CÓDIGOS CORRECTORES DE ERRORES CUÁNTICOS

Pastor Díaz, Ulises

Memoria presentada como parte de los requisitos para la obtención del título de Grado en Matemáticas por la Universidad de Sevilla.

Realizada por

Ulises Pastor Díaz

Tutorizada por

Prof. José María Tornero Sánchez

Índice general

Abstract

"Begin at the beginning," the King said, very gravely, "and go on till you come to the end: then stop."
-Lewis Carroll.

We could start our story talking about the revolution of quantum mechanics and the need to decipher the mystery that it creates, or we could start by talking about the birth of modern computation, which changed the world we live in in ways beyond repair. In any way, the gestation of quantum computation, unavoidable consequence of those events, led to a new and unsettling question: Is quantum computation the last link in the evolution towards the construction of efficient algorithms?

In 1985, David Deutsch - the procurer in this confusing story - presented his idea of *Universal Quantum Computer* and showed the world the first quantum algorithm, which seemed to insinuate a greater efficiency of quantum computers over classical computers. In 1994, Peter Shor climbed on the back of Deutsch to find efficient algorithms for the problems of factorization and discrete logarithm in quantum computation, and in 1995 Lov Grover did the same with search algorithms. At the same time, and following the steps of Richard Feynman, it was shown that a quantum computer can efficiently simulate any classical computer.

All the ingredients seemed to be on the table, but no one was able to cook the cake, and to this day, no one has been: despite all evidences there is no proof that quantum computation is more efficient than classical computation in all of its aspects.

The subject we will develop in this memoir, although connected, will be slightly different from what we have already discussed. Rather than focusing on computation, we will follow another young branch of mathematics: information theory.

The adventure of quantum information theory is short but intense. In 1995, Ben Schumacher defined the qubit, and announced a similar result to that of Claude Shannon in 1948 for noiseless channels. However, a result for the coding of channels in the presence of noise has not been found, although in the way we have found some interesting classes of quantum correcting codes which allow quantum computers to work in the presence of noise.

Despite of its youth, many results have been found in the field of quantum information, such as *superdense coding* - which allows to send two bits of

classical information using only one qubit -, *distributed quantum computing* -which shows that a network of computers need exponentially less communication to solve problems than classic computers - or the fact that two quantum channels with zero capacity may transmit information.

All these results move away from our path, which will take us, however, from the bases of quantum computation to the theory of quantum correction codes, walking by the formalisation of quantum noise and the introduction of metrics between quantum states. By doing this, we will try to answer two questions.

In the first place, is it possible to construct quantum correction codes which protect us against the action of noise when we broadcast quantum information? And secondly, do these codes offer any advantages over our well known classical codes?

Capítulo 1

Mecánica cuántica

> *"Why, sometimes I've believed as many as six impossible things before breakfast."*
> **-Lewis Carroll**.

Empecemos por el principio. Dado que vamos a tratar de construir un modelo de computación basado en la mecánica cuántica, ¿qué mejor punto de partida que la mecánica cuántica para comenzar nuestra ruta?

1.1. Postulados de la mecánica cuántica.

La mecánica cuántica es un marco matemático en el cual se fundamentan diferentes teorías físicas, y que podemos resumir en los siguientes cuatro postulados.

1.1.1. Primer postulado.

El primer postulado es el que establece el tablero de juego, el objeto matemático que nos va a permitir definir los sistemas cuánticos y trabajar con ellos.

Definición 1.1. *Postulado I: Espacio de estados, vector de estado.*
A cada sistema cuántico aislado le asociaremos un espacio de Hilbert $\mathcal{H}$ (espacio vectorial complejo con producto escalar) llamado espacio de estados. *El sistema cuántico quedará determinado completamente en cada instante por su* vector de estado*, un elemento del espacio cociente $\mathbb{P}(\mathcal{H})$, i.e., el espacio de vectores unitarios de $\mathcal{H}$ cocientado por la relación $|\psi\rangle \sim e^{i\theta}|\psi\rangle$ con $\theta \in \mathbb{R}$.*

Tras leer esta formulación cabe plantearse varias cuestiones sobre la motivación de esta definición. ¿Por qué tienen una estructura lineal los sistemas cuánticos? ¿Por qué usamos el espacio cociente como espacio de estados?

Para resolver nuestras inquietudes sobre la naturaleza lineal de los sistemas cuánticos debemos recordar que la física cuántica se fundamenta en el principio de la dualidad onda-corpúsculo, según la cual podemos asociar a las partículas subatómicas funciones de ondas, teniendo el conjunto de funciones de onda una estructura lineal.

En cuanto al espacio cociente, la razón principal es que dos estados relacionados vienen generados por la misma distribución de probabilidad, desarrollo que podemos encontrar en [1](1-4) y que nos permite realizar la construcción geométrica de la *esfera de Bloch*, pero podríamos considerar el espacio de estados como el conjunto de vectores unitarios por simplicidad.

El sistema cuántico más sencillo con el que vamos a trabajar y a partir del cuál construiremos sistemas complejos es el qubit.

Definición 1.2. *Qubit.*
Un qubit *es un espacio de estados bidimensional.*

Usando la notación de Dirac, notaremos como $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ y $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ los elementos de la base ortonormal canónica de dicho espacio (que llamaremos *base computacional del qubit*), y por tanto podemos escribir cualquier estado de nuestro qubit como:

$$|\psi\rangle = a|0\rangle + b|1\rangle, a, b \in \mathbb{C}.$$

Siendo la condición de normalización equivalente a $|a|^2 + |b|^2 = 1$.

Esta notación también nos permitirá simplificar los productos escalar y tensorial entre dos estados:

$$\Big(|\psi\rangle, |\varphi\rangle\Big) = \langle\psi|\varphi\rangle; \quad |\psi\rangle \otimes |\varphi\rangle = |\psi\rangle|\varphi\rangle.$$

Además, notaremos el vector dual de $|\psi\rangle$ como $\langle\psi|$.

Gracias a la definición del espacio de estados como espacio cociente podemos hacer la identificación geométrica entre el qubit y la llamada esfera de Bloch según la *fibración de Hopf* [2].

Lema 1.1. Sea $|\psi\rangle = a|0\rangle + b|1\rangle$ un qubit. Existen $\theta, \varphi, \gamma \in \mathbb{R}$ tales que $\psi = e^{i\gamma}(cos\frac{\theta}{2}|0\rangle + e^{i\varphi}sen\frac{\theta}{2}|1\rangle)$.

La demostración de este resultado es trivial. Viendo el qubit dentro de nuestro espacio cociente podemos eliminar el factor $e^{i\gamma}$ e identificar cada qubit con un punto de la esfera dada por las coordenadas esféricas (θ, φ).

Definición 1.3. *Esfera de Bloch.*
A la construcción anterior la llamaremos esfera de Bloch.

1.1.2. Segundo postulado.

Ahora que ya conocemos la arena de combate, empecemos a mover las piezas. El siguiente postulado establece cómo evolucionan los sistemas cuánticos aislados.

Definición 1.4. *Postulado II: Ecuación de Schrödinger.*
La evolución de un sistema cuántico cerrado viene dada por la ecuación de Schödinger*:*

$$i\hbar\frac{d|\psi\rangle}{dt} = H|\psi\rangle.$$

Siendo $\hbar$ la constante de Planck *y H un operador hermítico llamado* Hamiltoniano*.*

Resolviendo la ecuación entre dos instantes t_1 y t_2 obtenemos:

$$|\psi_2\rangle = exp\left[\frac{-iH(t_2-t_1)}{\hbar}\right]|\psi_1\rangle.$$

Por otro lado, nosotros estaremos interesados únicamente en cambios discretos del sistema, lo que motiva la siguiente proposición.

Proposición 1.1. La matriz

$$U(t_2,t_1) = exp\left[\frac{-iH(t_2-t_1)}{\hbar}\right]$$

es unitaria y para toda matriz unitaria U existe una matriz hermítica H tal que U se escribe de esta forma.

Demostración. Usando que

$$exp(X)^* = exp(X^*)$$

y que

$$exp(X)exp(-X) = Id$$

es fácil comprobar que

$$UU^* = exp\left[\frac{-iH(t_2-t_1)}{\hbar}\right]\cdot exp\left[\frac{iH^*(t_2-t_1)}{\hbar}\right] = Id$$

dado que H es un operador hermítico.
Sea ahora U una matriz unitaria, basta probar que $K = -i\,log(U)$ es un operador hermítico. Para ello consideremos la descomposición espectral de U: existe V unitaria tal que $\Sigma = V^*UV$ siendo Σ diagonal. De esta forma $log(U) = V^*log(\Sigma)V$, y para calcular el logaritmo de una matriz diagonal basta sustituir cada elemento de la diagonal por su logaritmo. Por tanto

$$K^* = i\,V^*(log(\Sigma))^*V$$

y dado que los autovalores de U son imaginarios puros por ser unitaria,

$$(log(\Sigma))^* = log(\Sigma^*) = log(-\Sigma) = -log(\Sigma)$$

y por tanto $K^* = K$ y el operador es hermítico.

Esta proposición nos permite considerar los cambios en sistemas cuánticos de manera equivalente desde una perspectiva discreta mediante las matrices unitarias.

Definición 1.5. *Postulado II. Transformación unitaria.*
La evolución de un sistema cuántico cerrado queda descrita por una transformación unitaria*. Es decir, sean $|\psi_1\rangle$ y $|\psi_2\rangle$ los estados de un mismo sistema en los instantes t_1 y t_2 respectivamente, estos quedan relacionados por una matriz unitaria U que depende únicamente de t_1 y t_2:*

$$|\psi_2\rangle = U|\psi_1\rangle.$$

Además, de manera recíproca, toda matriz unitaria que podamos considerar expresa una transformación cuántica así que la identificación es completa.

1.1.3. Tercer postulado.

Ya tenemos el tablero y conocemos las reglas, pero ahora hay que ensuciarse las manos y mover las piezas.
Hasta ahora hemos tratado con sistemas cuánticos aislados pero, ¿qué ocurre cuando queremos observar nuestro sistema? ¿Hacer una medición no hace que el sistema deje de estar aislado? El tercer postulado responde a estas preguntas.

Definición 1.6. *Postulado III. Medición cuántica.*
Una medición cuántica *es un conjunto $\{M_m\}$ de operadores actuando sobre el sistema, llamados* operadores de medición*, que satisfacen la* ecuación de completitud*:*

$$\sum_m M_m^* M_m = I.$$

Siendo I el operador identidad.
El índice m se corresponde con cada uno de los posibles resultados de la medición.
Sea $|\psi\rangle$ el estado previo a la medición, la probabilidad *de obtener el resultado m es:*

$$p(m) = \langle\psi|M_m^* M_m|\psi\rangle.$$

El estado tras obtener el resultado m en la medición pasará a ser:

$$|\psi_m\rangle = \frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^* M_m|\psi\rangle}}.$$

Sobre el significado de la ecuación de completitud cabe añadir el siguiente resultado.

Proposición 1.2. El conjunto de operadores $\{M_m\}$ satisface la ecuación de completitud si y sólo si para todo estado se cumple $\sum_m p(m) = 1$.

Demostración. Basta comprobar la siguiente secuencia:

$$\sum_m M_m^* M_m = I \iff \forall |\psi\rangle \, \langle\psi| \left(\sum_m M_m^* M_m \right) |\psi\rangle = \langle\psi|I|\psi\rangle \iff$$

$$\sum_m \langle\psi| M_m^* M_m |\psi\rangle = \langle\psi|\psi\rangle \iff \sum_m p(m) = 1.$$

Centrémonos ahora en un ejemplo muy ilustrativo, *la medición de un qubit en la base computacional*. En este caso, tomamos como operadores de medición $M_0 = |0\rangle\langle 0|$ y $M_1 = |1\rangle\langle 1|$. Estos operadores satisfacen la ecuación de completitud.
Sea $|\psi\rangle = a|0\rangle + b|1\rangle$ el estado previo a la medición, podemos comprobar que:

$$p(0) = \langle\psi| M_0^* M_0 |\psi\rangle = \langle\psi| M_0 |\psi\rangle = |a|^2.$$

Y de manera análoga $p(1) = |b|^2$.
Los resultados tras la medición son de esta forma:

$$|\psi_0\rangle = \frac{M_0|\psi\rangle}{|a|} = \frac{a}{|a|}|0\rangle.$$

$$|\psi_1\rangle = \frac{M_1|\psi\rangle}{|b|} = \frac{b}{|b|}|1\rangle.$$

Que podemos identificar con $|0\rangle$ y $|1\rangle$ respectivamente en nuestro espacio de estados. Obtenemos por tanto el resultado esperado.

Un resultado interesante que se deriva de la medición de sistemas cuánticos es el siguiente:

Proposición 1.3. Distinción de estados cuánticos.
Sean $\{|\psi_i\rangle\}_{1 \leq i \leq n}$ una colección de estados, y $|\psi_j\rangle$ uno de ellos, podemos distinguir de qué estado se trata si y sólo si los estados $|\psi_i\rangle$ son ortonormales dos a dos.

Demostración. Para mostrar la implicación recíproca basta considerar el conjunto

$$\{M_j = |\psi_j\rangle\langle\psi_j|, \quad 1 \leq j \leq n\}$$

y M_0 como la raíz cuadrada del operador positivo $I - \sum_{j=1}^{n} M_j$.[1] Este conjunto es una medición cuántica, ya que verifica la ecuación de completitud, y además, si el estado que queremos distinguir es $|\psi_i\rangle$, tenemos que

$$p(i) = \langle\psi_i| M_i |\psi_i\rangle = 1$$

por lo que obtenemos el resultado i con total certeza.

[1] Un operador positivo tiene una única raíz cuadrada positiva por el homeomorfismo de la exponencial.

La implicación directa la dejaremos sin probar, ya que carece de interés y se aleja del objetivo de este texto, pero podemos encontrarla en [3] (86-87).

Veamos ahora un caso concreto de medición, la *medición proyectiva.*

Definición 1.7. *Observable.*
Un observable *es un operador hermítico en el espacio de estados.*

Por el *teorema de descomposición espectral* ([3],69-71), un observable M se puede escribir de la forma:

$$M = \sum_m mP_m.$$

Siendo m los autovalores de M y P_m las proyecciones sobre los respectivos subespacios de autovalores.

Definición 1.8. *Medición proyectiva.*
Una medición proyectiva *es la dada por un observable* $M = \sum_m mP_m$*, siendo los posibles resultados los dados por los autovalores* m*.*
Sea $|\psi\rangle$ *el estado observado, la probabilidad de obtener el resultado* m *viene dada por:*

$$p(m) = \langle\psi|P_m|\psi\rangle.$$

Y el resultado tras la medición será:

$$|\psi_m\rangle = \frac{P_m|\psi_m\rangle}{\sqrt{p(m)}}.$$

Proposición 1.4. La medición proyectiva es un caso concreto de medición cuántica que se corresponde con la propiedad de que los operadores de medición sean proyecciones ortogonales.

Demostración. Dado que los P_m son hermíticos y $P_mP_{m'} = \delta_{m,m'}P_m$, lo único que tenemos que demostrar es que $\sum_m P_m = I$, lo que cumplen por ser proyecciones ortogonales. ∎

Veamos por último el *formalismo POVM* (positive-operator valued measure), una herramienta para trabajar con mediciones cuando los resultados finales no son importantes y nuestro objetivos son las probabilidades de cada resultado.

Definición 1.9. *POVM.*
Un POVM *es un conjunto* $\{E_m\}$ *de operadores, llamados* elementos POVM *que verifican:*

1. *Para todo* m, E_m *es definido positivo.*
2. *Ecuación de completitud:* $\sum_m E_m = I$.

