



Universidad de Valladolid

FACULTAD DE CIENCIAS

TRABAJO FIN DE GRADO

Grado en Física

Simulación OLCC de canales cuánticos

Autor: Arturo Juárez Carrillo

Tutores: Diego G. Bussandri, Luis Miguel Nieto Calzada

2024

Índice general

I	Introducción	I
1.1	Sistemas cuánticos	2
1.1.1	Estados cuánticos	2
1.1.2	Sistemas bipartitos y correlaciones cuánticas	4
1.1.3	Mediciones	7
1.2	Canales cuánticos abiertos	10
1.2.1	Operaciones cuánticas	10
1.2.2	Canales cuánticos y canales clásicos	10
1.2.3	Canales ruidosos	11
1.3	Representaciones	13
1.3.1	Representaciones \mathcal{A} y \mathcal{B}	13
1.3.2	Representación de Kraus	14
1.3.3	Matriz de Choi	15
1.3.4	Mapas unitales	16
1.3.5	Mapas no unitales	17
1.4	Fidelidad	17
2	Protocolos cuánticos	19
2.1	Teleportación	19
2.1.1	Teleportación clásica	19
2.1.2	Teleportación cuántica	20
2.2	Codificación densa	23
2.2.1	Protocolo de codificación densa general	24
3	Simulación de canales cuánticos	26
3.1	Aplicaciones de la simulación de canales cuánticos	28
3.1.1	Aplicación en estimación de parámetros de sistemas cuánticos	29
3.2	Simulación de canales de qubits	29
3.2.1	Los canales de Pauli son Choi-estirables	31
3.2.2	Simulación de canales que no sean de Pauli	31
4	Conclusiones	36
	Bibliografía	39

Índice de figuras

1.1	Construcción de la matriz de Choi.	16
2.1	Protócolo de codificación densa.	24

*"Dejo a los varios porvenires (no a todos)
mi jardín de senderos que se bifurcan."*

Borges, *Ficciones*.

*"Sí, comencé mi viaje solo y lo concluí solo.
Pero eso no significa que caminara solo."*

Brandon Sanderson, *El camino de los reyes*.

*"[...] Dejar quisiera
mi verso como deja el capitán su espada:
famosa por la mano viril que la blandiera,
no por el docto oficio del forjador preciada."*

A. Machado, *Campos de Castilla*.

Agradecimientos

Las primeras personas que se merecen ser mencionadas son mis dos tutores, Luismi y Diego. A Luismi por brindarme esta oportunidad y encargarse de que este trabajo fuera posible, además de ser un gran profesor, y a Diego por las innumerables horas que hemos pasado codo con codo (y por separado) pensando, revisando y peleando para escribir cada párrafo de este trabajo. Por motivarme a cada paso y por hacerme sentir como su compañero más que como un simple alumno.

Por otro lado, este trabajo no es algo aislado sino que representa el punto final de una carrera, que no ha sido tal si no más bien un paseo, gracias sobre todo al apoyo y confianza de mis padres desde un inicio. Ellos me han dado todo lo que soy y no puedo más que agradecerles que hayan sido tan buenos en lo suyo.

Para terminar me gustaría mencionar a la tercera pata de esta mesa de tres patas que me considero, a mis amigos y compañeros de fatiga, a todos los que han estado conmigo y me han brindado su apoyo y amistad durante todos estos años y que han hecho esta carrera mucho más llevadera y valiosa.

A todos, gracias.

Resumen

La simulación de canales cuánticos utilizando operaciones locales y comunicación clásica (simulación OLCC) facilita el cálculo de figuras de mérito en protocolos clave, como la codificación densa y la distribución cuántica de claves, además de tener aplicaciones significativas en metrología cuántica.

Nuestros resultados destacan la existencia de canales que no son de Pauli ni unitales, pero que pueden ser simulados utilizando el protocolo de teleportación estándar, una forma particular de OLCC. Este hallazgo contradice la suposición prevalente en la literatura de que solo los canales de Pauli son Choi-estirables mediante teleportación estándar, abriendo una nueva línea de investigación en la simulación OLCC de mapas cuánticos.

Abstract

The simulation of quantum channels using local operations and classical communication (LOCC simulation) simplifies the calculation of figures of merit in important protocols, such as dense coding and quantum key distribution, and has significant applications in quantum metrology.

Our results highlight the existence of channels that are neither Pauli nor unital but can be simulated using the standard teleportation protocol, a particular form of LOCC. This finding contradicts the prevailing assumption in the literature that only Pauli channels are Choi-stretchable via standard teleportation, thus our work opens a new line of research in the LOCC simulation of quantum maps.

Capítulo I

Introducción

En 1940, Claude Shannon estableció las bases de la teoría de información [1]. La misma consta de la formalización matemática de los procesos de cuantificación, transmisión y almacenamiento de información utilizando la electrodinámica y mecánica *clásicas* –el término *teoría clásica* habitualmente refiere a estas dos áreas de la física. La teoría de la información cuántica (TIC) es la contraparte de la teoría de Shannon, en la que se utilizan sistemas físicos regidos por los postulados de la mecánica y electrodinámica cuánticas. Nótese que las teorías cuántica y clásica establecen relaciones de causa y efecto muy diferentes; de este modo, la teoría de Shannon no agota todas las posibilidades en cuanto al procesamiento de información, lo que constituye el punto de motivación principal de la TIC [2].

Los *protocolos* de distribución de claves secretas, de teleportación de estados cuánticos y de codificación densa, entre otros, son ejemplos claros de las nuevas posibilidades a estudiar y comprender por la teoría de información cuántica [3]. Cabe aclarar que, en este contexto, *información clásica* refiere al valor que toma una variable aleatoria particular (o un conjunto de ellas), mientras que *transmitir información cuántica* supone el envío de estados cuánticos de un sistema a otro. De este modo, los tres protocolos mencionados anteriormente tienen un objetivo en común que es la transmisión de información: *teleportación* es el procedimiento por el cual se envían estados cuánticos, arbitrarios y desconocidos, de un sistema a otro; el protocolo de distribución cuántica de claves permite a dos entidades compartir una *clave* secreta completamente aleatoria, dando lugar a la denominada criptografía cuántica; y, por último, el algoritmo de codificación densa posibilita duplicar la cantidad de información clásica que podría enviarse a través de un canal clásico.

Las Operaciones Locales y Comunicación Clásica (OLCC) constituyen la herramienta matemática principal de la teoría de información cuántica, con la que los protocolos y algoritmos cuánticos se describen de forma general. *Operaciones locales* representan las evoluciones e interacciones a las que podría someterse un sistema cuántico, y se describen matemáticamente por medio de mapas completamente positivos que preservan la traza. Por otro lado, *comunicación clásica* hace referencia al envío de información clásica entre partes con un objetivo específico.

Un aspecto relevante en la teoría de la información cuántica consiste en investigar cómo el ruido presente en la implementación experimental de los protocolos mencionados afecta sus probabilidades. Así surgen *figuras de mérito* –es decir, funcionales que cuantifican el éxito o fracaso de determinadas operaciones, canales o protocolos cuánticos– como por ejemplo la *fidelidad media* en el caso del protocolo de teleportación, y las capacidades de distribución de

claves y codificación densa [4]. Estas dos últimas capacidades son generalmente muy costosas de calcular tanto numérica como analíticamente.

Este trabajo se desarrolla en torno a la simulación OLCC de canales cuánticos, una herramienta principalmente implementada y desarrollada por S. Pirandola [5] que permite simplificar en gran medida el cálculo de diferentes figuras de mérito de protocolo particulares, como por ejemplo, codificación densa, distribución de claves y metrología. En particular, la simulación OLCC de una canal cuántico implica la reescritura de este último utilizando OLCC conocidas. Esto es importante porque ayuda a abordar la fragilidad inherente de la información cuántica: Al utilizar las ya mencionadas operaciones locales asistidas por comunicación clásica, se pueden diseñar y evaluar protocolos adaptativos que maximizan las tasas de transmisión de información cuántica, distribución de entrelazamiento y generación de claves secretas, estableciendo así capacidades fundamentales de los canales cuánticos y proporcionando referencias esenciales para el desarrollo de repetidores cuánticos y otras infraestructuras de comunicación avanzadas [5, 6, 7].

El tipo de simulación OLCC sobre el que trabajaremos consta de la simulación de canales utilizando el protocolo de teleportación cuántica estándar. Nuestros principales resultados son los teoremas 3.2.1 y 3.2.2, que implican la existencia de canales no *unitales* y que tampoco son *de Pauli* pero con las propiedades que buscamos. La importancia de este hallazgo radica en que contradice la actual dirección de razonamiento que consideran los principales autores en el tema. Esto se puede apreciar en el artículo [6] en el que se afirma que sólo canales de Pauli pueden ser simulados haciendo uso de teleportación cuántica estándar.

En este primer capítulo planteamos una introducción teórica a los conceptos que nos serán de utilidad en el planteamiento y desarrollo del tema principal de este trabajo. Para ello comenzaremos con una breve explicación sobre estados y sistemas cuánticos bipartitos, Secs. 1.1.1 y 1.1.2, respectivamente. El proceso de medición de observables se resume en la Sec. 1.1.3, que forma parte ineludible de cualquier protocolo cuántico. Luego, en las Secs. 1.3 y 1.4, revisaremos cómo representar los canales cuánticos mediante la descomposición de Kraus o la matriz de Choi, además de introducir el concepto de fidelidad como herramienta básica para medir distinguibilidad entre estados cuánticos [8, 3, 2, 4, 9].

En el Capítulo 2 introduciremos los protocolos de teleportación, que utilizaremos para llevar a cabo la simulación de canales, y el de codificación densa, que emplearemos para ilustrar específicamente la utilidad que tiene la simulación OLCC de canales cuánticos.

Finalmente, en el Capítulo 3, profundizaremos en el concepto de simulación de canales cuánticos y, además, analizaremos nuestros principales resultados.

1.1 Sistemas cuánticos

1.1.1 Estados cuánticos

En la teoría cuántica, el comportamiento de los sistemas físicos está descrito por los *estados cuánticos*, que son elementos de un espacio de Hilbert \mathcal{H} . Los denominados sistemas de dos niveles,

o “*qubits*”¹, son representados por espacios de Hilbert de dimensión dos², es decir, los estados cuánticos son combinaciones lineales de dos elementos ortonormales $|0\rangle$ y $|1\rangle$ que forman una base en el espacio de Hilbert,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1. \quad (1.1)$$

Estos sistemas, constituyen el análogo cuántico de un bit clásico, con la diferencia de que el bit puede asumir un único estado: $|0\rangle$ o $|1\rangle$.

La definición que aparece en la Ecuación 1.1 no engloba todos los posibles estados que un sistema cuántico puede adoptar, ya que solo permite la representación de estados puros. Para dar una definición más general de los estados que puede tomar un sistema cuántico necesitamos introducir el *operador densidad*, ρ , el cuál sirve para representar tanto estados puros como estados mixtos:

$$\textbf{Estado puro: } \rho = |\psi\rangle\langle\psi|, \quad (1.2)$$

$$\textbf{Estado mixto: } \rho = \sum_j p_j |\psi_j\rangle\langle\psi_j| = \sum_j p_j \rho_j, \quad (1.3)$$

con $\sum_j p_j = 1$. Es fácil comprobar que este operador es semi-definido positivo, hermítico y su traza es igual a la unidad. Podemos escribir esta última propiedad como que $\rho \in \mathcal{B}_1^+(\mathcal{H})$.

A diferencia de los estados puros, los estados mixtos representan una mezcla estadística de estados puros. Esta mezcla surge cuando no se tiene información completa sobre el estado del sistema, o cuando este se encuentra interactuando con su entorno. Para describir matemáticamente los estados mixtos, se introduce el operador densidad. Este operador, que funciona como una analogía cuántica de las funciones de densidad de probabilidad en la física clásica [4], permite calcular las probabilidades de obtener diferentes resultados al medir una propiedad del sistema.

La esfera de Bloch

En la sección anterior introdujimos el concepto de estado cuántico y vimos que su representación matemática más general es el operador densidad. Cuando el sistema físico se puede describir utilizando un espacio de Hilbert de dimensión dos, podemos utilizar las *matrices de Pauli* para establecer un relación entre el espacio de operadores densidad y la esfera unidad en \mathbb{R}^3 . Esto se debe a que las matrices de Pauli, junto con la matriz identidad $\mathbf{1}$, forman una base del espacio de operadores hermíticos, es decir, todo operador hermítico (como el operador densidad) se puede escribir como suma de tales matrices.

La condición de normalización (i.e. traza igual a uno) y el hecho de que el operador densidad es semi-definido positivo, implican que el estado de cualquier qubit queda especificado por un vector en una esfera de radio unidad, que se denominan respectivamente *vector de Bloch* y *esfera*

¹En 1995, Benjamin Schumacher acuñó por primera vez el término “*qubit*” para referirse a los sistemas cuánticos de dos niveles.

²Por lo general, nuestro trabajo estará centrado en sistemas de dimensión dos pero habrá casos concretos, por ejemplo la Sección 2.2, donde definiremos sistemas en dimensión arbitraria n .

de Bloch. Cualquier qubit se puede representar mediante la siguiente expresión [2, pg. 105]:

$$\rho = \frac{1}{2}(\mathbf{1} + \vec{r} \cdot \vec{\sigma}), \quad (1.4)$$

siendo $\vec{r} = (x, y, z) \in \mathbb{R}^3$ el vector de Bloch asociado al estado del qubit, y $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z) = (\sigma_1, \sigma_2, \sigma_3)$ las matrices de Pauli. El módulo del vector de Bloch es una medida de la *pureza* del estado: para estados puros tenemos que $|\vec{r}| = 1$, mientras que para estados mixtos vale $|\vec{r}| < 1$. El estado máximamente mixto es $\mathbf{1}/2$ y cuanto mayor es su módulo, mayor es la pureza.

Las operaciones unitarias sobre la matriz densidad actúan como rotaciones sobre la esfera de Bloch. Cualquier operador unitario actuando sobre un espacio de Hilbert de dimensión dos se puede escribir de la siguiente forma:

$$U_{\hat{a}, \alpha} = \exp\left(-i\frac{\alpha}{2} \hat{a} \cdot \vec{\sigma}\right) = \cos\frac{\alpha}{2} \mathbf{1} - i \sin\frac{\alpha}{2} (\hat{a} \cdot \vec{\sigma}), \quad (1.5)$$

donde α es el ángulo de rotación y $\hat{a} = (a_1, a_2, a_3)$ un vector unitario que representa el eje de giro.

