Biblioteca Digital
F C E N - U B A

BIBLIOTECA CENTRAL LUIS F LELOIR
BIBLIOTECA CENTRAL LELOIR
FACULTAD DE CIENCIAS EXACTAS Y NATURALES UBA

Tesis Doctoral

Nuevos algoritmos cuánticos para tomografía de procesos y estados

Bendersky, Ariel Martín

2011

Este documento forma parte de la colección de tesis doctorales y de maestría de la Biblioteca Central Dr. Luis Federico Leloir, disponible en digital.bl.fcen.uba.ar. Su utilización debe ser acompañada por la cita bibliográfica con reconocimiento de la fuente.

This document is part of the doctoral theses collection of the Central Library Dr. Luis Federico Leloir, available in digital.bl.fcen.uba.ar. It should be used accompanied by the corresponding citation acknowledging the source.

Cita tipo APA:
Bendersky, Ariel Martín. (2011). Nuevos algoritmos cuánticos para tomografía de procesos y estados. Facultad de Ciencias Exactas y Naturales. Universidad de Buenos Aires.

Cita tipo Chicago:
Bendersky, Ariel Martín. "Nuevos algoritmos cuánticos para tomografía de procesos y estados". Facultad de Ciencias Exactas y Naturales. Universidad de Buenos Aires. 2011.

EXACTAS UBA
Facultad de Ciencias Exactas y Naturales

UBA
Universidad de Buenos Aires

Dirección: Biblioteca Central Dr. Luis F. Leloir, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires. Intendente Güiraldes 2160 - C1428EGA - Tel. (++54 +11) 4789-9293

Contacto: digital@bl.fcen.uba.ar

UNIVERSIDAD DE BUENOS AIRES

Facultad de Ciencias Exactas y Naturales

Departamento de Física

Nuevos algoritmos cuánticos para tomografía de procesos y estados

Trabajo de Tesis para optar por el título de
Doctor de la Universidad de Buenos Aires en el Área Ciencias Físicas

por Ariel Martín Bendersky

Director de Tesis: Juan Pablo Paz
Lugar de Trabajo: Depto. de Física, FCEyN, UBA

6/10/2011

Resumen

Caracterizar los estados y procesos es una tarea con la que los físicos se cruzan cotidianamente. En esta tesis estudiamos diferentes algoritmos cuánticos para la tomografía de procesos y estados. En una primera parte presentamos dos algoritmos cuánticos para tomografía de procesos selectiva y eficiente y una comparación entre ellos y otros métodos selectivos. En una segunda parte estudiamos la tomografía de estados. Allí vemos en primer lugar un algoritmo de tomografía de estados selectiva y eficiente. Luego presentamos una teoría general de la medición cuando se dispone de dos copias simultáneas del estado cuántico. Ambas partes se encuentran íntimamente relacionadas por la dualidad entre estados y canales, lo que permite mantener en la segunda parte una visión retrospectiva analizando los protocolos de tomografía de estados en virtud de su capacidad de realizar tomografía de procesos.

Palabras clave: información cuántica, tomografía de procesos, tomografía de estados

New quantum algorithms for process and state tomography

Abstract

Characterizing states and processes is a task that a physicist faces on a daily basis. In this thesis we study several quantum algorithms for process and state tomography. In a first part que introduce two quantum algorithms for selective and efficient quantum process tomography, along with a comparision between those and other algorithms. In a second part, we study state tomography. At first we introduce a quantum algorithm for selective and efficient state tomography. Then we present a general theory of measurement when two simultaneous copies of the quantum state are available. Both parts are closely related through a duality between quantum states and channels. This allows to keep a retrospective view analyzing quantum state tomography protocols as a tool for quantum process tomography.

Key words: quantum information, process tomography, state tomography

Índice general

1. Introducción **11**

I Tomografía de procesos cuánticos **15**

2. Tomografía de procesos **17**
2.1. Descripción del problema 18
2.2. Tomografía de procesos cuánticos estándar 19
2.3. Otros métodos para tomografía de procesos 22
2.3.1. Tomografía de procesos asistida por ancilla 22
2.3.2. Caracterización directa de la dinámica cuántica 23
2.3.3. Caracterización simetrizada de procesos cuánticos ruidosos y caracterización de error en procesamiento cuántico de la información 25
2.4. Conclusiones parciales 26

3. Tomografía de procesos cuánticos selectiva y eficiente **27**
3.1. Fidelidad media y promedios sobre el espacio de Hilbert . . . 30
3.1.1. Fidelidad media de un canal 30
3.1.2. Integrales en la medida de Haar y 2–diseños 30
3.2. Medición de coeficientes diagonales 33
3.3. Medición de coeficientes no diagonales 34
3.4. Analisis del error para SEQPT 36
3.5. Extensiones del método SEQPT 38
3.5.1. La importancia de los coeficientes diagonales 38
3.5.2. Medición simultánea de coeficientes diagonales usando probabilidades de transición 40
3.5.3. Detección de coeficientes diagonales principales 41

3.5.4. Análisis del error para la detección simultánea de coeficientes . . . 44
3.6. Conclusiones parciales . . . 44

4. Tomografía de procesos cuánticos selectiva y eficiente sin ancillas 47
4.1. Elementos no diagonales . . . 47
4.1.1. Preparación de estados con ancilla . . . 49
4.2. Tomografía diagonal en otra base . . . 49
4.2.1. Preparación de estados sin ancilla . . . 51
4.3. Conclusiones parciales . . . 53

5. Implementación fotónica de SEQPT y SEQPT sin ancilla 55
5.1. Experimento fotónico de SEQPT . . . 55
5.2. Experimento fotónico de SEQPT sin ancillas . . . 58
5.3. Conclusiones parciales . . . 60

6. Comparación entre métodos de tomografía de procesos 63
6.1. Comparación entre SEQPT y DCQD . . . 64
6.1.1. Preparación de estados mediante mediciones . . . 64
6.1.2. Medición de la fidelidad . . . 65
6.2. Métodos basados en la operación de twirl . . . 66
6.2.1. Twirl de un canal . . . 66
6.2.2. Métodos que utilizan un twirl de todo el espacio . . . 67
6.2.3. Métodos con twirl de un solo qubit . . . 73
6.3. Conclusiones parciales . . . 79

II Tomografía de estados cuánticos 81

7. Tomografía de estados cuánticos 83
7.1. Descripción de los estados cuánticos . . . 83
7.1.1. Expansión en operadores de Pauli generalizados . . . 84
7.1.2. Expansión en una base de $\mathcal{H}$ . . . 85
7.1.3. Tomografía de estados . . . 85
7.2. Mediciones proyectivas y generalizadas . . . 86
7.2.1. Mediciones proyectivas . . . 86
7.2.2. Mediciones generalizadas . . . 87

7.3. Conclusiones parciales 88

8. Teoría general de la medición con dos copias simultáneas del estado 89
8.1. Medición con dos copias simultáneas del estado 90
8.1.1. Medición basada en mapas completamente copositivos 90
8.2. Poder tomográfico de dos copias 92
8.2.1. Poder tomográfico y CCPMVM 96
8.2.2. Comparación con los detectores universales 97
8.2.3. Medición de pureza y concurrencia 98
8.3. Aplicación a la tomografía de procesos 102
8.4. Conclusiones parciales 104

9. Tomografía selectiva y eficiente de estados cuánticos 107
9.1. Tomografía selectiva, eficiente y directa de estados cuánticos . 108
9.2. Aplicación a la tomografía de procesos 110
9.3. Circuitos reducidos 112
9.4. Conclusiones parciales 114

10. Conclusiones generales 115

III Apéndices 117

A. Generalidades sobre mecánica cuántica 119
A.1. Estados puros y mixtos 119
A.1.1. Pureza 120
A.2. Observables y mediciones 120
A.3. Sistemas multipartitos y entrelazamiento 122
A.3.1. Subsistemas 122
A.3.2. Purificación 123
A.3.3. Entrelazamiento y medidas 124
A.4. Evoluciones y canales 125
A.4.1. Positividad y positividad completa 126
A.5. Los qubits y la base computacional 126
A.6. Los operadores de Pauli generalizados 127
A.7. Dualidad entre canales y operadores 128
A.8. Representaciones de procesos cuánticos 129

A.8.1. La matriz χ 129
A.8.2. La representación de Kraus 130
A.9. Computación cuántica basada en circuitos 132
A.9.1. Compuertas cuánticas 133
A.9.2. Complejidad en algoritmos cuánticos 135
A.10.El formalismo de los estabilizadores 136
A.11.El grupo de Clifford 137

B. Bases mutuamente no sesgadas **139**
B.1. Circuitos eficientes de cambio de base 141
B.1.1. Construcción de los circuitos 141

C. Bases mutuamente no sesgadas y 2–diseños **149**
C.1. t–diseños 149
C.2. MUBs y 2–diseños 152

D. Demostración de propiedades para SEQPT **157**

E. POVMs y Teorema de Neumark **159**

Agradecimientos **161**

Bibliografía **162**

Capítulo 1

Introducción

> Desocupado lector: sin juramento me podrás creer que quisiera que este libro, como hijo del entendimiento, fuera el más hermoso, el más gallardo y más discreto que pudiera imaginarse. Pero no he podido yo contravenir al orden de naturaleza, que en ella cada cosa engendra su semejante.
>
> *El Ingenioso Hidalgo Don Quijote de la Mancha.*
> *Miguel de Cervantes Saavedra.*

La utilización de las propiedades cuánticas de la materia para el procesamiento de la infomación ha sido un área de estudio que ha ganado mucho terreno en las últimas dos décadas a partir de las puertas que las nuevas tecnologías han abierto a la manipulación de materia a escalas subatómicas. Ese crecimiento impulsó tanto el área experimental como teórica de la información cuántica[NC04].

El primero en señalar que la mecánica cuántica podía aprovecharse para el procesamiento de la información en formas hasta antes impensadas, fue Richard Feynman en la década de 1980[Fey82]. En 1984, Charles Bennett y Gilles Brassard presentaron el primer protocolo de distribución de claves que aprovechaba las propiedades de la mecánica cuántica[BB84] para dar seguridad incondicional. La idea de que la mecánica cuántica podía permitir realizar aplicaciones computacionales más poderosas que la computación

clásica conocida hasta el momento comenzaba a tomar más fuerza. En el año 1985, David Deutsch mostró que la mecánica cuántica permitía computar algo de manera más eficiente que una computadora clásica[Deu85], con un algoritmo cuántico que fue extendido en 1992 por el propio Deutsch y Richard Jozsa[DJ92]. No quedaban dudas, la mecánica cuántica ofrecía posibilidades computacionales hasta ese momento impensadas.

Sin embargo, fue en 1994 que se produjo el punto de inflexión con la aparición del algoritmo de Shor para la factorización de números enteros[Sho99, NC04]. Ese fue el primer algoritmo cuántico cuyas características repercutían directamente en el mundo clásico: de ser factible fabricar una computadora cuántica, los métodos criptográficos clásicos quedarían obsoletos inmediatamente. La factorización de números enteros, un problema que hasta el momento requería de la utilización de recursos clásicos (tiempo o memoria) exponenciales en la cantidad de dígitos del número a factorizar, pasaba a necesitar una cantidad polinomial de recursos cuánticos. Ese salto de *eficiencia* se convertiría en uno de los puntos fuertes de la computación cuántica.

Por esa época, y en mayor medida a partir de ese momento, se sucedieron una gran cantidad de trabajos relacionando las clases de complejidad algorítmica clásicas con las cuánticas [Wat09, BV93, cY93]. Además se fueron descubriendo otros algoritmos cuyas versiones cuánticas superaban en eficiencia a sus análogos clásicos [Sho99, Gro96, BBBV97, BHT98, MSS05].

Esos desarrollos en algortimos cuánticos empujaron el desarrollo de teoría y experimentos sobre implementaciones de computadoras cuánticas. Para que dichos algoritmos fueran implementables, se volvió necesario tener arquitecturas de computadoras cuánticas tolerantes a errores [Got97, Got96, Got09, ABO97, DS96, NP09, Cho07, ND05]. En esa línea, mucho del esfuerzo fue puesto en la búsqueda de códigos de corrección de errores capaces de proteger al estado de un sistema cuántico frente al ruido.

Ese requerimiento de tolerancia a errores llevó a que se busquen métodos para caracterizar los errores que aparecían en la evolución controlada de un sistema cuántico dado. Dicha caracterización de las evoluciones, denominada tomografía de procesos cuánticos, es el eje central de la presente tesis. Pero para que dicha tarea resulte de alguna utilidad, es fundamental encontrar algoritmos cuánticos que, de manera eficiente, permitan obtener información relevante sobre la evolución de un sistema.

Todos los algoritmos que mencionamos implican, obviamente, la utilización de sistemas cuánticos descriptos por estados y la manipulación de los mismos mediante operaciones o canales cuánticos. La teoría de la información cuántica se nutre fuertemente del estudio de esas dos entidades. Ambas, estados y procesos, poseen muchas características en común debido a una relación de equivalencia entre ambos.

En los últimos años, además, el área de información cuántica se ha tornado cada vez más interdisciplinaria. Desde siempre cercana a la matemática, además se fue acercando a las ciencias de la computación a partir del desarrollo de algoritmos cuánticos y clases de complejidad para los mismos[Wat09]. Por otra parte, se encontraron recientemente sistemas biológicos que también responden a modelos cuánticos, acercando también la biología a la información cuántica[SIFW10, ECR$^+$07].

La presente tesis está organizada en dos grandes partes. La primera sobre la caracterización de procesos cuánticos, también llamada tomografía de procesos cuánticos (o QPT, por su sigla en inglés). Comenzamos en el Capítulo 2 contando generalidades sobre tomografía de procesos, seguido de una descripción de algunos de los principales algoritmos para dicha tarea. En el Capítulo 3 presentamos el método de tomografía de procesos selectiva y eficiente[BPP08, BPP09], desarrollado parcialmente durante esta tesis, que luego fue llevado al experimento en [SLP10]. Luego, en el Capítulo 4 vemos una modificación al método del Capítulo 3 que permite realizar la misma tarea sin necesidad de sistemas auxiliares[SBLP11] junto con su implementación fotónica, que es presentada en el Capítulo 5. El algoritmo de SEQPT sin ancilla fue desarrollado durante esta tesis. Su implementación, en cambio, fue realizada en el marco de la tesis de doctorado de Christian Schmiegelow y el análisis de datos del mismo fue realizado codo a codo durante ambas tesis.

Por último, el Capítulo 6 presenta una comparación entre distintos de los métodos tomográficos vistos que pueden agruparse dentro de una categoría de protocolos basados en la operación de *twirl*[LBPC10]. Dicho trabajo fue realizado en colaboración con David Cory y Cecilia López en ese momento en el MIT.

La segunda parte es sobre caracterización de estados cuánticos, o tomo-

grafía de estados cuánticos (QST por su sigla en inglés) y su relación con la tomografía de procesos. En el Capítulo 7 presentamos algunos aspectos generales sobre QST.

En el Capítulo 8 presentamos una teoría general de la medición cuando se dispone de copias simultáneas del estado a medir[BPC09]. Vemos que dicha teoría permite extraer, simultáneamente, mucha más información que lo que se podría obtener midiendo en ambas copias por separado. Por último, vemos que si se puede medir simultáneamente dos copias del estado, también se puede obtener mucha más información sobre canales cuánticos.

Luego, en el Capítulo 9 damos una presentación a un método de tomografía de estados selectiva y eficiente. Dicho método provee una herramienta que termina siendo de utilidad para una variante selectiva de uno de los protocolos de QPT vistos en la primera parte.

Finalmente, en el Capítulo 10 presentamos las conclusiones generales de la tesis.

Acerca de la lectura de esta tesis, dado el carácter cada vez más interdisciplinario de la información cuántica y la especificidad cada vez mayor de la gente formada en ciencias, se incluye en el Apéndice A una introducción breve y concisa a la mecánica cuántica y a varias de las herramientas que utilizaremos durante toda la tesis. Se recomienda fuertemente al lector que no provenga del estudio de la información cuántica, comenzar por dar una leída rápida pero cuidadosa de dicho apéndice ya que eso facilitará enormemente la lectura de toda la tesis.

La presente tesis ha dado lugar a las siguientes publicaciones originales: El Capítulo 3 se encuentra publicado en [BPP08, BPP09]. El Capítulo 4 está publicado en [SBLP11]. El Capítulo 6 fue publicado en [LBPC10]. Gran parte del Capítulo 8 se encuentra publicada en [BPC09]. Los resultados del Capítulo 9 se encuentran, al momento de la presentación de esta tesis, inéditos.

Parte I

Tomografía de procesos cuánticos

Capítulo 2

Tomografía de procesos

> Esta es la caja. El cordero que quieres está adentro. Con gran sorpresa mía el rostro de mi joven juez se iluminó
>
> ---
>
> *El principito*
> *Antoine de Saint–Exupéry*

Una de las principales limitaciones que se encuentran cuando se desea construir en un laboratorio un dispositivo que realice algún cómputo cuántico, es que la implementación no está libre de errores. Desde los errores al ajustar los parámetros del dispositivo (ángulos de láminas de onda, potenciales eléctricos, etc.) hasta el ruido térmico, todo hace que el dispositivo se comporte de manera levemente distinta al algoritmo teórico que se desea implementar.

Esa limitación hace que una nueva tarea cobre importancia: la tomografía de procesos cuánticos (QPT, por su sigla en inglés). Dicha tarea consiste en caracterizar la evolución de un sistema cuántico. Esa caracterización permite, por ejemplo, determinar las características de los errores cometidos para así buscar un método para proteger al sistema de los mismos.

En éste capítulo daremos una introducción al problema de la tomografía de procesos, y luego haremos un resumen de los principales métodos de tomograía de procesos que existían con anterioridad a nuestro trabajo o que fueron apareciendo durante la realización del mismo.

2.1. Descripción del problema

El estado de un sistema cuántico está descripto por un operador densidad ρ hermítico, positivo y de traza unitaria. Dicho operador puede escribirse en distintas bases. Una de esas bases, que resulta conveniente para varias aplicaciones cuando se trata de sistemas de n qubits, es la base de operadores $\{P_i\}$ que son producto tensorial de n operadores de Pauli. En esa base el estado se escribe como

$$\rho = \frac{1}{D} \sum_i \alpha_i P_i \tag{2.1}$$

donde los coeficientes $\alpha_i = \mathrm{Tr}\,(\rho P_i)$ son obtenidos como valores medios del operador de Pauli correspondiente en el estado ρ.

La descripción de la evolución temporal de un sistema cuántico está dada por un superoperador $\mathcal{E}$. Ese superoperador posee varias restricciones impuestas por la mecánica cuántica. Por un lado, dado que transforma operadores densidad en operadores densidad (se espera que un sistema, luego de la evolución, siga estando en un estado válido), el canal tiene que preservar hermiticidad y ser positivo (Ver Apéndice A.4 o [NC04]). Además, por la linealidad de la mecánica cuántica, tiene que tratarse de un superoperador lineal. El estado ρ' posterior a la evolución es

$$\rho' = \mathcal{E}\,(\rho) \tag{2.2}$$

La tomografía de procesos cuánticos se ocupa, entonces, de proveer algoritmos para la caracterización del superoperador $\mathcal{E}$[NC04]. En particular, nos ocuparemos aquí de sistemas de n qubits (ver Apéndice A.5), es decir, de dimensión $D = 2^n$.

Para caracterizar la evolución de un sistema cuántico, se requiere de algún tipo de descripción del mismo. Una posible descripción es la denominada matriz χ (ver Apéndice A.8.1). En ella se elige una base del espacio de operadores $\mathcal{S} = \{E_m : \mathcal{H} \to \mathcal{H}, m = 0, ..., D^2 - 1\}$, y se escribe el canal en la forma

$$\mathcal{E}\,(\rho) = \sum_{mm'} \chi_{mm'} E_m \rho E_{m'}^\dagger \tag{2.3}$$

donde la matriz χ es hermítica si el canal preserva hermiticidad, es positiva si el canal es completamente positivo (ver Apéndice A.4.1) y si el canal preserva traza, entonces $\sum_{mm'} \chi_{mm'} E_{m'}^\dagger E_m = \mathbb{I}$.

Un punto interesante a notar es que la descripción completa del canal requiere de $D^4 + D^2$ números reales, que corresponden a la matriz χ completa.

Por lo tanto, dicha tarea no es nunca eficiente ya que se trata de una cantidad exponencial en el número de qubits. Por lo tanto, además de los métodos de caracterización completa es importante tener algún algoritmo para obtener información parcial sobre el sistema. De esa forma, podría obtenerse información relevante sobre la evolución de forma eficiente.

Ejemplo: La matriz χ del CNOT

Una compuerta cuántica muy utilizada para un sistema de dos qubits es el CNOT. Ella actúa como un negador controlado de la siguiente forma:

$$U_{\text{CNOT}} |i\rangle \otimes |j\rangle = |i\rangle \otimes |j \oplus i\rangle \tag{2.4}$$

donde $i, j \in \{0, 1\}$ y $\oplus$ simboliza la suma módulo 2.

Para llevarla a la forma de la matriz χ en la base de operadores de Pauli generalizados, se debe desarrollar U_{CNOT} en dicha base de operadores. Al hacerlo se obtiene

$$U_{\text{CNOT}} = \frac{1}{2} \left((\mathbb{I} - \sigma_z) \otimes \sigma_x + (\mathbb{I} + \sigma_z) \otimes \mathbb{I} \right) \tag{2.5}$$

Este canal tiene la particularidad de tener una matriz χ real cuya representación puede verse en la Figura 2.1. La tomografía de procesos consiste en la determinación de la matriz χ de un proceso. A continuación veremos algunos algoritmos cuánticos para realizar dicha tarea. Todo esos algoritmos, sin embargo, poseen la limitación de ser ineficientes para la obtención de coeficientes no diagonales de la matriz χ de un canal arbitrario. En los Capítulos 3 y 4 nos centraremos en el desarrollo de dos algoritmos cuánticos que no poseen dicha limitación.

2.2. Tomografía de procesos cuánticos estándar

Veremos aquí el primer protocolo de tomografía de procesos presentado por Nielsen y Chuang en [NC04]. Este método fue el primero para realizar tomografía de estados, y aunque cumple bien con su cometido de manera simple, no permite obtener información parcial del canal de manera eficiente.

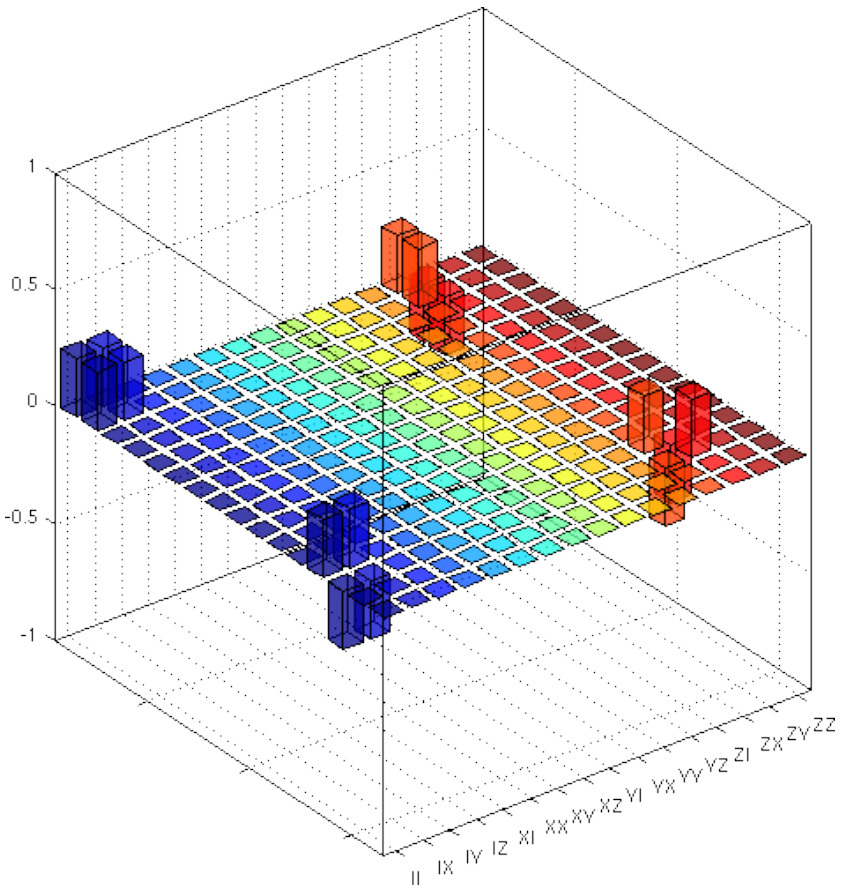

Figura 2.1: Matriz χ de la compuerta CNOT en la base de operadores de Pauli genealizados. Para esta compuerta en particular, la matriz χ es real.

Realizar tomografía de procesos completa a un canal $\mathcal{E}$, implica saber qué transformación realiza dicho canal a cada posible estado de entrada. Puesto que la mecánica cuántica es lineal, alcanza con determinar qué transformación realiza el canal sobre un conjunto de estados cuyos operadores densidad formen una base del espacio de operadores $\mathcal{B}(\mathcal{H})$, definido como el conjunto de operadores lineales $Q : \mathcal{H} \to \mathcal{H}$.

Con eso en mente, se debe elegir un conjunto de D^2 estados cuyos operadores densidad sean linealmente independientes, formando así una base de $\mathcal{B}(\mathcal{H})$ dada por $\mathcal{R} = \{\rho_i, i = 1, ..., D^2\}$. Si la base $\mathcal{R}$ es ortonormal, entonces al medir las transiciones entre los distintos estados de la base se obtiene la matriz λ definida como

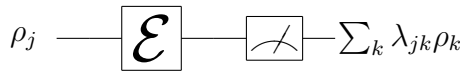

Figura 2.2: Esquema correspondiente a la tomografía de procesos cuánticos estándar.

$$\lambda_{jk} = \mathrm{Tr}\left(\rho_k \mathcal{E}\left(\rho_j\right)\right) \tag{2.6}$$

En el caso más general, en que la base de estados no es ortogonal (este caso general es importante porque muchas de las bases de estados que utilizaremos no lo son), se debe determinar el estado de salida como combinación lineal de los estados de $\mathcal{R}$ utilizando alguno de los algoritmos de tomografía de estados que veremos en la Parte II, obteniendo

$$\mathcal{E}\left(\rho_j\right) = \sum_k \lambda_{jk}\rho_k \tag{2.7}$$

La matriz λ contiene toda la información sobre el canal $\mathcal{E}$. Sin embargo, esa información no se encuentra en una forma en la que pueda resultar de utilidad. Como se explica en el Apéndice A.8.1, la matriz χ sí posee información relevante sobre el canal $\mathcal{E}$. Por lo tanto, debemos transformar la matriz λ a su representación χ en una base de operadores $\mathcal{S} = \{E_m, m = 1, ..., D\}$.

Para eso, de acuerdo a [NC04], se pueden definir coeficientes β_{jk}^{mn} tales que

$$E_m \rho_j E_n^\dagger = \sum_k \beta_{jk}^{mn} \rho_k \tag{2.8}$$

Es claro que esos coeficientes no dependen del canal en cuestión y que pueden calcularse clásicamente a partir de la elección de la base de estados y la de operadores. Eso da lugar a la siguiente relación entre la matriz λ y la matriz χ:

$$\sum_{mn} \beta_{jk}^{mn} \chi_{mn} = \lambda_{jk} \tag{2.9}$$

A partir de la inversión de β se puede obtener la matriz χ. Es importante notar algunos puntos: por un lado, la determinación de λ es ineficiente ya que requiere de $O(D^4)$ mediciones. Esto no es de sorprender ya que describir al canal es una tarea ineficiente. Otra punto negativo de este algoritmo tomográfico es que no permite obtener información parcial sobre la matriz χ

sin medir toda la información del canal en la matriz λ. La ventaja que sí posee, es la de ser un algoritmo simple y práctico para ilustrar la tomografía de procesos.

2.3. Otros métodos para tomografía de procesos

Veremos en esta sección otros métodos para tomografía de procesos que serviran como motivación para los métodos que presentaremos en los capítulos siguientes.

2.3.1. Tomografía de procesos asistida por ancilla

El método de tomografía de procesos asistida por ancilla (AAPT por sus siglas en inglés)[ABJ$^+$03, MRL08] utiliza n qubits auxiliares, y permite extraer toda la información sobre el estado. Sin embargo, ya que es un método pensado para realizar tomografía total, falla en la obtención de información parcial, y es ineficiente.

Este es el primero de dos métodos que mencionaremos aquí que explotan la dualidad entre estados y canales dada por el isomorfismo de Choi–Jamiołkowski (ver Apéndice A.7). Dicho isomorfismo establece una relación de uno a uno entre los canales $\mathcal{E} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ y los operadores de $\mathcal{B}(\mathcal{H} \otimes \mathcal{H})$. Más aún, si el canal es completamente positivo, el operador isomorfo es positivo, y si el canal preserva hermiticidad, el operador correspondiente es hermítico.

La idea del método tomográfico es construir el estado isomorfo al canal $\mathcal{E}$ sobre el que se desea hacer tomografía, y luego hacer tomografía al estado resultante.

El isomorfismo de Choi–Jamiołkowski consiste en la aplicación del canal a una de las partes de un sistema bipartito en el estado máximamente entrelazado en la forma

$$\rho_{\mathcal{E}} = \frac{1}{D} \left(\mathcal{E} \otimes \mathbb{I}\right) \left(\sum_{i,j} |ii\rangle \langle jj| \right). \tag{2.10}$$

Luego de la aplicación del canal a una de las partes, se procede a hacer tomgrafía de estados a $\rho_{\mathcal{E}}$ por alguno de los métodos tradicionales de tomografía de estados (como veremos en la Parte II). La Figura 2.3 ilustra el método.

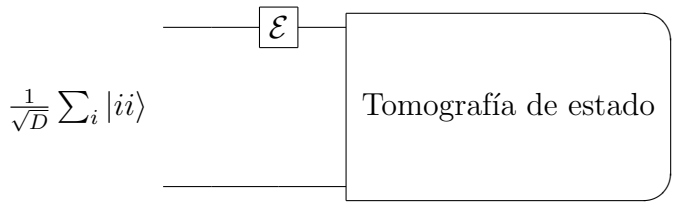

Figura 2.3: Esquema del protocolo de tomografía de procesos asistida por ancilla.

Un punto fuerte del algoritmo de AAPT, es que el estado inicial no tiene que ser necesariamente el máximamente entrelazado. De hecho, cualquier estado de entrada entrelazado con número de Schmidt D^2 capturará toda la dinámica del canal. El resto de los estados forma un conjunto de medida nula, por lo que casi cualquier estado sirve para realizar AAPT.

Este método, además de requerir de n qubits adicionales, posee los siguientes dos inconvenientes relacionados:

- No es claro el rol de la matriz χ del canal $\mathcal{E}$ en la descripción del mismo como estado. Es decir, evidentemente el estado que surge de aplicar el canal a uno de sus dos subsistemas posee toda la información sobre el canal. Sin embargo, no es claro que esa información sea (o no) accesible de manera directa.

- Los algoritmos de tomografía de estados no permiten obtener de manera eficiente la información parcial necesaria para realizar tomografía selectiva de procesos.

Ambos inconvenientes serán resueltos en el Capítulo 9. Por el momento, es importante quedarnos con la idea de que el estado isomorfo a un canal es, potencialmente, una buena herramienta para hacer tomografía de procesos.

2.3.2. Caracterización directa de la dinámica cuántica

La caracterización directa de la dinámica cuántica[MRL08, ML06] (llamado también DCQD por sus siglas en inglés) es un algoritmo parecido en muchos aspectos al AAPT. También utiliza n qubits auxiliares, y se nutre del isomorfismo de Choi–Jamiołkowski. A diferencia del método anterior, la medición de coeficientes diagonales es selectiva y directa. Sin embargo, a la

hora de medir coeficientes no diagonales el método es ineficiente ya que, en el peor caso, requiere invertir una matriz exponencialemente grande.

Consideremos un canal descripto en la base de operadores de Pauli generalizados

$$\mathcal{E}(\rho) = \sum_{mn} \chi_{mn} E_m \rho E_n^\dagger \tag{2.11}$$

Para obtener la parte diagonal de la matriz χ, el algoritmo comienza, igual que el AAPT, generando el estado isomorfo al canal por Choi–Jamiołkowski

$$\rho_{\mathcal{E}} = \frac{1}{D} \sum_{ijmn} \chi_{mn} E_m |i\rangle \langle j| E_n^\dagger \otimes |i\rangle \langle j| . \tag{2.12}$$

Ahora veamos lo siguiente: la probabilidad de obtener a la salida el estado $\frac{1}{\sqrt{D}} \sum_i |ii\rangle$ es

$$\begin{aligned} \frac{1}{D} \sum_{kl} \langle kk| \rho_{\mathcal{E}} |ll\rangle &= \frac{1}{D^2} \sum_{ijklmn} \chi_{mn} \langle kk| E_m |i\rangle \langle j| E_n^\dagger \otimes |i\rangle \langle j| |ll\rangle \\ &= \frac{1}{D^2} \sum_{ijklmn} \chi_{mn} \langle k| E_m |i\rangle \langle j| E_n^\dagger |l\rangle \langle k|i\rangle \langle j|l\rangle \\ &= \frac{1}{D^2} \sum_{mn} \chi_{mn} \mathrm{Tr}(E_m) \mathrm{Tr}\left(E_n^\dagger\right) = \chi_{00}. \end{aligned} \tag{2.13}$$

Es decir, la probabilidad de salir en el mismo estado de entrada es el coeficiente χ_{00}.

Análogamente puede verse que la probabilidad de obtener a la salida el estado $\frac{1}{\sqrt{D}} \sum_i E_k \otimes \mathbb{I} |ii\rangle$ es χ_{kk}. Además, puesto que el conjunto

$$\mathcal{R} = \left\{ \frac{1}{\sqrt{D}} \sum_i E_k \otimes \mathbb{I} |ii\rangle , k = 0, \ldots, D^2 - 1 \right\}$$

forma una base de $\mathcal{H} \otimes \mathcal{H}$, una medición en esa base será suficiente para obtener todos los coeficientes diagonales de la matriz χ.

La dificultad surge asociada a la medición de los coeficientes no diagonales de la matriz χ. La solución es utilizar como estado de entrada uno que no sea máximamente entrelazado. De esa forma, la medición en la base $\mathcal{R}$ incluye información sobre los coeficientes no diagonales. Sin emabrgo, para obtener los coeficientes en cuestión, en el peor caso, se debe invertir un sistema de

ecuaciones exponencialmente grande en el número de qubits n. Por lo tanto el método no es eficiente para la medición de los coeficientes no diagonales. Dicho problema se resuelve con el protocolo que mostraremos en el Capítulo 9.

2.3.3. Caracterización simetrizada de procesos cuánticos ruidosos y caracterización de error en procesamiento cuántico de la información

Los algoritmos para la caracterización simetrizada de procesos cuánticos ruidosos[ESM$^+$07] (SCNQP por sus siglas en inglés) y la caracterización de error en procesamiento cuántico de la información [LLC09, LLEC07] son dos métodos que permiten obtener, mediante operaciones de simetrización, información parcial sobre los canales en cuestión, pero que no permiten obtener ningún tipo de información sobre la parte no diagonal de la matriz χ. No entraremos aquí en demasiados detalles ya que la descripción detallada se dará en el Capítulo 6, pero sí daremos unos breves comentarios introductorios al método.

El método está basado en la idea de transformar el canal original $\mathcal{E}$ en una versión simetrizada $\mathcal{E}'$ a través de operaciones cuánticas denominadas twirl. Luego de la simetrización, sólo los elementos diagonales χ'_{mm} sobreviven, siendo estos los promedios de los coeficientes originales con el mismo peso de Pauli (es decir, con la misma cantidad de operadores de Pauli de un qubit distintos a la identidad). Dependiendo del tipo de twirl que se utilice, se podrá obtener información parcial distinta al medir cada coeficiente diagonal.

El twirl se obtiene utilizando $(O(n))$ compuertas de un solo qubit. Los valores de los coeficientes promediados están relacionados linealmente con las probabilidades medidas mediante una matriz diagonal de tamaño $n+1$. El método es ideal para evaluar cuál es el mejor método de corrección de errores para implementar, ya que obtiene directamente la probabilidad de tener errores de hasta k qubits.

La contra que tiene es que en el simetrizado se pierde toda la información sobre los coeficientes no diagonales, y que no es posible distinguir errores de Pauli distintos que tienen el mismo peso de Hamming.

Los detalles de éste tipo de protocolo se encuentran en el Capítulo 6.

2.4. Conclusiones parciales

Vimos en este capítulo algunas generalidades de tomografía de procesos cuánticos. Además, repasamos varios algoritmos cuánticos para realizar dicha tarea.

Todos esos algoritmos, sin embargo, poseen un problema en común: Ninguno permite obtener cualquier coeficiente de la matriz χ de manera selectiva. Aquellos algoritmos que permiten obtener coeficientes no diagonales (todos los que vimos aquí menos los de la Sección 2.3.3) lo hacen al alto precio de la ineficiencia, requiriendo una cantidad de recursos que crece exponencialmente con el número de subsistemas.

En los próximos tres capítulos nos meteremos de lleno en ese problema, presentando dos métodos para tomografía selectiva y eficiente de procesos cuánticos, y sus respectivas implementaciones experimentales.

Capítulo 3

Tomografía de procesos cuánticos selectiva y eficiente

> Oía pasar los coches ante la verja del jardín. A veces también los veía por los intersticios de la enramada movidos lentamente.
>
> *Contemplación*
> *Franz Kafka*

En este capítulo describiremos el protocolo de tomografía de procesos cuánticos selectiva y eficiente[BPP08, BPP09, Pas08] (SEQPT por sus siglas en inglés), uno de los resultados centrales de esta tesis.

Los protocolos descriptos en el Capítulo 2 poseen ciertas vitudes y defectos. El protocolo de tomografía de procesos estándar (Sección 2.2) resulta práctico cuando se desea caracterizar completamente un canal, pero a la hora de obtener una caracterización parcial de la matriz χ es ineficiente ya que, para dicha caracterización parcial, se debe obtener información completa sobre el canal. Por otra parte, la caracterización directa de la dinámica cuántica (Sección 2.3.2) sí permite obtener eficientemente información parcial sobre la matriz χ, pero el precio a pagar es demasiado alto: se emplean n qubits auxiliares que deben ser inmunes al ruido. Si bien es cierto que dichos recursos son polinomiales en el tamaño del sistema preservando su eficiencia, sería deseable tener un método que no precise utilizar tantos recursos auxiliares, que los mismos no dependan del tamaño del sistema a tomografiar. Por último, la caracterización simetrizada de procesos cuánticos ruidosos (Sección 2.3.3)

no utiliza sistemas auxiliares, permite obtener información parcial sobre el canal, pero falla a la hora de obtener información de fuera de la diagonal de la matriz χ ya que toda esa información es borrada por el protocolo. Además, no permite distinguir entre distintos errores con el mismo peso de Pauli.

El método que presentamos aqui, inspirado en los mencionados anteriormente, tiene la virtud de poder determinar cada elemento de la matriz χ de un canal por separado, es decir, *selectivamente*. La selectividad es fundamental ya que, entre otras cosas, permite caracterizar más eficientemente distintos tipos de canales. Por ejemplo, una compuerta CNOT sólo tiene 8 coeficientes no nulos. La medición de ellos permite afirmar la calidad con la que se la ha implementado sin necesidad de medir los 256 coeficientes de la matriz χ.

Además de eso, el SEQPT realiza la tomografía selectiva de manera eficiente, utilizando recursos que crecen polinomialmente con el número de qubits. Además, la determinación de los elementos diagonales no requiere el uso de sistemas auxiliares, mientras que la de los elementos no diagonales de la matriz χ sólo requiere la utilización de un qubit auxiliar, independientemente de la dimensión del espacio de Hilbert del sistema analizado.

Como hemos dicho en el Capítulo 2 y se detalla en el Apéndice A.8, todo canal lineal admite una representación de matriz χ. Esto es, dada una base del espacio de operadores $\mathcal{B}(\mathcal{H})$, se puede escribir la acción del canal $\mathcal{E}$ sobre un estado ρ arbitrario como

$$\mathcal{E}(\rho) = \sum_{mm'} \chi_{mm'} E_m \rho E_{m'}^\dagger. \tag{3.1}$$

Además, dado que $\mathcal{E}$ no es sólo un mapa sino que representa una operación cuántica, posee algunas propiedades adicionales a la linealidad. Tiene que, al menos, preservar hermiticidad, por lo que $\chi = \chi^\dagger$. También pondremos el requisito de que el canal preserve traza. Eso es, físicamente, hablar de un canal que preserva la probabilidad total. Esa condición, que se escribe como $\mathrm{Tr}\mathcal{E}(\rho) = \mathrm{Tr}\rho$ para todo ρ, se expresa como

$$\sum_{mm'} \chi_{mm'} E_{m'}^\dagger E_m = \mathbb{I} \tag{3.2}$$

dejando en claro que es una condición sobre la matriz χ y la base de operadores elegida[1].

[1]Si bien existen otras condiciones que provienen del hecho de pedir que $\mathcal{E}$ sea un canal

Queda claro, entonces, que la caracterización completa de un canal $\mathcal{E}$ requiere la determinación de $D^4 - D^2$ parámetros reales. Como esa cantidad es exponencialmente grande en el número de subsistemas n del sistema, la tomografía completa no resulta ser una tarea eficiente (es decir, que requiera recursos polinomiales en el número de subsistemas). Una de las ventajas principales de este método es que permite la obtención de información tomográfica importante, aunque no completa, mediante la utilización de recursos que aumentan polinomialmente con n.

Los métodos mencionados anteriormente no permiten la estimación eficiente de un coeficiente arbitrario de la matriz χ. Esta es una de las principales fortalezas del método que discutiremos en este capítulo. Este nuevo método, aunque similar en algunos aspectos al SCNQP (ver Sección 2.3.3), agrega la posibilidad de determinar cualquier coeficiente $\chi_{mm'}$, diagonal o no diagonal, mediante la utilización de recursos que escalean polinomialmente con n.

El método está basado principalmente en dos observaciones: La primera es que cada elemento $\chi_{mm'}$ está relacionado con una probabiidad de superviviencia promedio de ciertos estados de entrada bajo la acción del canal (o cantidades relacionadas con eso). El promedio involucrado es un promedio sobre todo el espacio de Hilbert realizado sobre la llamada medida de Haar, la única medida invariante unitaria normalizada sobre el espacio de estados. La segunda observación es que dichos promedios pueden ser estimados eficientemente mediante un muestreo sobre un conjunto finito de estados denominado 2–diseño, como mostraremos a continuación.

