

Tomografía de Procesos Cuánticos,  
un ejemplo motivante del uso de operadores aleatorios

Fernando Pastawski

*Director:* Juan Pablo Paz

*Codirector/Representante Local:* Omar Osenda

13 de febrero de 2008

## **Resumen**

La caracterización de la dinámica de sistemas cuánticos es uno de los problemas claves que debe sortear la computación cuántica para ser viable. Este problema, consiste en identificar y cuantificar los factores que actúan en una dinámica cuántica de una manera sistemática y se denomina tomografía de procesos cuánticos. En este trabajo, se hace un repaso de distintos métodos propuestos en la literatura para la caracterización de procesos cuánticos, para luego, en este contexto, dar propuestas superadoras. En particular, se presentan herramientas tales como la introducción intencional de aleatoriedad, los 2-diseños y las bases mutuamente no sesgadas; se demuestra su valor para la comprensión y creación de algoritmos tomográficos. Como resultado, se proponen algoritmos tomográficos novedosos, capaces de estimar coeficientes tomográficos de manera selectiva y eficiente.

### **Clasificación**

Física cuántica

Computación cuántica

Información cuántica

Medición cuántica

Diseño experimental

# Índice

<b>1. Introducción</b>	<b>1</b>
1.1. Marco y motivación . . . . .	1
1.2. Aleatoriedad . . . . .	1
1.3. Estructuración del trabajo . . . . .	2
<b>2. Canales y Operadores Cuánticos</b>	<b>5</b>
2.1. Representación de Kraus . . . . .	6
2.2. Representación con matriz chi ( $\chi$ ) . . . . .	7
2.3. Representación con matriz lambda ( $\lambda$ ) . . . . .	9
<b>3. Métodos para la tomografía de procesos cuánticos</b>	<b>11</b>
3.1. Tomografía cuántica de estados . . . . .	11
3.2. Tomografía estándar de procesos cuánticos . . . . .	13
3.2.1. Resumen y perspectivas . . . . .	13
3.3. Tomografía de procesos cuánticos asistida por ancila . . . . .	14
3.3.1. Resumen y perspectivas . . . . .	15
3.4. Caracterización directa de dinámicas cuánticas . . . . .	16
3.4.1. Caracterización de coeficientes diagonales (poblaciones) . . . . .	16
3.4.2. Condición de preservar traza en la base de Pauli . . . . .	17
3.4.3. Medición de coeficientes no diagonales (coherencias) . . . . .	18
3.4.4. Medición en sistemas de $N$ qubits . . . . .	20
3.4.5. Resumen y perspectivas . . . . .	20
3.5. Caracterización de procesos ruidosos simetrizados . . . . .	21
3.5.1. Resumen y perspectivas . . . . .	26
3.6. Comparación y nuevas metas . . . . .	26
<b>4. Tomografía selectiva de procesos cuánticos</b>	<b>27</b>
4.1. Una base de operadores conveniente . . . . .	27
4.2. Algunos promedios sobre el espacio de Hilbert . . . . .	29
4.3. Representación circuital . . . . .	32
4.3.1. Circuito para coeficientes diagonales de chi . . . . .	32
4.3.2. Circuito para coeficientes no diagonales de chi . . . . .	33
4.4. Estimadores en términos de fidelidades . . . . .	36
4.5. Medición de fidelidad . . . . .	36
4.5.1. Utilizar DCQD o SCNQP para medir fidelidades medias . . . . .	36
4.5.2. Usar 2-diseños de estados para medir fidelidades medias . . . . .	37

<b>5. <math>t</math>-diseños y Bases Mutuamente no Sesgadas</b>	<b>40</b>
5.1. Introducción a los $t$ -diseños . . . . .	40
5.2. Cuatro definiciones de $t$ -diseños . . . . .	41
5.3. Bases mutuamente no sesgadas (MUBs) . . . . .	44
5.4. MUBs y bases maximales de unitarios conmutativos . . . . .	48
<b>6. Bases mutuamente no sesgadas eficientes</b>	<b>49</b>
6.1. Operadores de Heisenberg-Weyl generalizados . . . . .	49
6.2. Formalismo de estabilizadores . . . . .	50
6.3. Cuerpos finitos y polinomio primitivo . . . . .	53
6.4. Matriz compañera . . . . .	54
6.5. Aplicación a MUBs estabilizadas . . . . .	55
6.6. Construcción del estado $ \psi_{\mathbf{J},\mathbf{k}}\rangle$ . . . . .	57
<b>7. Tomografía diagonal de procesos cuánticos</b>	<b>59</b>
7.1. Dando significado a otros estados finales . . . . .	59
7.2. Medición simultanea de todos los coeficientes $\chi_{mm}$ . . . . .	61
7.3. Mejorar el procesamiento clásico de mediciones . . . . .	62
7.3.1. Estimar un $\chi_{mm}$ . . . . .	63
7.3.2. Detectar y medir todos los $\chi_{mm}$ grandes . . . . .	63
7.3.3. Eficiencia relativo a $\epsilon$ , $\delta$ , $P$ y $N$ . . . . .	67
7.4. Medición simultanea de coeficientes no diagonales de $\chi$ . . . . .	68
<b>8. Conclusiones</b>	<b>71</b>
8.1. Resumen de resultados . . . . .	71
8.2. Perspectivas a futuro . . . . .	72
<b>A. Operaciones y circuitos cuánticos</b>	<b>73</b>
A.1. Operadores de Pauli . . . . .	73
A.2. Operadores de Clifford . . . . .	73
A.3. Operadores controlados . . . . .	74
<b>B. Algunas demostraciones</b>	<b>76</b>
B.1. MUBs y bases maximales de unitarios conmutativos (Demostraciones) . . . . .	76

# 1. Introducción

## 1.1. Marco y motivación

El área de información y computación cuántica es un campo multidisciplinario que busca entender y controlar el procesamiento de información en el contexto de las leyes de la mecánica cuántica [NC00]. Algunas de las áreas en las que la información cuántica ya está mostrando aplicaciones tecnológicas son la generación de números aleatorios y la criptografía cuántica. En el área de algoritmos, los modelos de computación cuántica permitirían implementar el algoritmo de factorización de Peter Shor o simulaciones de sistemas cuánticos naturales. Estas son algunas de las metas que motivan los desarrollos tecnológicos necesarios para la construcción de computadoras cuánticas.