Sea $|\psi\rangle$ *el estado previo a la medición, la probabilidad de obtener el resultado* m *es:*

$$p(m) = \langle\psi|E_m|\psi\rangle.$$

Proposición 1.5. El formalismo POVM describe una medición cuántica. Además, sea $\{M_m\}$ una medición cuántica y $E_m = M_m^* M_m$, el conjunto $\{E_m\}$ es un POVM.

Demostración. Dado que E_m es semidefinido positivo, podemos tomar cada operador $M_m = \sqrt{E_m}$ como la única raíz semidefinida positiva para cada m, y tenemos que

$$\sum_m M_m^* M_m = \sum_m E_m = I$$

por lo que los $\{M_m\}$ constituyen una medición.
La segunda parte es inmediata de la definición de medición cuántica. ∎

La pregunta que resta formularse ahora es cómo podemos construir sistemas cuánticos complejos a partir de nuestro qubit, lo que nos lleva al cuarto y último postulado.

1.1.4. Cuarto postulado.

Definición 1.10. *Postulado IV. Sistemas compuestos.*
Sean $\mathcal{H}_i, i \in \{1, \dots, n\}$ un conjunto de sistemas cuánticos, el sistema cuántico compuesto*, $\mathcal{H}$, viene dado por el producto tensorial:*

$$\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n = \bigotimes_{i=1}^{n} \mathcal{H}_i.$$

Este postulado nos permite además definir una de las nociones fundamentales de la mecánica cuántica, el *entrelazamiento cuántico.*

Definición 1.11. *Entrelazamiento cuántico.*
Un estado $|\psi\rangle \in \bigotimes_{i=1}^{n} \mathcal{H}_i$ se dice separable *si para todo $i \in \{1, \dots, n\}$ existe $|\psi_i\rangle \in \mathcal{H}_i$ tal que $|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$. En caso contrario se dice que el estado está* entrelazado*.*

Este concepto es fundamental para entender fenómenos como el *super-dense coding*, la *teleportación cuántica* o el *juego de Bell*, y es la base en la que se sustenta el poder de la computación cuántica, ya que sin entrelazamiento es perfectamente posible simular procesos cuánticos en ordenadores clásicos de forma eficiente.

1.2. Operadores de densidad.

Hasta ahora hemos representado los estados del qubit como vectores unitarios, pero dado que nuestro objetivo es estudiar el ruido y la corrección de errores, podemos llegar encontrarnos en una situación en la que no tengamos un estado

determinado, si no una distribución de probabilidad entre diferentes posibles estados.

Para poder trabajar con este tipo de situaciones vamos a considerar una formulación equivalente de los postulados de la mecánica cuántica usando *operadores de densidad*.

Definición 1.12. *Operador de densidad.*
Un operador $\rho \in End(\mathcal{H})$ *es un* operador de densidad *si cumple:*

1. ρ *es semidefinido positivo, i.e., para todo* $|\psi\rangle \in \mathcal{H}, \langle\psi|\rho|\psi\rangle \geq 0$.
2. $tr(\rho) = 1$, *siendo* $tr(\cdot)$ *la traza del operador.*

Supongamos ahora que tenemos una distribución de probabilidad entre un conjunto de posibles estados, que denotaremos $\{p_i, |\psi_i\rangle\}$. Es este caso, definiremos el operador de densidad asociado como:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|.$$

Proposición 1.6. Un operador $\rho \in End(\mathcal{H})$ es de densidad si y sólo si está asociado a una distribución $\{p_i, |\psi_i\rangle\}$.

Demostración. Como ρ es un operador semidefinido positivo (y por tanto hermítico) admite una descomposición espectral

$$\rho = \sum_j \lambda_j |j\rangle\langle j|,$$

siendo los $|j\rangle$ ortonormales y los λ_j autovalores no negativos. Dado que

$$tr(\rho) = tr\left(\sum_j \lambda_j |j\rangle\langle j|\right) = \sum_j \lambda_j tr\left(|j\rangle\langle j|\right) = \sum_j \lambda_j = 1$$

por la condición sobre la traza, tenemos que los $\{\lambda_j\}$ son una distribución de probabilidad, y por tanto $\{\lambda_j, |j\rangle\}$ es una distribución que da lugar a ρ.
Para comprobar la implicación recíproca basta verificar que $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ cumple que $tr(\rho) = \sum_i p_i = 1$ y que, siendo $|\phi\rangle$ un estado cualquiera,

$$\langle\phi|\rho|\phi\rangle = \sum_i p_i \langle\phi|\psi_i\rangle\langle\psi_i|\phi\rangle = \sum_i p_i |\langle\phi|\psi_i\rangle|^2 \geq 0,$$

por lo que ρ es semidefinido positivo y por tanto hermítico. ∎

En concreto, podemos considerar un estado conocido como la distribución trivial que asocia probabilidad 1 a dicho estado.

La pregunta relevante ahora es: ¿pueden distribuciones y estados diferentes generar el mismo operador? ¿Qué relación hay entre ambas?

Teorema 1.1. *Densidad unitaria en el conjunto de matrices de densidad. Dos distribuciones $\{p_i, |\psi_i\rangle\}$ y $\{q_i, |\varphi_j\rangle\}$ dan lugar al mismo operador de densidad ρ si y sólo si existe $U = (u_{ij})$ matriz unitaria tal que:*

$$\sqrt{p_i}|\psi_i\rangle = \sum_j u_{ij}\sqrt{q_j}|\varphi_j\rangle \quad \forall i.$$

Demostración. Supongamos en primer lugar

$$\sqrt{p_i}|\psi_i\rangle = \sum_j u_{ij}\sqrt{q_j}|\varphi_j\rangle$$

para $U = (u_{ij})$ unitaria. En este caso,

$$\sum_i p_i|\psi_i\rangle\langle\psi_i| = \sum_{ijk} u_{ij}u_{ik}^*\sqrt{q_j q_k}|\varphi_j\rangle\langle\varphi_k| = \sum_{jk}\delta_{jk}\sqrt{q_j q_k}|\varphi_j\rangle\langle\varphi_k| = \sum_j q_j|\varphi_j\rangle\langle\varphi_j|$$

y ambos conjuntos generan el mismo operador de densidad.

Supongamos ahora que

$$\sum_i p_i|\psi_i\rangle\langle\psi_i| = \sum_j q_j|\varphi_j\rangle\langle\varphi_j| = A.$$

Sea $A = \lambda_k|k\rangle\langle k|$ una descomposición de A con λ_k positivo para todo k y los $|k\rangle$ ortonormales. Sea $|\psi\rangle$ un vector ortonormal al espacio generado por los $|k\rangle$, entonces $\langle\psi|k\rangle\langle k|\psi\rangle = 0$ para todo k, y por tanto

$$0 = \langle\psi|A|\psi\rangle = \sum_i p_i\langle\psi|\psi_i\rangle\langle\psi_i|\psi\rangle = \sum_i q_i|\langle\psi|\psi_i\rangle|^2$$

y por tanto $\langle\psi|\psi_i\rangle = 0$ para todo i, luego todo $|\psi_i\rangle$ pertenece al espacio generado por los $|k\rangle$.

Sea

$$|\psi_i\rangle = \sum_k e_{ik}|k\rangle$$

tenemos que

$$A = \lambda_k|k\rangle\langle k| = \sum_i p_i|\psi_i\rangle\langle\psi_i| = \sum_{kl}\left(\sum_i p_i e_{ik}e_{il}^*\right)|k\rangle\langle l|$$

y como los $|k\rangle$ son ortonormales $e_{ik}e_{il}^* = \delta_{kl}$ y podemos obtener por tanto una matriz unitaria $V = (v_{ik})$ tal que

$$|\psi_i\rangle = \sum_k v_{ik}|k\rangle$$

añadiendo ceros. Haciendo lo mismo con los φ_j obtenemos otra matriz unitaria W, y basta tomar $U = VW^*$ unitaria. ∎

1.2.1. Reformulación de la mecánica cuántica.

Esta construcción nos permite reformular los postulados iniciales en función de estos nuevos elementos:

Definición 1.13. *Postulado I. Espacio de estados.*
Asociado a cada sistema cuántico existe un espacio de Hilbert $\mathcal{H}$, que llamaremos espacio de estados*.*
El sistema cuántico quedará completamente determinado por su operador de densidad *$\rho \in End(\mathcal{H})$.*

Definición 1.14. *Postulado II. Transformación unitaria.*
La evolución de un sistema cuántico cerrado viene dada por una transformación unitaria*. Es decir, sean ρ_1, ρ_2 los operadores de densidad de un mismo sistema asociados a dos instantes t_1, t_2 respectivamente, éstos quedan relacionados por una acción de grupos de $\mathcal{U}(\mathcal{H})$ (el grupo unitario) en $End(\mathcal{H})$, dada por:*

$$\rho_2 = U\rho_1 U^*,$$

dependiendo U únicamente de los instantes t_1 y t_2.

Definición 1.15. *Postulado III. Medición cuántica.*
Una medición cuántica *es un conjunto $\{M_m\}$ de operadores actuando sobre el sistema llamados* operadores de medición *que satisfacen la* ecuación de completitud*:*

$$\sum_m M_m^* M_m = I.$$

El índice m se corresponde con cada uno de los posibles resultados de la medición.
Sea ρ el estado previo a la medición, la probabilidad *de obtener el resultado m es:*

$$p(m) = tr(M_m^* M_m \rho).$$

El estado tras obtener el resultado m en la medición pasará a ser:

$$\rho_m = \frac{M_m \rho M_m^*}{tr(M_m^* M_m)}.$$

Definición 1.16. *Postulado IV. Sistemas compuestos.*
Sean $\mathcal{H}_i, i \in \{1, \dots, n\}$ un conjunto de sistemas cuánticos, el sistema cuántico compuesto*, $\mathcal{H}$, viene dado por el producto tensorial:*

$$\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n = \bigotimes_{i=1}^{n} \mathcal{H}_i.$$

Proposición 1.7. La formulación con vectores de estado es equivalente a la formulación con operadores de densidad.

Demostración. El primer y el cuarto postulados no presentan problemas. Veamos los otros dos:

- Segundo postulado: Supongamos que una transformación viene dada por la matriz unitaria U, entonces sea $\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$ un operador de densidad, entonces el resultado de la transformación será

$$\sum_i p_i U|\psi_i\rangle\langle\psi_i|U^* = U\left(\sum_i p_i|\psi_i\rangle\langle\psi_i|\right)U^* = U\rho U^*$$

  y esta igualdad funciona en ambos sentidos.
- Tercer postulado: Sea ahora $\{M_m\}$ una medición cuántica y

$$\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$$

  un operador de densidad, usando la ley de probabilidad total sabemos que $p(m) = \sum_i p(m|i)p_i$ y como

$$p(m|i) = \langle\psi_i|M_m^*M_m|\psi\rangle = tr(M_m^*M_m|\psi\rangle\langle\psi_i|)$$

  por lo que $p(m) = tr(M_m^*M_m\rho)$. Sean ahora $|\psi_i^m\rangle$ los resultados de obtener el resultado m en la medición para cada i, tenemos que

$$\rho_m = \sum_i p(i|m)|\psi_i^m\rangle\langle\psi_i^m|$$

  y usando que $p(i|m) = p(m|i)p_i/p(m)$ tenemos que

$$\rho_m = \sum_i p_i \frac{M_m|\psi_i\rangle\langle\psi_i|M_m^*}{tr(M_m^*M_m\rho)} = \sum_i p_i \frac{M_m\rho M_m^*}{tr(M_m^*M_m\rho)}.$$

Obtenemos de esta forma que los postulados para vectores de densidad se siguen de los originales. La equivalencia pasa por reinterpretar las mismas ecuaciones.

1.2.2. Propiedades de los operadores de densidad.

Una vez hemos reconstruido toda la estructura de la mecánica cuántica, cabe preguntarse acerca de la funcionalidad de estos operadores de densidad con los que vamos a trabajar. Por ejemplo, parece que trabajamos con dos casos diferenciados, aquel en el que tenemos un estado conocido, y aquel en el que tenemos una distribución de probabilidad. ¿Sabremos diferenciar en qué caso estamos conociendo únicamente el operador de densidad?

Definición 1.17. *Estado puro y estado mixto.*
Un estado se dice que es un estado puro *si proviene de una distribución de probabilidad trivial, es decir, conocemos con certeza el estado:* $\rho = |\psi\rangle\langle\psi|$.
Un estado que no es puro se dice estado mixto.

Proposición 1.8. Sea ρ un operador de densidad:

1. $tr(\rho^2) \leq 1$.
2. ρ es puro si y sólo si $tr(\rho^2) = 1$.

3. ρ es mixto si y sólo si $tr(\rho^2) < 1$.

Demostración. Tomando una descomposición espectral

$$\rho = \sum_j \lambda_j |j\rangle\langle j|,$$

siendo los $|j\rangle$ ortonormales y los λ_j autovalores positivos, sabemos que $\sum_j \lambda_j = 1$, luego para todo j, $\lambda_j \leq 1$ con igualdad si y sólo si tenemos un único λ_j distinto de cero (i.e., tenemos un estado puro). Es inmediato comprobar que

$$tr(\rho^2) = tr\left(\lambda_j^2 |j\rangle\langle j|j\rangle\langle j|\right) = \sum_j \lambda_j^2 tr(|j\rangle\langle j|) = \sum_j \lambda_j^2 \leq 1$$

y tenemos el resultado. ∎

Introduzcamos ahora las *matrices de Pauli*, que jugarán un rol fundamental hasta el último capítulo.

Definición 1.18. *Matrices de Pauli.*
Las matrices de Pauli son tres operadores del espacio de matrices hermíticas 2×2 *que forman una base de dicho espacio vectorial con la identidad. Son:*

$$\sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_Y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}, \quad \sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Usando la identificación entre las matrices de Pauli y la identidad con $\mathbb{R}^4$ podemos ver cada una de las matrices de Pauli como un eje de la esfera de Bloch como veremos en el siguiente resultado.

Lema 1.2. Sea ρ un operador de densidad, entonces existe $\overrightarrow{r} \in \mathbb{R}^3$ tal que $\|\overrightarrow{r}\| \leq 1$ y $\rho = \frac{I + \overrightarrow{r} \cdot \overrightarrow{\sigma}}{2}$, siendo $\overrightarrow{\sigma}$ las *matrices de Pauli*.

Demostración. Sea $\rho = \begin{pmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{pmatrix}$, definamos

$$\overrightarrow{r} = (\rho_{10} + \rho_{01}, i(\rho_{01} - \rho_{10}), \rho_{00} - \rho_{11}).$$

Como ρ es hermítico el vector es real, y tenemos que

$$\frac{I + \overrightarrow{r} \cdot \overrightarrow{\sigma}}{2} = \frac{1}{2} \begin{pmatrix} 1 + \rho_{00} - \rho_{11} & \rho_{01} + \rho_{10} + (\rho_{01} - \rho_{10}) \\ \rho_{01} + \rho_{10} - (\rho_{01} - \rho_{10}) & 1 - \rho_{00} + \rho_{11} \end{pmatrix} = \rho$$

ya que $\rho_{00} + \rho_{11} = 1$. ∎

Definición 1.19. *Vector de Bloch.*
Al vector $\overrightarrow{r}$ *anterior lo llamaremos* vector de Bloch.

De esta forma, la superficie de la esfera se corresponde con los estados puros, mientras que el interior de la esfera son los estados mixtos.