En este capítulo comenzaremos por explicar un prerrequisito para el protocolo de tomografía, veremos como se computan promedios sobre el espacio de Hilbert. Para eso definiremos y discutiremos brevemente el concepto de los 2–diseños. Luego presentaremos el protocolo tomográfico explicando detalladamente como se computa cada elemento de la matriz χ con el método SEQPT. Dicha explicación abordará por separado el caso de los coeficientes diagonales del de los no diagonales. A continuación daremos una descripción detallada de los recursos necesarios para la estimación. Finalmente, veremos como puede extenderse el protocolo para la medición simultánea de todos los coeficientes diagonales.

---

físico, como positividad completa si el estado inicial entre el sistema y su entorno tienen discordia nula[SL09], esta condición no tiene importancia para el protocolo tomográfico que, incluso enfrentado a un proceso que no sea completamente positivo, daría resultados correctos.

3.1. Fidelidad media y promedios sobre el espacio de Hilbert

3.1.1. Fidelidad media de un canal

La fidelidad media de un canal cuántico $\overline{F}(\mathcal{E})$ se define como la probabilidad de supervivencia de un estado al atravesar el canal, promediada sobre todo el espacio de Hilbert. Es decir:

$$\overline{F}(\mathcal{E}) = \int_{\mathcal{H}} d\psi \, \langle\psi| \, \mathcal{E}(|\psi\rangle \langle\psi|) \, |\psi\rangle \tag{3.3}$$

donde la integral es realizada en la medida de Haar sobre la que hablaremos más en la Sección 3.1.2. Esa supervivencia promedio representa, físicamente, la probabilidad de que el canal actúe como la identidad. En otras palabras, es el peso del operador $\mathbb{I}$ en la descripción del canal mediante su matriz χ.

Más en general, se puede hablar de una fidelidad promedio de un canal $\mathcal{E}$ respecto de una operación unitaria U como[Dan05]:

$$\overline{F}_U(\mathcal{E}) = \int_{\mathcal{H}} d\psi \, \langle\psi| \, U^\dagger \mathcal{E}(|\psi\rangle \langle\psi|) U \, |\psi\rangle \, . \tag{3.4}$$

La interpretación física de esa magnitud tiene que ver con la probabilidad de supervivencia promedio de los estados luego de evolucionar con $\mathcal{E}$ y evolucionar hacia atrás con U. Es decir, da una medida de qué tan cerca está la operación $\mathcal{E}$ de la evolución unitaria U. Una utilidad de dicha magnitud tiene que ver con saber qué tanto aproxima una implementación $\mathcal{E}$ al proceso ideal U que se desea implementar. Otra aplicación, que veremos en breve, tiene que ver con el protocolo de tomografía de procesos selectiva y eficiente.

Para que realizar esas integrales sea una tarea accesible, se debe tener una herramienta que permita, eficientemente, realizar esa integral sobre el espacio de Hilbert. Sobre esa integral y su medición como un promedio de una cantidad finita de parámetros hablaremos en la siguiente sección.

3.1.2. Integrales en la medida de Haar y 2–diseños

Un ingrediente primordial del método de tomografía que describiremos, en vistas de poder medir fidelidades medias, es la posibilidad de promediar mediciones sobre todo el espacio de Hilbert. En particular, nos interesará medir

cantidades que son productos de los valores de expectación de dos operadores de la forma

$$\int_{\mathcal{H}} \langle\psi| M |\psi\rangle \langle\psi| N |\psi\rangle \, d\psi \tag{3.5}$$

donde la integral es sobre la medida de Haar, que es la única medida normalizada sobre el espacio de Hilbert invariante frente a transformaciones unitarias. Dicha cantidad, que ya fue estudiada en [RBKSC04] y [Dan05] puede demostrarse (ver Apéndice C para una demostración completa) que tiene como resultado

$$\int_{\mathcal{H}} \langle\psi| M |\psi\rangle \langle\psi| N |\psi\rangle \, d\psi = \frac{\mathsf{tr}(M)\mathsf{tr}(N) + \mathsf{tr}(MN)}{D(D+1)}. \tag{3.6}$$

Si bien puede parecer experimentalmente imposible promediar sobre todo el espacio de Hilbert porque requeriría medir infinitos valores, esto no es tan así. Tanto como la integral numérica de una función $f : \mathbb{R} \to \mathbb{R}$ puede aproximarse evaluando la función en algunos puntos, y que dicha aproximación es exacta si la función es polinomial y los puntos de evaluación son suficientes y están adecuadamente elegidos, en las integrales sobre la medida de Haar ocurre lo mismo: para calcular exactamente la integral de cualquier función cuadrática en $|\psi\rangle$ y $\langle\psi|$ alcanzará con evaluarla sólo en algunos estados y promediar los resultados. El conjunto de esos estados se denomina 2–diseño[Dan05, DCEL09, AE07, KR05][2].

Delsarte [DGS77] mostró como integrar polinomios sobre la esfera puede reducirse al promedio del integrando sobre un conjunto finito de puntos, denominado diseño esférico. Dicho conjunto de puntos es independiente del polinomio en cuestión, por lo que un diseño esférico sirve para integrar cualquier polinomio sobre la esfera, siempre y cuando el grado del polinomio no supere al del diseño. La misma idea puede aplicarse a las integrales sobre el espacio de Hilbert. De esta forma, un 2–diseño de estados $\mathcal{X}$ es un conjunto de estados que satisface para todo par de operadores lineales M y N que

$$\int_{\mathcal{H}} \langle\psi| M |\psi\rangle \langle\psi| N |\psi\rangle \, d\psi = \frac{1}{|\mathcal{X}|} \sum_{\psi\in\mathcal{X}} \langle\psi| M |\psi\rangle \langle\psi| N |\psi\rangle , \tag{3.7}$$

De esta forma, promediar sobre todo el espacio de Hilbert deja de ser una tarea imposible para pasar a ser equivalente a promediar sobre un conjunto

[2]En general, se denomina t–diseño al conjunto de estados que da exactamente el resultado de la integración de un polinomio de grado t en $|\psi\rangle$ y $\langle\psi|$.

finito $\mathcal{X}$, cuyo cardinal es $|\mathcal{X}|$. Esto resuelve el problema de la imposibilidad de medir el promedio pero trae otro nuevo: los 2–diseños tienen una cantidad de estados que crece exponencialmente con n, el número de qubits del sistema. Es decir, pasamos de una tarea imposible a una ineficiente. Sin embargo, se puede encontrar eficientemente una estimación para los promedios que se deben medir. Esta estimación puede obtenerse muestreando al azar sobre todos los estados del conjunto $\mathcal{X}$. Esta idea será crucial para la tomografía selectiva y eficiente de procesos cuánticos.

El último ingrediente para que esto resulte en una herramienta adecuada para la tomografía de procesos, es que no es difícil generar un 2–diseño de estados. De hecho, si se encuentra un conjunto máximo de $D+1$ bases mutuamente no sesgadas (MUBs, por su sigla en inglés), los $D(D+1)$ estados de dichas bases formarán automáticamente un 2–diseño de estados (ver [KR05, Dan05] y el Apéndice C para una demostración completa). Además, siempre existe un conjunto de $D+1$ MUBs para un sistema de dimensión p^n [GHW04, BBRV02, Ben06a].

Para notar los estados del conjunto de MUBs utilizaremos un índice $J = 0, \ldots, D$ para cada una de las bases, y un índice $m = 1, \ldots, D$ para cada uno de los estados de las bases. De esta forma, el estado $\left|\psi_m^J\right\rangle$ corresponderá el m–ésimo estado de la base J–ésima (ver Apéndice B).

Para que el conjunto de $D+1$ bases ortonormales sea efectivamente un conjunto de MUBs, los estados de las mismas deben satisfacer la condición

$$\left|\left\langle \psi_m^J | \psi_n^K \right\rangle\right|^2 = \frac{1}{D} \tag{3.8}$$

para todo $J \neq K$ y para todos m y n. Para la construcción de las $D+1$ MUBs en el caso particular de $D = 2^n$ utilizamos el hecho de que los operadores de Pauli generalizados (ver Sección A.6) se pueden particionar en $D+1$ conjuntos de D operadores mutuamente conmutativos cada uno, con la identidad como único operador común a todos los conjuntos de la partición[BBRV02, Ben06a]. La base que diagonaliza cada uno de esos conjuntos de operadores resultará ser no sesgada con cada una de las otras bases. Así tenemos una descripción de todos los estados pero no una forma operativa de construirlos. La forma de construirlos utilizando $O(n^2)$[Ben06a] compuertas cuánticas de uno y dos qubits y $O(n^3)$ recursos clásicos, puede verse en el Apéndice B. Con esos circuitos cuánticos resulta fácil utilizar los estados de las MUBs para calcular probabilidades de supervivencia y transiciones entre los estados de cada una de esas bases.

3.2. Medición de coeficientes diagonales

La medición de los coeficientes diagonales se basa en una observación principal que se resume en la siguiente propiedad, cuya demostración puede verse en el Apéndice D.

Propiedad 3.1. *Sean un canal* $\mathcal{E}$ *que preserva traza y una base de operadores ortogonal* $\mathcal{S} = \{E_k, k = 0, \ldots, D^2 - 1\}$ *tal que* $\mathrm{Tr}\left(E_m^\dagger E_n\right) = D\delta_{mn}$ *y* $E_0 = \mathbb{I}$. *Entonces se cumple que*

$$\overline{F}\left(\mathcal{E}\right) = \frac{D\chi_{00} + 1}{D + 1}. \tag{3.9}$$

Esta propiedad relaciona la fidelidad media con el coeficiente χ_{00}. Si, además, consideramos el canal modificado $\mathcal{E}_{aa}\left(\rho\right) = \mathcal{E}\left(E_a^\dagger \rho E_a\right)$, su fidelidad media estará relacionada con el coeficiente χ_{aa}. Ese canal es fácilmente implementable como la aplicación de $E_a^\dagger$ seguido de la aplicación del canal $\mathcal{E}$. El otro ingrediente fundamental es que existe un 2–diseño cuyos estados son eficientemente generables y medibles. Si se puede implementar el canal $\mathcal{E}_{aa}$, entonces alcanzará con medir la probabilidad de supervivencia promedio de los estados del 2–diseño.

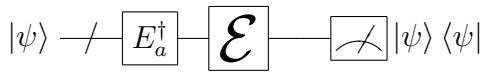

Figura 3.1: Circuito para la medición de los coeficientes χ_{aa} para un canal $\mathcal{E}$.

En la Figura 3.1 se observa el circuito para la medición de los coeficientes diagonales. Dicho circuito debe promediarse sobre todo el espacio de Hilbert o, como se ha mostrado que es equivalente, sobre los estados del 2–diseño. Más aún, un muestreo aleatorio sobre los estados del 2–diseño dará una aproximación al coeficiente χ_{aa}.

Un requisito importante para que el circtuito de la Figura 3.1 pueda implementarse, es que los operadores $E_a^\dagger$ sean implementables. Es deseable también, para que el método sea eficiente, que sean implementables eficientemente. Un ejemplo de operadores que forman una base, son unitarios (implementables) y requieren para su implementación apenas de $O\left(n\right)$ compuertas de un qubit, son los operadores de Pauli generalizados. No sólo eso, sino que la matriz χ en esa base posee información relevante, por ejemplo, para la

elección de un código de corrección de errores. Por ese motivo esa base de operadores es, en muchos casos, una opción adecuada.

Una descripción del algoritmo completo es la siguiente:

1. Inicializar en cero dos contadores $C = 0$ y $T = 0$.
2. Elegir al azar un estado $\left|\psi_m^J\right\rangle$.
3. Aplicarle el operador $E_a^\dagger$.
4. Pasar el estado resultante por el canal $\mathcal{E}$.
5. Medir en la base J. Si se mide el estado m, incrementar C.
6. Incrementar T.
7. Si $\frac{C}{T}$ alcanzó la precisión deseada, detenerse. Si no, volver al paso 2.
8. El resultado es $\frac{D\chi_{aa}+1}{D+1} = \frac{C}{T}$.

En el Apéndice B.1 se muestran los circuitos para obtener eficientemente todos los estados del 2–diseño en cuestión. Eso completa el método para la evaluación de los coeficientes diagonales. Más adelante veremos como calcular el error con el que se miden los coeficientes si se realizan M experimentos.

3.3. Medición de coeficientes no diagonales

Para los coeficientes no diagonales, hay una propiedad análoga a la 3.1 que relaciona el valor del coeficiente no diagonal con la fidelidad promedio de un mapa modificado (ver demostración en el Apéndice D), que es la que nos permitirá medirlos de manera eficiente.

Propiedad 3.2. *Sean un canal $\mathcal{E}$ que preserva traza, y una base de operadores ortogonal $\mathcal{S} = \{E_k, k = 0, \ldots, D^2 - 1\}$ tal que $\mathrm{Tr}\left(E_m^\dagger E_n\right) = D\delta_{mn}$ y $E_0 = \mathbb{I}$. Entonces se cumple que*

$$\overline{F}\left(\mathcal{E}_{ab}\right) = \frac{D\chi_{ab} + \delta_{ab}}{D+1} \tag{3.10}$$

donde $\mathcal{E}_{ab}\left(\rho\right) = \mathcal{E}\left(E_a^\dagger \rho E_b\right)$

A primera vista se ve la dificultad que tiene la medición de coeficientes no diagonales respecto de los diagonales: el mapa $\mathcal{E}_{ab}$ no es un canal físico. Esto se debe a que aplicar un operador por izquierda y otro distinto por derecha no es una operación física (ni siquiera es hermítico). ¿Cómo hacer, entonces, para aprovechar la Propiedad 3.2?

La clave es que mediante la ayuda de una ancilla es posible obtener un resultado parecido al de aplicar operadores distintos por derecha y por izquierda. El circuito de la Figura 3.2 muestra como realizarlo, utilizando un circuito similar al del esquema de computación cuántica DQC1 (computación cuántica determinística con un qubit limpio)[MPS+02].

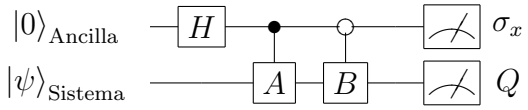

Figura 3.2: Circuito para aplicar operadores distintos por derecha y por izquierda.

El estado previo a la medición es:

$$\begin{aligned}\rho_f = \quad & \frac{1}{2}\left(|0\rangle\langle 0| \otimes B|\psi\rangle\langle\psi|B^\dagger + \right. \\ + \quad & |0\rangle\langle 1| \otimes B|\psi\rangle\langle\psi|A^\dagger + \\ + \quad & |1\rangle\langle 0| \otimes A|\psi\rangle\langle\psi|B^\dagger + \\ + \quad & \left.|1\rangle\langle 1| \otimes A|\psi\rangle\langle\psi|A^\dagger\right). \end{aligned} \tag{3.11}$$

La medición de σ_x elimina los elementos diagonales en la ancilla dejando sólo los no diagonales. El resultado de la medición de $\sigma_x \otimes Q$ es, entonces,

$$\mathrm{Tr}\left(\rho_f \ \ \sigma_x \otimes Q\right) = \frac{1}{2}\mathrm{Tr}\left[\left(B|\psi\rangle\langle\psi|A^\dagger + A|\psi\rangle\langle\psi|B^\dagger\right)Q\right]. \tag{3.12}$$

Es decir, se obtiene el promedio de medirle Q a un estado al que se le aplicaron operadores distintos a derecha y a izquierda sumado a su conjugado hermítico.

Esa observación nos permite, mediante el circuito de la Figura 3.3, medir los coeficientes no diagonales. Nuevamente, el estado $|\psi\rangle$ debe ser tomado al azar entre los estados del 2–diseño.

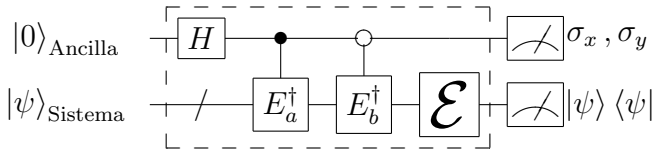

Figura 3.3: Circuito para la medición de χ_{ab} para un canal $\mathcal{E}$. Dependiendo de si se mide σ_x o σ_y en la ancilla, se obtendrá la parte real o la imaginaria, respectivamente.

En efecto, el estado previo a la medición está dado por

$$\begin{aligned}\rho_f = \quad & \frac{1}{2}\Big[|0\rangle\langle 0|\otimes\mathcal{E}\left(E_b^\dagger|\psi\rangle\langle\psi|E_b\right)+\\ + \quad & |0\rangle\langle 1|\otimes\mathcal{E}\left(E_b^\dagger|\psi\rangle\langle\psi|E_a\right)+\\ + \quad & |1\rangle\langle 0|\otimes\mathcal{E}\left(E_a^\dagger|\psi\rangle\langle\psi|E_b\right)+\\ + \quad & |1\rangle\langle 1|\otimes\mathcal{E}\left(E_a^\dagger|\psi\rangle\langle\psi|E_a\right)\Big]. \end{aligned} \tag{3.13}$$

Es fácil ver, ahora, que la medición del valor medio de σ_x y σ_y condicionada a la supervivencia del estado $|\psi\rangle$ y promediando sobre todos los estados del espacio de Hilbert en la medida de Haar, da como resultado el valor real y el imaginario, respectivamente, de los coeficientes no diagonales:

$$\int \mathsf{tr}(\rho_f\,(\sigma_x\otimes|\psi\rangle\langle\psi|))d\psi = \frac{D\mathrm{Re}\,(\chi_{ab})+\delta_{ab}}{D+1} \tag{3.14}$$

$$\int \mathsf{tr}(\rho_f\,(\sigma_y\otimes\ |\psi\rangle\langle\psi|))d\psi = \frac{D\mathrm{Im}\,(\chi_{ab})}{D+1}. \tag{3.15}$$

De esa forma, promediando sólo sobre los estados del 2–diseño, se pueden medir los coeficientes no diagonales. Ese es el núcleo del método de la SEQPT.

3.4. Analisis del error para SEQPT

Además del método para estimar los coeficientes de la matriz χ, es importante poder determinar el error con el que se obtienen.

Al medir los coeficientes diagonales, el resultado de cada experimento[3] sólo puede tener como resultado un 1, correspondiente a la supervivencia del

[3]Cuando hablamos de experimento nos estamos refiriendo a un click aislado del detector.

estado $|\psi\rangle$ o un 0, correspondiente a la no supervivencia. El promedio de todos esos valores resultará en una estimación del valor

$$F_{aa} = \frac{D\chi_{aa} + 1}{D + 1}. \tag{3.16}$$

La desviación estándar de la muestra para los coeficientes diagonales está acotada, entonces, por $\sigma^2_{\text{diag}} \leq \frac{1}{4}$. Por lo tanto, la distribución de los promedios de realizar experimentos en series de M, tendrá, por el teorema del límite central[Wik11b], una distribución normal de desviación estándar $\tilde{\sigma}_{\text{diag}} \leq \frac{1}{2\sqrt{M}}$.

Para los no diagonales, en cambio, el estimador es

$$F_{ab} = \frac{D\chi_{ab}}{D + 1}. \tag{3.17}$$

En este caso, cada experimento puede tomar uno de tres valores, 1 (supervivencia del estado y $|\sigma_x+\rangle$ en la ancilla), -1 (supervivencia del estado y $|\sigma_x-\rangle$ en la ancilla) o 0 (no supervivencia del estado). La cota para la desviación estándar es $\sigma_{\text{no diag}} \leq 1$. Por el teorema del límite central, si se toman M experimentos, la desviación estándar resultará $\tilde{\sigma}_{\text{no diag}} \leq \frac{1}{\sqrt{M}}$ siempre y cuando $M \gg 1$.

Además de eso, para saber cuántos experimentos son necesarios para obtener un error menor que ϵ con probabilidad p, utilizaremos la cota de Chernoff[Che52, Ló09, Wik11c]. Dicha cota dice que si $0 \leq x_i \leq 1$ son variables aleatorias independientes con $i = 1, \ldots, M$, y queremos tener una precisión ϵ y una probabilidad de fallar menor a p, entonces necesitamos que

$$M \geq \frac{\ln\left(\frac{2}{p}\right)}{2\epsilon^2}. \tag{3.18}$$

Esa cota funciona para los coeficientes diagonales. En el caso de los coeficientes no diagonales, la cantidad de experimentos es cuatro veces más ya que los resultados posibles (las variables aleatorias independientes) no están entre 0 y 1 sino entre -1 y 1.

Cada uno de los experimentos, tendrá una complejidad de $O(n^3)$ que proviene de la cantidad de recursos clásicos necesarios para determinar las $O(n^2)$ compuertas cuánticas de uno y dos qubits del circuito de cambio de base necesario (ver Apéndice B.1).

La eficiencia del método proviene de que la cantidad de experimentos, a pesar de depender de la precisión requerida, no depende del número de qubits (o subsistemas) del sistema.

3.5. Extensiones del método SEQPT

En esta sección veremos dos generalizaciones del algoritmo: Una que permite determinar simultáneamente todos los coeficientes diagonales y otra que permite detectar eficientemente los coeficientes diagonales principales. Antes de eso, y a modo de motivación, veremos dos resultados que resaltan la importancia de los coeficientes diagonales de la matriz χ.

3.5.1. La importancia de los coeficientes diagonales

Como se muestra en el Apéndice A.8.1, muchas de las propiedades de los canales cuánticos se reflejan en propiedades de la matriz χ: la positividad completa, la hermiticidad, etc. En esta sección veremos dos propiedades que resultan de gran utilidad para la tomografía de procesos ya que permiten relacionar los coeficientes diagonales con los no diagonales de la matriz χ. La primera de ellas, para canales completamente positivos, dada en [Ló09] y la segunda presentada en [LBPC10]. Esas relaciones permiten determinar, una vez conocidos los coeficientes diagonales, qué elementos no diagonales vale la pena medir.

Matriz χ de canales completamente positivos

La matriz χ de un canal CP, de acuerdo con el Teorema A.1, es positiva. Por lo tanto, se puede definir un producto interno como

$$(\vec{v_1}, \vec{v_2}) = \vec{v_1}^{\dagger} \chi \vec{v_2}. \tag{3.19}$$

Los elementos de la matriz χ se obtienen a partir del producto interno anterior como

$$(\vec{e_m}, \vec{e_n}) = \chi_{mn}, \tag{3.20}$$

donde $\vec{e_m}$ es el m–ésimo vector de la base canónica.

Utilizando el producto interno anterior y la desigualdad de Cauchy–Schwarz[Wik11a] se obtiene la siguiente relación:

$$|\chi_{mn}|^2 \leq \chi_{mm}\chi_{nn}. \tag{3.21}$$

Esto quiere decir que sólo es necesario conocer el bloque de la matriz χ cuyos elementos diagonales son mayores al mínimo valor deseado. El resto

de la matriz, al no tener elementos grandes en la diagonal, tampoco los tendrá fuera de ésta.

Otra propiedad que surge a partir de la norma $(\vec{e_m}, \vec{e_m})$, es que los elementos diagonales son todos positivos.

Matriz χ de canales positivos

Cuando se trata de un canal positivo, ya no es posible afirmar que su matriz χ también lo sea (ese es el caso si y sólo si es CP). Sin embargo, se pueden obtener relaciones similares.

Lo que sí puede hacerse con canales positivos, que llevan operadores positivos a operadores positivos, es definir un producto interno entre operadores de la siguiente forma:

$$\langle E_m, E_n \rangle \equiv \int d\psi \langle \psi | \mathcal{E}(E_m^\dagger |\psi\rangle \langle \psi | E_n) | \psi \rangle \tag{3.22}$$

Un primer resultado importante es que tenemos que $\langle E_m, E_m \rangle = (D\chi_{mm} + 1)/(D+1) \geq 0$. Eso implica que para un canal positivo (pero no necesariamente CP), los elementos diagonales de la matriz χ pueden ser negativos pero no más que un valor exponencialmente pequeño: $\chi_{mm} \geq -1/D$. Además, $\langle E_m, E_m \rangle$ es una probabilidad de supervivencia; la probabilidad que tiene el sistema de permanecer en su estado inicial luego de aplicarle el canal modificado $\mathcal{E}_{mm}$. Por lo tanto, $(D\chi_{mm} + 1)/(D+1) \leq 1$, lo que a su vez implica que $\chi_{mm} \leq 1$.

Más aún, usando nuevamente la desigualdad de Cauchy–Schwarz, pero con este nuevo producto interno, se obtiene que para $m \neq n$

$$|\chi_{mn}|^2 \leq \chi_{mm}\ \chi_{nn} + \frac{\chi_{mm} + \chi_{nn}}{D} + \frac{1}{D^2} \tag{3.23}$$

Luego, para sistemas grandes en los que se puede considerar que $D >> 1$, los elementos de matriz no diagonales están acotados efectivamente por los diagonales.

De esta forma, vimos cómo el conocimiento de los coeficientes diagonales dice mucho sobre los coeficientes no diagonales que se necesitan medir para caracterizar un canal.

3.5.2. Medición simultánea de coeficientes diagonales usando probabilidades de transición

Cuando las MUBs que se utilizan son bases estabilizadas[4] por los mismos operadores de la base $\mathcal{B}(\mathcal{H})$ con la que se describe el canal, pueden aprovecharse algunas propiedades adicionales. En particular, nos concentraremos en el caso en el que los operadores E_a son los operadores de Pauli generalizados.

Supongamos que los proyectores $\Pi_{J,\vec{k}}$ son los estados estabilizados por un conjunto abeliano de operadores de Pauli (ver Apéndice B), donde J sigue indicando la base y el vector $\vec{k}$ contiene los autovalores del estado para cada uno de los generadores del grupo estabilizador. En ese caso podemos simplemente averiguar cómo actúa el operador E_{a_0} por conjugación sobre el estado $\Pi_{J,\vec{k}}$ Por lo tanto, el valor de expectación de

$$\mathrm{Tr}\left(E_{a_0}^{\dagger}\mathcal{E}(\Pi_{J,\vec{k}})E_{a_0}\Pi_{J,\vec{k}}\right)$$

correspondiente a instancias del experimento es igual a

$$\mathrm{Tr}\left(\mathcal{E}(\Pi_{J,\vec{k}})\Pi_{J,\vec{k'}}\right) \tag{3.24}$$

para algún $\vec{k'}$ que depende de $\vec{k}$, J y E_{a_0}. Estamos utilizando aquí una variante del protocolo anterior para coeficientes diagonales en la que se aplica primero el canal y luego el operador E_{a_0}. Esta variante es equivalente a la presentada.

Así queda claro que detectando no sólo la probabilidad de supervivencia del estado, sino todas las probabilidades de transición a los distintos estados de la base J, podemos obtener toda la información necesaria para estimar cualquier coeficiente diagonal y no sólo uno.

La estrategia es simple: se debe mantener la elección aleatoria de los índices $(J,\vec{k})$, y guardar la información sobre el resultado $(J,\vec{k'})$. Dado el operador E_a, el evento debe contarse en la estimación de χ_{aa} sólo si el estado de entrada $(J,\vec{k})$ es mapeado al estado $(J,\vec{k'})$ por la acción del operador E_a.

De esta forma, podemos notar cada repetición del experimento mediante una terna $(J,\vec{k},\vec{k'})$, donde J indica la base elegida al azar para el experimento, $\vec{k}$ es el vector, elegido también al azar, que indica qué estado de la base J se coloca a la entrada del experimento, y $\vec{k'}$ es el vector que representa al estado que se obtiene al hacer, al final del experimento, una medición en la base J.

[4]Ver Apéndice A.10 para un resumen sobre el formalismo de los estabilizadores.

Cada experimento deberá contarse positivamente para la fidelidad de E_a si y solo si el vector $\vec{k'} - \vec{k}$ es el vector de conmutación del operador E_a con respecto a la base $\mathcal{B}_J$. El vector de conmutación de un operador E respecto de una base $\mathcal{B}_J$ es el vector binario $\vec{v}$ tal que

$$J_i E = (-1)^{v_i} E J_i, \tag{3.25}$$

donde $J_1, J_2, \ldots, J_n$ son los generadores canónicos del grupo estabilizador de la base $\mathcal{B}_J$.

El vector de conmutación resulta de gran importancia para la estimación simultánea de los coeficientes diagonales. Veamos como puede ser calculado eficientemente a partir de la descripción canónica de los operadores E_a y la base $\mathcal{B}_J$. El vector E_a puede escribirse a partir de dos vectores binarios $\vec{a_x}$ y $\vec{a_z}$ en la forma

$$E_a = \sigma_x^{\vec{a_x}} \sigma_z^{\vec{a_z}} = \bigotimes_{i=1}^{n} \sigma_x^{(\vec{a_x})_i} \sigma_z^{(\vec{a_z})_i} \tag{3.26}$$

Para la base $\mathcal{B}_J$ pueden ocurrir dos cosas: o bien la base $\mathcal{B}_J$ es la base computacional, o es la base estabilizada por un grupo $G_{\vec{b}_J}$ dado por

$$G_{\vec{b}_J} = \left\{ 1, P_{\vec{b}_J, j} = \sigma_x^{\vec{1}M^j} \sigma_z^{\vec{b}\hat{M}^j} : j = 1, \ldots, D-1 \right\} \tag{3.27}$$

como se detalla en el Apéndice B. En cualquier caso, la obtención de una representación de los n generadores del estabilizador puede obtenerse con a lo sumo $O(n^2)$ operaciones. El cálculo del vector de conmutación requiere, además, de n productos interncos simplécticos para su realización, por lo que mantiene la complejidad de $O(n^2)$.

Para la estimación de un χ_{aa} a partir de un conjunto de M experimentos se utilizará $O(Mn)$ recursos de memoria, para guardar la terna $\left(J, \vec{k}, \vec{k'}\right)$ de cada experimento. Además, se requerirán $O(Mn^2)$ operaciones de post-proceso para verificar los M vectores de conmutación. El término de complejidad dominante para cada experimento sigue siendo $O(n^3)$ proveniente de la construcción de los circuitos de cambio de base requeridos.

3.5.3. Detección de coeficientes diagonales principales

Teniendo en cuenta la desigualdad (3.21) entre los coeficientes diagonales y los no diagonales de un canal completamente positivo, queda clara la utilidad de detectar los coeficientes diagonales principales. En particular, un

algoritmo para determinar cuáles son los coeficientes principales sin necesidad de realizar tomografía completa diagonal permitiría realizar eficientemente tomografía completa siempre y cuando los coeficientes principales sean pocos. En la presente sección mostraremos como realizar dicha detección.

Hemos mostrado que que todos los coeficientes diagonales χ_{aa} pueden obtenerse a partir del mismo conjunto de resultados experimentales. Ahora mostraremos que, además de eso, puede determinarse cuales son los operadores E_a relacionados con los mayores χ_{aa}. Es claro que realizar una búsqueda exhaustiva estimando todos los coeficientes diagonales no es una solución eficiente (la cantidad de coeficientes diagonales es exponencialmente grande en n). Claro que, para que esa estimación sea eficiente, se debe tener un canal con pocos coeficientes diagonales grandes. Notablemente, ese caso es uno de los más relevantes para decidir el código de corrección de errores que se debe utilizar en un canal.

La observación que nos permitirá realizar dicha detección, es que las estimaciones que se pueden realizar a partir de M experimentos son discretas. Es decir, la estimación de $\overline{F}(\mathcal{E}_a) = \frac{D\chi_{aa}+1}{D+1}$, sólo puede dar resultados de la forma $\frac{k}{M}$, con $k \in \mathbb{N}$. Con esto en mente, veremos como estimar todos los valores de $F(\mathcal{E}_a)$ tales que su estimación es mayor a $\frac{2}{M}$. Más aún, veremos como calcular la probabilidad de que, incluso teniendo un valor de $\overline{F}(\mathcal{E}_a) > \frac{2}{M}$, no sea detectado.

La manera de detectar los coeficientes cuyas estimaciones son mayores a $\frac{2}{M}$ es tomar los M experimentos de a pares, Para cada par de experimentos (es decir, las ternas $\left(J, \vec{k_1}, \vec{k_2}\right)$ y $\left(J', \vec{k_1}', \vec{k_2}'\right)$) encontraremos uno, ninguno o varios operadores E_a tales que se cumplen simultáneamente

$$\begin{aligned} E_a \left|\psi^J_{\vec{k_1}}\right\rangle &\propto \left|\psi^J_{\vec{k_2}}\right\rangle \\ E_a \left|\psi^{J'}_{\vec{k_1}'}\right\rangle &\propto \left|\psi^{J'}_{\vec{k_2}'}\right\rangle \end{aligned} \tag{3.28}$$

Queda claro que, en caso de encontrarse ese operador E_a, la estimación de $\overline{F}(\mathcal{E}_a) \geq \frac{2}{M}$ por tener dos experimentos consistentes con la aplicación de E_a.

Veamos la manera de encontrar esos operadores E_a a partir de cada par de experimentos. En primer lugar, se deben separar los pares de experimentos en dos casos, el caso $J = J'$ y el caso $J \neq J'$.

En el primer caso, si $J = J'$, tenemos que la cada una de las dos ternas define el vector de conmutación de los operadores E_a con cada operador del estabilizador de la base J. Si los vectores de conmutación correspondientes a

cada experimento son distintos, entonces no existirá ningún operador E_a. En caso de que sean iguales, serán D operadores los que cumplan con esas relaciones de conmutación. Esos D operadores tendrán, entonces, estimaciones de sus $\overline{F}(\mathcal{E}_a)$ correspondienten mayores a $\frac{2}{M}$. Eso indica que hay una cantidad exponencialmente grande de coeficientes diagonales cuyas estimaciones superan ese umbral.

Más interesante es el caso en el que $J \neq J'$. En este caso siemrpe existirá exactamente un operador E_a compatible con ambos experimentos. Dicho operador puede encontrarse eficientemente. En efecto, notemos que cada operador puede escribirse de la forma[5]

$$E_a \cong \prod_{i=0}^{n-1} J_i^{q_i} \prod_{i=0}^{n-1} J_i'^{q_i'} \tag{3.29}$$

donde J_i y J_i' ($i \in \{1 \dots n\}$) son los generadores canónicos de los estabilizadores J yJ', respectivamente. Una vez obtenidos los vectores $\vec{q}$ y $\vec{q'}$, la obtención de la representación canónica de E_a es inmediata mediante la realización de $O(n^2)$ operaciones clásicas.

Tenemos que obtener $\vec{q}$ y $\vec{q'}$ tales que los E_a dados por la ecuación (3.29) obedezcan que

$$\begin{aligned} J_i E_a &= (-1)^{k_2 - k_1} E_a J_i \\ J'_i E_a &= (-1)^{k_2' - k_1'} E_a J'_i \end{aligned} \tag{3.30}$$

Para hacerlo, tenemos que determinar la matriz no singular C tal que

$$J_i J'_j = (-1)^{C_{i,j}} J'_j J_i \tag{3.31}$$

La condición 3.30 se convierte ahora en

$$\begin{aligned} \vec{k_2} - \vec{k_1} &= C\vec{q'} \\ \vec{k_2'} - \vec{k_1'} &= C^T \vec{q} \end{aligned} \tag{3.32}$$

Por lo tanto, invirtiendo C y C^T, obtenemos los vectores $\vec{q}$ y $\vec{q'}$. Este procedimiento debe repetirse para cada uno de los $\binom{M}{2}$ pares de experimentos para encontrar todo los E_m para los que la estimación $F(\mathcal{E}_m) \geq 2/M$.

[5]Esa forma es apenas una generalización de la representación canónica, donde $\mathcal{B}_J = \mathcal{B}_X = \mathcal{B}_{\mathbf{0}}$ and $\mathcal{B}_{J'} = \mathcal{B}_Z$

3.5.4. Análisis del error para la detección simultánea de coeficientes

Surge con esto la pregunta acerca de cuántos experimentos son necesarios para obtener los coeficientes diagonales χ_{mm} con una precisión dada. Si se quieren medir todos los coeficientes χ_{mm} mayores que un cierto valor ϵ, todos con una incerteza individual δ, se puede obtener el número de experimentos suficientes M para obtener eso con probabilidad de éxito p como[Pas08]

$$M \geq \frac{2\left(D+\frac{1}{\epsilon}\right)(D+1)}{D^2\delta^2(1-p)} = \frac{2\left(1+\frac{1}{D\epsilon}\right)(1+\frac{1}{D})}{\delta^2(1-p)}. \tag{3.33}$$

Esto se obtiene considerando que la estimación de cada $\overline{F}\left(\mathcal{E}_{mm}\right)$ se consigue con una varianza $2\overline{F}\left(\mathcal{E}_{mm}\right)\left[1-\overline{F}\left(\mathcal{E}_{mm}\right)\right]/M$, y usando una cota para la función de error.

Además, si se considera $\epsilon \gg \frac{1}{D}$ esta expresión puede simplificarse como

$$M \gtrsim \frac{2}{\delta^2(1-p)}. \tag{3.34}$$

Eso significa que podemos hacer tomografía diagonal completa con recursos que son polinomiales tanto en el número de qubits del sistema como en la precisión deseada δ. Una posible crítica a ese argumento es que para un canal tomado al azar, los coeficientes χ_{mm} van a tener valores típicos cercanos a $\frac{1}{D}$. Este método dará buenos resultados cuando el canal considerado no es aleatorio. En particular, cuando se trate de un canal con interacciones locales fuertes.

3.6. Conclusiones parciales

Hemos visto en este capítulo como medir de forma selectiva y eficiente cualquier coeficiente de la matriz χ de un canal. Para estimar esos coeficientes sirve cualquier método capaz de determinar eficientemente la fidelidad promedio de un canal. En particular, vimos en detalle como estimar dicha fidelidad a través del muestreo aleatorio de estados un conjunto de bases mutuamente no sesgadas que, a su vez, forman un 2–diseño. El hecho de que esos estados formen un 2–diseño es lo que posibilita que un muestreo finito sirva para hacer una estimación eficiente. Además, aprovechamos las propiedades

de esa base, en particular en lo que respecta al formalismo de los estabilizadores, para mostrar como obtener todos los coeficientes diagonales χ_{mm} a partir del mismo conjunto de resultados experimentales. No sólo eso, sino que además, mediante una idea similar, se pueden detectar todos los coeficientes diagonales mayores a cierta cota sin saber a priori nada sobre el canal. Dicha detección es de gran utilidad ya que los coeficientes diagonales establecen, a su vez, cuales de los coeficientes no diagonales poseen información relevante sobre el canal.

Capítulo 4

Tomografía de procesos cuánticos selectiva y eficiente sin ancillas

> Es un hombre o una piedra o un árbol el que va a dar comienzo al cuarto canto.
>
> *Los Cantos de Maldoror*
> *Conde de Lautréamont*

Un problema del método SEQPT que vimos en el Capítulo 3, es que requiere, como ancilla, de un qubit limpio. Si bien es cierto que eso no afecta en nada la eficiencia del método, sí hace que el propio tomógrafo sea más susceptible al ruido. Por ese mótivo sería deseable encontrar una versión alternativa que no requiera ningún recurso adicional.

En éste capítulo presentaremos una variante al método SEQPT que no requiere ancillas[SBLP11].

4.1. Elementos no diagonales

La tomografía de los elementos diagonales en el método SEQPT no requiere de sistemas auxiliares de ningún tipo. Por lo tanto, sólo nos concentraremos aquí en la medición de los elementos no diagonales de la matriz χ.

La primera observación que podemos hacer es respecto del circuito para medir coeficientes no diagonales de la Figura 4.1. En la figura se hace evidente

que el sistema auxiliar cumple un rol limitado en el tiempo y que es para la generación del estado que luego atravesará el canal.

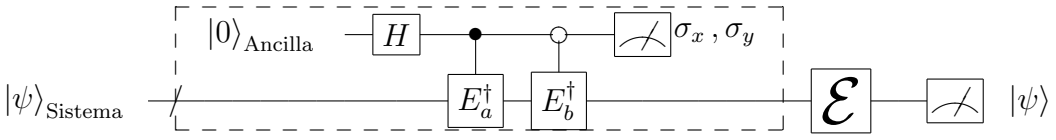

Figura 4.1: Circuito para la medición de χ_{ab} para un canal $\mathcal{E}$. Queda de manifiesto que el rol de la ancilla es únicamente para la preparación de los estados.

Analicemos un poco más el circtuito de la figura 4.1. En particular, el caso en el que en la ancilla se mide σ_x, correspondiente a querer determinar la parte real del coeficiente χ_{ab}. Para el caso en que se mida σ_y a la ancilla el análisis es igual. Cada experimento puede tener uno de cuatro resultados posibles:

1. Con probabilidad p_{+s}, ancilla en $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ y supervivencia del estado del sistema.

2. Con probabilidad p_{+n}, ancilla en $|+\rangle$ y no supervivencia del estado del sistema.

3. Con probabilidad p_{-s}, ancilla en $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ y supervivencia del estado del sistema.

4. Con probabilidad p_{-n}, ancilla en $|-\rangle$ y no supervivencia del estado del sistema.

Por la ecuación (3.14), tenemos que

$$\frac{D}{D+1}\text{Re}\,(\chi_{ab}) = p_{+s} - p_{-s} \tag{4.1}$$

Es decir, para obtener la parte real se deben medir dos de esas cuatro probabilidades. No sólo eso, sino que cada una de esas dos corresponde a la preparación de un estado distinto (el que se obtiene midiendo en la ancilla el estado $|+\rangle$ y el que se obtiene al medir $|-\rangle$).

Veremos a continuación cuáles son los estados del sistema que resultan cuando se mide cada uno de los dos posibles resultados de la ancilla. Puede pensarse esa etapa como una etapa de preparación de estados del sistema.

4.1.1. Preparación de estados con ancilla

Analizaremos aqui la preparación de los estados recuadrada en la Figura 4.1. Lo primero que vale la pena notar es que, durante la etapa de preparación, todos los estados involucrados son puros.

El estado conjunto de la ancilla y el sistema $|\Psi\rangle$ en el instante previo a la medición de la ancilla toma la forma

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \otimes E_b^\dagger |\psi\rangle + |1\rangle \otimes E_a^\dagger |\psi\rangle\right) \tag{4.2}$$

Al medir σ_x a la ancilla, se proyecta el estado sobre la base $\{|+\rangle, |-\rangle\}$ de la ancilla. Es decir, se pueden obtener los estados

$$|\Psi_+\rangle = (|+\rangle\langle+| \otimes \mathbb{I})|\Psi\rangle = \frac{1}{2\sqrt{2}}\left[|+\rangle \otimes \left(E_a^\dagger + E_b^\dagger\right)|\psi\rangle\right] \tag{4.3}$$

$$|\Psi_-\rangle = (|-\rangle\langle-| \otimes \mathbb{I})|\Psi\rangle = \frac{1}{2\sqrt{2}}\left[|-\rangle \otimes \left(E_b^\dagger - E_a^\dagger\right)|\psi\rangle\right] \tag{4.4}$$

Por lo tanto, los estados que hay que preparar para realizar tomografía no diagonal sin ancilla son de la forma $\left(E_a^\dagger \pm E_b^\dagger\right)|\psi_m^J\rangle$[1] para la parte real y $\left(E_a^\dagger \pm iE_b^\dagger\right)|\psi_m^J\rangle$ para la parte imaginaria. El esquema de tomografía no diagonal sin ancilla queda claro, se deben preparar esos estados, aplicar el canal, y luego a la salida medir la probabilidad de estar en el estado $|\psi_m^J\rangle$ correspondiente, promediando sobre todos los J y m del 2–diseño.

