(\left|\psi\right\rangle \left\langle\psi\right|)^{\frac{1}{2}}\sigma(\left|\psi\right\rangle \left\langle\psi\right|)^{\frac{1}{2}}}\right\} = Tr\left\{\sqrt{\left|\psi\right\rangle \left\langle\psi\right| \sigma \left|\psi\right\rangle \left\langle\psi\right|}\right\} = \\ = Tr\left\{\sqrt{\langle\psi|\sigma|\psi\rangle \left|\psi\right\rangle \left\langle\psi\right|}\right\} = \sqrt{\langle\psi|\sigma|\psi\rangle} \end{aligned} \tag{57}$$

Este caso es en el que nos centraremos de ahora en adelante. Nótese que, para aliviar notación, hemos escrito el estado como primer argumento de la función, en lugar del operador densidad.

La fidelidad es una operación simétrica. No obstante, como ya puntualizamos en la versión clásica, no es una distancia, debido a que cuando los estados son idénticos, el valor de la fidelidad es 1, tomando valores entre 0 y 1 para estados distintos.

Fidelidad de entrelazamiento

Como adelantábamos en la sección anterior, existe un concepto que se usa para establecer la capacidad de preservación de información de un canal cuántico. Esto es, al atravesar un qubit un canal ruidoso, en qué medida ese canal preserva la información del qubit. Por poner un ejemplo sencillo para ilustrarlo, supongamos que un qubit en un estado puro $\left|\psi\right\rangle$ atraviesa un canal despolarizador. A nivel intuitivo, podemos calcular la fidelidad entre los estados inicial y final. Como $\left|\psi\right\rangle$ es un estado puro, podemos usar la expresión 57:

$$F(\left|\psi\right\rangle, \mathcal{E}(\left|\psi\right\rangle \left\langle\psi\right|)) = \sqrt{\langle\psi|\left(p\frac{\mathbb{I}}{2} + (1-p)\left|\psi\right\rangle \left\langle\psi\right|\right)|\psi\rangle} = \sqrt{1-\frac{p}{2}}$$

Podemos observar que, acorde con nuestra intuición, cuanto más alta sea la probabilidad p de que el qubit se vea afectado por el ruido, más baja es la fidelidad, mientras que con una probabilidad nula, la fidelidad es 1. Desafortunadamente, comparar estados inicial y final no es tan sencillo, este procedimiento no se puede realizar en la práctica. Para empezar, no podemos conocer el estado $\left|\psi\right\rangle$ antes de que el qubit atraviese el canal ruidoso, ya que conocer el estado implicaría medirlo, lo cual colapsaría el estado en $\left|0\right\rangle$ o $\left|1\right\rangle$, destruyendo la superposición de estados.

Para definir correctamente una distancia dinámica, nos centraremos en la siguiente idea: **Un canal que preserva bien la información es un canal que preserva bien el entrelazamiento**. No podemos desarrollar nada a partir de las nociones clásicas de distancia dinámica expuestas en el apartado anterior, debido a que no existe un análogo cuántico para una distribución de probabilidad que existe en dos momentos diferentes. No obstante, como veremos ahora, podemos desarrollar un procedimiento análogo a crear un duplicado del estado original en un segundo qubit y compararlo con el estado final del primer qubit, tras atravesar el canal ruidoso.

Como en mecánica cuántica es imposible duplicar un estado (teorema 3.1), lo que aprovecharemos será el fenómeno del entrelazamiento cuántico. Consideramos para ello un sistema Q, que asumimos que se encuentra entrelazado de alguna manera con el entorno (lo cual no es una suposición disparatada en absoluto). Representaremos ese entrelazamiento cuántico introduciendo un sistema ficticio que denominaremos R, de tal manera que el sistema conjunto RQ se encuentre en un estado puro. Si sometemos al sistema Q a un canal ruidoso descrito por una operación cuántica $\mathcal{E}$. Podemos determinar en qué medida este canal ruidoso preserva el entrelazamiento cuántico mediante la fidelidad de entrelazamiento.

Definición 2.17. *Consideramos un sistema principal Q, entrelazado con un sistema R (que puede ser ficticio), consideramos el sistema RQ en un estado con operador de densidad ρ y sometemos el sistema Q a un canal ruidoso definido por una operación cuántica $\mathcal{E}$. Definimos la* ***fidelidad de entrelazamiento*** *$\mathcal{F}(\rho, \mathcal{E})$ a partir de la fidelidad entre los estados inicial $|RQ\rangle$ y final $\mathcal{E}(|RQ\rangle \langle RQ|)$ del sistema como:*

$$\mathcal{F}(\rho, \mathcal{E}) = F(|RQ\rangle, \mathcal{E}(|RQ\rangle \langle RQ|))^2 = \langle RQ| \left[(\mathbb{I}(R) \otimes \mathcal{E})(|RQ\rangle \langle RQ|)\right] |RQ\rangle$$

Igual que antes, un valor cercano a 1 indica que el entrelazamiento ha sido bien preservado, mientras que valores bajos indican que la mayoría del entrelazamiento se ha perdido. La elección de elevar al cuadrado la fidelidad estática con la que hemos definido la fidelidad de entrelazamiento es arbitraria, pero conveniente para simplificar cálculos.

Una propiedad interesante de la fidelidad de entrelazamiento es la existencia de una expresión sencilla de cálculo exacto:

Proposición 2.18. *En las condiciones de la definición anterior, si $\{E_i\}_i$ son los elementos de operación de la operación cuántica $\mathcal{E}$, entonces la fidelidad de entrelazamiento puede expresarse como:*

$$\mathcal{F}(\rho, \mathcal{E}) = \sum_i |\langle RQ|E_i|RQ\rangle|^2$$

De hecho, si el operador de densidad ρ del estado $|RQ\rangle$ es diagonal,

$$\rho = \sum_j p_j |u_j\rangle \langle u_j|$$

Entonces se tiene que:

$$\langle RQ|E_i|RQ\rangle = \sum_{jk} \sqrt{p_j p_k} \langle u_j|u_k\rangle \langle u_j|E_i|u_k\rangle = \sum_j p_j \langle u_j|E_i|u_j\rangle = Tr\{E_i \rho\}$$

Es decir,

$$\mathcal{F}(\rho, \mathcal{E}) = \sum_i |Tr\{\rho E_i\}|^2$$

Ejemplo 2.19. Para ilustrar la conveniencia de esta expresión, podemos calcular la fidelidad de entrelazamiento del canal de phase flip (2.2.4), descrito por la operación cuántica:

$$\mathcal{E} = p\rho + (1-p) Z\rho Z$$

La fidelidad de entrelazamiento vendría dada por:

$$\mathcal{F}(\rho, \mathcal{E}) = p|Tr\{\rho\}|^2 + (1-p)|Tr\{\rho Z\}|^2 = p + (1-p)Tr\{\rho Z\}^2$$

Aquí podemos observar que cuando p decrece, la fidelidad de entrelazamiento también decrece, como cabría esperar, ya que el efecto del canal ruidoso es menor cuanto menor sea la probabilidad de que el estado se vea afectado.

3. Corrección de errores cuánticos

3.1. Códigos clásicos

En computación clásica, si enviamos un bit a través de un canal ruidoso, hay una probabilidad p de que el bit sufra un bit flip, mientras que la probabilidad de que el bit quede inalterado es $(1-p)$. Este canal se conoce como un canal binario simétrico y la manera más sencilla de proteger un mensaje ante los efectos de este canal es añadiendo redundancia, es decir, podemos enviar tres copias del mismo bit para cada bit que queramos enviar. Supongamos que enviamos el bit 0, codificado como 000. Si el receptor recibe, por ejemplo, 010, suponiendo una probabilidad muy baja de flip, es más probable que el bit original haya sido 0 que 1. Este tipo de decodificación se conoce como *voto mayoritario*, que falla con probabilidad $3p^2 - 2p^3$. Considerando que la probabilidad de error del bit sin codificar es p, esta codificación hace las transmisiones más fiables, siempre que $p < 1/2$.

Este tipo de código se conoce como *código de repetición* y es la manera más sencilla de añadir redundancia a un mensaje, que es en lo que se van a basar las codificaciones cuyo objetivo sea evitar o minimizar los efectos de un canal ruidoso.

3.2. Códigos cuánticos

Los códigos correctores de errores cuánticos van a basarse en principios similares de redundancia. No obstante, dada la distinta naturaleza de los qubits respecto a los bits, es necesario introducir nuevos conceptos para desarrollar códigos correctores de errores cuánticos. Tenemos que hacer frente, concretamente, a tres problemas: la imposibilidad de clonar un estado cuántico, la naturaleza continua de los errores y el hecho de que medir destruye la información contenida en el estado de superposición.

Teorema 3.1 (no clonación)**.** *No existe un operador unitario capaz de clonar estados cuánticos diferentes no ortogonales entre sí.*

Demostración.
Suponemos que tenemos un sistema A en un estado $|\psi\rangle$ y un sistema B en el que queremos replicar el estado. Podemos asumir que el estado inicial del sistema B es un estado puro $|s\rangle$ Por tanto, el estado inicial del sistema global es:

$$|\psi\rangle \otimes |s\rangle$$

La evolución que impondremos a este sistema para copiar el estado $|\psi\rangle$ en el estado $|s\rangle$ vendrá descrita por un operador unitario U, que idealmente tendrá el siguiente efecto:

$$|\psi\rangle \otimes |s\rangle \xrightarrow{U} U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$

Supongamos que este procedimiento de copia funciona en dos casos distintos, $|\psi\rangle$ y $|\varphi\rangle$:

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$
$$U(|\varphi\rangle \otimes |s\rangle) = |\varphi\rangle \otimes |\varphi\rangle$$

Tomando el producto interno de estas dos ecuaciones, obtenemos:

$$\langle\psi|U^\dagger U|\varphi\rangle \otimes \langle s|U^\dagger U|s\rangle = \langle\psi|\varphi\rangle \otimes \langle\psi|\varphi\rangle$$
$$\langle\psi|\varphi\rangle \otimes \langle s|s\rangle = \langle\psi|\varphi\rangle^2$$
$$\langle\psi|\varphi\rangle = \langle\psi|\varphi\rangle^2$$

Entonces necesariamente $\langle\psi|\varphi\rangle$ es 0 o 1, por lo que o bien los dos estados son iguales o bien son ortogonales. □

Lo que acabamos de ver es que no podemos clonar un estado cuántico desconocido utilizando operadores unitarios de evolución, es decir, que no existe un "clonador universal" de estados. Tampoco podemos seleccionar el operador unitario adecuado dependiendo de cada estado porque recordemos que no podemos conocer de antemano el estado que queremos clonar, ya que eso implicaría medirlo y, por tanto, destruir la información. Un dispositivo de clonación de estados cuánticos mediante un operador unitario de evolución solo podría clonar diferentes estados si son ortogonales entre sí. Por ejemplo, no podría clonar los dos estados $|\psi\rangle = |0\rangle$ y $|\varphi\rangle = (|0\rangle+|1\rangle)/\sqrt{2}$, ya que no son ortogonales.