Otra importante utilidad de los operadores de densidad es el llamado *operador de densidad reducido*, que nos permite considerar únicamente uno de los subsistemas de un sistema cuántico compuesto. Para ello introducimos la traza parcial

Definición 1.20. *Traza parcial.*
Sea $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ un espacio de estados compuesto. Usando que

$$End(\mathcal{H}) \cong \mathcal{H}^* \otimes \mathcal{H} \cong \mathcal{H}_1^* \otimes \mathcal{H}_2^* \otimes \mathcal{H}_1 \otimes \mathcal{H}_2,$$

podemos definir la traza parcial *con respecto a $\mathcal{H}_1$, como la aplicación $tr_{\mathcal{H}_1} : End(\mathcal{H}) \to End(\mathcal{H}_2)$ dada por:*

$$tr_{\mathcal{H}_1}(\langle\psi_1| \otimes \langle\psi_2| \otimes |\varphi_1\rangle \otimes |\varphi_2\rangle) = tr(|\varphi_1\rangle\langle\psi_1|)|\varphi_2\rangle\langle\psi_2| = \langle\psi_1|\varphi_1\rangle|\varphi_2\rangle\langle\psi_2|.$$

Definición 1.21. *Operador de densidad reducido.*
Sea $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ un espacio de estados compuesto, y sea $\rho \in \mathcal{H}$ un operador de densidad, se define el operador de densidad reducido *para el sistema $\mathcal{H}_2$ como:*

$$\rho^{\mathcal{H}_2} = tr_{\mathcal{H}_1}(\rho).$$

Remarquemos que esta definición es consistente con los resultados elementales que podríamos esperar, por ejemplo, dado un operador compuesto $\rho \otimes \sigma$ siendo ρ y σ estados puros, entonces el operador de densidad reducido para el primer sistema es:

$$(\rho \otimes \sigma)^{\mathcal{H}_1} = \rho\, tr(\sigma) = \rho,$$

como cabría esperar.

Veamos las últimas herramientas que nos ofrecen los operadores de densidad: la *descomposición de Schmidt* y la *purificación*.

Teorema 1.2. *Descomposición de Schmidt.*
Sean $\mathcal{H}_1$ y $\mathcal{H}_2$ dos sistemas y $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ un estado del sistema compuesto, entonces existen $\{|\alpha_i\rangle\}$ y $\{|\beta_i\rangle\}$ conjuntos ortonormales de $\mathcal{H}_1$ y $\mathcal{H}_2$ respectivamente tales que:

$$|\psi\rangle = \sum_i \lambda_i |\alpha_i\rangle|\beta_i\rangle.$$

Siendo los λ_i coeficientes no negaivos cumpliendo $\sum_i \lambda_i^2 = 1$ llamados coeficientes de Schmidt*. El número de coeficientes de Schmidt no nulos se llama* número de Schmidt*, y si los sistemas tienen la misma dimensión, los conjuntos $\{|\alpha_i\rangle\}$ y $\{|\beta_i\rangle\}$ se llaman* bases de Schmidt*.*

Demostración. Sean $|j\rangle$ y $|k\rangle$ bases ortonormales de A y B respectivamente, sabemos que $|\psi\rangle$ estado puro puede escribirse como

$$|\psi\rangle = \sum_{jk} a_{jk} |j\rangle|k\rangle$$

con $a_{ij} \in \mathbb{C}$. Sea $A = (a_{ij})$, rellenando con ceros (en caso de que A y B tengan distinta dimensión) podemos encontrar una descomposición en valores singulares $A = U\Sigma V$ con Σ diagonal y U y V unitarias, y por tanto

$$|\psi\rangle = \sum_{ijk} u_{ji}\sigma_{ii}v_{ik}|j\rangle|k\rangle.$$

Sean ahora

$$|i_A\rangle = \sum_j u_{ji}|j\rangle, \quad |i_B\rangle = \sum_k v_{ik}|k\rangle, \quad \lambda_i = \sigma_{ii},$$

podemos comprobar que tanto $|i_A\rangle$ como $|i_B\rangle$ son unitarios y que

$$|\psi\rangle = \sum_i \lambda_i|\alpha_i\rangle|\beta_i\rangle.$$

Este teorema nos permite descomponer un estado compuesto en dos operadores de densidad reducidos de mismos autovalores, lo que resulta útil para la construcción posterior.

El número de Schmidt es un invariante por transformación unitaria que cuantifica la "cantidad de entrelazamiento" entre los dos sistemas.

Previamente señalamos que la composición de dos estados mixtos podría dar como resultado un estado puro. La pregunta que nos hacemos ahora es, dado un estado mixto, ¿podremos encontrar un estado de un sistema compuesto cuyo operador de densidad reducido con respecto a nuestro sistema original es nuestro estado mixto? La respuesta a esta pregunta es la *purificación*, y para su construcción usaremos la descomposición de Schmidt.

Proposición 1.9. Sea ρ un operador de densidad de $\mathcal{H}$, podemos encontrar un sistema compuesto $\mathcal{H} \otimes \mathcal{R}$ y un operador de densidad σ en dicho sistema tal que $\rho = \sigma^H$.

Demostración. Sea ρ un operador de densidad, supongamos que tiene una descomposición ortonormal $\rho = \sum_i p_i|i^{\mathcal{H}}\rangle\langle i^{\mathcal{H}}|$ en $\mathcal{H}$. Tomando ahora $\mathcal{R}$ como el mismo espacio de estados con una base ortonormal $|i^{\mathcal{R}}\rangle$ y definiendo el estado puro en $\mathcal{H} \otimes \mathcal{R}$,

$$|\psi_\sigma\rangle = \sum_i \sqrt{p_i}|i^{\mathcal{H}}\rangle|i^{\mathcal{R}}\rangle,$$

podemos comprobar que, si $\sigma = |\psi_\sigma\rangle\langle\psi_\sigma|$, el correspondiente operador de densidad reducido a $\mathcal{H}$ es ρ:

$$\sigma^{\mathcal{H}} = tr_{\mathcal{R}}(\sigma) = \sum_{ij} \sqrt{p_i p_j}|i^{\mathcal{H}}\rangle\langle j^{\mathcal{H}}|tr\left(|i^{\mathcal{R}}\rangle\langle j^{\mathcal{R}}|\right)$$

$$= \sum_{ij} \sqrt{p_i p_j}|i^{\mathcal{H}}\rangle\langle j^{\mathcal{H}}|\delta_{ij} = \sum_i p_i|i^{\mathcal{H}}\rangle\langle i^{\mathcal{H}}| = \rho.$$

Y obtenemos el resultado.

Definición 1.22. *Purificación y referencia.*
En la situación de la proposición anterior, diremos que el operador σ es una purificación *de ρ.*
Al sistema $\mathcal{R}$ lo llamaremos sistema de referencia.

Capítulo 2

Ruido cuántico

> *"I'm afraid I can't explain myself, sir. Because I am not myself, you see?"*
> **-Lewis Carroll**.

Acabamos de conocer a los protagonistas de nuestra aventura, pero toda historia que se precie tiene algo más; una mente maquiavélica que se encargue de complicarle la vida a nuestros héroes y al que tendremos que derrotar. Un villano. Presentemos al nuestro: el ruido.

Hasta ahora hemos considerado sistemas aislados que evolucionan sin ser afectados por su ambiente, pero en el mundo real ningún sistema (salvo el Universo) es aislado. Esto se hace incluso más visible en el mundo de la computación cuántica, en el cual cualquier pequeña interacción puede tener consecuencias desastrosas en la transmisión de información.

El primer trabajo que tendremos que llevar a cabo será introducir el concepto de ruido en un sistema cuántico, para lo cual usamos el *formalismo de las operaciones cuánticas.*

2.1. Operaciones cuánticas.

Frente a otras herramientas, el *formalismo de las operaciones cuánticas* nos permite estudiar cambios discretos del sistema, facilitando la tarea desde el punto de vista computacional.

2.1.1. Formulación axiomática.

Existen tres formas diferentes de introducir las operaciones cuánticas, resultando las tres equivalentes. Vamos a considerar en primer lugar la definición puramente matemática, la formulación axiomática de las operaciónes cuánticas.

Definición 2.1. *Operación cuántica.*

Sean $\mathcal{H}$ y $\mathcal{G}$ dos sistemas y $D(\mathcal{H}) \subset End(\mathcal{H})$ el conjunto de operadores de densidad de $\mathcal{H}$, una operación cuántica *es una aplicación $\mathcal{E} : D(\mathcal{H}) \to End(\mathcal{G})$ tal que:*

1. *$\forall \rho \in D(\mathcal{H})$, $0 \leq tr(\mathcal{E}(\rho)) \leq 1$.*
2. *$\mathcal{E}$ es lineal.*
3. *$\mathcal{E}$ es completamente positiva, i.e., es positiva y si introducimos cualquier sistema $\mathcal{F}$, la aplicación $Id \otimes \mathcal{E} : \mathcal{F} \otimes D(\mathcal{H}) \to \mathcal{F} \otimes End(\mathcal{G})$ es positiva, siendo Id la identidad en el sistema $\mathcal{F}$.*

El primer punto de esta definición puede parecer un poco chocante. ¿No debería ser el resultado de una operación cuántica un operador de densidad? ¿Qué significa entonces una traza inferior a 1? Podríamos haber considerado únicamente operaciones que preserven la traza, pero en ese caso no estaríamos teniendo en cuenta las mediciones. Si llevamos a cabo una medición, cada uno de los posibles resultados se corresponderá con una operación cuántica, coincidiendo la traza de la misma con la probabilidad asociada a dicho resultado.

El segundo y tercer punto responden a la necesidad de que los estados mixtos y los estados que formen parte de sistemas mayores respectivamente se comporten de forma lógica y den lugar a operadores de densidad.

Caminemos ahora hacia nuestra primera caracterización de las operaciones cuánticas. Para ello debemos introducir la siguiente relación de orden parcial entre operadores.

Sean A y B operadores de un espacio $\mathcal{H}$, entonces:

$$A \leq B \iff \langle\psi|A|\psi\rangle \leq \langle\psi|B|\psi\rangle \quad \forall|\psi\rangle \in \mathcal{H}.$$

O lo que es equivalente, $B - A$ es semidefinido positivo.

Teorema 2.1. *Caracterización por la representación como operadores suma. Una aplicación $\mathcal{E}$ es una operación cuántica si y sólo si existe un conjunto de operadores $\{E_i\}$ entre los espacios $\mathcal{H}$ y $\mathcal{G}$ tales que $\sum_i E_i^* E_i \leq I$ y además:*

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^*.$$

A la relación $\sum_i E_i^* E_i \leq I$ la llamaremos relación de completitud.

Demostración. Mostremos en primer lugar la condición suficiente. Sea una aplicación $\mathcal{E}(\rho) = \sum_i E_i \rho E_i^*$ es inmediato que se trata de una aplicación lineal. Además, sea $\rho = |\psi\rangle\langle\psi|$, se cumple que

$$tr\left(\mathcal{E}(\rho)\right) = tr\left(\sum_i E_i \rho E_i^*\right) = tr\left(\sum_i \langle\psi|E_i^* E_i|\psi\rangle\right) \leq 1,$$

por lo que la condición sobre la traza también se mantiene.

Sólo falta demostrar que $\mathcal{E}$ es completamente positiva. Sea en primer lugar A un operador positivo cualquiera que actúe en el sistema conjunto $\mathcal{F} \otimes \mathcal{H}$ y sea $|\psi\rangle$ un estado de dicho sistema, podemos definir $|\varphi_i\rangle = (I_{\mathcal{F}} \otimes E_i^*)|\psi\rangle$ y entonces:

$$\langle\psi|(I_{\mathcal{F}} \otimes E_i)A(I_{\mathcal{F}} \otimes E_i^*)|\psi\rangle = \langle\varphi_i|A|\varphi_i\rangle \geq 0,$$

ya que A es un operador positivo. Además,

$$\langle\psi|(I \otimes \mathcal{E})(A)|\psi\rangle = \sum_i \langle\varphi_i|A|\varphi_i\rangle \geq 0.$$

Y por tanto llegamos a la conclusión buscada.

Veamos ahora la condición necesaria. Suponiendo que $\mathcal{E}$ cumple nuestros axiomas, introduzcamos un sistema $\mathcal{F}$ de la misma dimensión que $\mathcal{H}$ y con bases ortonormales $|i_{\mathcal{F}}\rangle$ e $|i_{\mathcal{H}}\rangle$ respectivamente.

Definamos ahora $|\alpha\rangle$ del estado conjunto como:

$$|\alpha\rangle = \sum_i |i_{\mathcal{F}}\rangle|i_{\mathcal{H}}\rangle,$$

del cual aprovecharemos su alto grado de entrelazamiento. Definimos ahora el operador σ del sistema conjunto como:

$$\sigma = (I \otimes \mathcal{E})(|\alpha\rangle\langle\alpha|),$$

que a primera vista parece que sólo nos aporta información del efecto de la operación para un estado concreto, pero usando que este estado está en máximo grado de entrelazamiento podemos recuperar la operación completa a partir de σ de la siguiente forma:

Sean $|\psi\rangle = \sum_j \psi_j|j_{\mathcal{F}}\rangle$ y de forma análoga $|\bar{\psi}\rangle = \sum_j \psi_j^*|j_{\mathcal{H}}\rangle$, cabe destacar que

$$\langle\bar{\psi}|\sigma|\bar{\psi}\rangle = \langle\bar{\psi}|\Big(\sum_{ij} |i_{\mathcal{F}}\rangle\langle j_{\mathcal{F}}| \otimes \mathcal{E}(|j_{\mathcal{H}}\rangle\langle i_{\mathcal{H}}|)\Big)|j_{\mathcal{F}}\rangle =$$

$$\sum_{ij} \psi_i\psi_j^*\mathcal{E}(|j_{\mathcal{H}}\rangle\langle i_{\mathcal{H}}|) = \mathcal{E}(|\psi\rangle\langle\psi|).$$

Sea ahora $\sigma = \sum_i |s_i\rangle\langle s_i|$ una descomposición no necesariamente normalizada, podemos definir el operador lineal

$$E_i(|\psi\rangle) = \langle\bar{\psi}|s_i\rangle.$$

Por lo que tenemos que

$$\sum_i E_i|\psi\rangle\langle\psi|E_i^* = \sum_i \langle\bar{\psi}|s_i\rangle\langle s_i|\bar{\psi}\rangle = \langle\bar{\psi}|\sigma|\bar{\psi}\rangle = \mathcal{E}(|\psi\rangle\langle\psi|),$$

de donde obtenemos el resultado para estados puros. Para estados mixtos basta aplicar el segundo axioma y la ecuación de completitud se deduce del primer axioma.

2.1.2. Representación como operadores suma

Definición 2.2. *Representación como operadores suma.*
Sea $\mathcal{E}$ una operación cuántica, la ecuación $\mathcal{E}(\rho) = \sum_i E_i \rho E_i^*$ se dice que es una representación como operadores suma *de $\mathcal{E}$.*
Los elementos de $\{E_i\}$ son llamados elementos de la operación.

Esta representación de las operaciones cuánticas nos permite trabajar de forma fácil con las operaciones cuánticas, sobre todo a la hora de hacer cálculos, además de tener una significación importante en el mundo de la corrección de errores.

Veamos ahora si distintos conjuntos de elementos pueden dar lugar a la misma operación cuántica.