Al aplicar cualquier transformación unitaria sobre la matriz densidad $U\rho U^\dagger$, el vector de Bloch se transforma de la siguiente forma

$$\vec{r}' = \vec{r} \cdot \hat{a} \mathbf{1} + [\vec{r} - (\vec{r} \cdot \hat{a})\hat{a}] \cos \alpha + \hat{a} \times \vec{r} \sin \alpha \quad (1.6)$$

Algunas propiedades del operador densidad que nos serán muy útiles:

1. $\text{Tr}[\sigma_\alpha \sigma_\beta] = 2\delta_{\alpha\beta}$.
2. $r_\mu = \text{Tr}[\rho \sigma_\mu]$.

De este modo, usando las propiedades anteriores, es fácil ver que para un observable $O = s\mathbf{1} + \vec{c} \cdot \vec{\sigma}$, su valor medio es $\langle O \rangle = \text{Tr}[\rho O] = s + \vec{r} \cdot \vec{c}$.

1.1.2 Sistemas bipartitos y correlaciones cuánticas

El entrelazamiento es una de las propiedades de los sistemas cuánticos más relevantes en la teoría de la información cuántica. Este fenómeno es, matemáticamente, consecuencia directa de dos elementos clave de la mecánica cuántica: el principio de superposición y la estructura tensorial del espacio de Hilbert. Sin embargo, el entrelazamiento no es el único tipo de correlación que pueden exhibir los sistemas cuánticos bipartitos. Veamos una pequeña síntesis de la descripción de este tipo de sistemas y de sus correlaciones.

Comencemos con la representación matemática de un sistema bipartito compuesto por dos qubits. El espacio de Hilbert correspondiente está dado por el producto tensorial entre los espacios de Hilbert de cada una de las partes: $\mathcal{H} = \mathcal{H}_a \otimes \mathcal{H}_b$, siendo $\{|0\rangle_a, |1\rangle_a\}$ y $\{|0\rangle_b, |1\rangle_b\}$ las

bases de dichos subespacios, la base que define el espacio completo es

$$\begin{aligned} |0\rangle_a \otimes |0\rangle_b &= |00\rangle, \\ |0\rangle_a \otimes |1\rangle_b &= |01\rangle, \\ |1\rangle_a \otimes |0\rangle_b &= |10\rangle, \\ |1\rangle_a \otimes |1\rangle_b &= |11\rangle. \end{aligned}$$

En la notación del operador densidad, el estado más general posible para un sistema de dos qubits viene dado por:

$$\rho = \frac{1}{4} \left(\mathbf{1}_a \otimes \mathbf{1}_b + \vec{a} \cdot \vec{\sigma} \otimes \mathbf{1}_b + \mathbf{1}_a \otimes \vec{b} \cdot \vec{\sigma} + \sum_{i,j=1}^3 C_{ij} \sigma_i \otimes \sigma_j \right), \quad (1.7)$$

donde \vec{a} y \vec{b} representan los vectores de Bloch de los subsistemas y C_{ij} son los elementos de la matriz de correlaciones C entre ambos subsistemas. Más adelante veremos algunas implicaciones asociadas a los valores que pueden tomar estos elementos. Por ejemplo, para un estado producto tensorial, $\rho = \rho_a \otimes \rho_b$, la representación anterior se puede obtener calculando el producto entre las representaciones de cada subsistema (1.4) por separado, en dicho caso la matriz de correlaciones entre ambos subsistemas es simplemente

$$C = \vec{a} \vec{b}^\top \quad (1.8)$$

Veamos a continuación los tipos de correlaciones que pueden aparecer en un sistema cuántico.

Estados puros

Si el sistema está preparado en un estado puro $|\psi\rangle_{AB} \in \mathcal{H}_{AB}$ tal que $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$, pueden darse dos posibilidades [10]. La primera es que ambos subsistemas son completamente independientes, en cuyo caso el estado del sistema global es:

$$|\psi\rangle_{AB} = |\alpha\rangle_A \otimes |\beta\rangle_B. \quad (1.9)$$

En este caso no existen correlaciones entre los subsistemas ni clásicas ni cuánticas.

La segunda posibilidad es que esta representación no sea posible, en dicho caso $|\psi\rangle_{AB}$ describe un estado entrelazado de los dos subsistemas A y B. El entrelazamiento aquí engloba todo tipo de correlaciones entre subsistemas, es más, entrelazamiento, *no-localidad* y correlaciones cuánticas son sinónimos para estados bipartitos puros.

Estados mixtos

Para los estados mixtos el asunto se vuelve más complejo. Si $\rho_{AB} \in \mathcal{B}_1^+(\mathcal{H}_{AB})$ describe el estado del sistema bipartito, el conjunto de estados separables $\mathcal{S}_{AB} \subset \mathcal{B}_1^+(\mathcal{H}_{AB})$ está dado por

$$\mathcal{S}_{AB} := \left\{ \rho_{AB} \mid \rho_{AB} = \sum_i p_i \eta_A^i \otimes \tau_B^i \right\}. \quad (1.10)$$

Cualquier otro estado $\rho_{AB} \notin \mathcal{S}_{AB}$ está entrelazado.

Nótese que el conjunto de estados separables es estrictamente mayor que el conjunto de estados producto tensorial, $\mathcal{P}_{AB} \subset \mathcal{S}_{AB}$, donde

$$\mathcal{P}_{AB} := \{\rho_{AB} \mid \rho_{AB} = \rho_A \otimes \rho_B\}. \quad (1.11)$$

¿Son las correlaciones en los estados separables únicamente clásicas? Veamos a continuación porque, en general, la respuesta a esta pregunta es negativa. Definamos ahora un estado compuesto por un elemento clásico (un bit) en A y uno cuántico (un qubit) en B. Por conveniencia, adoptaremos el mismo formalismo para ambos. El bit clásico puede estar en el estado $|0\rangle$ o en el estado $|1\rangle$. Si el bit clásico está en $|0\rangle$, se puede escribir el estado compuesto como $|0\rangle\langle 0|_A \otimes \rho_B$, donde hemos identificado el bit clásico como el subsistema A y el qubit como el subsistema B, siendo ρ_B un estado cuántico. Sin embargo, si se desconoce el estado del bit clásico, entonces el estado compuesto ρ_{AB} es una mezcla estadística, es decir

$$\rho_{AB} = p_0 |0\rangle\langle 0|_A \otimes \rho_B^{(0)} + p_1 |1\rangle\langle 1|_A \otimes \rho_B^{(1)}, \quad (1.12)$$

donde p_0 y p_1 son probabilidades que suman uno, mientras que $\rho_B^{(0)}$ y $\rho_B^{(1)}$ denotan el estado del bit cuántico B cuando el bit clásico A está en $|0\rangle$ y $|1\rangle$, respectivamente. Este es un ejemplo de lo que llamamos un estado cuántico clásico, o clásico en A, ya que el subsistema A es clásico. Por el contrario, también podríamos definir un estado en el que qubit se encuentre en el subsistema A y el bit en el B. Podemos definir respectivamente ambos conjuntos de estados como

$$\mathcal{C}_A := \left\{ \rho_{AB} \mid \rho_{AB} = \sum_i |i\rangle\langle i|_A \otimes \rho_B^i \right\}, \quad (1.13)$$

$$\mathcal{C}_B := \left\{ \rho_{AB} \mid \rho_{AB} = \sum_i \rho_A^i \otimes |i\rangle\langle i|_B \right\}. \quad (1.14)$$

Y la intersección de ambos conjuntos engloba a todos los estados clásicos en A y en B que presentan únicamente correlaciones clásicas,

$$\mathcal{C}_{AB} := \left\{ \rho_{AB} \mid \rho_{AB} = \sum_{ij} p_{ij} |i\rangle\langle i|_A \otimes |j\rangle\langle j|_B \right\}, \quad (1.15)$$

donde $\{p_{ij}\}$ se puede entender como una distribución de probabilidad conjunta.

La jerarquía entre todos los estados que hemos descrito es la siguiente:

$$\mathcal{P}_{AB} \subset \mathcal{C}_{AB} \subset \{\mathcal{C}_A, \mathcal{C}_B\} \subset \mathcal{S}_{AB} \subset \mathcal{B}_1^+(\mathcal{H}_{AB}). \quad (1.16)$$

En esta jerarquía sólo los dos conjuntos de la derecha son convexos.

Estados de Bell

Los estados de Bell son un conjunto de cuatro estados máximamente entrelazados definidos para una pareja de qubits, esto implica que la medición sobre uno de los subsistemas que componen el estado de Bell nos permite saber inmediatamente el estado del otro subsistema sin necesidad

de aplicar ninguna medición sobre él. La base de estados de Bell es la siguiente:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad (1.17)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \quad (1.18)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad (1.19)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \quad (1.20)$$

La matriz densidad asociada a cada uno de estos estados se expresa como:

$$\rho_{Bell}^k = |\Psi_{Bell}^k\rangle\langle\Psi_{Bell}^k| = \frac{1}{4} \left(\mathbf{1}_a \otimes \mathbf{1}_b + \sum_i^3 W_i^k \sigma_i \otimes \sigma_i \right), \quad (1.21)$$

donde $\vec{a} = \vec{b} = 0$, ya que al ser un estado completamente entrelazado perdemos toda la información asociada a cada subsistema, y $\{W^k\}_{k=1}^4$ son las matrices diagonales asociadas a los estados de Bell:

$$W^1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad W^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \quad W^3 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad W^4 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \quad (1.22)$$

Para dimensiones superiores en las que aparecen sistemas de más de dos qubits es habitual sustituir los estados de Bell por las representaciones GHZ y W [11]. El estado GHZ para un sistema con n qubits se define como

$$|\text{GHZ}\rangle = \frac{1}{\sqrt{2}} (|00 \dots 0\rangle + |11 \dots 1\rangle). \quad (1.23)$$

Son estados máximamente entrelazados en los que todos los qubits están en una superposición de estar todos en el estado $|0\rangle$ y todos en el estado $|1\rangle$. La medida de un solo qubit afecta inmediatamente a los demás. Sin embargo, son muy frágiles frente a la decoherencia; la pérdida o medición de un solo qubit puede destruir el entrelazamiento global.

Por otro lado, el estado W para un sistema con n qubits se define como

$$|W\rangle = \frac{1}{\sqrt{n}} (|100 \dots 0\rangle + |010 \dots 0\rangle + \dots + |000 \dots 1\rangle). \quad (1.24)$$

También son estados altamente entrelazados, pero a diferencia de los estados de GHZ, son más robustos frente a la pérdida de un qubit. Si se mide o se pierde un qubit, el estado restante de los qubits sigue estando entrelazado. Esto se debe a que el entrelazamiento en los estados de W está distribuido de manera diferente que en los estados de GHZ.

1.1.3 Mediciones

W. Pauli [12, pg. 75] categorizó las mediciones en dos grupos bien diferenciados:

1. Mediciones que son repetibles, es decir, que se pueden aplicar varias veces sobre un mismo estado sin que den lugar resultados nuevos, forman parte del primer grupo y también son las que recoge el postulado de proyección de von Neumann (tercer postulado de la mecánica cuántica). La medida del espín de Stern-Gerlach es usado habitualmente como ejemplo práctico de este tipo de medición.
2. Mediciones en las que el estado del sistema medido cambia de forma controlable de tal manera que su repetición conducirá a resultados estadísticos diferentes a los de la medición inicial. Cuando se pueden sacar conclusiones definitivas sobre la cantidad que se mide de esta manera, las mediciones son mediciones del segundo tipo. Es, por ejemplo, el caso del conteo de fotones, proceso por el cual la partícula queda destruida imposibilitando tomar nuevas medidas.

Las mediciones de von Neumann de un observable discreto ordinario son repetibles, pero una medición repetible de ese mismo observable no es necesariamente de von Neumann.

El tercer postulado de la mecánica cuántica dice lo siguiente [2, pg. 84]:

Tercer Postulado: Las mediciones cuánticas están descritas por un conjunto $\{M_m\}$ de operadores de medición. Estos son operadores que actúan sobre el espacio de estados del sistema medido. El subíndice m hace referencia a los posibles resultados de la medición. Si el estado del sistema es ρ inmediatamente antes de la medición entonces la probabilidad de obtener el resultado m es

$$p(m) = \text{Tr}[M_m \rho M_m^\dagger] \quad (1.25)$$

Y el estado del sistema después de la medición,

$$\rho \rightarrow \rho' = \frac{M_m \rho M_m^\dagger}{\text{Tr}[M_m^\dagger M_m \rho]} \quad (1.26)$$

Los operadores de medición satisfacen la ecuación de completitud,

$$\sum_m M_m^\dagger M_m = \mathbf{1} \quad \iff \quad \sum_m p_m = 1 \quad (1.27)$$

A la hora de diferenciar dos estados no existe ninguna medición capaz de diferenciarlos si estos no son ortogonales [2, pg. 87].

Mediciones proyectivas (PVMs)

Una medida proyectiva está descrita por un observable físico del sistema, i.e. un operador hermítico en el espacio de estados del sistema que se está midiendo. De este modo, si M es el operador en cuestión, podemos tomar su descomposición espectral:

$$M = \sum_m m P_m, \quad \text{con} \quad P_i P_j = \delta_{ij} P_i, \quad (1.28)$$

donde P_m es el proyector al subespacio de M con autovalor m .

La medida proyectiva de este observable está dada por los proyectores $\{P_m\}_m$. Los posibles resultados de la medición corresponden con los autovalores m del observable. Las medidas proyectivas se pueden entender como un caso especial de lo que menciona el Postulado 3.

POVMs

Una medida POVM (*Positive operator-valued measure*) es un conjunto de operadores hermíticos no negativos que actúan sobre el espacio de Hilbert que describe el sistema cuántico en cuestión. A diferencia de las medidas PVM o proyectivas, las cuales son un caso particular de las medidas aquí tratadas y son válidas solo para sistemas cerrados, las medidas POVM, también conocidas como medidas generalizadas, tienen en cuenta la interacción del sistema con el entorno.

Supongamos una medida descrita por los operadores de medición M_m que se realiza sobre un sistema en el estado ρ . En ese caso la probabilidad de obtener el resultado m al hacer la medición es $p(m) = \text{Tr}[M_m^\dagger M_m \rho]$. Definamos ahora una medida POVM como el conjunto de operadores hermíticos y no negativos $\{E_m\}$ tales que

$$E_m = M_m^\dagger M_m \quad \text{con} \quad \sum_m E_m = \mathbf{1}, \quad (1.29)$$

de forma que los operadores E_m son suficientes para encontrar las probabilidades de obtener cualquier resultado en la medición, cumpliéndose ahora que $p(m) = \text{Tr}[E_m \rho]$.