Un problema que aparece, es que la preparación de esos estados sin ancilla no es tan simple como aplicar los operadores $E_a^\dagger \pm E_b^\dagger$ y $E_a^\dagger \pm iE_b^\dagger$ sobre los estados del 2–diseño, ya que esos operadores ni siquiera son unitarios en el caso en que la base de operadores $\{E_a\}$ sí lo es. Sin embargo, veremos en breve como superar ese inconveniente.

4.2. Tomografía diagonal en otra base

Otra manera de interpretar los resultados de la sección anterior, es pensar que se trata de tomografía diagonal en una base de operadores distinta a

[1] Queda explícito en este punto que el promedio sobre la medida de Haar se realiza, igual que en el Capítulo 3, únicamente sobre estados de un 2–diseño formado por un conjunto de MUBs.

la $\{E_a\}$. Es evidente que cambiar de base puede llevar la información de afuera de la diagonal hacia la diagonal, permitiendo utilizar las técnicas de tomografía diagonal.

En efecto, consideremos el circuito de la Figura 4.2. El esquema es completamente equivalente a lo dicho en la sección anterior, pero está presentado como un circuito similar a los de medición de coeficientes diagonales de la Figura 3.1.

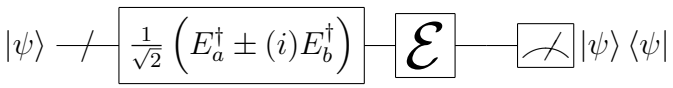

Figura 4.2: Circuito para la medición de los coeficientes χ_{ab} para un canal $\mathcal{E}$. La i entre paréntesis debe interpretarse como una fase que puede o no estar, dependiendo de si se desean medir partes reales o imaginarias de los coeficientes.

De nuevo, estamos frente a la dificultad de que aplicar los operadores que son combinación lineal de los de la base puede no ser fácil y, en el caso general, se trata de operadores que ni siquiera son unitarios. Pero dejando de lado ese detalle con el que nos enfrentaremos en la Sección 4.2.1, podemos analizar el funcionamiento del circuito.

El resultado de la medición promediado sobre la medida de Haar es

$$\overline{F}\left(\tilde{\mathcal{E}}_{ab}\right) = \frac{1}{2}\int d\psi \,\langle\psi|\,\mathcal{E}\left[\left(E_a^\dagger \pm (i)E_b^\dagger\right)|\psi\rangle\langle\psi|\left(E_a \pm (-i)E_b\right)\right]|\psi\rangle \qquad (4.5)$$

donde la fase entre paréntesis indica que dicha fase puede o no estar, dependiendo de si se desea medir la parte real o la imaginaria del coeficiente, y el canal $\tilde{\mathcal{E}}_{ab}$ es la composición del operador $E_a^\dagger \pm (i)E_b^\dagger$ con el canal $\mathcal{E}$. Utilizando la linealidad del canal $\mathcal{E}$ y la linealidad de la integral en la medida de Haar se obtiene

$$\begin{aligned}
\overline{F}\left(\tilde{\mathcal{E}}_{ab}\right) = \quad & \frac{1}{2}\int d\psi \,\langle\psi|\,\mathcal{E}\left[E_a^\dagger|\psi\rangle\langle\psi|E_a\right]|\psi\rangle + \\
\pm(-i) \quad & \frac{1}{2}\int d\psi \,\langle\psi|\,\mathcal{E}\left[E_a^\dagger|\psi\rangle\langle\psi|E_b\right]|\psi\rangle + \\
\pm(i) \quad & \frac{1}{2}\int d\psi \,\langle\psi|\,\mathcal{E}\left[E_b^\dagger|\psi\rangle\langle\psi|E_a\right]|\psi\rangle + \\
+ \quad & \frac{1}{2}\int d\psi \,\langle\psi|\,\mathcal{E}\left[E_b^\dagger|\psi\rangle\langle\psi|E_b\right]|\psi\rangle
\end{aligned} \qquad (4.6)$$

y comparando con la ecuación (3.10) se obtiene

$$\begin{aligned}\overline{F}\left(\tilde{\mathcal{E}}_{ab}\right) = & \quad \tfrac{D}{2(D+1)}\left(\chi_{aa}+\chi_{bb}\right. \\ & \left.\pm(-i)\chi_{ab}\pm(i)\chi_{ba}+\tfrac{2}{D}\pm(-i)\tfrac{\delta_{ab}}{D}\pm(i)\tfrac{\delta_{ba}}{D}\right)\end{aligned} \tag{4.7}$$

Es simple ver que la medición de los cuatro valores (dos signos y con o sin fase $\pi/2$) se obtiene el coeficiente χ_{ab} como

$$\begin{aligned}\overline{F}\left(\tilde{\mathcal{E}}_{ab}\right)_{+} - \overline{F}\left(\tilde{\mathcal{E}}_{ab}\right)_{-} &= \frac{2D}{D+1}\mathrm{Re}\left(\chi_{ab}\right) \\ \overline{F}\left(\tilde{\mathcal{E}}_{ab}\right)_{+i} - \overline{F}\left(\tilde{\mathcal{E}}_{ab}\right)_{-i} &= \frac{2D}{D+1}\mathrm{Im}\left(\chi_{ab}\right)\end{aligned} \tag{4.8}$$

El único punto que queda por resolver, que veremos a continuación, es cómo implementar los operadores $\left(E_a^\dagger \pm (i)E_b^\dagger\right)$.

4.2.1. Preparación de estados sin ancilla

Una primera observación, es que no es necesario implementar los operadores $\left(E_a^\dagger \pm (i)E_b^\dagger\right)$ en general, ya que únicamente actuarán sobre estados del 2–diseño. Además, el muestreo sobre los $D\left(D+1\right)$ estados del 2–diseño es un muestreo clásico, por lo que para cada experimento uno sabe cuál es el estado de entrada.

Por lo tanto, una vez elegido el coeficiente χ_{ab} que se desea medir, para cada estado que se va muestreando al azar de entre los del 2–diseño, se puede construir un operador unitario que actúe sobre ese estado en particular como $\left(E_a^\dagger \pm (i)E_b^\dagger\right)$. De esa forma, el resultado es el deseado. Dicho en otras palabras, no importa implementar los operadores en cuestión sino simplemente generar los estados necesarios (ver Sección 4.1.1). Si la base de operadores elegida es la base de operadores de Pauli generalizados, dichos estados se pueden contruir eficientemente.

El método para generar estos estados está basado en algunas observaciones:

1. Cualquier estado del 2–diseño que estamos utilizando $\left|\psi_m^J\right\rangle$ se puede generar eficientemente a partir del estado $\left|\psi_0^0\right\rangle = \left|0\right\rangle^{\otimes n}$ (ver Apéndice B.1).

2. Cualquier operador de la base $\{E_m, m = 0, \ldots, D^2-1\}$ actúa como una traslación sobre los estados del 2–diseño en cuestión. Es decir,

$E_a \left|\psi_m^J\right\rangle \propto \left|\psi_{m'}^J\right\rangle$, donde hemos abandonado la conjugación hermítica de los operadores por tratarse de la base de operadores de Pauli generalizados.

3. El estado normalizado $\left|\Psi_{\beta,a,b,m}^J\right\rangle = K\left(E_a + e^{i\beta}E_b\right)\left|\psi_m^J\right\rangle$ también puede generarse eficientemente. Eso, claro está, siempre que el estado en cuestión no sea el vector nulo. Y la constante de normalización K también puede computarse eficientemente.

Se trata, entonces, de contruir estados de la forma $\left(E_a + e^{i\beta}E_b\right)\left|\psi_m^J\right\rangle$, donde β es un múltiplo de $\pi/2$. Para hacerlo, primero debemos establecer un orden para los estados dentro de las bases que conforman el conjunto de MUBs. Para la base computacional ($J = 0$) utilizaremos el orden lexicográfico. Para las demás bases utilizaremos la convención

$$\left|\psi_m^J\right\rangle = V_0^J \left|\psi_m^0\right\rangle \tag{4.9}$$

donde V_0^J es el operador de cambio de base de la base computacional a la base J (ver Apéndice B.1). Es decir, los operadores de cambio de base no alteran el orden de los estados. Además, los estados de la base computacional se construyen todos como $\sigma_x^{(m)}\left|\psi_0^0\right\rangle$ donde $\sigma_x^{(m)}$ es el producto tensorial de σ_x para cada qubit donde la representación binaria de m tiene un 1 e identidades en los demás qubits.

Así, los estados que se deben preparar pueden escribirse en la forma

$$\left|\Psi_{\beta,a,b,m}^J\right\rangle = \left(E_a + e^{i\beta}E_b\right) V_0^J \sigma_x^{(m)} \left|\psi_0^0\right\rangle \tag{4.10}$$

Teniendo en cuenta que los operadores de cambio de base V_0^J son operadores del grupo de Clifford construidos con $O\left(n^2\right)$ compuertas de Hadamard, CNOT y compuertas de fase, es eficiente ver como transforman los operadores E_a y E_b frente a la conjugación por V_0^J (ver Apéndice B.1). Por lo tanto, los estados $\left|\Psi_{\beta,a,b,m}^J\right\rangle$ pueden llevarse a la forma

$$\left|\Psi_{\beta,a,b,m}^J\right\rangle = V_0^J \left(\tilde{E}_a \sigma_x^{(m)} + e^{i\beta}\tilde{E}_b \sigma_x^{(m)}\right)\left|\psi_0^0\right\rangle \tag{4.11}$$

Pero puesto que los operadores de Pauli $\tilde{E}_a$ y $\tilde{E}_b$ son traslaciones de los estados dentro de la misma base computacional, se obtiene que

$$\left|\Psi_{\beta,a,b,m}^J\right\rangle = e^{i\alpha} V_0^J \left(\left|\psi_r^0\right\rangle + e^{i\gamma}\left|\psi_t^0\right\rangle\right) \tag{4.12}$$

donde r, t, α y β se pueden computar eficientemente.

Por lo tanto, lo único que falta es construir un estado que sea combinación lineal de dos estados de la base computacional. Dicha combinación lineal se puede obtener siempre mediante una compuerta de Hadamard, $O(n)$ compuertas CNOT y a lo sumo una compuertas de fase.

Resumiendo, hemos visto aquí que, a pesar de no poder implementar eficientemente el operador $E_a + e^{i\beta} E_b$, se pueden implementar eficientemente operadores que, sobre un dado estado del 2–diseño, actúan como $E_a + e^{i\beta} E_b$. Esto es el punto clave del protocolo de tomografía selectiva y eficiente sin ancilla.

Luego se procede exactamente igual que para la tomografía SEQPT diagonal. Se eligen estados del 2-diseño al azar, se aplica el operador correspondiente a $E_a + e^{i\beta} E_b$ para ese estado, se hace actuar el canal $\mathcal{E}$ y se mide la supervivencia del estado de entrada. La supervivencia promedio sobre todos los estados del 2–diseño es el coeficiente buscado.

4.3. Conclusiones parciales

En este capítulo vimos como realizar tomografía selectiva y eficiente de procesos cuánticos sin la utilización de sistemas auxiliares. La principal observación que nos permitió desarrollar el método, es que puede reinterpretarse el rol de la ancilla del protocolo de SEQPT del Capítulo 3 como formando parte sólo de la preparación de estados.

Luego, vimos que el protocolo sin ancilla era similar al SEQPT diagonal en una base de operadores modificada $(E_a \pm (i) E_b)$. A pesar de que dichos operadores no son eficientemente implementables, como sólo actúan sobre estados del 2–diseño, desarrollamos un esquema para construir operadores que, aunque diferentes a los que queríamos, tienen en mismo efecto sobre un dado estado del 2–diseño. Sobre esa construcción, pudimos desarrollar el protocolo de SEQPT sin ancilla.

Capítulo 5

Implementación fotónica de SEQPT y SEQPT sin ancilla

> Hay hombres que nacen comprometidos:
> no tienen la facultad de elegir; han sido
> arrojados a un camino; al final del
> camino los espera un acto, su acto
>
> *Las Moscas*
> *Jean–Paul Sartre*

La tomografía de procesos estándar fue implementada numerosas veces, en diversos contextos y sobre diferentes sistemas físicos [BSS$^+$10, MKH$^+$09, WGP$^+$07, NAB$^+$08, BAH$^+$10]. En este capítulo mostraremos las implementaciones fotónicas de los algoritmos de los capítulos 3 y 4. La primera, presentada en [SLP10] es una implementación de un qubit codificado en la polarización de un único fotón, utilizando un fotón gemelo como heraldo.

La implementación del protocolo de SEQPT sin ancilla, presentada en [SBLP11, Sch11], utiliza dos qubits: uno codificado en la polarización de un fotón, y otro en un grado de libertad espacial del mismo. Dicha implementación fue realizada en colaboración durante la presente tesis y la tesis de doctorado de Christian Schmiegelow.

5.1. Experimento fotónico de SEQPT

El experimento del algoritmo de SEQPT fue llevado a cabo por Schmiegelow et al. en [SLP10]. En la Figura 5.1 puede verse el dispositivo experimental

montado.

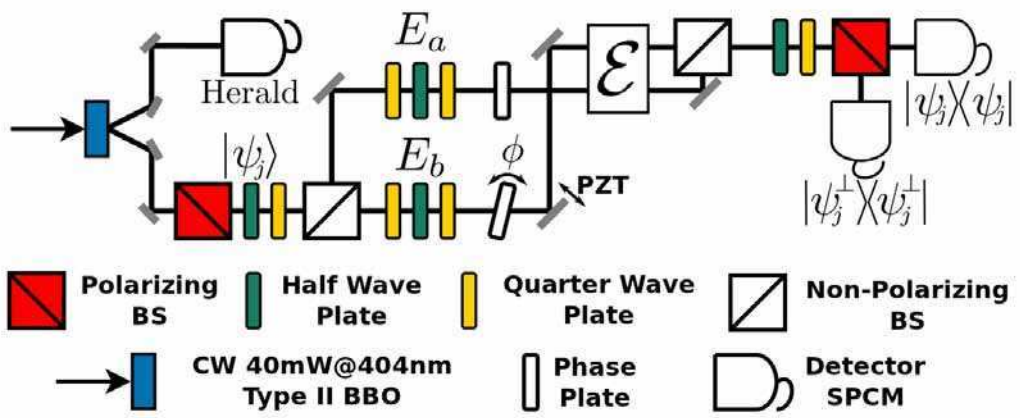

Figura 5.1: Dispositivo experimental para la tomografía selectiva y eficiente de procesos implementada sobre un qubit de polarización de un fotón, utilizando como ancilla el grado de libertad del camino. Figura tomada de [Sch11].

Para el experimento se utilizó un láser diodo contínuo de $405nm$ y $40mW$ incidente sobre un cristal BBO cortado para conversión paramétrica inversa de tipo II. Uno de los dos fotones resultantes fue usado de heraldo, para detectar coincidencias con el fotón que pasaba por el experimento. Para el fotón del experimento, se utilizó el grado de libertad de polarización como qubit, y el grado de libertad de camino como ancilla. De esta forma, la preparación del estado se realiza antes de la división en caminos (ver Figura 5.1). Luego de dividir en los dos caminos con un divisor de haz no polarizante que hace las veces de compuerta de Hadamard, se realizan las compuertas controladas (cada una en el camino correspondiente). Luego ambos caminos son pasados por el canal en polarización. Por último, la medición de σ_x o σ_y se obtiene haciendo interferir ambos caminos controlando la diferencia entre ellos mediante la inclinación en un ángulo ϕ de una lámina de vidrio en uno de ellos.

Una diferencia entre este experimento y el protocolo SEQPT que presentamos, es que en el protocolo original, cada experimento corresponde a una coincidencia medida por el detector. Luego de esa coincidencia, se debe elegir otro estado del 2–diseño, al azar, y repetir el experimento. Al trabajar con fotones, en cambio, el orden cambia: es más fácil elegir un estado del 2–diseño y medir muchas coincidencias antes de preparar otro. Sin embargo, el método

funciona de igual forma, sólo que tomando el promedio de las probabilidades de supervivencia de cada estado del 2–diseño. Un muestreo aleatorio sobre esas probabilidades da el resultado correcto. De hecho, si no se repiten estados del 2–diseño al realizar el muestreo, la desviación estándar en la estimación pasa a estar acotada por $\sigma \leq \sqrt{\frac{1}{M}\left(1 - \frac{M-1}{K-1}\right)}$, con $K = D\,(D+1)$, en lugar del $\sigma \leq \frac{1}{\sqrt{M}}$ del caso de coincidencias individuales.

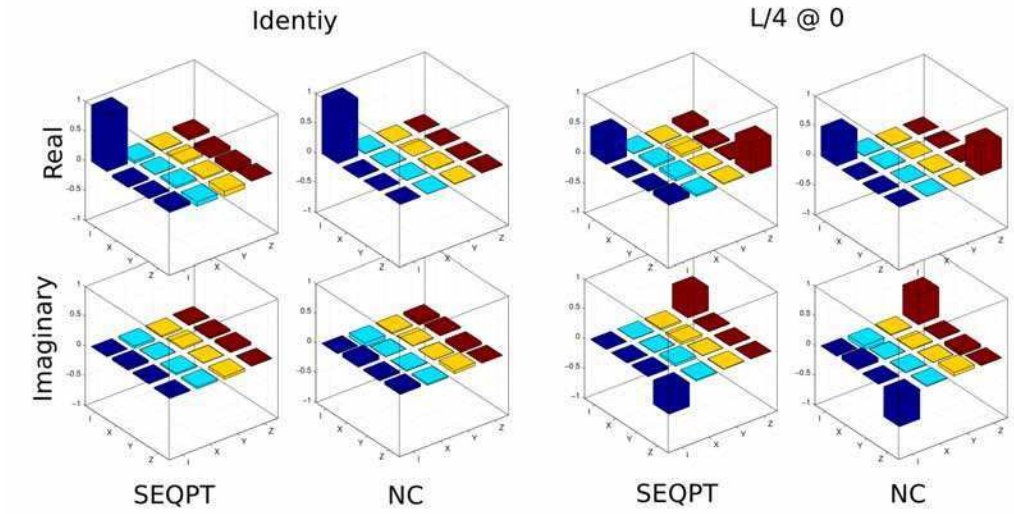

Figura 5.2: Resultados obtenidos para ambos canales tanto por el método SEQPT como por el método estándar (NC, por Nielsen y Chuang[NC04]). Figura tomada de [Sch11].

En la Figura 5.2 se observan los resultados obtenidos para ambos canales. En ambos casos, la fidelidad entre la tomografía estándar y la SEQPT es superior al 95 %. En este caso, es poco lo que puede decirse sobre la eficiencia ya que los 6 estados del 2–diseño son pocos para hacer consideraciones estadísticas, y porque toda la discusión sobre eficiencia tiene que ver con como se modifica el número de recursos con el número de qubits, cosa que en un experimento con un solo qubit no puede apreciarse.

5.2. Experimento fotónico de SEQPT sin ancillas

El método de tomografía selectiva y eficiente sin ancilla fue llevado al experimento para un sistema de dos qubits [SBLP11, Sch11], siendo estos la polarización y el camino de un fotón, y usando un fotón gemelo como heraldo. Para eso, se bombeó un cristal BBO (β-borato de bario) con un diodo láser de $405nm$ para que ocurra la conversión paramétrica inversa y se produzcan dos fotones de $810nm$. Uno de ellos se utilizó cono heraldo, y el otro para codificar los dos qubits del experimento.

El experimento se dividió en tres etapas, la preparación de los estados, la evolución mediante el canal que se desea tomografiar y la medición de las probabilidades de transición. En la Figura 5.3 se observa el dispositivo experimental utilizado.

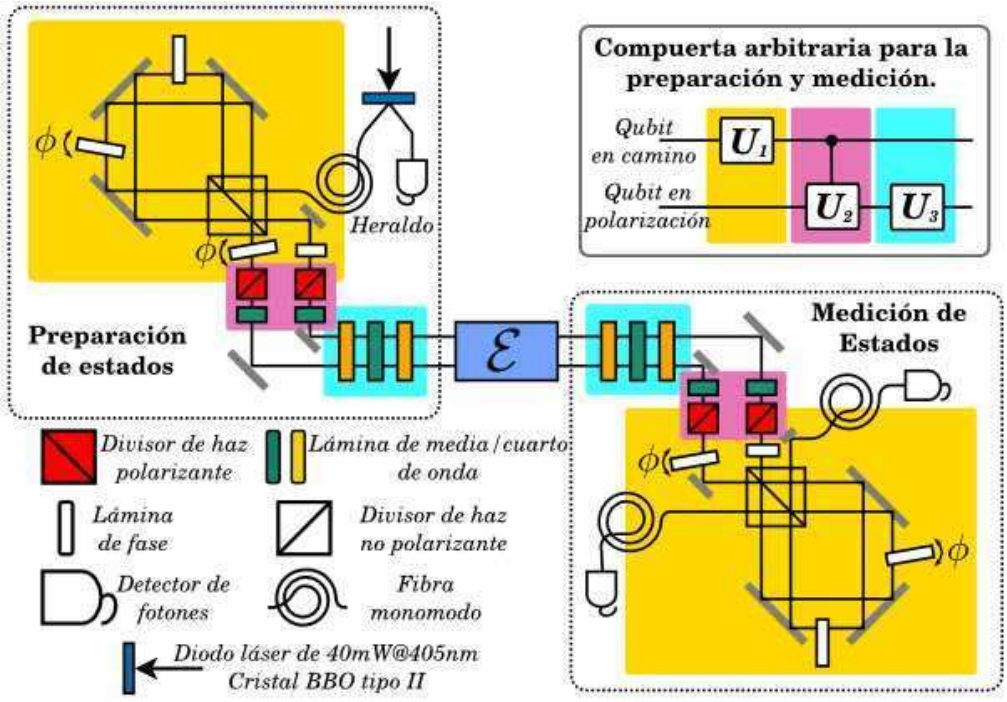

Figura 5.3: Montaje experimental para la medición de los coeficientes χ_{ab} de un canal $\mathcal{E}$. Se utilizaron fotones gemelos, uno como heraldo y el otro como dos qubits codificados en polarización y camino. Figura tomada de [Sch11].

Se observa en la Figura 5.3 que el bloque de preparación y el de medición son similares, conformados por una compuerta en camino U_1 realizada mediante un interferómetro Sagnac, luego una compuerta U_2 en polarización controlada por camino (es decir, operaciones distintas a la polarización de cada camino), y por último las tres láminas de onda que permiten realizar una operación U_3 en polarización, afectando a ambos caminos por igual. Esas tres operaciones permiten preparar –o medir– cualquier estado. En particular, los que se deben preparar y medir para el algoritmo en cuestión. Entre la etapa de la preparación y la de medición se encuentra el proceso, compuesto por un interferómetro de Mach–Zehnder estabilizado activamente para operaciones en camino y, dependiendo del proceso a analizar, láminas de onda para la fase.

Varios procesos fueron estudiados con el dispositivo descripto: El proceso identidad; un proceso unitario en polarización obtenido con una lámina de onda en ambos caminos; una operación U_c controlada por camino, colocando láminas de onda distintas en cada camino ($U_c = (\mathbb{I} - \sigma_z) \otimes \sigma_z/2 + (\mathbb{I} + \sigma_z) \otimes \sigma_x/2$); y una versión ruidosa de U_c, donde se agrega ruido al qubit de camino mediante un barrido aleatorio de la fase del Mach-Zehnder. La Figura 5.4 muestra los resultados obtenidos para la reconstrucción completa de la matriz χ de los cuatro canales en la base de operadores de Pauli generalizados. La fidelidad entre la matriz χ medida con el protocolo SEQPT y aquella medida mediante la tomografía de procesos estándar fue, en los cuatro casos, superior al 90 %.

Para la tomografía completa se dejó de lado la eficiencia y se midieron independientemente los valores de los 256 coeficientes χ_{ab}. Para cada una de las $D\,(D+1) = 20$ probabilidades de supervivencia de cada uno de los estados del 2–diseño se prepararon los estados $(E_a \pm E_b)\left|\psi_m^J\right\rangle$ y se midió la probabilidad de salir en el mismo $\left|\psi_m^J\right\rangle$. Eso da un total de $256 \times 20 \times 2 = 10240$ probabilidades de transición. Sin embargo, muchas de ellas estaban repetidas[1], por lo que alcanzó con medir 560 probabilidades de transición con 140 arreglos experimentales distintos.

[1]Eso se debe a que $(E_a \pm E_b)\left|\psi_m^J\right\rangle$ puede ser igual a $(E_{a'} \pm E_{b'})\left|\psi_{m'}^{J'}\right\rangle$ en algunos casos.

5.3. Conclusiones parciales

Vimos en este capítulo que tanto el algoritmo de tomografía selectiva y eficiente de procesos cuánticos como su versión sin sistemas auxiliares fueron implementados fotónicamente.

El primero de ellos utilizó como ancilla el grado de libertad de camino de un fotón, siendo la polarización del mismo el qubit sobre el cual actuaba el proceso. Para el caso sin ancilla se realizó tomografía de un sistema de dos qubits codificados en la polarización y camino de un fotón respectivamente. En ambos casos se utilizó un fotón gemelo como heraldo.

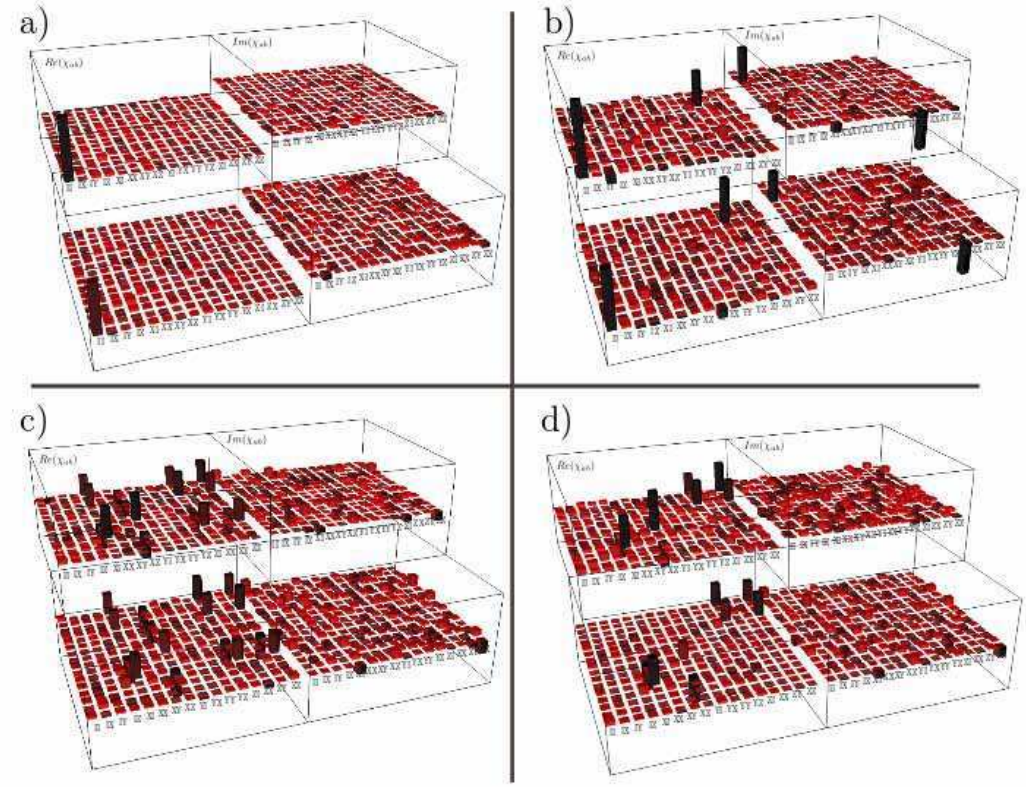

Figura 5.4: Resultados experimentales del experimento de SEQPT sin ancilla. Se observan en a) el proceso identidad, en b) el resultado de la compuerta en polarización con una lámina de cuarto de onda, en c) la compuerta controlada por camino y en d) la compuerta ruidosa controlada por camino. En todos los casos, los dos gráficos de arriba muestran el resultado obtenido mediante el SEQPT, y los dos de abajo los obtenidos mediante tomografía de procesos estándar. Figura tomada de [Sch11].

Capítulo 6

Comparación entre métodos de tomografía de procesos

> La trenza había vuelto a crecerle, pero no
> la llevaba suelta en la espalda sino
> terciada sobre el hombro izquierdo (...).
>
> *El amor en los tiempos del cólera*
> *Gabriel García Márquez*

En este capítulo realizaremos una comparación entre distintos de los métodos que hemos estado estudiando. En primer lugar, veremos que el método de tomografía selectiva y eficiente de procesos cuánticos (SEQPT) de los capítulos 3 y 4 es un pariente cercano de la caracterización directa de la dinámica cuántica (DCQD) de la Sección 2.3.2, siendo la única diferencia entre ambos que en uno se aprovechan las correlaciones cuánticas y que en el otro las mismas son evaluadas clásicamente.

Luego veremos que varios de los métodos vistos (SEQPT, caracterización simétrica de procesos cuánticos ruidosos y la caracterización de error en procesamiento cuántico de la información, de la Sección 2.3.3) pueden agruparse en una categoría de métodos basados en la simetrización del canal por medio de la operación de twirl. A la comparación de esos métodos nos dedicaremos en la segunda sección del presente capítulo.

6.1. Comparación entre SEQPT y DCQD

En esta sección veremos que el protocolo de SEQPT y el de DCQD de la Sección 2.3.2 pueden interpretarse a partir de un marco teórico común, permitiendo entender un poco mejor ambos protocolos.

Lo que veremos para ello es cómo generar los estados de un 2–diseño de $\mathcal{H}$ a partir del estado máximamente entrelazado. Eso nos dará un indicio de la relación que terminaremos de analizar posteriormente.

6.1.1. Preparación de estados mediante mediciones

Supongamos que disponemos del estado máximamente entrelazado $|I\rangle = \frac{1}{\sqrt{D}} \sum_i |ii\rangle$. Si se mide la segunda parte del estado en una base que incluye a estado $|\psi\rangle$, y se encuentra que esa parte está en el estado $|\psi\rangle$, el estado posterior a la medición es el

$$\Pi_{\psi_B} |I\rangle = \frac{1}{\sqrt{D}} \sum_i \left(\mathbb{I}_A \otimes |\psi_B\rangle \langle\psi_B|\right) |i_A i_B\rangle \tag{6.1}$$

donde $\Pi_{\psi_B} = \mathbb{I}_A \otimes |\psi_B\rangle \langle\psi_B|$. Si desarrollamos el estado $|\psi_B\rangle$ en la base computacional $\{|i\rangle, i = 1, \ldots, D\}$ como

$$|\psi_B\rangle = \sum_j \alpha_j |j_B\rangle \tag{6.2}$$

obtenemos que la ecuación (6.1) se escribe como

$$\begin{aligned} \Pi_{\psi_B} |I\rangle &= \frac{1}{\sqrt{D}} \sum_{ijk} \alpha_j \alpha_k^* \left(\mathbb{I}_A \otimes |j_B\rangle \langle k_B|\right) |i_A i_B\rangle \\ &= \frac{1}{\sqrt{D}} \sum_{ijk} \alpha_j \alpha_k^* |i_A\rangle \otimes |j_B\rangle \delta_{ki} \\ &= \frac{1}{\sqrt{D}} |\psi_A^*\rangle \otimes |\psi_B\rangle \end{aligned} \tag{6.3}$$

donde el asterisco indica que se trata del estado conjugado en la base computacional al original. Es decir, la parte A termina en el estado conjugado (en la base computacional) al que se midió en B. Para preparar un estado de manera no determinista, entonces, se debe medir su conjugado a la parte B, y con eso se sabe que el estado que quedó en A es el deseado.

6.1.2. Medición de la fidelidad

Como vimos en las secciones 3.1 y 3.2, el coeficiente χ_{00} está asociado a la fidelidad promedio del canal, que a su vez es la probabilidad de supervivencia promedio de los estados del 2–diseño al atravesar el canal.

Utilizando el resultado de la sección anterior se puede proceder de la siguiente manera: utilizar el estado máximamente entrelazado $|I\rangle$ y medir a la parte B en la base J^* formada por los estados conjugados a los de la base J. Luego hacer que la parte A atraviese el canal, y medir a la salida en la base J. Si el resultado de la medición en la base J de A y el de la base J^* de B es el mismo, eso corresponde a supervivencia de un estado tomado al azar de la base J. Repitiendo el procedimiento para todas las bases y promediando las supervivencias se obtiene la fidelidad promedio. La Figura 6.1 ilustra éste esquema.

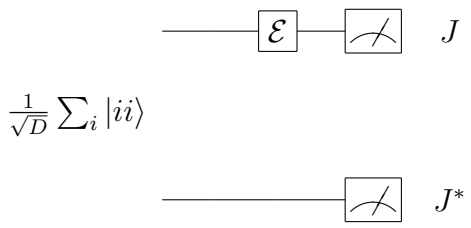

Figura 6.1: Medición de la fidelidad preparando estados con un sistema auxiliar.

El promedio en la Figura 6.1 se hace manualmente, guardando resultados experimentales y promediando a posteriori. El esquema de DCQD es muy parecido, pero la medición que hace a la salida es la de supervivencia del estado $|I\rangle$ conjunta entre las dos partes del estado. El promedio, entonces, es realizado cuánticamente. Aprovechando el poder adicional que dan las mediciones conjuntas, se obtiene el mismo resultado que haciendo mediciones separadas y promediando a mano. Una forma de interpretar eso es que medir el estado $|I\rangle$ implica medir correlaciones entre los dos subsistemas. En cambio, al hacer la medición separada, es el físico a cargo quien debe analizar las correlaciones entre los dos subsistemas al ver si ambos dieron el mismo resultado en la medición.

6.2. Métodos basados en la operación de twirl

Varios de los métodos que estudiamos de tomografía de procesos pueden englobarse en una categoría de métodos basados en *twirl*[LBPC10][1]. El twirl de un canal, que definiremos a continuación, es una operación de simetrización de un canal cuántico. Dependiendo del tipo de simetrización elegida se puede obtener diferente información sobre el canal.

Comenzaremos por definir la noción de twirl de un canal, y luego veremos cuáles de los métodos previamente introducidos se ajustan a dicha definición, y cómo compararlos.

6.2.1. Twirl de un canal

La acción del twirl está ilustrada en la Figura 6.2. Tenemos un proceso cuántico definido por un mapa $\mathcal{E}$ que actúa sobre un sistema (como en casi cualquier tarea de información cuántica) preparado en el estado ρ_0. El twirl del mapa consiste en la aplicación de un operador U_i antes del canal, seguido por la aplicación de $U_i^\dagger$ posterior a la acción del mismo, promediado sobre un conjunto de operadores $\{U_i\}$ sobre los que se hace el twirl.

Típicamente, el twirl es considerado un promedio sobre diferentes elementos U_i, resultando en un canal efectivo $\mathcal{E}^{\mathrm{T}}$. Distintos conjuntos de operadores U_i resultan en distintos tipos de twirl que, a su vez, proveen distintos tipos de información al realizar tomografía.

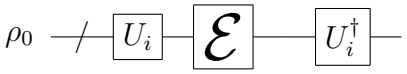

Figura 6.2: Representación circuital del twirl del mapa $\mathcal{E}$. El promedio se realiza sobre los operadores U_i del conjunto sobre el que se realiza el twirl.

En particular, un twirl que nos va a interesar por su relación con el algoritmo de SEQPT (ver Capítulo 3) es el twirl sobre la medida de Haar, o twirl de Haar definido como

$$\mathcal{E}^{HT}(\rho) \;=\; \int dU U^\dagger \mathcal{E}(U\rho U^\dagger) U \tag{6.4}$$

[1]Una posible traducción sería referirse al canal *retorcido*. Pero conservaremos ese nombre en inglés para estar en consonancia con la literatura al respecto.

donde dU se refiere a la medida invariante unitaria de Haar.

Ese twirl puede reformularse como un promedio en el espacio de estados, para llevarlo a una forma similar a la utilizada en el protocolo SEQPT del Capítulo 3.

$$\langle\psi_0|\mathcal{E}^{HT}(|\psi_0\rangle\langle\psi_0|)|\psi_0\rangle = \int_{\mathcal{H}} d\psi \langle\psi|\mathcal{E}(|\psi\rangle\langle\psi|)|\psi\rangle \tag{6.5}$$

Formalmente, la equivalencia se debe a que la medida de Haar es invariante unitaria. Puede pensarse de la siguiente forma: dado $|\psi_0\rangle$, si se toma un U al azar en la medida de Haar, el estado $|\psi\rangle = U|\psi_0\rangle$ corresponde a un vector al azar en la misma medida, pero en el espacio de estados.

Esa dualidad entre la medida de Haar de operadores y de estados hace que haya relaciones análogas a las del Capítulo 3, como por ejemplo la (3.7), pero para la medida de Haar del espacio de operadores [Sam80, Mel90, BB96, EAZ05]. Nos limitaremos aquí a resumir esos resultados en la siguiente ecuación:

$$\begin{aligned}
&\int dU \mathrm{Tr}[A_1 U^\dagger B_1 U A_2 U^\dagger B_2 U] \\
&= \frac{\mathrm{Tr}[A_1 A_2]}{D^2-1}\left(\mathrm{Tr}[B_1]\mathrm{Tr}[B_2] - \frac{\mathrm{Tr}[B_1 B_2]}{D}\right) \\
&+ \frac{\mathrm{Tr}[A_1]\mathrm{Tr}[A_2]}{D^2-1}\left(\mathrm{Tr}[B_1 B_2] - \frac{\mathrm{Tr}[B_1]\mathrm{Tr}[B_2]}{D}\right)
\end{aligned} \tag{6.6}$$

para cualesquiera operadores A_1, A_2, B_1, B_2 en $\mathcal{B}(\mathcal{H})$.

Usando eso y la condición de preservación de traza, se recupera la Propiedad 3.2 que volvemos a enunciar aquí como

$$\frac{D\chi_{mn} + \delta_{mn}}{D+1} = \int_{\mathcal{H}} d\psi \langle\psi|\mathcal{E}(E_m^\dagger|\psi\rangle\langle\psi|E_n)|\psi\rangle. \tag{6.7}$$

6.2.2. Métodos que utilizan un twirl de todo el espacio

En esta sección veremos la comparación entre dos métodos que utilizan la operación de twirl. Uno es el ya presentado en el Capítulo 3, SEQPT. El otro, consiste en utilizar un twirl con los operadores del llamado grupo de Clifford. Comenzaremos por ver que el método SEQPT es un método basado en twirl.

SEQPT como método basado en twirl

La equivalencia entre el twirl de Haar en el espacio de operadores y en el espacio de estados es la base de la reinterpretación de SEQPT como un método basado en twirl. Sin embargo ambos twirls mencionados son twirls sobre espacios continuos (la medida de Haar incluye a *todos* los operadores unitarios). El salto para pasar a un conjunto discreto en el método SEQPT era a partir de los 2–diseños. De esa forma, se convertía la ecuación (6.7) en

$$\frac{D\chi_{mn}+\delta_{mn}}{D+1}=\frac{1}{D(D+1)}\sum_{Js}\left\langle\psi_s^J\right|\mathcal{E}\left(E_m^\dagger\left|\psi_s^J\right\rangle\left\langle\psi_s^J\right|E_n\right)\left|\psi_s^J\right\rangle. \tag{6.8}$$

La manera de convertir esto en un twirl es a partir de que sabemos transformar eficientemente un estado de un 2–diseño en otro (ver Apéndice B.1 para los circuitos). Si llamamos $|\psi_0\rangle$ a un estado particular del 2–diseño, y llamamos U_m^J al operador unitario eficiente tal que

$$U_m^J\left|\psi_0\right\rangle=\left|\psi_m^J\right\rangle, \tag{6.9}$$

entonces la ecuación (6.7) toma la forma

$$\frac{D\chi_{mn}+\delta_{mn}}{D+1}=\frac{1}{D(D+1)}\sum_{Js}\left\langle\psi_0\right|U_s^{J\dagger}\mathcal{E}(E_m^\dagger U_s^J\left|\psi_0\right\rangle\left\langle\psi_0\right|U_s^{J\dagger}E_n)U_s^J\left|\psi_0\right\rangle. \tag{6.10}$$

que no es otra cosa que un twirl del mapa $\mathcal{E}_{mn}$ sobre uno de los llamados 2–diseños unitarios, en este caso formado por los operadores U_s^J. A ese twirl (tanto en estados como en operadores) se lo denomina MUB twirl, por ser un twirl sobre un conjunto de bases mutuamente no sesgadas.

Vale destacar que no hemos hecho hasta aquí otra cosa que reinterpretar el algoritmo SEQPT en términos de la operación de twirl. Operacionalmente, seguimos hablando de exactamente el mismo algoritmo cuántico. En particular, para los mapas $\mathcal{E}_{mm}$, esto dice que, en lugar de muestrear sobre los estados del 2–diseño, debemos muestrar sobre los operadores del mismo (los U_s^J de la ecuación anterior) y medir la superviviencia promedio del estado $|\psi_0\rangle$.

SEQPT Vs. Twirl de Clifford

La equivalencia entre el twirl de Haar, el de MUBs y el twirl sobre el grupo de Clifford[Dan05] (la misma operación de twirl, pero esta vez tomando todos

los operadores del grupo de Clifford que se muestra en el Apéndice A.11) nos permite establecer una similitud entre ambos protocolos tomográficos. Esa equivalencia está reflejada en la siguiente ecuación

$$\begin{aligned}
&\langle\psi_0|\mathcal{E}^{\mathrm{HT}}(|\psi_0\rangle\langle\psi_0|)|\psi_0\rangle = \\
&= \frac{1}{|\mathcal{C}|}\sum_{l=1}^{|\mathcal{C}|}\langle\psi_0|\mathcal{C}_l^\dagger\mathcal{E}(\mathcal{C}_l|\psi_0\rangle\langle\psi_0|\mathcal{C}_l^\dagger)\mathcal{C}_l|\psi_0\rangle \\
&= \frac{1}{D(D+1)}\sum_{J,m}\langle\psi_{J,m}|\mathcal{E}(|\psi_{J,m}\rangle\langle\psi_{J,m}|)|\psi_{J,m}\rangle
\end{aligned} \tag{6.11}$$

donde los $\mathcal{C}_l$ son los operadores de Clifford en dimensión D y $|\psi_0\rangle$ es un estado arbitrario fijo. Ambos twirls utilizan la misma cantidad de recursos, ya que preparar un estado de una MUB a partir de la base computacional e implementar los $\mathcal{C}_l$ requieren, ambos, $O(n^2)$ compuertas de uno y dos qubits[BPP09, Dan05, Got97, Got96]. Además, el número de operadores de Clifford también es exponencial en el número de qubits n, como también lo es el número de estados en un conjunto de MUBs, por lo que en ambos casos hay que recurrir a un muestreo sobre el twirl. Es cierto que hay muchos más operadores de Clifford que estados en un conjunto de MUBs, pero en lo que hace a la complejidad, ambos son exponenciales.