No obstante, el ruido y la decoherencia en los sistemas cuánticos parece ser uno de los principales obstáculos para la construcción de sistemas capaces de controlar un gran número de qubits por periodos largos, condición que sería necesaria para el cómputo cuántico. Se han diseñado códigos correctores de errores y representaciones de circuitos cuánticos resistentes a fallas que serían capaces de contener la propagación descontrolada de errores [Got97]. Pero antes de poder aplicar estos métodos, es necesario reducir el ruido a un nivel aceptable, denominado *fault tolerance threshold*. Es aquí donde aparece el problema de tomografía de procesos cuánticos. De manera maniquea, se puede decir que la caracterización de los procesos cuánticos, es responsable de discernir entre tres situaciones:

- No hay errores significativos (se tiene un espacio libre de decoherencia).
- Hay pocos errores con peso significativo, los cuales podrán corregirse con códigos correctores.
- Hay muchos errores con peso significativo y debe evitarse codificar información en los subespacios afectados.

Permitirá en este contexto concentrar los recursos destinados a la aplicación de los métodos de corrección de errores sobre los errores más significativos.

En el contexto de la física experimental, la tomografía de procesos cuánticos también juega un rol fundamental. La caracterización de procesos cuánticos permite poner a prueba hipótesis respecto al comportamiento de sistemas físicos y permite un acceso completo a un espacio muy rico de parámetros observables experimentalmente.

## 1.2. Aleatoriedad

En el campo de la computación clásica, muchos problemas algorítmicos encuentran respuestas eficientes al permitir el uso de aleatoriedad en los mismos (algoritmos randomizados). Sin ser exhaustivo, el uso de números aleatorios en algoritmos clásicos puede apreciarse en

estimación estocástica <sup>1</sup>, métodos criptográficos, algoritmos geométricos e incluso para problemas generales como ordenar., criptografía.

Los números aleatorios, representan la manera de introducir aleatoriedad en algoritmos clásicos en la computación clásica. Es por ello, que el problema de la generación de números aleatorios resulta muy importante. Puede tomarse el capítulo sobre el tema escrito por Donald Knuth [Knu97] como testimonio de esta afirmación. En la práctica, la imposibilidad de generar números aleatorios en un contexto determinista, lleva a que se utilicen sucesiones pseudoaleatorias de números que resultan adecuadas para la mayor parte de las aplicaciones. No obstante, el formalismo cuántico vuelve trivial a este problema. Para generar un bit aleatorio, solo es necesario preparar un qbit en un estado conocido, y medirlo en una base complementaria. Por ejemplo, preparar el estado  $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$  y medirlo en la base computacional  $\{|0\rangle, |1\rangle\}$ . Se obtiene así todos los resultados posibles de la medición con igual probabilidad y de manera independiente. Al día de la fecha, los generadores de números aleatorios son el producto comercial más importante ofrecido por la industria de la información cuántica[idQ].

Podemos preguntarnos entonces, cual es el análogo cuántico de los números aleatorios. La literatura sugiere que son los operadores unitarios aleatorios y estados cuánticos aleatorios. En un artículo [EWS<sup>+</sup>03], Joseph Emerson et al. proponen el uso de operadores pseudoaleatorios que requieran de pocos recursos para su generación manteniendo propiedades estadísticas importantes de los operadores unitarios aleatorios.

Nuestro tratamiento del problema de la tomografía de procesos cuánticos se basa en la introducción explícita de aleatoriedad. Es sorprendente que este enfoque no se haya tomado más seriamente en el pasado, dado que de todas maneras se trata de un problema que inherentemente involucra estimar probabilidades que describan unívocamente al proceso. La aleatoriedad permite obtener algoritmos tomográficos mas eficientes y sorprendentemente, también permite simplificar el análisis de los errores de estimación.

### 1.3. Estructuración del trabajo

En las sección 2, presentamos la noción de canal cuántico o proceso que utilizaremos. Introducimos sus distintas representaciones así como métodos generales para pasar de una a otra. Se introduce primero la representación de Kraus o suma de operadores, que suele tener interpretación más directa en términos de fenómenos físicos. Luego, presentamos la representación  $\chi$  (Chi), que describe a un canal cuántico de manera única en términos de una base de operadores elegidos. Está sera la representación más utilizada a la hora de presentar los métodos tomográficos. Finalmente, incluimos también la representación  $\lambda$  (Lambda) cuyos coeficientes admiten una interpretación directa respecto a como se mapean estados iniciales a estados finales.

---

<sup>1</sup>Las simulaciones de Monte Carlo pueden tomarse como un caso particular de estimación estocástica de cantidades que son imprácticas de calcular.

En la sección 3 presentamos los métodos existentes de tomografía cuántica de procesos. Comenzamos por describir la tomografía estándar de estados cuánticos y de procesos cuánticos [NC00, CN97], por ser estos los métodos de referencia para cualquier otra propuesta. Luego, presentamos sucesivamente el método de tomografía cuántica asistida por ancila [ABJ<sup>+</sup>03], la caracterización directa de dinámicas cuánticas [ML06] y finalmente, la caracterización simetrizada de procesos cuánticos ruidosos [ESM<sup>+</sup>07].

En la sección 4, presentamos como cualquier coeficiente de la matriz  $\chi$  puede describirse en términos de propiedades globales del canal. En particular, damos una propuesta original de como expresar los distintos elementos de  $\chi$  en términos de fidelidades medias de canales que resultan de modificaciones sobre el canal original. Este técnica, junto con métodos eficientes para estimar la fidelidad, permiten selectivamente medir cualquier coeficiente de la matriz tomográfica  $\chi$  con una cantidad de experimentos independiente de la dimensión y sin más que un qubit auxiliar. Dejamos planteada la posibilidad de resolver este problema mediante el uso de 2-diseños, que serán presentados con más detalle en las siguientes secciones.