Se puede demostrar que si $\{E_m\}$ es un conjunto de operadores positivos siempre vamos a poder encontrar un conjunto de operadores $\{M_m\}$ que describan una medición [2, pg. 91].

Veamos un ejemplo útil de POVM para la computación cuántica. Supongamos que Alice le da a Bob un qubit que puede estar en uno de los estados $|\psi_1\rangle = |0\rangle$ o $|\psi_2\rangle = |+\rangle$, dado que no son estados ortogonales, Bob es incapaz de saber con total certeza el estado de su qubit. Aun así, es capaz de idear unas mediciones que le permitan acertar el estado del qubit algunas veces pero que evite que lo identifique erróneamente.

$$\begin{aligned} E_1 &= \frac{\sqrt{2}}{1 + \sqrt{2}} |1\rangle\langle 1|, \\ E_2 &= \frac{1}{2 + \sqrt{2}} (|0\rangle\langle 0| - |0\rangle\langle 1| - |1\rangle\langle 0| + |1\rangle\langle 1|), \\ E_3 &= \mathbf{1} - E_1 - E_2, \end{aligned} \quad (1.30)$$

Supongamos que a Bob se le da el estado $|\psi_1\rangle = |0\rangle$. Realiza la medición descrita por la POVM $\{E_1, E_2, E_3\}$. Hay probabilidad cero de que observe el resultado E_1 , ya que E_1 ha sido elegido inteligentemente para asegurar que $\langle \psi_1 | E_1 | \psi_1 \rangle = 0$. Por lo tanto, si el resultado de su medición es E_1 , Bob puede concluir con seguridad que el estado que recibió debe haber sido $|\psi_2\rangle$. Una línea de razonamiento similar muestra que si se produce el resultado de la medición E_2 , entonces debe haber sido el estado $|\psi_1\rangle$ que recibió Bob. Algunas veces, sin embargo, Bob obtendrá el resultado de la medición E_3 y no podrá inferir nada sobre la identidad del estado que se le dio. Sin embargo, el punto clave es que Bob nunca se equivoca al identificar el estado que se le ha otorgado. Esta infalibilidad tiene el precio de que a veces Bob no obtiene información sobre la identidad del Estado.

1.2 Canales cuánticos abiertos

1.2.1 Operaciones cuánticas

La dinámica de un sistema cuántico aislado, descrito por un grupo de operadores unitarios, es reversible en el tiempo. La evolución de un sistema abierto, sujeto a influencias exteriores, ya sea el proceso de establecimiento del equilibrio con el medio ambiente o la interacción con los aparatos de medición, revela características de irreversibilidad. Estos cambios irreversibles se describen matemáticamente mediante mapas completamente positivos. Por lo tanto, es útil considerar la clase de operaciones lineales completamente positivas,

$$\rho \xrightarrow{\mathcal{E}} \rho', \quad (1.31)$$

y que cumplen las siguientes condiciones:

1. $\text{Tr}[\mathcal{E}(\rho)]$ es la probabilidad de que la operación \mathcal{E} ocurra, siendo

$$\rho' = \frac{\mathcal{E}(\rho)}{\text{Tr}[\mathcal{E}(\rho)]}, \quad (1.32)$$

el nuevo estado tras la operación.

2. $\mathcal{E}(\rho)$ es un mapa lineal convexo de operadores estadísticos, i.e.,

$$\mathcal{E}\left(\sum_i p_i \rho_i\right) = \sum_i p_i \mathcal{E}(\rho_i), \quad (1.33)$$

siendo $\sum_i p_i = 1$ las probabilidades que describen el estado mixto.

3. $\mathcal{E}(\rho)$ es un mapa (o mapa dinámico reversible) completamente positivo.

Las operaciones $\mathcal{E}(\rho)$ satisfacen estas tres condiciones si y solo si admiten una descomposición en sus operadores de Kraus (Sección 1.3.2).

A partir del teorema de Wigner [9, pg. 22], se deduce que los mapas dinámicos reversibles son de la forma:

$$\mathcal{E}(\rho) = U\rho U^\dagger, \quad (1.34)$$

donde U es una matriz unitaria que actúa en el espacio de estados \mathcal{H} del sistema descrito por el estado ρ .

1.2.2 Canales cuánticos y canales clásicos

Un canal consiste en la capacidad de usar un medio físico para transmitir información entre dos puntos (Alice y Bob)³. En cuanto a lo que interesa para nuestro estudio, podemos hacer una clasificación en dos grandes grupos:

1. **Canales clásicos:** en la teoría de la información clásica, un canal clásico describe la distribución de probabilidad en el envío de información clásica entre dos puntos. La capacidad

³Usaremos habitualmente estos dos nombres para hacer referencia a los extremos de un canal cuántico o clásico de la misma forma en la que podrían ser dos laboratorios.

de envío de información de un canal clásico se deduce el teorema de codificación y viene dada por la entropía de Shannon (H).

2. **Canales cuánticos:** en la teoría de la información cuántica, un canal cuántico sirve para el envío de información cuántica (e información clásica) aprovechando las propiedades de entrelazamiento que aparecen entre sistemas cuánticos. Más formalmente, un canal cuántico es un mapa completamente positivo que, además, conserva la traza (CPTP)⁴ entre dos espacios de estados

$$\mathcal{E}(\rho) : \mathcal{B}_1^+(\mathcal{H}) \rightarrow \mathcal{B}_1^+(\mathcal{H}), \quad (1.35)$$

es decir $\text{Tr}[\mathcal{E}(\rho)] = 1$. La medida estándar de la información contenida en un estado ρ es la entropía de Von Neumann (S).

La entropía de Shannon y la de Von Neumann son análogas en cuanto a que nos permiten describir la capacidad de almacenar información de los sistemas clásicos y cuánticos, respectivamente, pero existen diferencias importantes entre ambas magnitudes. En el caso de los sistemas clásicos, la entropía puede verse como la información obtenida al identificar el estado del sistema, mientras que en general el estado ρ de un sistema no puede identificarse completamente mediante la observación de un evento.

La entropía de Shannon y la entropía de von Neumann coinciden sólo para un conjunto formado por estados cuánticos puros mutuamente ortogonales. Por lo tanto, si se enviara un mensaje codificado en un conjunto de estados de qubits ortogonales, cada uno de ellos puro, que pueda describirse mediante un estado de producto tensorial general, la transmisión equivaldría a enviar la misma información que un conjunto de bits clásicos. Porque cada qubit es perfectamente distinguible una vez determinada la base de codificación.

Esto último hace referencia a los tipos de correlaciones que pueden surgir entre sistemas cuánticos como vimos en la Sección 1.1.2, resaltando nuevamente que el interés principal en el uso de canales cuánticos recae en la presencia de entrelazamiento entre los sistemas que los componen.

1.2.3 Canales ruidosos

Cuando la información se transmite sin errores en el mensaje decimos que el canal no tiene ruido o que es un canal sin ruido el cual es el tipo de canal más simple que podemos estudiar. Sin embargo, a la hora de estudiar implementaciones reales, tenemos que considerar canales arbitrarios que podrían modelar ruidos experimentales.

En el momento en el que el ruido aparece en nuestro sistema, las operaciones dejan de ser reversibles. La generalización de lo que hemos visto hasta ahora se define con un conjunto de transformaciones unitarias que se realizan con cierta probabilidad, $\{p(k), U_k\}$. Estas definen un canal \mathcal{E} , actuando sobre un estado ρ de la siguiente forma

$$\rho \xrightarrow{\mathcal{E}} \rho' = \sum_k p(k) U_k \rho U_k^\dagger, \quad (1.36)$$

⁴Por sus siglas en inglés: *Completely Positive and Trace Preserving*

siendo $p(k)$ una distribución de probabilidad. Este canal es un ejemplo que representa un modelo de ruido particular. A continuación, presentamos algunos otros canales *ruidosos* utilizados en la literatura.

Canales de Pauli

Un canal de Pauli es una generalización del canal desfasador y del canal *bit-flip* [3, pg. 158]. Este canal simplemente aplica un operador de Pauli de forma aleatoria de acuerdo con una distribución de probabilidad. El mapa para un canal de Pauli es [4, pg. 128]

$$\rho \rightarrow \rho' = \sum_{i,j=0}^1 p(i,j) \sigma_z^i \sigma_x^j \rho \sigma_x^j \sigma_z^i = \sum_{k=0}^4 p_k \mathcal{U}_k(\rho) \quad (1.37)$$

donde σ_x, σ_z y $i\sigma_y = \sigma_x \sigma_z$ son las matrices de Pauli que, para este caso, son iguales a los operadores de Kraus del mapa. Y donde el conjunto $\{\sigma_x^m \sigma_z^n\}$ también se conoce como el grupo de Weyl-Heisenberg [6] que son la generalización de las matrices de Pauli para dimensiones superiores.

Podemos describir la acción de cualquier canal cuántico mediante su representación afín:

$$\mathcal{E}(\rho) : \vec{t} \rightarrow \vec{t}' = A\vec{t} + \vec{v}, \quad (1.38)$$

que queda definida por una matriz A y un vector \vec{v} , ambos de elementos reales. Para resumir, en ocasiones se refiere a la descomposición afín de \mathcal{E} como (A, \vec{v}) . Los canales de Pauli son uniales⁵ y por lo tanto $\vec{v} = 0$.

Estos canales son importantes, por ejemplo, para el estudio de la distribución cuántica de claves debido a que, para este tipo de protocolos, la presencia de un espía induce la aparición de canales de Pauli [3].

Canal despolarizador

El canal despolarizador representa el escenario en el que perdemos toda la información acerca del estado de un qubit con una probabilidad p . Es decir, transforma cualquier qubit en el estado máximamente mixto $\pi = \mathbf{1}/2$, i.e., un estado con su vector de Bloch nulo $\vec{r} = 0$. La forma del mapa que describe este canal es

$$\rho \rightarrow \rho' = (1-p)\rho + p\pi, \quad (1.39)$$

y sobre el vector de Bloch,

$$\mathcal{E}(\rho) : \vec{t} \rightarrow \vec{t}' = \text{diag}(1-p, 1-p, 1-p) \vec{t}. \quad (1.40)$$

⁵En la Sección 1.3.4 profundizamos en la definición y caracterización de los mapas uniales.

Con sus matrices de Kraus [13]:

$$\begin{aligned} K_1 &= \sqrt{1 - \frac{3p}{4}} \mathbf{1}, & K_2 &= \sqrt{\frac{p}{4}} \sigma_x, \\ K_3 &= \sqrt{\frac{p}{4}} \sigma_y, & K_4 &= \sqrt{\frac{p}{4}} \sigma_z. \end{aligned} \quad (1.41)$$

Canal amortiguador de amplitud

El canal amortiguador de amplitud (*amplitude damping channel*) se puede expresar en las matrices de Kraus:

$$K_1 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-p} \end{pmatrix}, \quad K_2 = \begin{pmatrix} 0 & \sqrt{p} \\ 0 & 0 \end{pmatrix}, \quad (1.42)$$

Dicho mapa actúa sobre el vector de Bloch \vec{t} de un estado cualquiera ρ tal que

$$\mathcal{E}(\rho) : \vec{t} \rightarrow \vec{t}' = \text{diag}(\sqrt{1-p}, \sqrt{1-p}, 1-p) \vec{t} + p\hat{k} = A\vec{t} + p\hat{k}. \quad (1.43)$$

Interacción con el entorno

En ocasiones nos puede ser útil modelizar el ruido como una interacción con el entorno. Supongamos un sistema S que comienza en un estado ρ_S y existe otro sistema asociado al entorno, E, en un estado puro $\rho_E = |0\rangle\langle 0|_E$, entonces el estado inicial del sistema es

$$\rho = \rho_S \otimes |0\rangle\langle 0|_E. \quad (1.44)$$

Supongamos ahora que ambos subsistemas interactúan de acuerdo a un operador U_{SE} que actúa en el espacio conjunto, si nos interesa únicamente la evolución del sistema S podemos definir nuestro canal haciendo uso de la traza parcial

$$\mathcal{E}(\rho) = \text{Tr}_E [U_{SE}(\rho_S \otimes |0\rangle\langle 0|_E)U_{SE}^\dagger]. \quad (1.45)$$

Esta evolución es equivalente a un mapa CPTP con los operadores de Kraus

$$K_i \equiv \langle i|_E U_{SE} |0\rangle_E. \quad (1.46)$$

En la próxima sección daremos una definición más general sobre este tipo de representación.

1.3 Representaciones

1.3.1 Representaciones \mathcal{A} y \mathcal{B}

Podemos expresar la operación dinámica cuántica más general como [13]:

$$\rho'(t) = \mathcal{A}(t)\rho(t_0), \quad (1.47)$$

donde los elementos de los operadores densidad se han reorganizado como vectores columna. Veamos esta expresión de forma más explícita:

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

denota la matriz densidad de un qubit en la base computacional, $|0\rangle = (1, 0)^T$ y $|1\rangle = (0, 1)^T$. Entonces $\rho' = \mathcal{A}\rho$ se puede entender como

$$\begin{pmatrix} \rho'_{00} \\ \rho'_{01} \\ \rho'_{10} \\ \rho'_{11} \end{pmatrix} = \begin{pmatrix} \mathcal{A}_{00;00} & \mathcal{A}_{00;01} & \mathcal{A}_{00;10} & \mathcal{A}_{00;11} \\ \mathcal{A}_{01;00} & \mathcal{A}_{01;01} & \mathcal{A}_{01;10} & \mathcal{A}_{01;11} \\ \mathcal{A}_{10;00} & \mathcal{A}_{10;01} & \mathcal{A}_{10;10} & \mathcal{A}_{10;11} \\ \mathcal{A}_{11;00} & \mathcal{A}_{11;01} & \mathcal{A}_{11;10} & \mathcal{A}_{11;11} \end{pmatrix} \begin{pmatrix} \rho_{00} \\ \rho_{01} \\ \rho_{10} \\ \rho_{11} \end{pmatrix}. \quad (1.48)$$

La matriz \mathfrak{B} se obtiene reorganizando los elementos de \mathcal{A} de forma que $\mathfrak{B}_{i',j'ij} = \mathcal{A}_{i'j'ij}$, por lo tanto

$$\mathfrak{B} = \begin{pmatrix} \mathcal{A}_{00;00} & \mathcal{A}_{00;01} & \mathcal{A}_{01;00} & \mathcal{A}_{01;01} \\ \mathcal{A}_{00;10} & \mathcal{A}_{00;11} & \mathcal{A}_{01;10} & \mathcal{A}_{01;11} \\ \mathcal{A}_{10;00} & \mathcal{A}_{10;01} & \mathcal{A}_{11;00} & \mathcal{A}_{11;01} \\ \mathcal{A}_{10;10} & \mathcal{A}_{10;11} & \mathcal{A}_{11;10} & \mathcal{A}_{11;11} \end{pmatrix} = \rho\mathcal{E}. \quad (1.49)$$

La matriz \mathfrak{B} (también llamada matriz de Choi [14], matriz dinámica o mapa dinámico), representa la transformación más general que se le puede aplicar a un sistema cuántico además de tener numerosas aplicaciones como veremos más adelante.