En el Capítulo 3 vimos como medir selectivamente cualquier coeficiente diagonal de la matriz χ usando un twirl de MUB. Equivalentemente, con el twirl de Clifford se puede hacer lo mismo. Como hicimos en ese momento, si aplicamos un operador E_l antes de completar el twirl (ver Figura 6.3), la probabilidad de superviviencia es

$$\mathrm{Tr}[|\psi_0\rangle\langle\psi_0|\mathcal{E}_{ll}^{HT}(|\psi_0\rangle\langle\psi_0|)] = \frac{D\chi_{ll}+1}{D+1} \tag{6.12}$$

Esto se demuestra directamente a partir de la Ecuación (6.7).

De esta forma podemos medir eficientemente un coeficiente χ_{ll} por vez utilizando el twirl de Clifford. Esto no es de sorprender porque el grupo de Clifford también forma un 2–diseño, sólo que es un 2–diseño con muchos más operadores que el de las MUBs.

El protocolo SEQPT, como vimos en el Capítulo 3, se puede modificar para detectar y medir todos los coeficientes diagonales mayores a cierto valor

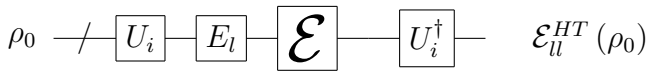

Figura 6.3: Representación circuital del twirl del mapa $\mathcal{E}_{ll}$. El promedio se realiza sobre los operadores U_i del conjunto sobre el que se realiza el twirl.

relacionado con la cantidad de experimentos realizados. Vimos que si se utiliza como base de operadores para describir al canal a los operadores de Pauli generalizados, entonces se pueden detectar todos los coeficientes $\chi_{ll} \geq 2/M$, donde M es el número de experimentos. La estrategia para ello se basa en tomar los experimentos de a pares, y en lugar de medir sólo supervivencia, medir todas las transiciones a los estados de la base en cuestión. Por ejemplo, si se toma como estado de entrada el $\left|\psi_m^J\right\rangle$ y se mide a la salida el estado $\left|\psi_{m'}^J\right\rangle$, ese experimento se nota como una terna (J, m, m'). De esa forma, dos experimentos en distintas bases sólo son compatibles con la acción de un único operador de Pauli E_l, aportando positivamente a la estimación de χ_{ll} (ver Capítulo 3 para más detalles).

Esta estrategia se puede utilizar también con operadores de Clifford actuando en el estado inicial en lugar de estados de las MUBs. Utilizaremos aquí el formalismo de los estabilizadores (ver Sección A.10).

Como el grupo Clifford transforma los operadores de Pauli en operadores de Pauli por conjugación, se tiene que

$$\mathcal{C} E_k \mathcal{C}^\dagger \cong E_{k'} \tag{6.13}$$

donde $\cong$ significa que son iguales a menos de una fase global. Eso quiere decir que si llamamos $(\mathcal{S}_Z, \bar{s})$ al estado estabilizado por el conjunto $\mathcal{S}_Z$ con autovalores $\bar{s}$, entonces la acción de $\mathcal{C}_j$ sobre ese estado es equivalente a cambiar $(\mathcal{S}_Z, \bar{s})$ por $(\mathcal{S}_P, \bar{s})$, donde ahora $\mathcal{S}_P$ es otro conjunto de n operadores de Pauli conmutativos.

Por lo tanto, en cada experimento también se entrará al canal con un estado $(\mathcal{S}_P, \bar{s}_{in})$ que surge de la aplicación del operador de Clifford al estado $|\psi_0\rangle$. A la salida, al volver atrás el cambio de base del Clifford, es equivalente a medir, luego del canal, en la misma base estabilizada por $\mathcal{S}_P$. Por lo tanto, cada experimento está caracterizado por una terna $(\mathcal{S}_P, \bar{s}_{in}, \bar{s}_{out})$. Esto es análogo al caso del MUB twirl; el primero elemento de la terna indica la base, el segundo el estado de entrada y el tercero el estado de salida. Nuevamente,

hay D operadores de Pauli posibles que realizan esa transformación (es decir, que conmutan o anticonmutan con los operadores de $\mathcal{S}_P$). Hasta aquí, todo sigue igual que en el twirl de MUB. La diferencia surge al intentar combinar pares de experimentos.

Nuevamente podemos intentar tomar los experimentos de a pares. Sin embargo, en el caso del twirl de Clifford no es tan simple como con el caso de las MUBs. Lo que deja de ser cierto es que dadas dos ternas (o sea, dos experimentos con sus resultados) exista un único posible Pauli que realice ambas transformaciones. Eso se debe a que dos operaciones de Clifford diferentes pueden mapear los operadores $\mathcal{S}_Z$ en dos conjuntos $\mathcal{S}_{P_1}$ y $\mathcal{S}_{P_2}$ que generan dos subgrupos de Pauli que tienen algunos operadores en común. Por eso, no todo par de experimentos con $\mathcal{C}_1 \neq \mathcal{C}_2$ servirá para establecer un único χ_{ll} sobre la cota $2/M$. Eso hace que la detección de coeficientes mayores a $2/M$ sea levemente más complicada y, en el peor caso, requiera mucha más memoria para guardar la lista de coeficientes mayores a dicho valor.

En la práctica, necesitamos determinar $2n$ operadores $\mathcal{C}_k \sigma_z^{(j)} \mathcal{C}_k^\dagger$ (donde $k = 1, 2$ son dos compuertas de Clifford elegidas al azar) y chequear si son dos conjuntos de generadores independientes. Si ese es el caso, entonces de hecho hay un único operador de Pauli que pueda ser responsable de ambos experimentos. Gracias al teorema de Gottesman–Knill[NC04], eso siempre se puede hacer eficientemente con una computadora clásica.

Para comparar ambos métodos, consideremos la probabilidad de determinar satisfactoriamente un único Pauli que pueda ser responsable de los resultados de dos experimentos tomados al azar. En el caso del twirl de MUB, la probabilidad de éxito es $p_{MUB} = D/(D+1)$, ya que hay $D+1$ bases, y cada vez que se agarren experimentos hechos en bases distintas se encontrará un único operador posible.

Para el caso de Clifford, la probabilidad se puede calcular de la siguiente forma: dados dos subgupos de Pauli abelianos máximos, ¿cuál es la probabilidad de que el único elemento en común sea la identidad? Para calcular dicha probabilidad, procedemos de la siguiente forma: fijamos el primer grupo abeliano máximo y computamos la probabilidad de que esto ocurra a medida que vamos agregando uno por uno los elementos del segundo grupo. El primer grupo tiene, a menos de una fase, $D-1$ operadores de Pauli (sin contar la identidad). Si elegimos al azar un operador de Pauli distinto a la identidad, por ejemplo E_1, ¿cuál es la probabilidad de que no pertenezca al primer grupo? Es directo ver que esa probabilidad es $\frac{D^2-D}{D^2-1}$. Ahora, de los

operadores de Pauli que conmutan con E_1, ¿cuál es la probabilidad de elegir otro operador E_2 que no pertenezca al primer grupo? Nuevamente, hay un total de $D^2/2 - 2$ operadores de Pauli que conmutan con E_1 y no son ni E_1 ni la identidad, pero $D/2 - 1$ de ellos pertenecen al primer grupo. Luego, la probabilidad de que esto ocurra es $\frac{D^2/2-1-D/2}{D^2/2-2}$. Seguimos de la misma forma, computando la probabilidad de elegir un operador de Pauli que no pertenezca ni al primer grupo ni al grupo generado por los operadores ya elegidos. El producto de todas esas probabilidades es la probabilidad p_C de tener sólo un operador de Pauli posible responsable por ambos experimentos:

$$p_C = \prod_{j=0}^{n-1} \frac{D^2/2^j - 2^j - D/2^j}{D^2/2^j - 2^j} \tag{6.14}$$

Como se muestra en la Figura 6.4, esta probabilidad es menos pero asintóticamente equivalente a p_{MUB}. Para los experimentos hechos hasta el momento, de tan solo unos pocos qubits, el twirl de MUB sigue siendo más práctico para obtener los coeficientes más grandes.

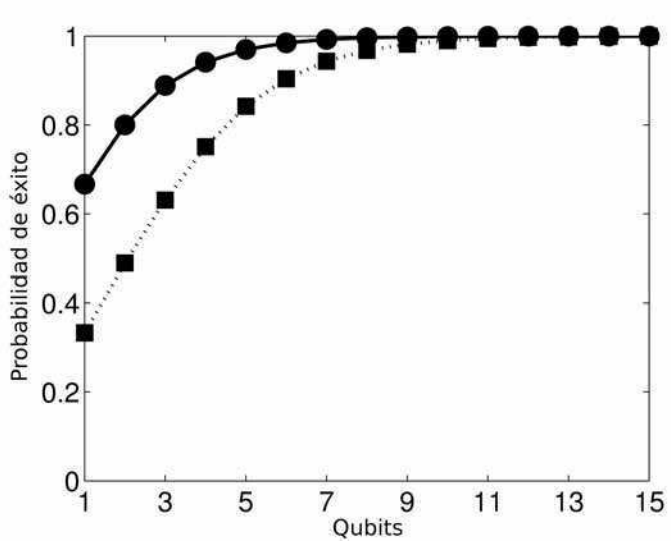

Figura 6.4: Probabilidad de éxito de los dos métodos: p_{MUB}, usando un twirl de MUBs (●) y p_C, usando un twirl de Clifford (■).

En este punto podemos concluir que el SEQPT presentado en el Capítulo 3 es levemente superior al protocolo con el twirl de Clifford. Sin embargo,

ambos son asintóticamente equivalentes.

Estos dos protocolos con twirl de todo el espacio, a pesar de ser eficientes, requieren de la implementación sin errores de los operadores sobre los que se hace el twirl (ya sea el 2–diseño o el de Clifford), o al menos con menos errores que la implementación de $\mathcal{E}$. Si poseemos un sistema cuántico que permite implementar compuertas de Hadamard, de fase, operadores de Pauli y CNOT (son las que se utilizan tanto para los operadores de Clifford como para el 2–diseño) con suficiente precisión, estamos en condiciones de estudiar mapas complejos con estos twirls. Si, en cambio, queremos estudiar compuertas y secuencias de compuertas cuya complejidad es comparable a la de las compuertas del grupo de Clifford o el 2–diseño, entonces el método no servirá. Para ese caso, es que resulta conveniente realizar twirls en espacios más pequeños, como en los métodos que se detallan en la próxima sección.

6.2.3. Métodos con twirl de un solo qubit

En esta sección hablaremos de métodos basados en el twirl de un qubit del canal. Ya hemos hablado muy brevemente de ellos en la Sección 2.3.3, pero entraremos aquí en más detalle sobre esos y otros métodos similares[ESM+07, LLC09, LLEC07]. Un twirl de un solo qubit es un twirl que actúa como el producto tensorial de los distintos operadores del twirl en cada qubit. Tanto el método de SCNQP de la Sección 2.3.3 como el presentado en [LLC09] pueden interpretarse como casos particulares de un método general que mostraremos aquí. Vale destacar que ambos métodos han sido implementados experimentalmente.

Ya vimos en la Sección 6.2.2 la importancia del twirl de Haar y mencionamos su equivalencia con el twirl de Clifford. En ésta sección trabajaremos directamente con el twirl de Clifford. Para ello, vamos a usar el hecho de que los operadores de Clifford pueden descomponerse en operadores de Pauli (el normalizador del grupo de Clifford) y otros operadores denominados *operadores simplécticos*[2].

Seguiremos aquí la notación de [ESM+07]. Antes utilizábamos un índice m para los operadores de la base E_m (es decir, m identificaba al operador

[2]Los operadores de Pauli dejan invariantes, a menos de una fase, al grupo de Pauli. Los operadores simplécticos, en cambio, son los que hacen mapeos no triviales entre los mismos.

de Pauli E_m) y dos para los de la matriz χ_{mn}. Ahora reemplazaremos cada subíndice m por una terna

$$m \longrightarrow w, \nu_w, \mathbf{i}_w \tag{6.15}$$

donde w indica el peso de Pauli de E_m. Es decir, que E_m actúa de manera distinta a la identidad en w qubits. El índice $\nu_w \in \left\{1, 2, \ldots, \binom{n}{w}\right\}$ indica sobre cuáles de esos w está actuando el Pauli de manera no trivial. Por último, el índice $\mathbf{i}_w$ es un vector de longitud w de la forma $\mathbf{i}_w = (i_1, i_2, \ldots, i_w)$, en el que cada componente índica qué Pauli ($1 \to \sigma_x$, $2 \to \sigma_y$, o $3 \to \sigma_z$) actúa en cada uno de los qubits seleccionados por $\mathbf{i}_w$.

Comenzamos por analizar el twirl de Pauli (PT) del canal. Eso transforma a $\mathcal{E}$ en

$$\mathcal{E}^{\mathrm{PT}}(\rho) = \frac{1}{D^2} \sum_{l=0}^{D^2-1} E_l \mathcal{E}(E_l \rho E_l) E_l \tag{6.16}$$

$$= \frac{1}{D^2} \sum_{l=0}^{D^2-1} \sum_{mn}^{D^2-1} \chi_{mn} E_l E_m E_l \rho E_l E_n E_l \tag{6.17}$$

$$= \sum_{m=0}^{D^2-1} \chi_{mm} E_m \rho E_m \tag{6.18}$$

Este resultado, probado en [Dan05], puede entenderse de la siguiente forma: para $m = n$, $E_l E_m E_l \rho E_l E_m E_l = E_m \rho E_m$ ya que cada E_m conmuta o anti-conmuta con cada E_l. Y en el caso en que $m \neq n$ en cada qubit j en el que difieren tenemos que $E_l^{(j)} E_m^{(j)} E_l^{(j)} \rho E_l^{(j)} E_n^{(j)} E_l^{(j)} = \pm E_m^{(j)} \rho E_n^{(j)}$, con cada signo apareciendo la mitad de las veces. Por lo tanto, todos se cancelan en la suma.

Ahora consideremos el twirl simpléctico de un qubit (S1T), que es de la forma

$$\mathcal{E}^{\mathrm{S1T}}(\rho) = \frac{1}{3^n} \sum_{m=1}^{3^n} S_m^\dagger \mathcal{E}(S_m \rho S_m^\dagger) S_m \tag{6.19}$$

$$S_m = \bigotimes_{j=1}^{n} S_m^{(j)} \tag{6.20}$$

donde los $S_m^{(j)}$ son los elementos del conjunto formado por los operadores $\{\exp(-i(\pi/4)\sigma_p),\ p = x, y, z\}$[3].

[3]Es simple comprobar explícitamente que dichos operadores mapean el grupo de Pauli en sí mismo de manera no trivial.

Es fácil mostrar que

$$\frac{1}{3}\sum_{l=1}^{3} S_l^{(j)\dagger}\sigma_j S_l^{(j)}\rho S_l^{(j)\dagger}\sigma_j S_l^{(j)} = \frac{\sigma_x\rho\sigma_x + \sigma_y\rho\sigma_y + \sigma_z\rho\sigma_z}{3}$$

Por lo tanto, luego del twirl de Clifford de un qubit (C1T, compuesto por el de Pauli y el simpléctico) se obtiene

$$\begin{aligned}
\mathcal{E}^{\mathrm{C1T}}(\rho) &= \frac{1}{3^n}\sum_{l=0}^{3^n} S_l^\dagger \mathcal{E}^{\mathrm{PT}}(S_l\rho S_l^\dagger)S_l && (6.21)\\
&= \sum_{w=0}^{n}\sum_{\nu_w}^{\binom{n}{w}} \frac{\chi^{col}_{w,\nu_w}}{3^w}\left(\sum_{\mathbf{i}_w} E_{w,\nu_w,\mathbf{i}_w}\rho E_{w,\nu_w,\mathbf{i}_w}\right) && (6.22)
\end{aligned}$$

donde los coeficientes colectivos χ^{col}_{w,ν_w} no son otra cosa que los coeficientes diagonales χ_{mm} de la matriz χ renombrados a $\chi_{w,\nu_w,\mathbf{i}_w}$, luego de promediar sobre los $\mathbf{i}_w$:

$$\chi^{col}_{w,\nu_w} \equiv \sum_{\mathbf{i}_w}\chi_{w,\nu_w,\mathbf{i}_w} \tag{6.23}$$

Esté es el corazón del método presentado en [ESM+07].

Veamos cómo se realciona ese resultado con probabilidades de supervivencia. Consideremos un estado de la base computacional $|\bar{v}_h\rangle$, donde $\bar{v}_h$ es un vector booleano de longitud n y peso de Hamming h. (El peso de Hamming h de un vector binario es el número de unos que contiene). El primer resultado que podemos obtener es que la probabilidad de supervivencia del estado $|\bar{v}_h\rangle$ es independiente del estado,

$$\begin{aligned}
& f(\mathcal{E}^{\mathrm{C1T}}, |\bar{v}_h\rangle) = \langle\bar{v}_h|\mathcal{E}^{\mathrm{C1T}}(|\bar{v}_h\rangle\langle\bar{v}_h|)|\bar{v}_h\rangle && (6.24)\\
=\ & \sum_{w=0}^{n}\sum_{\nu_w}^{\binom{n}{w}} \frac{\chi^{col}_{w,\nu_w}}{3^w}\left(\sum_{\mathbf{i}_w}^{3^w} |\langle\bar{v}_h|E_{w,\nu_w,\mathbf{i}_w}|\bar{v}_h\rangle|^2\right) && (6.25)\\
=\ & \sum_{w=0}^{n}\sum_{\nu_w}^{\binom{n}{w}} \frac{\chi^{col}_{w,\nu_w}}{3^w}\left(\sum_{\mathbf{i}_w}^{3^w} |\langle 0|E_{w,\nu_w,\mathbf{i}_w}|0\rangle|^2\right) && (6.26)\\
=\ & \sum_{w=0}^{n}\sum_{\nu_w}^{\binom{n}{w}} \frac{\chi^{col}_{w,\nu_w}}{3^w} && (6.27)
\end{aligned}$$

Para pasar de (6.25) a (6.26), debemos tener en cuenta que $|\bar{v}_h\rangle$ se obtiene de aplicar el operador de Pauli $E_x^{\bar{v}_h}$ (que tiene σ_x en cada posición en que $\bar{v}_h$ tiene unos e identidades en el resto) a $|0\rangle$. Ese operador $E_x^{\bar{v}_h}$ va a conmutar o anticonmutar con $E_{w,\nu_w,\mathbf{i}_w}$ y el signo será absorbido por el módulo cuadrado. La ecuación (6.27) se obtiene teniendo en cuenta que el único operador no trivial $E_{w,\nu_w,\mathbf{i}_w}$ que lleva el estado $|0\rangle$ a sí mismo (a menos de una fase) es aquel que tiene σ_z en todas las posiciones indicadas por ν_w, y por lo tanto el único posible de todos los $\mathbf{i}_w$ dados ν_w y w.

Vale aclarar que aunque $f(\mathcal{E}^{\mathrm{C1T}}, |\bar{v}_h\rangle)$ es equivalente a la fidelidad promedio $\overline{F}(\mathcal{E}^{\mathrm{C1T}})$ del proceso $\mathcal{E}^{\mathrm{C1T}}$, esa no es la fidelidad promedio del canal estudiado (es decir, el canal sin *twirlear*). Es decir, no obtenermos $\overline{F}(\mathcal{E}) = (D\chi_{00}+1)/(D+1)$ del método SEQPT (ver Capítulo 3). Sin embargo, este twirl factorizado provee una información distinta sobre la estructura del canal $\mathcal{E}$. El primer resultado a mencionar, presentado en [ESM+07], es que se pueden obtener ciertos coeficientes de la matriz χ agrupados por peso de Pauli

$$p_w \equiv \sum_{\nu_w}^{\binom{n}{w}} \sum_{\mathbf{i}_w} \chi_{w,\nu_w,\mathbf{i}_w} = \sum_{\nu_w}^{\binom{n}{w}} \chi^{col}_{w,\nu_w} \tag{6.28}$$

Los parámetros p_w y χ^{col}_{w,ν_w} son parámetros promedio de los elementos diagonales de la matriz χ. Los p_w se relacionan con la probabilidad $\mathrm{Prob}\,(\bar{v}_h, h)$ de obtener cualquier estado $|\bar{v}_h\rangle$ con peso de Hamming h al medir sobre el estado $\mathcal{E}^{\mathrm{C1T}}(|0\rangle\langle 0|)$. En efecto, tenemos que

$$\begin{aligned} \mathrm{Prob}\,(\bar{v}_h, h) &= \langle \bar{v}_h | \mathcal{E}^{\mathrm{C1T}}(|0\rangle\langle 0|) | \bar{v}_h \rangle \\ &= \sum_{w=0}^{n} \sum_{\nu_w}^{\binom{n}{w}} \frac{\chi^{col}_{w,\nu_w}}{3^w} \left(\sum_{\mathbf{i}_w}^{3^w} |\langle 0 | E_{w,\nu_w,\mathbf{i}_w} | \bar{v}_h \rangle|^2 \right) \end{aligned} \tag{6.29}$$

Para que $\langle 0|E_{w,\nu_w,\mathbf{i}_w}|\bar{v}_h\rangle$ sea distinto de cero (es decir, ± 1), ν_w tiene que tener factores distintos de la identidad al menos donde hay unos en $\bar{v}_h$, por lo que tiene que $w \geq h$. Además, los i_j en $\mathbf{i}_w$ tienen que ser $1 = x$ o $2 = y$ para los qubits con unos en $\bar{v}_h$, y $3 = z$ para los $w - h$ qubits que tienen ceros en $\bar{v}_h$ pero no una identidad en $E_{w,\nu_w,\mathbf{i}_w}$. Entonces habrá exactamente 2^h de esos operadores para w y ν_w dados, por lo tanto

$$\mathrm{Prob}\,(\bar{v}_h, h) = \sum_{w=h}^{n} \sum_{\nu_w^*=1}^{\binom{n-h}{w-h}} \frac{2^h}{3^w} \chi^{col}_{w,\nu_h+\nu_w^*} \tag{6.30}$$

donde ν_h indica χ^{col}_{w,ν_w} para operadores de Pauli que no tienen una identidad en al menos todos los qubits cuya componente en $\bar{v}_h$ correspondiente es un uno. La etiqueta ν^*_w indica los $\binom{n-h}{w-h}$ coeficientes con $w \geq h$ que satisfacen esa condición. Si descartamos la información acerca de cuáles qubits tienen un uno al medir, sumando sobre todas las $\binom{n}{h}$ posibilidades, entonces

$$\begin{aligned}
\text{Prob}\,(h) &= \sum_{\bar{v}_h} \text{Prob}\,(\bar{v}_h, h) && (6.31)\\
&= \sum_{w=h}^{n} \frac{2^h}{3^w} \sum_{\nu^*_w=1}^{\binom{n-h}{w-h}} \sum_{\nu_h=1}^{\binom{n}{h}} \chi^{col}_{w,\nu_h+\nu^*_w} && (6.32)\\
&= \sum_{w=h}^{n} \frac{2^h}{3^w} \binom{w}{h} \left(\sum_{\nu_w=1}^{\binom{n}{w}} \chi^{col}_{w,\nu_w} \right) && (6.33)\\
&= \sum_{w=h}^{n} \frac{2^h}{3^w} \binom{w}{h} p_w && (6.34)
\end{aligned}$$

De esta forma, todos los p_w están relacionados con las probabilidades de medir una salida con peso de Hamming h mediante una matriz de $n \times n$ $R_{h,w} = \frac{2^h}{3^w}\binom{w}{h}$, como se explica en [ESM+07].

Veamos ahora la estrategia seguida en [LLC09], dentro de éste mismo marco teórico. La idea es mantener la información acerca de qué qubits tienen uno en la salida, usando toda la información de $\text{Prob}\,(\bar{v}_h, h)$.

Para empezar, reemplacemos w y ν_w por $\bar{v}_w$, un vector booleano de longitud n y peso de Hamming w que caracteriza parcialmente un operador de Pauli E_l. $\bar{v}_w$ tiene cero en la j–ésima posición si y sólo si $E^{(j)}_l = \mathbb{I}$, en cualquier otro caso, tiene un uno. Por ejemplo, el operador $\sigma^{(1)}_z \sigma^{(3)}_x$ de $n = 4$ qubits tiene $\bar{v}_2 = (1, 0, 1, 0)$. Hay, por supuesto, $\sum_{w=0}^{n} \binom{n}{w} = 2^n = D$ de esos vectores para describir a los operadores de Pauli.

Usando la ecuación (6.30) y comenzando por la probabilidad de tener todos los qubits en uno a la salida, y bajando sucesivamente hasta la probabilidad de superviviencia del estado $|0\rangle$ correspondiente a todos ceros a la

salida, se obtiene que

$$\text{Prob}\,(n) = \frac{2^n}{3^n}\chi^{col}_{\bar{v}_n} \tag{6.35a}$$

$$\text{Prob}\,(\bar{v}_{n-1}, n-1) = \frac{2^{n-1}}{3^{n-1}}\chi^{col}_{\bar{v}_{n-1}} + \frac{2^{n-1}}{3^n}\chi^{col}_{\bar{v}_n} \tag{6.35b}$$

$$\text{Prob}\,(\bar{v}_{n-2}, n-2) = \frac{2^{n-2}}{3^{n-2}}\chi^{col}_{\bar{v}_{n-2}} + \sum_{\bar{v}_{n-1}} \frac{2^{n-2}}{3^{n-1}}\chi^{col}_{\bar{v}_{n-1}} + \frac{2^{n-2}}{3^n}\chi^{col}_{\bar{v}_n} \tag{6.35c}$$

$$\ldots \; etc.$$

Por lo tanto, podemos determinar $\chi^{col}_{\bar{v}_n}$ usando (6.35a), luego combinarlo con (6.35b) y obtener los n posibles $\chi^{col}_{\bar{v}_{n-1}}$ a partir de las diferentes probabilidades $\text{Prob}\,(\bar{v}_{n-1}, n-1)$, para luego combinar eso con la ecuación (6.35c), y así sucesivamente. Esas ecuaciones definen una matriz triangular que relaciona las probabilidades $\text{Prob}\,(\bar{v}_h, h)$ con los coeficientes colectivos $\chi^{col}_{\bar{v}_w}$. Vale la pena destacar que no es necesario realizar diferentes experimentos para obtener diferentes probabilidades. Sólo necesitamos implementar M operadores del twirl y guardar los resultados de las mediciones para cada uno de ellos. Ese resultado es un string binario de longitud n que indica si cada qubit fue encontrado en el estado $|0\rangle$ o $|1\rangle$.

El problema no es la obtención experimental de los datos, sino el post-proceso clásico necesario para obtener los coeficientes buscados. La matriz dada por las ecuaciones (6.35) es de $D \times D$, por lo que la complejidad del procesamiento de la misma (aunque sea sólo en capacidad de almacenamiento) escalea exponencialmente con n. Para que esta estrategia funcione es fundamental relacionarla jerárquicamente con la determinación de los p_w: la información experimental requerida es la misma y puede obtenerse eficientemente mediante un muestreo. La idea es la siguiente: si estamos analizando un mapa $\mathcal{E}$ que es cercano a la identidad (un canal de ruido, por ejemplo) o un circuito cuántico que involucra sólo algunos qubits, entonces podemos esperar que por encima de un cierto peso de Pauli de corte w_{co}, los p_w sean nulos. Esta es una condición rasonable. Puesto que por la preservación de la traza del canal vale que $\sum_{w=0}^{n} p_w = 1$, los p_w no pueden ser todos arbitrariamente grandes, haciendo posible acotar los coeficientes por encima del corte por una cantidad despreciable. En un caso así, la matriz que relaciona las probabilidades $\text{Prob}\,(\bar{v}_h, h)$ con los $\chi^{col}_{\bar{v}_w}$ tendrá tamaño $M_{co} \times M_{co}$, $M_{co} = \sum_{m=0}^{w_{co}} \binom{n}{m}$,

que escalea polinomialmente con n. Hay, sin embargo, una segunda dificultad. Como se explica en [ESM+07, LLC09], los errores en la determinación de los p_w o los χ^{col}_{w,ν_w} escalean ineficientemente con w como consecuencia de las matrices que los relacionan con las correspondientes probabilidades de las ecuaciones (6.34) y (6.35), respectivamente. A pesar de que las probabilidades medidas tienen una desviación estándar $\leq 1/\sqrt{M}$, este error se propagará hacia los p_w o los χ^{col}_{w,ν_w} con un factor que crece polinomialmente con n pero exponencialmente con w. Nuevamente, necesitamos despreciar las probabilidades p_w inferiores a un cierto valor de corte. El sistema puede ser arbitrariamente grande, pero siempre y cuando las probabilidades p_w sean despreciables por encima de un cierto w_{co} (con w_{co} escaleando a lo sumo polinomialmente con n) podremos obtener toda la información no despreciable de los χ^{col}_{w,ν_w} eficientemente.

Nótese que, en la sección anterior, el requerimiento de que sólo unos pocos ($<< D$) coeficientes $\chi_{w,\nu_w,\mathbf{i}_w}$ sean no despreciables no es a priori. Podemos ejecutar el protocolo y arribar a esa conclusión eficientemente.

Con el twirl de Clifford completo (Clifford de n qubits) obtenemos directamente los coeficientes con una desviación estándar $\sigma \leq 1/\sqrt{M}$, mientras que con el twirl de Clifford de un qubit sólo obtenemos *probabilidades* Prob $(\bar{v}_h, h)$ con desviaciones estándar $\sigma \leq 1/\sqrt{M}$, que luego deben ser propagadas para obtener los errores estimados para los coeficientes colectivos χ^{col}_{w,ν_w}.

Con el protocolo SEQPT, la medición de los ρ_{mm} más grandes puede hacerse más precisamente, sin perder información y sin restricciones sobre el canal estudiado. Claramente, el protocolo de esta sección [ESM+07, LLC09] requiere de menos recursos ya que sólo es necesario implementar $12n$ compuertas de un qubit en lugar de $O(n^2)$ compuertas de un qubit y CNOTs. En la práctica, sin embargo, el método que se elija dependerá de la capacidad experimental que se posea, y del tipo de información que se desee obtener de los procesos.

6.3. Conclusiones parciales

En éste capítulo comparamos diferentes métodos tomográficos. En primer lugar, vimos que SEQPT y DCQD son métodos muy parecidos si se los observa desde la perspectiva de DCQD: ambos utilizan el mismo tipo de circuito cuántico, pero DCQD aprovecha correlaciones cuánticas a la hora de

realizar la medición y SEQPT da cuenta de las correlaciones manualmente.

Luego estudiamos los métodos basados en twirl. Vimos que el SEQPT es un método basado en el twirl sobre el conjunto de estados de un 2–diseño, y que da los mismos resultados que el método basado en el twirl de Clifford. Sin embargo, el SEQPT es levemente más simple cuando se trata de la determinación simultánea de coeficientes diagonales.

Por último, vimos en detalle los métodos basados en el twirl de cada qubit por separado. Esos métodos permiten la obtención de información que resulta muy importante, en especial, para la elección de un método de corrección de errores adecuado.

Parte II

Tomografía de estados cuánticos

Capítulo 7

Tomografía de estados cuánticos

> Por surcar mejores aguas alza las velas
> ahora la navecilla de mi ingenio,
> tan cruel mar detrás de sí dejando
>
> *La Divina Comedia*
> *Dante Alighieri*

El estado de un sistema cuántico no es una magnitud observable. Ese hecho es una particularidad importante de la mecánica cuántica: todo el formalismo se basa en la evolución de estados cuánticos y, sin embargo, los mismos no se pueden medir. A pesar de eso, si uno dispone de múltiples copias de sistemas preparados en el mismo estado, se pueden realizar distintas mediciones a cada copia permitiendo reconstruir el estado en cuestión. A esa tarea se la denomina tomografía de estados cuánticos.

En éste capítulo introduciremos algunos conceptos generales sobre la tomografía de estados cuánticos. Aunque existen infinidad de métodos para realizar dicha tarea[NC04, PŘ04a, GLF$^+$10, CPF$^+$10, MPS$^+$02], sólo daremos un breve reapso a los que nos servirán más adelante.

7.1. Descripción de los estados cuánticos

El estado de un sistema cuántico ρ es un operador lineal, hermítico, positivo y de traza unitaria perteneciente al conjunto $\mathcal{B}(\mathcal{H})$ de operadores $\mathcal{H} \to \mathcal{H}$, como se comenta en el Apéndice A.1.

De igual forma que todo operador lineal, el operador densidad de un estado puede escribirse en una base arbitraria de $\mathcal{B}(\mathcal{H})$. Algunas de esas bases resultan más convenientes para la descripción del estado por la forma en que manifiestan ciertas características del mismo, y por la conveniencia operacional para, por ejemplo, utilizar el conocimiento de esos estados para realizar algún algoritmo cuántico.

En general, dada una base $\mathcal{S} = \{B_a \in \mathcal{B}(\mathcal{H}), a = 0, \ldots, D^2 - 1\}$ del espacio $\mathcal{B}(\mathcal{H})$, un operador densidad puede escribirse como

$$\rho = \sum_a \alpha_a B_a \tag{7.1}$$

Y dependiendo de la elección de la base de operadores, los coeficientes $\alpha_a \in \mathbb{C}$ reflejaran las propiedades del estado ρ de distinta manera.

7.1.1. Expansión en operadores de Pauli generalizados

Una opción habitual es utilizar como base $\mathcal{S}$ la base de operadores de Pauli generalizados. En esta base, el estado se escribe como

$$\frac{1}{D} \sum_a \alpha_a P_a \tag{7.2}$$

donde el factor $\frac{1}{D}$ se utiliza para la normalización.

En esta base, las propiedades del operador densidad se traducen en propiedades simples sobre los coeficientes α_a:

- Si $P_0 = \mathbb{I}$, entonces la normalización $\mathrm{Tr}\rho = 1$ se traduce en $\alpha_0 = 1$.
- La condición $\rho = \rho^\dagger$ se traduce en $\alpha_a \in \mathbb{R}$.
- La pureza del estado es $\mathrm{Tr}(\rho^2) = \frac{1}{D} \sum_a \alpha_a^2$.

Además, dada la ortomormalidad de los operadores de Pauli, la tomografía selectiva es directa ya que

$$\mathrm{Tr}(\rho P_k) = \alpha_k \tag{7.3}$$

Es decir, para medir cada coeficiente sólo es necesario medir el valor medio del operador de Pauli generalizado correspondiente.

7.1.2. Expansión en una base de $\mathcal{H}$

Otra representación habitual del operador densidad es mediante la matriz densidad en una base dada del espacio de Hilbert. Si la base de $\mathcal{H}$ en cuestión es $\mathcal{Q} = \{|\psi_a\rangle, a = 1, \ldots, D\}$ el estado se escribe como

$$\rho = \sum_{ab} \langle\psi_a| \rho |\psi_b\rangle |\psi_a\rangle \langle\psi_b| = \sum_{ab} \alpha_{ab} |\psi_a\rangle \langle\psi_b| \tag{7.4}$$

En este caso, todas las propiedades del operador densidad (hermiticidad, positividad y traza) se traducen directamente a las mismas propiedades sobre la matriz α.

En la próxima sección veremos como realizar tomografía selectiva de los coeficientes de la matriz α.

7.1.3. Tomografía de estados

Supongamos que se desea hacer tomografía de un estado en la base $\mathcal{Q}$ de $\mathcal{H}$, como se describió en la Sección 7.1.2[NC04]. Los elementos diagonales son las probabilidades de obtener cada uno de los estados de la base $\mathcal{Q}$ al realizar una medición en dicha base. En efecto,

$$\begin{aligned} \mathrm{Tr}\left(\rho |\psi_j\rangle \langle\psi_j|\right) &= \sum_{abk} \alpha_{ab} \langle\psi_k|\psi_a\rangle \langle\psi_b|\psi_j\rangle \langle\psi_j|\psi_k\rangle \\ &= \sum_{abk} \alpha_{ab}\delta_{ka}\delta_{bj}\delta_{jk} = \alpha_{jj} \end{aligned} \tag{7.5}$$

Es decir, medir en la base $\mathcal{Q}$ recupera toda la información sobre los elementos diagonales de ρ.

La medición de los elementos no diagonales es levemente más complicada. Para ello, es necesario poder medir proyecciones sobre estados que son combinaciones de los de la base $\mathcal{Q}$. Consideremos los estados

$$|\psi_{ab,\pm}\rangle = \frac{1}{\sqrt{2}} \left(|\psi_a\rangle \pm |\psi_b\rangle\right). \tag{7.6}$$

Si se mide la probabilidad de tener el estado $|\psi_{ab,\pm}\rangle$, se tiene que

$$\mathrm{Tr}\left(\rho |\psi_{ab,\pm}\rangle \langle\psi_{ab,\pm}|\right) = \langle\psi_{ab,\pm}| \rho |\psi_{ab,\pm}\rangle = \frac{1}{2} \left(\alpha_{aa} + \alpha_{bb} \pm \alpha_{ab} \pm \alpha_{ba}\right) \tag{7.7}$$

de donde se obtiene que

$$\mathrm{Tr}\left(\rho |\psi_{ab,+}\rangle \langle\psi_{ab,+}|\right) - \mathrm{Tr}\left(\rho |\psi_{ab,-}\rangle \langle\psi_{ab,-}|\right) = 2\mathrm{Re}\left(\alpha_{ab}\right) \tag{7.8}$$

Luego, a partir de medir la probabilidad de que el estado sea el $|\psi_{ab,+}\rangle$ o el $|\psi_{ab,-}\rangle$ se obtiene la parte real del coeficiente α_{ab}. La parte imaginaria se obtiene de la misma forma, a partir de las probabilidades de encontrar al estado ρ en cualquiera de los estados

$$|\psi_{ab,\pm i}\rangle = \frac{1}{\sqrt{2}} \left(|\psi_a\rangle \pm i \, |\psi_b\rangle \right). \tag{7.9}$$

De esta forma se puede medir selectivamente cada coeficiente de la matriz α. Cabe destacar que el método no es eficiente porque medir la probabilidad de estar en un estado particular tiene la misma eficiencia que preparar dicho estado y, en general, la preparación de un estado arbitrario no es eficiente. Por lo tanto, la eficiencia del método depende de la base elegida.

7.2. Mediciones proyectivas y generalizadas

Una parte fundamental de la tomografía de estados es la medición. La mecánica cuántica, desde sus postulados, permite las mediciones proyectivas. Sin embargo, existe otro tipo de mediciones denominadas *mediciones generalizadas* o *POVMs* que utilizan un sistema auxiliar y que aumentan el poder de las mediciones. Veremos en esta sección una breve introducción a ambos tipos de mediciones que extenderemos en el capítulo próximo al caso en el que se dispone de copias simultáneas del estado a medir.

7.2.1. Mediciones proyectivas

Uno de los problemas más interesantes de la mecánica cuántica tiene que ver con la medición. Uno de los postulados de la mecánica cuántica, formalizado por von Neumann, explica cómo calcular la probabilidad de obtener cada posible resultado de una medición: Si el sistema fue preparado en un estado ρ, entonces para cada resultado μ de una medición existe un proyector Π_μ tal que la probabilidad de obtener el resultado μ es el valor de expectación del proyector Π_μ en el estado ρ. Es decir,

$$Prob(\mu) = Tr(\rho \Pi_\mu) \tag{7.10}$$

La representación de operadores mutuamente exclusivos es mediante projectores ortogonales, es decir, $\Pi_\mu \Pi_\nu = \delta_{\mu\nu} \Pi_\mu$. Y el hecho de siempre obtener algún resultado de entre los resultados posibles se traduce en que la suma

de los proyectores asociados a todos los posibles resultados de una medición deben sumar la identidad,

$$\sum_{\mu} \Pi_{\mu} = \mathbb{I}. \tag{7.11}$$

Esta última ecuación se puede interpretar diciendo que una medición tiene siempre un resultado.

7.2.2. Mediciones generalizadas

Los POVMs (Medición valorada por operadores positivos) son una extensión al postulado de las mediciones proyectivas que fue introducida en la década de 1970 [SoQT83] con la noción de medición generalizada. En ese tipo de medición, los proyectores son reemplazados por operadores positivos A_{μ}, donde μ es cada resultado posible de la medición y la probabilidad de obtener el resultado μ está dada por

$$Prob(\mu) = Tr(\rho A_{\mu}). \tag{7.12}$$

Los operadores A_{μ}, al igual que los proyectores Π_{μ} de las mediciones proyectivas, deben sumar la identidad:

$$\sum_{\mu} A_{\mu} = \mathbb{I} \tag{7.13}$$

El conjunto de operadores A_{μ} define los llamados POVM. El teorema de Neumark[Per95, Pre98] (ver Apéndice E para una demostración) establece que la medición de un POVM es equivalente a la medición proyectiva en conjunto del sistema y un sistema auxiliar debidamente preparado. Todo POVM puede ser implementado via una medición proyectiva en un sistema extendido, como se ilustra en la Figura 7.1.

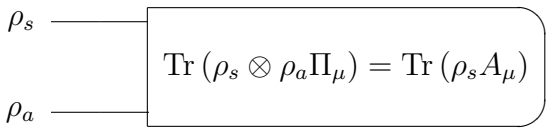

Figura 7.1: Esquema de medición de los POVMs. Todo POVM puede implementarse como una medición proyectiva sobre el sistema ρ_s y un sistema auxiliar ρ_a debidamente preparado.

Este tipo de mediciones incluye a las mediciones proyectivas (los proyectores son operadores positivos) y agrega nueva capacidad a la medición sobre sistemas cuánticos.

7.3. Conclusiones parciales

Vimos en este capítulo algunas generalidades sobre tomografía de estados cuánticos. En particular, estudiamos como desarrollar un estado en una base de operadores y en una base del espacio de Hilbert. En ambos casos, vimos como realizar tomografía de estados. Por último, introdujimos la noción de POVM.

En el próximo capítulo extenderemos esas nociones al caso en que se dispone más de una copia del estado para realizar mediciones simultáneas.