No obstante, la aplicación de operadores no unitarios o la clonación de estados no puros es un campo que ha sido objeto de extensa investigación (ver, por ejemplo, [11]), aunque la conclusión es que incluso para operadores no unitarios, la clonación de estados no ortogonales sigue siendo imposible a menos que se admita una cierta pérdida de fidelidad en los estados clonados.

A continuación, veremos ejemplos de códigos correctores de errores cuánticos sencillos que nos servirán de introducción a la formalización de la teoría de errores cuánticos.

3.3. Código de tres qubits para bit flip

El mecanismo de redundancia que nos permitirá "hacer varias copias de un qubit" es el entrelazamiento cuántico. Supongamos que tenemos un qubit en un estado:

$$a\,|0\rangle + b\,|1\rangle$$

Lo podemos codificar con tres qubits como:

$$a\,|000\rangle + b\,|111\rangle$$

Observación 3.2. En este punto, la pregunta lógica es: ¿Acaso no es esta codificación una clonación de estados? No debería serlo, pues ya hemos visto en el apartado anterior que no puede hacerse. Entonces, ¿Qué es esto de, a partir de un qubit, establecer otros qubits diferentes en el mismo estado?

La clonación de estados consiste en, a partir de un qubit (1) en un estado $|\psi(1)\rangle = a\,|0\rangle + b\,|1\rangle$, establecer el estado de otro qubit (2) en $|\psi(2)\rangle = a\,|0\rangle + b\,|1\rangle$. En cambio, el mecanismo que estamos utilizando para codificar estados no es la clonación, sino el entrelazamiento cuántico, que consiste en, a partir de un qubit (1) en un estado $|\psi(1)\rangle = a\,|0\rangle + b\,|1\rangle$ y otro qubit (2) en un estado arbitrario, establecer el estado del sistema conjunto en:

$$|\psi(1,2)\rangle = a\,|00\rangle + b\,|11\rangle$$

En una clonación de estados, obtendríamos dos qubits independientes en el mismo estado $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$, de manera que podríamos realizar mediciones independientes sobre ambos qubits, obteniendo, por ejemplo, en la medición del primer qubit el estado $|0\rangle$ y en la del segundo qubit el estado $|1\rangle$, por lo que, iterando un método de clonación, podríamos obtener un número arbitrariamente grande de qubits idénticos y realizar un número de medidas tal que nos permitiese inferir las distribuciones de probabilidad y, en consecuencia, los módulos de los coeficientes del estado. En cambio, en el entrelazamiento cuántico, la medida de uno de los qubits colapsa automáticamente el estado del resto. Si un sistema de dos qubits está en un estado $|\psi\rangle = a\,|00\rangle + b\,|11\rangle$ y la medida del primer qubit da $|0\rangle$, entonces por el postulado 5 (expresión 43) el estado del sistema inmediatamente después de la medida es $|\psi'\rangle = |00\rangle$, por lo que el estado del segundo qubit queda completamente definido y lo conocemos sin necesidad de medirlo. Es decir, medir un qubit de un sistema entrelazado colapsa el estado de todos los qubits entrelazados, al contrario de lo que sucedería con la clonación de estados.

Consideramos entonces un canal de bit flip, que deja un qubit inalterado con probabilidad (1-p) y permuta los estados $|0\rangle$ y $|1\rangle$ con probabilidad p. Esto es, con una probabilidad p aplica la matriz de Pauli X al estado del qubit. Si sometemos los 3 qubits entrelazados al canal de bit flip

por separado, el canal ruidoso alterará el estado del qubit correspondiente con una probabilidad p, es decir, la interacción con el entorno romperá el entrelazamiento, alterando el estado de uno de los qubits. Podemos utilizar un sencillo procedimiento de corrección de errores en dos etapas para recuperar el estado cuántico original:

- Detección de errores o diagnóstico del síndrome

  Esta etapa consiste en realizar medidas conocidas como "diagnósticos de síndrome" sobre el estado entrelazado. Los resultados de estas medidas se conocen como "síndromes de error". En este caso de tres qubits entrelazados, podemos medir cuatro observables diferentes:

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$
$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$
$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$
$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

  Estos cuatro proyectores son operadores observables y sabemos (ejemplo 1.40) que sus autovalores son 0 o 1. Estos observables tienen la propiedad de que no colapsan el estado cuántico, ya que únicamente nos proporcionan información sobre en qué qubit en el que ha ocurrido un bit flip. Para ilustrarlo, consideramos un caso concreto, sabiendo que el razonamiento para el resto de casos es análogo.

  Supongamos que el estado del sistema tras la acción del canal ruidoso es:

$$|\psi\rangle = a\,|010\rangle + b\,|101\rangle$$

  Aplicamos sobre este sistema los observables descritos y, en virtud del cuarto postulado (expresión 39), la probabilidad de obtener el autovalor $a_0 = 1$ del observable P_0 es:

$$\mathcal{P}(a_0 = 1) = |(\langle 000|\psi\rangle|^2 + |\langle 111|\psi\rangle|^2 =$$
$$= |a\langle 000|010\rangle + b\langle 000|101\rangle|^2 + |a\langle 111|010\rangle + b\langle 111|101\rangle|^2 = 0$$

  Siendo $|000\rangle$ y $|111\rangle$ los dos autovectores de P_0 asociados al autovalor 1. De la misma manera, la probabilidad de obtener el autovalor $a_i = 1$ de los respectivos observables P_i, con $i = \{1, 2, 3\}$, es:

$$\mathcal{P}(a_1 = 1) = |\langle 100|\psi\rangle|^2 + |\langle 011|\psi\rangle|^2 = 0$$
$$\mathcal{P}(a_2 = 1) = |\langle 010|\psi\rangle|^2 + |\langle 101|\psi\rangle|^2 = |a|^2 + |b|^2 = 1$$
$$\mathcal{P}(a_3 = 1) = |\langle 001|\psi\rangle|^2 + |\langle 110|\psi\rangle|^2 = 0$$

  Como estos observables solo poseen los autovalores 1 y 0, deducimos que las probabilidades de obtener el autovalor 0 son las complementarias. Con esto deducimos que únicamente vamos a obtener el autovalor 1 al medir el observable P_2, obteniendo 0 al medir el resto de observables. Comprobamos ahora el estado en el que se proyecta el sistema tras realizar alguna de las medidas, siguiendo el argumento del quinto postulado (expresión 43). Tomamos para visualizarlo el ejemplo de haber medido el operador P_2 y obtener el autovalor 1:

$$|\psi'\rangle = \frac{Q_{2,1}\,|\psi\rangle}{\sqrt{\langle\psi|Q_{2,1}|\psi\rangle}} = \frac{|010\rangle\langle 010|\psi\rangle + |101\rangle\langle 101|\psi\rangle}{\sqrt{\langle\psi|010|\psi\rangle + \langle\psi|101|\psi\rangle}} =$$
$$= \frac{a\,|010\rangle + b\,|101\rangle}{\sqrt{|a|^2 + |b|^2}} = a\,|010\rangle + b\,|101\rangle = |\psi\rangle$$

  Donde $Q_{2,1}$ es el proyector sobre el subespacio de los autovectores de P_2 asociados al autovalor 1. El procedimiento es análogo para los otros tres observables, y en todos los casos el estado permanece inalterado.

Observación 3.3. Nótese que, en general, las medidas destruyen el estado de superposición. El motivo físico por el que esta medida en concreto no lo hace es porque no estamos obteniendo información alguna sobre los coeficientes a y b, no estamos tratando de conocer el estado. La única información que extraemos es qué qubit ha sufrido un bit flip, independientemente de cuáles fueran los estados inicial y final del qubit correspondiente.

- Recuperación

  Usaremos los valores del síndrome de error calculados en el proceso anterior para recuperar el estado inicial. Dependiendo de cuál de las cuatro medidas nos haya proporcionado el valor 1, realizaremos a propósito una operación de bit flip en el qubit correspondiente, es decir, le aplicaremos el operador X. En resumen, si hemos obtenido en la medida de P_0 un valor de 1, significa que el estado ya es el original y no es necesario realizar ninguna modificación. En cambio, si obtenemos el valor 1 en la medida de P_2, realizaremos una operación de bit flip sobre el segundo qubit, recuperando el estado original.

De la misma manera que para errores clásicos, la probabilidad de que un error no quede corregido mediante este procedimiento es $3p^2 - 2p^3$, por lo que obtenemos, para probabilidades bajas de bit flip en el canal ruidoso, un procedimiento fiable de corrección de este tipo de errores.

Podemos analizar este código corrector empleando el parámetro de fidelidad. Para ello, consideramos que el estado del qubit previo a atravesar el canal de bit flip es un estado puro $|\psi\rangle$ y, tras atravesar el canal, el estado pasa a una mezcla estadística descrita por el operador de densidad:

$$\rho = (1-p)\,|\psi\rangle\langle\psi| + pX\,|\psi\rangle\langle\psi|\,X$$

Por tanto, la fidelidad entre estos dos estados vendrá dada por:

$$F(|\psi\rangle, \rho) = \sqrt{\langle\psi|\rho|\psi\rangle} = \sqrt{(1-p) + p\,\langle\psi|X|\psi\rangle\,\langle\psi|X|\psi\rangle}$$

El segundo término bajo la raíz cuadrada es no negativo, anulándose solo cuando $|\psi\rangle = |0\rangle, |1\rangle$, por lo que el mínimo valor de la fidelidad sin realizar la corrección del error es:

$$F_{min} = \sqrt{1-p}$$

El estado del sistema tras la acción del canal ruidoso y de la corrección mediante el procedimiento descrito antes, viene dado por el operador densidad:

$$\rho' = [(1-p)^3 + 3p(1-p)^2]\,|\psi\rangle\langle\psi| + \dots$$

Donde los puntos suspensivos representan las contribuciones de las posibilidades de que más de un qubit haya sufrido un bit flip. En todo caso son operadores positivos, de manera que:

$$F(|\psi\rangle, \rho') = \sqrt{\langle\psi|\rho|\psi\rangle} \geq \sqrt{(1-p)^3 + 3p(1-p)^2} = \sqrt{1 - 3p^2 + 2p^3}$$

Por lo tanto, la fidelidad del estado cuántico mejora con este código corrector siempre que $p < 1/2$.