Teorema 2.2. *Relación entre diferntes representaciones de operadores suma. Sean $\{E_i\}_{0\leq i\leq n}$ y $\{F_j\}_{0\leq j\leq m}$ dos conjuntos de operadores que dan lugar a las operaciones $\mathcal{E}$ y $\mathcal{F}$ respectivamente, entonces $\mathcal{E} = \mathcal{F}$ si y sólo si existe una matriz unitaria $U = (u_{ij})$ tal que $E_i = \sum_j u_{ij} F_j$ para todo $i \in \{1, \ldots, n\}$.*

Demostración. Esta prueba se basa en el teorema 1.1. Veamos primero la condición necesaria y recojamos la notación de la demostración del teorema anterior. Si $\{E_i\}$ y $\{F_j\}$ generan la misma operación, entonces

$$\sum_i E_i \rho E_i^* = \sum_j F_j \rho F_j^*.$$

Definiendo ahora

$$|e_i\rangle = \sum_k |k_{\mathcal{F}}\rangle (E_i |k_{\mathcal{H}}\rangle)$$

$$|f_j\rangle = \sum_k |k_{\mathcal{F}}\rangle (F_j |k_{\mathcal{H}}\rangle).$$

Y ambos conjuntos generan el operador σ, por lo que podemos aplicar el teorema 1.1 y llegamos al resultado.
La condición suficiente es inmediata. ∎

Este teorema nos permite además responder a la pregunta siguiente, ¿cuál es el mínimo número de elementos que necesitamos para representar una operación cuántica? Esto facilita nuestra tarea a la hora de calcular errores.

Teorema 2.3. *Toda operación cuántica $\mathcal{E}$ en un espacio de dimensión d puede ser generada por una representación como operadores suma que contenga como máximo d^2 elementos:*

$$\mathcal{E}(\rho) = \sum_{i=1}^{M} E_i \rho E_i^*,$$

con $1 \leq M \leq d^2$.

Demostración. Definamos $W_{jk} = tr(E_j^* E_k)$. La matriz $W = (W_{jk})$ es hermítica y de rango, como mucho, d^2, por lo que podemos diagonalizarla a través de una matriz unitaria U para obtener UWU^* una matriz diagonal con, como mucho, d^2 entradas. Basta tomar las entradas correspondientes y definir $F_i = E_i U^*$.

Veamos por fin la última caracterización, que nos aporta una interpretación física de lo que significa una operación cuántica.

Teorema 2.4. *Caracterización como modelo sistema-ambiente.*
Un conjunto $\{E_i\}$ es una representación suma de una operación cuántica $\mathcal{E}$ en el sistema $\mathcal{H}$ si y sólo si existe un sistema E, inicialmente en el estado $|e_0\rangle$ y una matriz unitaria en el sistema conjunto $\mathcal{H} \otimes E$ tal que:

$$\mathcal{E}(\rho) = tr_E(U[\rho \otimes |e_0\rangle\langle e_0|]U^*).$$

Demostración. En primer lugar, cabe señalar que podemos considerar el sistema ambiente como empezando en un estado puro ya que en caso contrario sustituimos dicho sistema por una purificación.

Visto esto, procedamos a demostrar la implicación hacia la izquierda. Partamos de una base $|e_k\rangle$ del sistema ambiente, en la cual:

$$\mathcal{E}(\rho) = \sum_k \langle e_k|U\left[\rho \otimes |e_0\rangle\langle e_0|\right]U^*|e_k\rangle = \sum_k E_k \rho E_k^*,$$

siendo $E_k = \langle e_k|U|e_0\rangle$. Dado que

$$1 \leq tr\left(\mathcal{E}(\rho)\right) = tr\left(\sum_k E_k \rho E_k^*\right) = tr\left(\sum_k E_k^* E_k \rho\right),$$

y esta relación se cumple para todo ρ, es sencillo comprobar la relación de completitud $\sum_k E_k^* E_k \leq I$.

Veamos ahora la otra implicación, en la que supondremos que tratamos con una operación que preserva la traza, desarrollando la desmostración en otro caso de forma análoga.

En primer lugar construimos E a partir de una base ortonormal $|e_k\rangle$ con la misma indexación que nuestros elementos de la operación y definimos un operador U que lleve a cabo la siguiente acción en estados de la forma $|\psi\rangle|e_0\rangle$:

$$U|\psi\rangle|e_0\rangle = \sum_k E_k|\psi\rangle|e_k\rangle,$$

donde hemos fijado $|e_0\rangle$ de forma arbitraria. En este caso, sean $|\psi\rangle$ y $|\varphi\rangle$ dos estados cualesquiera del sistema principal,

$$\langle\psi|\langle e_0|U^*U|\varphi\rangle|e_0\rangle = \sum_k \langle\psi|E_k^* E_k|\varphi\rangle = \langle\psi|\varphi\rangle,$$

usando la relación de completitud. Y podemos generalizar U a un operador unitario en el sistema conjunto que cumpla nuestra ecuación.

2.1.3. Modelo sistema-ambiente.

Definición 2.3. *Modelo sistema-ambiente.*
En las condiciones del teorema anterior, llamaremos sistema ambiente *al sistema E.*
A la ecuación $\mathcal{E}(\rho) = tr_E(U[\rho \otimes |e_0\rangle\langle e_0|]U^*)$ *la llamaremos* modelo sistema-ambiente.

Esta definición es la que esperamos intuitivamente, ya que podemos considerar una operación cuántica como una transformación unitaria según el proceso siguiente. En primer lugar consideramos el sistema conjunto de nuestro sistema original y el ambiente con el que interacciona. Tras esto, aplicamos una transformación unitaria en el sistema conjunto (ya que lo suponemos cerrado) obteniendo un nuevo estado del sistema total. Finalmente, descartamos una parte del sistema conjunto para obtener un nuevo estado del sistema que nos interesa estudiar.

2.1.4. Ejemplos de operaciones cuánticas.

Terminemos el capítulo con algunos ejemplos de operaciones cuánticas, comenzando por un caso de gran utilidad.

Proposición 2.1. La traza y la traza parcial son operaciones cuánticas.

Demostración. Sea $\mathcal{H}$ un espacio de Hilbert generado por la base ortonormal $|1\rangle, \ldots, |d\rangle$ y $\mathcal{G}$ un espacio de Hilbert unidimensional engendrado por $|0\rangle$. Sea ahora

$$\mathcal{E}(\rho) = \sum_{i=1}^{d} |0\rangle\langle i|\rho|i\rangle\langle i|.$$

Es una operación cuántica según la representación como operadores suma, pero $\mathcal{E}(\rho) = tr(\rho)|0\rangle\langle 0|$ y por tanto la traza es una operación cuántica.

Para ver el resultado de la traza parcial, tomemos dos espacios de Hilbert $\mathcal{H}$ y $\mathcal{G}$ y el espacio conjunto $\mathcal{HG}$. Tomando ahora $|j\rangle$ como base de $\mathcal{G}$, definimos el operador lineal $E_i : \mathcal{HG} \to \mathcal{H}$ dado por:

$$E_i\Big(\sum_j \lambda_j |h_j\rangle|j\rangle\Big) = \lambda_i |h_i\rangle,$$

donde λ_j son números complejos y $|h_j\rangle$ estados arbitrarios de $\mathcal{H}$.

Sea ahora $\mathcal{E}$ dada por

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^*,$$

que vuelve a ser una operación por la representación como operadores suma, pero

$$\mathcal{E}(\rho \otimes |j\rangle\langle j'|) = \delta_{jj'}\rho = tr_{\mathcal{G}}(\rho \otimes |j\rangle\langle j'|),$$

y por linealidad nuestra operación es la traza parcial. ∎

Además, podemos introducir una interpretación geométrica de las operaciones cuánticas en la esfera de Bloch, lo que nos permite trabajar con otros canales cuánticos como el *bit flip* o el *phase flip*, que retomaremos en el capítulo 4, el *depolarizing channel* o el llamado *aplitude damping*, pero el análisis de estos canales específicos se aleja de nuestro sendero, por lo que los dejaremos para otra ocasión.

Capítulo 3

Distancia cuántica

"If you don't know where you are going any road can take you there"
-Lewis Carroll.

3.1. Distancias entre estados cuánticos.

¿Cómo de cercanos son dos estados cuánticos? Parece que para continuar nuestro camino tendremos primero que resolver este problema. Para poder hacerlo, vamos a definir dos formas distintas de medir la cercanía entre estados, la *distancia traza* y la *fidelidad*.

3.1.1. Distacia traza.

Comencemos por esta distancia inspirada en la *distancia de Kolmogorov* para distribuciones de probabilidad.

Definición 3.1. *Distancia traza.*
Sean ρ y σ dos operadores de densidad de un sistema $\mathcal{H}$, definimos la distancia traza *entre ambos como:*

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

siendo $|A| = \sqrt{A^* A}$.

Veamos en primer lugar el nexo con las distribuciones de probabilidad y posteriormente visualicemos su significado usando la representación en la *esfera de Bloch*.

Observación 3.1. Si σ y ρ conmutan, entonces son diagonales en la misma base:

$$\rho = \sum_i r_i |i\rangle\langle i|, \quad \sigma = \sum_i s_i |i\rangle\langle i|.$$

Y por tanto:

$$D(\rho,\sigma)=\frac{1}{2}tr\left|\sum_i(r_i-s_i)|i\rangle\langle i|\right|=\frac{1}{2}\sum_i|r_i-s_i|=D(\{r_i\},\{s_i\}).$$

Siendo esta última distancia que hemos introducido entre las distribuciones de probabilidad $\{r_i\}$ y $\{s_i\}$ la llamada *distancia de Kolmogorov*:

$$D(\{r_i\},\{s_i\})=\frac{1}{2}\sum_i|r_i-s_i|.$$

Además, si $\rho=\frac{I+\vec{r}\cdot\vec{\sigma}}{2}$ y $\sigma=\frac{I+\vec{s}\cdot\vec{\sigma}}{2}$ en la esfera de Bloch, entonces:

$$D(\rho,\sigma)=\frac{1}{4}tr\left|(\vec{r}-\vec{s})\cdot\vec{\sigma}\right|=\frac{|\vec{r}-\vec{s}|}{2}.$$

Y por tanto en la *esfera de Bloch* la distancia traza es la mitad de la distancia euclídea.

Además, esto nos sugiere que rotaciones en la *esfera de Bloch* dejan invariante la distancia traza, lo que inspira el siguiente resultado.

Lema 3.1. Sean ρ y σ dos operadores de densidad de un sistema $\mathcal{H}$ y U una transformación unitaria, entonces:

$$D(\rho,\sigma)=D(U\rho U^*,U\sigma U^*).$$

Demostración. Es inmediato a partir de las propiedades de la traza. ∎

Veamos una última interpretación.

Lema 3.2. Sean ρ y σ dos operadores de densidad de un sistema $\mathcal{H}$, entonces:

$$D(\rho,\sigma)=\max_P\ tr(P(\rho-\sigma)),$$

variando P entre las proyecciones positivas.

Dado que los elementos de una medición POVM son operadores positivos, la distancia traza puede verse como el máximo entre todos los P de la diferencia de probabilidad en una medición POVM con resultado P.

En lugar de probar el resultado anterior, probaremos el siguiente, que presenta una idea similar.

Teorema 3.1. *Sean ρ y σ dos operadores de densidad de un sistema $\mathcal{H}$ y $\{E_m\}$ un POVM con $p_m=tr(\rho E_m)$ y $q_m=tr(\sigma E_m)$ respectivas probabilidades, entonces*

$$D(\rho,\sigma)=\max_{\{E_m\}}\frac{1}{2}\sum_m|p_m-q_m|=\max_{\{E_m\}}D(p_i,q_i),$$

donde maximizamos entre todos los POVM.

Demostración. No demostraremos este resultado, pero la clave reside en que

$$D(\rho,\sigma) = \max_P tr(P(\rho-\sigma)),$$

donde maximizamos entre todas las proyecciones. Esta propiedad, además de aportar un nuevo significado a esta distancia será usada con bastante frecuencia. La demostración completa la encontraremos en [3](404-405).

Estas interpretaciones además de resultar útiles para visualizar nuestra distancia nos permiten comprobar que, de hecho, se trata de una distancia.

Lema 3.3. La *distancia traza* es una distancia.

Demostración. Está claro que

$$D(\rho,\sigma) = 0 \iff \rho = \sigma,$$

y que la distancia traza es simétrica, por lo que realmente sólo falta demostrar la desigualdad triangular. Para ello, hagamos notar que según hemos comentado en el teorema anterior, existe una proyección P tal que

$$D(\rho,\tau) = tr(P(\rho-\tau)) = tr(P(\rho-\sigma)) + tr(P(\sigma-\tau)) \leq D(\rho,\sigma) + D(\sigma,\tau).$$

Veamos ahora rápidamente algunas de las propiedades más interesantes de esta distancia, comenzando por el efecto que tienen las operaciones cuánticas en la distancia entre operadores de densidad.

Teorema 3.2. *Contractividad de las operaciones que preservan la traza. Sea $\mathcal{E}$ una operación que preserva la traza y σ y ρ dos operadores de densidad, entonces:*

$$D(\mathcal{E}(\rho),\mathcal{E}(\sigma)) \leq D(\rho,\sigma).$$

Demostración. Sea P la proyección tal que

$$D(\mathcal{E}(\rho),\mathcal{E}(\sigma)) = tr[P(\mathcal{E}(\rho)-\mathcal{E}(\sigma))].$$

Usando la descomposición espectral $\rho-\sigma = Q-S$ siendo Q y S matrices positivas sobre dominios ortogonales, sabemos que

$$tr(\rho)-tr(\sigma) = tr(Q)-tr(S) = 0,$$

y por tanto $tr(Q) = tr(S)$ y $tr(\mathcal{E}(Q)) = tr(\mathcal{E}(S))$ por lo que:

$$D(\rho,\sigma) = \frac{1}{2}tr|\rho-\sigma| = \frac{1}{2}tr(Q) - \frac{1}{2}tr(S) = tr(\mathcal{E}(Q)) \geq tr(P\mathcal{E}(Q)) \geq$$

$$tr(P(\mathcal{E}(Q)-\mathcal{E}(S))) = D(\mathcal{E}(\rho),\mathcal{E}(\sigma)).$$

Veamos finalmente una última propiedad de la *distancia traza* que nos permite comprobar la convexidad de la misma y otras propiedades relacionadas.

Teorema 3.3. *Convexidad fuerte de la distancia traza.*
Sean $\{p_i\}$ y $\{q_i\}$ dos distribuciones de probabilidad sobre los índices de σ_i y ρ_i operadores de densidad, entonces:

$$D\left(\sum_i p_i\rho_i, \sum_i q_i\sigma_i\right) \leq D(\{p_i\},\{q_i\}) + \sum_i p_i D(\rho_i,\sigma_i).$$

Demostración. Sea P la proyección tal que:

$$D\left(\sum_i p_i\rho_i, \sum_i q_i\sigma_i\right) = \sum_i p_i tr(P\rho_i) + \sum_i q_i tr(P\sigma_i) =$$

$$\sum_i p_i tr(P(\rho_i-\sigma_i)) + \sum_i (p_i-q_i)tr(P\sigma_i) \leq \sum_i p_i D(\rho_i,\sigma_i) + D(p_i,q_i).$$

3.1.2. Fidelidad.

Veamos ahora nuestra segunda medida, que en este caso no se trata de una distancia.

Definición 3.2. *Fidelidad.*
Se define la fidelidad entre dos operadores de densidad ρ y σ como:

$$F(\rho,\sigma) = tr\sqrt{\rho^{1/2}\sigma\rho^{1/2}}.$$

En principio no es evidente la utilidad de esta medida, que ni siquiera parece simétrica, así que veamos algunos casos especiales.

Observación 3.2. Si ρ y σ conmutan entonces son diagonales en la misma base y por tanto:

$$F(\rho,\sigma) = tr\sqrt{\sum_i r_i s_i |i\rangle\langle i|} = tr\left(\sum_i \sqrt{r_i s_i}|i\rangle\langle i|\right) = \sum_i \sqrt{r_i s_i} = F(\{r_i\},\{s_i\}),$$

donde definimos la fidelidad para distribuciones de probabilidad.