Capítulo 8

Teoría general de la medición con dos copias simultáneas del estado

Corté la naranja en dos,
y las dos partes no pudieron quedar
iguales.
¿Para cuál fui injusto,
yo, que voy a comer ambas?

Ayer el predicador de sus verdades
Fernando Pessoa

En este capítulo veremos, en primer término, como se extiende la teoría de las mediciones generalizadas, cuando se poseen dos copias simultáneas del estado. Esta se tranforma en una teoría de la medición por mapas completamente copositivos[BPC09] (Completely co-positive map valued measure o CCPMVM). A continuación veremos cómo aplicar dicha teoría a la tomografía de estados, y a la medición de algunas propiedades ineresantes de estados cuánticos como la pureza y la concurrencia. Finalmente veremos como esta teoría puede ser aprovechada para la tomografía de procesos.

8.1. Medición con dos copias simultáneas del estado

El teorema de Neumark y la teoría de los POVMs establecen los límites y alcances de todo lo que puede medirse a un estado cuántico. Surge a partir de eso la pregunta acerca de qué magnitudes pueden medirse si se dispone de dos copias simultáneas del estado en cuestión. Un resultado conocido al respecto, es que la concurrencia (ver Apéndice A.3.3) del estado es un observable sobre dos copias simultáneas [AM06a]. De manera similar es posible medir la pureza de un estado y la pureza de sus subsistemas.

Lo que veremos a continuación es una teoría general que, al igual que los POVMs, establece los límites y alcances de lo que puede medirse si se dispone de dos copias simultáneas de un estado cuántico.

8.1.1. Medición basada en mapas completamente copositivos

Vamos a considerar una fuente que produce el estado ρ, y que se dispone de algún medio para mantener el estado hasta que otra copia sale de la fuente, resultando en un estado conjunto de la forma

$$\rho^{(A,B)} = \rho \otimes \rho \tag{8.1}$$

donde A y B son etiquetas para designar los dos subsistemas preparados en el mismo estado ρ. Nuestro objetivo es determinar cuáles son los posibles resultados de las mediciones de POVMs sobre el estado $\rho^{(A,B)}$. Para eso necesitaremos la siguiente definición:

Definición 8.1 (Mapas completamente copositivos)**.** *Se dice que un mapa $\mathcal{E}$ es completamente copositivo (CCP) si y sólo si el mapa $\tilde{\mathcal{E}}(\rho) = \mathcal{E}\left(\rho^T\right)$ es completamante positivo. Es decir, un mapa es CCP si su composición con la transposición es CP.*

Ahora sí podemos presentar el siguiente teorema que, similar al de Neumark, define los alcances de la medición con dos copias simultáneas del estado.

Teorema 8.2. *Sean dos sistemas preparados en el mismo estado ρ. Entonces μ puede etiquetar un conjunto de resultados posibles de una medición*

sobre $\rho^{(A,B)} = \rho \otimes \rho$ si y sólo si existe un conjunto de mapas completamente copositivos (CCP) $\{C_\mu\}$ tal que la probabilidad de ocurrencia $Prob(\mu)$ es la fidelidad del mapa C_μ en el estado ρ (es decir, $Prob(\mu) = Tr(\rho\ C_\mu(\rho))$). Los mapas satisfacen la condición $\sum_\mu C_\mu = \mathcal{I}$, donde $\mathcal{I}$ es el mapa para el cual $\mathcal{I}(\rho) = \mathbb{I}$ para todo estado ρ.

Demostración. Lo primero que queremos demostrar es que un POVM formado por los operadores $A_\mu \in \mathcal{B}(\mathcal{H} \otimes \mathcal{H})$ satisface que

$$\mathrm{Tr}\left(\rho \otimes \rho A_\mu\right) = \mathrm{Tr}\left(\rho \tilde{\mathcal{C}}_\mu\left(\rho^T\right)\right) \tag{8.2}$$

donde $\tilde{\mathcal{C}}_\mu\left(\rho^T\right) = \mathcal{C}_\mu(\rho)$. Lo que queremos probar es que los mapas $\tilde{\mathcal{C}}_\mu$ son CP (es decir, los mapas $\mathcal{C}_\mu$ son CCP).

Veamos que, en efecto, si $\tilde{\mathcal{C}}_\mu$ es el canal isomorfo al operador $\frac{1}{D}A_\mu$ via Choi–Jamiołkowski, se cumple la ecuación (8.2) y dado que el isomorfismo relaciona operadores positivos con canales CP, entonces $\tilde{\mathcal{C}}_\mu$ es CP. Usando que $A_\mu = \left(\tilde{\mathcal{C}}_\mu \otimes \mathbb{I}\right)\left(\sum_{i,j} |ii\rangle\langle jj|\right)$ se obtiene que

$$\begin{aligned}
\mathrm{Tr}\left(\rho \otimes \rho A_\mu\right) &= \mathrm{Tr}\left(\rho \otimes \rho\left(\tilde{\mathcal{C}}_\mu \otimes \mathbb{I}\right)\left(\sum_{i,j} |ii\rangle\langle jj|\right)\right) \\
&= \sum_{ij} \mathrm{Tr}\left((\rho \otimes \rho)\left(\tilde{\mathcal{C}}_\mu\left(|i\rangle\langle j|\right) \otimes |i\rangle\langle j|\right)\right) \\
&= \sum_{ijkl} \langle kl|\left((\rho \otimes \rho)\left(\tilde{\mathcal{C}}_\mu\left(|i\rangle\langle j|\right) \otimes |i\rangle\langle j|\right)\right)|kl\rangle \\
&= \sum_{ijkl} \langle k|\,\rho\tilde{\mathcal{C}}_\mu\left(|i\rangle\langle j|\right)|k\rangle\langle l|\,\rho\,|i\rangle\langle j|l\rangle
\end{aligned} \tag{8.3}$$

Sumando sobre l y usando que $\tilde{\mathcal{C}}_\mu$ es $\mathcal{C}_\mu$ compuesto con la transposición, sale que

$$\begin{aligned}
\mathrm{Tr}\left(\rho \otimes \rho A_\mu\right) &= \sum_{ijk} \langle k|\,\rho\mathcal{C}_\mu\left(|j\rangle\langle j|\,\rho\,|i\rangle\langle i|\right)|k\rangle \\
&= \mathrm{Tr}\left(\rho\mathcal{C}_\mu(\rho)\right),
\end{aligned} \tag{8.4}$$

que es el resultado buscado.

Falta probar que la suma de los canales $\mathcal{C}_\mu$ es el canal $\mathcal{I}$. Para eso, observemos que $\sum_\mu A_\mu = \mathbb{I}$. Pero como A_μ están relacionados con $\tilde{\mathcal{C}}_\mu$ con el

isomorfismo de Choi–Jamiołkowski, se tiene que

$$\begin{aligned}\mathbb{I} &= \sum_{\mu} A_{\mu} = \sum_{\mu} \left(\tilde{\mathcal{C}}_{\mu} \otimes \mathbb{I}\right) \left(\sum_{i,j} |ii\rangle \langle jj|\right) \\ &= \sum_{\mu,ij} \left(\tilde{\mathcal{C}}_{\mu} \left(|i\rangle \langle j|\right) \otimes |i\rangle \langle j|\right) \\ &= \sum_{\mu,ij} \left(\mathcal{C}_{\mu} \left(|j\rangle \langle i|\right) \otimes |i\rangle \langle j|\right). \end{aligned} \tag{8.5}$$

Mirando cada elemento de matriz tanto para $\mathbb{I}$ como para la última expresión se obtiene que

$$\begin{aligned}\langle mn| \mathbb{I} |qr\rangle &= \delta_{mq}\delta_{nr} \\ &= \langle m| \sum_{\mu} \mathcal{C}_{\mu} \left(|r\rangle \langle n|\right) |n\rangle \end{aligned} \tag{8.6}$$

Y para que se cumpla esa igualdad la única opción es el canal completamente depolarizante

$$\sum_{\mu} \mathcal{C}_{\mu} (\rho) = \mathcal{I} (\rho) = \mathrm{Tr} (\rho) \mathbb{I}, \tag{8.7}$$

lo que finaliza la demostración. □

El teorema anterior muestra que todo lo que se puede medir cuando se dispone de dos copias simultáneas de un estado cuántico son fidelidades de canales completamente copositivos. El teorema, además, le da un sentido físico a los canales completamente copositivos como aquellos cuya fidelidad está asociada a una medición con copias.

8.2. Poder tomográfico de dos copias

Realizar tomografía completa de un estado es siempre una tarea difícil que, en general, requiere de la medición de $O(D^2)$ parámetros y una gran cantidad de procesamiento clásico (cada coeficiente, típicamente, requiere de un arreglo experimental diferente). En esta sección analizaremos las ventajas de poseer dos copias simultáneas del estado cuando se desea realizar tomografía al mismo. Ese problema puede pensarse como una aplicación del teorema anterior. El uso de copias ya fue analizado en este contexto y fue

mostrado que permite extraer más información que la medición con una sola copia [VLPT99, MP95, LPT98, DBbuE98, CMB04, AM06b]. Aquí mostraremos que la medición con copias reduce enormemente el número de recursos cuánticos necesarios para realizar tomografía *casi* completa, en un sentido que quedará claro en breve.

Supongamos que poseemos dos copias de un estado ρ de un sistema de n qubits. El estado conjunto es $\rho^{(A,B)} = \rho \otimes \rho$. Supongamos que realizamos una medición de Bell a cada par formado por el j–ésimo qubit de cada copia, como se muestra en la Figura 8.1. El estado de cada copia puede escribirse en la base de operadores de Pauli generalizados como

$$\rho = \frac{1}{D} \sum_{q,p} c_{q,p} T(q,p), \tag{8.8}$$

donde $q = (q_1, \ldots, q_n)$ y $p = (p_1, \ldots, p_n)$ son n–uplas binarias que definen a los operadores de Pauli generalizados $T(q,p)$ en la forma

$$T(q,p) = \sigma_x^{q_1} \sigma_z^{p_1} \otimes \ldots \otimes \sigma_x^{q_n} \sigma_z^{p_n} (i)^{\sum_i q_i p_i}. \tag{8.9}$$

Los D^2 coeficientes $c_{q,p}$ que dan la descripción de ρ son todos reales por la hermiticidad de ρ y, debido a la ortogonalidad de los operadores de Pauli generalizados, cumplen que $c_{q,p} = Tr(\rho\, T(q,p))$. Veremos aquí que la obtención de todos los coeficientes $c_{q,p}^2$ con precisión fija puede realizarse con un número de experimentos que sólo depende de la precisión y no del número de qubits n del sistema.

Este resultado sobre tomografía se basa en las siguientes observaciones:

1. El valor medio de $T(q,p) \otimes T(q,p)$ es $\mathrm{Tr}\left(\rho^{(A,B)} T(q,p) \otimes T(q,p)\right) = c_{q,p}^2$.

2. El conjunto de operadores

$$\mathcal{W} = \{T(q,p) \otimes T(q,p), q_i \in \{0,1\}, p_i \in \{0,1\}, i = 1, \ldots, n\} \tag{8.10}$$

   forma un grupo abeliano[1].

3. El conjunto $\mathcal{V} = \{\sigma_{x_i} \otimes \sigma_{x_i}, \sigma_{y_i} \otimes \sigma_{y_i}, i = 1, \ldots, n\}$, donde σ_{x_i} representa el operador σ_x actuando sobre el i–ésimo qubit, es un conjunto conmutativo y genera al conjunto de operadores $\mathcal{W}$.

[1]Debe tenerse en cuenta que dicho conjunto es un grupo conmutativo si se considera el producto entre operadores a menos de una fase.

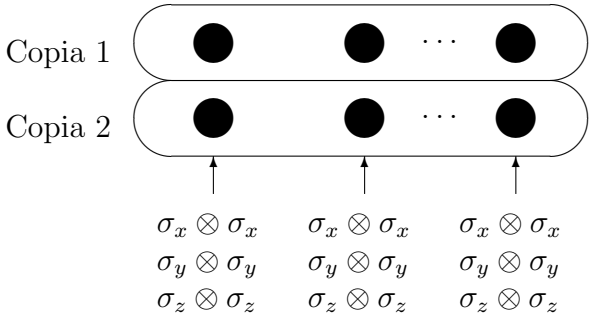

Figura 8.1: Esquema para la tomografía de estados con dos copias. Se realiza una medición de Bell a cada par formado por el j–ésimo qubit de cada copia.

4. Medir los operadores del conjunto $\mathcal{V}$ es equivalente a realizar una medición en la base de Bell en cada qubit, como en la Figura 8.1.

La primera observación nos dice que si medimos los valores medios de los operadores de la forma $T(q,p) \otimes T(q,p)$, obtenemos los cuadrados de los coeficientes de la expansión de la ecuación (8.8). Como todos esos coeficientes son reales, es equivalente a obtenerlos a menos de un signo.

La segunda observación dice más todavía: todos los operadores de la forma $T(q,p) \otimes T(q,p)$ *pueden medirse simultáneamente* ya que el grupo $\mathcal{W}$ es abeliano. Sin embargo, todavía no sabemos cómo medirlo.

La observación siguiente, la tercera, es la más importante y la que merece más explicaciones. Supongamos que sabemos medir los observables asociados a un conjunto de generadores de un grupo, pero estamos interesados en todos los valores de expectación de los operadores del mismo (en este caso, sabemos medir los observables asociados al conjunto $\mathcal{V}$, como muestra la última observación, pero nos interesa reconstruir los valores de expectación de los operadores del grupo $\mathcal{W}$). La manera de proceder es la siguiente: en cada medición tomar nota del autovalor medido a cada generador. El autovalor que se hubiera medido a cada operador del grupo es el producto correspondiente

Resultado de medir A	Resultado de medir B
a_1	b_4
a_3	b_1
a_5	b_0
a_2	b_2
a_7	b_2
a_8	b_1

Tabla 8.1: Resultados de cada medición de dos observables A y B.

de los resultados de la medición de los generadores. De esa forma, guardar registro de cada medición de los generadores, es equivalente a guardar registro del resultado de medir cada operador del grupo generado. Promediando dichos valores, se obtiene el valor medio deseado.

Ejemplo

Veamos un ejemplo. Supongamos que sabemos medir los operadores A y B, con $[A, B] = 0$ y tales que $A\,|a_i, b_i\rangle = a_i\,|a_i, b_i\rangle$ y $B\,|a_i, b_i\rangle = b_i\,|a_i, b_i\rangle$. Pero nos interesa el valor medio de AB. Lo que se debe hacer es medir A y B simultáneamente repetidas veces, y armar una tabla como la 8.1.

Aunque no se haya medido AB, el resultado si se lo hubiera hecho, dado que AB conmuta con A y B, sería el producto de los dos valores de cada fila de la tabla. Así, la estimación del valor medio sería $\langle AB\rangle \simeq \frac{1}{6}\left(a_1b_4 + a_3b_1 + a_5b_0 + a_2b_2 + a_7b_2 + a_8b_1\right)$. De igual forma, midiendo sólo los operadores del conjunto $\mathcal{V}$ se pueden reconstruir todos los operadores de $\mathcal{W}$ que son los cuadrados de los coeficientes de la expansión de ρ

Podemos ver que el número total de experimentos realizados M_E requeridos para obtener todos los coeficientes $c_{q,p}$ a menos de un signo y con precisión fija es independiente del número de qubits y sólo fijado por la precisión requerida. De hecho, cada medición da como resultado un valor ± 1 para $T(q,p) \otimes T(q,p)$. Por lo tanto, después de $\tilde{M}_E$ repeticiones podemos calcular el resultado promedio que notamos como $\tilde{c}^2_{q,p}$. El teorema del límite central implica que la desviación estándar $\sigma_{q,p}$ para $c^2_{q,p}$ satisface $\sigma_{q,p} \leq 1/\sqrt{\tilde{M}_E}$. Por lo tanto, existe un número k tal que $c^2_{q,p} \in \left[\tilde{c}^2_{q,p} - k\sigma_{q,p}; \tilde{c}^2_{q,p} + k\sigma_{q,p}\right]$ con probabilidad p. Esta cota se propaga a $|c_{q,p}|$ dando como resultado que con la misma probabilidad p se lo encontrará en un intervalo centrado en $|\tilde{c}_{q,p}|$

con ancho $\frac{k\sigma_{q,p}}{2\left|\tilde{c}_{q,p}\right|}$. Por otro lado, si se quiere estimar casa $|c_{q,p}|$ mayor que un δ dado con un error ϵ y obtener el valor correcto con probabilidad p, el número de experimentos necesario debe cumplir que

$$\tilde{M}_E \geq k^2/4\delta^2\epsilon^2 \tag{8.11}$$

donde k es elegido para satisfacer $p = \text{erf}\left(\frac{k}{\sqrt{2}}\right)$. Luego, el número de repeticiones necesaria no depende de n sino sólo de la precisión ϵ, del mínimo valor detectable δ y de la probabilidad de éxito p. Éste método es *cuánticamente eficiente* ya que el número de recursos cuánticos (i.e., copias del estado cuántico, mediciones, etc) es constante dada una precisión deseada. Sin embargo, los recursos clásicos para determinar todos los $|c_{q,p}|$ siguen siendo exponenciales en n dado que hay D^2 coeficientes.

8.2.1. Poder tomográfico y CCPMVM

¿Cómo se relacionan esas mediciones tomográficas con los mapas completamente copositivos? Supongamos que armamos una lista con los resultados de las mediciones de Bell locales en dos n–uplas binarias (a, b), donde (a_k, b_k) indica que se encontró el estado $|\beta_{a_k,b_k}\rangle$ en el qubit $k = 1, \ldots, n$ (Los estados de la base de Bell $|\beta_{a_k,b_k}\rangle$ son autoestados de los operadores $\sigma_{x_k} \otimes \sigma_{x_k}$ y $\sigma_{z_k} \otimes \sigma_{z_k}$ con autovalores $(-1)^{a_k}$ y $(-1)^{b_k}$ respectivamente).

La probabilidad de obtener cada par de n–uplas (a, b) es

$$Prob(a, b) = \frac{1}{D^2} \sum_{q,p} (-1)^{aq+bp+qp} c_{q,p}^2. \tag{8.12}$$

Estas probabilidades, de acuerdo con el Teorema 8.2, son fidelidades de canales completamente copositivos. De hecho, es fácil mostrar que pueden obtenerse esas probabilidades como

$$Prob(a, b) = Tr(\rho\ C_{a,b}(\rho)) \tag{8.13}$$

donde los mapas $C_{a,b}$ son

$$C_{a,b}(\rho) = \frac{T(b, a)\rho^T T(b, a)}{D}. \tag{8.14}$$

El carácter completamente copositivo del mapa es evidente ya que es un mapa CP (todo mapa que admite forma de Kraus lo es), compuesto con la transposición.

Es interesante analizar el caso más simple, de un solo qubit, donde los coeficientes $c_{1,0}$, $c_{0,1}$ and $c_{1,1}$ son las tres componentes cartesianas del vector de Bloch $\vec{p}$ que parametriza al estado como una combinación lineal de los tres operadores de Pauli en la forma

$$\rho = \frac{(\mathbb{I} + \vec{p} \cdot \vec{\sigma})}{2}. \tag{8.15}$$

Los mapas $C_{a,b}$ son tales que $C_{a,b}(\rho) = (I + \vec{p}_{a,b} \cdot \vec{\sigma})/4$. Esos operadores son proporcionales a estados con vectores de polarización $\vec{p}_{a,b} = (-1)^a p_x \hat{x} + (-1)^{a+b+1} p_y \hat{y} + (-1)^b p_z \hat{z}$. De esta forma, el mapa $C_{1,1}$ correspondiente al estado singlete $|\beta_{1,1}\rangle$ realiza una inversión en la esfera de Bloch. Los otros tres estados de Bell tienen mapas que corresponden a realizar reflexiones alrededor de los tres planos cartesianos, manteniendo constantes dos componentes del vector de Bloch $\vec{p}$ y cambiando de signo la restante. La suma de esos cuatro mapas da como resultado el mapa completamente depolarizante, como afirma el Teorema CCPMVM 8.2. Las probabilidades de las cuatro mediciones de Bell son, además, cuadráticas en las componentes de $\vec{p}$:

$$Prob(a, b) = \frac{1 + \vec{p} \cdot \vec{p}_{a,b}}{4}. \tag{8.16}$$

Es interesante como esos mapas, que son ejemplos típicos de mapas positivos pero no completamente positivos, aparecen naturalmente en éste contexto.

8.2.2. Comparación con los detectores universales

Los denominados detectores universales de estados fueron introducidos en [DPS04] pero, como mostraremos, son ineficientes para la tomografía de estados. Estos detectores universales no usan copias sino un sistema auxiliar preparado en un estado conocido

$$\rho_0 = \frac{1}{D} \sum_{q,p} c^{(0)}_{q,p} T(q, p). \tag{8.17}$$

Cuando los sistemas (A) y (B) se encuentran en los estados ρ y ρ_0, respectivamente, es fácil mostrar que haciendo mediciones de Bell en todos los pares correspondientes se obtienen como resultados

$$c_{q,p} c^{(0)}_{q,p} = \langle T(q, p) \otimes T(q, p) \rangle_{\rho \otimes \rho_0}. \tag{8.18}$$

Por lo tanto, conociendo el estado ρ_0 (es decir, conociendo los $c^{(0)}_{q,p}$) y midiendo los valores de expectación que aparecen en (8.18), se pueden determinar todos los $c_{q,p}$.

Sin embargo, para que el detector sea universal, el estado ρ_0 debe ser el mismo, independientemente del estado ρ que se desee tomografiar. Eso hace que el método sea ineficiente, ya que se pueden determinar los coeficientes $c_{q,p}$ sólo si el $c^{(0)}_{q,p}$ correspondiente es distinto de cero. Más aún, cuanto menor es el valor de $c^{(0)}_{q,p}$, mayor es la precisión necesaria para la estimación de $\langle T(q,p) \otimes T(q,p) \rangle_{\rho \otimes \rho_0}$.

Dicho eso, consideremos un estado cuyos $\left| c^{(0)}_{q,p} \right|$ son máximos. Ese es el caso para los estados estabilizadores (autoestados comunes de un conjunto de D operadores de Pauli $T(q,p)_S$). Para esos estados hay D coeficientes no nulos $c^{(0)}_{q,p_S}$ que toman valores ± 1. Para cada ρ_0, este tipo de detector puede utilizarse únicamente para estimar D coeficientes $c_{q,p}$, sin obtener ninguna información sobre los demás $D^2 - D$.

Otra opción sería usar un estado ρ_0 tal que todos los coeficientes $c^{(0)}_{q,p}$ sean distintos de cero.. El problema con un ρ_0 tan no sesgado es que todos los $c^{(0)}_{q,p}$ son exponencialmente chicos[2]. Luego, si usamos (8.18) para estimar todos los coeficientes de ρ con precisión fija, necesitamos una precisión exponencialmente alta para el valor de expectación de cada $\langle T(q,p) \otimes T(q,p) \rangle$. Por lo tanto, ese método es ineficiente para tomografía completa.

En estos términos puede entenderse la ventaja del método aquí presentado de la siguiente forma: Al elegir la ancilla en el mismo estado que el sistema (medir con copias es equivalente a elegir $\rho_0 = \rho$), se está ponderando más a los coeficientes más grandes, permitiendo medirlos eficientemente.

8.2.3. Medición de pureza y concurrencia

La pureza y la concurrencia de un estado son magnitudes fundamentales para la información cuántica. La primera es una medida de qué tan cerca está un estado de un estado puro, y la segunda es una medida del entrelazamiento bipartito de todas las posibles biparticiones del estado. Ya en [AM06a] habían mostrado que la concurrencia era un observable factorizable en dos qubits. Aquí extenderemos ese resultado y mostraremos que el esquema de

[2]Eso se debe a que la pureza del estado es a lo sumo 1. Por lo tanto $\mathrm{Tr}\left(\rho_0^2\right) = \frac{1}{D} \sum_{p,q} c^{(0)2}_{q,p} = 1$, en el mejor caso. De ahí sale que $c^{(0)2}_{q,p} = \frac{1}{D}$

la Figura 8.1 permite obtener tanto la pureza como la concurrencia de un estado cuántico.

Pureza

Un resultado importante para la obtención de la pureza con dos copias, es que la pureza puede obtenerse como el valor medio del operador de intercambio S. Es decir

$$\mathrm{Tr}\left(\rho^2\right) = \mathrm{Tr}\left(\rho \otimes \rho S\right) \tag{8.19}$$

donde $S\left|\psi\right\rangle\left|\phi\right\rangle = \left|\phi\right\rangle\left|\psi\right\rangle$.

Además, el operador de intercambio es factorizable como $S = \bigotimes_i S_i$, donde S_i es el operador de intercambio del i–ésimo qubit de la primera copia con el i–ésimo de la segunda.

De esta forma, al realizar la medición de Bell en cada par como en la Figura 8.1 se contará cada medición de la siguiente forma:

- Si la cantidad de pares en el estado singlete es par, el experimento cuenta como $+1$.
- Si la cantidad de pares en el estado singlete es impar, el experimento cuenta como -1.

Así, la pureza será el promedio de todos esos valores.

Un circuito para medir pureza es el mostrado por Ekert [EAO+02] y que se observa en la Figura 8.2. La ventaja del esquema de la Figura 8.1 es que la medición se realiza de manera factorizada, sin la necesidad realizar operaciones en todos los qubits simultáneamente.

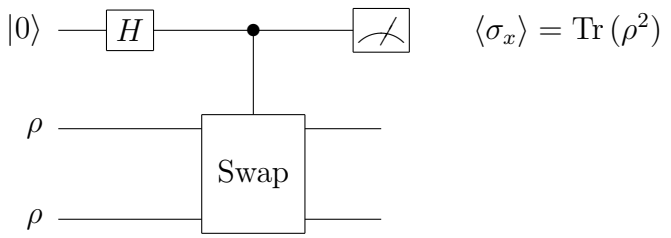

Figura 8.2: Circuito cuántico para la determinación de la pureza de un estado ρ.

Concurrencia

La concurrencia está asociada al entrelazamiento bipartito entre todas las biparticiones posibles. En nuestro caso, se refiere a todas las biparticiones de los n qubits del sistema.

Para un estado puro n–partito $|\Psi\rangle$, la concurrencia $\mathcal{K}(\Psi)$ se define como

$$\mathcal{K}(\Psi) = 2^{1-\frac{n}{2}} \sqrt{(2^n - 2) - \sum_I \mathrm{Tr}\rho_{\Psi_I}^2} \tag{8.20}$$

donde el índice I recorre todas las biparticiones no triviales, y ρ_{Ψ_I} es el operador densidad reducido correspondiente a la primera parte de la bipartición I.

Como medida de entrelazamiento, la concurrencia tiene las siguientes propiedades:

1. Es positiva: $\mathcal{K}(\Psi) \geq 0$.
2. Si $|\Psi\rangle$ es n–separable entonces $\mathcal{K}(\Psi) = 0$.
3. Si uno de los n subsistemas es separable del resto, entonces $\mathcal{K}(\Psi) = \mathcal{K}_{n-1}(\Psi_{n-1})$.

A partir de la definición de la ecuación (8.20), no es dificil probar que

$$\mathcal{K}(\Psi) = 2\sqrt{1 - p_+^n} \tag{8.21}$$

donde p_+^n es la probabilidad de encontrar a los n subsistemas de una copia un estado simétrico frente al intercambio con el subsistema correspondiente de la otra. Es decir, en el esquema de la Figura 8.1, es la probabilidad de encontrar a todos los pares en algún estado del triplete.

Ese esquema posee la virtud de ser facilmente implementable, ya que todas las mediciones son locales en cada subsistema. Sin embargo, al igual que para la pureza, existe un circuito para realizar esa medición. En la Figura 8.3 se observa dicho circuito.

Veamos que el circuito de la Figura 8.3 funciona. El estado inicial que entra al circuito es

$$|\varsigma_0\rangle = \frac{1}{\sqrt{2^N}} |0\rangle \otimes \sum_{\vec{J}} \left|\vec{J}\right\rangle \otimes |\Psi\rangle \otimes |\Psi\rangle \tag{8.22}$$

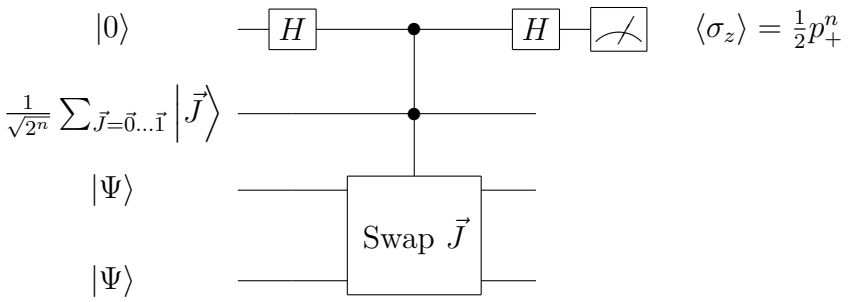

Figura 8.3: Circuito cuántico para la determinación de la concurrencia de un estado $|\Psi\rangle$. El vector binario $\vec{J}$ controla sobre qué qubits debe realizar el intercambio la compuerta Swap.

Luego de la aplicación de la compuerta de Swap controlada se obtiene el estado

$$|\varsigma_1\rangle = \frac{1}{\sqrt{2^{n+1}}}\left[|1\rangle\otimes\sum_{\vec{J}}\left|\vec{J}\right\rangle\otimes\vec{S}^{\vec{J}}\left(|\Psi\rangle\otimes|\Psi\rangle\right)+ + |0\rangle\otimes\sum_{\vec{J}}\left|\vec{J}\right\rangle\otimes|\Psi\rangle\otimes|\Psi\rangle\right] \tag{8.23}$$

La aplicación de la compuerta de Hadamard previa a la medición da

$$|\varsigma_2\rangle = \frac{1}{\sqrt{2^{n+2}}}\left[|0\rangle\otimes\sum_{\vec{J}}\left|\vec{J}\right\rangle\otimes\left(1+\vec{S}^{\vec{J}}\right)|\Psi\rangle\otimes|\Psi\rangle+ + |1\rangle\otimes\sum_{\vec{J}}\left|\vec{J}\right\rangle\otimes\left(1-\vec{S}^{\vec{J}}\right)|\Psi\rangle\otimes|\Psi\rangle\right] \tag{8.24}$$

Finalmente, la medición de σ_z da el resultado buscado:

$$\begin{aligned}
\langle\sigma_z\rangle &= \frac{1}{2^{n+1}}\sum_{\vec{J}}\langle\Psi|\otimes\langle\Psi|\,\vec{S}^{\vec{J}}\,|\Psi\rangle\otimes|\Psi\rangle \\
\langle\sigma_z\rangle &= \frac{1}{2^{n+1}}\langle\Psi|\otimes\langle\Psi|\,(1+S_1)\ldots(1+S_N)\,|\Psi\rangle\otimes|\Psi\rangle \\
\langle\sigma_z\rangle &= \frac{1}{2}p_+^n
\end{aligned} \tag{8.25}$$

8.3. Aplicación a la tomografía de procesos

Uno podría pensar qué ventaja puede tenerse al realizar tomografía de procesos sabiendo realizar mediciones de estados con copias. Como veremos aquí, la posibilidad de medir sobre copias simultáneas de estados permitirá extraer, con mediciones compatibles, mucha información sobre los procesos cuánticos. Para eso veremos qué información puede extraerse si se dispone de dos copias simultáneas del estado isomorfo al canal en cuestión.

Para estudiar ese problema, primero veremos un teorema que establece la relación entre la matriz χ de un canal y la representación matricial del estado isomorfo. Ese teorema nos permitirá, luego, ver qué información se puede extraer al disponer de dos copias simultáneas de dicho estado.

Teorema 8.3. *Sea* $\mathcal{S}=\{E_m\in\mathcal{B}(\mathcal{H}),m=0,\ldots,D^2-1\}$ *una base de* $\mathcal{B}(\mathcal{H})$. *Entonces existe una base* $\mathcal{Q}=\{|\psi_m\rangle\in\mathcal{H}\otimes\mathcal{H},m=0,\ldots,D^2-1\}$ *de* $\mathcal{H}\otimes\mathcal{H}$ *tal que para todo canal* $\mathcal{E}(\rho)=\sum_{ab}\chi_{ab}E_a\rho E_b^\dagger$ *su operador isomorfo via Choi–Jamiołkowski es* $\mu=\sum_{ab}\chi_{ab}\,|\psi_a\rangle\langle\psi_b|$.

Más aún, el producto interno entre los operadores de la base $\mathcal{S}$ *y los vectores de la base* $\mathcal{Q}$ *se relaciona mediante*

$$\langle\psi_a|\psi_b\rangle=\frac{1}{D}\mathrm{Tr}\left(E_a^\dagger E_b\right) \tag{8.26}$$

Es decir, para toda elección de una base del espacio de operadores, existe una base de $\mathcal{H}\otimes\mathcal{H}$ tal que la representación matricial del canal y la de su estado isomorfo en esa base es la misma. Veamos la demostración que, además, nos dirá quién es esa base de $\mathcal{H}\otimes\mathcal{H}$.

Demostración. Consideremos el estado μ isomorfo al canal $\mathcal{E}$:

$$\mu=(\mathcal{E}\otimes\mathbb{I})\,(|I\rangle\langle I|) \tag{8.27}$$

donde $|I\rangle = \frac{1}{\sqrt{d}} \sum_i |ii\rangle$ es el estado máximamente entrelazado.

Reemplazando $\mathcal{E}$ por su representación χ en la base $\mathcal{S}$ se obtiene

$$\mu = \sum_{ab} \left(\chi_{ab} E_a \otimes \mathbb{I} \, |I\rangle \langle I| \, E_b^\dagger \otimes \mathbb{I} \right) \tag{8.28}$$

Sea $|\psi_m\rangle = E_m \otimes \mathbb{I} \, |I\rangle$. Luego

$$\mu = \sum_{ab} \chi_{ab} \, |\psi_a\rangle \langle \psi_b| \tag{8.29}$$

es el resultado buscado.

Falta ver qué pasa con los productos internos. Veamos:

$$\langle \psi_a | \psi_b \rangle = \langle I| \left(E_a^\dagger \otimes \mathbb{I} \right) (E_b \otimes \mathbb{I}) \, |I\rangle \, . \tag{8.30}$$

Escribiendo $|I\rangle$ explícitamente en una base ortonormal cualquiera se obtiene

$$\begin{aligned} \langle \psi_a | \psi_b \rangle &= \sum_{ij} \langle ii| \left(E_a^\dagger \otimes \mathbb{I} \right) (E_b \otimes \mathbb{I}) \, |jj\rangle \, . \\ &= \frac{1}{D} \sum_{ij} \langle i| \, E_a^\dagger E_b \, |j\rangle \langle i|j\rangle \\ &= \frac{1}{D} \mathrm{Tr} \left(E_a^\dagger E_b \right) \end{aligned} \tag{8.31}$$

Y eso completa la demostración. □

Es decir, si el canal es tal que

$$\mathcal{E}(\rho) = \sum_{mn} \chi_{mn} E_m \rho E_n^\dagger, \tag{8.32}$$

entonces el estado isomorfo via Choi–Jamiołkowski se escribe como

$$\rho_{\mathcal{E}} = \sum_{mn} \chi_{mn} \, |\alpha_m\rangle \langle \alpha_n| \, . \tag{8.33}$$

Supongamos ahora que tenemos dos copias simultáneas del estado $\rho_{\mathcal{E}}$. El estado conjunto es

$$\rho_{\mathcal{E}}^{\otimes 2} = \sum_{mnm'n'} \chi_{mn} \chi_{m'n'} \, |\alpha_m \alpha_{m'}\rangle \langle \alpha_n \alpha_{n'}| \, . \tag{8.34}$$

Consideremos ahora la siguiente familia de observables:

$$Q_{ij} = |\alpha_i \alpha_j\rangle \langle \alpha_j \alpha_i| + |\alpha_j \alpha_i\rangle \langle \alpha_i \alpha_j| \, . \tag{8.35}$$

La primera observación que se puede hacer es que todos los observables distintos (recorriendo i y j) de esa familia conmutan. Por lo tanto, se los puede medir simultáneamente. La segunda observación es respecto del valor medio en el estado $\rho_{\mathcal{E}}^{\otimes 2}$. Se tiene que

$$\mathrm{Tr}\left(\rho_{\mathcal{E}}^{\otimes 2} Q_{ij}\right) = 2\left|\chi_{ij}\right|^2. \tag{8.36}$$

Es decir, los módulos cuadrados de *todos* los coeficientes de la matriz χ se pueden medir simultáneamente con copias. Es fácil ver que sin copias y midiendo en la base $\{|\alpha_i\rangle\}$ se obtienen todos los elementos diagonales. Lo novedoso, al tener dos copias simultáneas, es que se obtienen los módulos no sólo de los coeficientes diagonales sino de todos al mismo tiempo.

Este resultado puede parecer poco sorprendente ya que, como vimos en la Sección 8.2.2 sobre detectores universales, se puede hacer tomografía completa –aunque ineficiente– con un POVM. Sin embargo, los observables Q_{ij}, corresponden a realizar una medición proyectiva en una base. En efecto, los autoestados de Q_{ij} son $|\alpha_{ij}\pm\rangle = \frac{1}{\sqrt{2}}\left(|\alpha_i\alpha_j\rangle \pm |\alpha_j\alpha_i\rangle\right)$. Todos esos estados, en conjunto con los $|\alpha_i\alpha_i\rangle$ forman una base de $\mathcal{H}\otimes\mathcal{H}$ que llamaremos $\mathcal{Q}$.

Si llamamos p_{ij}^{+} a la probabilidad de encontrar el estado en $|\alpha_{ij}+\rangle$ y p_{ij}^{-} a la probabilidad de encontrar el estado en $|\alpha_{ij}-\rangle$, entonces se cumple que

$$\mathrm{Tr}\left(\rho_{\mathcal{E}}^{\otimes 2} Q_{ij}\right) = p_{ij}^{+} - p_{ij}^{-} = 2\left|\chi_{ij}\right|^2. \tag{8.37}$$

Es decir, con una medición proyectiva sobre las dos copias en la base $\mathcal{Q}$, se obtienen todos coeficientes $\left|\chi_{ij}\right|^2$, dando información no sólo sobre la diagonal de la matriz χ de $\mathcal{E}$ sino también sobre los elementos no diagonales.

8.4. Conclusiones parciales

Hemos visto en este capítulo que si se dispone de dos copias simultáneas de un estado cuántico, la información que se puede obtener mediante la medición de un POVM al sistema compuesto es equivalente a medir las fidelidades de un conjunto de canales completamente copositivos. Ese resultado, además de establecer los límites y alcances de la medición con copias simultáneas, permite darle un significado físico a los canales CCP.

Luego vimos que con dos copias se puede realizar tomografía casi completa del estado cuántico de un sistema (faltando sólo los signos que acompañan a los coeficientes de la expansión en operadores de Pauli generalizados) con

recursos cuánticos que no dependen del tamaño del sistema sino sólo de la precisión deseada. Además, el método de tomografía provee eficientemente información muy valiosa sobre el sistema como ser la pureza del mismo, de sus subsistemas y la concurrencia.

Por último, estudiamos cómo podía aplicarse la teoría de la medición con copias a la tomografía de procesos. Valiéndonos nuevamente del isomorfismo de Choi–Jamiołkowski vimos que es posible determinar simultáneamente *todos* los módulos de los coeficientes de la matriz χ, tanto los diagonales como los no diagonales.

Capítulo 9

Tomografía selectiva y eficiente de estados cuánticos

> Dios engendró un huevo, el huevo engendró la espada, la espada engendró a David, David engendró el púrpura, el púrpura engendró al duque, el duque engendró al marqués, el marqués engendró al conde, que soy yo.
>
> *El Alienista*
> *Machado de Assis*

En este capítulo presentaremos un método operacional para realizar la tomografía de estados mostrada en la Sección 7.1.3. Uno de los problemas que se presentan al realizar tomografía de estados en una base $\mathcal{Q}$ de $\mathcal{H}$ es que se deben preparar combinaciones lineales de dos estados de la base $\mathcal{Q}$. En general, aún si preparar estados de una base resulta ser una tarea eficiente, preparar combinaciones lineales de los mismos puede no serlo. Veremos a continuación que sabiendo preparar sólo los estados de la base $\mathcal{Q}$, podemos realizar tomografía selectiva y eficiente, tanto diagonal como no diagonal, de un estado arbitrario.

Luego mostraremos que ese método, combinado con el isomorfismo de Choi–Jamiołkowski, resulta en un nuevo método de tomografía eficiente y selectiva de procesos que, aunque no es más que una aplicación del método AAPT (ver Sección 2.3.1), permite la obtención directa de los elementos diagonales y no diagonales de la matriz χ. Y a diferencia del presentado en

el Capítulo 3, no requiere aumentar la cantidad de arreglos experimentales para aumentar la precisión, sino simplemente medir un mayor tiempo.

9.1. Tomografía selectiva, eficiente y directa de estados cuánticos

Supongamos que se desea medir eficiente y selectivamente la descripción de la matriz densidad de un estado en una base ortonormal $\mathcal{Q} = \{|\psi_a\rangle, a = 1, \ldots, d\}$. Esto es, medir los elementos de la matriz α definida como

$$\rho = \sum_{ab} \alpha_{ab} |\psi_a\rangle \langle\psi_b| . \tag{9.1}$$

Utilizaremos una suposición adicional que servirá tanto para analizar la eficiencia del método como para la implementación del mismo, que es que todos los estados de la base $\mathcal{Q}$ pueden prepararse eficientemente a partir de un estado $|0\rangle$ como

$$|\psi_a\rangle = V_a |0\rangle , \tag{9.2}$$

con V_a un operador unitario que se puede implementar eficientemente, y que además, los V_a se pueden utilizar de manera controlada.

Para la determinación de los coeficientes diagonales, utilizaremos un resultado de Ekert y colaboradores [EAO+02]. En ese trabajo, muestran que la traza del producto de dos operadores densidad ρ_1 y ρ_2 se puede obtener a partir de una operación de intercambio controlada, como se muestra en el circuito de la Figura 9.1.

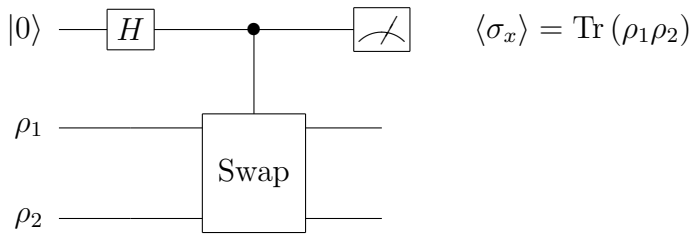

Figura 9.1: Circuito cuántico para la determinación de la traza del producto de dos operadores densidad ρ_1 y ρ_2.