1.3.2 Representación de Kraus

Como ya vimos brevemente en la Sección 1.2.3, dado un mapa CPTP, \mathcal{E} , sobre el conjunto de operadores del sistema S positivos semi-definidos, hermíticos y de traza unidad, $\mathcal{B}_1^+(\mathcal{H}_S)$, tal que

$$\mathcal{E}(\rho) = \text{Tr}_E[U(t)(\rho_S(t_0) \otimes |0\rangle\langle 0|)U^\dagger(t)], \quad (1.50)$$

donde tomamos un sistema auxiliar puro $\rho_E = |0\rangle\langle 0|$ y $U(t)$ es una transformación unitaria sobre $\mathcal{H} = \mathcal{H}_S \otimes \mathcal{H}_E$ (esta se conoce como la representación de sistema-entorno de Stinesprig [15]). Podemos definir los operadores de Kraus (K_α) como [2] [13]

$$K_\alpha = \langle e_k|A|0\rangle, \quad (1.51)$$

siendo $|e_k\rangle$ un conjunto de estados puros que forman una base ortonormal en \mathcal{H}_E . Y la representación de Kraus de un mapa cuántico se obtiene reescribiendo la Ecuación 1.50,

$$\mathcal{E}(\rho) = \sum_\alpha K_\alpha \rho K_\alpha^\dagger. \quad (1.52)$$

Esta representación no es única y que exista para un mapa es equivalente a que la matriz de Choi sea positiva. Por otro lado también podemos relacionar \mathcal{A} con los operadores de Kraus de la siguiente forma

$$\mathcal{A} = \sum_\alpha K_\alpha \otimes K_\alpha^*. \quad (1.53)$$

Y a partir de esto podemos deducir que los operadores de Kraus son la versión en forma de matriz de los autovectores de \mathfrak{B} ,

$$\mathfrak{B} = \sum_{\alpha} \lambda_{\alpha} |\alpha\rangle\langle\alpha| = \sum_{\alpha} |K_{\alpha}\rangle\rangle\langle\langle K_{\alpha}|, \quad (1.54)$$

i.e., $K_{\alpha} = \sqrt{\lambda_{\alpha}} \text{mat} |\alpha\rangle$. Como dijimos antes, los operadores de Kraus no son únicos y este resultado en concreto se conoce como el conjunto canónico de operadores de Kraus. Entonces un mapa tendrá tantos operadores de Kraus como autovalores no nulos tenga la matriz \mathfrak{B} que lo define [13].

1.3.3 Matriz de Choi

Como mencionamos anteriormente, la matriz \mathfrak{B} recibe también el nombre de matriz de Choi y es de gran utilidad ya que describe por completo la acción de un mapa⁶. El teorema de Choi [14] dice que para un mapa lineal $\mathcal{E} : \mathcal{C}^{m \times n} \rightarrow \mathcal{C}^{m \times m}$ las siguientes afirmaciones son equivalentes:

1. \mathcal{E} es completamente positivo.
2. La matriz (Matriz de Choi)

$$\rho_{\mathcal{E}} = (\mathbf{1} \otimes \mathcal{E})\rho_{Bell}, \quad (1.55)$$

es una matriz positiva, donde $\rho_{Bell} = |\Phi^+\rangle\langle\Phi^+|$ siendo $|\Phi^+\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle_A \otimes |i\rangle_B$ con $d = 2$ para la base computacional. Esta relación entre canales cuánticos (descritos por mapas completamente positivos) y estados cuánticos (descritos por operadores densidad), se conoce como el isomorfismo de Choi–Jamiołkowski.

Teorema 1.3.1. (Isomorfismo de Choi-Jamiołkowski) El conjunto de los estados cuánticos $\rho : \mathcal{H} \otimes \mathcal{H} \rightarrow \mathcal{H} \otimes \mathcal{H}$ es isomorfo al conjunto de los mapas $\mathcal{E} : \mathcal{B}_1^+(\mathcal{H}) \rightarrow \mathcal{B}_1^+(\mathcal{H})$ completamente positivos y que preservan la traza, de modo que

$$\rho_{\mathcal{E}} = (\mathbf{1} \otimes \mathcal{E})\rho_{Bell}, \quad (1.56)$$

siendo $\rho_{\mathcal{E}}$ la matriz de Choi del mapa. La correspondencia es además uno a uno.

Vemos que para definir la matriz de Choi ha sido necesario añadir un sistema recurso que forma un estado de Bell con el sistema sobre el que actúa el mapa (Fig. 1.1). Veamos más explícitamente la forma de la matriz de Choi usando la notación de la esfera de Bloch,

$$\begin{aligned} \rho_{\mathcal{E}} &= (\mathbf{1} \otimes \mathcal{E})\rho_{Bell}^k = (\mathbf{1} \otimes \mathcal{E})\frac{1}{4} \left(\mathbf{1}_a \otimes \mathbf{1}_b + \sum_i^3 W_i^k \sigma_i \otimes \sigma_i \right) \\ &= \frac{1}{4} \left(\mathbf{1}_a \otimes \mathcal{E}(\mathbf{1}_b) + \sum_i^3 W_i^k \sigma_i \otimes \mathcal{E}(\sigma_i) \right). \end{aligned} \quad (1.57)$$

⁶Además la matriz de Choi es única para cada mapa.

Si tenemos en cuenta la representación afín del mapa (\vec{v}, A) , se puede demostrar que la expresión anterior se reescribe como

$$\rho_{\mathcal{E}} = (\mathbf{1} \otimes \mathcal{E})\rho_{Bell}^k = \frac{1}{4} \left(\mathbf{1}_{ab} + \mathbf{1}_a \otimes \vec{v} \cdot \vec{\sigma} + \sum_{\alpha, \beta=1}^3 A_{\alpha\beta} W_{\alpha}^k \sigma_{\alpha} \otimes \sigma_{\beta} \right). \quad (1.58)$$

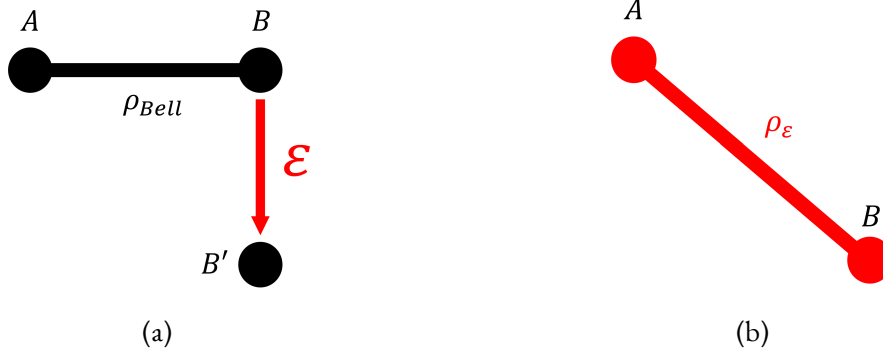


Figura 1.1: Construcción de la matriz de Choi de un mapa a partir de un estado de Bell máximamente entrelazado.

1.3.4 Mapas unitales

Consideremos un mapa \mathcal{E} definido en la base $\{\mathbf{1}, \sigma_{i=1,2,3}\}$ como

$$\mathcal{E}(\mathbf{1}) = \mathbf{1}, \quad (1.59)$$

$$\mathcal{E}(\sigma_i) = z_i \sigma_i, \quad z_i \in \mathbb{R}. \quad (1.60)$$

O escrito de otra forma

$$\mathcal{E}(\rho) = \rho' = \frac{1}{2} (\mathbf{1} + \sum_i z_i a_i \sigma_i) \quad (1.61)$$

donde $\rho = \frac{1}{2} (\mathbf{1} + \sum_i a_i \sigma_i)$. El mapa en la forma de Kraus es unital si y solo si,

$$\sum_{\alpha} K_{\alpha}^{\dagger} K_{\alpha} = \mathbf{1}. \quad (1.62)$$

Estas transformaciones convierten la esfera de Bloch en otra de menor radio o en elipsoides, pero no puede aplastarla hasta formar un disco, ya que eso iría en contra de la condición de un mapa completamente positivo. Además, tampoco desplazan el centro de la esfera de Bloch.

Por otro lado, a partir de la Ecuación 1.61, podemos encontrar la expresión de la matriz de Choi de estos mapas,

$$\mathfrak{B} = \frac{1}{2} \begin{pmatrix} 1 + z_3 & 0 & 0 & z_1 + z_2 \\ 0 & 1 - z_3 & z_1 - z_2 & 0 \\ 0 & z_1 - z_2 & 1 - z_3 & 0 \\ z_1 + z_2 & 0 & 0 & 1 + z_3 \end{pmatrix}. \quad (1.63)$$

Los mapas unitales son todos aquellos que en su descomposición afín $\vec{v} = 0$. Algunos ejem-

plos de mapas unitales son el *phase damping channel*, el *depolarizing channel* o, como ya mencionamos, los canales de Pauli.

1.3.5 Mapas no unitales

También podemos definir mapas dinámicos con cambios afines que además desplazan el centro de la esfera de Bloch. Dichos mapas son no unitales y se definen de la siguiente forma

$$\mathcal{E}(\mathbf{1}) = \mathbf{1} + \sum_i t_i \sigma_i, \quad t_i \in \mathbb{R}, \quad (1.64)$$

$$\mathcal{E}(\sigma_i) = z_i \sigma_i, \quad z_i \in \mathbb{R}. \quad (1.65)$$

Mientras que la forma de la matriz de Choi es

$$\mathfrak{B} = \frac{1}{2} \begin{pmatrix} 1 + t_3 + z_3 & t_1 - it_2 & 0 & z_1 + z_2 \\ t_1 + it_2 & 1 - t_3 - z_3 & z_1 - z_2 & 0 \\ 0 & z_1 - z_2 & 1 + t_3 - z_3 & t_1 - it_2 \\ z_1 + z_2 & 0 & t_1 + it_2 & 1 - t_3 + z_3 \end{pmatrix}. \quad (1.66)$$

Son mapas no unitales, por ejemplo, el *amplitude damping channel* o el canal de despolarización parcial.

1.4 Fidelidad

La medida de la fidelidad nos permite cuantificar como de similares son dos estados cuánticos, lo cuál se vuelve muy útil cuando aparece ruido en nuestros canales cuánticos para poder comprobar como de efectivo es el envío de información. Existen diferentes métodos a la hora de comparar dos estados, dos de las más habituales son la distancia traza y la fidelidad.

Distancia traza

Comenzamos definiendo la distancia traza entre dos estados ρ y σ [2, pg. 403],

$$D(\rho, \sigma) \equiv \frac{1}{2} \text{Tr}[|\rho - \sigma|], \quad (1.67)$$

donde se define $|A| = \sqrt{AA^\dagger}$. Una buena forma de entender lo que está midiendo esta magnitud es a través de la representación en la esfera de Bloch de los estados ρ y σ , supongamos que

$$\rho = \frac{1}{2}(\mathbf{1} + \vec{r} \cdot \vec{\sigma}) \quad \text{y} \quad \sigma = \frac{1}{2}(\mathbf{1} + \vec{s} \cdot \vec{\sigma}). \quad (1.68)$$

Ahora podemos reescribir la Definición 1.67 de la siguiente forma

$$D(\rho, \sigma) = \frac{1}{4} \text{Tr}[|(\vec{r} - \vec{s}) \cdot \vec{\sigma}|]. \quad (1.69)$$

$(\vec{r} - \vec{s}) \cdot \vec{\sigma}$ tiene como autovalores $\pm|\vec{r} - \vec{s}|$, por lo que

$$D(\rho, \sigma) = \frac{1}{2}|\vec{r} - \vec{s}|, \quad (1.70)$$

esto quiere decir que la distancia traza entre dos qubits coincide como la mitad de la distancia euclídea entre sus respectivos vectores en la esfera de Bloch.

Fidelidad

Una segunda medida de la distancia entre dos estados es la fidelidad, aunque a diferencia de la distancia traza esta no es una métrica sobre los qubits. La fidelidad de los estados ρ y σ se define como [2, pg. 409]

$$F(\rho, \sigma) \equiv \text{Tr} \left[\sqrt{\rho^{1/2} \sigma \rho^{1/2}} \right]^2. \quad (1.71)$$

Aunque a primera vista no lo pueda parecer, la fidelidad es simétrica respecto de los estados sobre los que se mide. Un caso particular es cuando ambos estados conmutan, es decir, ambos se pueden expresar en una misma base

$$\rho = \sum_i r_i |i\rangle\langle i| \quad \text{y} \quad \sigma = \sum_i s_i |i\rangle\langle i|, \quad (1.72)$$

lo que nos lleva a que

$$F(\rho, \sigma) = \sum_i \sqrt{r_i s_i} = F(r_i, s_i), \quad (1.73)$$

donde $F(r_i, s_i)$ se conoce como la fidelidad clásica entre las distribuciones de autovalores r_i y s_i .

Capítulo 2

Protocolos cuánticos

El término *protocolos cuánticos* hace referencia al conjunto de procesos cuánticos que se usan en el ámbito de la comunicación cuántica. El modo más general de representarlos matemáticamente es mediante el uso de las denominadas Operaciones Locales y Comunicación Clásica (OLCC). Veamos a continuación los protocolos de teleportación y codificación densa.

2.1 Teleportación

El objetivo que persiguen los diferentes protocolos de teleportación, en cualquiera de sus variantes, es el envío de un estado cuántico, ρ , de un sistema a otro con la mayor fidelidad posible. Utilizando la notación usual: *Alice* es la entidad que *envía* el estado del sistema *A* a otro sistema diferente *B*, controlado por *Bob*.

2.1.1 Teleportación clásica

La versión clásica de la teleportación no aprovecha las propiedades cuánticas del entrelazamiento que, como ya hemos mencionado anteriormente, son de especial interés para la comunicación cuántica. Este protocolo supone que las partes que se quieren comunicar puede utilizar sólo un canal clásico entre ellos. Podemos resumir el protocolo en la siguiente serie de pasos:

1. Alice realiza una **medición POVM** sobre *A*.
2. Alice **transmite** los resultados de la medición a Bob a través de un canal clásico.
3. Bob **prepara** un estado en base a los resultados de la medición de Alice (aquí se supone que Bob tiene una estrategia de preparación óptima en función del resultado de la medición de Alice).