Además, sea $|\psi\rangle$ un estado puro:

$$F(|\psi\rangle,\rho) = \sqrt{\langle\psi|\rho|\psi\rangle}.$$

Al contrario que con la distancia traza, con la fidelidad no podemos dar una interpretación geométrica, pero aún así se puede comprobar que la medida es invariante al aplicar transformaciones unitarias.

Lema 3.4. Sean ρ y σ dos operadores de densidad y U una transformación unitaria, entonces:

$$F(\rho,\sigma) = F(U\rho U^*, U\sigma U^*).$$

Demostración. Es inmediato dado que $\sqrt{U\rho U^*} = U\sqrt{\rho}U^*$.

Veamos ahora una caracterización similar a la que dimos con la distancia traza.

Teorema 3.4. *Teorema de Uhlmann.*
Sean ρ y σ dos operadores de densidad en un sistema R y Q una copia de dicho sistema, entonces:

$$F(\rho,\sigma) = \max_{|\psi\rangle,|\varphi\rangle} |\langle\psi|\varphi\rangle|,$$

variando $|\psi\rangle$ y $|\varphi\rangle$ entre todas las posibles purificaciones de ρ y σ en RQ respectivamente.

Demostración. Podemos encontrar la prueba en [3](410-411).

Observación 3.3. Aunque este resultado no nos aporta una forma de calcular la fidelidad explícitamente, sí nos muestra toda una colección de interesantes consecuencias, entre las que podemos encontrar:

- La fidelidad es simétrica.
- $0 \leq F(\rho,\sigma) \leq 1$.
- Si $\rho = \sigma$, entonces $F(\rho,\sigma) = 1$.
- Si $\rho \neq \sigma$, entonces $F(\rho,\sigma) \leq 1$.
- $F(\rho,\sigma) = 0$ si y sólo si ρ y σ tienen sus dominios respectivos en subespacios ortogonales.

Además, gracias a este resultado podemos transformar la fidelidad en una distancia aprovechando que el ángulo entre estados sí conforma una distancia:

$$A(\rho,\sigma) = arccos(F(\rho,\sigma)).$$

Probemos para terminar algunas propiedades interesantes de la fidelidad.

Teorema 3.5. *Monotonía de la fidelidad.*
Sean ρ y σ operadores de densidad y $\mathcal{E}$ una operación que preserva la traza, entonces:

$$F(\mathcal{E}(\rho),\mathcal{E}(\sigma)) \geq F(\rho,\sigma).$$

Demostración. Sean $|\psi\rangle$ y $|\varphi\rangle$ purificaciones de ρ y σ en $R \otimes Q$ tales que

$$F(\rho,\sigma) = |\langle\psi|\varphi\rangle|.$$

Introducimos un sistema ambiente, E, para la operación cuántica que se encuentra originalmente en estado $|0\rangle$ y que interacciona con Q mediante la transformación U. Se puede comprobar que $U|\psi\rangle|0\rangle$ y $U|\varphi\rangle|0\rangle$ son

respectivamente purificaciones de $\mathcal{E}(\rho)$ y $\mathcal{E}(\sigma)$. Usando ahora el teorema de Uhlmann:

$$F(\mathcal{E}(\rho),\mathcal{E}(\sigma)) \geq |\langle 0|\langle\psi|U^*U|\varphi\rangle|0\rangle| = |\langle\psi|\varphi\rangle| = F(\rho,\sigma).$$

Esta propiedad se traducirá en la propiedad inversa en la distancia ángulo.

Teorema 3.6. *Concavidad fuerte de la fidelidad.*
Sean $\{p_i\}$ y $\{q_i\}$ distribuciones de probabilidad y $\{\rho_i\}$ y $\{\sigma_i\}$ operadores de densidad con la misma indexación, entonces:

$$F\left(\sum_i p_i\rho_i, \sum_i q_i\sigma_i\right) \geq \sum_i \sqrt{p_iq_i}F(\rho_i,\sigma_i).$$

Demostración. Sean $|\psi_i\rangle$ y $|\varphi_i\rangle$ purificaciones de ρ_i y σ_i elegidas de forma que $F(\rho_i,\sigma_i) = \langle\psi_i|\varphi_i\rangle$. Introduciendo ahora un sistema auxiliar con base ortonormal $|i\rangle$ correspondiente a los índices, podemos definir:

$$|\psi\rangle = \sum_i \sqrt{p_i}|\psi_i\rangle|i\rangle; \quad |\varphi\rangle = \sum_i \sqrt{q_i}|\varphi_i\rangle|i\rangle$$

purificaciones respectivas de $\sum_i p_i\rho_i$ y $\sum_i q_i\sigma_i$. Por la fórmula de Uhlmann:

$$F\left(\sum_i p_i\rho_i, \sum_i q_i\sigma_i\right) = |\langle\psi|\varphi\rangle| = \sum_i \sqrt{p_iq_i}\langle\psi_i|\varphi_i\rangle = \sum_i \sqrt{p_iq_i}F(\rho_i,\sigma_i).$$

Por último, veamos la relación entre ambas medidas:

Proposición 3.1. Equivalencia entre fidelidad y distancia traza.
Sean ρ y σ dos operadores de densidad, entonces:

$$1 - F(\rho,\sigma) \leq D(\rho,\sigma) \leq \sqrt{1 - F(\rho,\sigma)^2}.$$

Demostración. Para empezar veamos la equivalencia con dos estados puros $|a\rangle$ y $|b\rangle$. Usando Gram-Schmidt podemos encontrar una base ortonormal $\{|0\rangle,|1\rangle\}$ tal que

$$|a\rangle = |0\rangle, \quad |b\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle.$$

Dado que $F(|a\rangle,|b\rangle) = |\cos\theta|$, podemos comprobar que:

$$D(|a\rangle,|b\rangle) = \frac{1}{2}tr\left|\begin{bmatrix} 1-\cos^2\theta & -\cos\theta\sin\theta \\ -\cos\theta\sin\theta & -\sin^2\theta \end{bmatrix}\right|$$

$$= |\sin\theta| = \sqrt{1 - F(|a\rangle,|b\rangle)^2}.$$

Usando este resultado podemos encontrar las desigualdades para estados mixtos ρ y σ mediante dos purificaciones $|\psi\rangle$ y $|\varphi\rangle$ de los mismos tales que

$$F(|a\rangle, |b\rangle) = |\langle\psi|\varphi\rangle| = F(\rho, \sigma).$$

Gracias a esto es sencillo deducir:

$$D(\rho, \sigma) \leq D(|\psi\rangle, |\varphi\rangle) = F(\rho, \sigma).$$

Finalmente, para ver la otra desigualdad basta considerar un POVM $\{E_m\}$ tal que

$$F(\rho, \sigma) = \sum_m \sqrt{p_m, q_m},$$

siendo $p_m = tr(\rho E_m)$ y $q_m = tr(\sigma E_m)$ las probabilidades de cada resultado. En primer lugar

$$\sum_m (\sqrt{p_m} - \sqrt{q_m})^2 = \sum_m p_m + \sum_m q_m - 2F(\rho, \sigma) = 2(1 - F(\rho, \sigma)).$$

Pero por otro lado:

$$\sum_m (\sqrt{p_m} - \sqrt{q_m})^2 \leq \sum_m |\sqrt{p_m} - \sqrt{q_m}||\sqrt{p_m} + \sqrt{q_m}| =$$

$$\sum_m |p_m - q_m| = 2D(p_m, q_m) \leq 2D(\rho, \sigma).$$

Este resultado nos hace pensar que la distancia traza y la fidelidad son equivalentes a nivel cualitativo, y no importa realmente cuál de las dos usemos.

Capítulo 4

Corrección de errores cuánticos.

"Why is a raven like a writing desk?"
-Lewis Carroll.

Llegamos por fin a nuestro objetivo final: construir códigos correctores de errores cuánticos.

Para elaborarlos nos enfrentamos a tres problemas fundamentales que impiden desarrollar los códigos correctores de errores de forma análoga al caso clásico.

- No se puede clonar: como veremos más adelante, no es posible clonar un estado cuántico.
- Los errores son continuos: los posibles resultados de un error en computación cuántica son infinitos.
- Medir destruye la información: no es posible observar el estado cuántico sin cambiarlo.

4.1. Códigos específicos.

Veamos en primer lugar algunos ejemplos de códigos preparados para errores concretos que nos permitiran generalizar ciertas propiedades y definiciones.

4.1.1. Bit flip code.

Supongamos que tenemos un qubit en el estado $|\psi\rangle$. Este se ve afectado por un tipo concreto de ruido: con probabilidad $1-p$ el estado permanece igual y con probabilidad p se produce un bit flip $\sigma_X|\psi\rangle$, siendo σ_X la matriz de Pauli con respecto al eje X.

Para proteger nuestro qubit del error seguimos el siguiente algoritmo:

1. Codificación: en primer lugar, sea $|\psi\rangle = a|0\rangle + b|1\rangle$ codificamos nuestro estado en tres qubits:
$$|0\rangle \to |0_L\rangle = |000\rangle$$
$$|1\rangle \to |1_L\rangle = |111\rangle$$
Y obtenemos por tanto el estado codificado $|\tilde{\psi}\rangle = a|0_L\rangle + b|1_L\rangle$. Basta introducir un nuevo qubit $|0\rangle$ y aplicar la transformación unitaria CNOT dos veces consecutivas:
$$U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

2. Detección del error: tras la exposición al ruido, llevamos a cabo una medición para determinar qué tipo de error se ha producido, obteniendo un síndrome de error. En este caso tenemos 4 posibles síndromes:

   No hay error: $P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$.
   Bit flip en el primer qubit: $P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$.
   Bit flip en el segundo qubit: $P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$.
   Bit flip en el tercer qubit: $P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$.

   Proposición 4.1. Detección de errores.
   La medición cuántica $\{P_m\}_{m=0,1,2,3}$ permite detectar un error en el código definido anteriormente.

   Demostración. El proceso es análogo para cada uno de los posibles casos. Supongamos que se produce un único error un el primer qubit. En este caso el estado final es $|\psi'\rangle = a|100\rangle + b|011\rangle$, y como
   $$p(1) = \langle\psi'|P_1|\psi'\rangle = |a|^2 + |b|^2 = 1$$
   el único resultado posible de la medición es 1 y detectamos el error. ∎

   Corolario 4.1. Esta medición no altera el valor de nuestro estado compuesto.

3. Corrección del error: Aprovechando el corolario anterior podemos simplemente aplicar nuestra matriz σ_X para el qubit en el que se haya producido el error y obtener el estado original.

Observación 4.1. En primer lugar, aunque hayamos corregido el error, en ningún momento hemos obtenido información sobre los valores de a y b.
Por otro lado, comparando nuestro código con el código clásico por repetición, obtenemos un grado de eficacia análogo, ya que podemos detectar y corregir un error en ambos casos.
Además, sean $Z_1Z_2 = \sigma_Z \otimes \sigma_Z \otimes I$ y de forma análoga Z_2Z_3, la medición anterior equivale a hacer dos mediciones, según los observables Z_1Z_2 y Z_2Z_3,

comparando la primera los dos primeros qubits y la segunda el segundo y el tercero.
Usaremos de forma reiterada la notación anterior para describir el producto tensorial de matrices de Pauli.

Hagamos ahora un análisis de nuestro código. Para ello hemos de considerar que el mismo error no afecta igual a todos los estados, y por tanto, hemos de utilizar la fidelidad para analizar nuestro código.

Supongamos pues que tenemos un estado original $|\psi\rangle$ que se ve afectado por nuestro canal bit flip. El efecto del canal se puede medir según la operación cuántica

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

por lo que nuestro estado final será

$$\rho' = (1-p)|\psi\rangle\langle\psi| + p\sigma_X|\psi\rangle\langle\psi|\sigma_X.$$

Suponiendo que no llevamos a cabo ningún tipo de corrección, la fidelidad será:

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

El término $p\langle\psi|\sigma_X|\psi\rangle\langle\psi|\sigma_X|\psi\rangle$ es no negativo e igual a 0 cuando $|\psi\rangle = |0\rangle$ por lo que la fidelidad mínima (el peor de los casos) será $F = \sqrt{1-p}$.

Si aplicamos ahora nuestro código, sea $|\psi\rangle = a|000\rangle + b|111\rangle$, el resultado de la operación cuántica será

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

siendo el resto de términos operadores positivos que representan bit flips en dos o tres qubits. Gracias a esto podemos acotar la fidelidad por:

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

Y podemos llegar por tanto a la conclusión siguiente.

Proposición 4.2. Análisis del código.
Aplicar el código del bit flip mejora la fidelidad del resultado si $p < \frac{1}{2}$.

Demostración. Basta desarrollar la desigualdad anterior. ∎

4.1.2. Phase flip code.

Veamos un código más interesante. En este caso, el error al que se ve sometido nuestro canal es el del cambio de fase, es decir: con probabilidad $1-p$ el estado permanece igual y con probabilidad p el estado $|\psi\rangle = a|0\rangle + b|1\rangle$ se transforma en el estado

$$|\psi'\rangle = a|0\rangle - b|1\rangle = \sigma_Z|\psi\rangle,$$

siendo σ_Z la matriz de Pauli con respecto al eje Z.

En este caso nuestro ruido no tiene un equivalente clásico, pero veamos que podemos reducirlo a un canal bit flip.

Definición 4.1. *Canales unitariamente equivalentes.*
Decimos que dos canales de ruido son unitariamente equivalentes si existe una transformación unitaria que transforma uno en el otro, es decir, sean $\mathcal{E}_1$ y $\mathcal{E}_2$ dos canales, son unitariamente equivalentes si existe U unitaria tal que:

$$\mathcal{E}_1(\rho) = U\mathcal{E}_2(U\rho U^*)U^*.$$

Nuestro enunciado anterior se traduce pues en la siguiente afirmación.

Proposición 4.3. Equivalencia entre bit flip y phase flip.
Los canales de bit flip y phase flip son equivalentes.

Demostración. Basta tomar

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

la matriz de Hadamard. Dado que $\sigma_X = H\sigma_Z H$ el resultado es inmediato.

La importancia de esta equivalencia es que nos permite emplear el mismo código corrector de error para ambos canales. No podemos demostrar todavía este resultado ya que no hemos definido el concepto de código corrector de error cuántico, pero es fácil ver que el algoritmo descrito para el canal bit flip nos permite corregir errores para el canal phase flip.

En primer lugar debemos considerar la base ortogonal

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

y tomar $|0_L\rangle = |+++\rangle$ y $|1_L\rangle = |---\rangle$. Entonces la matriz σ_Z tiene un efecto de bit flip sobre esta base, por lo que podemos aplicar el mismo tipo de medición sobre esta nueva base tras la exposición del error. Tras la correción del error basta volver a la base original, lo que equivale a la transformación de la matriz de Hadamard.

4.2. El código de Shor.

Veamos por fin un código que nos permite protegernos de cualquier tipo de error, y que además destaca por su importancia histórica: *el código de Shor.*

El principio en el que se basa este código y que veremos a nivel formal más adelante es la llamada *discretización de errores.* Según este principio, a pesar de tener todo un continuo de errores en un qubit, estos se pueden expresar a partir de un subconjunto discreto de esos errores de forma que basta corregir estos últimos para corregir cualquier error. Dicho de otra forma, tenemos el siguiente resultado:

Lema 4.1. Supongamos que tenemos un canal con ruido representado por $\{E_k\}$ operadores suma, entonces cada E_k puede expresarse como combinación de I, σ_X, σ_Z y $\sigma_X\sigma_Z$:

$$E_k = e_{k0}I + e_{k1}\sigma_X + e_{k2}\sigma_Z + e_{k3}\sigma_X\sigma_Z.$$

La prueba es evidente dado que los cuatro operadores considerados son linealmente independientes.