Puesto que la base $\mathcal{Q}$ es ortonormal, los coeficientes diagonales son tales

que

$$\alpha_{aa} = \mathrm{Tr}\left(\rho \left|\psi_a\right\rangle \left\langle\psi_a\right|\right). \tag{9.3}$$

Por lo tanto, el circuito para medición de coeficientes diagonales queda como se muestra en la Figura 9.2.

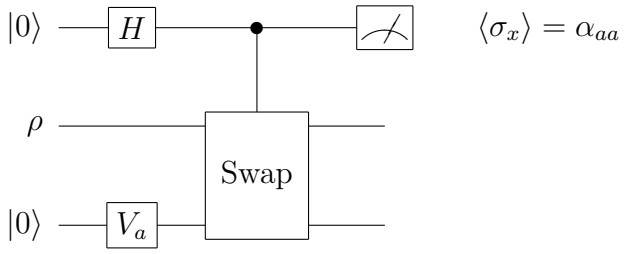

Figura 9.2: Circuito cuántico para la determinación de los elementos diagonales de la matriz de ρ en la base $\mathcal{Q}$.

Vale aclarar que el método es eficiente siempre y cuando la aplicación de la compuerta V_a sea eficiente. Además, el método es *directo* en el sentido en que el valor medio que se mide a la salida es exactamente el valor del coeficiente que se desea medir.

Para los elementos no diagonales, uno puede estar tentado de hacer actuar el operador $V_a \pm V_b$ sobre el tercer registro de la Figura 9.2. Sin embargo, que V_a y V_b se puedan implementar eficientemente no garantiza que lo mismo ocurra para las combinaciones lineales de ambos. Es más, ni siquiera garantiza que dichas combinaciones sean un múltiplo de una operación unitaria, por lo que, en principio, ni siquiera podrían implementarse de manera ineficiente.

Sin embargo, no es esta la primera vez que nos topamos con ese problema, y la solución resulta ser exactamente la misma que la que vimos en el Capítulo 4. En efecto, la familia de estados contra los que se quiere comparar a ρ via el circuito de swap controlado son de la forma

$$\frac{1}{2}\left(\left|\psi_a\right\rangle \pm \left|\psi_b\right\rangle\right)\left(\left\langle\psi_a\right| \pm \left\langle\psi_b\right|\right) \tag{9.4}$$

para medir la parte real o con una fase adicional en el caso de querer medir la parte imaginaria de χ_{ab}. Es interesante notar que de los cuatro sumandos de la ecuación 9.4, sólo los no diagonales aportan a la medición de los coeficientes no diagonales. Aplicando un V_a controlado por una ancilla y un V_b controlado por la ancilla negada y midiendo σ_x (σ_y para la parte imaginaria) se obtiene el resultado deseado, como se muestra en la Figura 9.3. Puede probarse de

manera directa que $\langle \sigma_{x_1} \otimes \sigma_{x_4} \rangle = \mathrm{Re}\,(\alpha_{ab})$ y $\langle \sigma_{x_1} \otimes \sigma_{y_4} \rangle = \mathrm{Im}\,(\alpha_{ab})$. Es decir, medimos selectivamente los coeficientes no diagonales, de manera directa, y tan eficientemente como la aplicación controlada de los operadores V_a y V_b.

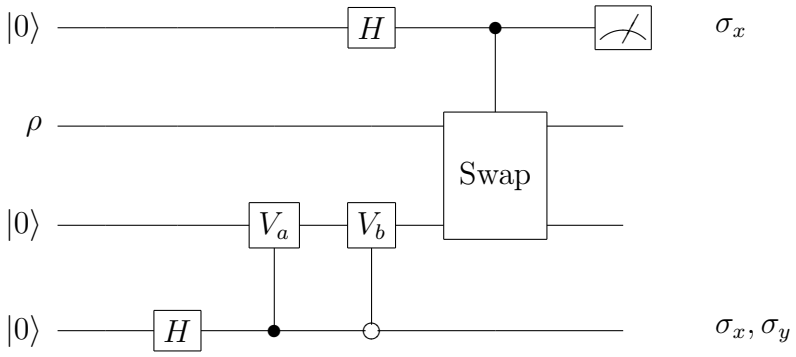

Figura 9.3: Circuito cuántico para la determinación de los elementos no diagonales de la matriz de ρ en la base $\mathcal{Q}$.

Vale la pena recalcar que no necesitamos saber preparar los estados que son combinación lineal de los de la base sino sólo los de la base de manera controlada.

9.2. Aplicación a la tomografía de procesos

Ese método de tomografía de estados puede adaptarse fácilmente a la tomografía de procesos. La manera de hacerlo es recordar que existe el isomorfismo de Choi–Jamiołkowski (ver Apéndice A.7) que da una relación uno a uno entre canales cuánticos $\mathcal{E} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ y operadores de $\mathcal{B}(\mathcal{H} \otimes \mathcal{H})$. Dicha observación no es nueva, sino que estaba ya presente en los métodos de AAPT y DCQD (ver secciones 2.3.1 y 2.3.2). En ese método, la medición de los coeficientes no diagonales requería la inversión una matriz que, en el peor caso, era exponencialmente grande.

Ese problema tiene su origen en que la matriz χ del canal, al transformarlo en un estado via el isomorfismo de Choi–Jamiołkowski se mezcla entre los coeficientes del estado. El teorema 8.3 muestra mejor el rol de los coeficientes de la matriz χ en su estado isomorfo. En efecto como mencionamos en el Capítulo 8, para toda elección de una base del espacio de operadores $\{E_m\}$, existe una base $\mathcal{Q} = \{|\psi_m\rangle = E_m \otimes \mathbb{I}\,|I\rangle\,, E_m \in \mathcal{S}\}$ de $\mathcal{H} \otimes \mathcal{H}$ tal que la

representación matricial del canal y la de su estado isomorfo en esa base es la misma.

El algoritmo para realizar tomografía selectiva, eficiente y directa de procesos cuánticos es ahora claro: se debe realizar tomografía al estado isomorfo al canal en cuestión en la base $\mathcal{Q}$.

De esa forma, el circuito completo para realizar tomografía selectiva, eficiente y directa de procesos cuánticos es el mostrado en la Figura 9.4, donde se nota $\tilde{E}_m = E_m \otimes \mathbb{I}$ y $\tilde{\mathcal{E}} = \mathcal{E} \otimes \mathbb{I}$.

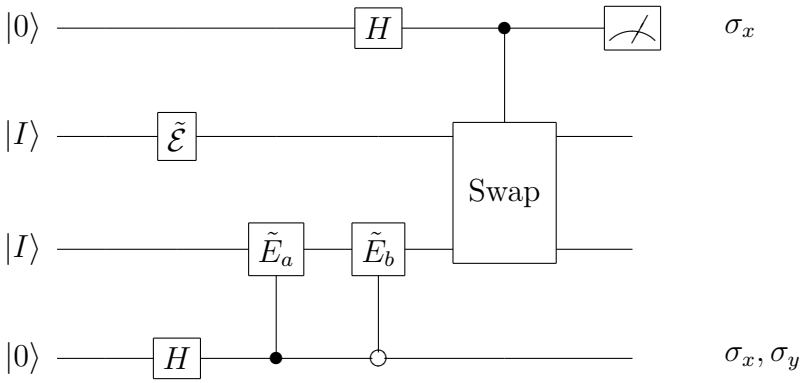

Figura 9.4: Circuito cuántico para la tomografía de procesos cuánticos selectiva, eficiente y directa.

Vale destacar algunos detalles. La tomografía es selectiva ya que la elección de los operadores E_a y E_b de la Figura 9.4 determina el coeficiente χ_{ab} que se va a medir. Es directa porque el resultado de la medición es el valor que se busca en la forma

$$\langle \sigma_{x_1} \otimes \sigma_{x_4} \rangle = \mathrm{Re}\,(\chi_{ab}) \tag{9.5}$$

$$\langle \sigma_{x_1} \otimes \sigma_{y_4} \rangle = \mathrm{Im}\,(\chi_{ab}) \tag{9.6}$$

En cuanto a la eficiencia del método valen algunas aclaraciones. Primero, se asume que los operadores controlados se pueden implementar eficientemente. Además de eso, el sistema utiliza $O\,(n)$ qubits auxiliares, y $O\,(n)$ operaciones cuánticas de uno y dos qubits, principalmente utilizadas para la preparación de los estados máximamente entrelazados.

En cuanto a la cantidad de veces que debe ejecutarse el algoritmo hasta que el valor medio aproxime el resultado exacto, basta notar que cada experimento puede dar como resultado $+1$ o -1, correspondientes a los autovalores de los operadores que se miden. La desviación estándar de la muestra

está acotada por $\sigma \leq 1$. Por el teorema del límite central, si se toman de a M experimentos[1], se tiene que la distribución de los resultados aproxima a una distribución normal de desviación $\tilde{\sigma} \leq \frac{1}{\sqrt{M}}$.

Utilizando nuevamente una cota de Chernoff, se obtiene que si se desea obtener con probabiidad P un error menor a ϵ, la cantidad de experimentos necesaria es:

$$M \geq \frac{2 \ln\left(\frac{2}{p}\right)}{\epsilon^2}. \tag{9.7}$$

Un punto importante a resaltar es que, mientras que en SEQPT (ver Capítulo 3) la cantidad de experimentos estaba asociada a un número igual de arreglos experimentales (en ese contexto, un experimento adicional implicaba la elección de un estado más del 2–diseño y su correspondiente preparación y medición), en este esquema la cantidad de experimentos es simplemente realizar más mediciones en el mismo sistema. Para una implementación fotónica eso es apenas capturar una mayor cantidad de coincidencias en los detectores, es decir, dejar más tiempo encendido el sistema.

9.3. Circuitos reducidos

Existe una forma de reducir el circtuito de tomografía de estados de la Figura 9.3 de manera de requerir la mitad de los recursos, reduciendo también en $2n + 1$ la cantidad de qubits auxiliares del circuito de la Figura 9.4. La reducción se basa en una observación simple: puesto que el swap controlado permite medir la traza del producto de los dos canales que permuta, son equivalentes los dos circuitos cuánticos de la Figura 9.5.

El segundo circuito, en el caso en que ρ_2 es un estado puro se interpreta como la probabilidad de medir el estado ρ_2 habiendo entrado con el estado ρ_1.

Eso permite construir un circuito equivalente al de la Figura 9.3, como se ilustra en la Figura 9.6.

Para la tomografía de procesos, esa misma reducción sigue siendo válida permitiendo eliminar la primera ancilla del circuito de la Figura 9.4 y convertir las $2n$ ancillas del segundo estado $|I\rangle$ en una medición sobre el primer

[1]Se entiende por un experimento a un click de los detectores correspondiente a haber medido un valor ± 1 al operador $\sigma_{x_1} \otimes \sigma_{x_4}$ o $\sigma_{x_1} \otimes \sigma_{y_4}$.

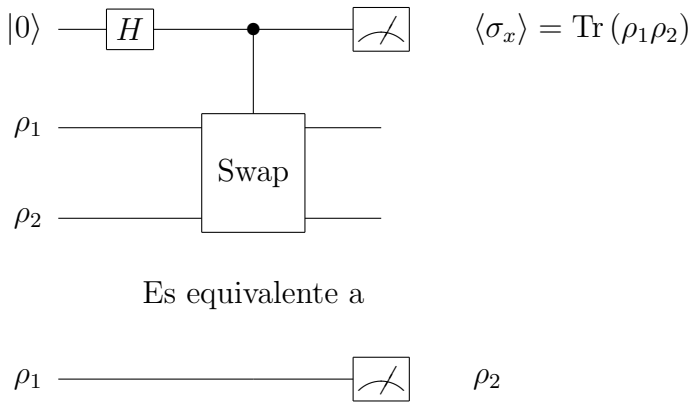

Figura 9.5: Circuitos cuánticos equivalentes para la determinación de la traza del producto de dos operadores densidad ρ_1 y ρ_2.

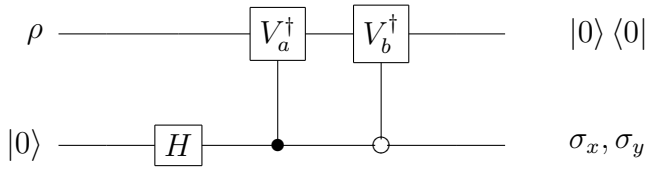

Figura 9.6: Circuito reducido para la tomografía de estados cuánticos selectiva, eficiente y directa.

estado $|I\rangle$. Dicha medición necesita de $O(n)$ operaciones de uno y dos qubits, pero son las mismas que se ahorran en la preparación del estado $|I\rangle$ que se elimina. Por lo tanto, se mantiene la eficiencia del método ahorrándose $2n+1$ valiosos sistemas cuánticos auxiliares. El circuito final puede observarse en la Figura 9.7.

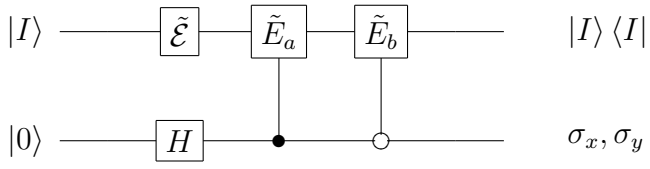

Figura 9.7: Circuito reducido para la tomografía de procesos cuánticos selectiva, eficiente y directa.

Puede parecer que el circuito es muy parecido al del Capítulo 3, pero eso es apenas de aspecto. En ese capítulo el promedio era realizado mediante el

muestreo de estados del 2–diseño. En este circuito no hace falta ningún muestreo. El promedio es obtenido de manera directa a través de las correlaciones entre las dos partes del estado $|I\rangle$. La medición es, en ese sentido, directa. Este método puede entenderse como un híbrido entre DCQD y SEQPT.

9.4. Conclusiones parciales

En este capítulo presentamos un circuito para realizar tomografía selectiva, eficiente y directa de estados cuánticos. Dicho esquema permite la medición de cualquier coeficiente de la representación matricial de un estado cuántico. El único requisito del método es que se necesita saber preparar todos los estados de la base en la que se desea hacer la tomografía, y que dicha preparación debe poder hacerse de manera controlada y eficiente.

Luego recordamos que el isomorfismo de Choi–Jamiołkowski transforma un canal con una matriz χ dada en un estado cuya representación matricial es la misma matriz χ, siempre y cuando se elija adecuadamente la base en la que se lo representa. Esa observación, en conjunto con el esquema de tomografía de estados presentado, permitió la construcción de un nuevo esquema de tomografía de procesos cuánticos selectivo, eficiente y directo. La ventaja de éste método frente a los anteriores es que permite medir cada coeficiente de manera directa y, a diferencia del SEQPT, requerir mayor precisión no aumenta la cantidad de arreglos experimentales necesaria. Como contrapartida, el esquema requiere $O(n)$ qubits auxiliares.

Por último, vimos como reducir la cantidad de recursos auxiliares de $2n+2$ a $n+1$, permitiendo que la tomografía de procesos se realice con casi la misma cantidad de recursos que la DCQD mostrada en la Sección 2.3.2, pero de manera directa, es decir, sin necesidad de invertir ninguna matriz incluso para los elementos no diagonales.

Capítulo 10

Conclusiones generales

alguna vez
alguna vez tal vez
me iré sin quedarme
me iré como quien se va

Árbol de Diana
Alejandra Pizarnik

Durante esta tesis hemos estudiado dos herramientas fundamentales para toda aplicación relacionada con información cuántica: la tomografía de procesos cuánticos y la tomografía de estados cuánticos. Ambas poseen una íntima relación debida a la relación biunívoca entre procesos cuánticos y estados dada por el isomorfismo de Choi–Jamiołkowski.

En la primera parte de la tesis, estudiamos la tomografía de procesos. Luego de dar una introducción a la misma en el Capítulo 2 entramos de lleno en los métodos desarrollados en el marco de la presente.

En el Capítulo 3 presentamos un método de tomografía selectiva y eficiente de procesos. El mismo, permite medir coeficientes individuales de la matriz χ (de ahí su *selectividad*) empleando recursos polinomiales en la cantidad de qubits del sistema (de ahí su *eficiencia*). Para dicha tarea, uno de los principales ingredientes son los 2–diseños de estados, que permiten, realizando un promedio sobre un conjunto finito de estados, obtener la fidelidad promedio de un canal. Un muestreo aleatorio sobre esos estados resulta suficiente para una estimación eficiente. Además, para la medición de coeficientes no diagonales, el método se vale de un qubit auxiliar.

Luego, en el Capítulo 4 presentamos una modificación al método anterior que permite obtener la misma información pero sin necesidad de una ancilla. Para conseguir eso reinterpretamos el uso de la ancilla en el método anterior como la preparación de estados y encontramos circuitos eficientes para construir los mismos estados sin necesidad de ancillas. Ambos protocolos, con y sin ancilla, fueron llevados al laboratorio en el marco de la tesis doctoral de Christian Schmiegelow, como se muestra en el Capítulo 5. El último de ellos permitió una colaboración cercana en lo que refiere a los detalles experimentales (convertir elementos matemáticos abstractos en ángulos de láminas de onda y fases de interferómetros) y al análisis de los datos obtenidos.

En el Capítulo 6, desarrollado en colaboración con Cecilia López y David Cory, vimos que algunos de los métodos presentados anteriormente podían interpretarse como parte de una familia de métodos basados en la transformación de twirl y estudiamos para esos métodos sus ventajas y desventajas de unos frente a otros.

La segunda parte de esta tesis se centró en el estudio de la tomografía de estados, siempre con una visión retrospectiva a la tomografía de procesos.

Comenzamos por dar una introducción a la tomografía de estados cuánticos en el Capítulo 7. Luego, en el Capítulo 8 introdujimos una teoría general de la medición cuando se dispone de dos copias simultáneas del sistema a medir. Dicha teoría mostró ser muy poderosa para la tomografía de estados, permitiendo extraer más información que la medición de los estados por separado. Luego, vimos cómo aplicar dicha teoría a la tomografía de procesos, y como eso nos permitía, mediante la utilización de dos copias del estado isomorfo al proceso estudiado, extraer mucha información simultánea sobre el canal.

Por último, en el Capítulo 9, como realizar tomografía selectiva y eficiente de estados. Ese algoritmo es un pariente muy cercano al de SEQPT, pero para estados. Vimos que aplicándolo debidamente al estado isomorfo a un canal, se podía realizar tomografía selectiva y eficiente de procesos de manera directa. Es decir, sin necesidad de promediar sobre 2–diseños. Ese método de tomografía de procesos, si bien similar conceptualmente al de tomografía de procesos asistida por ancilla, le saca una ventaja exponencial a la hora de la medición de coeficientes aislados.

Parte III

Apéndices

Apéndice A

Generalidades sobre mecánica cuántica

La teoría cuántica de la información se ha tornado cada vez un área más interdisciplinaria. Hoy día hay gente proveniente de la matemática, de las ciencias de la computación y de la biología haciendo distintos abordajes al área.

Aunque no es el objetivo de este apéndice ser un libro introductorio a la mecánica cuántica, es importante dejar abierta la posibilidad de que este trabajo sea leído por gente proveniente de otras áreas de la física y de otras disciplinas. Por eso, haremos aquí un breve repaso de herramientas que serán de mucha importancia a lo largo de todo el trabajo. En particular, veremos algunas generalidades sobre la mecánica cuántica, los estados y sus evoluciones temporales, que a la vez resultan de motivación para todo el trabajo.

A.1. Estados puros y mixtos

El estado de un sistema físico está representado, en mecánica cuántica, por un vector unitario $|\psi\rangle$ en un espacio de Hilbert complejo $\mathcal{H}$. Ese tipo de estados se llaman estados puros.

Sin embargo, puede ocurrir que el sistema se encuentre en una mezcla estadística de m estados puros distintos $|\psi_i\rangle\,, i = 1, ..., m$, cada uno con probabilidad p_i. En ese caso, la descripción del estado del sistema se hará mediante

un *operador densidad* ρ definido como

$$\rho = \sum_{i=1}^{m} p_i \left|\psi_i\right\rangle \left\langle\psi_i\right| \tag{A.1}$$

Puede verse que el operador densidad posee las siguientes propiedades:

1. Es positivo ($\rho > 0$).
2. Es hermítico ($\rho^\dagger = \rho$).
3. Cumple que $\mathrm{T}r\rho = 1$.

A.1.1. Pureza

Una magnitud que resulta de interés es la *pureza* de un estado cuántico. Dicha magnitud da cuenta de qué tan cerca de un estado puro se encuentra un operador densidad. Se define la pureza $\mathcal{P}$ de un estado ρ como:

$$\mathcal{P}(\rho) = \mathrm{Tr}\left(\rho^2\right) \tag{A.2}$$

No es difícil demostrar que la pureza cumple las siguientes propiedades

1. La pureza de un estado es 1 si y solo si el estado es puro.
2. El estado de mínima pureza, también llamado *estado máximamente mixto* es $\rho_{mm} = \frac{1}{D}\mathbb{I}$, con $\mathbb{I}$ la matriz identidad y $D = \dim\mathcal{H}$. Su pureza es $\mathcal{P}(\rho_{mm}) = \frac{1}{D}$.

A.2. Observables y mediciones

Las magnitudes medibles, llamadas *observables*, están representadas en mecánica cuántica por operadores hermíticos. Con dichos operadores se puede calcular cuál será el valor medio estadístico de una magnitud física A dada, cuál es la probabilidad de obtener como resultado de la medición cada valor posible para A y cuál es el estado del sistema posterior a la medición.

Los posibles resultados que pueden obtenerse al medir el observable A a un sistema son sus autovalores, que por tratarse de un operador hermítico son todos reales. Supongamos que conocemos la base de autovectores de A

$$A\left|a_i\right\rangle = a_i\left|a_i\right\rangle, \tag{A.3}$$

los posibles resutados que se obtendrán de medir A son todos los a_i. La probabilidad de obtener un cierto a_k cuando se mide a un estado puro $|\psi\rangle$ resultado está dada por

$$Prob\left(a_k\right) = \langle\psi| \Pi_{a_k} |\psi\rangle \tag{A.4}$$

donde Π_{a_k} es el proyector asociado al subespacio de autovalor a_k. De manera consistente con esa definición, si el estado del sistema es un estado mixto ρ (o un estado puro descripto mediante su operador densidad), la probabilidad de obtener ese resultado será

$$Prob\left(a_k\right) = \mathrm{Tr}\left(\Pi_{a_k}\rho\right). \tag{A.5}$$

Como es bien sabido, la medición afecta al estado del sistema. Si se obtiene un resultado a_k, el estado en el que quedará el sistema luego de la medición será la proyección del estado inicial sobre el subespacio correspondiente.

$$|\psi_d\rangle = \frac{\Pi_{a_k} |\psi\rangle}{\sqrt{\langle\psi| \Pi_{a_k} |\psi\rangle}} \tag{A.6}$$

donde el subíndice d indica que se trata del estado posterior a la medición. Para estados mixtos este resultado se expresa como

$$\rho_d = \frac{\Pi_{a_k}\rho\Pi_{a_k}}{\mathrm{Tr}\left(\rho\Pi_{a_k}\right)}. \tag{A.7}$$

Es fácil ver, a partir de los resultados anteriores, que el valor medio del operador A se escribe como

$$\langle A\rangle_{|\psi\rangle} = \langle\psi| A |\psi\rangle \tag{A.8}$$

$$\langle A\rangle_{\rho} = \mathrm{Tr}\left(A\rho\right) \tag{A.9}$$

para estados puros y mixtos, respectivamente.

Por último, notemos que cualquier base ortonormal del espacio de Hilbert se puede utilizar para construir un observable tal que esa base sea su base de autovectores. Dada la base $\{|k\rangle\}, k = 1, \ldots, D$ se puede construir el observable $A = \sum_k a_k |k\rangle \langle k|$. Por lo tanto, dada una base de $\mathcal{H}$, diremos que la probabilidad de encontrar al sistema en el estado $|k\rangle$ es la probabilidad de medir a_k a dicho observable. Esto permite medir la probabilidad de encontrar al sistema en cada uno de los estados de una base.

A.3. Sistemas multipartitos y entrelazamiento

Cuando un sistema físico está compuesto por varios sistemas menores, se lo denomina *sistema multipartito*. Si el sistema es n-partito, el estado de Hilbert del mismo estará dado por el producto tensorial de los espacios de Hilbert individuales. Es decir $\mathcal{H} = \bigotimes_{i=1}^{n} \mathcal{H}_i$. Con esto, aparece una nueva propiedad emergente: el entrelazamiento.

Algunos estados puros pueden escribirse como un producto tensorial de vectores en los distintos espacios de Hilbert individuales. Esto es, $|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_i\rangle$. Esos estados, se denominan *estados separables* o *estados producto*. Tienen la particularidad de que los resultados de las mediciones en cada una de sus partes son independientes de los resultados en las otras partes. Todo estado puro que no pueda escribirse como un estado producto se denomina *estado entrelazado*.

Cuando se trata de estados mixtos, la definición cambia levemente. En este caso los estados productos están dados por una combinación convexa de productos tensoriales, es decir:

$$\rho = \sum_j p_j \bigotimes_{i=1}^{n} \rho_i^{(j)} \tag{A.10}$$

De igual forma que para los estados puros, si un estado no puede escribirse como estado producto, se dice que está *entrelazado*.

A.3.1. Subsistemas

Cuando uno está tratando con sistemas que poseen muchas partes, uno puede estar interesado por el estado efectivo de una sola de ellas. Supongamos que tenemos un sistema bipartito[1] cuyo espacio de Hilbert es $\mathcal{H}_A \otimes \mathcal{H}_B$. Si el estado del sistema es ρ_{AB}, entonces el estado *reducido* de A está dado por

$$\rho_A = \mathrm{Tr}_B \left(\rho_A B\right) \tag{A.11}$$

[1]Todo sistema compuesto se puede pensar como un sistema bipartito, dividiéndolo en la parte cuyo estado se quiere conocer, y la parte cuyo estado no importa.

donde la traza que aparece es la traza reducida sobre el subsistema B definida como

$$\mathrm{Tr}_B\left(\rho_A B\right) = \sum_k \langle k_B| \rho_{AB} |k_B\rangle . \tag{A.12}$$

Debe tenerse en cuenta que al multiplicar $\rho_A B$ por un bra y un ket correspondientes a estados de B, lo que se obtiene es un operador $\rho_A : \mathcal{H}_A \to \mathcal{H}_A$, como era de esperarse para un estado del subsistema A.

No está de más notar que el estado reducido de un estado bipartito puro, puede ser mixto, ya que al tomar la traza parcial se pierde información sobre las correlaciones entre los subsistemas A y B.

A.3.2. Purificación

Mencionamos que un estado puro entrelazado da lugar a subsistemas en estados mixtos. El resultado opuesto a ese también es cierto. Todo estado mixto puede pensarse como proveniendo de un estado puro en un espacio de Hilbert mayor.

Veamos que esto es efectivamente así. Comencemos por un estado mixto ρ, y veamos que se puede llegar a un estado $|\psi\rangle$ cuya traza parcial sobre un subsistema devuelve el estado ρ. En primer lugar, debido a que ρ es hermítico, es diagonalizable. Por lo tanto se puede escribir como

$$\rho = \sum_k p_k |\phi_k\rangle \langle\phi_k| \tag{A.13}$$

Ahora consideremos el estado

$$|\psi\rangle = \sum_i \sqrt{p_i} |i\rangle_A \otimes |\phi_i\rangle_B . \tag{A.14}$$

Ese estado es el buscado. En efecto si trazamos sobre el primer subsistema obtenemos que

$$\begin{aligned}
\mathrm{Tr}_A |\psi\rangle\langle\psi| &= \mathrm{Tr}_A \left(\sum_{ij} \sqrt{p_i p_j} |i\rangle \otimes |\phi_i\rangle \langle j| \otimes \langle\phi_j| \right) \\
&= \sum_k \langle k| \left(\sum_{ij} \sqrt{p_i p_j} |i\rangle \otimes |\phi_i\rangle \langle j| \otimes \langle\phi_j| \right) |k\rangle \\
&= \sum_{ijk} \sqrt{p_i p_j} \delta_{ik} \delta_{ij} |\phi_i\rangle \langle\phi_j| \\
&= \sum_k p_k |\phi_k\rangle \langle\phi_k| = \rho
\end{aligned} \tag{A.15}$$

Es decir, todo estado mixto es un estado puro en un espacio de Hilbert mayor.

A.3.3. Entrelazamiento y medidas

Existen numerosos criterios y medidas para saber qué tan entrelazado está un estado[NC04, HW97, Woo98, HHHH09, CKW00, OV06, Ved02, BDSW96, Ba05]. De ellas, un par resultarán de utilidad durante el presente trabajo.

Criterio de Peres-Horodecki

El cirterio de Peres[Per96] es un criterio suficiente para que un estado esté entrelazado, pero no necesario. Es decir, todo estado que cumple con el criterio es un estado entrelazado, pero no todo estado entrelazado lo cumple.

El criterio se basa en la siguiente observación: si ρ es un estado, entonces su operador transpuesto ρ^T también lo es (es hermítico, positivo y tiene la misma traza que ρ).

Consideremos un estado biseparable como el de la ecuación (A.10)

$$\rho_{AB} = \sum_i p_i \rho_i^{(A)} \otimes \rho_i^{(B)}. \tag{A.16}$$

Dado que $\rho_i^{(B)}$ son todos estados válidos, sus transpuestas también lo son. Por lo tanto, la transpuesta parcial sobre el segundo subsistema de un estado separable, da también un estado. El criterio de Peres dice, entonces, que si un estado tiene transpuesta parcial no positiva (es decir, con algún autovalor negativo), es entrelazado.

El agregado de Horodecki, Horodecki y Horodecki [HHH96] fue mostrar que en dimensiones 2×2 y 2×3 el criterio también es suficiente.

Concurrencia

La concurrencia es una de muchas maneras de cuantificar el entrelazamiento, en este caso, bipartito. Para estados puros, la idea es sencilla: ya que un estado puro bipartito tiene como estados reducidos de sus dos partes a estados mixtos, la pureza de un subsistema cuantifica, en algún sentido, el entrelazamiento.

En este sentido, se define la concurrencia de un estado puro bipartito $|\psi\rangle$ como

$$\mathcal{K}(\psi) = \sqrt{2\left(1 - \mathrm{Tr}\rho_A^2\right)} \tag{A.17}$$

donde ρ_A es la densidad reducida de uno de los dos subsistemas.

Para estados mixtos la definición no es tan simple ya que un mismo estado puede escribirse de muchas formas, según la base elegida[2]. Lo que se utiliza en ese caso es buscar la base en la que el entrelazamiento es mínimo. Es decir, se define la concurrencia para un estado mixto ρ como

$$\tilde{\mathcal{K}}(\rho) = \min_{\mathcal{T}} \left(\sum_i p_i \mathcal{K}(\psi_i) \right) \tag{A.18}$$

donde la minimización se realiza sobre todos los los conjuntos de estados puros tales que $\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i|$.

A.4. Evoluciones y canales

No sólo de estados se nutre la mecánica cuántica. También es importante conocer la evolución temporal de los mismos. Cuando se trata de un sistema aislado incicalmente en un estado puro $|\psi, t = 0\rangle$, la evolución estará dada por un operador unitario U en la forma

$$|\psi, t\rangle = U |\psi, t = 0\rangle \tag{A.19}$$

con $U^\dagger U = \mathbb{I}$

Sin embargo, puede ocurrir que la evolución unitaria afecte a nuestro sistema y un entorno y sólo estemos interesados en la evolución efectiva de nuestro sistema. En este caso ya no podremos referirnos a la evolución como un operador unitario, sino por un superoperador lineal[3] $\mathcal{E} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ que lleva operadores densidad en operadores densidad.

[2]El caso más claro de esto es el estado máximamente mixto. Ese estado puede escribirse en una base entrelazada o en una separable. El entrelazamiento del estado, como recurso físico, tiene que ser independiente de la base en la que se lo escriba.

[3]Llamaremos indistintamente a estos superoperadores canales o mapas.

A.4.1. Positividad y positividad completa

Canales positivos

Diremos que un canal $\mathcal{E}$ es positivo cuando para todo ρ positivo (es decir, con todos sus autovalores mayores o iguales a cero), el resultado de pasar por el canal $\rho' = \mathcal{E}(\rho)$ es también positivo.

Este tipo de canales son de gran importancia ya que las operaciones cuánticas, entendidas como evoluciones de un estado cuántico, tienen que dar como resultado *siempre* un estado. Ese requisito es la positividad del canal.

Canales k–positivos y completamente positivos

Además, un canal $\mathcal{E}$ será llamado k–positivo si su extensión $\mathcal{E} \otimes \mathbb{I}_k$, con $\mathbb{I}_k$ el canal identidad de dimensión k, también es un canal positivo.

Si un canal es k–positivo para todo k, entonces diremos que es completamente positivo. Puede mostrarse que un canal es completamente positivo si y solo si es D–positivo.

Los canales completamente positivos son de gran importancia en mecánica cuántica ya que en condiciones bastante generales (por ejemplo, discordia nula entre el estado inicial del sistema y del entorno[SL09]), la evolución del sistema está representada por un canal completamente positivo, o CP.

A.5. Los qubits y la base computacional

En computación clásica la unidad básica de información es el bit, que puede tomar como valores el 0 y el 1. El análogo cuántico de esa unidad es un sistema que puede tomar dos valores, y que esos valores son distinguibles en una medición. Es decir, un sistema cualquiera de dimensión 2 (cuyo espacio de Hilbert notaremos como $\mathcal{H}_2$). Ese tipo de sistemas son llamados *qubits*.

Una base arbitraria ortonormal de ese espacio de Hilbert, aunque por lo general elegida por alguna motivación física, se denomina base computacional y sus estados se notan como $\{|0\rangle, |1\rangle\}$. Por convención, los operadores de Pauli se escriben en esa base tomandola como autoestados de σ_z. De esa

forma se tiene que

$$\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0| \tag{A.20}$$
$$\sigma_y = -i|0\rangle\langle 1| + i|1\rangle\langle 0| \tag{A.21}$$
$$\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1| \tag{A.22}$$

Para sistemas de n qubits, el espacio de Hilbert es $\mathcal{H}_2^{\otimes n}$. La base computacional, en ese caso, se define como la base producto de estados de la base computacional de un solo qubit.

A.6. Los operadores de Pauli generalizados

Los operadores de Pauli de las ecuaciones (A.20), (A.21) y (A.22) junto con el operador identidad $\mathbb{I}$ forman una base real de los operadores hermíticos y una compleja de los operadores lineales. Por ese motivo y por algunas relaciones de ortogonalidad y conmutación que poseen, son muy utilizados en mecánica cuántica.

Estos operadores poseen las siguientes propiedades:

- Salvo la identidad, poseen traza nula ($\mathrm{Tr}(\sigma_i) = 2\delta_{i0}$, donde se toma por convención que $\sigma_0 = \mathbb{I}$).
- Son hermíticos ($\sigma_i^\dagger = \sigma_i$).
- Salvo la identidad, todos tienen un autovalor $+1$ y otro -1.
- Son todos operadores unitarios.
- El producto de dos matrices de Pauli es tal que

$$\sigma_j\sigma_k = i\epsilon_{jkl}\sigma_l + \delta_{jk} \tag{A.23}$$

  donde ϵ_{jkl} es el tensor de Levi–Civita.
- Todo operador de Pauli distinto de la identidad conmuta con sí mismo y con la identidad y anticonmuta con los otros dos operadores de Pauli.
- Forman una base ortogonal del espacio de operadores ya que, usando el producto interno de Schmidt (el usual entre operadores) se tiene que $\mathrm{Tr}(\sigma_j\sigma_k) = 2\delta_{jk}$.

Los *operadores de Pauli generalizados* se definen para sistemas de n qubits como el producto tensorial de n operadores de Pauli (algunos de los cuales pueden ser la identidad). Formalmente, se los define como

$$\sigma_{\vec{a},\vec{b}} = \bigotimes_{i=1}^{n} \sigma_x^{a_1} \sigma_z^{b_i} e^{i\frac{\pi a_i b_i}{2}} = \sigma_x^{\vec{a}} \sigma_z^{\vec{b}} e^{i\frac{\pi \vec{a}\cdot\vec{b}}{2}}. \tag{A.24}$$

Los operadores de Pauli generalizados poseen propiedades muy parecidas a las de los operadores de Pauli de un qubit:

- Son hermíticos.
- Son unitarios.
- La mitad de sus autovalores son $+1$ y la otra mitad -1.
- A excepción de la identidad, todos poseen traza nula.
- El producto de dos operadores de Pauli generalizados es otro operador de Pauli generalizado, a menos de un fase.
- Todo par de operadores de Pauli generalizados conmuta o anticonmuta. En efecto, dos operadores $\sigma_{\vec{a},\vec{b}}$ y $\sigma_{\vec{c},\vec{d}}$ verifican que:

$$\begin{array}{rcll} \left[\sigma_{\vec{a},\vec{b}}, \sigma_{\vec{c},\vec{d}}\right] & = & 0 & \text{si} \quad \vec{a}\cdot\vec{d} - \vec{c}\cdot\vec{b} = 0 \pmod 2 \\ \left\{\sigma_{\vec{a},\vec{b}}, \sigma_{\vec{c},\vec{d}}\right\} & = & 0 & \text{si} \quad \vec{a}\cdot\vec{d} - \vec{c}\cdot\vec{b} = 1 \pmod 2 \end{array} \tag{A.25}$$

- Son ortogonales en el producto de Schmidt, y forman una base del espacio real de operadores hermíticos, y del espacio complejo de operadores lineales.

A.7. Dualidad entre canales y operadores

Existe una dualidad entre los operadores lineales en $\mathcal{B}(\mathcal{H}\otimes\mathcal{H})$ y los mapas de $\mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ dada por el isomorfismo de Choi–Jamiołkowski[Cho75, Jam72]. El mismo establece una relación de uno a uno entre operadores y canales.

Se define el operador $\mu_{\mathcal{E}}$ isomorfo al canal $\mathcal{E}$ como

$$\mu_{\mathcal{E}} = (\mathcal{E}\otimes\mathbb{I})\left(|I\rangle\langle I|\right), \tag{A.26}$$

donde $|I\rangle = \frac{1}{\sqrt{D}} \sum_i |ii\rangle$ es el estado máximamente entrelazado. Es decir, el operador isomorfo al canal $\mathcal{E}$ es el que se obtiene al hacer actuar el canal sobre una de las partes del estado máximamente entrelazado.

Además de esa relación de uno a uno entre operadores y canales, esa misma expresión da una relación de uno a uno entre operadores positivos y canales completamente positivos, como demostraremos en la Sección A.8.

A.8. Representaciones de procesos cuánticos

Existen diversas formas de describir un proceso cuántico. En particular, hay dos descripciones que resultarán de utilidad para los protocolos tomográficos. Describiremos aquí dos de ellas: la *matriz* χ y la *representación de Kraus*.

A.8.1. La matriz χ

La descripción de canales mediante la llamada *matriz* χ permite representar cualquier canal lineal. Para dar la descripción de un canal se debe, en primer lugar, elegir una base del espacio de operadores

$$\mathcal{S} = \left\{ E_m \in \mathcal{B}\left(\mathcal{H}\right), m = 0, ..., D^2 - 1 \right\}. \tag{A.27}$$

La matriz χ del canal en dicha base será tal que

$$\mathcal{E}\left(\rho\right) = \sum_{mm'} \chi_{mm'} E_m \rho E_{m'}^{\dagger} \tag{A.28}$$

Es fácil ver que todo canal lineal puede escribirse en esa representación. Además, muchas de las propiedades del canal pueden traducirse en propiedades de la matriz χ.

1. El canal es hermítico (es decir, preserva hermiticidad) si y solo si la matriz χ es hermítica ($\chi^{\dagger} = \chi$).

2. Si el mapa preserva traza ($\mathrm{Tr}\rho = \mathrm{Tr}\left(\mathcal{E}\left(\rho\right)\right)$), entonces su matriz χ será tal que $\sum_{mm'} \chi_{mm'} E_{m'}^{\dagger} E_m = \mathbb{I}$.

3. El mapa es completamente positivo si y solo si su matriz χ es positiva.

Las dos primeras propiedades son simples de demostrar. La tercera, que demostraremos en breve, está relacionada con otra representación de los canales completamente positivos denominada *representación de Kraus*.

A.8.2. La representación de Kraus

La representación de Kraus permite describir la dinámica de cualquier canal completamente positivo (CP). A diferencia de la matriz χ, ésta representación no permite describir canales que no sean CP.

Dado un canal $\mathcal{E}$ completamente positivo, se lo puede escribir como:

$$\mathcal{E}(\rho) = \sum_k A_k \rho A_k^\dagger \tag{A.29}$$

donde los A_k se denominan *operadores de Kraus*.

El siguiente teorema da cuenta de las limitaciones y alcances de la representación de Kraus[Wik11d]:

Teorema A.1. *Sea $\mathcal{E} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ un mapa positivo, con $Dim(\mathcal{H}) = D$. Son equivalentes:*

1. *$\mathcal{E}$ es D–positivo.*
2. *La matriz χ de $\mathcal{E}$ en la base de operadores*

   $$\mathcal{S} = \{|i\rangle\langle j|, i = 1, ..., D, j = 1, ..., D\},$$

   también llamada matriz de Choi y denotada $\chi^{(c)}$, es positiva. [4]
3. *$\mathcal{E}$ admite representación en la forma de Kraus.*
4. *$\mathcal{E}$ es completamente positivo.*

Demostración. Comenzaremos la demostración mostrando que (1) $\Rightarrow$ (2). Notemos que la matriz de Choi es la representación matricial del operador μ en la base $\mathcal{S}$:

$$\mu = \frac{1}{D}(\mathcal{E} \otimes \mathbb{I}_D)\left(\sum_{i,j} |ii\rangle\langle jj|\right)$$

Es decir, μ es el operador isomorfo a $\mathcal{E}$. Por hipótesis, $\mathcal{E}$ es D–positivo. Por lo tanto μ es positivo, lo que implica que su representación matricial es positiva. Puesto que su representación matricial es la matriz de Choi del canal, esta es positiva.

[4] Vale aclarar que dada esta elección de $\mathcal{S}$, cada índice de la matriz χ tendrá dos componentes. De esta forma, $\chi_{\substack{ij \\ kl}}$ corresponderá al coeficiente asociado a los operadores $|i\rangle\langle j|$ y $|k\rangle\langle l|$.