En la sección 5, presentamos la noción de  $t$ -diseño, conjuntos de puntos que permiten reducir integrales a promedios sobre los mismos. Presentamos algunas de sus propiedades más importantes y definiciones alternativas guiados por el artículo de Andreas Klappenecker y Martin Roetteler [KR05]. Luego, presentamos las bases mutuamente no sesgadas, bases que en la mecánica cuántica están asociadas a observables complementarios, mostrando que un conjunto maximal de las mismas constituye un 2-diseño. Finalmente, repetimos algunos resultados de [BBRV02] que permiten relacionar las bases mutuamente no sesgadas con bases de unitarios ortogonales como los operadores de Pauli.

En la sección 6 mostramos una construcción explícita de un conjunto maximal de bases mutuamente no sesgadas siguiendo las líneas trazadas en la tesis de Ariel Bendersky [Ben06]. En una tomografía computada, ya sea en resonancia magnética, en rayos-X o la técnica de preferencia, se pueden reconstruir imágenes bidimensionales a partir de información obtenida sobre las líneas que se obtiene externamente. La transformación que se aplica para procesar la información en este caso, se llama transformada de Radón. En el caso de espacios finitos discretos, no existe una geometría continua natural. Para lograr resultados análogos, se dará una geometría discreta a estos espacios a partir de construcciones de cuerpos finitos. Esta es la construcción se da en la sección 6, y sus orígenes pueden trazarse a un trabajo de William K. Wootters y B. D. Fields [WF89]. El principal aporte en esta sección es la definición explícita de un conjunto maximal de bases mutuamente no sesgadas con buenas propiedades a partir de una descripción de tamaño polinomial. Se hace especial énfasis en comprender el efecto que tienen los operadores de la base de unitarios ortogonales sobre los vectores de las bases mutuamente no sesgadas asociadas. Es por ello, que los resultados de esta sección resultan esenciales para entender el método tomográfico diagonal que se presenta en la sección 7, pues su definición hace un fuerte uso de la construcción explícita particular dada para las bases mutuamente no sesgadas.

En la sección 7 se muestran resultados originales que permiten aprovechar mediciones completas para hacer tomografía de procesos. Se muestra en este contexto como, con recursos

polinomiales pueden darse estimaciones de cualquiera y de todos los coeficientes diagonales que representan al proceso cuántico. Este método original, representa la primer propuesta polinomial capaz de dar una reconstrucción completa de los coeficientes diagonales de  $\chi$  sin la utilización de sistemas auxiliares. También bosquejamos la posibilidad de obtener algunos conjuntos de coeficientes no diagonales de manera simultanea.

Una versión resumida de los principales resultados obtenidos, se encuentra disponible publicamente por medio del arXiv [BPP08] y ha sido enviada solicitando su publicación.

## 2. Canales y Operadores Cuánticos

Primero que nada, resulta importante describir con algún detalle, que noción tenemos de un proceso cuántico. Es posible deducir desde primeros principios que la evolución de sistemas cuánticos cerrados siempre vendrá dada por un operador unitario  $|\psi'\rangle = U|\psi\rangle$  o bien  $\mathcal{E}(\rho) = \rho' = U\rho U^\dagger$ . Esta evolución puede presentarse como el resultado de la acción de un Hamiltoniano externo, o bien como el resultado de aplicar un circuito cuántico compuesto de elementos básicos unitarios. La ventaja del modelo circuital es la falta de referencia explícita al paso del tiempo.

En el caso de sistemas abiertos, la descripción de los mismos se vuelve un tanto más compleja. Ya no podremos afirmar que el sistema evolucione bajo la acción de un operador unitario ya que es necesario considerar la interacción con su ambiente. En este caso, la evolución unitaria corresponde al sistema junto con su ambiente.

$$\rho \text{ --- } \boxed{U} \text{ --- } U\rho U^\dagger \quad | \quad \begin{array}{c} \rho \text{ --- } \\ \rho_{env} \text{ --- } \end{array} \boxed{U} \text{ --- } \mathcal{E}(\rho)$$

Nielsen y Chuang [NC00, pages 356-373], proponen tres definiciones equivalentes de operaciones cuánticas sobre sistemas abiertos. La primera, que físicamente resulta la más motivante de las tres, propone arrancar con un estado que admita una descomposición producto entre los espacios correspondientes al sistema y al ambiente y luego dejar evolucionar el conjunto con una operación unitaria. Más aun, la descomposición producto propuesta utiliza un  $\rho_{env}$  fijo para el ambiente.

$$\mathcal{E}(\rho) = \rho' = \text{tr}_{env} (U(\rho \otimes \rho_{env})U^\dagger) \quad (1)$$

Se dice que esta representación de un canal es extrínseca, ya que hace referencia a componentes externas al sistema, como  $\rho_{env}$  y  $U$ . Antes de continuar con el desarrollo de representaciones intrínsecas de canales, veamos que propiedades físicas esperamos que tengan los canales. Éstas propiedades suelen tomarse de manera axiomática como definición alternativa.

1. Se interpreta a  $\text{tr}(\mathcal{E}(\rho))$  como la probabilidad de que ocurra el proceso  $\mathcal{E}$ . Por lo tanto, tenemos que para cualquier matriz que describa un estado cuántico  $\rho$ , tenemos que  $0 \leq \text{tr}(\mathcal{E}(\rho)) \leq 1$ . Muchas veces puede incluso pedirse que  $\mathcal{E}$  preserve traza o dicho de otra manera, que  $\text{tr}(\mathcal{E}(\rho)) = 1$  como manera de afirmar que se describe un proceso que efectivamente ocurre.
2. Se espera que cuando se habla del canal, se trate de un único proceso cuántico. Una condición matemática con este espíritu es pedir que el canal sea un mapa lineal convexo sobre el conjunto de estados. Este requisito permite respetar la interpretación de matrices densidad como una superposición de distintos estados cuánticos con respectivas

probabilidades asociadas. Esto, es que para un conjunto de probabilidades  $p_i$  asociadas a estados  $\rho_i$  se tiene que:

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

3. Finalmente, se espera que el mapa  $\mathcal{E}$  envíe operadores positivos en operadores positivos ( $\mathcal{E}$  es un mapa definido positivo). Más aun, se pide que para cualquier sistema auxiliar sobre el que se extienda el mapa  $\mathcal{E}$ , el mapa  $\mathcal{E} \otimes I$  seguirá enviando operadores positivos en operadores positivos ( $\mathcal{E}$  es un mapa completamente positivo).