Veamos ahora el algoritmo que debemos seguir para aplicar nuestro código, que nos permitirá corregir un error.

1. Codificación: En primer lugar, sea $|\psi\rangle = a|0\rangle + b|\psi\rangle$ nuestro estado original, aplicamos en primer lugar el phase flip code y luego el bit flip code, obteniendo:

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

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

   Este es lo que llamamos concatenación de códigos.
2. Detección de errores: Veamos el siguiente resultado.

   Proposición 4.4. Esta codificación nos permite detectar errores de bit flip, phase flip y también ambos simultáneamente en un qubit.

   Demostración. Primero debemos llevar a cabo mediciones de la forma Z_1Z_2 y Z_2Z_3 para cada bloque de qubits, que nos detectan los bit flips. Tras esto, llevamos a cabo una medición con respecto a los observables $\prod_{1\leq i\leq 6} X_i$ y $\prod_{4\leq i\leq 9} X_i$ para encontrar phase flips. ∎

3. Corrección: Para corregir los bit flips procedemos como en el código bit flip. Para corregir los phase flips basta aplicar el operador $Z_1Z_2Z_3$.

Tras ver nuestro primer ejemplo de código y habernos familiarizado con el problema que tenemos entre manos, procedamos ahora a formalizar la teoría de códigos correctores de errores cuánticos.

4.3. Teoría de códigos.

Definición 4.2. *Código corrector cuántico.*
Sea $\mathcal{E}$ un canal cuántico, un código corrector cuántico *es un subespacio $\mathcal{C}$ de un espacio de Hilbert $\mathcal{H}$*

Observación 4.2. Será relevante el papel de la proyección ortogonal en nuestro código, que notaremos $P_{\mathcal{C}}$ de forma estándar.

Análogamente a los casos que hemos estudiado hasta ahora, dado un estado cualquiera, en primer lo codificaremos por un elemento de $\mathcal{C}$. Tras esto se verá afectado por el ruido del canal y finalmente llevaremos a cabo una medición para determinar el error y corregirlo.

Definición 4.3. *Operación de recuperación.*
Sea $\mathcal{E}$ un canal con ruido y $\mathcal{C}$ un código, diremos que $\mathcal{R}$ es una operación de recuperación *si $\mathcal{R}$ es una operación cuántica que preserva la traza y además:*

$$(\mathcal{R} \circ \mathcal{E})(\rho) = \rho \quad \forall \rho = P_{\mathcal{C}} \rho P_{\mathcal{C}}.$$

Veamos ahora las condiciones necesarias para la existencia de una operación de recuperación en un código.

Teorema 4.1. *Condiciones para la corrección de errores.*
Sea $\mathcal{E}$ un canal con elementos $\{E_k\}$ y $\mathcal{C}$ un código, entonces la condición necesaria y suficiente para la existencia de una operación de corrección $\mathcal{R}$ es:

$$P_{\mathcal{C}} E_i^* E_j P_{\mathcal{C}} = a_{ij} P_{\mathcal{C}},$$

para alguna matriz hermítica $A = (a_{ij})$. Llamamos a los $\{E_k\}$ errores, y decimos que son corregibles si cumplen la condición.

Demostración. Veamos en primer lugar la condición suficiente. Dado que A es un operador hermítico, podemos diagonalizarlo mediante una matriz unitaria U: $D = U^* A U$ con D diagonal. Considerando ahora $F_k = \sum_i u_{ik} E_i$, por el Teorema 3.2 sabemos que $\{F_k\}$ es también un conjunto de operadores de $\mathcal{E}$, y sustituyendo encontramos que

$$P_{\mathcal{C}} F_k^* F_l P_{\mathcal{C}} = \sum_{ij} u_{ki}^* u_{jl} P_{\mathcal{C}} E_i^* E_j P_{\mathcal{C}} = \sum_{ij} u_{ki}^* a_{ij} u_{jl} P_{\mathcal{C}} = d_{kl} P_{\mathcal{C}},$$

por lo que obtenemos otros errores $\{F_k\}$ que simplifican las condiciones. Considerando ahora las matrices $F_k P_{\mathcal{C}}$, para cada una de ellas podemos aplicar la descomposición polar y hallar por tanto una matriz unitaria V_k tal que

$$F_k P_{\mathcal{C}} = V_k \sqrt{P_{\mathcal{C}} F_k^* F_k P_{\mathcal{C}}} = \sqrt{d_{kk}} V_k P_{\mathcal{C}}.$$

Definiendo ahora las nuevas proyecciones ortogonales

$$P_k = V_k P_{\mathcal{C}} V_k^* = \frac{F_k P_{\mathcal{C}} V_k^*}{\sqrt{d_{kk}}}$$

cada uno de estos proyectores determina un subespacio que será ortogonal al resto, ya que:

$$P_l^* P_k = \frac{V_l P_{\mathcal{C}} F_l^* F_k P_{\mathcal{C}} V_k^*}{\sqrt{d_{ll} d_{kk}}} = 0.$$

Basta ahora aplicar una corrección en dos pasos: detección de error mediante las proyecciones P_k (añadiendo si es necesario uno más para obtener la

relación de completitud) y recuperando el estado original tras aplicar V_k^*. Es decir, la operación de recuperación es:

$$\mathcal{R}(\sigma) = \sum_k V_k^* P_k \sigma P_k V_k.$$

Y podemos comprobar fácilmente que $\mathcal{R}(\mathcal{E}(\sigma)) = \sigma$ como estado.

Veamos ahora la condición necesaria, y para ello consideremos un conjunto de errores $\{E_i\}$ corregible por una operación $\mathcal{R}$ de elementos $\{R_j\}$.

Tomando ahora una nueva operación cuántica dada por $\mathcal{E}_\mathcal{C}(\sigma) = \mathcal{E}(P_\mathcal{C}\sigma P_\mathcal{C})$, sabemos que $\mathcal{R}(\mathcal{E}_\mathcal{C}(\sigma)) = P_\mathcal{C}\sigma P_\mathcal{C}$ como estado, y además por linealidad el factor de proporcionalidad es constante para todo σ, por lo que podemos reescribir la ecuación como:

$$\sum_{ij} R_j E_i P_\mathcal{C} \sigma P_\mathcal{C} E_i^* R_j^* = c P_\mathcal{C} \sigma P_\mathcal{C}.$$

Y por el Teorema 3.2 obtenemos la existencia de $\{c_{ki}\}$ tales que

$$R_k E_i P_\mathcal{C} = c_{ki} P_\mathcal{C},$$

y obtenemos por tanto

$$P_\mathcal{C} E_i^* R_k^* R_k E_j P_\mathcal{C} = c_{ki}^* c_{kj} P_\mathcal{C}.$$

Finalmente, dado que $\mathcal{R}$ es una operación que preserva la traza, podemos sumar en el índice k y obtener las condiciones buscadas:

$$P_\mathcal{C} E_i^* E_j P_\mathcal{C} = a_{ij} P_\mathcal{C},$$

con $a_{ij} = \sum_k c_{ki}^* c_{kj}$.

Estas condiciones son útiles pero verificarlas cuesta mucho tiempo, por lo que intentaremos construir ciertas familias de códigos a partir de ellas para evitar esta comprobación.

4.3.1. Discretización de errores.

Procedamos ahora a formalizar el concepto de discretización de errores que hemos introducido anteriormente usando el siguiente teorema.

Teorema 4.2. *Corrección de errores dependientes.*
Sea $\mathcal{C}$ un código y $\mathcal{R}$ la operación de recuperación construida según el teorema anterior para corregir el canal $\mathcal{E}$ de elementos $\{E_i\}$. Sea ahora $\mathcal{F}$ otra operación cuántica de elementos $\{F_j\}$ dependientes de los $\{E_i\}$, es decir, tales que $F_j = \sum_i m_{ji} E_i$ para todo j, siendo los m_{ji} números complejos. En estas condiciones, $\mathcal{R}$ corrige los efectos de $\mathcal{F}$ en el código $\mathcal{C}$.

Demostración. Sin pérdida de generalidad supongamos que se satisfacen las condiciones

$$P_{\mathcal{C}} E_i E_j^* P_{\mathcal{C}} = d_{ij} P_{\mathcal{C}}$$

con (d_{ij}) matriz diagonal. Además $\mathcal{R}$ tiene por elementos $V_k^* P_k$, que cumplen para todo σ:

$$V_k^* P_k E_i \sqrt{\sigma} = \frac{V_k^* V_k P_{\mathcal{C}} E_k^* E_i P_{\mathcal{C}} \sqrt{\sigma}}{\sqrt{d_{kk}}} = \delta_{ki} \sqrt{d_{kk}} \sqrt{\sigma}.$$

Sustituyendo ahora $F_j = \sum_i m_{ji} E_i$:

$$V_k^* P_k F_j \sqrt{\sigma} = \sum_i m_{ji} \delta_{ki} \sqrt{d_{kk}} \sqrt{\sigma} = m_{jk} \sqrt{d_{kk}} \sqrt{\sigma},$$

y por lo tanto:

$$\mathcal{R}(\mathcal{F}(\sigma)) = \sum_{kj} V_k^* P_k F_j \sigma F_j^* P_k V_k = \sum_{kj} |m_{jk}|^2 d_{kk} \sigma.$$

Recuperamos de esta forma el estado original, por lo que probamos el resultado. ∎

Gracias a este resultado podemos hablar de los elementos $\{E_i\}$ como errores en lugar de trabajar con las operaciones.

De esta forma, para demostrar que el código de Shor permite corregir cualquier error sobre un qubit basta comprobar las condiciones de corrección de errores para las matrices de Pauli y la identidad.

Recapitulando, gracias a los dos últimos teoremas podemos derrotar a una cantidad continua de errores centrándonos en ganar la batalla frente una cantidad discreta de ellos.

4.3.2. Códigos no degenerados.

En la corrección de errores cuántica se produce un curioso fenómeno, según el cual diferentes errores pueden dar lugar al mismo resultado al aplicarse a elementos del código. Este es el caso del código de Shor, en el cual los errores Z_1 y Z_2 (siguiendo la notación que introdujimos al inicio del capítulo) dan lugar al mismo resultado.

Esto inspira la siguiente definición:

Definición 4.4. *Códigos no degenerados.*
Un código se dice que es no degenerado si al aplicar diferentes errores a un elemento del código obtenemos resultados diferentes.

La importancia de los códigos degenerados radica en que son capaces de incorporar más información que los códigos usuales, aunque por contra no cumplen cotas como la que veremos a continuación.

4.3.3. Cota de Hamming cuántica.

Proposición 4.5. Cota de Hamming cuántica.
Sea $\mathcal{C}$ un código no degenerado que codifica k qubits en n qubits y capaz de corregir t o menos errores, entonces:

$$\sum_{j=0}^{t} \binom{n}{j} 3^j 2^k \leq 2^n.$$

Demostración. Como en el caso clásico, la prueba consiste en hacer un conteo de la contidad de posibles errores, y dado que el código es no degenerado otorgarle a cada error un subespacio de dimensión 2^k dentro de nuestro espacio de dimensión 2^n. Para cada $j \leq t$ habrá $\binom{n}{j}$ posiciones en las que pueden ocurrir los errores, y dado que consideramos 3 posibles errores por qubit (las matrices de Pauli) obtenemos:

$$\sum_{j=0}^{t} \binom{n}{j} 3^j$$

posibles errores, de donde deducimos la desigualdad. ∎

Más adelante veremos más cotas que satisfacen también los códigos degenerados.

4.4. Contrucción de códigos cuánticos.

Por fin vamos a conocer a los actores de los que habla nuestra historia. En primer lugar vamos a construir una familia de códigos llamada *códigos Calderbank-Shor-Steane* o códigos *CSS*, que constituirán una subfamilia de *códigos estabilizadores*, los cuáles introduciremos más adelante.

4.4.1. Códigos CSS.

Vamos a introducir la situación en la que nos encontraremos a lo largo de la sección. En primer lugar vamos a tomar dos códigos correctores de errores lineales clásicos binarios $\mathcal{C}_1$ de tipo $[n, k_1]$ y $\mathcal{C}_2$ de tipo $[n, k_2]$, es decir, que usan n bits para codificar k_1 y k_2 bits de información respectivamente, tales que $\mathcal{C}_2 \subset \mathcal{C}_1$ y que tanto $\mathcal{C}_1$ como $\mathcal{C}_2^{\perp}$ corrijan t errores, siendo $\mathcal{C}_2$ el código dual a $\mathcal{C}_2$.

Comencemos por asociar a cada elemento de $\mathcal{C}_1$ un estado cuántico.

Definición 4.5. *Estado cuántico asociado.*
Sea $x \in \mathcal{C}_1$ un elemento de nuestro código, definimos su estado cuántico asociado por $\mathcal{C}_2$ como:

$$|x + \mathcal{C}_2\rangle = \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y \in \mathcal{C}_2} |x + y\rangle.$$

Tomando + como la adición bit a bit módulo 2 como es habitual.

El interés de esta definición se muestra con el siguiente resultado.

Lema 4.2. Recogiendo la notación anterior, sea $x' \in \mathcal{C}_1$, entonces $x - x' \in \mathcal{C}_2$ si y sólo si $|x + \mathcal{C}_2\rangle = |x' + \mathcal{C}_2\rangle$.

Observación 4.3. La demostración es inmediata y nos permite establecer una identificación biyectiva entre el conjunto de estados cuánticos resultantes y $\mathcal{C}_1/\mathcal{C}_2$, lo que justifica nuestra notación anterior. Además, este resultado también implica que dos estados asociados diferentes son ortogonales.

Definición 4.6. *Código CSS.*
En las condiciones anteriores, definimos como el código $CSS(\mathcal{C}_1, \mathcal{C}_2)$ *al subespacio generado por los elementos* $\{x + \mathcal{C}_2 \mid x \in \mathcal{C}_1\}$ *en el espacio total de dimensión* 2^n.

Lema 4.3. Según la notación anterior, nuestro código $CSS(\mathcal{C}_1, \mathcal{C}_2)$ es de tipo $[n, k_1 - k_2]$.

Demostración. El conjunto de clases de $\mathcal{C}_1/\mathcal{C}_2$ es $|\mathcal{C}_1|/|\mathcal{C}_2| = 2^{k_1 - k_2}$ por lo que la dimensión de $CSS(\mathcal{C}_1, \mathcal{C}_2)$ es $2^{k_1 - k_2}$.

Veamos ahora el poder que se esconde dentro de nuestro nuevo código.