Veamos de forma más pormenorizada en qué consiste el protocolo. Alice dispone de un sistema en un estado ρ desconocido, para extraer información de su estado realiza una medición POVM con n posibles resultados. Dicha medición viene dada por los operadores $\{M_i\}$ que cumplen las siguientes propiedades:

1. $\sum_i^n M_i^\dagger = \sum_i^n c_i^2 \rho_i = \mathbf{1}$,
2. $\rho_i = \rho_i^\dagger \geq 0$,
3. $\text{Tr}[\rho_i] = 1$.

Que implican que

$$\sum_i^n c_i^2 = 2 \quad \text{y} \quad \sum_i^n c_i^2 \vec{s}_i = 0, \quad (2.1)$$

siendo \vec{s}_i el vector de Bloch asociado a ρ_i . La probabilidad de obtener cada uno de los n posibles resultados asociados al operador M_i viene dada por

$$p(\rho_i) = p_i = \frac{c_i^2}{2} (1 + \vec{t} \cdot \vec{s}_i), \quad (2.2)$$

donde \vec{t} es el vector de Bloch del estado ρ .

Tras la medición, Alice envía a Bob los resultados que ha obtenido a través de un canal clásico (sin ruido) y Bob prepara un estado de acuerdo a una estrategia preestablecida. Esto da lugar a un nuevo estado $\tilde{\rho}_i$ (asociado al vector \vec{r}_i) que dependerá de los resultados de la medición de Alice.

La estrategia de preparación óptima, es decir, la que maximiza la fidelidad entre el estado a transmitir y el estado que Bob prepara, está dada por $\vec{r}_i = \vec{s}_i$ [16].

El principal problema de este protocolo reside en que nunca obtendremos el caso óptimo, ya que no hay forma de que Alice extraiga suficiente información de su estado como para que Bob lo reconstruya a la perfección. La fidelidad promedio del protocolo para el envío de un estado puro depende del número N de copias del estado original de las que dispongamos [17],

$$\bar{F}_{max}^N = \frac{N+1}{N+2}. \quad (2.3)$$

Posteriormente G. Vidal [16] generalizó el cálculo de la fidelidad del protocolo para estados mixtos.

2.1.2 Teleportación cuántica

El protocolo de teleportación cuántica aporta otro planteamiento a este problema. En esta ocasión aprovecharemos el entrelazamiento entre dos qubits que formen un estado recurso para aumentar la fidelidad del protocolo. Al igual que antes, organicemos el protocolo en una serie de pasos:

1. **Preparación y reparto** del estado recurso entre Alice y Bob.
2. **Medición** sobre el sistema de Alice.
3. **Transmisión** del resultado de la medición a Bob.
4. **Reconstrucción** del estado original.

Dependiendo del estado recurso que compartan Alice y Bob obtendremos resultados diferentes. Primero veamos como funciona el protocolo si dicho estado pertenece a la base de estados de Bell.

Teleportación con un estado de Bell

El primer paso del protocolo consiste en preparar un estado de Bell a partir de un sistema de dos qubits

$$\rho_{Bell}^{AB} = \frac{1}{4} \left(\mathbf{1}_A \otimes \mathbf{1}_B + \sum_{\alpha=1}^3 W_{\alpha}^k \sigma_{A\alpha} \otimes \sigma_{B\alpha} \right). \quad (2.4)$$

A continuación, enviamos uno de los qubits a Alice y el otro a Bob que se encuentran en laboratorios diferentes. Una vez ambas partes comparten el estado entrelazado, Alice decide que quiere transmitir el estado ρ_a (asociado al vector \vec{t}) a Bob aplicando el protocolo de teleportación cuántica. Para ello realiza una medición PVM sobre su sistema de dos qubits (el que quiere teleportar y el que forma parte del estado de Bell), dicha medición está definida por los operadores

$$M_i = \rho_{Bell}^i = \frac{1}{4} \left(\mathbf{1}_a \otimes \mathbf{1}_A + \sum_{\alpha=1}^3 W_{\alpha}^i \sigma_{a\alpha} \otimes \sigma_{A\alpha} \right), \quad (2.5)$$

que actúa únicamente sobre el subespacio $\mathcal{H}_{aA} = \mathcal{H}_a \otimes \mathcal{H}_A$, es decir, nuestra medición es una proyección sobre la base de estados de Bell (ver Ecs. 1.17-1.20).

A partir del tercer postulado (1.26), sabemos que después de la medición el sistema estará en el estado

$$\rho_i = \frac{1}{p_i} M_i \rho_0 M_i^{\dagger}, \quad (2.6)$$

donde hemos definido $\rho_0 = \rho_a \otimes \rho_{Bell}^{AB}$ ⁷. El estado de Alice quedará destruido después de la medición pero el estado del qubit de Bob se verá afectado debido al entrelazamiento:

$$\rho_{B|i} = \text{Tr}_{aA} [\rho_i] = \frac{1}{p_i} \text{Tr}_{aA} [M_i \rho_0 M_i^{\dagger}] = \frac{1}{p_i} \text{Tr}_{aA} [M_i^{\dagger} M_i \rho_0],$$

por las propiedades de la traza y al ser M_i proyectores, podemos reescribir la expresión anterior como

$$\rho_{B|i} = \frac{1}{p_i} \text{Tr}_{aA} [M_i \rho_0] = \frac{1}{p_i} \text{Tr}_{aA} [(\rho_{Bell}^i \otimes \mathbf{1}_B) (\rho_a \otimes \rho_{Bell}^{AB})]. \quad (2.7)$$

Este es entonces el estado en el que se encuentra el qubit de Bob condicionado por la medición de Alice. Por otro lado, se puede comprobar fácilmente que la probabilidad de obtener cada resultado es $p_i = \frac{1}{4}$.

Desarrollemos la expresión 2.7 para extraer más información sobre el estado de Bob, tras una serie de pasos y simplificaciones llegamos a que

$$\rho_{B|i} = \frac{1}{2} \left(\mathbf{1}_B + \sum_{\alpha} W_{\alpha}^i W_{\alpha}^k t_{\alpha} \sigma_{\alpha} \right) = \frac{1}{2} (\mathbf{1}_B + \vec{t}_{B|i} \cdot \vec{\sigma}), \quad (2.8)$$

donde

- \vec{t} es el vector de Bloch asociado al estado original ρ_a que Alice desea transmitir.
- $\vec{t}_{B|i}$ es el vector de Bloch asociado al estado $\rho_{B|i}$ del qubit de Bob.

⁷Recordemos que para conocer el estado de los subsistemas necesitamos aplicar la traza parcial sobre el estado global: $\rho_a = \text{Tr}_{AB}[\rho_0]$, $\rho_A = \text{Tr}_{aB}[\rho_0]$ y $\rho_B = \text{Tr}_{aA}[\rho_0]$.

- W^i y W^k son las matrices diagonales (1.22) que definen los estados de Bell correspondientes al resultado de la medición (2.5) y al estado que Alice y Bob compartían al principio del protocolo(2.4), respectivamente.

Vemos entonces que el protocolo transforma el vector de Bloch del estado de Bob de forma que coincide con una rotación sobre el vector de Bloch del estado original que Alice quería transmitir:

$$\vec{t}_{B|i} = W^k W^i \vec{t}. \quad (2.9)$$

El paso final consiste en que Bob aplique una rotación R_{ik}^{Bob} sobre su sistema para reconstruir el estado original de Alice,

$$R_{ik}^{Bob} = (W^k W^i)^{-1} = W^k W^i. \quad (2.10)$$

Aplicando este protocolo somos capaces de teleportar un estado cualquiera⁸ sin perder información en el proceso, esto plantea una gran ventaja respecto de la teleportación clásica.

Teleportación con un estado arbitrario

Veamos ahora cómo cambia el protocolo si hacemos que Alice y Bob compartan un estado cualquiera. Nuestro sistema queda descrito inicialmente por el producto tensorial entre el estado a teleportar, ρ_a , y el compartido, ρ_{AB} ,

$$\rho_a = \frac{1}{2} (\mathbf{1} + \vec{t} \cdot \vec{\sigma}), \quad (2.11)$$

$$\rho_{AB} = \frac{1}{4} \left(\mathbf{1}_A \otimes \mathbf{1}_B + \vec{r}_A \cdot \vec{\sigma}_A \otimes \mathbf{1}_B + \mathbf{1}_A \otimes \vec{r}_B \cdot \vec{\sigma}_B + \sum_{i,j=1}^3 C_{ij} \sigma_i \otimes \sigma_j \right). \quad (2.12)$$

Las propiedades de nuestro sistema han cambiado (comparándolo con la Ecuación 2.4) ya que ahora $\vec{r}_A \neq 0$ y $\vec{r}_B \neq 0$, y la matriz C no es necesariamente diagonal. Al igual que antes vamos a mantener la medición sobre la base de estado de Bell,

$$M_i = \rho_{Bell}^i = \frac{1}{4} \left(\mathbf{1}_a \otimes \mathbf{1}_A + \sum_{\alpha=1}^3 W_\alpha^i \sigma_{a\alpha} \otimes \sigma_{A\alpha} \right). \quad (2.13)$$

El estado del qubit de Bob tras la medición de Alice sobre sus qubits es:

$$\rho_{B|i} = \text{Tr}_{aA} \left[(\rho_{Bell}^i \otimes \mathbf{1}_B) (\rho_a \otimes \rho_{AB}) \right] \frac{1}{p_i}. \quad (2.14)$$

Se puede comprobar que el valor que toma la probabilidad de obtener cada estado de Bell tras la medición es:

$$p_i = \frac{1}{4} \left(1 + \sum_{\alpha=1}^3 W_\alpha^i t_\alpha r_{A\alpha} \right) = \frac{1}{4} (1 + W^i \vec{t} \cdot \vec{r}_A), \quad (2.15)$$

ahora no es igual de probable obtener cualquiera de los estados de Bell, sino que la probabilidad de obtener el estado ρ_{Bell}^i al medir va a depender de la medida que hagamos (W^i), del estado que

⁸No es necesario conocer el estado que vamos a teleportar, es más, siempre vamos a considerar un estado genérico.

queramos teleportar (\vec{t}) y del estado del qubit del sistema auxiliar que posee Alice (\vec{r}_A).

Si desarrollamos la expresión del estado $\rho_{B|i}$ llegamos a que

$$\rho_{B|i} = \frac{1}{2} \left[\mathbf{1}_B + \left(\frac{\vec{r}_B + (W^i C)^T \vec{t}}{4p_i} \right) \cdot \vec{\sigma} \right]. \quad (2.16)$$

Entonces, llegados a este punto del protocolo, el vector de Bloch del estado de Bob viene dado por la siguiente expresión:

$$\vec{t}_{B|i} = \frac{\vec{r}_B + (W^i C)^T \vec{t}}{4p_i} = \frac{\vec{r}_B + (W^i C)^T \vec{t}}{1 + W^i \vec{t} \cdot \vec{r}_A} \quad (2.17)$$

Es fácil comprobar que si tomamos $\vec{r}_A = \vec{r}_B = 0$ y $C = W^k$ recuperamos el resultado que obtuvimos en el apartado anterior usando un estado de Bell como sistema recurso (2.17).

En este caso es más complicado para Bob reconstruir el estado original de Alice. Con esta versión del protocolo no podremos teleportar un estado sin perder información, por ello necesitamos que las operaciones que aplique Bob en el paso final sean las óptimas para maximizar la fidelidad del protocolo. Sin precisar que tipo de rotaciones optimizan el protocolo, el estado resultante tras aplicarlo será la suma convexa de los posibles resultados y sus probabilidades, en la notación de la esfera de Bloch,

$$\vec{t} = \sum_i p_i \vec{t}_i = \sum_i p_i R_i^{Bob} \vec{t}_{B|i}. \quad (2.18)$$

2.2 Codificación densa

En esta sección detallaremos el protocolo de codificación densa ya que, como mencionamos antes, la simulación de canales cuánticos constituye una herramienta importante a la hora de caracterizar la capacidad de codificación densa de un canal. El protocolo de codificación densa permite la transmisión de información clásica entre dos partes mediante el uso de sistemas cuánticos. Como veremos a continuación, la preparación de estados de Bell máximamente entrelazados permite codificar $2 \log_2 d$ bits de información clásica en un sistema de dimensión d , sobrepasando el límite clásico $\log_2 d$ [7].

Veamos a continuación el protocolo de codificación densa para $d = 2$, es decir, el sistema global sobre el que el protocolo está definido son dos qubits a los que llamaremos A y B . Supongamos además que Bob desea comunicar a Alice el valor que toma una variable aleatoria discreta $X = \{x_i\}_{i=1}^4$ con cuatro resultados posibles.

En condiciones ideales, la codificación densa hace uso de un canal cuántico sin ruido entre Alice y Bob. En el primer paso del protocolo, Alice usa esta canal para enviar a Bob la parte B de un estado de Bell⁹ ρ_{Bell}^1 , dado por la Ecuación 1.21. Una vez Bob lo ha recibido, aplica sobre él una transformación unitaria \mathcal{U}_i dada por U_i ; esto codifica el mensaje $X = x_i$ en el estado cuántico del sistema. Consecuentemente, el estado que resulta es $\mathbf{1}_A \otimes \mathcal{U}_i(\rho_{Bell}^1)$.

⁹Alice podría usar cualquier estado de Bell.

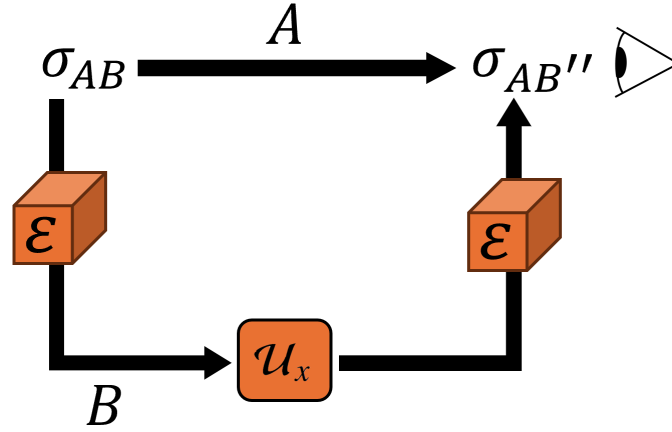


Figura 2.1: Protocolo de codificación densa.