Existe otra manera de realizar el diagnóstico de síndrome: en lugar de medir los cuatro proyectores P_i, $i = \{0, 1, 2, 3\}$, podemos medir los dos observables Z_1Z_2 y Z_2Z_3, es decir, el producto de los dos observables Z de los qubits correspondientes. Este observable, en el caso de dos qubits está representado por la matriz:

$$Z_1 \otimes Z_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Y tiene autovalores +1 y -1, con multiplicidad 2 cada uno. Teniendo en cuenta que estamos trabajando con tres qubits, la descomposición espectral de estos operadores será:

$$Z_1Z_2 = (|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes \mathbb{I} - (|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes \mathbb{I}$$
$$Z_2Z_3 = \mathbb{I} \otimes (|00\rangle\langle 00| + |11\rangle\langle 11|) - \mathbb{I} \otimes (|01\rangle\langle 01| + |10\rangle\langle 10|)$$

Si obtenemos el autovalor +1, significa que los dos qubits correspondientes son iguales, mientras que si obtenemos el valor -1, quiere decir que son diferentes. De esta manera, sin conocer cuál es

el estado de los qubits, podemos saber en qué qubit se ha producido el bit flip usando solamente dos observables:

$$Z_1Z_2 = 1 = Z_2Z_3 \Longrightarrow \text{El código no ha sufrido cambios}$$
$$Z_1Z_2 = -1; Z_2Z_3 = 1 \Longrightarrow \text{El qubit 1 ha cambiado}$$
$$Z_1Z_2 = -1 = Z_2Z_3 \Longrightarrow \text{El qubit 2 ha cambiado}$$
$$Z_1Z_2 = 1; Z_2Z_3 = -1 \Longrightarrow \text{El qubit 3 ha cambiado}$$

3.4. Código de tres qubits para phase flip

Un canal de phase flip aplica el operador Z sobre el qubit con probabilidad p, es decir, intercambia las fases relativas de los estados $|0\rangle$ y $|1\rangle$, y deja el qubit inalterado con probabilidad 1-p. En vez de trabajar en la base habitual $\{|0\rangle, |1\rangle\}$, podemos utilizar una base mucho más conveniente para analizar este tipo de errores: $\{|+\rangle, |-\rangle\}$, con:

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

De este modo, la operación de phase flip no es más que un bit flip entre los estados $|+\rangle$ y $|-\rangle$. Consecuentemente, vamos a poder construir un código corrector análogo al código de tres qubits para bit flip, codificando el estado $|0\rangle$ como $|+++\rangle$ y $|1\rangle$ como $|---\rangle$, de manera que realizamos las mismas operaciones que en el caso de bit flip, pero en la base $\{|+\rangle, |-\rangle\}$. El cambio de base se puede implementar físicamente en un sistema, conociéndose el dispositivo que realiza tal operación cuántica como "Puerta de Hadamard", que aplica el operador unitario H sobre el qubit. el operador de Hadamard se representa mediante la siguiente matriz:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{58}$$

Las propiedades de este código corrector son las mismas que su análogo para bit flip, por lo que también mejora la fidelidad del proceso siempre que $p < 1/2$.

Decimos que los canales de bit flip y phase flip son unitariamente equivalentes, ya que existe un operador unitario que relaciona las operaciones cuánticas asociadas, en este caso el operador de Hadamard. De hecho, la manera alternativa de expresar este código ya no es con los operadores Z, sino con los operadores $X = HZH^\dagger = HZH$. En el caso de dos qubits, en la base $\{|+\rangle, |-\rangle\}$, el operador X_1X_2 está representado por la misma matriz que Z_1Z_2 en la base $\{|0\rangle, |1\rangle\}$:

$$X_1 \otimes X_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Teniendo en cuenta que estamos trabajando con tres qubits, la descomposición espectral de estos dos operadores es:

$$X_1X_2 = (|++\rangle\langle++| + |--\rangle\langle--|) \otimes \mathbb{I} - (|+-\rangle\langle+-| + |-+\rangle\langle-+|) \otimes \mathbb{I}$$
$$X_2X_3 = \mathbb{I} \otimes (|++\rangle\langle++| + |--\rangle\langle--|) - \mathbb{I} \otimes (|+-\rangle\langle+-| + |-+\rangle\langle-+|)$$

Por lo que tenemos las implicaciones análogas al caso de bit flip, solo que en la base $\{|+\rangle, |-\rangle\}$:

$$X_1X_2 = 1 = X_2X_3 \Longrightarrow \text{El código no ha sufrido cambios}$$
$$X_1X_2 = -1; X_2X_3 = 1 \Longrightarrow \text{El qubit 1 ha cambiado}$$
$$X_1X_2 = -1 = X_2X_3 \Longrightarrow \text{El qubit 2 ha cambiado}$$
$$X_1X_2 = 1; X_2X_3 = -1 \Longrightarrow \text{El qubit 3 ha cambiado}$$

Por último, para la recuperación del estado original tras la detección del error, debemos transformar de nuevo el estado codificado mediante la puerta de Hadamard a la base original $\{|0\rangle, |1\rangle\}$ y aplicar el operador Z al qubit que haya sido afectado por la operación de phase flip.

3.5. Código de Shor

Por sorprendente que parezca, existe un código corrector capaz de corregir errores arbitrarios producidos sobre un qubit. Se trata del código de Shor, una combinación de los códigos de tres qubits para bit flip y para phase flip: primero codificamos los qubits como en el caso del phase flip ($|0\rangle \to |+++\rangle$, $|1\rangle \to |---\rangle$) y a continuación codificamos los estados resultantes como en el código de bit flip,

$$|+\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$
$$|-\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$$

De manera que obtenemos un código de nueve qubits, dado por:

$$|0_L\rangle = \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}$$
$$|1_L\rangle = \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}$$

Donde $|0_L\rangle$ y $|1_L\rangle$ es lo que conocemos como "0 lógico" y "1 lógico", que son los vectores tales que el estado codificado es:

$$a\,|0_L\rangle + b\,|1_L\rangle$$

Por lo que un estado arbitrario $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ lo codificaremos como:

$$\begin{aligned}|\psi\rangle = a\,|0_L\rangle + b\,|1_L\rangle = \\ = a\frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}} + \\ + b\frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}\end{aligned}$$

Y sobre este código podemos realizar el diagnóstico del síndrome para bit flip, midiendo los observables Z_iZ_{i+1}, con $i = \{1, 2, \ldots, 8\}$, y detectando así qué qubit ha sufrido un bit flip, y recuperar el estado aplicando el operador X sobre el qubit correspondiente. También podemos realizar el diagnóstico del síndrome para phase flip: si alguno de los qubits ha sido afectado por la operación de phase flip, el estado se verá afectado de manera que cambiará la fase relativa entre los estados correspondientes al bloque del qubit afectado. Es decir, si por ejemplo el quinto qubit ha sido afectado por la operación de phase flip, entonces el estado será:

$$\begin{aligned}|\psi\rangle = a\frac{(|000\rangle + |111\rangle)(|000\rangle - |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}} + \\ + b\frac{(|000\rangle - |111\rangle)(|000\rangle + |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}\end{aligned}$$

Entonces podremos aplicar los operadores $X_1X_2X_3X_4X_5X_6$ y $X_4X_5X_6X_7X_8X_9$ para comprobar si alguno de los tres bloques tiene la fase cambiada. Los autovalores de estos dos operadores siguen siendo ± 1 y la descomposición espectral es análoga a la de los anteriores apartados, teniendo en cuenta que esta vez consideramos nueve qubits a la vez. Por tanto, si medimos +1 en ambos observables, significa que el estado no ha sido afectado, mientras que si medimos +1 en el primero y -1 en el segundo significa que el qubit 3 ha sido afectado, siendo el qubit 1 en el caso contrario y el 2 en el caso en que ambas medidas sean -1. Una vez detectado el bloque en el que se encuentra el error, la recuperación del estado original se consigue aplicando el operador $Z_iZ_{i+1}Z_{i+2}$ para $i = \{1, 4, 7\}$, dependiendo de en qué bloque se haya detectado, de manera que la fase del bloque correspondiente se vea modificada.

De hecho, este código también sirve para detectar y corregir errores en el caso de que una combinación de bit flip y phase flip haya afectado a uno de los qubits, es decir, que el operador ZX haya sido aplicado sobre un qubit, puede verse que los procedimientos para corregir el bit flip y el phase flip aplicados por separado corregirán el estado.

Como adelantábamos al principio del apartado, el código de Shor no solo es efectivo contra errores de bit flip y phase flip, sino que puede corregir una gran variedad de errores, desde una rotación minúscula de un qubit respecto del eje Z de la esfera de Bloch hasta un gran error como borrar completamente un qubit y reemplazarlo por otro diferente. Esto es un ejemplo de algo que desarrollaremos más adelante, el hecho de que un conjunto de errores aparentemente continuo puede ser corregido solamente considerando un subconjunto discreto de ellos. Podemos considerar por ahora un ejemplo sencillo para ilustrar la idea:

Ejemplo 3.4. Supongamos que tenemos un qubit codificado con el código de Shor y que el primer qubit es afectado por un ruido arbitrario, descrito por una operación cuántica $\mathcal{E}$ cuyos elementos de operación son $\{E_i\}_i$. Sea $|\psi\rangle$ el estado codificado con el código de Shor antes de que actúe el ruido, el estado tras atravesar el canal ruidoso será:

$$\mathcal{E}(|\psi\rangle\langle\psi|) = \sum_i E_i |\psi\rangle\langle\psi| E_i^\dagger$$

Analicemos un término del sumatorio con i arbitrario. Como el operador E_i actúa solamente sobre el primer qubit, podemos expandirlo como una combinación lineal de los operadores $\mathbb{I}, X_1, Z_1, X_1Z_1$:

$$E_i = e_{i0}\mathbb{I} + e_{i1}X_1 + e_{i2}Z_1 + e_{i3}X_1Z_1$$

Por tanto el estado $E_i|\psi\rangle$ puede ser escrito como superposición de los cuatro estados:

$$E_i|\psi\rangle = a\mathbb{I}|\psi\rangle + bX_1|\psi\rangle + cZ_1|\psi\rangle + dX_1Z_1|\psi\rangle$$

Medir el síndrome de error colapsa esta superposición en uno de los cuatro estados correspondientes $\mathbb{I}|\psi\rangle, X_1|\psi\rangle, Z_1|\psi\rangle, X_1Z_1|\psi\rangle$, estados con los que, al aplicar el operador correspondiente para recuperar el estado original, obtenemos el estado original $|\psi\rangle$. Esto da una somera idea de que aunque el error haya sido arbitrario, dentro de un espectro continuo que es la posible información contenida en un qubit, es posible recuperar el estado original considerando únicamente un subconjunto discreto y finito de errores. Esta idea, que formalizaremos y generalizaremos en el teorema 3.7, es la idea bajo la que subyace la teoría de corrección de errores cuánticos.