Teorema 4.3. *Corrección de errores del código CSS.*
Recogiendo la notación ya establecida, el código $CSS(\mathcal{C}_1, \mathcal{C}_2)$ *puede corregir hasta* t *errores de los tipos bit flip o phase flip.*

Demostración. Sea $|x + \mathcal{C}_2\rangle$ el estado original, e_1 un vector de n bits representando lo errores de bit flip y e_2 un vector de n bits representando los phase flips, entonces el estado tras los errores será:

$$\frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y \in \mathcal{C}_2} (-1)^{(x+y)\cdot e_2} |x + y + e_1\rangle.$$

Para llevar a cabo la detección del error será necesario introducir un nuevo sistema cuántico, que comenzará en estado $|0\rangle$, obteniendo el estado total:

$$\frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y \in \mathcal{C}_2} (-1)^{(x+y)\cdot e_2} |x + y + e_1\rangle |0\rangle.$$

Tras esto, llevamos nuestro nuevo estado al anterior y aplicamos la matriz de paridad H_1 del código $\mathcal{C}_1$, obteniendo:

$$\frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y \in \mathcal{C}_2} (-1)^{(x+y)\cdot e_2} |x + y + e_1\rangle |H_1 e_1\rangle,$$

ya que $x + y \in \mathcal{C}_1$. Tras esto podemos medir el sistema adicional que hemos añadido, obtener el valor de $H_1 e_1$ y descartar el sistema, para finalmente

aplicar matrices σ_X en los valores que hallan sufrido bit flip para revertirlo. Para detectar ahora los errores phase flip aplicamos matrices de Hadamard a cada qubit, obteniendo:

$$\frac{1}{\sqrt{|\mathcal{C}_2|2^n}} \sum_z \sum_{y \in \mathcal{C}_2} (-1)^{(x+y)\cdot(e_2+z)} |z\rangle,$$

donde z toma por valores todos los vectores de n bits. Tomando ahora $z' = z + e_2$:

$$\frac{1}{\sqrt{|\mathcal{C}_2|2^n}} \sum_{z'} \sum_{y \in \mathcal{C}_2} (-1)^{(x+y)\cdot z'} |z' + e_2\rangle.$$

Y sabiendo ahora que cuando $z' \in \mathcal{C}_2^\perp$ se cumple que

$$\sum_{y \in \mathcal{C}_2} (-1)^{y \cdot z'} = |\mathcal{C}_2|,$$

mientras que en caso contrario

$$\sum_{y \in \mathcal{C}_2} (-1)^{y \cdot z'} = 0,$$

por lo que obtenemos el estado:

$$\sqrt{\frac{|\mathcal{C}_2|}{2^n}} \sum_{z' \in \mathcal{C}_2^\perp} (-1)^{x \cdot z'} |z' + e_2\rangle,$$

que no es más que un estado en el que ha ocurrido un error del tipo bit flip dado por e_2, que era nuestro objetivo al multiplicar por las matrices de Hadamard siguiendo el ejemplo que vimos al inicio del capítulo. Aplicamos el mismo método que usamos anteriormente para corregir este error, aunque en este caso usando el código $\mathcal{C}_2^\perp$ y su matriz de paridad, obteniendo finalmente el estado corregido:

$$\sqrt{\frac{|\mathcal{C}_2|}{2^n}} \sum_{z' \in \mathcal{C}_2^\perp} (-1)^{x \cdot z'} |z'\rangle.$$

Como era de esperar, tras volver a aplicar matrices de Hadamard en cada qubit obtenemos el estado original.

Observación 4.4. Como hemos podido comprobar en la demostración, se pueden corregir tantos errores del tipo bit flip como errores pueda corregir $\mathcal{C}_1$, y tantos del tipo phase flip como pueda corregir $\mathcal{C}_2$.

Una importante consecuencia de este tipo de códigos es la cota de Gilbert-Varshamov para códigos cuánticos, que nos asegura la existencia de buenos códigos CSS.

4.4.2. El códgo de Steane.

Veamos ahora un ejemplo de este tipo de códigos: el *código de Steane*. Para construir este código, debemos definir en primer lugar nuestros códigos lineales clásicos. $\mathcal{C}$ será el código de Hamming $[7, 4, 3]$ con matriz de paridad:

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Tomaremos ahora $\mathcal{C}_1 = \mathcal{C}$ y $\mathcal{C}_2 = \mathcal{C}^{\perp}$, siendo sencillo comprobar que $\mathcal{C}_2 \subset \mathcal{C}_1$. Además ambos códigos tienen distancia mínima tres, por lo que pueden corregir un error.

Definición 4.7. *Código de Steane.*
Recogiendo el desarrollo anterior, definiremos el código de Steane como $CSS(\mathcal{C}_1, \mathcal{C}_2)$.

Observación 4.5. El código de Steane será por tanto un código $[7, 1]$. Además, se puede comprobar que:

$$\begin{aligned} |0_L\rangle = \frac{1}{\sqrt{8}}\big(&|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\ &+|0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle\big). \\ |1_L\rangle = \frac{1}{\sqrt{8}}\big(&|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \\ &+|1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle\big). \end{aligned}$$

4.5. Códigos estabilizadores.

Pasemos a tratar la herramienta más poderosa con la que contamos para construir códigos cuánticos y que nos permitirá construir toda una familia de códigos que contendrá a los códigos CSS. Estos códigos serán los *códigos estabilizadores* y la herramienta que emplearemos será el llamado *formalismo de estabilizadores*.

4.5.1. Formalismo de estabilizadores.

Veamos qué queremos decir con estabilizador.

Definición 4.8. *Estabilizador.*
Un operador S *es un estabilizador del estado* $|\psi\rangle$ *si* $S|\psi\rangle = |\psi\rangle$.

La utilidad de estos estabilizadores se basa en el uso de los *grupos de Pauli*, que nos permiten trabajar con una cantidad limitada de operadores.

Definición 4.9. *Grupos de Pauli G_n.*
Definiremos estos grupos de forma recursiva:

1. *El primer grupo de Pauli será el generado por las matrices de Pauli:*

$$G_1 = \{\pm I, \pm iI, \pm\sigma_X, \pm i\sigma_X, \pm\sigma_Y, \pm i\sigma_Y, \pm\sigma_Z, \pm i\sigma_Z\}.$$

   Se trata de un grupo no abeliano y nilpotente isomorfo a $(\mathbb{Z}/_{\mathbb{Z}4} \times \mathbb{Z}/_{\mathbb{Z}2}) \rtimes \mathbb{Z}/_{\mathbb{Z}2}$.
2. *Cada grupo de Pauli generalizado, G_n, estará conformado por todos los productos tensoriales de n términos de G_1.*

Veamos ahora la definición de estabilizadores de forma más precisa:

Definición 4.10. *Subespacio de vectores estabilizados.*
Sea $S \subset G_n$ un subgrupo, llamaremos subespacio de vectores estabilizados por S, V_S, al conjunto de qubits de longitud n estabilizados por S.

Lema 4.4. En las condiciones anteriores, V_S es un subespacio vectorial.

Este resultado inmediato justifica el uso de dicha palabra en la definición.

La importancia de introducir la estructura de grupo es que en lugar de probar que todo elemento de S estabiliza nuestro estado basta con hacerlo para los generadores del grupo, lo que facilita enormemente la tarea.

El objetivo principal ahora es estudiar el subespacio V_S en función de los generadores de S , tarea que comenzaremos por la siguiente proposición.

Proposición 4.6. Condición necesaria para que V_S sea no trivial.
En las condiciones anteriores, si $V_S \neq \{0\}$, entonces los elementos de S conmutan y además $-I \notin S$.

Demostración. La base de esta prueba y las posteriores es que las matrices de Pauli o bien conmutan o bien anticonmutan, por lo que dos operadores N y M construidos por productos tensoriales de matrices de Pauli o bien conmutarán o bien cumplirán $NM = -MN$. Volviendo ahora a la proposición, sea $|\psi\rangle \in V_S$ distinto de 0 y $M, N \in S$. Si estos operadores no conmutan tenemos la siguiente igualdad:

$$|\psi\rangle = MN|\psi\rangle = -NM|\psi\rangle = -|\psi\rangle,$$

lo que es una evidente contradicción porque hemos supuesto $|\psi\rangle$ distinto de 0. De la misma forma, si $-I \in S$, entonces:

$$|\psi\rangle = -I|\psi\rangle = -|\psi\rangle.$$

Y llegamos a la misma contradicción.

Para ver la condición suficiente necesitamos las herramientas que introducimos a continuación.

Definición 4.11. *Matriz de comprobación.*
Sea $S = \langle g_1, \ldots, g_l \rangle$ un subgrupo de Pauli, definimos la matriz de comprobación como la matriz $l \times 2n$ cuyas filas corresponden a los generadores ordenados. La parte izquierda de la matriz contiene unos para indicar la presencia de σ_X en cierta posición del producto tensorial, mientras que la parte derecha hará lo mismo con la matriz σ_Z. La presencia de unos en ambos lados en la misma posición indicará la presencia de σ_Y, mientras que si hay cero en ambas posiciones el operador representado será I.

Observación 4.6. La matriz de comprobación no nos dice nada sobre los factores multiplicativos que acompañan a los operadores. También podemos considerar por separado la representación de cada generador g_i por un vector de dimensión $2n$ que denotaremos $r(g_i)$, y que se corresponde con la i-ésima fila de la matriz de comprobación.

Proposición 4.7. Conmutatividad de elementos del grupo.
Sean $g, g' \in G_n$ dos elementos del grupo de Pauli, estos conmutarán si y sólo si $r(g)\Lambda r(g')^T = 0$, siendo Λ la matriz $2n \times 2n$ dada por:

$$\Lambda = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix},$$

donde I representa la matriz identidad de orden n. Toda la aritmética se llevará a cabo módulo 2.

Demostración. La prueba nuevamente se basa en que las matrices de Pauli anticonmutan si son diferentes, por lo que necesitaremos contabilizar la cantidad de factores que, ocupando la misma posición, vienen dados por matrices de Pauli diferentes, que es exactamente lo que realiza la expresión $r(g)\Lambda r(g')^T = 0$, ya que si tomamos $r(g) = M$ y $r(g') = N$ y dividimos en las dos partes correspondientes:

$$\begin{pmatrix} N_1 & N_2 \end{pmatrix} \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} \begin{pmatrix} M_1 \\ M_2 \end{pmatrix} = \begin{pmatrix} N_2 & N_1 \end{pmatrix} \begin{pmatrix} M_1 \\ M_2 \end{pmatrix} = N_2 \cdot M_1 + N_1 \cdot M_2.$$

Para probar que un subgrupo S conmuta bastará probar este resultado para los generadores.

Continuemos con la batería de resultados que conformarán las baldosas de nuestro camino.

Proposición 4.8. Independencia de los generadores.
Sea $S = \langle g_1, \ldots, g_l \rangle$ tal que $-I \notin S$, entonces los generadores son independientes si y sólo si las correspondientes filas $\{r(g_1), \ldots, r(g_l)\}$ lo son.

Demostración. En primer lugar, cabe destacar que $r(g) + r(g') = r(gg')$ por las propiedades de las matrices de Pauli, y por tanto:

$$\sum_i a_i r(g_i) = 0 \text{ con } a_j \neq 0 \iff \prod_i g_i^{a_i} = I.$$

No hay ningún factor delante de la identidad por la condición de que $-I \notin S$. Además, $g_i^2 = I$ para todo i, y por tanto:

$$g_j = g_j^{-1} = \prod_{i \neq j} g_i^{a_i},$$

y tenemos la relación.

Proposición 4.9. Sea $S = \rangle g_1, \ldots, g_l \langle$ tal que $-I \notin S$ y los generadores sean independientes, entonces para todo índice $i \in \{1, \ldots, l\}$ podemos encontrar $g \in S$ tal que:

- $g g_i g^T = -g_i$.
- $g g_j g^T = g_j, \quad \forall j \neq i$.

Demostración. Sea G la matriz de comprobación, dado que los generadores son linealmente independientes, se sigue de la Proposición 5.8 que sus filas son linealmente independientes. Por tanto, para todo e_i vector de la base canónica podremos encontrar un x tal que $G\Lambda x = e_i$, siendo Λ la matriz anteriormente definida.

Tomando ahora g tal que $r(g) = x^T$ es inmediato comprobar que cumple nuestras condiciones por la Proposición 5.7.

Y finalmente llegamos a la condición suficiente que buscábamos probar.

Proposición 4.10. Condición suficiente para que V_S sea no trivial. Sea $S = \langle g_1, \ldots, g_{n-k} \rangle$ tal que $-I \notin S$ y los $n-k$ generadores sean independientes, entonces V_S es un subespacio de dimensión 2^k.

Demostración. En primer lugar debemos definir para cada $x \in (\mathcal{F}_2)^{n-k}$ el operador:

$$P_S^x = \frac{\prod_{j=1}^{n-k} (I + (-1)^{x_j} g_j)}{2^{n-k}}.$$

Analizando cada uno de estos factores, podemos comprobar que $(I + g_j)/2$ es la proyección sobre el subespacio propio de autovalor $+1$ de g_j, por lo que $P_S^{(0,\ldots,0)}$ es la proyección sobre V_S.

Es más, para distintos x tendremos P_S^x ortogonales, por lo que usando

$$I = \sum_x P_S^x,$$

tenemos al lado derecho una proyección en un espacio de dimensión 2^n, mientras que a la izquierda tenemos 2^{n-k} proyecciones ortogonales que tienen la misma dimensión al ser conjugados según la Proposición 5.9, por lo que cada subespacio y en concreto V_S tendrán dimensión 2^k.

4.5.2. Transformaciones unitarias en el formalismo de los estabilizadores.

Hasta ahora hemos sido capaces de representar subespacios mediante grupos de estabilizadores, pero para cumplir nuestro objetivo de usar este formalismo para corregir errores esto no será suficiente. Tendremos que ver la forma de representar transformaciones unitarias y mediciones según este proceso.

Proposición 4.11. Transformaciones unitarias y estabilizadores.
Sea V_S el subespacio estabilizado por el subgrupo S y U una transformación unitaria, entonces UV_S será estabilizado por el subgrupo USU^T.
Además, si S está generado por $g_1, \ldots, g_l$, entonces USU^T vendrá generado por $Ug_1U^T, \ldots, Ug_lU^T$.

Demostración. Sean $|\psi\rangle \in V_S$ y $g \in S$ se cumple que:

$$U|\psi\rangle = Ug|\psi\rangle = UgU^TU|\psi\rangle,$$

por lo que UgU^T estabiliza Ug.

Veamos ahora un poco del poder de este formalismo.

Definición 4.12. *Normalizador.*
Llamamos normalizador de G_n, $N(G_n)$, al conjunto de las transformaciones unitarias tales que $UG_nU^T = G_n$.

Teorema 4.4. *Composición de $N(G_n)$.*
Sea $U \in N(G_n)$, entonces U se puede escribir como composición de una cantidad del orden de $\mathcal{O}(n^2)$ operadores de los tipos Hadamard, C-NOT y Fase, donde

$$U_{Fase} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}.$$

Demostración. La prueba se realiza por inducción sobre n.

La importancia de este resultado radica en que podemos llevar a cabo corrección de errores usando únicamente esta clase de operadores como veremos más adelante.

4.5.3. Mediciones en el formalismo de estabilizadores.

Veamos ahora cómo podemos representar una medición con el formalismo de los estabilizadores.

Proposición 4.12. Medición en el formalismo de los estabilizadores.
Sea $g \in G_n$, dado que se trata de un operador hermítico podemos llevar a cabo una medición tomando g como observador. Suponemos que el sistema está en estado $|\psi\rangle$ con estabilizador $\langle g_1, \ldots, g_n\rangle$. En ese caso tenemos dos posibilidades:

- g conmuta con todos los generadores.
- g conmuta con todos los generadores menos con g_1, con quien anticonmuta.

En el primer caso no cambia el estado tras la medición y por tanto tampoco los estabilizadores, obteniendo el resultado $+1$ o -1 con probabilidad 1.

En el segundo supuesto obtenemos el resultado $+1$ con probabilidad $1/2$ siendo el grupo estabilizador tras la medición será $\langle g, g_2, \ldots, g_n\rangle$, y el resultado -1 con probabilidad $1/2$, obteniendo el grupo estabilizador final $\langle -g, g_2, \ldots, g_n\rangle$.

Demostración. Supongamos sin pérdida de generalidad que g es producto de matrices de Pauli sin factores.