Bob envía el sistema nuevamente a Alice haciendo uso del mismo canal cuántico sin ruido. Finalmente, Alice realiza una medición conjunta sobre todo el sistema AB para recuperar la información clásica, es decir, el valor particular que codificó Bob. El protocolo de codificación densa se basa en que si las operaciones unitarias \mathcal{U}_i están dadas por las matrices $\{U_1 = \mathbf{1}, U_2 = \sigma_3, U_3 = \sigma_1, U_4 = i\sigma_2\}$, entonces $\mathbf{1}_A \otimes \mathcal{U}_i(\rho_{Bell}^1) = \rho_{Bell}^i$, es decir, Alice siempre obtiene alguno de los cuatro estados de Bell dados por la Ecuación 1.21. Como estados estados son ortogonales, si Alice realiza una proyección en la base de Bell, entonces puede obtener el mensaje que Bob codificó. Nótese que esta medición es la misma que se realiza en el protocolo de teleportación, descrito en la Sección 2.1.2.

Ahora bien, consideremos una situación más general: el estado recurso es uno arbitrario, σ_{AB} , y la dimensión ahora es $d \in \mathbb{N}$. Las transformaciones unitarias que Bob aplica están dadas por $U_x = X^l Z^m$ (estos operadores son una generalización de las matrices de Pauli para dimensión d , grupo de Weyl-Heisenberg). La capacidad de este protocolo es: $C(\sigma_{AB})$ es [7]

$$C(\sigma_{AB}) = \max\{\log_2 d, \log_2 d + S(\sigma_B) - S(\sigma_{AB})\} \quad (2.19)$$

donde $\sigma_B = \text{Tr}_A[\sigma_{AB}]$ y $S(\sigma) = -\text{Tr}[\sigma \log_2 \sigma]$ es la entropía de Von Neumann [2, pg. 510]. Para un estado máximamente entrelazado recuperamos el valor de $C = 2 \log_2 d$ que vimos antes.

2.2.1 Protocolo de codificación densa general

Fijémonos ahora en la Figura 2.1 donde el canal de comunicación entre Alice y Bob puede estar sometido a la presencia de ruidos, caracterizados por un mapa \mathcal{E} CPTP. Del mismo modo que en la sección anterior, Alice tiene un estado arbitrario σ_{AB} y envía la parte B de dicho estado a Bob, quien codifica una variable clásica $X := \{x, \pi_x\}_x$ a partir de los operadores \mathcal{U}_x los cuales aplica con una probabilidad π_x . De esta forma Bob genera el estado:

$$\sigma_{AB'}(x) := [\mathbf{1}_A \otimes (\mathcal{U}_x \circ \mathcal{E})_B](\sigma_{AB}). \quad (2.20)$$

A continuación, se devuelve el sistema B' a través del canal cuántico y Alice recibe el sistema B'' en el estado

$$\rho_{AB''}(x) := [\mathbf{1}_A \otimes \mathcal{E}_x](\sigma_{AB}), \quad (2.21)$$

donde $\mathcal{E}_x := \mathcal{E} \circ \mathcal{U}_x \circ \mathcal{E}$. Para recuperar el valor de x , Alice realiza una medida POVM conjunta sobre el sistema AB'' . Asintóticamente, i.e., para muchas repeticiones del protocolo, la información a la que Alice puede acceder del conjunto $\{\pi_x, \rho_{AA''}(x)\}$ viene dada por la cota Holevo [18],

$$\chi(\{\pi_x, \rho_{AB''}\}) = S \left[\sum_x \pi_x \rho_{AB''}(x) \right] - \sum_x \pi_x S [\rho_{AB''}(x)]. \quad (2.22)$$

La capacidad de codificación del canal $C_D^{(1)}(\mathcal{E})$, se obtiene optimizando sobre la variable aleatoria X que Bob desea transmitir, y sobre el estado recurso del protocolo σ , es decir:

$$C_D^{(1)}(\mathcal{E}) = \max_{\sigma, \pi_x} \chi(\{\pi_x, \rho_{AB''}\}). \quad (2.23)$$

Dado que esta cantidad depende de un proceso de optimización complejo, el tratamiento analítico es general muy complicado y, dependiendo de la dimensión a considerar, el cálculo numérico resulta también muy costoso. Como veremos en la Sección 3.1, la simulación de canales cuánticos permite simplificar esta optimización en gran medida.

Capítulo 3

Simulación de canales cuánticos

De cara a entender el punto principal de nuestro estudio necesitamos profundizar en un concepto introducido por Pirandola et al. en 2017 [5]: la simulación de canales cuánticos. En primer lugar necesitamos entender a qué nos referimos con simulación. Lejos de profundizar en métodos de análisis numérico o simulaciones por ordenador, el tipo de simulación a la que hacemos referencia en esta sección es estrictamente teórica ya que se trata de una herramienta que se utiliza como antesala al cálculo de otras magnitudes y medidas que nos ayudan a caracterizar un canal cuántico.

Recordemos brevemente el proceso de teleportación cuántica estándar¹⁰. Al comienzo de nuestro protocolo, Alice posee un estado ρ_a y, al finalizar, ese mismo estado (en el caso ideal) es transferido a Bob, mientras que Alice lo pierde, por esta razón decimos que ocurre una teleportación. Así, podemos representar nuestro protocolo mediante un mapa que devuelve el mismo estado que se introdujo, aunque cambiando el espacio de Hilbert al que pertenece.

$$\mathcal{E}(\rho_a) = \mathcal{T}(\rho_a \otimes \rho_{Bell}) = \rho_b, \quad (3.1)$$

con $\mathcal{E} : \mathcal{B}_1^+(\mathcal{H}_a) \rightarrow \mathcal{B}_1^+(\mathcal{H}_b)$ y \mathcal{T} la representación del protocolo de teleportación cuántica estándar, tomando como estado original ρ_a y como estado recurso ρ_{Bell} . Podemos ampliar esta definición para cualquier otro mapa usando una OLCC (no necesariamente la teleportación estándar¹¹) y un estado recurso σ :

$$\mathcal{E}(\rho) = \mathcal{S}(\rho \otimes \sigma). \quad (3.2)$$

Este nuevo método con el que podemos recrear el efecto de un mapa sobre un estado cuántico usando OLCC es a lo que llamaremos **simulación OLCC de canales cuánticos** [5]. En general, podemos simular el mismo canal \mathcal{E} con diferentes elecciones de \mathcal{S} y σ , es por ello que nos interesa encontrar la combinación que nos permita optimizar el proceso. Por lo general, esto último se consigue utilizando la matriz de Choi del canal como estado recurso, i.e., $\sigma = \rho_{\mathcal{E}}$.

¹⁰Llamaremos a este protocolo “estándar” siempre que Alice tome la base de estados de Bell para realizar sus mediciones.

¹¹Teleportación estándar o teleportación cuántica estándar son términos análogos a lo largo de este trabajo.

Mencionemos ahora algunas definiciones importantes [5]:

Definición 3.0.1 (Canales σ -estirables). Decimos que un canal cuántico \mathcal{E} es “ σ -estirable” si existe una OLCC \mathcal{S} y un estado recurso σ que nos permitan simular el canal. En dicho caso podremos escribir:

$$\mathcal{E}(\rho) = \mathcal{S}(\rho \otimes \sigma). \quad (3.3)$$

Definición 3.0.2 (Canales Choi-estirables). Un canal cuántico \mathcal{E} se denomina como “Choi-estirable” si se puede simular usando una OLCC que tenga como estado recurso la matriz de Choi de dicho canal.

Definición 3.0.3 (Unitarias de teleportación). Una matriz U es una unitaria de teleportación si, dado un estado de Bell ρ_{Bell}^k ,

$$\mathbf{1} \otimes \mathcal{U}(\rho_{Bell}^k) = \rho_{Bell}^j,$$

da como resultado otro estado de Bell para todo j , donde $\mathcal{U}(\sigma) = U\sigma U^\dagger$.

Definición 3.0.4 (Covariante de teleportación). Un canal cuántico es covariante de teleportación (a partir de ahora tele-covariante) si, para cualquier operador unitario de teleportación U , existe un operador unitario V tal que

$$\mathcal{E}(U\rho U^\dagger) = V\mathcal{E}(\rho)V^\dagger. \quad (3.4)$$

El conjunto de matrices U forman el grupo de Weyl-Heisenberg¹² y conforman la generalización de las matrices de Pauli para dimensión n .

Debido a la covarianza de teleportación podemos simular un canal cuántico usando la teleportación estándar mediante su matriz de Choi. Entonces si \mathcal{E} es tele-covariante podemos escribir

$$\mathcal{E}(\rho) = \mathcal{S}(\rho \otimes \rho_{\mathcal{E}}), \quad (3.5)$$

i.e., \mathcal{E} es Choi-estirable (esto lo veremos más en detalle en la Sección 3.2.2). Todos los canales de Pauli (independientemente de su dimensión) son covariantes de teleportación, y por lo tanto Choi-estirables [6].

¹²Ya mencionamos estas matrices en la Sección 1.2.3 en la explicación de canales de Pauli.

3.1 Aplicaciones de la simulación de canales cuánticos

Como anticipamos en la Sección 2.2, una aplicación específica de la simulación OLCC de canales cuánticos es la simplificación del cálculo de capacidades de protocolos como el de codificación densa. Recuperemos entonces la Ecuación 2.23:

$$C_D^{(1)}(\mathcal{E}) = \max_{\sigma, \pi_x} \chi(\{\pi_x, \rho_{AB''}\}).$$

Si el canal \mathcal{E} , cuya capacidad queremos calcular, es tele-covariante (ver Definición 3.0.4) entonces $\mathcal{E}_x = \mathcal{E} \circ \mathcal{U}_x \circ \mathcal{E}$ también es tele-covariante; se sigue entonces que \mathcal{E}_x es Choi-estirable (ver Definición 3.0.2), con lo cual, podemos usar el protocolo de teleportación estándar para simular este canal para todo valor de x :

$$\mathcal{E}_x(\rho) = \mathcal{T}(\rho \otimes \rho_{\mathcal{E}_x}), \quad (3.6)$$

en el cual $\rho_{\mathcal{E}_x} = \mathbf{1} \otimes \mathcal{E}_x(\rho_{Bell})$ es la matriz de Choi del canal \mathcal{E}_x , y ρ_{Bell} es alguno de los estados de Bell dados por la Ecuación 1.21. Este resultado nos permite reescribir [7]

$$\chi(\{\pi_x, \rho_{AB''}\}) = \chi(\{\pi_x, [\mathbf{1}_A \otimes \mathcal{E}_x](\sigma_{AB})\}) = \quad (3.7)$$

$$= \chi(\{\pi_x, [\mathbf{1}_A \otimes \mathcal{T}](\sigma_{AB} \otimes \rho_{\mathcal{E}_x})\}), \quad (3.8)$$

en donde hemos utilizado la expresión de los estados finales del protocolo, Ecuación 2.21, en la primera igualdad, Ecuación 3.7, mientras que en la segunda empleamos la Ecuación 3.6. Por otro lado, la cota Holevo en general se puede expresar utilizando la entropía relativa $S(\rho \parallel \sigma) = \text{Tr}(\rho(\log_2 \rho - \log_2 \sigma))$, del siguiente modo [2],

$$\chi(\{\pi_x, \rho_x\}) = \sum_x \pi_x S(\bar{\rho} \parallel \rho_x), \quad (3.9)$$

para un conjunto arbitrario $\{p_x, \rho_x\}_x$, donde el estado a priori es $\bar{\rho} = \sum_x \pi_x \rho_x$. Por lo tanto, la Ecuación 3.8, resulta:

$$\begin{aligned} \chi(\{\pi_x, [\mathbf{1}_A \otimes \mathcal{T}](\sigma_{AB} \otimes \rho_{\mathcal{E}_x})\}) &= \sum_x \pi_x S(\bar{\rho} \parallel [\mathbf{1}_A \otimes \mathcal{T}](\sigma_{AB} \otimes \rho_{\mathcal{E}_x})) = \\ &= \sum_x \pi_x S\left(\sum_y \pi_y [\mathbf{1}_A \otimes \mathcal{T}](\sigma_{AB} \otimes \rho_{\mathcal{E}_y}) \parallel [\mathbf{1}_A \otimes \mathcal{T}](\sigma_{AB} \otimes \rho_{\mathcal{E}_x})\right) = \\ &= \sum_x \pi_x S\left([\mathbf{1}_A \otimes \mathcal{T}](\sigma_{AB} \otimes \sum_y \pi_y \rho_{\mathcal{E}_y}) \parallel [\mathbf{1}_A \otimes \mathcal{T}](\sigma_{AB} \otimes \rho_{\mathcal{E}_x})\right) \leq \\ &= \sum_x \pi_x S\left(\sigma_{AB} \otimes \sum_y \pi_y \rho_{\mathcal{E}_y} \parallel \sigma_{AB} \otimes \rho_{\mathcal{E}_x}\right) = \sum_x \pi_x S\left(\sum_y \pi_y \rho_{\mathcal{E}_y} \parallel \rho_{\mathcal{E}_x}\right). \end{aligned} \quad (3.10)$$

Para llegar a la Ecuación 3.10, hemos utilizado que la entropía relativa es una cantidad monótona ante la acción de mapas CPTP y, además, la propiedad de subaditividad (última igualdad) [2]. Este es un resultado muy importante puesto que, usando la definición de canales Choi-estirables, la capacidad del protocolo de codificación densa está acotada por:

$$\sum_x \pi_x S\left(\sum_y \pi_y \rho_{\mathcal{E}_y} \parallel \rho_{\mathcal{E}_x}\right) = \chi(\{\pi_x, [\mathbf{1}_A \otimes \mathcal{E}_x](\rho_{Bell})\}), \quad (3.11)$$

es decir, una cantidad que no depende del estado recurso σ . Más aún,

$$C_D^{(1)}(\mathcal{E}) = \max_{\sigma, \pi_x} \chi(\{\pi_x, [\mathbf{1}_A \otimes \mathcal{E}_x](\sigma_{AB})\}) \leq \max_{\pi_x} \chi(\{\pi_x, [\mathbf{1}_A \otimes \mathcal{E}_x](\rho_{Bell})\}), \quad (3.12)$$

para todo estado σ , pero como tenemos igualdad para $\sigma = \rho_{Bell}$, concluimos que la capacidad $C_D^{(1)}(\mathcal{E})$ es máxima cuando el estado recurso es un estado de Bell para cualquier canal \mathcal{E} telecovariante:

$$C_D^{(1)}(\mathcal{E}) = \max_{\pi_x} \chi(\{\pi_x, [\mathbf{1}_A \otimes \mathcal{E}_x](\rho_{Bell})\}). \quad (3.13)$$

Estos argumentos se puede encontrar en los trabajos de Pirandola [5], Cope [6] y Laurenza [7].