Hasta ahora, tan solo hemos visto ejemplos de códigos correctores de errores que solamente actúan en uno de los qubits del código. Cuando los errores actúan en más de un qubit, lo cual se vuelve algo a tener en cuenta cuando codificamos la información utilizando un gran número de qubits, existen varias maneras de abordarlo. En la mayoría de situaciones es razonable asumir que los errores actúan de manera independiente, de manera que, suponiendo que los errores son pequeños, podremos expandir el efecto total del ruido como una suma de términos correspondientes a que el ruido afecte a 0, 1, 2, 3 qubits, etc., pudiendo realizar una corrección de errores a primer orden, segundo orden o superiores, dependiendo de la exactitud que busquemos. Este será el caso en el que nos centraremos.

3.6. Teoría de la corrección de errores

En este apartado desarrollaremos y formalizaremos las ideas introducidas por el código de Shor, construyendo una teoría general de corrección de errores cuánticos que nos permitirá demostrar ciertas propiedades generales y construir códigos más sofisticados.

Notación: Consideramos un estado cuántico $|\psi\rangle$ que codificamos mediante una operación unitaria en un código corrector, que definimos como un subespacio C de un espacio de Hilbert más amplio. Llamaremos P al proyector sobre el subespacio C.

Por ejemplo, en el caso del código de tres qubits para bit flip, $P = |000\rangle\langle 000| + |111\rangle\langle 111|$. Tras la acción del canal ruidoso, no asumiremos que la corrección del error se realiza en dos etapas, como en los procedimientos anteriores, que consistían en la realización el diagnóstico del síndrome, obteniendo el síndrome de error y la recuperación el estado mediante la operación correspondiente. Las asunciones que realizaremos en esta teoría serán: la descripción del ruido mediante una operación cuántica $\mathcal{E}$ y la realización del procedimiento completo de corrección de errores mediante una operación cuántica $\mathcal{R}$ que preserva la traza, que llamaremos *operación de corrección de errores*. De esta manera, para cualquier estado representado por un operador densidad ρ, con soporte en C, se tiene que:

$$(\mathcal{R} \circ \mathcal{E})(\rho) \propto \rho$$

Y si $\mathcal{E}$ es una operación que preserva la traza de ρ, entonces es una igualdad. No obstante, en general es proporcional porque los casos en los que la operación cuántica de ruido no preserva la traza pueden ser interesantes, por ejemplo, cuando el ruido se trata de una medida, con el consecuente colapso del estado.

A continuación vamos a estudiar dos teoremas importantes sobre las condiciones para la existencia de códigos correctores y la discretización de errores, cuyas consecuencias son, incluso, sorprendentes. En particular, veremos que, bajo ciertas condiciones, existen códigos correctores, como el de Shor, capaces de corregir cualquier error, siempre que ocurra sobre un solo qubit de la codificación y se pueda expresar como combinación lineal de ciertos operadores. A priori, esto sería disparatado, ya que dicho conjunto de errores que pueden ocurrir sobre un qubit no es finito ni discreto (podemos considerar, por ejemplo, el conjunto continuo de errores en los que el qubit sufre una rotación alrededor del eje Z de la esfera de Bloch, de ángulo $\theta \in (0, 2\pi)$).

Lema 3.5 (Descomposición polar de un operador)**.** *Sea A un operador lineal en un espacio vectorial, entonces existe un operador unitario U y dos operadores positivos J y K tales que:*

$$A = UJ = KU$$

Donde J y K son únicos y satisfacen las expresiones:

$$J = \sqrt{A^\dagger A}$$
$$K = \sqrt{AA^\dagger}$$

Además, si A es invertible, entonces U también es único.

Demostración.

Como $J = \sqrt{A^\dagger A}$ es un operador positivo, puede descomponerse espectralmente como:

$$\sum_i \lambda_i |v_i\rangle\langle v_i|$$

Con $\lambda_i \geq 0$ para todo i, $\{|v_i\rangle\}_i$ una base de V. Definimos $|\psi_i\rangle = A|v_i\rangle$, con lo que tenemos que $\langle\psi_i|\psi_i\rangle = \lambda_i^2$. Consideramos solamente aquellos i para los que $\lambda_i \neq 0$ y definimos para esos coeficientes no nulos:

$$|e_i\rangle = \frac{|\psi_i\rangle}{\lambda_i}$$

Con esto, los vectores $|e_i\rangle$ están normalizados. Además, es fácil ver que también son ortogonales entre sí, ya que para todo $i \neq j$ se tiene que

$$\langle e_i|e_j\rangle = \frac{\langle v_i|A^\dagger A|v_j\rangle}{\lambda_i\lambda_j} = \frac{\langle u_i|J^2|u_j\rangle}{\lambda_i\lambda_j} = 0$$

Ahora podemos utilizar el procedimiento de Gram-Schmidt para extender el conjunto ortonormal $\{|e_i\rangle\}_i$ con los índices que proporcionan coeficientes no nulos en una base ortonormal, que también denotaremos por simplicidad $\{|e_i\rangle\}_i$.

Definimos un operador unitario:

$$U = \sum_i |e_i\rangle \langle v_i|$$

Si $\lambda_i \neq 0$ tenemos que $UJ|v_i\rangle = \lambda_i |e_i\rangle = |\psi_i\rangle = A|v_i\rangle$, mientras que si $\lambda_i = 0$ tenemos que $UJ|v_i\rangle = 0 = |\psi_i\rangle$. Por tanto, $A = UJ$.

Además, J es único, ya que multiplicar $A = UJ$ por la izquierda por la ecuación adjunta $A^\dagger = JU^\dagger$ da $J^2 = A^\dagger A$, por lo que deducimos que $J = \sqrt{A^\dagger A}$. También tenemos que si A es invertible, entonces J también lo es, por lo que U estaría en este caso unívocamente determinado por $U = AJ^{-1}$.

La prueba de la descomposición polar por la derecha con K se deduce de lo anterior, ya que $A = UJ = UJU^\dagger U = KU$, donde $K = UJU^\dagger$ es un operador positivo, y como $AA^\dagger = KUUU^\dagger K = K^2$, entonces $K = \sqrt{AA^\dagger}$ □

A las expresiones $A = UJ$ y $A = KU$ las llamaremos descomposiciones polares (por la izquierda y por la derecha, respectivamente) de A.

Teorema 3.6. *Sean C un código cuántico, P el proyector sobre C, consideramos $\mathcal{E}$ una operación cuántica con elementos de operación $\{E_i\}_i$. Una condición necesaria y suficiente para la existencia de una operación correctora $\mathcal{R}$ de $\mathcal{E}$ en C es:*

$$PE_i^\dagger E_j P = \alpha_{ij} P \tag{59}$$

Para alguna matriz hermítica α.

Demostración.
Comenzamos probando que si se cumple 59 para alguna matriz hermítica α, entonces existe la operación $\mathcal{R}$.

Vamos a construir una operación de corrección de errores en dos etapas, por lo que esta prueba también nos muestra que la corrección de errores puede realizarse siempre con con este tipo de procedimiento en dos fases, detección del error y recuperación del estado. Supongamos que $\{E_i\}_i$ son elementos de operación que satisfacen la condición 59. Como α es hermítica, podemos diagonalizarla como

$$d = u^\dagger \alpha u \tag{60}$$

Donde u es una matriz unitaria y d es una matriz diagonal. Definimos los elementos de operación:

$$F_k = \sum_i u_{ik} E_i$$

En virtud del teorema 2.6, podemos observar que los elementos de operación $\{F_k\}_k$ son también elementos de operación de $\mathcal{E}$. Por tanto tenemos que, sustituyendo en la expresión 59:

$$PF_k^\dagger F_l P = \sum_{ij} u_{ki}^\dagger u_{jl} P E_i^\dagger E_j P = \sum_{ij} u_{ki}^\dagger \alpha_{ij} u_{jl} P = d_{kl} P \tag{61}$$

Donde hemos usado la expresión 60. Vamos a usar esta expresión que acabamos de calcular y la descomposición polar descrita en el lema anterior para definir el diagnóstico del síndrome. De la descomposición polar podemos ver que:

$$F_k P = U_k \sqrt{P F_K^\dagger F_k P} = \sqrt{d_k k} U_k P$$

Para algún operador unitario U_k.

El efecto de F_k, por tanto, es el de rotar el subespacio del código C en el subespacio definido por el proyector $P_k = U_k P U_k^\dagger = F_k P U_k^\dagger / \sqrt{d_{kk}}$. La ecuación 61 implica que estos subespacios son ortogonales, ya que si $k \neq l$:

$$P_l P_k = P_l^\dagger P_k = \frac{U_l P F_l^\dagger F_k P U_k^\dagger}{\sqrt{d_{ll} d_{kk}}} = 0$$

El diagnóstico del síndrome es una medida definida por los proyectores P_k, quizá completados por otros proyectores adicionales para satisfacer $\sum_k P_k = \mathbb{I}$. Por otro lado, la recuperación se efectúa con los operadores $U_k^\dagger$. La combinación de diagnóstico y recuperación corresponde a la operación cuántica:

$$\mathcal{R}(\mathcal{E}(\rho)) = \sum_k U_k^\dagger P_k \mathcal{E}(\rho) P_k U_k$$

Para los estados ρ en el código, siguiendo las definiciones podemos deducir que:

$$U_k^\dagger P_k F_l \sqrt{\rho} = U_k^\dagger P_k^\dagger F_l P \sqrt{\rho} = \frac{U_k^\dagger U_k P F_k^\dagger F_l P \sqrt{\rho}}{\sqrt{d_{kk}}} = \delta_{kl}\sqrt{d_{kk}} P\sqrt{\rho} = \delta_{kl}\sqrt{d_{kk}}\sqrt{\rho}$$

Y por lo tanto:

$$\mathcal{R}(\mathcal{E}(\rho)) = \sum_{kl} U_k^\dagger P_k F_l \rho F_l^\dagger P_k U_k = \sum_{kl} \delta_{kl} d_{kk} \rho \propto \rho$$