## 2.1. Representación de Kraus

A partir de reescribir la ecuación 1, se puede llegar rápidamente a la forma de Kraus. Una manera de hacerlo es utilizando la descomposición espectral de  $\rho_{env}$  en estados puros  $\rho_{env} = \sum_m p_m |\psi_m\rangle \langle \psi_m|$  y utilizando esta misma descomposición para tomar la traza parcial.

$$\mathcal{E}(\rho) = \rho' = \sum_{l,m} p_m \langle \psi_l | U(\rho \otimes |\psi_m\rangle \langle \psi_m|) U^\dagger | \psi_l \rangle \quad (2)$$

Si tomamos a  $A_{l,m} = \sqrt{p_m} \langle \psi_l | U | \psi_m \rangle$  y llamamos  $k$  al índice compuesto  $l, m$  podemos expresar al canal como:

$$\mathcal{E}(\rho) = \sum_k A_k \rho A_k^\dagger \quad (3)$$

Esta representación de un canal se llama representación de Kraus o representación como suma de operadores y los operadores  $A_k$  suelen denominarse operadores de Kraus. Claramente, se trata de un mapa lineal que envía operadores densidad a operadores densidad. Veamos a que conclusión llegamos si imponemos que el mapa preserve la traza. Esto equivale a decir que todas las transiciones físicamente posibles mantienen al sistema en el espacio de Hilbert en consideración. La primera igualdad de la siguiente secuencia es la motivada físicamente, mientras que las siguientes resultan de manipulaciones algebraicas:

$$\forall \rho, \text{tr}(\rho) = \text{tr}\left(\sum_k A_k \rho A_k^\dagger\right) = \sum_k \text{tr}\left(A_k \rho A_k^\dagger\right) = \sum_k \text{tr}\left(\rho A_k^\dagger A_k\right) = \text{tr}\left(\rho \sum_k A_k^\dagger A_k\right) \quad (4)$$

Ahora bien, los operadores forman un espacio de Hilbert complejo de dimensión  $D \times D$  provistos del producto escalar  $\langle A | B \rangle = \text{tr}(A B^\dagger)$ . Además, puede tomarse una base del espacio de operadores compuesta exclusivamente de operadores densidad. En efecto, puede darse una tal base de operadores  $\{\rho(i, j)\}_{i, j \in 0 \dots D-1}$  como:

$$\rho(i, j) = \begin{cases} (i = j) & \rightarrow |i\rangle \langle i| \\ (i < j) & \rightarrow \frac{(i+j)}{\sqrt{2}} \times \text{c.c.} \\ (i > j) & \rightarrow \frac{(i-i)}{\sqrt{2}} \times \text{c.c.} \end{cases} \quad (5)$$

Esto significa que para cualquier par de operadores  $B, C$  las siguientes dos afirmaciones son equivalentes.

$$\forall \rho, \text{tr}(\rho B^\dagger) = \text{tr}(\rho C^\dagger) \quad \text{si y solo si} \quad B = C \quad (6)$$

En particular, de la ecuación (4) obtenemos:

$$\sum_k A_k^\dagger A_k = I \quad (7)$$

## 2.2. Representación con matriz chi ( $\chi$ )

Dada una base arbitraria del espacio de operadores,  $\{E_0, E_1, \dots, E_{D^2-1}\}$  tenemos que cada uno de los  $A_k$  puede expresarse como una combinación:

$$A_k = \sum_l a_{kl} E_l$$

Luego, el canal puede describirse como

$$\mathcal{E}(\rho) = \sum_k \sum_{mn} a_{km} E_m \rho E_n^\dagger a_{kn}^*$$

La representación chi ( $\chi$ ) surge de identificar  $\chi_{mn} = \sum_k a_{km} a_{kn}^*$ . La matriz  $\chi$  tiene  $D^2$  columnas por  $D^2$  filas y es por definición hermítica y definida positiva (independiente de la base de  $E_k$  elegida).

$$\begin{aligned} \chi_{mn} &= \sum_k a_{km} a_{kn}^* = \chi_{nm}^* \\ \sum_{mn} v_m^* \chi_{mn} v_n &= \sum_{mnk} v_m^* a_{km} a_{kn}^* v_n = \sum_k \langle v | a_k \rangle \langle a_k | v \rangle \geq 0 \end{aligned}$$

La representación de un proceso mediante la matriz  $\chi$  puede darse pues como:

$$\mathcal{E}(\rho) = \sum_{mn} \chi_{mn} E_m \rho E_n^\dagger \quad (8)$$

La condición de preservar la traza para cualquier operador densidad  $\rho$  puede expresarse como:

$$\sum_{mn} \chi_{mn} E_n^\dagger E_m = I \quad (9)$$

Si una representación de Kraus tiene hasta  $D^2$  operadores linealmente independientes, puede pensarse como una representación Chi diagonal. Recíprocamente, si se tiene una matriz  $\chi$  diagonal, puede interpretarse como una representación de Kraus.

La diagonalización de la matriz hermítica  $\chi$ , nos permite pasar a una representación de Kraus. Sea  $G$  una matriz unitaria de cambio de base que nos permite diagonalizar  $D = G\chi G^\dagger$ .