3.1.1 Aplicación en estimación de parámetros de sistemas cuánticos

En términos generales, otra aplicación de la simulación OLCC de canales es en *metrología*, cuyo objetivo principal es la estimación de parámetros en información cuántica. En el caso de un canal cuántico \mathcal{E}_θ , caracterizado por un parámetro clásico θ desconocido [19], la simulación permite explorar y entender el comportamiento del canal bajo restricciones de operaciones locales y comunicación clásica (OLCC), lo cual es crucial para numerosas aplicaciones.

Específicamente, un problema relevante en la teoría de la información cuántica es determinar el valor óptimo de θ que minimiza la varianza del estimador $\hat{\theta}$. En este contexto, se busca que la desviación estándar $\delta\theta$ decrezca de manera óptima con el número de pruebas n . Para ciertos canales, el escalado óptimo de $\delta\theta$ es $\delta\theta \sim n^{-1/2}$, conocido como el "límite cuántico estándar" (SQL). Sin embargo, en sistemas cuánticos se puede superar este límite, alcanzando el "límite de Heisenberg" (HL), donde $\delta\theta \sim n^{-1}$.

Para determinar si un canal \mathcal{E}_θ está limitado por el SQL o puede alcanzar el HL, es esencial adoptar los protocolos cuánticos más generales permitidos por la mecánica cuántica. Estos protocolos suelen ser *adaptativos* e involucran el uso de entrelazamiento máximo, optimizando las operaciones cuánticas conjuntas a lo largo de múltiples rondas de prueba. Este enfoque, aunque poderoso, es extremadamente complejo de estudiar y requiere técnicas avanzadas para reducir dicha complejidad [19].

3.2 Simulación de canales de qubits

En su artículo de 2017, Cope et al. [6] afirman que no es posible utilizar el protocolo de teleportación estándar, que involucra tres qubits, para simular canales que no sean de Pauli. De este modo, proponen una modificación de dicho protocolo que implica añadir un canal clásico ruidoso entre Alice y Bob. En este apartado, demostraremos que esta afirmación es, al menos parcialmente, incorrecta, ya que existen canales que, aunque no sean de Pauli, cumplen los requisitos para ser simulados mediante el protocolo de teleportación estándar.

Consideremos entonces un canal cuántico arbitrario \mathcal{E} entre sistemas de dimensión dos. Este tipo de canales se puede expresar mediante su descomposición afín (A, \vec{v}) (ver Ecuación 1.38).

Como vimos en la Sección 2.1.2, el vector del estado final tras aplicar el protocolo de teleportación cuántica estándar, Ec. 2.18, está dado por:

$$\vec{r} = \sum_i p_i \vec{r}_i = \sum_i p_i R_i^{Bob} \vec{r}_{B|i} = \frac{1}{4} \left[\sum_i R_i^{Bob} \vec{r}_B + \sum_i R_i^{Bob} (W^i C)^T \vec{r} \right], \quad (3.14)$$

donde hemos tenido en cuenta la forma explícita que obtuvimos para $\vec{r}_{B|i}$ en la Ec. 2.17, para el estado recurso dado por la Ec. 2.12. Si queremos que nuestro canal sea Choi-estirable necesitamos sustituir nuestro estado recurso por la matriz de Choi del canal, esto es:

$$\vec{r}_B = \vec{v} \quad y \quad C = W^k A^T, \quad (3.15)$$

lo cual viene de la expresión que obtuvimos en Ec. 1.58. De este modo, llegamos a:

$$\vec{r} = \frac{1}{4} \left[\sum_i R_i^{Bob} \vec{v} + \sum_i R_i^{Bob} (A W^k W^i) \vec{r} \right]. \quad (3.16)$$

Para que el canal \mathcal{E} en cuestión sea Choi-estirable por medio de teleportación estándar, tenemos que encontrar las rotaciones R_i^{Bob} de forma que se cumpla la siguiente igualdad,

$$\vec{r} = \frac{1}{4} \left[\sum_i R_i^{Bob} \vec{v} + \sum_i R_i^{Bob} (A W^k W^i) \vec{r} \right] = \vec{v} + A \vec{r}, \quad \forall \vec{r}. \quad (3.17)$$

No todo canal \mathcal{E} es Choi-estirable, con lo cual, buscaremos para qué mapas \mathcal{E} podemos encontrar operaciones de corrección R_i^{Bob} tales que la Ec. 3.17 se cumpla.

Un punto importante es que la Ec. 3.17 se puede reescribir como una composición de mapas:

$$\mathcal{E}(\rho) = \frac{1}{4} \sum_i (\mathcal{U}_i^{Bob} \circ \mathcal{E} \circ \mathcal{U}_i^M)(\rho), \quad (3.18)$$

donde \mathcal{U}_i^M son las transformaciones unitarias asociadas a la medición de Alice¹³, y \mathcal{U}_i^{Bob} son las operaciones de reconstrucción que realiza Bob. Esta es una condición que el canal debe cumplir para cualquier estado cuántico para que sea Choi-estirable.

Combinando los resultados de las ecuaciones 3.16 y 3.18, vemos que cada uno de estos mapas actúa sobre el estado original de la siguiente forma:

$$\mathcal{U}_i^M(\rho) = U_i \rho U_i^\dagger, \quad \text{sobre el vector de Bloch: } \vec{r} \longrightarrow W^k W^i \vec{r}. \quad (3.19)$$

$$\mathcal{E}(\rho), \quad \text{sobre el vector de Bloch: } \vec{r} \longrightarrow \vec{v} + A \vec{r}. \quad (3.20)$$

$$\mathcal{U}_i^{Bob}(\rho), \quad \text{sobre el vector de Bloch: } \vec{r} \longrightarrow R_i^{Bob} \vec{r}. \quad (3.21)$$

Ahora nos hacemos la pregunta: ¿Para qué canales \mathcal{E} podemos encontrar operaciones \mathcal{U}_i^{Bob} tales que la Ecuación 3.18 se satisfaga? Veamos en primer lugar el caso de los canales de Pauli.

¹³Nótese que estas operaciones son las *unitarias de teleportación* que definimos en la Def. 3.0.3.

3.2.1 Los canales de Pauli son Choi-estirables

Antes de adentrarnos en los canales que dan fundamento a este trabajo, detengámonos primero para demostrar por qué los canales de Pauli son siempre Choi-estirables [6]. Partiendo de lo que vimos en la Sección 1.2.3, estos canales son unitales, es decir $\vec{v} = 0$, entonces de acuerdo con la Ec. 3.16, tenemos que:

$$\frac{1}{4} \sum_i R_i^{Bob} (AW^k W^i) \vec{t} = A\vec{t}, \quad \forall \vec{t} \iff \frac{1}{4} \sum_i R_i^{Bob} (AW^k W^i) = A \quad (3.22)$$

Reemplazando ahora la descomposición afín de los canales de Pauli $A = \sum_j q_j W^{k'} W^j$, que podemos calcular a partir de la Ec. 1.37, llegamos a que

$$\frac{1}{4} \sum_i R_i^{Bob} \left(\sum_j q_j W^{k'} W^j \right) W^k W^i = \sum_j q_j W^{k'} W^j. \quad (3.23)$$

Al ser matrices diagonales conmutan entre ellas, entonces tomando $R_i^{Bob} = (W^k W^i)^{-1}$, podemos cumplir con la ecuación anterior. De este modo, hemos comprobado que si reemplazamos la descomposición afín de los canales de Pauli en la Ec. 3.17, podemos encontrar las rotaciones R_i^{Bob} de corrección. Es decir, los canales de Pauli siempre se pueden simular haciendo uso de la teleportación cuántica estándar.

3.2.2 Simulación de canales que no sean de Pauli

Los canales de Pauli constituyen una herramienta importante para modelar ruidos en la teoría de la información cuántica, pero no son los únicos de interés, es por ello que el objetivo de este trabajo se centra en encontrar otro tipo de canales que también se puedan simular a través de su matriz de Choi.

Analicemos a continuación los casos que nos permiten satisfacer la Ecuación 3.18 (que es la condición general para que un canal se pueda simular usando teleportación estándar) y que no sean de Pauli.

Conmutación general

Supongamos que se da

$$\mathcal{E} \circ \mathcal{U} = \mathcal{U} \circ \mathcal{E}, \quad \forall \mathcal{U}, \quad (3.24)$$

es decir, que el canal \mathcal{E} conmute con cualquier operación unitaria (suponemos que actúen en un mismo sistema). En notación del vector de Bloch, la acción compuesta de estas dos operaciones se reescribe como

$$AO\vec{t} + \vec{v} = O(A\vec{t} + \vec{v}), \quad \forall \vec{t} \forall O, \quad (3.25)$$

siendo O una matriz de rotación arbitraria. Dado que esta igualdad se debe cumplir para todo \vec{t} vamos a tomar el caso $\vec{t} = 0$. Entonces, $\vec{v} = O\vec{v}$, para lo cual tenemos que estar en una de las siguientes situaciones:

- i. $\vec{v} = 0$.

2. \vec{v} es el eje de rotación de la rotación O .

Dado que el segundo caso no puede valer para todo O , nos queda que $\vec{v} = 0$. Entonces,

$$AO\vec{t} = OA\vec{t} \quad \forall \vec{t} \quad \implies \quad AO = OA, \quad \forall O, \quad (3.26)$$

que es la definición del centro del grupo de las matrices ortogonales 3×3 y sabemos que toma los valores $\pm \mathbf{1}$, entonces

$$A = \pm \mathbf{1} \quad \text{y} \quad \vec{v} = 0, \quad (3.27)$$

i.e., el caso trivial que ya sabemos que es Choi-estirable, por lo que no nos aporta nada nuevo.

Tele-covariante

Supongamos que nuestro canal conmuta con las unitarias de teleportación \mathcal{U}_i^M (Def. 3.0.3) de la siguiente forma

$$\mathcal{E} \circ \mathcal{U}_i^M = \mathcal{V}_i \circ \mathcal{E}, \quad (3.28)$$

siendo esta la definición de un canal tele-covariante (3.4). A partir de la Ecuación 3.18, que es la condición para que el canal sea Choi-estirable, vemos que es suficiente con tomar $\mathcal{U}_i^{Bob} = \mathcal{V}_i^{-1}$ para que se cumpla. Por lo tanto hemos comprobado que es una condición suficiente para que un canal sea Choi-estirable como se menciona en la Ref. [6].

Igualdad en la suma

Hasta ahora nos hemos centrado en imponer condiciones que se cumplan para cada término de la suma, i.e., para cada i , tratemos de ver qué ocurre si consideramos la suma global. Recordemos que tratamos de encontrar los canales \mathcal{E} con matriz A y vector \vec{v} tales que

$$\frac{1}{4} \sum_i R_i^{Bob} (\vec{v} + AW^k W^i \vec{t}) = \vec{v} + A\vec{t}, \quad \forall \vec{t}. \quad (3.29)$$

Como se tiene que cumplir para todo \vec{t} , tomemos $\vec{t} = 0$,

$$\frac{1}{4} \sum_i R_i^{Bob} \vec{v} = \vec{v}. \quad (3.30)$$

Para que esto ocurra pueden darse tres situaciones:

1. $\vec{v} = 0$. Este caso no nos interesa porque buscamos simular canales que no sean de Pauli.
2. $\frac{1}{4} \sum_i R_i^{Bob} = \mathbf{1}$. Se puede demostrar que esta igualdad se cumple sólo si $R_i^{Bob} = \mathbf{1}$, y este caso no es interesante dado que introduce el término $\sum_i W^i$, que es nulo, en la Ecuación 3.29, lo que implica que podríamos en principio simular canales con la matriz A nula; una cuestión que no es interesante porque el mapa no tendría información del estado sobre el que se aplica (es un caso trivial).
3. $R_i^{Bob} \vec{v} = \vec{v}$ para todo i , es decir, que \vec{v} sea el eje de rotación de R_i^{Bob} . El conjunto de todas las rotaciones en torno al eje definido por \vec{v} viene dado por la fórmula de Rodrigues:

$$R_i^{Bob} = \mathbf{1} + \sin(\theta_i) \hat{v} \cdot \vec{L} + [1 - \cos(\theta_i)] (\hat{v} \cdot \vec{L})^2, \quad (3.31)$$

donde $\hat{v} = \vec{v}/|\vec{v}|$, θ_i define el ángulo de rotación y $\vec{L} = (L_x, L_y, L_z)$ forma la base del grupo de rotaciones $SO(3)$ o rotaciones tridimensionales que preservan la orientación y tienen un determinante igual a uno.

Consideremos ahora este último caso. Siguiendo con la otra parte de la condición impuesta en 3.29, la que hace referencia a la matriz A , tenemos que cumplir con,

$$\frac{1}{4} \sum_i R_i^{Bob} A W^k W^i \vec{r} = A \vec{r}, \quad \forall \vec{r}, \quad (3.32)$$

lo que es equivalente a

$$\frac{1}{4} \sum_i R_i^{Bob} A W^k W^i = A. \quad (3.33)$$

A partir de esta última ecuación podemos demostrar el siguiente resultado:

Teorema 3.2.1. Sea \mathcal{E} un canal cuántico cuya descomposición afín es (A, \vec{v}) . Si A es una matriz con sólo una columna no nula dada por el vector columna \vec{a} y además $\hat{a} \cdot \hat{v} = 0$, i.e., ambos vectores son ortogonales, entonces el canal cuántico \mathcal{E} es Choi-estirable (ver Def. 3.0.2).

Para este caso el canal también es tele-covariante dado que la Ecuación 3.33 se cumple también para cada elemento de la suma.

Demostración:

Retomamos el caso $R_i^{Bob} \vec{v} = \vec{v}$, con

$$R_i^{Bob} = \mathbf{1} + \sin(\theta_i) \hat{v} \cdot \vec{L} + [1 - \cos(\theta_i)] (\hat{v} \cdot \vec{L})^2, \quad (3.34)$$

Y si tomamos $W^k = W^4 = -\mathbf{1}$, por comodidad, la condición 3.33 se reescribe como

$$M = \frac{1}{4} \sum_i R_i^{Bob} A (-W^i). \quad (3.35)$$

Analicemos cada uno de los elementos de la matriz M ,

$$\begin{aligned} M_{\alpha\beta} &= (R_i^{Bob} A)_{\alpha\beta} (-W^i)_{\beta} \\ &= \left[\vec{A}_{\beta} (-W^i)_{\beta} + \sin(\theta_i) (\hat{v} \times \vec{A}_{\beta} (-W^i)_{\beta}) + (1 - \cos(\theta_i)) (\hat{v} \times (\hat{v} \times \vec{A}_{\beta} (-W^i)_{\beta})) \right]_{\alpha} \\ &= (-W^i)_{\beta} \left[\vec{A}_{\beta} \cos(\theta_i) + \sin(\theta_i) (\hat{v} \times \vec{A}_{\beta}) + (1 - \cos(\theta_i)) \hat{v} (\hat{v} \cdot \vec{A}_{\beta}) \right]_{\alpha}, \end{aligned} \quad (3.36)$$

donde hemos aplicado la propiedad $(\hat{v} \cdot \vec{L}) \vec{u} = \hat{v} \times \vec{u}$ y \vec{A}_{β} representa las columnas de la matriz A .