Veamos ahora que (2) $\Rightarrow$ (3). Como la matriz de Choi es positiva, es diagonalizable:

$$\chi^{(c)} = \sum_r \vec{v_r}\vec{v_r}^\dagger$$

donde los vectores $\vec{v_r} \in \mathbb{C}^{D^2}$. El canal se escribe como:

$$\mathcal{E}(\rho) = \sum_{\substack{ij\\kl}} \left(\sum_r \vec{v_r}\vec{v_r}^\dagger \right)_{\substack{ij\\kl}} |i\rangle \langle j| \rho |l\rangle \langle k|$$

Reordenando las sumas se obtiene:

$$\mathcal{E}(\rho) = \sum_r \left[\sum_{ij} (\vec{v_r})_{ij} |i\rangle \langle j| \right] \rho \left[\sum_{kl} (\vec{v_r})^*_{kl} |l\rangle \langle k| \right]$$

Que es precisamente la forma de Kraus del canal, con

$$A_k = \sum_{ij} (\vec{v_k})_{ij} |i\rangle \langle j|$$

Ahora demostraremos que (3) $\Rightarrow$ (4). Por (3), $\mathcal{E}(\rho) = \sum_k A_k \rho A_k^\dagger$. Pero como una combinación convexa de canales completamente positivos es, también, completamente positiva, alcanza con ver que los canales de la forma $\tilde{\mathcal{E}}(\rho) = A\rho A^\dagger$ son CP. En efecto, consideremos la extensión a una dimensión arbitraria del canal, y veamos que, en efecto, es positiva:

$$\langle\psi| (A \otimes \mathbb{I}) \rho \left(A^\dagger \otimes \mathbb{I}\right) |\psi\rangle = \langle\phi| \rho |\phi\rangle \geq 0$$

donde $|\phi\rangle = \left(A^\dagger \otimes \mathbb{I}\right) |\psi\rangle$ y la positividad se desprende de la positividad de ρ.

Finalmente, (4) $\Rightarrow$ (1) de manera trivial.

□

La representación de Kraus tiene la ventaja de que es simple de interpretar físicamente. La ecuación (A.29) se puede reescribir, normalizando los operadores de Kraus, como

$$\mathcal{E}(\rho) = \sum_k \alpha_k \tilde{A}_k \rho \tilde{A}_k^\dagger \tag{A.30}$$

con $\sum_k \alpha_k = 1$.

Es decir, el canal $\mathcal{E}$ se comporta como cada uno de los operadores A_k con una probabilidad α_k.

A.9. Computación cuántica basada en circuitos

Veremos aquí una breve intruducción al modelo de circuitos de la computación cuántica, que nos permitirá leer y comprender los diversos circuitos cuánticos que aparecen a lo largo de esta tesis.

Los circuitos cuánticos son una representación de las evoluciones, en muchos casos unitarias, de los sistemas cuánticos. Como tal, es pariente cercana de los circuitos lógicos clásicos y del paradigma clásico de la programación imperativa, en el sentido en que uno describe paso a paso las transformaciones a realizarle a un sistema. Una descripción detallada sobre el modelo de computación cuántica basado en circuitos puede encontrarse en [NC04].

La idea del modelo de circuitos es describir la evolución mediante una serie sucesiva de evoluciones simples. La Figura A.1 muestra la representación circuital del operador $(U_1 \otimes \mathbb{I})\,(U_{12})\,(\mathbb{I} \otimes U_2)$ sobre un sistema bipartito inicialmente en el estado $|\psi_1\rangle \otimes |\psi_2\rangle$.

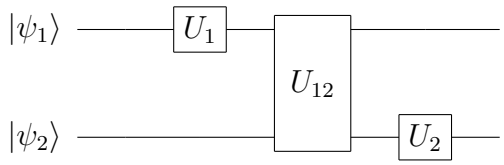

Figura A.1: Ejemplo de un circuito cuántico para realizar la operación $(U_1 \otimes \mathbb{I})\,(U_{12})\,(\mathbb{I} \otimes U_2)$ al estado $|\psi_1\rangle \otimes |\psi_2\rangle$.

Veremos a continuación algunas *compuertas cuánticas* (es decir, operadores unitarios en representación circuital) que son, en conjunto con el resto de rotaciones de un qubit y operadores de Pauli, muy utilizadas en computación cuántica. Además, son utilizadas una y otra vez a lo largo de todo el presente trabajo.

A.9.1. Compuertas cuánticas

La transformada de Hadamard

La transformada de Hadamard H actúa sobre un qubit de la base computacional como:

$$\begin{aligned} H|0\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ H|1\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned} \tag{A.31}$$

Es fácil ver que esta operación es tanto hermítica como unitaria.

En el modelo de circuitos, se la suele notar como vemos en la Figura A.2.

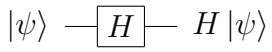

Figura A.2: Representación circuital de la transformada de Hadamard.

Esta compuerta es una rotación de un qubit que actúa sobre los operadores de Pauli por conjugación como se ve en las ecuaciones (A.32), (A.33) y (A.34). La representación circuital de dichas igualdades puede verse en la Figura A.3.

$$H\sigma_x H = \sigma_z \tag{A.32}$$
$$H\sigma_z H = \sigma_x \tag{A.33}$$
$$H\sigma_y H = -\sigma_y \tag{A.34}$$

Es decir, pasa de la base de autoestados de X a la de Z, y viceversa.

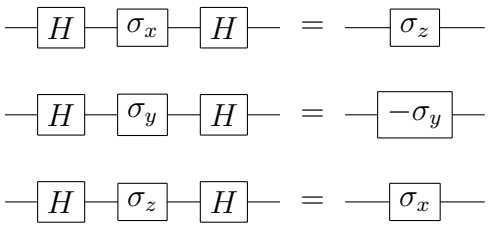

Figura A.3: Modo en el que actúa el operador de Hadamard sobre los operadores de Pauli.

Operador de fase

La transformada de Hadamard es una rotación alrededor del eje Y. Deja invariante al operador σ_y, pero intercambia a los otros dos operadores de Pauli. Para realizar rotaciones que modifican también al operador σ_y, es necesario apelar al operador de fase T definido como

$$\begin{aligned} T\,|0\rangle &= |0\rangle \\ T\,|1\rangle &= i\,|1\rangle \end{aligned} \tag{A.35}$$

En la figura A.4 puede verse la representación circuital del operador T.

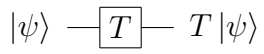

Figura A.4: Representación circuital del operador de fase.

En éste caso, resultarán de importancia las equivalencias dadas en la figura A.5.

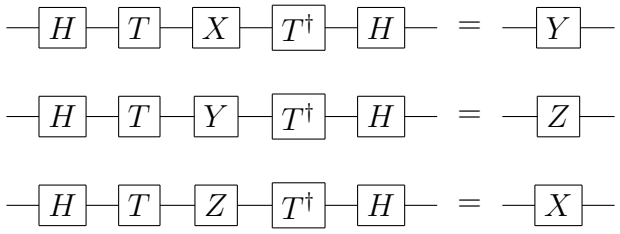

Figura A.5: El operador T, en conjunto con H, permite moverse cíclicamente por los operadores de Pauli.

La compuerta C-Not

La compuerta C-Not, también llamada control-not, es un negador cuántico controlado, una suerte de versión cuántica del XOR clásico. Esa compuerta hace interactuar dos qubits por lo que es, de las que vimos, la única que puede modificar propiedades de entrelazamiento de los estados por su calidad no local.

En la Figura A.6 se muestra el resultado de la aplicación de la compuerta C-Not sobre una base del espacio de dos qubits, con lo que queda completamente definido el operador.

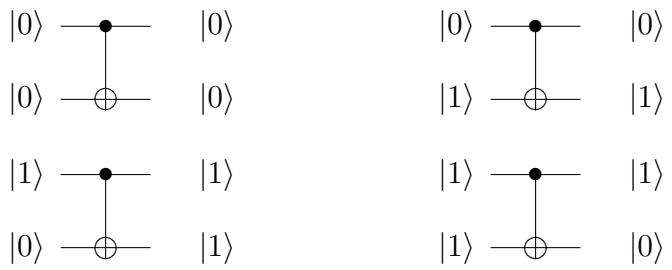

Figura A.6: La compuerta C-Not y su accionar sobre una base del espacio de Hilbert de dos qubits.

Una característica importante de la compuerta C-Not es que puede ser utlizada para construir una compuerta de intercambio entre dos qubits, combinando tres C-Not de la forma ilustrada en la Figura A.7.

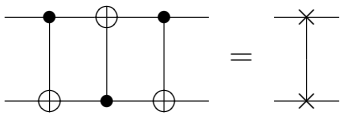

Figura A.7: Las compuertas C-Not se pueden combinar para intercambiar la información de dos qubits.

Obedece, además, las reglas de conmutación con los operadores de Pauli que se ilustran en las figuras A.8 y A.9.

A.9.2. Complejidad en algoritmos cuánticos

En computación clásica, la complejidad de un algoritmo se da mediante una cota superior asintótica $O(f(n))$, que indica que para una entrada de tamaño n a un algoritmo, la cantidad de operaciones que el mismo realiza hasta informar la salida es asintóticamente menor a $f(n)$. De esa forma, encontrar un elemento en una base de datos desordenada, por citar algún ejemplo, requiere $O(n)$ operaciones; ordenar de menor a mayor una lista de números $O(n \log n)$, etc.

En computación cuántica, la noción análoga corresponde a contar cuantas operaciones se realizaron. Sin embargo, como todo algoritmo cuántico puede resumirse en una única operación unitaria, hay que ser un poco más específico acerca de qué quiere decir operaciones (además, dicha operación

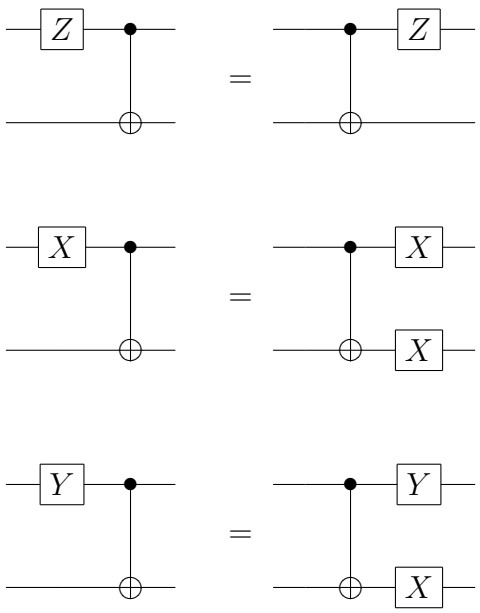

Figura A.8: Reglas de conmutación de la compuerta C-Not con operadores de Pauli en el qubit de control.

podría ser absorbida en la medición final, por lo que todo algoritmo puede pensarse como una medición en una base adecuada). Con eso en mente, se define la complejidad como *la cantidad de compuertas cuánticas necesarias de un solo qubit y C-Not para obtener el resultado del algoritmo en la base computacional.*

A.10. El formalismo de los estabilizadores

El formalismo de los estabilizadores, originalmente desarrollado para su utilización en los códigos de corrección de errores[Got97, Got98, Got00] provee una herramienta para describir estados que, en algunos contextos, resulta más práctica que la de etiquetas de un vector en el espacio de Hilbert.

Diremos que un estado $|\psi\rangle$ es estabilizado por el operador A con autovalor ± 1 si

$$A\,|\psi\rangle = \pm\,|\psi\rangle \tag{A.36}$$

De esa forma, un estado estará caracterizado por los generadores de su grupo estabilizador y los autovalores. Por ejemplo, si el grupo estabilizador es

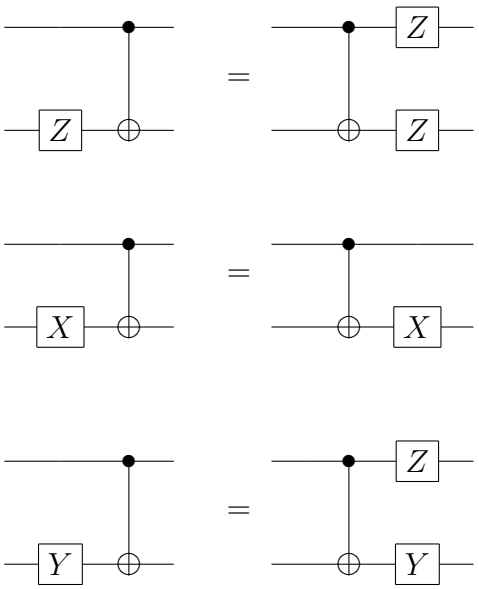

Figura A.9: Reglas de conmutación de la compuerta C-Not con operadores de Pauli en el qubit de objetivo.

el generado por el operador σ_x y su autovalor $+1$, es claro que nos referimos al estado $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

Si, en cambio, hablamos de un grupo estabilizador $\mathcal{S}\{\sigma_x \otimes \sigma_x, \sigma_y \otimes \sigma_y\}$[5], y sus autovalores $\vec{s} = (+1, +1)$, entonces estamos hablando del estado de Bell $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. En general, en el formalismo de estabilizadores, notaremos ese estado como $(\mathcal{S}, \vec{s})$.

A.11. El grupo de Clifford

El grupo de Clifford $\mathcal{C}$, que también utilizamos a lo largo de la tesis, es un grupo de operadores unitarios que, por conjugación, mapean operadores de Pauli en operadores de Pauli.

Si $\{E_k, k = 1, \ldots, D^2\}$ es la base de operadores de Pauli y $\mathcal{C}_l$ es un operador de Clifford, entonces

$$\mathcal{C}_l E_k \mathcal{C}_l^\dagger = E_{k'}. \tag{A.37}$$

[5]Dejaremos siempre implícito al operador identidad en todos los grupos.

Los operadores simplécticos son los que realizan mapeos no triviales del grupo de Pauli en sí mismo.

El grupo de Clifford se divide en dos subconjuntos, el de operadores de Pauli, que evidentemente son operadores de Clifford, y los operadores simplécticos, que son todos los operadores de Clifford que no son de Pauli.

Los mapeos realizados por el grupo de Clifford, por tratarse de operadores unitarios, preservan las relaciones de conmutación.

Apéndice B

Bases mutuamente no sesgadas

Los conjuntos de bases mutuamente no sesgadas (MUBs por su sigla en inglés) son una construcción matemática que se ha ido convirtiendo en una herramienta cada vez más presente en la información cuántica [Ben06a, BRKSS07, BW08, RBKSS05, KR05, PR04b, GHW04, BBRV02, Ben06b].

Decimos que dos bases ortonormales $\mathcal{B}_J = \{|\psi_m^J\rangle : m \in 1..D\}$ y $\mathcal{B}_K = \{|\psi_l^K\rangle : l \in 1..D\}$ son mutuamente no sesgadas si y sólo si

$$|\langle\psi_m^J|\psi_l^K\rangle| = \frac{1}{D}. \ \forall m, l \tag{B.1}$$

Típicamente, diremos que la medición en la base $\mathcal{B}_J$ no da ninguna información sobre la medición en la base $\mathcal{B}_K$, ya que para cada resultado de la primera medición, los resultados de la segunda son equiprobables. De ahí que se llamen *no sesgadas*. Está demostrado que pueden existir a lo sumo $D+1$ bases mutuamente no sesgadas, y sólo se conocen construcciones para esos conjuntos máximos de bases en dimensiones que son potencias de un número primo.

Klappenecker y Roetteler [KR05] demostraron que un conjunto de máximo de bases mutuamente no sesgadas forma un 2–diseño de estados (ver demostración completa en el Apéndice C), y de ahí parte de nuestro interés en las bases mutuamente no sesgadas. Previamente, Bandyopadhyay y colaboradores[BBRV02] habían demostrado una relación importante entre los conjuntos de bases mutuamente no sesgadas y conjuntos abelianos máximos de operadores unitarios ortogonales. Uno de sus resultados es que si uno construye una partición de un conjunto completo de D^2-1 operadores mutuamente ortogonales sin traza en $D+1$ subconjuntos abelianos de

$D-1$ operadores cada uno, entonces las $D+1$ bases estabilizadas por cada uno de esos subconjuntos son mutuamente no sesgadas. Daremos aquí una construcción explícita de uno de esos conjuntos.

Si los $2^{2n}-1$ operadores de Pauli generalizados son particionados en 2^n+1 subconjuntos conmutativos máximos, entonces cada uno de esos subconjuntos será el estabilizador de una base, y cada una de esas bases será no sesgada con las demás. Por lo tanto, el problema de encontrar los grupos estabilizadores del conjunto de MUBs se reduce al de particionar los operadores de Pauli generalizados en 2^n+1 grupos abelianos.

La forma más simpre de construir esa partición es mediante la utilización de cuerpos finitos, como fue realizado primero por Wooters[Woo04] y luego usada por Paz y colaboradores[PRS05]. El primer requisito en la construcción de la matriz compañera M para un polinomio primitivo del cuerpo finito $GF(2^n)$:

$$M = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & & & & & 1 \\ r_0 & r_1 & r_2 & \cdots & & r_{n-1} \end{pmatrix} \tag{B.2}$$

donde el polinomio primitivo del cuerpo finito es $p(x) = r_0 + r_1 x + r_2 x^2 + \ldots + r_{n-1}x^{n-1} + x^n$.

Esa matriz tiene la propiedad que $M^D = M$ y $M^k \neq M \ \forall k < D$, donde todas las operaciones están hechas módulo 2. Consideremos el siguiente conjunto de operadores de Pauli generalizados,

$$G_{\vec{b}} = \left\{ 1, P_{\vec{b},j} = \sigma_x^{\vec{1}M^j} \sigma_z^{\vec{b}\hat{M}^j} : j = 1, \ldots, D-1 \right\}, \tag{B.3}$$

donde $\vec{b} \in \{0,1\}^n$ es un vector binario, $\hat{M}$ es la transpuesta de M, $\vec{1} = (1,0,0,\ldots)$ es el primer vector binario de la base canónica y se nota $\sigma_x^{\vec{b}} = \bigotimes_i \sigma_x^{b_i}$. Además, puesto que $M^D = M$, tenemos que $j = 0$ es equivalente a $j = D-1$.

Es fácil verificar que $G_{\vec{b}}$ es un grupo abeliano, y que el único operador en común entre todos los grupos es la identidad. Por lo tanto, esos conjuntos, junto con el formado por los operadores que son producto tensorial de σ_z e identidades, es la partición buscada.

Eso completa la construcción explícita del conjunto máximo de bases mutuamente no sesgadas. Veremos a continuación, en la Sección B.1, como

construir eficientemente los estados del conjunto a partir de un estado de la base computacional, y como medir en una base dada de las MUBs.

B.1. Circuitos eficientes de cambio de base

Repetiremos aquí la construcción de circuitos de cambio de base mostrada en [Ben06a]. Veremos que existen circuitos que, utilizando recursos polinomiales en el tamaño del sistema ($O(n^2)$ compuertas cuánticas y $O(n^3)$ operaciones clásicas para determinar las compuertas cuánticas a utilizar), permiten cambiar de base entre las de un conjunto de MUBs de dimensión 2^n. Para ver que existen dichos circuitos, procederemos a construirlos explícitamente, dando también el algoritmo mediante el cual una computadora clásica puede construirlos. Es decir, veremos como, dadas dos bases de un conjunto de MUBs, construir un circuito de cambio de base entre ellas.

B.1.1. Construcción de los circuitos

En primer término, es importante notar que si es posible construir eficientemente circuitos que lleven cualquier base estabilizada por operadores de Pauli generalizados a aquella estabilizada por los operadores σ_z, entonces será posible construir circuitos que lleven de cualquier base estabilizada por un conjunto de operadores de Pauli a cualquier otra base estabilizada por otro conjunto de operadores de Pauli, combinando dos de estos circuitos. Se trata, por lo tanto, de encontrar circuitos para pasar de cualquier base estabilizada por operadores de Pauli a la base estabilizada por los operadores σ_z.

Para llevar a cabo la construcción del circuito de cambio de base de la estabilizada por $\left\{\sigma_x^{\vec{q}}\sigma_z^{\vec{q}S}, \forall \vec{q}\right\}$ a la base estabilizada por $\left\{\sigma_z^{\vec{q}}, \forall \vec{q}\right\}$, resulta conveniente comenzar por construir una transformación unitaria $\tilde{U}$ que convierta un autovector de $X^{\vec{1}}\sigma_z^{\vec{1}S}$ en un autovector de $\sigma_z^{\vec{1}}$ de igual autovalor, donde $\vec{1}$ es el vector binario de dimensión n que tiene un 1 en la primera componente y ceros en las demás. Es decir, encontrar una transformación unitaria $\tilde{U}$ tal que se verifique la siguiente implicación:

$$\begin{aligned} \sigma_x^{\vec{1}}\sigma_z^{\vec{1}S}\left|\psi\right\rangle &= \lambda\left|\psi\right\rangle \\ \Longrightarrow \sigma_z^{\vec{1}}\tilde{U}\left|\psi\right\rangle &= \lambda\tilde{U}\left|\psi\right\rangle \end{aligned} \tag{B.4}$$

Equivalentemente, $\sigma_z^{\vec{1}} = \tilde{U}\sigma_x^{\vec{1}}\sigma_z^{\vec{1}S}\tilde{U}^\dagger$. Por lo tanto, se construirá una operador $\tilde{U}$ que actúe convirtiendo por conjugación (es decir, multiplicando a izquierda por $\tilde{U}$ y a derecha por $\tilde{U}^\dagger$) un operador de Pauli dado en el operador $\sigma_z^{\vec{1}}$,

Para conseguir dicha transformación es necesario, en primer lugar, convertir al operador en cuestión en un operador formado sólo por σ_z e identidades. Esto puede conseguirse aplicando, por conjugación, transformaciones de Hadamard y operadores de fase a los qubits individuales:

$$\bigotimes_{j=1}^{n} R_j \left[\vec{1}_j, \left(\vec{1}S\right)_j\right] \tag{B.5}$$

donde el subíndice j indica el qubit sobre el que actúa la operación, y R_j está dada por:

$$\begin{array}{rcl} R_j\left(0,0\right) & = & 1_j \\ R_j\left(1,0\right) & = & H_j \\ R_j\left(0,1\right) & = & 1_j \\ R_j\left(1,1\right) & = & H_j T_j^\dagger \end{array} \tag{B.6}$$

Supongamos, a modo de ejemplo, que se intenta construir una transformación unitaria V que convierta al operador $\sigma_z \otimes 1 \otimes \sigma_x \otimes \sigma_z \otimes \sigma_y$ en el operador $\sigma_z \otimes 1 \otimes \sigma_z \otimes \sigma_z \otimes \sigma_z$. Es decir, $V\left(\sigma_x \otimes 1 \otimes \sigma_x \otimes \sigma_z \otimes \sigma_y\right)V^\dagger = \sigma_z \otimes 1 \otimes \sigma_z \otimes \sigma_z \otimes \sigma_z$. De acuerdo a las ecuaciones (B.5) y (B.6), el operador V estaría dado por:

$$V = H \otimes 1 \otimes 1 \otimes 1 \otimes HT^\dagger \tag{B.7}$$

que, considerando la representación circuital mostrada en la Figura B.1 de $V\sigma_x \otimes 1 \otimes \sigma_x \otimes \sigma_z \otimes \sigma_y V^\dagger$ y las identidades exhibidas en las Figuras A.5 y A.3, es igual a $\sigma_z \otimes 1 \otimes \sigma_z \otimes \sigma_z \otimes \sigma_z$.

Luego debe aplicarse alguna transformación que convierta todos los operadores σ_z en identidades, a excepción del operador del primer qubit, que debe permanecer σ_z. Esto puede conseguirse aplicando un C-Not con control en cada uno de los qubits que no tienen a la identidad y objetivo en el primero:

$$\prod_{j=2}^{n} \left(\mathrm{C-Not}\left(j,1\right)\right)^{\left(1-\delta_{\vec{1}_j,0}\delta_{\left(\vec{1}S\right)_j,0}\right)} \tag{B.8}$$

donde el exponente da cuenta de que sólo se realiza el $\mathrm{C-Not}$ utilizando los qubits que no tienen una identidad.

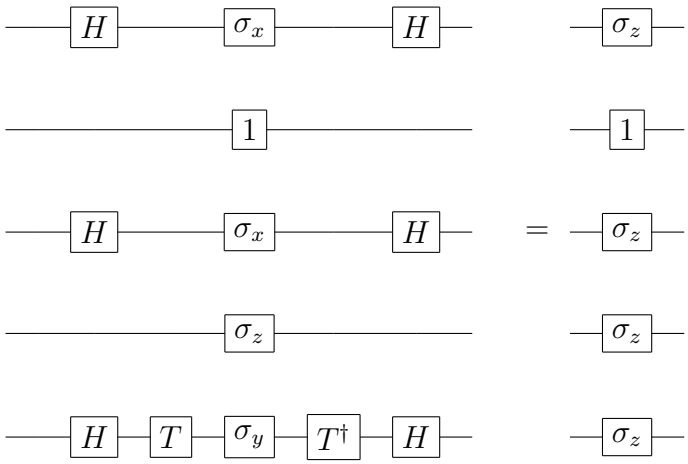

Figura B.1: Un operador de Pauli generalizado puede convertirse, mediante la aplicación de transformaciones de sólo un qubit, en un producto de operadores σ_z e identidades.

Continuando con el ejemplo de B.1, puede verse dicha transformación en la Figura B.2. La operación completa para convertir un Pauli que no posee una identidad en el primer qubit del grupo estabilizador en el operador σ_z del primer qubit es, entonces:

$$\tilde{U} = \prod_{j=2}^{n} \left(\mathrm{C-Not}\,(j,1)\right)^{\left(1-\delta_{\vec{1}_j,0}\delta_{(\vec{1}S)_j,0}\right)} \bigotimes_{j=1}^{n} R_j \left[\vec{1}_j, \left(\vec{1}S\right)_j\right] \tag{B.9}$$

Sin embargo, el problema no se resuelve aquí; al convertir un cierto operador del estabilizador original en un operador σ_z sobre el primer qubit, el resto de los operadores del estabilizador también se transforman. Pero puesto que la transformación $\tilde{U}$ conserva la característica abeliana del grupo, se obtendrá luego de la transformación, un grupo abeliano estabilizador al cual pertenece el operador σ_z del primer qubit. Se debe, en éste punto, determinar generadores de dicho grupo abeliano. Para eso, se deben tomar los n generadores O_j del grupo, y transformarlos como $\tilde{U}O_j\tilde{U}^\dagger$. Determinar el resultado de dicha transformación, puesto que los O_j son operadores de Pauli y $\tilde{U}$ está compuesta por rotaciones entre los operadores de Pauli y compuertas $\mathrm{C-Not}$ es eficiente, mediante las reglas de conmutación ya presentadas. Se requiere, para cada generador, del orden de n operaciones clásicas para

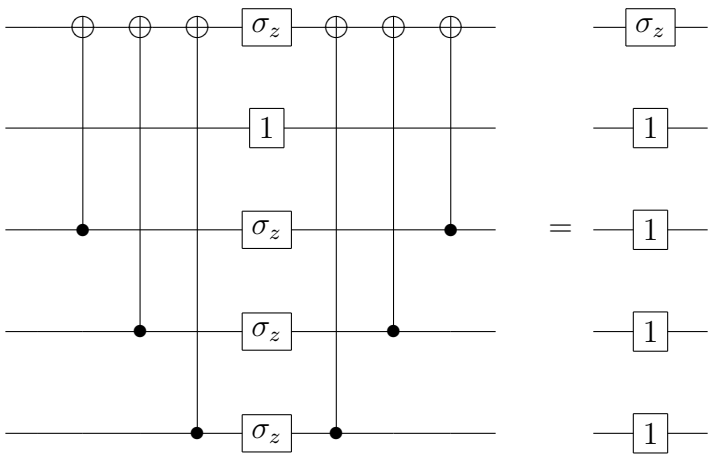

Figura B.2: Mediante la aplicación de compuertas C-Not puede llevarse un producto de operadores σ_z a un operador σ_z en el primer qubit.

determinar el resultado; es decir, n^2 operaciones para ver como transforma el grupo estailizador.

Dicho grupo estabilizador transformado poseerá operadores con identidades y σ_z en el primer qubit, cualquier otra opción violaría la propiedad abeliana del grupo. Por lo tanto existirá un subgrupo con identidades en el primer qubit que es simple de encontrar: se debe, a cada generador que no posee una identidad en el primer qubit, multiplicarlo por σ_{z_1}, donde el subíndice indica el qubit sobre el que actúa el operador en cuestión. Y debido a que σ_{z_1} también pertenece al grupo, el resultado será un generador del grupo con una identidad en el primer qubit. Sobre ese subgrupo que actúa sobre los últimos $n-1$ qubits, se repite el procedimiento para convertir un autoestado de uno de los operadores en autoestado de σ_{z_2}, y así sucesivamente hasta convertir a todos los generadores en operadores σ_z.

De esta forma, con n operadores unitarios como el descripto anteriormente, cada uno utilizando del orden de n compuertas cuánticas, se lleva un grupo estabilizador arbitrario al grupo de las Z. Es decir, se requieren del orden de n^2 operaciones fundamentales. Los recursos clásicos necesarios son del orden de n^3, puesto que para cada uno de los n circuitos que llevan un operador de los generadores a un operador σ_z en el primer qubit, se deben propagar n generadores por el circuito, requiriendo n operaciones clásicas cada uno; es decir n^3 operaciones clásicas para determinar el circuito.

Algoritmo de construcción del circuito de cambio de base

Se puede describir el algoritmo de construcción del circuito de cambio de base de manera recursiva mediante el algoritmo que se incluye a continuación. De acuerdo a las consideraciones anteriores:

- El procedimiento para generar el circuito recibe como parámetros la lista de generadores del grupo estabilizador y el primer qubit k.
- - Seleccionar algún generador $\sigma_x^{\vec{q}}\sigma_z^{\vec{p}}$ que no tenga la identidad en el qubit k.
  - Rotar todos los qubits hasta convertir el generador en cuestión en σ_z e identidades. Requiere del orden de n operaciones clásicas determinar las rotaciones correspondientes:

$$\bigotimes_{j=k}^{n} R_j\left(q_j, p_j\right) \tag{B.10}$$

  - Aplicar $\mathrm{C-Not}$ con control en cada qubit distinto del k que no tiene la identidad, y objetivo en el qubit k:

$$\prod_{j=k+1}^{n} \left(\mathrm{C-Not}\left(j,k\right)\right)^{\left(1-\delta_{q_j,0}\delta_{p_j,0}\right)} \tag{B.11}$$

  - Propagar los $n-1$ generadores restantes por el circuito descripto en los items anteriores. Requiere del orden de n^2 operaciones clásicas.
  - Multiplicar aquellos generadores que tienen al operador σ_z en el qubit k por σ_{z_k}.
  - Todos los generadores tienen una identidad en el primer qubit. Si $k \neq n$, llamar al procedimiento de generación del circuito con el grupo de generadores para los qubits $k+1$ al n y con $k+1$ como el primer qubit.

Una aclaración importante sobre el algoritmo es que, para comenzar, se debe generar la lista de generadores asociados a la matriz S y llamar al procedimiento con dicha lista y $k = 1$. No es conveniente que el procedimiento recursivo reciba como parámetro a la matriz S, porque podría suceder que alguno de los subgrupos de menor cantidad de qubits con los que se realice el llamado recursivo posea operadores σ_z, para los que no hay matriz S asociada.

Ejemplo

Supongamos que se quiere convertir el grupo estabilizador G en aquel estabilizado por los operadores σ_z, donde G está generado por:

$$G = \{\sigma_z \otimes \sigma_z \otimes 1, \sigma_z \otimes \sigma_y \otimes \sigma_z, 1 \otimes \sigma_z \otimes \sigma_y\} \tag{B.12}$$

Notemos que alcanza con dar 3 operadores, puesto que los demás son productos de ellos.

Dice el algoritmo anterior que, en primer lugar, debe tomarse el operador $\sigma_x \otimes \sigma_z \otimes 1$ y aplicar las tranformaciones correspondientes para llevar cada qubit a operadores σ_z para luego, mediante compuertas C-Not, llevar el operador a un operador σ_z sobre el primer qubit. Las rotaciones son simples, sólo aplicar H al primer qubit. En la Figura B.3 puede verse el circuito parcial.

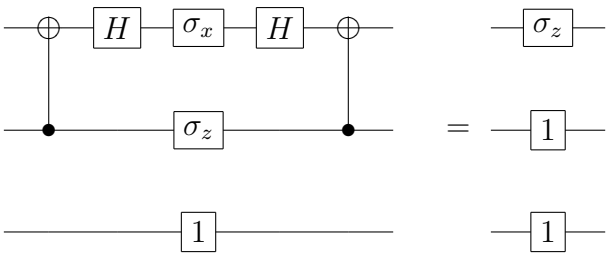

Figura B.3: Primera etapa del circuito de cambio de base.

El problema que surge es que el circuito de la Figura B.3 también modifica los demás operadores del estabilizador. Luego de aplicado el circuito, el estabilizador se convierte en:

$$G' = \{\sigma_z \otimes 1 \otimes 1, 1 \otimes \sigma_y \otimes \sigma_z, 1 \otimes \sigma_z \otimes \sigma_y\} \tag{B.13}$$

La segunda etapa del algoritmo debe tomar el operador $1 \otimes \sigma_y \otimes \sigma_z$ y transformarlo, mediante $\tilde{\tilde{U}}$, de la misma forma; pero puesto que dicho operador sólo aparece una vez realizada la transformación $\tilde{U}$ como imagen del operador $\sigma_z \otimes \sigma_y \otimes \sigma_z$, debe implementarse luego de ésta. Los pasos son los mismos, en primer lugar transformar la σ_y del segundo qubit en σ_z, y luego mediante un C-Not convertir la σ_z del tercero en una identidad, como se ve en la figura B.4.

Es importante notar que ésta segunda etapa no afecta al primer qubit, por lo que lo conseguido con la primera de llevar el primer operador a una

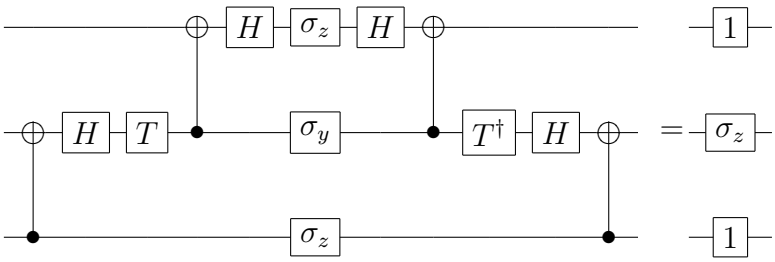

Figura B.4: Segunda etapa del circuito de cambio de base.

σ_z sobre el primer qubit se mantiene, mientras que se consigue, además, que el segundo operador se convierta en una σ_z del segundo qubit.

Nuevamente, esta modificación actúa sobre el tercer operador, por lo que nuevamente hay que ver como queda dicho operador luego de la segunda etapa. El grupo estabilizador queda, luego de la segunda etapa:

$$G'' = \{\sigma_z \otimes 1 \otimes 1, 1 \otimes \sigma_z \otimes 1, 1 \otimes 1 \otimes \sigma_y\} \tag{B.14}$$

Debe, para corregirse el tercer operador, aplicar una tranformación al tercer qubit. Dicho circuito se puede observar en la Figura B.5.

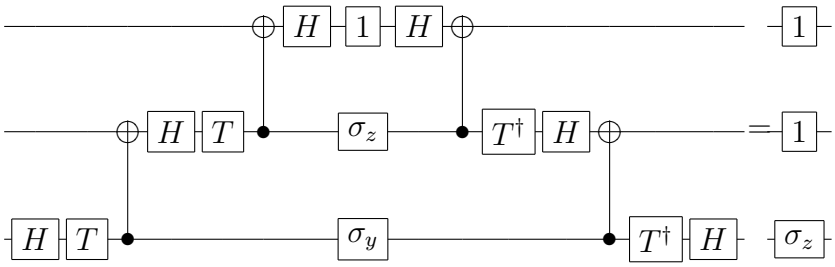

Figura B.5: Tercera etapa del circuito de cambio de base.

Por lo tanto, el circuito al que entra un autoestado del estabilizador G y sale un autoestado del grupo estabilizador de operadores σ_z es el ilustrado en la Figura B.6.

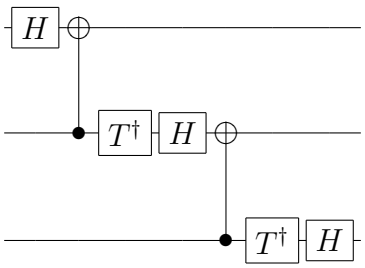

Figura B.6: Circuito de cambio de base. Convierte un autoestado del grupo estabilizador G en uno del grupo estabilizado por los operadores σ_z.

Apéndice C

Bases mutuamente no sesgadas y 2–diseños

En éste Apéndice probaremos que los conjuntos de bases mutuamente no sesgadas forman un 2–diseño de estados[KR05, Dan05, AE07]. Esta demostración, aunque no es original, es una de las piezas fundamentales de los protocolos de SEQPT y SEQPT sin ancilla de los Capítulos 3 y 4, por lo que vale la pena incluirla con este trabajo.

Para llegar a demostrar eso, pasaremos por varios resultados y definiciones intermedios. Es importante, sin embargo, no perder de vista que lo que queremos probar, en última instancia, es que los conjuntos de MUBs forman un 2–diseño.

C.1. t–diseños

Veremos ahora algunos resultados generales sobre t–diseños. Definiremos un t–diseño de la siguiente forma:

Definición C.1. *Una distribución de probabilidades sobre un conjunto de estados* $(p_i, |\phi_i\rangle)$ *es un* t*–diseño si*

$$\sum_i p_i \left(|\phi_i\rangle \langle\phi_i|\right)^{\otimes t} = \int_{\mathcal{H}} |\psi\rangle \langle\psi|^{\otimes t} \, d\psi. \tag{C.1}$$

Es fácil ver que si el t–diseño es uniforme (todos los p_i iguales) y $t = 2$, si multiplicamos por $A \otimes B$ y tomamos la traza, recuperamos el resultado

$$\frac{1}{|X|}\sum_i \langle\phi_i| A |\phi_i\rangle \langle\phi_i| B |\phi_i\rangle = \int_{\mathcal{H}} \langle\psi| A |\psi\rangle \langle\psi| B |\psi\rangle \, d\psi \tag{C.2}$$

donde $|X|$ es la cantidad de estados en el 2–diseño X.

Ahora demostraremos un lema técnico, y a continuación daremos los dos teoremas principales sobre 2–diseños y MUBs.

Lema C.2. *Sea $|x\rangle \in \mathcal{H}$. Se cumple que*

$$\int_{\mathcal{H}} |\langle x|\psi\rangle|^{2k} d\psi = \frac{1}{\binom{D+k-1}{k}} \tag{C.3}$$

donde la integral es en la medida invariante unitaria y normalizada de Haar, y $Dim(\mathcal{H}) = D$.

Demostración. En primer lugar, existe una transformación unitaria U tal que $U|1\rangle = |x\rangle$, donde $|1\rangle$ es un vector de la base canónica de $\mathcal{H}$[1]. Por lo tanto

$$\int_{\mathcal{H}} |\langle x|\psi\rangle|^{2k} d\psi = \int_{\mathcal{H}} \left|\langle 1| U^\dagger |\psi\rangle\right|^{2k} d\psi \tag{C.4}$$

$$= \int_{\mathcal{H}} |\langle 1|\psi\rangle|^{2k} \, d\psi \tag{C.5}$$

donde utilizamos la invariancia unitaria de la medida de Haar para llegar a la segunda igualdad.

Ahora recordemos que la medida de Haar integra sobre vectores que están en la superficie de una esfera unitaria en $\mathbb{C}^D$. Además, el $\langle 1|\psi\rangle$ que aparece en el integrando es una componente de un vector. Entonces intentaremos realizar esa integral en coordenadas esféricas[2].

Para realizar eso, veamos la siguiente integral sobre todo $\mathbb{C}^D$:

$$I = \int_{\mathbb{C}^D} \left|z_1^k\right|^2 e^{-|z|^2} dV_{\mathbb{C}^D} \tag{C.6}$$

donde $z = (z_1, z_2, \ldots, z_D)$. Esa integral es factorizable como

$$I = \int_{\mathbb{C}} \left|z_1^k\right|^2 e^{-|z_1|^2} dz_1 \prod_{j=2}^{D} \int_{\mathbb{C}} e^{-|z_j|^2} dz_j = \pi^D k!. \tag{C.7}$$

[1]En el contexto de información cuántica, hablar de base canónica y base computacional es equivalente.

[2]Eso es parecido a tener que integrar en $\mathbb{R}^3$ algo de la forma $\int x d\Omega$.

Además, la integral de la ecuación (C.6) se puede hacer en esféricas como

$$\pi^D k! = c_D 2D \int_0^\infty r^{2k+2D-1} e^{-r^2} dr \int_S \left|\sigma_1^k\right|^2 dS(\sigma) \tag{C.8}$$

donde S es la integral sobre la superficie de la esfera. Esa integral sobre la superficie de la esfera es la misma de la ecuación (C.5) que buscábamos.

$$\int_S \left|\sigma_1^k\right|^2 dS(\sigma) = \int_{\mathcal{H}} |\langle 1|\psi\rangle|^{2k} \, d\psi. \tag{C.9}$$

Integrando la parte radial de (C.8), se obtiene el resultado buscado.

□

Veremos ahora un teorema general sobre t–diseños, y luego la relación con los conjuntos de MUBs.

Teorema C.3. *Sea X un conjunto finito de $\mathcal{H}$. Entonces son equivalentes las siguientes proposiciones:*

1. *X es un t–diseño uniforme.*
2. *Para todo $|\psi\rangle \in \mathcal{H}$ y para todo $0 \leq k \leq t$ vale que*

$$\frac{\langle\psi|\psi\rangle^k}{\binom{k+D-1}{k}} = \frac{1}{|X|} \sum_{|\phi\rangle \in X} |\langle\phi|\psi\rangle|^{2k}. \tag{C.10}$$

3. *Para todo $0 \leq k \leq t$ vale que*

$$\frac{1}{|X|^2} \sum_{|\phi_i\rangle, |\psi_i\rangle \in X} |\langle\phi_i|\psi_i\rangle|^{2k} = \frac{1}{\binom{k+D-1}{k}} \tag{C.11}$$

Demostración. Comenzaremos por probar que (1) implica (2). Notemos que como $k \leq t$ y X es un t–diseño, entonces se tiene que

$$\frac{1}{|X|} \sum_{|\psi\rangle \in X} |\langle\psi|\phi\rangle|^{2k} = \int_{\mathcal{H}} |\langle\psi|\phi\rangle|^{2k} \, d\phi. \tag{C.12}$$

Usando ahora el lema C.2 y recordando que, ahora, el vector $|\psi\rangle$ no está normalizado, sale que

$$\frac{1}{|X|} \sum_{|\psi\rangle \in X} |\langle\psi|\phi\rangle|^{2k} = \frac{|\langle\psi|\psi\rangle|^k}{\binom{D+k-1}{k}}. \tag{C.13}$$

.