O similarmente  $G^\dagger DG = \chi$ . Donde,  $D$  puede ser descrito por  $D_{m,n} = \delta_{m,n}\lambda_m$  con los  $\lambda_m$  reales. Esto significa que podemos escribir  $\chi_{m,n}$  como  $\sum_k G_{m,k}^\dagger \lambda_k G_{k,n}$ .

$$\mathcal{E}(\rho) = \sum_{m,n,k=0}^{D^2-1} G_{k,m}^* \lambda_k G_{k,n} E_m \rho E_n^\dagger = \sum_{k=0}^{D^2-1} \lambda_k \left( \sum_{m=0}^{D^2-1} G_{k,m}^* E_m \right) \rho \left( \sum_{n=0}^{D^2-1} G_{k,n} E_n^\dagger \right)$$

Inspirados en esta representación, definimos  $V_k = \sqrt{\lambda_k} \sum_{m=0}^{D^2-1} G_{k,m}^* E_m$ . Obtenemos entonces una nueva representación de Kraus.

$$\mathcal{E}(\rho) = \sum_{k=0}^{D^2-1} V_k \rho V_k^\dagger$$

En este caso, los operadores de Kraus obtenidos para el canal serian los  $V_k$ .

Una ventaja de la representación chi, es que la base puede ser elegida de manera arbitraria. Por ejemplo, puede elegirse una base de operadores ortogonales  $O_k$  normalizados de modo que  $\text{tr}(O_m O_n^\dagger) = D\delta_{mn}$ , como lo son los operadores de Pauli. En este caso los coeficientes para la descomposición de cualquier operador pueden hallarse de manera directa:

$$A_k = \sum_l \frac{\text{tr}(A_k O_l^\dagger)}{D} O_l$$

Tomando la traza en la (Ec. 9), la condición de ortonormalidad sobre la base de operadores implica:

$$\sum_m \chi_{mm} = 1 \tag{10}$$

Esto significa que la diagonal de la matriz chi puede pensarse como una distribución de probabilidades. Adicionalmente, es fácil probar que partiendo de una representación chi con base ortonormal el procedimiento anterior nos lleva a una descomposición de Kraus ortogonal.

Efectivamente, podemos verificar que  $\text{tr} \left( V_i V_j^\dagger \right) = \sqrt{\lambda_i \lambda_j} D \delta_{i,j}$ .

$$\begin{aligned}
\text{tr} \left( V_i V_j^\dagger \right) &= \text{tr} \left( \sqrt{\lambda_i} \left( \sum_{k=0}^{D^2-1} G_{i,k}^* O_k \right) \sqrt{\lambda_j} \left( \sum_{l=0}^{D^2-1} G_{j,l} O_l^\dagger \right) \right) \\
&= \sqrt{\lambda_i \lambda_j} \sum_{k,l=0}^{D^2-1} G_{i,k}^* G_{j,l} \text{tr} \left( O_k O_l^\dagger \right) \\
&= \sqrt{\lambda_i \lambda_j} \sum_{k,l=0}^{D^2-1} G_{i,k}^* G_{j,l} \delta_{k,l} D \\
&= \sqrt{\lambda_i \lambda_j} D \sum_{k=0}^{D^2-1} G_{i,k}^* G_{j,k} \\
&= \sqrt{\lambda_i \lambda_j} D (GG^\dagger)_{j,i} \\
&= \sqrt{\lambda_i \lambda_j} D \delta_{j,i}
\end{aligned}$$

Este resultado, nos permite afirmar que todo canal tiene una forma de Kraus con a lo sumo  $D^2$  operadores ortogonales.

La representación chi de un canal requiere de  $D^4$  parametros reales ( $\chi$  es hermítica) sin importar la base de operadores utilizada. Si imponemos que  $\mathcal{E}$  preserve trazas, (Ec. 9) impone  $D^2$  condiciones adicionales. Esta representación nos da una noción más tangible de que coeficientes deben determinarse mediante mediciones para caracterizar un canal cuántico  $\mathcal{E}$ .

### 2.3. Representación con matriz lambda ( $\lambda$ )

Sea  $\rho_j$ , con  $j \in \{1 \dots d^2\}$  una base del conjunto de matrices de  $D \times D$ . De esta manera, cualquier operador densidad  $\rho$  puede escribirse de manera univoca como una combinación lineal de de los  $\rho_j$ . En particular, para cada canal  $\mathcal{E}$ , quedan determinados  $\lambda_{jk}$  tales que:

$$\mathcal{E}(\rho_j) = \sum_k \lambda_{jk} \rho_k \tag{11}$$

Entonces, la matriz  $\lambda$  describe de manera unívoca al canal  $\mathcal{E}$ . Estos coeficientes pueden determinarse de manera sencilla y directa. Basta con preparar el estado  $\rho_j$  y hacer tomografía de estados sobre el estado que resulte de aplicar el canal sobre la preparación  $\rho_j$  para obtener los  $\lambda_{jk}$ . Es por eso que la primer técnica conocida de tomografía de procesos se basa en la determinación de estos coeficientes.

De manera directa, se pueden obtener los coeficientes de  $\chi$  a partir de los coeficientes de  $\lambda$  y viceversa. Si la base de operadores utilizada para la representación chi es  $\{E_m\}$ , podemos

definir el tensor  $\beta$  como:

$$E_m \rho_j E_n^\dagger = \sum_k \beta_{jk}^{mn} \rho_k \quad (12)$$

Es decir que  $\beta^{mn}$  es la matriz  $\lambda$  correspondiente a un canal ficticio que aplica  $E_m$  a izquierda y  $E_n^\dagger$  a derecha. Con esta definición, puede establecerse la relación entre  $\chi$  y  $\lambda$  como:

$$\sum_{mn} \beta_{jk}^{mn} \chi_{mn} = \lambda_{jk} \quad (13)$$

Ahora, es de interés poder obtener la representación  $\chi$  de un canal a partir de una representación accesible experimentalmente como  $\lambda$ . Para ello, puede utilizarse la inversa generalizada de  $\beta$ . Esta es una matriz  $\kappa$  tal que:

$$\beta_{jk}^{mn} = \sum_{st,xy} \beta_{jk}^{st} \kappa_{st}^{xy} \beta_{xy}^{mn} \quad (14)$$

Podemos pues definir  $\chi$  como:

$$\chi_{mn} = \sum_{jk} \kappa_{mn}^{jk} \lambda_{jk} \quad (15)$$

Esto nos permite obtener los coeficientes de la matriz  $\chi$  que representa a un canal a partir de su representación  $\lambda$ . A partir de la representación  $\chi$  obtenida es posible continuar hacia una representación de Kraus del canal mediante el procedimiento mostrado en la subsección anterior.