Comencemos con el primer caso, en el cual o bien g estabiliza $|\psi\rangle$ o bien lo hace $-g$, ya que para todo generador:

$$g_j g|\psi\rangle = g g_j|\psi\rangle = g|\psi\rangle.$$

Y por tanto $g|\psi\rangle \in V_S$ por lo que $|\psi\rangle$ es múltiplo de $|\psi\rangle$. Como además $g^2 = I$ es evidente que o bien $g \in S$ o bien $-g \in S$. Supongamos que se trata de g (el razonamiento para $-g$ es análogo), en este caso el estado no cambia tras la medición y obtenemos como resultado $+1$ (análogamente -1) con probabilidad 1.

Cambiemos ahora al segundo caso. En primer lugar, si g anticonmutase con algún otro generador distinto de g_1 bastaría con cambiar dicho generador, g_j, por un nuevo generador gg_j, por lo que nuestros casos son exhaustivos. Estudiemos ahora el caso. En primer lugar, g tendrá autovalores ± 1, por lo que los proyectores serán $(I \pm g)/2$ respectivamente y las probabilidades:

$$p(+1) = tr\left(\frac{I+g}{2}|\psi\rangle\langle\psi|\right).$$

$$p(-1) = tr\left(\frac{I-g}{2}|\psi\rangle\langle\psi|\right).$$

Y usando que $g_1|\psi\rangle = g_1$ y que $gg_1 = -g_1 g$ podemos concluir:

$$p(+1) = tr\left(\frac{I+g}{2}g_1|\psi\rangle\langle\psi|\right) = tr\left(g_1\frac{I-g}{2}|\psi\rangle\langle\psi|\right) =$$

$$tr\left(\frac{I-g}{2}|\psi\rangle\langle\psi|\right) = p(-1).$$

Y dado que $p(+1) + p(-1) = 1$ tenemos nuestro resultado:
$p(+1) = p(-1) = 1/2$.
Los estados finales serán:

$$|\psi^{\pm}\rangle = \frac{(I \pm g)|\psi\rangle}{\sqrt{2}},$$

lo que concuerda con los estabilizadores que habíamos propuesto. ∎

4.5.4. El Teorema de Gottesman-Knill.

Podemos resumir todos nuestros resultados en el siguiente teorema.

Teorema 4.5. *Teorema de Gottesman-Knill.*
Se puede simular de forma eficiente en un ordenador clásico cualquier tipo de computación cuántica que incluya unicamente el uso las transformaciones unitarias U_{CNOT}, U_{Fase} o la puerta de Hadamard y las mediciones según observables en el grupo de Pauli.

La demostración de este resultado es todo el desarrollo que hemos hecho hasta ahora.

El interés de este resultado es que podemos simular operaciones con un alto grado de *entrelazamiento*, como la *teleportación cuántica* o el *superdense coding*, usando un ordenador clásico. Es obvio que existen otro tipo de operaciones que no podremos representar de forma eficiente con el formalismo de los estabilizadores, pero será suficiente para desarrollar una amplia variedad de códgos correctores de errores.

4.5.5. Construcción de códigos estabilizadores.

Centrémonos por fin en la tarea de construir códigos usando el formalismo de los estabilizadores.

Definición 4.13. *Código estabilizador.*
Sea $S = \langle g_1, \ldots, g_{n-k} \rangle$ subgrupo de G_n dado por $n-k$ generadores que conmutan y son independientes y tal que $-I \notin S$, definimos el código estabilizador $\mathcal{C}(S)$ de tipo $[n,k]$ como el subespacio V_S estabilizado por nuestro conjunto S.

La pregunta ahora es, ¿cómo llevamos a cabo la corrección de errores? Abramos boca con el siguiente teorema.

Teorema 4.6. *Condiciones para corrección de errores en códigos estabilizadores.*
Sea $\mathcal{C}(S)$ un código estabilizador y sea $\{E_j\}$ un conjunto de operadores en G_n tales que $E_j^* E_k \notin N(S) - S$ para todo j y k, entonces $\{E_j\}$ es un conjunto corregible de errores para $\mathcal{C}(S)$.

Demostración. Sea P el proyector en $\mathcal{C}(S)$. Dado que $S \subset N(S)$ tenemos dos posibilidades excluyentes: $E_j^* E_k \in S$ o $E_j^* E_k \in G_n - N(S)$.

En el primer caso es inmediato que $P E_j^* E_k P = P$ y se satisfacen las condiciones.

En el segundo caso $E_j^* E_k$ debe anticonmutar con algún elemento de S, g_1. Tomando ahora un conjunto de generadores de S, $\langle g_1, \ldots, g_{n-k} \rangle$ tales que:

$$P = \frac{\prod_{l=1}^{n-k} (I + g_l)}{2^{n-k}}.$$

Por la anticonmutatividad:

$$E_j^* E_k P = (I - g_1) E_j^* E_k \frac{\prod_{l=2}^{n-k}(I + g_l)}{2^{n-k}}.$$

Y dado que $P(I - g_1) = 0$ tenemos que $PE_j^* E_k P = 0$ por lo que se cumplen nuevamente nuestras condiciones y los errores son corregibles.

Esta consecuencia de las condiciones de corrección de errores cuánticos es interesante desde un punto de vista teórico, pero no nos aporta ninguna información concreta sobre como llevar a cabo la corrección de errores mediante el formalismo de los estabilizadores, pero tenemos todas las herramientas para hacerlo.

Para corregir utilizaremos un sistema de síndromes $\beta_1, \ldots, \beta_{n-k}$, que se corresponderán con las respectivas mediciones de $g_1, \ldots, g_{n-k}$. Suponiendo que ocurre el error E_j, el síndrome vendrá dado por los β_l tal que:

$$E_j g_l E_j^* = \beta_j g_l.$$

En el caso de ser el único error con dicho síndrome basta con aplicar nuevamente E_j^*. Si hubiese dos errores E_j y $E_{j'}$ con el mismo síndrome, entonces:

$$E_j P E_j^* = E_{j'} P E_{j'}^* \implies E_{j'}^* E_j P E_j^* E_{j'} = P.$$

Y por tanto $E_j^* E_{j'} \in S$ por lo que recuperamos el resultado original tras aplicar E_j^* tras haber ocurrido el error $E_{j'}$.

El teorema anterior motiva además la definición de *peso* para este tipo de códigos, y por tanto la noción de distancia mínima.

Definición 4.14. *Peso y distancia.*
Definimos el peso de un error $E \in G_n$ como el número de factores distintos a la identidad que contiene en su producto tensorial.
Definimos la distancia de un código estabilizador como el mínimo de los pesos entre los elementos de $N(S) - S$.
Sea $\mathcal{C}(S)$ un código estabilizador con $S = \langle g_1, \ldots, g_{n-k} \rangle \subset G_n$ y distancia mínima d, diremos que es de tipo $[n, k, d]$.

Por el teorema 4.6 sabemos que se pueden corregir hasta $\lfloor \frac{d-1}{2} \rfloor$ errores.

4.5.6. Ejemplos de códigos estabilizadores.

Veamos ahora algunos ejemplos de códigos que podemos representar de esta forma, comenzando con algunos de los más sencillos y avanzando hacia los más complejos.

Proposición 4.13. Bit flip como código estabilizador.
El código bit flip mencionado al principio del capítulo puede estudiarse como un tipo de código estabilizador con $S = \{Z_1 Z_2, Z_2 Z_3\}$ que puede corregir los errores dados por $\{I, X_1, X_2, X_3\}$.

Demostración. Basta ver que todo producto de dos errores anticonmuta con alguno de los generadores del código, por lo que podemos aplicar el teorema 4.6.

Podemos comprobar que el método genérico para la corrección de errores en códigos estabilizadores que explicamos anteriormente funciona a la perfección para este código, y es de hecho el mismo método que introdujimos al principio con el código bit flip, siendo la única novedad el uso de síndromes. Veamos un ejemplo.

Supongamos que ocurre un error del tipo X_1. En este caso nuestro estabilizador se transforma a $\langle -Z_1Z_2, Z_2Z_3\rangle$ por lo que obtenemos como síndromes -1 y $+1$. Análogamente, X_2 dará como síndromes -1 y -1 y X_3 hará lo propio con $+1$ y -1. (En caso de no haber errores obtenemos los síndromes 1 y 1).

Subamos un poco la complejidad formalizando el *código de Shor*.

Proposición 4.14. Código de Shor como código estabilizador.
El código de Shor es un código estabilizador dado por los siguientes generadores:

$$g_i = Z_iZ_{i+1} \text{ para } i \text{ entre 1 y 6,}$$
$$g_7 = XXXXXXIII \text{ y } g_8 = IIIXXXXXX.$$

Y es capaz de corregir cualquier error en un sólo qubit.

Demostración. La prueba de este resultado análoga al anterior, basta comprobar que los errores o bien están en S o bien anticonmutan con al menos un generador.

Pasemos ahora a códigos nuevos y algo más interesantes. Por ejemplo, ¿cuál será el mínimo tamaño necesario para construir un código capaz de codificar un qubit y corregir un error en un solo qubit? Ya hemos visto que el código de Shor cumple esta tarea, pero el siguiente código prueba que no lo hace de forma eficiente.

Proposición 4.15. El código de los 5 qubits.
El código estabilizador generado por:

$$g_1 = XZZXI,$$

$$g_2 = IXZZX,$$

$$g_3 = XIXZZ,$$

$$g_4 = ZXIXZ,$$

Es capaz de corregir cualquier error en un solo qubit.

La demostración del resultado vuelve a ser usar el teorema 4.6. Además, a causa de la cota de Hamming no es posible construir un código de menor tamaño que satisfaga esta función. A pesar de esto a veces es preferible emplear otros códigos como el *código de Steane*, que se trata además de un código CSS y que por tanto también es un código estabilizador como veremos a continuación.

Proposición 4.16. Códigos CSS como códigos estabilizadores.
Sean $\mathcal{C}_1$ y $\mathcal{C}_2$ dos códigos clásicos de tipo $[n, k_1]$ y $[n, k_2]$ respectivamente tales que $\mathcal{C}_2 \subset \mathcal{C}_1$ y tanto $\mathcal{C}_1$ como $\mathcal{C}_2^{\perp}$ son capaces de corregir t errores, entonces la matriz de comprobación dada por

$$\begin{bmatrix} H(\mathcal{C}_2^{\perp}) & 0 \\ 0 & H(\mathcal{C}_1) \end{bmatrix},$$

engendra un código estabilizador que coincide con el código $CSS(\mathcal{C}_1, \mathcal{C}_2)$.
Siendo $H(\mathcal{C}_2^{\perp})$ y $H(\mathcal{C}_1)$ las respectivas matrices de paridad.

Demostración. Para ver que la matriz de comprobación realmente nos genera un código estabilizador sólo hace falta comprobar la condición de conmutatividad:

$$H(\mathcal{C}_2^{\perp})H(\mathcal{C}_1)^T = [H(\mathcal{C}_1)G(\mathcal{C}_2)]^T = 0,$$

siendo $G(\mathcal{C}_2)$ la matriz generadora.

Al haber construido la matriz de comprobación a partir de las matrices de paridad resulta inmediato que nuestro código estabiliza exactamente los elementos de $CSS(\mathcal{C}_1, \mathcal{C}_2)$.

4.5.7. Forma estándar.

Para terminar con los códigos estabilizadores debemos establecer un método para obtener las bases de los códigos $\mathcal{C}(S)$ a partir de su estabilizador $S = \langle g_1, \ldots, g_{n-k} \rangle$.

El método es el siguiente:

1. Para empezar elegimos unos operadores $\bar{Z}_1, \ldots, \bar{Z}_k \in G_n$ tales que al añadirlos a los generadores formen un conjunto que conmute.
2. Estos operadores jugarán el papel de la matriz de Pauli σ_Z, por lo que el estado $|x_1, \ldots, x_k\rangle_L$ vendrá dado por:

$$\langle g_1, \ldots, g_{n-k}, (-1)^{x_1}\bar{Z}_1, \ldots, (-1)^{x_k}\bar{Z}_k \rangle.$$

3. Definimos los operadores $\bar{X}_j$ como aquellos que transforman $\bar{Z}_j$ en $-\bar{Z}_j$, que jugará el papel de σ_X y conmutará con todos los generadores y y operadores $\bar{Z}_i$ salvo con $\bar{Z}_j$.

La pregunta que se nos plantea es, ¿cómo construímos estos operadores artificiales? Para hacerlo, introducimos la llamada *forma estándar* de un código estabilizador.

Proposición 4.17. Forma estándar.
Sea $G = [G_1|G_2]$ la matriz de comprobación de un código estabilizador, entonces podemos encontrar generadores para dicho código tales que la matriz de comprobación sea de la forma:

$$\begin{array}{c} \\ \text{(r)} \\ \text{(n-k-r)} \end{array} \begin{array}{c} \begin{array}{ccc|ccc} \text{(r)} & \text{(n-k-r)} & \text{(k)} & \text{(r)} & \text{(n-k-r)} & \text{(k)} \end{array} \\ \left(\begin{array}{ccc|ccc} I & A_1 & A_2 & B & 0 & C \\ 0 & 0 & 0 & D & I & E \end{array}\right), \end{array}$$

siendo r el rango de G_1.

Demostración. La prueba se basa fundamentalmente en el hecho que de podemos aplicar eliminación gaussiana sin afectar el conjunto estabilizado. ∎

Usando esto, es sencillo comprobar que los operadores dados por la matriz de comprobación:

$$G_z = [000|A_2^T 0 I],$$

cumplen nuestras necesidades.

Capítulo 5

Conclusión.

> *"It would be so nice if something made sense for a change."*
> **-Lewis Carroll**.

Al igual que en toda historia, sólo hemos podido contar una pequeña porción; una visión reducida de todos las narraciones que se cruzan con la nuestra. Podríamos haber hablado de la construcción de circuitos o de la entropía. Podríamos haber expandido más las ideas sobre distancia o habernos centrado en las operaciones y el ruido.

En cualquier caso, esta ha sido nuestra historia. Hemos dado una perspectiva general sobre los postulados de la mecánica cuántica y de su interpretación dentro de la computación cuántica. Hemos introducido, definido y formalizado las operaciones cuánticas. Hemos construido medidas para controlar el efecto de dichas operaciones y analizar el éxito de códigos cuánticos. Por último, hemos enunciado el concepto de código corrector de error, aportando algunas cotas y casos especiales y demostrado que podemos llevar a cabo la corrección de errores en sistemas cuánticos de manera eficiente usando los estabilizadores.

¿Qué puertas se abren a parir de este punto? Quizás la más relevante es la llamada computación *fault-tolerant* y el *teorema del Threshold*, que nos ilustran como podemos construir circuitos para codificar y decodificar usando la llamada *concatenación de circuitos codificados* y asumiendo que se producen errores en cualquier proceso (incluso en la misma codificación) cuando la probabilidad de que estos errores ocurran es inferior a una barrera. También nos podríamos adentrar en el mundo de la optimización de códigos o haber entrado en mayor profundidad en el mundo de las cotas.

Podríamos haber hablado de todas estas cosas y otras más, pero esta es la historia que hemos decidido contar.

Bibliografía

[1] Landsberg, J. M. (2018) *A very brief introduction to quantum computing and quantum information theory for mathematicians.* https://arxiv.org/abs/1801.05893

[2] Lyons, D. W. (2003). *An elementary introduction to the Hopf fibration.* Mathematics magazine, 76(2), 87-98.

[3] Nielsen, M. A. y Chuang I.L. (2010). *Quantum Computation and Quantum Information.* New York: Cambridge University Press.