Para probar el recíproco, supongamos que $\{E_i\}_i$ es un conjunto de elementos de operación corregible por una operación correctora de errores $\mathcal{R}$ con elementos de operación $\{R_j\}_j$. Definimos una operación cuántica $\mathcal{E}_C$ como:

$$\mathcal{E}_C(\rho) = \mathcal{E}(P\rho P)$$

Como $P\rho P$ está en el espacio del código para cualquier ρ, se tiene que:

$$\mathcal{R}(\mathcal{E}_C(\rho)) \propto P\rho P$$

Para cualquier operador de densidad ρ. Además, ambos lados han de ser lineales, por lo que el factor de proporcionalidad ha de ser una constante que podemos llamar $c \in \mathbb{R}$. Reescribiendo la ecuación en términos de elementos de operación obtenemos, para ρ arbitrario:

$$\sum_{ij} R_j E_i P \rho P E_i^\dagger R_j^\dagger = cP\rho P$$

Podemos deducir que las operaciones cuánticas con elementos de operación $\{R_j E_i\}$ son idénticas a las operaciones cuánticas con $\sqrt{c}P$ como único elemento de operación. El teorema 2.6 nos asegura qu existen $c_{ki} \in \mathbb{C}$ tales que:

$$R_k E_i P = c_{ki} P$$

El adjunto de esta ecuación es $PE_i^\dagger R_k^\dagger = c_{ki}^* P$, y por tanto tenemos que:

$$PE_i^\dagger R_k^\dagger R_k E_j P = c_{ki}^* c_{kj} P$$

Y como $\mathcal{R}$ es una operación que conserva la traza, es decir, $\sum_k R_k^\dagger R_k = \mathbb{I}$, sumando la ecuación anterior en k obtenemos:

$$PE_i^\dagger E_j P = \alpha_{ij} P$$

Donde $\alpha_{ij} = \sum_k c_{ki}^* c_{kj}$ es una matriz hermítica compleja. □

Teorema 3.7 (Discretización de errores)**.** *Sean C un código cuántico y $\mathcal{R}$ la operación correctora construida en la demostración del teorema 3.6 para corregir un proceso de ruido descrito por una operación $\mathcal{E}$ con elementos de operación $\{E_i\}_i$, suponemos que $\mathcal{F}$ es una operación cuántica con elementos de operación $\{F_i\}_i$, que son combinaciones lineales de los E_i, es decir, $F_j = \sum_i m_{ij} E_i$ para alguna matriz compleja m. Entonces la operación $\mathcal{R}$ también corrige los efectos de $\mathcal{F}$ en C.*

Demostración.
Según el teorema 59, los elementos de operación $\{E_i\}$ deben satisfacer las condiciones:

$$PE_i E_j^\dagger P = \alpha_{ij} P$$

Al igual que en la demostración anterior, podemos asumir sin pérdida de generalidad que los elementos de operación para $\mathcal{E}$ han sido elegidos de manera que $\alpha_{ij} = d_{ij}$ es diagonal y real. La operación $\mathcal{R}$ tiene como elementos de operación $\{U_k^\dagger P_k\}$, y por la ecuación 3.6, U_k y P_k se eligen tal que para cualquier ρ en el espacio del código:

$$U_k^\dagger P_k E_i \sqrt{\rho} = \delta_{ki}\sqrt{d_k k}\sqrt{\rho}$$

Sustituyendo $F_j = \sum_i m_{ij} E_i$ obtenemos:

$$U_k^\dagger P_k F_j \sqrt{\rho} = \sum_i m_{ij}\delta ki\sqrt{d_{kk}}\sqrt{\rho} = m_{ij}\sqrt{d_{kk}}\sqrt{\rho}$$

Y, por tanto:

$$\mathcal{R}(\mathcal{F}(\rho)) = \sum_{kj} U_k^\dagger P_k F_j \rho F_j^\dagger P_k U_k = \sum_{kj} |m_{jk}|^2 d_{kk}\rho \propto \rho$$

□

Estos dos teoremas implican que cualquier proceso ruidoso $\mathcal{E}$ cuyos elementos de operación estén construidos mediante combinaciones lineales de sus elementos de operación pueden ser corregidos por la misma operación $\mathcal{R}$. Podemos ilustrar las consecuencias de estos teoremas con un ejemplo en el que analizamos el código de Shor.

Ejemplo 3.8. Sea $\mathcal{E}$ una operación cuántica arbitraria que actúa sobre un solo qubit y cuyos elementos de operación pueden ser descritos como combinaciones lineales de operadores de Pauli:

$$\sigma_0 = \mathbb{I} \quad \sigma_1 = X \quad \sigma_2 = Y \quad \sigma_3 = Z$$

Para comprobar que el código de Shor es capaz de corregir un error arbitrario siempre que actúe sobre un solo qubit y sea combinación lineal de los operadores de Pauli, tan solo hay que verificar que se satisfacen las ecuaciones:

$$P\sigma_i\sigma_j P = \alpha_{ij} P$$

Donde α es una matriz hermítica compleja y $\{\sigma_i\}_{i=0}^3$ son los operadores de Pauli actuando sobre un qubit. En este caso, el proyector toma la forma:

$$P = |0_L\rangle\langle 0_L| + |1_L\rangle\langle 1_L|$$

De manera que la verificación de estas ecuaciones es sencilla. Podemos ejemplificarlo para el caso en que el ruido actúa en el primer qubit:

$$\begin{aligned}
&P\mathbb{I}X_1P = P\mathbb{I}Y_1P = P\mathbb{I}Z_1P = 0\\
&P\mathbb{I}\,\mathbb{I}P = PX_1X_1P = PY_1Y_1P = PZ_1Z_1P = P\\
&PX_1Y_1P = PiZ_1P = 0\\
&PX_1Z_1P = PY_1Z_1P = 0
\end{aligned}$$

La comprobación puede realizarse simplemente aplicando las operaciones cuánticas al proyector, por ejemplo, de la derecha y hacer el producto de los dos proyectores teniendo en cuenta la ortonormalidad de los estados.

Observación 3.9. En un canal despolarizador, la operación cuántica es:

$$\mathcal{E}(\rho) = (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z)$$

Es decir, es una combinación lineal de las cuatro matrices de Pauli. Esto implica que cualquier código corrector capaz de corregir el error de depolarización en un qubit, puede corregir cualquier error que sea también combinación de los operadores de Pauli sobre un qubit.

3.7. Codificaciones clásicas lineales

En esta sección, centrada de nuevo en la información clásica, revisaremos los conceptos utilizados en las codificaciones clásicas lineales, una alternativa a los códigos correctores clásicos que veníamos desarrollando, fundamentales para el desarrollo de los códigos cuánticos.

Una codificación lineal C de tipo [n,k] que codifica k bits de información en un código de n bits se expresa por una matriz generatriz G de n filas y k columnas cuyos elementos son 0 y 1, y todas las operaciones entre estas matrices se realizan en módulo 2. Representamos un mensaje de k bits por un vector columna x, de manera que se codifica como el producto Gx.

Ejemplo 3.10. Un código que codifica dos bits usando una repetición triple de cada uno es de tipo [6,2] y viene dado por la matriz generatriz:

$$G = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}$$

De esta manera, para dos bits dados por $x = \binom{a}{b}$:

$$Gx = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ a \\ a \\ b \\ b \\ b \end{pmatrix}$$

Para $a, b = \{0, 1\}$.

Ahora, para ver cómo se realiza la corrección de errores en el contexto de estas codificaciones, debemos introducir una formulación de las codificaciones equivalente a la anterior, con *matrices de comprobación de paridad*, en lugar de con matrices generatrices. En esta definición, una codificación [n,k] viene dada por todos los vectores de n bits x formados por ceros y unos tales que:

$$Hx = 0$$

Donde H es una matriz con n-k filas y n columnas, conocida como *matriz de comprobación de paridad* y sus elementos son también 0 y 1. A partir de una matriz generatriz G se puede obtener la matriz correspondiente de comprobación de paridad H seleccionando, de la matriz G, n-k vectores linealmente independientes que sean ortogonales (producto interior nulo en módulo 2) a las columnas de G, y establecemos dichos vectores como las filas de H. Para obtener la matriz G a partir de H, se escogen k vectores linealmente independientes tales que generen el núcleo de la matriz H (vista como aplicación) y los establecemos como columnas de la matriz G.

Ejemplo 3.11. Consideramos la matriz generatriz de codificación de repetición triple para un solo bit, de tipo [3,1]:

$$G = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

Para obtener la matriz H, escogemos n-k=2 vectores linealmente independientes ortogonales a las columnas de G, en este caso solamente una. Por ejemplo, (1,1,0) y (0,1,1). Entonces:

$$H = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

Y para el proceso contrario, escogemos k vectores linealmente independientes del núcleo de H, en este caso solamente uno. Como $Hx = 0$ solamente si $x = (0,0,0)$ o $x = (1,1,1)$, entonces escogemos el vector (1,1,1) que es el que genera el núcleo, de manera que poniéndolo como columna recuperamos la matriz generatriz G.

Para ver la corrección de errores en este contexto, supongamos que codificamos un mensaje x como $y = Gx$. Representaremos un error mediante un código e de la misma dimensión que y, formado también por ceros y unos, tal que el código corrompido por el error es $y' = y + e$ (recuérdese que las operaciones se realizan módulo 2). Como la matriz de comprobación de paridad se define por $Hy = 0$, obtenemos que $Hy' = He$. Llamaremos a Hy' *síndrome de error* y funcionará de manera similar al definido en los capítulos anteriores de códigos correctores de errores cuánticos. Si no actúa ningún error sobre el código, entonces $Hy = Hy' = 0$. En cambio, si ocurre un error en el bit j del código y, vendrá representado por un vector e con un 1 en la posición j y ceros en el resto, concepto fácilmente generalizable a la acción del error sobre varios bits. En este caso, $Hy \neq Hy'$ y, en función del valor del síndrome de error Hy' se actuará para corregir el error.

Para corregir estos errores, utilizaremos los *códigos de Hamming*, para los que necesitamos introducir algunos conceptos.

Definición 3.12. *Sean x e y dos vectores de la misma dimensión cuyas entradas son ceros y unos, la* ***distancia de Hamming*** *$d(x,y)$ entre ambos se define como el número de posiciones en las que las entradas de x e y no coinciden.*

Definición 3.13. *Sea x un vector cuyas entradas son ceros y unos, el* ***peso de Hamming*** *$wt(x)$ se define como la distancia de Hamming entre x y el vector nulo, es decir, el número de posiciones en las que las entradas de x son unos.*

Propiedad 3.14. A partir de estas dos definiciones, es fácil comprobar que

$$d(x,y) = wt(x+y)$$

Con esto, supongamos que codificamos un mensaje x como $y = Gx$ y este código es corrompido por un error, produciendo $y' = y + e$. Considerando que la probabilidad de este bit flip es menor que 1/2, la codificación original más probable a partir de la corrupta es aquella que minimice el número de bit flips necesarios para pasar de y a y', es decir, aquella que minimice la distancia de Hamming $d(y,y') = wt(e)$. La corrección consistiría sencillamente en reemplazar y' por dicho y que minimiza la distancia, aunque en la práctica esto es bastante ineficiente, dado que determinar esa distancia mínima requiere considerar todas las posibles codificaciones y.