### 3. Métodos para la tomografía de procesos cuánticos

En esta sección, presentaremos algunos de los distintos métodos para la tomografía de procesos cuánticos presentes en la bibliografía. La elección de los métodos presentados es guiada por el requisito de que los mismos permitan una reconstrucción del proceso en términos de las representaciones presentadas en la sección 2. Arrancaremos con una introducción a la tomografía de estados cuánticos. A partir de esta, podremos obtener como extensión natural una presentación de la tomografía de procesos cuánticos estándar. Mostraremos como también pueden caracterizarse dinámicas cuánticas mediante el estudio de su efecto en sistemas extendidos con una ancila. Estos métodos toman el nombre de tomografía de procesos cuánticos asistida por ancila. En particular, mostraremos como el método de *caracterización directa de procesos cuánticos* logra una respuesta interesante al problema tomográfico aprovechando las virtudes de una ancila junto con el uso de una base de operadores adaptada al formalismo de estabilizadores. Mostraremos finalmente como la simetrización resulta un recurso útil para la obtención de coeficientes tomográficos específicos. Concluiremos con una discusión de las ventajas y desventajas de cada método y las perspectivas generales que sugieren.

#### 3.1. Tomografía cuántica de estados

Para entender los métodos de tomografía de procesos, es necesario primero comprender la tomografía de estados cuánticos. Esto es, el proceso mediante el cual puede determinarse experimentalmente un estado cuántico desconocido  $\rho$ .

Supongamos que disponemos de una sola copia del estado cuántico  $\rho$ . En este caso, será imposible determinar  $\rho$ , sin importar que tan ingeniosa sea la medición que realicemos. Más aun, no hay ninguna medición que permita distinguir determinísticamente entre dos estados ( $\rho_1$  y  $\rho_2$ ) a menos que estos sean ortogonales ( $\text{tr}(\rho_1\rho_2) = 0$ ). No obstante, si se dispone de un gran número de copias del estado  $\rho$ , veremos que es posible dar una estimación del mismo. Generalmente, si  $\rho$  es el resultado de un procedimiento experimental reproducible, se podrá repetir el procedimiento experimental cada vez que se requiera una copia de  $\rho$ . Si  $\rho$  es un estado cuántico de origen desconocido, la imposibilidad de la clonación cuántica, nos prohibirá disponer de copias del estado  $\rho$ . Esto nos señala que la diferencia esencial entre la tomografía de estados cuánticos y la de estados clásicos, es la imposibilidad de realizar tomografía sobre una instancia <sup>2</sup>.

Dada una base ortonormal de operadores  $\{O_0, \dots, O_{D^2-1}\}$ , el estado  $\rho$  puede expandirse como:

$$\rho = \sum_{i=0}^{D^2-1} \text{tr}(O_i^\dagger \rho) O_i \quad (16)$$

---

<sup>2</sup>Esto permite que equipos médicos modernos realicen tomografía clásica de rayos-X, resonancia magnética u otras sobre instancias como usted sin tener la posibilidad de producir copias.

Si además, los operadores  $O_i$  son hermíticos,  $\text{tr}(O_i^\dagger \rho) = \text{tr}(O_i \rho)$  puede interpretarse como el valor medio de expectación de un observable. Por ejemplo, el estado de una partícula de espín-1/2, puede describirse en términos de los observables de polarización en 3 direcciones ortogonales.

$$\rho = I/2 + P_x X + P_y Y + P_z Z$$

Donde las polarizaciones están dadas precisamente por:  $P_x = \text{tr}(X\rho)/2$ ,  $P_y = \text{tr}(Y\rho)/2$  y  $P_z = \text{tr}(Z\rho)/2$ . Los factores 1/2 provienen de que estos operadores están normalizados para ser unitarios con lo que  $\text{tr}(O_i O_i^\dagger) = D$  en lugar de 1. En el caso de la polarización  $P_z$ , se mide el observable  $Z$  un gran número de veces  $M$ . Cada medición arroja un resultado que puede ser 1 o  $-1$ , obteniéndose así una secuencia binaria de valores,  $z_1, z_2, \dots, z_M$ . El resultado empírico de promediar estos valores  $\frac{\sum_i z_i}{M}$  es un estimador para el valor  $\text{tr}(Z\rho)$ . El valor de expectación de este estimador es el mismo que el valor de expectación de cualquier  $z_i$  individual, precisamente  $\text{tr}(Z\rho)$ . Análogamente, la varianza del estimador es  $M$  veces más chica que la varianza correspondiente a un  $z_i$  individual que esta acotada por 1. En algunos casos, no estará justificado utilizar el teorema del límite central pero si estarán bien definidas la varianza y la desviación estándar de los estimadores, estando esta última acotada por  $\frac{1}{\sqrt{M}}$ .

Esta situación puede generalizarse de manera directa a sistemas cuánticos de  $N$  qubits. Una de las elecciones favoritas para la base de operadores a utilizar es el conjunto de operadores de Pauli generalizados (producto tensorial de matrices de Pauli). Así pues tenemos:

$$\rho = \sum_{\mathbf{v}} \frac{\text{tr}(\sigma_{v_1} \otimes \sigma_{v_2} \otimes \dots \otimes \sigma_{v_N} \rho)}{2^N} \sigma_{v_1} \otimes \sigma_{v_2} \otimes \dots \otimes \sigma_{v_N} \quad (17)$$

Donde los  $v_i$  pueden tomar los valores 0, 1, 2 o 3 para indicar respectivamente un operador  $I$ ,  $X$ ,  $Y$  o  $Z$  en la posición  $i$ .