Vemos que si $\hat{v} \cdot \vec{A}_{\beta'} = 0$ para algún $\beta = \beta'$ entonces la Ecuación 3.36 se reescribe como

$$\vec{A}_{\beta'} = (-W^i)_{\beta'} \left[\vec{A}_{\beta'} \cos(\theta_i) + \sin(\theta_i) \hat{v} \times \vec{A}_{\beta'} \right], \quad (3.37)$$

$$\vec{a} = (-W^i)_{\beta'} \left[\vec{a} \cos(\theta_i) + \sin(\theta_i) \hat{v} \times \vec{a} \right], \quad (3.38)$$

donde hemos renombrado la columna β' -ésima de la matriz A como \vec{a} . Además hemos aplicado el cambio $M = A$ como impusimos en la igualdad 3.29. Dado que podemos elegir las rotaciones R_i^{Bob} de forma arbitraria sin pérdida de generalidad, tomamos $\theta_i = n\pi$ con $n \in \mathbb{Z}$, i.e., $\sin(\theta_i) = 0$, para todo i . Entonces

$$\vec{a} = (-W^i)_{\beta'} \cos(\theta_i) \vec{a} \quad \Rightarrow \quad (-W^i)_{\beta'} \cos(\theta_i) = 1. \quad (3.39)$$

Las rotaciones R_i^{Bob} quedan definidas entonces a partir de las ecuaciones 3.34 y 3.39, por lo que cualquier mapa que cumpla las condiciones del Teorema 3.2.1 es Choi-estirable. ■

Una vez hemos obtenido y demostrado el Teorema 3.2.1, pasemos ahora al segundo y último resultado de nuestro trabajo, el cual se deduce también a partir de la Ecuación 3.33:

Teorema 3.2.2. Sea \mathcal{E} un canal cuántico cuya descomposición afín es (A, \vec{v}) . Si A es una matriz con sólo una columna no nula dada por el vector columna \vec{a} y es además antiparalela a \vec{v} , i.e., $\hat{a} \cdot \hat{v} = -1$, entonces el canal cuántico \mathcal{E} es Choi-estirable (ver Def. 3.0.2). Si por el contrario, son vectores paralelos, i.e., $\hat{a} \cdot \hat{v} = 1$, el canal no será Choi-estirable.

Demostración:

Retomemos la Ecuación 3.36,

$$M_{\alpha\beta} = (-W^i)_{\beta} \left[\vec{A}_{\beta} \cos(\theta_i) + \sin(\theta_i) (\hat{v} \times \vec{A}_{\beta}) + (1 - \cos(\theta_i)) \hat{v} (\hat{v} \cdot \vec{A}_{\beta}) \right]_{\alpha}. \quad (3.40)$$

Veamos qué ocurre si tomamos un canal cuántico definido por una matriz A y un vector \vec{v} de tal forma que A tenga su única columna no nula en la misma dirección que \vec{v} . Al considerar esto, $\vec{v} \times \vec{A}_{\beta'} = 0$ para $\beta = \beta'$; podemos reescribir la Ecuación 3.40 tal que

$$\begin{aligned} \vec{A}_{\beta'} &= (-W^i)_{\beta'} \left[\vec{A}_{\beta'} \cos(\theta_i) + (1 - \cos(\theta_i)) \hat{v} (\hat{v} \cdot \vec{A}_{\beta'}) \right], \\ \vec{a} &= (-W^i)_{\beta'} \left[\vec{a} \cos(\theta_i) \pm (1 - \cos(\theta_i)) |\vec{a}| \hat{v} \right] \\ &= (-W^i)_{\beta'} \left[\vec{a} \cos(\theta_i) \pm (1 - \cos(\theta_i)) \vec{a} \right], \end{aligned} \quad (3.41)$$

donde, de nuevo, hemos aplicado el cambio $M = A$ como impusimos en la igualdad 3.29. Entonces se pueden dar dos casos en función de si \vec{v} es paralelo o antiparalelo a \vec{a} . Cuando ambos

son paralelos,

$$\begin{aligned}\vec{a} &= (-W^i)_{\beta'} [\vec{a} \cos(\theta_i) + (1 - \cos(\theta_i)) \vec{a}] \\ &= (-W^i)_{\beta'} \vec{a},\end{aligned}\tag{3.42}$$

llegamos entonces a la conclusión de que **no es Choi-estirable** porque la igualdad no se cumple para todos los casos. Si por el contrario son antiparalelos

$$\begin{aligned}\vec{a} &= (-W^i)_{\beta'} [\vec{a} \cos(\theta_i) - (1 - \cos(\theta_i)) \vec{a}] \\ &= \vec{a} [1 - 2 \cos(\theta_i)] W_{\beta'}^i.\end{aligned}\tag{3.43}$$

Para que se cumpla la igualdad anterior es necesario que

$$1 = [1 - 2 \cos(\theta_i)] W_{\beta'}^i \iff W_{\beta'}^i = [1 - 2 \cos(\theta_i)].\tag{3.44}$$

De este modo, de la ecuación anterior podemos despejar los ángulos correspondientes a R_i^{Bob} , entonces el canal **sí es Choi-estirable**. ■

Capítulo 4

Conclusiones

En este trabajo hemos abordado el desafío de simular canales cuánticos que no son de Pauli utilizando el protocolo de teleportación estándar, introducido en la Sec. 2.1.2. Asimismo, en la Sec. 3.1, vimos un ejemplo específico de por qué estas simulaciones son relevantes, y citamos otras aplicaciones en el ámbito de la estimación de parámetros en la teoría cuántica, ver Sec. 3.1.1.

En el Capítulo 3, hemos demostrado que existe un conjunto de canales cuánticos (Teorema 3.2.1 y Teorema 3.2.2), que se diferencian del grupo de los canales de Pauli y que sí pueden ser simulados mediante el protocolo de teleportación estándar usando su matriz de Choi, i.e., Choi-estirable. Este resultado enriquece las posibilidades de simular canales, puesto que incrementa la cantidad de tipos de canales cuánticos estirables por medio de teleportación estándar [6], y sirve como punto de partida para explorar casos adicionales.

Como hemos mencionado en la Sec. 3.2.2, nuestros resultados contradicen afirmaciones realizadas en el artículo [6]. Es interesante analizar posibles razones por las cuales en este trabajo se afirma que sólo canales de Pauli son simulables por medio de teleportación estándar. Aunque no nos detuvimos a explicarlo en el apartado sobre el protocolo de teleportación cuántica, se puede demostrar que al optimizar el protocolo para aumentar la fidelidad del proceso, la transformación del vector de Bloch del estado inicial luego de aplicar el protocolo de teleportación está dada por:

$$\mathcal{E}_{SQT}^{opt}(\rho) : \vec{t} \rightarrow \vec{t}' = \frac{1}{4} \sum_i [(-W_i) O_{opt} C^T W_i] \vec{t}, \quad (4.1)$$

siendo $R_i = (-W_i) O_{opt}$ las rotaciones que optimizan el protocolo maximizando la figura de mérito correspondiente, es decir, la fidelidad media. En la Ref. [6], sugieren que las operaciones de corrección de Bob son siempre *unitarias de teleportación*, ver Def. 3.0.3. Bajo las suposiciones anteriores, el protocolo sería equivalente a un canal de Pauli, ver Ec. 1.37, lo cual impediría la simulación de cualquier otro canal cuántico que no sea de este tipo. Sin embargo, en el mismo artículo se supone la posibilidad de modificar estas operaciones de corrección sin restricción alguna.

Por último, es importante destacar que nuestros resultados son parciales y aún quedan diversas cuestiones por investigar. Por ejemplo, es necesario identificar la naturaleza de los canales que hemos encontrado y explorar todos los casos en los que su simulación mediante teleportación estándar pueda tener implicancias interesantes. En particular, es crucial calcular la capacidad de codificación densa y estudiar su aplicación en metrología. Además, debemos continuar exhaustivamente con la exploración de todas las posibilidades de simulación para canales de qubits, es

decir, determinar las condiciones necesarias y suficientes para su simulación mediante teleportación. El próximo paso en esta línea de investigación es considerar OLCC más generales que la teleportación estándar.

Bibliografía

- [1] C. Shannon. *The mathematical theory of communication*. University of Illinois Press, 1998. ISBN: 9780252725463. URL: <https://search.worldcat.org/es/title/40716662> (vid. pág. 1).
- [2] Michael A. Nielsen e Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2011. ISBN: 9781107002173 (vid. págs. 1, 2, 4, 8, 9, 14, 17, 18, 24, 28).
- [3] Gregg Jaeger. *Quantum Information: An Overview*. New York, NY, USA: Springer, 2007. DOI: <https://doi.org/10.1007/978-0-387-36944-0> (vid. págs. 1, 2, 12).
- [4] Mark M. Wilde. *Quantum Information Theory*. Cambridge University Press, 2013. ISBN: 9781107176164. URL: <https://books.google.es/books?id=gYcHDgAAQBAJ> (vid. págs. 2, 3, 12).
- [5] Stefano Pirandola et al. «Fundamental limits of repeaterless quantum communications». En: *Nature Communications* 8.1 (abr. de 2017). ISSN: 2041-1723. DOI: [10.1038/ncomms15043](https://doi.org/10.1038/ncomms15043) (vid. págs. 2, 26, 27, 29).
- [6] Thomas P. W. Cope et al. «Simulation of non-Pauli channels». En: *Phys. Rev. A* 96 (2 ago. de 2017), pág. 022323. DOI: [10.1103/PhysRevA.96.022323](https://doi.org/10.1103/PhysRevA.96.022323) (vid. págs. 2, 12, 27, 29, 31, 32, 36).
- [7] Riccardo Laurenza et al. «Dense coding capacity of a quantum channel». En: *Phys. Rev. Res.* 2 (2 abr. de 2020), pág. 023023. DOI: [10.1103/PhysRevResearch.2.023023](https://doi.org/10.1103/PhysRevResearch.2.023023) (vid. págs. 2, 23, 24, 28, 29).
- [8] C. Cohen-Tannoudji, B. Diu y F. Laloë. *Quantum Mechanics, Volume 3: Fermions, Bosons, Photons, Correlations, and Entanglement*. Wiley, 2019. ISBN: 9783527345557. URL: <https://books.google.es/books?id=B3EoswEACAAJ> (vid. pág. 2).
- [9] A.S. Holevo. *Statistical Structure of Quantum Theory*. Lecture Notes in Physics Monographs. Springer, 2001. ISBN: 9783540420828. URL: <https://books.google.es/books?id=CX4-064Rao8C> (vid. págs. 2, 10).
- [10] Gerardo Adesso, Thomas R Bromley y Marco Cianciaruso. «Measures and applications of quantum correlations». En: *Journal of Physics A: Mathematical and Theoretical* 49.47 (nov. de 2016), pág. 473001. DOI: [10.1088/1751-8113/49/47/473001](https://doi.org/10.1088/1751-8113/49/47/473001) (vid. pág. 5).
- [11] Daniel M. Greenberger, Michael A. Horne y Anton Zeilinger. «Going Beyond Bell's Theorem». En: *Bell's Theorem, Quantum Theory and Conceptions of the Universe*. Ed. por Menas Kafatos. Dordrecht: Springer Netherlands, 1989, págs. 69-72. ISBN: 978-94-017-0849-4. DOI: [10.1007/978-94-017-0849-4_10](https://doi.org/10.1007/978-94-017-0849-4_10) (vid. pág. 7).
- [12] W. Pauli. *General Principles of Quantum Mechanics*. Springer-Verlag, 1980. ISBN: 9783540098423. URL: <https://books.google.es/books?id=A84NAQAATAAJ> (vid. pág. 7).

- [13] Vinayak Jagadish y Francesco Petruccione. «An Invitation to Quantum Channels». En: *Quanta* 7.1 (jul. de 2018), pág. 54. ISSN: 1314-7374. DOI: [10.12743/quanta.v7i1.77](https://doi.org/10.12743/quanta.v7i1.77) (vid. págs. 13-15).
- [14] Man-Duen Choi. «Completely positive linear maps on complex matrices». En: *Linear Algebra and its Applications* 10.3 (1975), págs. 285-290. ISSN: 0024-3795. DOI: [https://doi.org/10.1016/0024-3795\(75\)90075-0](https://doi.org/10.1016/0024-3795(75)90075-0) (vid. págs. 14, 15).
- [15] W. Forrest Stinespring. «Positive Functions on C*-Algebras». En: *Proceedings of the American Mathematical Society* 6.2 (1955), págs. 211-216. ISSN: 00029939, 10886826. URL: <http://www.jstor.org/stable/2032342> (visitado 27-04-2024) (vid. pág. 14).
- [16] G. Vidal et al. «Optimal minimal measurements of mixed states». En: *Physical Review A* 60.1 (jul. de 1999), págs. 126-135. ISSN: 1094-1622. DOI: [10.1103/physreva.60.126](https://doi.org/10.1103/physreva.60.126) (vid. pág. 20).
- [17] S. Massar y S. Popescu. «Optimal Extraction of Information from Finite Quantum Ensembles». En: *Phys. Rev. Lett.* 74 (8 feb. de 1995), págs. 1259-1263. DOI: [10.1103/PhysRevLett.74.1259](https://doi.org/10.1103/PhysRevLett.74.1259) (vid. pág. 20).
- [18] A.S. Holevo. «Bounds for the Quantity of Information Transmitted by a Quantum Communication Channel». En: *Probl. Peredachi Inf.* 9 (3 feb. de 1973), págs. 3-11. URL: <https://api.semanticscholar.org/CorpusID:118312737> (vid. pág. 25).
- [19] Riccardo Laurenza et al. «Channel Simulation in Quantum Metrology». En: *Quantum Measurements and Quantum Metrology* 5.1 (2018), págs. 1-12. DOI: [doi : 10 . 1515 / qmetro-2018-0001](https://doi.org/10.1515/qmetro-2018-0001) (vid. pág. 29).