Las propiedades globales del código pueden entenderse también usando la distancia de Hamming, como ilustran las siguientes definiciones.

Definición 3.15. *Sea C una codificación lineal, la* ***distancia de Hamming del código*** *C es la mínima distancia entre dos mensajes codificados con C.*

$$d(C) = \min_{x,y \in C, x \neq y} d(x,y)$$

Y como $d(x,y) = wt(x+y)$, entonces:

$$d(C) = \min_{x \in C, x \neq 0} wt(x)$$

Estableciendo $d = d(C)$, diremos que C es una codificación de tipo $[n, k, d]$. Un código de distancia $d \geq 2t+1$, con $t \in \mathbb{N}$, incluyendo $t = 0$, será capaz de corregir errores en hasta t bits, decodificando el mensaje de manera que $d(y', y) \leq t$.

Para concluir este apartado de códigos clásicos, exponemos una construcción de codificaciones conocida como *construcción dual*: si consideramos una codificación C de tipo $[n, k]$ con matriz generatriz G y matriz de comprobación de paridad H, podemos definir otra codificación, que denotaremos por $C^{\perp}$ y llamaremos *dual* de C, que será la codificación con matriz generatriz H^T y matriz de comprobación de paridad G^T. Los mensajes de la codificación dual de C serán ortogonales a los de C, y diremos que una codificación es *autodual* si es la misma que su dual. Estos conceptos son clave para construir la clase de códigos correctores con la que finalizaremos esta memoria: los códigos CSS.

3.8. Códigos CSS

Los códigos correctores de errores de Calderbank-Shor-Steane, más conocidos como códigos CSS, son una subclase de códigos correctores cuánticos que pertenecen la clase de códigos estabilizadores.

Supongamos que C_1 y C_2 son, respectivamente, $[n, k_1]$ y $[n, k_2]$ codificaciones clásicas tales que $C_2 \subset C_1$ (es decir, que C_1 es capaz de generar todos los códigos y que genera C_2) y tales que C_1 y $C_2^{\perp}$ corrigen t errores. Vamos a definir un código cuántico de tipo $[n, k_1 - k_2]$, $CSS(C_1, C_2)$ capaz de corregir errores en t qubits, llamado *código CSS de* C_1 *sobre* C_2.

Supongamos que x es una codificación de C_1. Definimos el estado cuántico $|x + C_2\rangle$ como:

$$|x + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle \tag{62}$$

Realizando la suma en módulo 2. El código cuántico $CSS(C_1, C_2)$ forma un espacio vectorial con los vectores $|x + C_2\rangle$. Ahora, podemos explotar las propiedades clásicas lineales de C_1 y $C_2^{\perp}$ para detectar y corregir errores cuánticos. Veámoslo para el caso de bit flip y phase flip.

Supongamos que los errores de bit flip y phase flip están descritos por vectores de n bits e_1, e_2, respectivamente, con unos en las posiciones donde ocurre el error, y ceros en el resto. Si $|x + C_2\rangle$ es el estado original, entonces el estado corrupto viene descrito por:

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)e_2} |x + y + e_1\rangle \tag{63}$$

Para detectar dónde han ocurrido los bit flips, guardaremos en unos qubits auxiliares el síndrome de error del código C_1. Estos qubits auxiliares se encontrarán en un estado inicial preparado $|0\rangle$. Podemos, para grabar los efectos del bit flip en unos qubits auxiliares, aplicar la matriz de comprobación de paridad H_1 del código C_1, de manera que pasamos del estado $|0\rangle$ al estado $H_1 |x + y + e_1\rangle = |H_1 e_1\rangle$, ya que como $(x + y) \in C_1$, la aplicación de la matriz H_1 anula este vector. Por tanto, esta operación produce el estado:

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)e_2} |x + y + e_1\rangle |H_1 e_1\rangle$$

Donde simplemente hemos añadido el qubit auxiliar. Al medir el qubit auxiliar, obteniendo el resultado $H_1 e_1$, obtenemos de nuevo el estado de la expresión 63. Conociendo el síndrome de error $H_1 e_1$ podemos inferir el error e_1, lo que completa la detección. Para la recuperación del estado, simplemente debemos invertir los qubits en las posiciones adecuadas, dadas por el síndrome de error, obteniendo el estado:

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)e_2} |x + y\rangle$$

Para detectar los errores de phase flip, aplicamos puertas de Hadamard a cada qubit (recuérdese la definición de puerta de Hadamard, 58), obteniendo el estado:

$$\frac{1}{\sqrt{|C_2|2^n}} \sum_z \sum_{y \in C_2} (-1)^{(x+y)(e_2+z)} |z\rangle$$

Donde la suma en z se hace sobre todos los posibles valores del vector z, de n bits. Estableciendo $z' = z + e_2$, podemos escribir:

$$\frac{1}{\sqrt{|C_2|2^n}} \sum_{z'} \sum_{y \in C_2} (-1)^{(x+y)(z')} |z' + e_2\rangle$$

Antes de continuar debemos establecer un resultado ([1]):

Proposición 3.16. *Sea C una codificación lineal, si $x \in C^\perp$, entonces se tiene que:*

$$\sum_{y \in C} (-1)^{xy} = |C|$$

Mientras que si $x \notin C^\perp$, entonces:

$$\sum_{y \in C} (-1)^{xy} = 0$$

Por tanto, suponiendo que $z' \in C_2^\perp$, entonces $\sum_{y \in C_2} (-1)^{yz'} = |C_2|$, mientras que si $z' \notin C_2^\perp$, entonces $\sum_{y \in C_2} (-1)^{yz'} = 0$. con esto, podemos reescribir el estado como:

$$\frac{1}{\sqrt{\frac{2^n}{|C_2|}}} \sum_{z' \in C^\perp} (-1)^{(xz')} |z' + e_2\rangle$$

Este estado tiene la misma forma que el del error de bit flip para el vector e_2, por lo que al igual que en el caso de bit flip, introduciremos un sistema auxiliar y aplicaremos la matriz de comprobación de paridad H_2 para $C_2^\perp$ para obtener el síndrome de error $H_2 e_2$ y corregir el error, obteniendo:

$$\frac{1}{\sqrt{\frac{2^n}{|C_2|}}} \sum_{z' \in C^\perp} (-1)^{(xz')} |z'\rangle$$

Por último, la corrección del error se completa aplicando de nuevo una puerta de Hadamard a cada qubit, por lo que nos devuelve el estado original de la expresión 62.

Ejemplo 3.17 (Código de Steane)**.** Podemos construir un código CSS a partir de la matriz de comprobación de paridad del código de Hamming [7,4,3], que es:

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Denotamos a este código por C y definimos $C_1 = C$, $C_2 = C^\perp$. Para construir un código CSS a partir de estos dos, primero debemos verificar que $C_2 \subset C_1$. Por definición, la matriz de comprobación de paridad de C_2 es la matriz generatriz traspuesta de C_1, que se calcula como ilustramos en el ejemplo 3.11:

$$H_{C_2} = G_{C_1}^T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Podemos ver que el espacio generado por las filas de H_{C_2} contiene el espacio generado por las filas de H_{C_1} (la primera fila de H_{C_1} es la cuarta de H_{C_2}, la segunda fila de H_{C_1} puede escribirse como suma de la segunda y la tercera de H_{C_2} y la tercera fila de H_{C_1} puede expresarse como la suma de la primera y la tercera de H_{C_2}) y como los códigos correspondientes son, respectivamente, los núcleos de H_{C_2} y H_{C_1}, concluimos que $C_2 \subset C_1$. De hecho, $C_2^{\perp} = (C^{\perp})^{\perp} = C$, por lo que tanto C_1 como $C_2^{\perp}$ son códigos de distancia 3 que pueden corregir errores en un bit. Como C_1 es un código de tipo $[7, 4]$ y C_2 es de tipo $[7, 3]$, se tiene que el código $CSS(C_1, C_2)$ es un código cuántico de tipo $[7, 1]$ que puede corregir errores en un qubit. Este código se conoce como el código de Steane.

3.9. Códigos asistidos por entrelazamiento

Como apunte final en esta memoria, vamos a arrojar un poco de luz sobre la línea actual de desarrollo de los códigos correctores de errores cuánticos, una de cuyas ramas está enfocada al desarrollo de códigos asistidos por entrelazamiento cuántico (concepto desarrollado en la observación 3.2).

El entrelazamiento juega un papel central en el procesamiento de información cuántica. Permite la teleportación de estados cuánticos sin enviar físicamente sistemas cuánticos, es decir, produce una teleportación de la información contenida, duplica la capacidad de los canales cuánticos para enviar información clásica [12] y se sabe que el futuro de la potencia de la computación cuántica reside en este concepto [13][14].

En los códigos correctores cuánticos estándar, como hemos visto en los apartados anteriores, el proceso de codificación consta de dos pasos, primero se añade al sistema de k qubits que queremos codificar un número $n-k$ de qubits auxiliares en un estado concreto, habitualmente $|0\rangle$, y posteriormente aplicamos la codificación, que es una operación unitaria U.

$$|\psi\rangle \to |\psi\rangle \otimes |0\rangle^{\otimes n-k} \to |\Psi_L\rangle = U\,|\psi\rangle \otimes |0\rangle^{\otimes n-k} \tag{64}$$

Donde $|\Psi_L\rangle$ es el estado lógico codificado.

En los códigos cuánticos asistidos por entrelazamiento (*EAQECC*, por sus siglas en inglés), en cambio, además de qubits auxiliares incorporamos c qubits extra denominados *ebits*, de la siguiente forma:

$$|\psi\rangle \to |\psi\rangle \otimes |0\rangle^{\otimes n-k-c} \otimes |\Phi_+\rangle_{AB}^{\otimes c} \to (U \otimes \hat{I}_B)\,|\psi\rangle \otimes |0\rangle^{\otimes n-k-c} \otimes |\Phi_+\rangle_{AB}^{\otimes c} \tag{65}$$

Donde los estados $|\Phi_+\rangle_{AB}$ son parejas de ebits entrelazados compartidas entre el emisor y el receptor de la información, el operador U actúa únicamente sobre la información del emisor y escribimos $(U \otimes \hat{I}_B)$ para indicar que la codificación actúa sobre el receptor como la identidad. El subíndice A se refiere al emisor (comúnmente conocido como *Alice*) y B al receptor (denotado por *Bob*). Alice y Bob deben tener c ebits compartidos previamente entrelazados, y cuando Alice realiza la codificación envía a través del canal correspondiente los n qubits, de modo que el procedimiento consume los c ebits, aunque los de Bob no atraviesan el canal, así que asumimos que no sufren ningún tipo de error.