Así pues, una tomografía completa de un estado de  $N$  qubits requiere la estimación de  $D^2 = 4^N$  parámetros. Una pregunta interesante, es cuantas copias del estado  $\rho$  se requieren para poder realizar  $M$  mediciones independientes de cada uno de los parámetros. Pueden medirse dos operadores que conmuten sobre una misma copia del estado  $\rho$ . Hay a lo sumo  $D$  operadores ortogonales que conmuten ( $D - 1$  sin contar la identidad). Esto se enuncia y prueba en el lemma B.1. En el mejor de los casos, la base de observables que se desea estimar puede partirse en  $D + 1$  grupos de operadores que conmutan. En este caso alcanzará con  $M(D+1)$  copias del estado para realizar  $M$  mediciones de cada parámetro. Veremos que esto corresponde a medir el estado utilizando un conjunto maximal de  $D + 1$  bases mutuamente no sesgadas [Ivo81].

## 3.2. Tomografía estándar de procesos cuánticos

El primer método conocido para la caracterización completa de procesos cuánticos se denomina *tomografía estándar de procesos cuánticos*<sup>3</sup>. Este método de tomografía de procesos es conceptualmente uno de los más sencillos. Una presentación resumida del método puede encontrarse en el libro de Nielsen y Chuang [NC00]. El método se basa en la preparación de distintos estados cuánticos y la tomografía de los resultados obtenidos al aplicarles el proceso  $\mathcal{E}$  que se desea caracterizar. En este método, se considera el efecto del canal  $\mathcal{E}$  sobre un conjunto de estados iniciales de prueba. Para hacer una caracterización completa, se necesita un conjunto linealmente independiente de estados de prueba  $\rho_k$  que forme una base del espacio de matrices densidad. Gracias a la linealidad del canal  $\mathcal{E}$ , la caracterización de  $\mathcal{E}(\rho_k)$  para cada  $k \in \{1, \dots, D^2\}$ , nos permitirá dar una descripción completa del operador  $\mathcal{E}$ .

$$\mathcal{E}(\rho_k) = \sum_j \lambda_{kj} O_j \quad (18)$$

Donde los  $\lambda_{kj}$  se estiman empíricamente mediante la tomografía del estado cuántico  $\mathcal{E}(\rho_k)$ . Y los  $\rho_j$  son la base de operadores que se utiliza para la tomografía de estados.

Concluimos que este método tomográfico nos proporciona de manera directa una representación  $\lambda$  del proceso  $\mathcal{E}$ . Esto es, cualquiera de los coeficientes  $\lambda_{kj}$  puede obtenerse independientemente de los restantes, sin posprocesamiento de datos, mediante la preparación de  $\rho_k$  y la medición de  $\text{tr}(\mathcal{E}(\rho_k)O_j)$ . Notemos que de manera sencilla, podemos considerar en lugar de los estados  $\rho_k$ , las desviaciones de los mismos respecto de la identidad. En tal caso, podríamos medir casi directamente  $\text{tr}(\mathcal{E}(O_k)O_j)$ .

Para obtener las restantes representaciones de  $\mathcal{E}$  a partir de este procedimiento tomográfico, es necesario utilizar la transformación descrita en la sección 2.3 para obtener los coeficientes de una representación  $\chi$ , y de allí posiblemente una representación de Kraus. El problema que surge aquí, es que típicamente, la transformación requiere de todos los coeficientes de  $\lambda$  para obtener cada coeficiente de  $\chi$  y la cantidad de posprocesamiento requerido es exponencial en  $N$ .

### 3.2.1. Resumen y perspectivas

Tal como lo hemos presentado, el método resulta ineficiente y sus únicas virtudes son la extracción directa de coeficientes  $\lambda$  y quizá, ser simple de comprender. Requiere de una cantidad exponencial de estados iniciales  $D^2$ , de mediciones  $O(D^4)$ , e incluso de posprocesamiento clásico si se desea cambiar de representación. En nuestra presentación de la tomografía de procesos estándar, no hemos hecho referencia a ninguna elección particular de los estados iniciales  $\rho_k$  ni tampoco de los observables con los que hacer la tomografía de los estados resultantes. Es por ello, que para obtener una representación  $\chi$  a partir de los coeficientes  $\lambda$ ,

---

<sup>3</sup>Las referencias en inglés suelen llamarlo *standard quantum process tomography* o SQPT.

debemos recurrir a la transformación lineal genérica que resulta muy costosa ( $O(D^6)$  operaciones). Es tratando este cambio de representación con más detalle que podremos llegar a resultados fructíferos. Es probable que este pueda simplificarse fuertemente dando una buena elección de estados iniciales y observables, adecuada a la base utilizada para la representación  $\chi$ . Siendo optimistas, esto podría incluso permitir la estimación selectiva de coeficientes  $\chi_{mn}$ .

### 3.3. Tomografía de procesos cuánticos asistida por ancila

Como hemos visto, la tomografía estándar de procesos cuánticos requiere de la preparación de al menos  $D^2$  estados iniciales linealmente independientes. Esto puede entenderse del hecho de que hacer tomografía de estados del resultado de aplicar el canal sobre cada uno de ellos solo puede proveer  $D^2 - 1$  parámetros independientes por cada estado inicial.

El isomorfismo de Jamiołkowski que hay entre matrices densidad en un espacio de Hilbert de dimensión  $D \times D$  y los mapas completamente positivos que preservan traza, lleva a la idea de codificar la información del canal en el estado de un sistema de dimensión  $D \times D$ . Se da por primera vez el nombre de *Ancilla-assisted process tomography* AAPT en un publicación [ABJ<sup>+</sup>03]. En este artículo, se presenta la idea de utilizar tan solo un estado inicial correlacionado  $\rho$  de dimensión  $D \times D$ . Se obtiene toda la información de  $\mathcal{E}$  a partir de realizar tomografía de estado sobre el estado  $(\mathcal{E} \otimes I)(\rho)$ . Esto divide a  $\rho$  en dos subsistemas, el subsistema  $A$ , donde actúa  $\mathcal{E}$  y  $B$ , que permanecerá intacto. Cuando el estado inicial  $\rho$  es máximamente entrelazado, el método toma el nombre de *entanglement assisted process tomography*, EAPT o en castellano, tomografía de procesos cuánticos asistida por entrelazamiento.