Que (2) implica (3) sale directo sumando la ecuación (C.13) sobre todos los estados normalizados de X.

Por último, tenemos que demostrar que (3) implica (1). Para eso vamos a usar que $\langle\psi|^{\otimes k}\,|\phi\rangle^{\otimes k} = \langle\psi|\phi\rangle^k$. Definimos el vector $|v\rangle$ como

$$|v\rangle = \frac{1}{|X|}\sum_{|\psi\rangle\in X}|\psi\rangle^{\otimes k}\otimes|\psi\rangle^{*\otimes k} - \int_{\mathcal{H}}|\psi\rangle^{\otimes k}\otimes|\psi\rangle^{*\otimes k}\,d\psi. \tag{C.14}$$

Si probamos que ese vector es el vector nulo usando (3), entonces podemos concluir que X es un t–diseño uniforme, como queríamos probar. Veamos la norma de $|v\rangle$:

$$\langle v|v\rangle = \frac{1}{|X|^2}\sum_{|\phi\rangle,|\psi\rangle\in X}|\langle\psi|\phi\rangle|^{2k} - \int_{\mathcal{H}}\int_{\mathcal{H}}|\langle\psi|\phi\rangle|^{2k}\,d\psi d\phi. \tag{C.15}$$

Usando (3), el lema C.2 para una de las integrales y la normalización de la medida de Haar para la otra se obtiene que

$$\begin{aligned}\langle v|v\rangle &= \frac{1}{\binom{D+k-1}{k}} - \int_{\mathcal{H}}\frac{1}{\binom{D+k-1}{k}}d\psi &\text{(C.16)}\\ &= \frac{1}{\binom{D+k-1}{k}} - \frac{1}{\binom{D+k-1}{k}} = 0. &\text{(C.17)}\end{aligned}$$

Con lo que finaliza la demostración. □

Ahora utilizaremos todos estos resultados para ver que un conjunto de MUBs es un 2–diseño.

C.2. MUBs y 2–diseños

Teorema C.4. *Los estados de un conjunto de $D+1$ bases mutuamente no sesgadas forman un 2–diseño.*

Demostración. La demostración es simple usando la propiedad (3) del Teorema C.3. Para $k=1$ tenemos que

$$\frac{1}{|X|^2}\sum_{J,m,J',m'}\left|\left\langle\psi_m^J|\psi_{m'}^{J'}\right\rangle\right|^{2k} = \frac{1}{D^2\,(D+1)^2}\left[2\binom{D+1}{2}D + \binom{D+1}{D}D\right]. \tag{C.18}$$

Por lo tanto

$$\frac{1}{|X|^2}\sum_{J,m,J',m'}\left|\left\langle\psi_m^J|\psi_{m'}^{J'}\right\rangle\right|^{2k}=\frac{1}{D}=\frac{1}{\binom{D+1-1}{1}}. \tag{C.19}$$

Para el caso $k=2$ es similar:

$$\frac{1}{|X|^2}\sum_{J,m,J',m'}\left|\left\langle\psi_m^J|\psi_{m'}^{J'}\right\rangle\right|^{2k}=\frac{1}{D^2\left(D+1\right)^2}\left[2\binom{D+1}{2}+\binom{D+1}{D}D\right], \tag{C.20}$$

y eso da

$$\frac{1}{|X|^2}\sum_{J,m,J',m'}\left|\left\langle\psi_m^J|\psi_{m'}^{J'}\right\rangle\right|^{2k}=\frac{2}{D\left(D+1\right)}=\frac{1}{\binom{D+2-1}{2}}. \tag{C.21}$$

Por lo tanto, como en el Teorema C.3 es equivalente la propiedad (3) que demostramos aquí para las MUBs a que el conjunto X sea un 2–diseño, probamos que las MUBs forman un 2–diseño. □

Sólo falta probar la relación (3.6) de la medida de Haar con las trazas que reproducimos a continuación

$$F\left(M,N\right)=\int_{\mathcal{H}}\left\langle\psi\right|M\left|\psi\right\rangle\left\langle\psi\right|N\left|\psi\right\rangle d\psi=\frac{\mathsf{tr}(M)\mathsf{tr}(N)+\mathsf{tr}(MN)}{D(D+1)} \tag{C.22}$$

donde M y N son dos operadores en $\mathcal{B}\left(\mathcal{H}\right)$ cualesquiera. Para demostrar eso, notemos que la ecuación anterior es una forma bilineal, simétrica frente al intercambio de M por N e invariante unitaria debido a la invariancia unitaria de la medida de Haar ($F\left(M,N\right)=F\left(UMU^{-1},UNU^{-1}\right)$ para todo operador U unitario). Dicho esto, veremos ahora un teorema general sobre formas bilineales simétricas e invariantes unitarias.

Teorema C.5. *Sea $F:\mathcal{B}\left(\mathcal{H}\right)\otimes\mathcal{B}\left(\mathcal{H}\right)\to\mathbb{C}$ una forma bilineal, simétrica ($F\left(M,N\right)=F\left(N,M\right)$) e invariante frente a transformaciones unitarias ($F\left(M,N\right)=F\left(UMU^{-1},UNU^{-1}\right)$), entonces vale que*

$$F\left(M,N\right)=d\mathrm{Tr}\left(MN\right)+q\mathrm{Tr}\left(M\right)\mathrm{Tr}\left(M\right) \tag{C.23}$$

Demostración. Veremos primero qué ocurre para operadores M y N de la base de operadores $\{|j\rangle\langle j|\}$. Vamos a dividir el problema en varios casos.

En primer lugar, supongamos que tomamos $M = |j\rangle\langle k|$ y $N = |l\rangle\langle m|$, y que uno de los cuatro número j, k, l o m es distinto a los otros tres. Tomaremos el caso $j \neq k$, $j \neq l$ y $j \neq m$, pero para los otros tres casos el procedimiento es el mismo. Consideremos el operador unitario $C_j = \mathbb{I} - 2|j\rangle\langle j|$. Usando la invariancia unitaria de F con C_j tenemos que

$$\begin{aligned} F(|j\rangle\langle k|, |l\rangle\langle m|) &= F\left(C_j|j\rangle\langle k|C_j^\dagger, C_j|l\rangle\langle m|C_j^\dagger\right) = & \text{(C.24)} \\ &= -F(|j\rangle\langle k|, |l\rangle\langle m|) = 0 & \text{(C.25)} \end{aligned}$$

donde la anteúltima igualdad proviene de la bilinealidad de F. Ya sabemos que en todos esos pares de operadores F da cero.

Los casos que quedan son los que no tienen ningún número de los j, k, l y m distinto a los otros tres. Esos casos son los que enumeramos a continuación

1. $M = |j\rangle\langle j|$ y $N = |k\rangle\langle k|$ con $k \neq j$.
2. $M = |j\rangle\langle k|$ y $N = |k\rangle\langle j|$ con $k \neq j$.
3. $M = |j\rangle\langle j|$ y $N = |j\rangle\langle j|$.
4. $M = |j\rangle\langle k|$ y $N = |j\rangle\langle k|$ con $k \neq j$.

Veamos el resultado uno por uno. En el caso 1, consideremos los operadores $S_{kl} = \mathbb{I} - |k\rangle\langle k| - |l\rangle\langle l| + |k\rangle\langle l| + |l\rangle\langle k|$. Tenemos que

$$\begin{aligned} F(|j\rangle\langle j|, |k\rangle\langle k|) &= F\left(S_{kl}|j\rangle\langle j|S_{kl}^\dagger, S_{kl}|k\rangle\langle k|S_{kl}^\dagger\right) = \\ &= F(|j\rangle\langle j|, |l\rangle\langle l|) = \\ &= F\left(S_{jm}|j\rangle\langle j|S_{jm}^\dagger, S_{jm}|l\rangle\langle l|S_{jm}^\dagger\right) \\ &= F(|m\rangle\langle m|, |l\rangle\langle l|). & \text{(C.26)} \end{aligned}$$

Por lo tanto, $F(|j\rangle\langle j|, |k\rangle\langle k|) = q$, con q independiente de j y k.

Para el caso 2, usando los mismos operadores S_{kl} y procediendo de la misma forma, puede verse que $F(|k\rangle\langle j|, |j\rangle\langle k|) = d$, con d independiente de j y k.

En el caso 3, utilizando también con los operadores S_{kl} de la misma forma, se obtiene que $F(|j\rangle\langle j|, |j\rangle\langle j|) = g$, con g independiente de j.

Por último, en el caso 4, consideremos el operador unitario $D_k = \mathbb{I} - |k\rangle\langle k| + i\,|k\rangle\langle k|$. Usando nuevamente la invariancia unitaria sale que

$$\begin{aligned} F\left(|j\rangle\langle k|, |j\rangle\langle k|\right) &= F\left(D_k\,|j\rangle\langle k|\,D_k^\dagger, D_k\,|j\rangle\langle k|\,D_k^\dagger\right) = & \text{(C.27)} \\ &= -F\left(|j\rangle\langle k|, |j\rangle\langle k|\right) = 0 & \text{(C.28)} \end{aligned}$$

Con esto ya tenemos todas las herramientas para estudiar el caso general. Escribimos los operadores generales M y N como

$$\begin{aligned} M &= \sum_{kl} \alpha_{kl}\,|k\rangle\langle l| & \text{(C.29)} \\ N &= \sum_{mn} \beta_{mn}\,|m\rangle\langle n|\,. & \text{(C.30)} \end{aligned}$$

Luego, tenemos que por la bilinealidad de F y con los resultados anteriors vale que

$$F\left(M,N\right) = \sum_{klmn} \alpha_{kl}\beta_{mn} F\left(|k\rangle\langle l|, |m\rangle\langle n|\right). \qquad \text{(C.31)}$$

De esa suma, sólo guardamos los términos que sobreviven por los casos anteriores. Luego

$$\begin{aligned} F\quad (M,N) &= g\textstyle\sum_k \alpha_{kk}\beta_{kk} + d\sum_{j\neq k}\alpha_{jk}\beta_{kj} + q\sum_{j\neq k}\alpha_{jj}\beta_{kk} = & \text{(C.32)} \\ &= (g-d-q)\textstyle\sum_k \alpha_{kk}\beta_{kk} + d\sum_{j,k}\alpha_{jk}\beta_{kj} + q\sum_{j,k}\alpha_{jj}\beta_{kk} = & \text{(C.33)} \\ &= (g-d-q)\textstyle\sum_k \alpha_{kk}\beta_{kk} + d\mathrm{Tr}\left(MN\right) + q\mathrm{Tr}\left(M\right)\mathrm{Tr}\left(N\right). & \text{(C.34)} \end{aligned}$$

Solo falta ver que la sumatoria que queda no puede ser invariante unitaria para todo par de operadores M y N. En efecto, si consideramos $M = \sigma_x$ y $N = \sigma_x$, tenemos que $\sum_k \alpha_{kk}\beta_{kk} = 0$. Pero si intentamos ver su invariancia unitaria frente al operador de Hadamard, veremos que no se anula. Por lo tanto, no es invariante unitario. Eso termina nuestra demostración:

$$F\left(M,N\right) = d\mathrm{Tr}\left(MN\right) + q\mathrm{Tr}\left(M\right)\mathrm{Tr}\left(M\right). \qquad \text{(C.35)}$$

□

Al teorema anterior, sólo falta agregarle los valores de las constanter d y q cuando F es la integral de la ecuación (C.22). Para eso usamos por un lado, la normalización de la medida de Haar, y por otro el hecho de que la

integral en la medida de Haar puede realizarse como el promedio sobre un 2–diseño. La normalización de la medida de Haar dice que

$$1 = \int_{\mathcal{H}} d\psi = \int_{\mathcal{H}} d\psi \, \langle\psi|\psi\rangle \, \langle\psi|\psi\rangle = F\left(\mathbb{I}, \mathbb{I}\right) = dD + qD^2. \tag{C.36}$$

Es decir, $d + qD = \frac{1}{D}$.

Ahora consideremos los proyectores sobre estados del 2–diseño $M = \left|\psi_m^J\right\rangle \left\langle\psi_m^J\right|$ y $N = \left|\psi_n^J\right\rangle \left\langle\psi_n^J\right|$ con $m \neq n$. Aqui tenemos que $F\left(M, N\right) = q$. Además, como la integral es el promedio sobre el 2–diseño, sale que

$$\begin{aligned} q &= F\left(M, N\right) \\ &= \frac{1}{D\left(D+1\right)} \sum_{Kq} \left\langle\psi_q^K|\psi_m^J\right\rangle \left\langle\psi_m^J|\psi_q^K\right\rangle \left\langle\psi_q^K|\psi_n^J\right\rangle \left\langle\psi_n^J|\psi_q^K\right\rangle \\ &= \frac{1}{D\left(\left(\, D+1\right)\right.} \sum_{K\neq J,q} \frac{1}{D^2} = \frac{1}{D\left(D+1\right)} \end{aligned} \tag{C.37}$$

Por lo tanto, se obtiene el resultado buscado para d y q, con lo que

$$F\left(M, N\right) = \int_{\mathcal{H}} \langle\psi| \, M \, |\psi\rangle \, \langle\psi| \, N \, |\psi\rangle \, d\psi = \frac{\mathsf{tr}(M)\mathsf{tr}(N) + \mathsf{tr}(MN)}{D(D+1)} \tag{C.38}$$

como queríamos demostrar.

Apéndice D

Demostración de propiedades para SEQPT

En éste apéndice demostraremos las propiedades 3.1 y 3.2 que son fundamentales para los protocolos de tomografía selectiva y eficiente de procesos, tanto con como sin ancilla.

Propiedad 3.1. *Sean un canal $\mathcal{E}$ que preserva traza y una base de operadores ortogonal $\mathcal{S} = \{E_k, k = 0, \ldots, D^2 - 1\}$ tal que $\mathrm{Tr}\left(E_m^\dagger E_n\right) = D\delta_{mn}$ y $E_0 = \mathbb{I}$. Entonces se cumple que*

$$\overline{F}\left(\mathcal{E}\right) = \frac{D\chi_{00} + 1}{D + 1}. \tag{D.1}$$

Demostración. Tenemos que

$$\overline{F}\left(\mathcal{E}\right) = \int_{\mathcal{H}} d\psi \sum_{mn} \chi_{mn} \left\langle \psi \right| E_m \left| \psi \right\rangle \left\langle \psi \right| E_n^\dagger \left| \psi \right\rangle .$$

Invirtiendo el orden de la suma y la integral, y utilizando la ecuación (3.6) junto con la ortogonalidad de la base se obtiene que

$$\overline{F}\left(\mathcal{E}\right) = \sum_{mn} \frac{\chi_{mn}}{D\left(D+1\right)} \left[\mathrm{Tr}E_m \mathrm{Tr}E_n^\dagger + \mathrm{Tr}\left(E_m E_n^\dagger\right)\right] \tag{D.2}$$

y usando la otogonalidad de la base $\mathcal{S}$ y que la misma contiene al operador $\mathbb{I}$ se obtiene que

$$\overline{F}\left(\mathcal{E}\right) = \frac{D\chi_{00} + \sum_m \chi_{mm}}{D + 1} \tag{D.3}$$

Ésta última relación vale para cualquier canal. Si nos limitamos a los canales que preservan traza tenemos que

$$D = \mathrm{Tr}\mathbb{I} = \mathrm{Tr}\mathcal{E}\left(\mathbb{I}\right) = \sum_{mn} \chi_{mn} \mathrm{Tr}\left(E_m E_n^\dagger\right) = D \sum_m \chi_{mm}$$

que insertándolo en la ecuación (D.3) da el resultado buscado:

$$\overline{F}\left(\mathcal{E}\right) = \frac{D\chi_{00} + 1}{D+1}.$$

□

Propiedad 3.2. *Sean un canal $\mathcal{E}$ que preserva traza, y una base de operadores ortogonal $\mathcal{S} = \{E_k, k = 0, \ldots, D^2 - 1\}$ tal que $\mathrm{Tr}\left(E_m^\dagger E_n\right) = D\delta_{mn}$ y $E_0 = \mathbb{I}$. Entonces se cumple que*

$$\overline{F}\left(\mathcal{E}_{ab}\right) = \frac{D\chi_{ab} + \delta_{ab}}{D+1} \tag{D.4}$$

donde $\mathcal{E}_{ab}\left(\rho\right) = \mathcal{E}\left(E_a^\dagger \rho E_b\right)$

Demostración. La demostración es parecida a la de la propiedad 3.1, salvo por algunos detalles. El uso de la ecuación (3.6) nos lleva a

$$\overline{F}\left(\mathcal{E}_{ab}\right) = \int_{\mathcal{H}} d\psi \left\langle\psi\right| \mathcal{E}_{ab}\left(\left|\psi\right\rangle\left\langle\psi\right|\right)\left|\psi\right\rangle = \sum_{mn} \frac{\chi_{mn}}{D\left(D+1\right)} \left[\mathrm{Tr}\left(E_m E_a^\dagger\right) \mathrm{Tr}\left(E_b E_n^\dagger\right) + \mathrm{Tr}\left(E_m E_a^\dagger E_b E_n^\dagger\right)\right]$$

Luego, usando la ortogonalidad de los operadores y la linealidad de la traza, se lo puede llevar a la forma

$$\overline{F}\left(\mathcal{E}_{ab}\right) = \sum_{mn} \frac{\chi_{mn}}{D\left(D+1\right)} \left(\delta_{am}\delta_{bn}\right) + \frac{1}{D(D+1)} \mathrm{Tr}\left[\mathcal{E}\left(E_a^\dagger E_b\right)\right]$$

Por último, como el canal preserva traza, se obtiene la expresión deseada:

$$\overline{F}\left(\mathcal{E}_{ab}\right) = \frac{D\chi_{ab} + \delta_{ab}}{D+1}. \tag{D.5}$$

□

Apéndice E

POVMs y Teorema de Neumark

Como fue mencionado varias veces, la medición más general que puede realizarse a un estado ρ está dada por los POVMs (Medición basada en operadores positivos). Esto es, dado un conjunto de operadores positivos $\{A_\mu\}$ tales que $\sum_\mu A_\mu = \mathbb{I}$, se puede diseñar un aparato que mida todos los valores medios de la forma $\mathrm{Tr}\,(\rho A_\mu)$. Dicho aparato realizará una medición proyectiva sobre el estado y un sistema auxiliar debidamente preparado.

No es trivial ver que todo conjunto de operadores $\{A_\mu\}$ pueda medirse, ni que toda medición proyectiva sobre un estado y un sistema auxiliar dé lugar a un conjunto con esas características. Eso es precisamente lo que viene a demostrar el Teorema de Neumark. Por tratarse de un teorema central para el Capítulo 8, incluíremos aquí una demostración del mismo.

Empezaremos por probar que dado un estado auxiliar ρ_A y una medición proyectiva dada por los proyectores $\{\Pi_\mu\}$ sobre el espacio $\mathcal{H}_S \otimes \mathcal{H}_A$ tal que $\sum_\mu \Pi_\mu = \mathbb{I}$, entonces para todo $\rho \in \mathcal{H}_S$, dicha medición proyectiva es equivalente a un POVM. En efecto, el resultado de realizar esa medición proyectiva es

$$\begin{aligned} \mathrm{Tr}\left((\rho_S \otimes \rho_A)\,\Pi_\mu\right) &= \mathrm{Tr}\left((\rho_S \otimes \mathbb{I})\,(\mathbb{I} \otimes \rho_A)\,\Pi_\mu\right) \\ &= \mathrm{Tr}_S\left(\rho_S \mathrm{Tr}_A\left((\mathbb{I} \otimes \rho_A)\,\Pi_\mu\right)\right) \end{aligned} \tag{E.1}$$

Definimos ahora el operador $A_\mu = \mathrm{Tr}_A\left((\mathbb{I} \otimes \rho_A)\,\Pi_\mu\right)$, que es positivo por ser la traza parcial de un operador positivo. Esos A_μ son los operadores

del POVM, y suman la identidad porque $\mathrm{Tr}\rho_A = 1$ y $\sum_\mu \Pi_\mu = \mathbb{I}$. Con eso terminamos la demostración en un sentido.

Ahora nos falta probar que dado un conjunto de operadores positivos A_μ cuya suma es la identidad, se lo puede implementar como un POVM mediante una medición proyectiva sobre el sistema y una ancilla debidamente preparada. Para eso, haremos la siguiente observación. Como los operadores A_μ son positivos, entonces son diagonalizables como $A_\mu = \sum_b \left|\tilde{\psi}_b^\mu\right\rangle \left\langle\tilde{\psi}_b^\mu\right|$, donde los vectores de la suma no están normalizados. Sea $\left\{\left|\tilde{\psi}_a\right\rangle\right\}$ el conjunto de todos los vectores $\left|\tilde{\psi}_b^\mu\right\rangle$ correspondientes todos los operadores A_μ, entonces si se pueden medir todos los valores medios de la forma

$$\mathrm{Tr}\left(\rho_S \left|\tilde{\psi}_a\right\rangle \left\langle\tilde{\psi}_a\right|\right), \tag{E.2}$$

combinando sus resultados, se pueden medir todos los valores medios de la forma $\mathrm{Tr}\left(\rho_S A_\mu\right)$. De esta forma podemos probar el teorema de Neumark sólo para operadores positivos de dimensión 1 sin perder generalidad.

Dicho esto, consideremos un POVM formado por los operadores $F_a = \left|\tilde{\psi}_a\right\rangle \left\langle\tilde{\psi}_a\right|$ con $a = 1, \ldots, m$. Consideremos, además, una ancilla preparada en el estado $\rho_A = \sum_b p_b \left|b\right\rangle \left\langle b\right|$, donde $p_b = \left\langle\tilde{\psi}_b|\tilde{\psi}_b\right\rangle$ y $\{|\psi_b\rangle\}$ es una base ortonormal del espacio $\mathcal{H}_A$. Si se miden a dicho estado conjunto los proyectores $\left|\psi_a\right\rangle \left\langle\psi_a\right| \otimes \left|a\right\rangle \left\langle a\right|$ se obtiene que

$$\mathrm{Tr}\left(\left(\rho_S \otimes \sum_b p_b \left|b\right\rangle \left\langle b\right|\right) \left|\psi_a\right\rangle \left\langle\psi_a\right| \otimes \left|a\right\rangle \left\langle a\right|\right) = \mathrm{Tr}\left(\rho_S \left|\tilde{\psi}_a\right\rangle \left\langle\tilde{\psi}_a\right|\right) \tag{E.3}$$

que es el resultado buscado. Eso termina la demostración del teorema de Neumark.

Agradecimientos

Quiero agradecer a todos los que de una forma u otra formaron parte de todos estos años de trabajo de doctorado.

En primer lugar mi agradecimiento es a Juan Pablo por su dirección y orientación durante todos estos años. Y también a todos los docentes que fueron fundamentales durante mi formación.

Quiero agradecer también a todos los que, de manera más directa, participaron de esta tesis: Marcelo Terra Cunha, Fernando Pastawski, Miguel Larotonda, Cecilia López, David Cory, Christian Schmiegelow y Rafael Grimson.

Pero este doctorado tuvo también una gran parte que no figura en los papeles y que tiene que ver con la gente que me acompañó durante estos años. En especial, todo mi agradecimiento para mi familia: Eduardo, Violeta, Lila, Pablo, Karina y para los flamantes Matías y Julieta, que me llenaron de alegría los últimos meses de doctorado.

Además hubo montones de amigos que siempre estuvieron cerca, y que hicieron que pueda pasarla tan bien durante todos estos años. No estaría bien dejar de nombrar a Fer, el Tano, Cor, Andre, Ale, Fromer, Marzop, Pablo, Lute, Diego, Chochi, Vale, Christian, Denise, Juan y Fontana. Y también amigos de la facultad y gente que pasó por el grupo, Christian (otro agradecimiento más), Augusto, Ceci, Leo, Diana, Bruno y todos los que alguna vez fueron a las quantum drunken.

También quiero agradecer a todos los que hicieron que me sienta como en casa en cada viaje a Brasil. Por un lado, y en especial, a la familia de São Paulo, Daniel, Pequi, Julián, Yamila, Sandra, Carlos, Anita y Marianito. Y por el otro, a todos los amigos entrañables que fui cosechando por allá. A todos los que fui conociendo en los dos Paratys; a todos los chicos del grupo de Rio, especialmente a Gabo, Osvaldo, Bruno y Adriana; y a toda la banda mineira, a los que están en el chat(o) que fueron una presencia inagotable desde mi viaje a Belo Horizonte, y a todos los amigos que fui haciendo y con los que compartí tanto en ese viaje. Pero quiero nombrar, especialmente, a algunos amigos que hicieron que esos viajes sean inolvidables y que me den ganas de volver a visitarlos: Júlia, Pablo, Léo, Gabi y Mónica.

A todos ellos, mi enorme agradecimiento.

Bibliografía

[ABJ+03] J. B. Altepeter, D. Branning, E. Jeffrey, T. C. Wei, P. G. Kwiat, R. T. Thew, J. L. O'Brien, M. A. Nielsen, and A. G. White. Ancilla-assisted quantum process tomography. *Phys. Rev. Lett.*, 90(19):193601, May 2003.

[ABO97] D. Aharonov and M. Ben-Or. Fault-tolerant quantum computation with constant error. pages 176–188, 1997.

[AE07] Andris Ambainis and Joseph Emerson. Quantum t-designs: t-wise independence in the quantum world. In *IEEE Conference on Computational Complexity'07*, pages 129–140, 2007.

[AM06a] Leandro Aolita and Florian Mintert. Measuring multipartite concurrence with a single factorizable observable. *Phys. Rev. Lett.*, 97(5):050501, Aug 2006.

[AM06b] Leandro Aolita and Florian Mintert. Measuring multipartite concurrence with a single factorizable observable. *Phys. Rev. Lett.*, 97(5):050501, Aug 2006.

[Ba05] Fernando G. S. L. Brandão. Quantifying entanglement with witness operators. *Phys. Rev. A*, 72(2):022310, Aug 2005.

[BAH+10] R. C. Bialczak, M. Ansmann, M. Hofheinz, E. Lucero, M. Neeley, A. D. O/'Connell, D. Sank, H. Wang, J. Wenner, M. Steffen, A. N. Cleland, and J. M. Martinis. Quantum process tomography of a universal entangling gate implemented with josephson phase qubits. *Nat Phys*, 6(6):409–413, June 2010.

[BB84] C H Bennett and G Brassard. *Quantum cryptography: Public key distribution and coin tossing*, volume 175, pages 175–179. Bangalore, India, 1984.

[BB96] P. W. Brouwer and C. W. J. Beenakker. Diagrammatic method of integration over the unitary group, with applications to quantum transport in mesoscopic systems. *J.Math.Phys.*, 37:4904, 1996.

[BBBV97] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh V. Vazirani. Strengths and weaknesses of quantum computing. *SIAM J. Comput.*, 26(5):1510–1523, 1997.

[BBRV02] Somshubhro Bandyopadhyay, P. Oscar Boykin, Vwani P. Roychowdhury, and Farrokh Vatan. A new proof for the existence of mutually unbiased bases. *Algorithmica*, pages 512–528, 2002.

[BDSW96] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters. Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 54(5):3824–3851, Nov 1996.

[Ben06a] Ariel Bendersky. Conjuntos de Bases Mutuamente No Sesgadas y Sus Aplicaciones. Master's thesis, Universidad de Buenos Aires, Argentina, 2006.

[Ben06b] Ingemar Bengtsson. Three ways to look at mutually unbiased bases. *Foundations*, (October):18, 2006.

[BHT98] Gilles Brassard, Peter Høyer, and Alain Tapp. Quantum counting. In *In Proceedings of 25th ICALP, volume 1443 of lecture*, pages 820–831. Springer, 1998.

[BPC09] Ariel Bendersky, Juan Pablo Paz, and Marcelo Terra Cunha. General theory of measurement with two copies of a quantum state. *Phys. Rev. Lett.*, 103(4):040404, Jul 2009.

[BPP08] Ariel Bendersky, Fernando Pastawski, and Juan Pablo Paz. Selective and efficient estimation of parameters for quantum process tomography. *Phys. Rev. Lett.*, 100(19):190403, May 2008.

[BPP09] Ariel Bendersky, Fernando Pastawski, and Juan Pablo Paz. Selective and efficient quantum process tomography. *Phys. Rev. A*, 80(3):032116, Sep 2009.

[BRKSS07] Gunnar Björk, José L. Romero, Andrei B. Klimov, and Luis L. Sánchez-Soto. Mutually unbiased bases and discrete wigner functions. *J. Opt. Soc. Am. B*, 24(2):371–378, Feb 2007.

[BSS+10] Irene Bongioanni, Linda Sansoni, Fabio Sciarrino, Giuseppe Vallone, and Paolo Mataloni. Experimental quantum process tomography of non-trace-preserving maps. *Phys. Rev. A*, 82:042307, Oct 2010.

[BV93] Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. In *in Proc. 25th Annual ACM Symposium on Theory of Computing, ACM*, pages 11–20, 1993.

[BW08] Stephen Brierley and Stefan Weigert. Maximal sets of mutually unbiased quantum states in dimension 6. *Phys. Rev. A*, 78(4):042312, Oct 2008.

[Che52] H. Chernoff. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *Ann. Math. Stat.*, 23:493–507, 1952.

[Cho75] M Choi. Completely positive linear maps on complex matrices. *October*, 10(3):285–290, 1975.

[Cho07] Jaeyoon Cho. Fault-tolerant linear optics quantum computation by error-detecting quantum state transfer. *Phys. Rev. A*, 76:042311, Oct 2007.

[CKW00] Valerie Coffman, Joydip Kundu, and William K. Wootters. Distributed entanglement. *Phys. Rev. A*, 61(5):052306, Apr 2000.

[CMB04] André R. R. Carvalho, Florian Mintert, and Andreas Buchleitner. Decoherence and multipartite entanglement. *Phys. Rev. Lett.*, 93(23):230501, Dec 2004.

[CPF+10] M. Cramer, M.B. Plenio, S.T. Flammia, R. Somma, D. Gross, S.D. Bartlett, O. Landon-Cardinal, D. Poulin, and Y.-K. Liu. Efficient quantum state tomography. *Nature Comm.*, 1:149, 2010.

[cY93] Andrew Chi chih Yao. Quantum circuit complexity, 1993.

[Dan05] Christoph Dankert. Efficient Simulation of Random Quantum States and Operators. Master's thesis, University of Waterloo, Canada, 2005.

[DBbuE98] R. Derka, V. Buz˘ek, and A. K. Ekert. Universal algorithm for optimal estimation of quantum states from finite ensembles via realizable generalized measurement. *Phys. Rev. Lett.*, 80(8):1571–1575, Feb 1998.

[DCEL09] Christoph Dankert, Richard Cleve, Joseph Emerson, and Etera Livine. Exact and approximate unitary 2-designs and their application to fidelity estimation. *Phys. Rev. A*, 80(1):012304, Jul 2009.

[Deu85] David Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. *Proceedings of the Royal Society (London)*, 400:97–117, 1985.

[DGS77] P. Delsarte, J. M. Goethals, and J. J. Seidel. Spherical codes and designs. *Geometriae Dedicata*, 6:363–388, 1977.

[DJ92] D Deutsch and R Jozsa. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society A Mathematical Physical and Engineering Sciences*, 439(1907):553–558, 1992.

[DPS04] G. M. D'Ariano, P. Perinotti, and M. F. Sacchi. Quantum universal detectors. *EPL (Europhysics Letters)*, 65(2):165, 2004.

[DS96] David P. DiVincenzo and Peter W. Shor. Fault-Tolerant Error Correction with Efficient Quantum Codes. *Physical Review Letters*, 77(15):3260–3263, October 1996.

[EAO+02] Artur K. Ekert, Carolina Moura Alves, Daniel K. L. Oi, Michał Horodecki, Paweł Horodecki, and L. C. Kwek. Direct estimations of linear and nonlinear functionals of a quantum state. *Phys. Rev. Lett.*, 88(21):217901, May 2002.

[EAZ05] Joseph Emerson, Robert Alicki, and Karol Zyczkowski. Scalable noise estimation with random unitary operators. *Quantum Semiclass. Opt.*, 7:S347, 2005.

[ECR+07] Gregory S Engel, Tessa R Calhoun, Elizabeth L Read, Tae-Kyu Ahn, Tomás Mancal, Yuan-Chung Cheng, Robert E Blankenship, and Graham R Fleming. Evidence for wavelike energy transfer through quantum coherence in photosynthetic systems. *Nature*, 446(7137):782–786, 2007.

[ESM+07] Joseph Emerson, Marcus Silva, Osama Moussa, Colm Ryan, Martin Laforest, Jonathan Baugh, David G. Cory, and Raymond Laflamme. Symmetrized Characterization of Noisy Quantum Processes. *Science*, 317(5846):1893–1896, September 2007.

[Fey82] Richard Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6):467–488, June 1982.

[GHW04] Kathleen S. Gibbons, Matthew J. Hoffman, and William K. Wootters. Discrete phase space based on finite fields. *Phys. Rev. A*, 70:062101, 2004.

[GLF+10] David Gross, Yi-Kai Liu, Steven T. Flammia, Stephen Becker, and Jens Eisert. Quantum state tomography via compressed sensing. *Phys. Rev. Lett.*, 105(15):150401, Oct 2010.

[Got96] Daniel Gottesman. Class of quantum error-correcting codes saturating the quantum hamming bound. *Phys. Rev. A*, 54(3):1862–1868, Sep 1996.

[Got97] D. Gottesman. *Stabilizer Codes and Quantum Error Correction*. PhD thesis, California Institute of Technology, 1997.

[Got98] D. Gottesman. The Heisenberg Representation of Quantum Computers. *ArXiv Quantum Physics e-prints*, July 1998.

[Got00] D. Gottesman. An Introduction to Quantum Error Correction. *ArXiv Quantum Physics e-prints*, April 2000.

[Got09] Daniel Gottesman. An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation. April 2009.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *ANNUAL ACM SYMPOSIUM ON THEORY OF COMPUTING*, pages 212–219. ACM, 1996.

[HHH96] Michal Horodecki, Pawel Horodecki, and Ryszard Horodecki. Separability of mixed states: necessary and sufficient conditions. *Physics Letters A*, 223(1-2):1 – 8, 1996.

[HHHH09] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81(2):865–942, Jun 2009.

[HW97] Scott Hill and William K. Wootters. Entanglement of a pair of quantum bits. *Phys. Rev. Lett.*, 78(26):5022–5025, Jun 1997.

[Jam72] A Jamiolkowski. Completely positive linear maps on complex matrices. *Rep. Math. Phys.*, 3:275, 1972.

[KR05] A. Klappenecker and M. Roetteler. Constructions of mutually unbiased bases . In *Proceedings of the IEEE International Symposium on Information Theory*, pages 1740–1744, 2005.

[LBPC10] Cecilia C. López, Ariel Bendersky, Juan Pablo Paz, and David G. Cory. Progress toward scalable tomography of quantum maps using twirling-based methods and information hierarchies. *Phys. Rev. A*, 81(6):062113, Jun 2010.

[LLC09] Cecilia C. López, Benjamin Lévi, and David G. Cory. Error characterization in quantum information processing: A protocol for analyzing spatial correlations and its experimental implementation. *Phys. Rev. A*, 79(4):042328, Apr 2009.

[LLEC07] Benjamin Lévi, Cecilia C. López, Joseph Emerson, and D. G. Cory. Efficient error characterization in quantum information processing. *Phys. Rev. A*, 75(2):022314, Feb 2007.

[LPT98] J. I. Latorre, P. Pascual, and R. Tarrach. Minimal optimal generalized quantum measurements. *Phys. Rev. Lett.*, 81(7):1351–1354, Aug 1998.

[Ló09] C. C. López. *Scalable approaches to the characterization of open quantum system dynamics*. PhD thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, 2009.

[Mel90] P. A. Mello. Averages on the unitary group and applications to the problem of disordered conductors. *Journal of Physics A: Mathematical and General*, 23(18):4061+, September 1990.

[MKH+09] T. Monz, K. Kim, W. Hänsel, M. Riebe, A. S. Villar, P. Schindler, M. Chwalla, M. Hennrich, and R. Blatt. Realization of the quantum toffoli gate with trapped ions. *Phys. Rev. Lett.*, 102:040501, Jan 2009.

[ML06] M. Mohseni and D. A. Lidar. Direct characterization of quantum dynamics. *Phys. Rev. Lett.*, 97(17):170501, Oct 2006.

[MP95] S. Massar and S. Popescu. Optimal extraction of information from finite quantum ensembles. *Phys. Rev. Lett.*, 74(8):1259–1263, Feb 1995.

[MPS+02] Cesar Miquel, Juan P. Paz, Marcos Saraceno, Emanuel Knill, Raymond Laflamme, and Camille Negrevergne. Interpretation of tomography and spectroscopy as dual forms of quantum computation. *Nature*, 418(6893):59–62, July 2002.

[MRL08] M. Mohseni, A. T. Rezakhani, and D. A. Lidar. Quantum-process tomography: Resource analysis of different strategies. *Phys. Rev. A*, 77(3):032322, Mar 2008.

[MSS05] Frédéric Magniez, Miklos Santha, and Mario Szegedy. Quantum algorithms for the triangle problem. In *Proceedings of SODA'05*, pages 1109–1117, 2005.

[NAB+08] Matthew Neeley, M. Ansmann, Radoslaw C. Bialczak, M. Hofheinz, N. Katz, Erik Lucero, A. O/'Connell, H. Wang, A. N. Cleland, and John M. Martinis. Process tomography of quantum memory in a josephson-phase qubit coupled to a two-level state. *Nat Phys*, 4(7):523–526, July 2008.

[NC04] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information (Cambridge Series on Information and the Natural Sciences)*. Cambridge University Press, 1 edition, January 2004.

[ND05] Michael A. Nielsen and Christopher M. Dawson. Fault-tolerant quantum computation with cluster states. *Phys. Rev. A*, 71:042323, Apr 2005.

[NP09] Hui Khoon Ng and John Preskill. Fault-tolerant quantum computation versus gaussian noise. *Phys. Rev. A*, 79:032318, Mar 2009.

[OV06] Tobias J. Osborne and Frank Verstraete. General monogamy inequality for bipartite qubit entanglement. *Phys. Rev. Lett.*, 96(22):220503, Jun 2006.

[Pas08] Fernando Pastawski. Tomografía de Procesos Cuánticos. Master's thesis, Universidad Nacional de Córdoba, Argentina, 2008.

[Per95] Asher Peres. *Quantum Theory: Concepts and Methods*. 1995.

[Per96] Asher Peres. Separability criterion for density matrices. *Phys. Rev. Lett.*, 77(8):1413–1415, Aug 1996.

[PŘ04a] M. Paris and J. Řeháček. *Quantum state estimation*. Lecture notes in physics. Springer, 2004.

[PR04b] Arthur O. Pittenger and Morton H. Rubin. Mutually unbiased bases, generalized spin matrices and separability. *Linear Algebra and its Applications*, 390:255 – 278, 2004.

[Pre98] John Preskill. Quantum information and computation, June 1998.

[PRS05] Juan Pablo Paz, Augusto José Roncaglia, and Marcos Saraceno. Qubits in phase space: Wigner-function approach to quantum-error correction and the mean-king problem. *Phys. Rev. A*, 72(1):012309, Jul 2005.

[RBKSC04] Joseph M. Renes, Robin Blume-Kohout, A. J. Scott, and Carlton M. Caves. Symmetric informationally complete quantum measurements. *J. Math. Phys.*, 45:2171, 2004.

[RBKSS05] J. L. Romero, G. Björk, A. B. Klimov, and L. L. Sánchez-Soto. Structure of the sets of mutually unbiased bases for n qubits. *Phys. Rev. A*, 72(6):062310, Dec 2005.

[Sam80] Stuart Samuel. U(N) integrals, $1/N$, and the De Wit-'t Hooft anomalies. *J. Math. Phys.*, 21(12):2695–2703, dec 1980.

[SBLP11] Christian Tomás Schmiegelow, Ariel Bendersky, Miguel Antonio Larotonda, and Juan Pablo Paz. Selective and efficient quantum process tomography without ancilla. *Phys. Rev. Lett.*, 107:100502, Sep 2011.

[Sch11] Christian Schmiegelow. *Photonic Experiments on Selective Efficient Quantum Process Tomography*. PhD thesis, Universidad de Buenos Aires, 2011.

[Sho99] P. W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Review*, 41:303–332, January 1999.

[SIFW10] Mohan Sarovar, Akihito Ishizaki, Graham R. Fleming, and K. Birgitta Whaley. Quantum entanglement in photosynthetic light harvesting complexes. *Nature Physics*, 6:462, 2010.

[SL09] Alireza Shabani and Daniel A. Lidar. Vanishing quantum discord is necessary and sufficient for completely positive maps. *Phys. Rev. Lett.*, 102(10):100402, Mar 2009.

[SLP10] Christian Tomás Schmiegelow, Miguel Antonio Larotonda, and Juan Pablo Paz. Selective and efficient quantum process tomography with single photons. *Phys. Rev. Lett.*, 104(12):123601, Mar 2010.

[SoQT83] Effects States and Operations Fundamental Notions of Quantum Theory. *Quantum state estimation*. Lecture notes in physics. Springer, 1983.

[Ved02] V. Vedral. The role of relative entropy in quantum information theory. *Rev. Mod. Phys.*, 74(1):197–234, Mar 2002.

[VLPT99] G. Vidal, J. I. Latorre, P. Pascual, and R. Tarrach. Optimal minimal measurements of mixed states. *Phys. Rev. A*, 60(1):126–135, Jul 1999.

[Wat09] John Watrous. *Encyclopedia of Complexity and Systems Science, Quantum Computational Complexity.* Springer New York, 2009.

[WGP+07] Andrew G. White, Alexei Gilchrist, Geoffrey J. Pryde, Jeremy L. O'Brien, Michael J. Bremner, and Nathan K. Langford. Measuring two-qubit gates. *J. Opt. Soc. Am. B*, 24(2):172–183, Feb 2007.

[Wik11a] Wikipedia. Cauchy–schwarz inequality — Wikipedia, the free encyclopedia, 2011. [Online; accessed 16-August-2011].

[Wik11b] Wikipedia. Central limit theorem — Wikipedia, the free encyclopedia, 2011. [Online; accessed 16-August-2011].

[Wik11c] Wikipedia. Chernoff bound — Wikipedia, the free encyclopedia, 2011. [Online; accessed 16-August-2011].

[Wik11d] Wikipedia. Choi's theorem on completely positive maps — Wikipedia, the free encyclopedia, 2011. [Online; accessed 16-August-2011].

[Woo98] William K. Wootters. Entanglement of formation of an arbitrary state of two qubits. *Phys. Rev. Lett.*, 80(10):2245–2248, Mar 1998.

[Woo04] W. K. Wootters. Picturing qubits in phase space. *IBM J. Res. Dev.*, 48:99–110, January 2004.