Para ver las ventajas de los EAQECC, podemos comparar este sistema con los *códigos superdensos*. En este tipo de códigos, usando un ebit podemos enviar dos bits clásicos de información mediante un solo qubit. Cada qubit auxiliar en un código cuántico estándar puede ser interpretado como un portador de un bit de información clásica sobre los errores que han ocurrido. Sustituyendo el qubit auxiliar por medio ebit, en principio, permitiría extraer dos bits de información clásica sobre los errores, y con más información, más errores podemos corregir con menos coste.

Para desarrollar esta idea, vamos a introducir el formalismo estabilizador de códigos correctores cuánticos, donde los códigos son una vez más subespacios de un espacio de Hilbert que se especifican en este caso dando los generadores de un subgrupo abeliano del grupo de Pauli, llamado

estabilizador del espacio de código. El requisito de que un código contenga su dual, como es el caso de los códigos CSS vistos anteriormente, es consecuencia de la necesidad de un formalismo estabilizador. La virtud de este enfoque es que podemos construir códigos cuánticos a partir de códigos clásicos con ciertas propiedades, en lugar de tener que desarrollar una nueva teoría de corrección de errores cuánticos desde cero. Aunque, desafortunadamente, la necesidad de una matriz de comprobación de paridad auto-ortogonal presenta un obstáculo considerable para importar directamente la teoría clásica, especialmente en el contexto de códigos modernos como los *códigos de comprobación de paridad de baja densidad (LDPC)* [15].

Asumimos que el codificador Alice y el decodificador Bob tienen acceso a entrelazamiento compartido. Argumentaremos que, en este entorno, cada código lineal clásico puede transformarse en un código cuántico y lo ilustraremos con un ejemplo.

Formalismo estabilizador estándar

El poder del formalismo estabilizador proviene del uso ingenioso de la teoría de grupos. Sea $\Pi = \{I, X, Y, Z\}$ el conjunto de operadores de Pauli, y sea $\Pi^n = \{I, X, Y, Z\}^{\otimes n}$ el conjunto de productos tensoriales de operadores de Pauli de un solo qubit. Entonces Π^n junto con los posibles factores generales $\pm 1, \pm i$ forman un grupo G_n con el producto, conocido como el n-grupo de Pauli, algunas de cuyas propiedades son:

- (i) Cada elemento de G_n se eleva al cuadrado para dar la identidad $\pm I_n$.
- (ii) Dos elementos de G_n cualesquiera o bien conmutan o bien anticonmutan.
- (iii) Todo elemento de G_n es unitario.
- (iv) Los elementos de G_n son o bien Hermíticos o anti-Hermíticos.

La conexión del grupo G_n con la corrección de errores es inmediata, ya que podemos identificar los elementos de este grupo con los posibles conjuntos de errores que pueden afectar a un conjunto de n qubits. Para ver esto, supongamos que S es un subgrupo abeliano de G_n y definamos el código estabilizador $C(S)$ asociado con S como:

$$C(S) = \{|\psi\rangle : M|\psi\rangle = |\psi\rangle, \forall M \in S\} \tag{66}$$

El código $C(S)$ es un subespacio fijado por S, por lo que llamaremos a S el grupo *estabilizador del código*. En otras palabras, este espacio de código es el autoespacio con autovalor $+1$ de todos los elementos de S. Además, se tiene que para un código $[n, k]$, que codifica k qubits lógicos en n qubits físicos, $C(S)$ tiene dimensión 2^k y S tiene 2^{n-k} elementos. Es importante señalar que para que un grupo S pueda ser estabilizador de un subespacio de código no trivial, debe satisfacer que sus elementos conmuten y que el grupo no contenga a la identidad negativa, lo que implica que todos sus elementos son hermíticos y por tanto tienen autovalores ± 1.

Un grupo S puede especificarse mediante un conjunto de generadores independientes, $\{M_i\}$. Estos son los elementos de S que se pueden expresar como productos de elementos del grupo y tales que cada elemento de S se puede escribir como un producto de los elementos de este conjunto. Si un subgrupo abeliano S de G_n tiene 2^{n-k} elementos distintos, entonces hay $n-k$ generadores independientes. El beneficio de usar generadores es que proporciona una representación compacta del grupo; para ver si un vector $|\psi\rangle$ está estabilizado por un grupo S, solamente necesitamos verificar si $|\psi\rangle$ está estabilizado por los generadores de S.

Supongamos que S es un código estabilizador, y que el estado cuántico $|\psi\rangle$ está sujeto a errores de un conjunto $\mathcal{E} = \{E_a\} \subset G_n$. Para ver cómo están las propiedades de corrección de errores de $C(S)$ relacionadas con los generadores de S, suponemos que E_a anticonmuta con un generador particular M_i de S. Entonces $M_i E_a |\psi\rangle = -E_a M_i |\psi\rangle = -E_a |\psi\rangle$.

$E_a|\psi\rangle$ es un autovector de M_i con autovalor -1 y por tanto debe ser ortogonal al espacio de código, cuyos autovalores son siemore $+1$. Como el operador de error E_a lleva el espacio de código

$C(S)$ a un subespacio ortogonal, un error de E_a puede ser detectado midiendo M_i. Para cada generador M_i y operador de error E_a, podemos definir un coeficiente $s_{i,a} \in \{0,1\}$, dependiendo si M_i y E_a conmutan o anticonmutan:

$$M_i E_a = (-1)^{s_i,a} E_a M_i$$

El vector $\vec{s}_a = (s_{1,a}, s_{2,a}, \ldots, s_{n-k,a})$ representa el síndrome del error E_a. En el caso de un código no degenerado, el síndrome del error es distinto para todos los $E_a \in \mathcal{E}$, por lo que medir los $n-k$ generadores estabilizadores diagnosticará el error completamente. Sin embargo, un síndrome único no siempre se requiere para que un error sea corregible.

Códigos cuánticos asistidos por entrelazamiento

A continuación ilustraremos la idea de los EAQECC mediante un ejemplo.

Ya sabemos del apartado anterior que un código estabilizador puede construirse a partir de un conjunto de operadores que conmutan en G_n. Veamos si podríamos seguir construyendo un código cuántico en el caso de que los operadores no conmutasen. Sea S el grupo generado por el siguiente conjunto de operadores que no conmutan:

$$\begin{aligned} M_1 &= Z \quad X \quad Z \quad I \\ M_2 &= Z \quad Z \quad I \quad Z \\ M_3 &= X \quad Y \quad X \quad I \\ M_4 &= X \quad X \quad I \quad X \end{aligned} \tag{67}$$

Aquí, M_1 y M_4 anticonmutan con los otros tres, y M_2 y M_3 conmutan. En este ejemplo, primero buscaremos un conjunto diferente de generadores con determinadas relaciones de conmutación, luego relacionaremos S con un grupo B que posee una forma particularmente simple y nos ayudará a discutir las condiciones de corrección de errores, para luego volver a relacionar los resultados con el grupo S. Para seguir avanzando necesitamos dos lemas:

Lema 3.18. *Sea ν un subgrupo arbitrario de G_n con 2^m elementos distintos, entonces existe un conjunto de m generadores independientes de nu de la forma $\{\bar{Z}_1, \bar{Z}_2, \ldots, \bar{Z}_l, \bar{X}_1, \ldots, \bar{X}_{m-1}$, con $m/2 \leq l \leq m$ y tales que $[\bar{Z}_i, \bar{Z}_j] = [\bar{X}_i, \bar{X}_j] = 0, \forall i,j$; $[\bar{Z}_i, \bar{X}_j] = 0, \forall i \neq j$; y $\{\bar{Z}_i, \bar{X}_i\} = 0, \forall i$. Aquí, los corchetes denotan el conmutador y las llaves el anticonmutador. Llamamos $\nu_I = \langle \bar{Z}_{m-l+1}, \ldots, \bar{Z}_l \rangle$ al grupo generado por el conjunto de generadores que conmutan, y llamamos $\nu_S = \langle \bar{Z}_1, \ldots, \bar{Z}_{m-l}, \bar{X}_1, \ldots, \bar{X}_{m-l} \rangle$ al subgrupo generado por el conjunto de pares de conmutadores que anticonmutan. Entonces ν está generado por ν_I y ν_S, que podemos indicar con la misma notación: $\nu = \langle \nu_I, \nu_S \rangle$.*

Para el grupo S que estamos considerando, podemos usar el siguiente conjunto de generadores independientes:

$$\begin{aligned} \bar{Z}_1 &= Z \quad X \quad Z \quad I \\ \bar{X}_1 &= Z \quad Z \quad I \quad Z \\ \bar{Z}_2 &= Y \quad X \quad X \quad Z \\ \bar{Z}_3 &= Z \quad Y \quad Y \quad X \end{aligned} \tag{68}$$

De manera que $S_S = \langle \bar{Z}_1, \bar{X}_1 \rangle$, $S_I = \langle \bar{Z}_2, \bar{Z}_3 \rangle$ y $S = \langle S_I, S_S \rangle$.

La elección de la notación $\bar{Z}_i, \bar{X}_i$ no es arbitraria, estos generadores tienen las mismas relaciones de conmutación que un conjunto de operadores de Pauli Z_i, X_i sobre un conjunto de qubits representados por los índices i.

Ahora, sea B el grupo generado por el conjunto:

$$\begin{aligned} Z_1 &= Z \quad I \quad I \quad I \\ X_1 &= X \quad I \quad I \quad I \\ Z_2 &= I \quad Z \quad I \quad I \\ Z_3 &= I \quad I \quad Z \quad I \end{aligned} \tag{69}$$

Del lema previo sabemos que $B = \langle B_I, B_S \rangle$, donde $B_S = \langle Z_1, X_1 \rangle$ y $B_I = \langle Z_2, Z_3 \rangle$. Por tanto, los grupos B y S son isomorfos, de manera que podemos relacionar S con B, que es más simple, mediante el siguiente lema:

Lema 3.19. *Si S y B son isomorfos, entonces existe un operador unitario U tal que para todo $b \in B$ existe un $s \in S$ tal que $b = USU^{-1}$, salvo quizá un factor de fase global.*

Como consecuencia, las potencias de $C(B)$ y $C(S)$ están también relacionadas a través de una transformación unitaria. En lo que sigue, usaremos B para estudiar las condiciones de corrección de errores y después trasladaremos los resultados a S.

Como B no es un grupo conmutativo, $C(B)$ no está definido de manera usual, ya que B no es un grupo conmutativo y entonces los generadores no comparten un espacio propio. Sin embargo, extendiendo los generadores podemos encontrar un nuevo grupo conmutativo para el que podemos aplicar la definición usual del espacio de código. Esto lo haremos añadiendo un operador Z al final de Z_1, un operador X al final de X_1 y la identidad al final de Z_2 y Z_3, para hacer B abeliano.

$$\begin{aligned} Z_1' &= Z \quad I \quad I \quad I \quad Z \\ X_1' &= X \quad I \quad I \quad I \quad X \\ Z_2' &= I \quad Z \quad I \quad I \quad I \\ Z_3' &= I \quad I \quad Z \quad I \quad I \end{aligned} \tag{70}$$

Asumimos que los 4 qubits originales están en posesión de Alice y el qubit adicional en posesión de Bob, no estando este último sujeto a ningún error. Sea B_e el grupo extendido generado por $\{Z - 1', X_1', Z_2', Z_3'\}$, definimos el espacio de código $C(B)$ como el espacio propio de autovalor $+1$ de todos los elementos de B_e, pudiendo escribirlo explícitamente:

$$C(B) = \{|\Phi\rangle^{AB} |0\rangle |0\rangle |\Psi\rangle\} \tag{71}$$

Donde $|\Phi\rangle^{AB}$ es un estado entrelazado compartido entre Alice y Bob, y $|\Psi\rangle$ es un estado puro de un qubit individual. Como usamos entrelazamiento, esto ya es un EAQECC, para el que usaremos la notación $[n, k; c]$ para denotar un código corrector cuántico asistido por entrelazamiento que codifica K qubits en n qubits con la ayuda de c ebits. El número de ebits necesarios para la codificación es igual al número de pares de generadores anticonmutativos en B_S. El número s de bits auxiliares es igual al número de generadores independientes en B_I, y el número de qubits codificados k es igual a $n - c - s$, y definimos la tasa del código como $(k - c)/n$. Por tanto, el código $C(B)$ es, en este caso, un código $[4, 1; 1]$ de tasa nula y 2 qubits auxiliares. Aquí, la tasa nula no significa que los qubits no se transmitan mediante este código, sino que implica que el número de bits de entrelazamiento es igual al número de bits transmitidos. En general $(k - c)$ puede ser positivo, negativo o cero.

Ahora podemos ver las propiedades de corrección de errores del código estabilizador original S. Podemos construir un código corrector a partir de un grupo no abeliano S si se puede aplicar el entrelazamiento, igual que hicimos con B. Podemos añadir operadores extra Z y X para hacer S abeliano:

$$\begin{aligned} \bar{Z}_1 &= Z \quad X \quad Z \quad I \quad Z \\ \bar{X}_1 &= Z \quad Z \quad I \quad Z \quad X \\ \bar{Z}_2 &= Y \quad X \quad X \quad Z \quad I \\ \bar{Z}_3 &= Z \quad Y \quad Y \quad X \quad I \end{aligned} \tag{72}$$

Donde asumimos de nuevo que el qubit extra está en posesión de Bob y, por tanto, está libre de errores. Sea S_e el grupo generado por los operadores anteriores, como S es isomorfo a B, con el operador unitario U del segundo lema podemos definir el espacio de código $C(S)$ como:

$$C(S) = U^{-1}[C(B)] \tag{73}$$

Donde el operador unitario U puede interpretarse como la operación de codificación del código asistido por entrelazamiento definido por S.

En resumen, este código se traduce en lo siguiente: Alice desea codificar $k = 1$ estado de un qubit $|\Psi\rangle$ en $n = 4$ qubits y transmitirlos a través de un canal ruidoso a Bob. Inicialmente, Alice y Bob comparten $c = 1$ ebit, es decir, un par de qubits entrelazados. Alice ejecuta la operación unitaria U sobre su qubit $|\Psi\rangle$, su mitad de par entrelazado y $s = 2$ qubits auxiliares. Tras eso, envía los cuatro qubits a través del canal ruidoso a Bob. Bob entonces mide los generadores extendidos $\{\bar{Z}_1', \bar{X}_1', \bar{Z}_2', \bar{Z}_3'\}$, en los cuatro qubits recibidos y su mitad de par entrelazado. El resultado de estas cuatro medidas proporcionará el síndrome de error, por lo que Bob podrá corregir el error y decodificar el qubit $|\Psi\rangle$. A partir de este ejemplo se deduce el procedimiento para cualquier EAQECC. En particular, los parámetros n, k, c y s variarán dependiendo del código, y en función de sus valores podremos proceder de forma análoga a la anterior.

En general, dado un código corrector de errores cuánticos estándar que codifica k qubits en n qubits, existe un código corrector de errores cuánticos asistido por entrelazamiento que, utilizando n qubits y c ebits, puede codificar más de k qubits, reduciendo el número de qubits auxiliares necesarios. Esto es debido a la capacidad de los EAQECC para usar el entrelazamiento preexistente para reducir la redundancia necesaria en los qubits de control, dado que parte de la información de corrección es proporcionada por el estado entrelazado, haciendo de estos códigos una herramienta poderosa y prometedora en el futuro de esta disciplina.

Referencias

[1] Michael A.Nielsen and Isaac L.Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2010.

[2] Claude Cohen-Tannoudji, Bernard Diu, and Franck Laloë. *Quantum mechanics, volume 1: Basic concepts, tools and applications.* Wiley-VCH, 2020.

[3] Victor Rivero Arranz and Carlos Baladrón García (tutor). Trabajo de fin de grado: Interpretaciones de la mecánica cuántica. url: Enlace en el repositorio de la UVa, 2016.

[4] D. F. Styer, M. S. Balkin, K. M. Becker, M. R. Burns, C. E. Dudley, S. T. Forth, J.S. Gaumer, M. A. Kramer, D. C. Oertel, L. H. Park, M. T. Rinkoski, C. T. Smith, and T. D. Wotherspoon. Nine formulations of quantum mechanichs. *Am. J. Phys. 70, 288–297*, 2002.

[5] Biografía de john von neumann. url: John Von Neumann. Última visita el 5/4/2024.

[6] Franck Laloë. *Comprenons-nous vraiment la mécanique quantique?: 2ème édition.* EDP Sciences, 2021.

[7] Esfera de bloch. url: Esfera de Bloch. Última visita el 23/4/2024.

[8] Phase flip. url: Phase flip. Última visita el 23/4/2024.

[9] Mark Fox. *Quantum Optics, an introduction.* Oxford University Press, 2006.

[10] Claude Cohen-Tannoudji, Bernard Diu, and Franck Laloë. *Quantum mechanics, volume 2: Angular Momentum, Spin, and Approximation Methods.* Wiley-VCH, 2019.

[11] Howard Barnum, Carlton M. Caves, Christopher A. Fuchs, Richard Jozsa, and Benjamin Schumacher. Noncommuting mixed states cannot be broadcast. *Physical Review Letters*, 1995.

[12] Todd Brun, Igor Devetak, and Min-Hsiu Hsieh. Correcting quantum errors with entanglement. *Science. Vol 314*, 2006.

[13] R. Josza and N. Linden. On the role of entanglement in quantum computational speed-up. *Proc. R. Soc. London Ser. A 459,*, 2003.

[14] R. Blume-Kohout, C. Caves, and I. Deutsch. Climbing mount scalable: Physical resource requirements for a scalable quantum computer. *Found. Phys. 32, 1641*, 2002.

[15] D.J.C. MacKay, G. Mitchison, and P.L. McFadden. Sparse-graph codes for quantum error correction. *IEEE Transactions on Information Theory*, 50(10):2315–2330, October 2004.

I. Anexo. Programa para imágenes

Para la generación de las imágenes correspondientes a la deformación de la esfera de Bloch, se ha escrito un código en MatLab consistente en representar primeramente números complejos como puntos de la esfera de Bloch, interpretados como los estados cuánticos reflejados por el operador de densidad correspondiente, y posteriormente aplicar las operaciones del formalismo de suma de operadores al operador de densidad para volver a representar los resultados en el mismo entorno, de tal manera que se aprecien los cambios sufridos en la posición de dichos puntos. El código a continuación es el de bit flip, y variando las operaciones cuánticas se obtienen el resto de canales ruidosos.

```
% Inicializamos la matriz para almacenar los puntos

num_repetitions = 1000;

points = zeros(num_repetitions, 3);

for i = 1:num_repetitions % Generamos la parte real e imaginaria aleatoria de a y b

a_real = randn();

a_imag = randn();

b_real = randn();

b_imag = randn();

% Normalizamos a y b para que cuadren con un estado

a_mod = sqrt(a_real^2 + a_imag^2);

b_mod = sqrt(b_real^2 + b_imag^2);

a = (a_real + 1i * a_imag) / sqrt(a_mod^2+b_mod^2);

b = (b_real + 1i * b_imag) / sqrt(a_mod^2+b_mod^2);

% Calculamos los elementos de la matriz densidad original del sistema

element_11 = abs(a)^2;

element_12 = a * conj(b);

element_21 = conj(a) * b;

element_22 = abs(b)^2;

% Calculamos las coordenadas del punto en la esfera de Bloch

x = 2 * real(element_12);

y = 2 * imag(element_21);

z = element_11 - element_22;

p = 0.2; % Parámetro de probabilidad

xx = 2 * real(p*element_12+(1-p)*element_21);

yy = 2 * imag(p*element_21+(1-p)*element_12);
```

```
zz = p * (element_11 - element_22) + (1-p) * (element_22 - element_11);
% Almacenamos las coordenadas del punto en la matriz
points(i, :) = [x, y, z];%Esfera de Bloch original
pointss(i, :) = [xx, yy, zz];%Esfera de Bloch deformada
end
% Graficamos todos los puntos en un solo gráfico tridimensional
figure;
scatter3(points(:, 1), points(:, 2), points(:, 3), 100, 'r', '.');
title('Esfera de Bloch');
xlabel('X');
ylabel('Y');
zlabel('Z');
grid on;
axis equal;
xlim([-1, 1]);
ylim([-1, 1]);
zlim([-1, 1]);
% Y ahora los de la esfera deformada
figure;
scatter3(pointss(:, 1), pointss(:, 2), pointss(:, 3), 100, 'r', '.');
title('Esfera de Bloch deformada');
xlabel('X');
ylabel('Y');
zlabel('Z');
grid on;
axis equal;
xlim([-1, 1]);
ylim([-1, 1]);
zlim([-1, 1]);
```