Veamos para que estados iniciales  $\rho$  es posible aplicar este método. Supongamos que el operador  $\rho$  tiene una descomposición de Schmidt<sup>4</sup> dada por:

$$\rho = \sum_l s_l A_l \otimes B_l \quad (19)$$

Donde los  $\{A_l\}$  y los  $\{B_l\}$  son conjuntos de operadores ortonormales (i.e  $\text{tr}(A_m^\dagger A_n) = \delta_{mn}$  y  $\text{tr}(B_m^\dagger B_n) = \delta_{mn}$ ). Además, la descomposición requiere que los coeficientes  $s_l$  sean reales y positivos. Queremos conocer la condición para que toda la información de  $\mathcal{E}$  se encuentre codificada en el estado final  $\rho' = (\mathcal{E} \otimes I)(\rho)$ . En particular, si  $\{A_l\}$  forma una base completa de operadores, podemos reconstruir  $\mathcal{E}$  a partir de los  $\mathcal{E}(A_l)$ , como se mostró en el método de tomografía estándar de procesos cuánticos. Veamos cuando es posible extraer esta información de  $\rho'$ .

$$\rho' = \sum_l s_l \mathcal{E}(A_l) \otimes B_l \quad (20)$$

---

<sup>4</sup>Ver glosario por una definición y breve comentario acerca de la descomposición de Schmidt.

Una vez que disponemos de una reconstrucción tomográfica del estado  $\rho'$ , podemos obtener  $\mathcal{E}(A_l)$  como:

$$\mathcal{E}(A_l) = \frac{\text{tr}_B \left( (I \otimes B_l^\dagger) \rho' \right)}{s_l} \quad (21)$$

Es decir, que siempre que  $s_l$  sea distinto de 0, podremos reconstruir  $\mathcal{E}(A_l)$  a partir de  $\rho'$ . Si esto es cierto para todo  $l$ , podremos continuar con los pasos como en SQPT y reconstruir  $\mathcal{E}$  a partir de  $\rho'$ . Es decir que la condición para poder dar una reconstrucción tomográfica de  $\mathcal{E}$ , es que el número de Schmidt (Cantidad de coeficientes  $s_l$  mayores que 0) sea  $D_A^2$ . Donde  $D_A$  es la dimensión del espacio de Hilbert del sistema sobre el que actúa  $\mathcal{E}$ . Esto implica que la dimensión del sistema auxiliar debe ser mayor o igual que  $D_A$ .

Si definimos el estado puro y máximamente entrelazado:

$$|I\rangle = \frac{1}{\sqrt{D_A}} \sum_m |m, m\rangle$$

Tomamos  $\rho = |I\rangle\langle I|$  la descomposición de Schmidt de  $\rho$  sera óptima y puede explicitarse como:

$$\rho = \sum_{mn} \frac{1}{D_A} |m\rangle\langle n| \otimes |m\rangle\langle n|$$

En este caso, el doble índice  $m, n$  juega el rol de  $l$ . Los operadores  $|m\rangle\langle n|$  son efectivamente ortonormales. Y todos los coeficientes  $s_l$  toman el mismo valor de  $\frac{1}{D_A}$ . Efectivamente, el isomorfismo de Jamiołkowski entre mapas completamente positivos y estados esta dado por:

$$\rho' = (\mathcal{E} \otimes I)(|I\rangle\langle I|) \quad (22)$$

Aquí,  $\rho'$  es el representante del mapa  $\mathcal{E}$  en el espacio de los estados.

### 3.3.1. Resumen y perspectivas

El método de tomografía de procesos cuánticos asistido por ancila, permite reducir el problema de tomografía de mapas que operen en un espacio de dimensión  $D$  a la tomografía de estados de dimensión  $D \times D$ . El método propone utilizar un único estado inicial  $\rho$ , pero no da una prescripción de cual utilizar. Uno máximamente entrelazado parece una buena opción pero el entrelazamiento entre el sistema y la ancila no es necesario. Tampoco se especifica la manera de realizar la tomografía de estado sobre  $\rho'$ . Es aquí donde puede existir la posibilidad de definir observables que permitan estimar selectivamente coeficientes del proceso original. Un enfoque similar a este se toma en el siguiente método que presentaremos. La fortaleza de este método, proviene de poder codificar más información por medición gracias al sistema auxiliar. Al mismo tiempo esta es su debilidad, ya que no debe tomarse a la ligera el requisito de un sistema auxiliar de igual dimensión que se mantenga intacto mientras recorre la misma distancia y tiempo que el sistema principal.

### 3.4. Caracterización directa de dinámicas cuánticas

Un método de tomografía de procesos cuánticos que toma algunos elementos de AAPT, fue propuesto por M. Mohseni y D. A. Lidar en [ML06, ML07] y bautizado *Direct Characterization of Quantum Dynamics* (DCQD). El primer objetivo del método, será caracterizar la representación  $\chi$  de un canal  $\mathcal{E}$ . Es decir que utilizan la representación:

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

En primera instancia, daremos por simplicidad una descripción de como funciona el método en el caso de canales que actúan sobre un qubit. En este caso, se toma  $\{E_m\}_{m=0}^3$  como la identidad y los operadores de Pauli de 1 qubit  $\{I, X, Y, Z\}$ . En su presentación, presentan primero la medición de coeficientes diagonales de  $\chi$  llamandolos poblaciones y luego coeficientes no diagonales llamandolos coherencias, quizás haciendo alusión al isomorfismo de Jamiołkowski entre procesos cuánticos y matrices densidad.

#### 3.4.1. Caracterización de coeficientes diagonales (poblaciones)

Veamos como puede hacerse la caracterización de los coeficientes diagonales  $\chi_{mm}$ . El primer paso consiste en construir un estado  $|\psi\rangle$  máximamente entrelazado entre el subsistema principal  $A$  y un subsistema auxiliar o ancila  $B$ .

$$|\phi^+\rangle = \frac{1}{\sqrt{2}} (|0_A 0_B\rangle + |1_A 1_B\rangle)$$

Notemos que es un autoestado con autovalor  $+1$  de los operadores  $X^A X^B$  y  $Z^A Z^B$  con lo cual, se dice que  $|\phi^+\rangle$  es el estado estabilizador de los operadores. Luego de la preparación, se hace pasar al estado por el canal  $\mathcal{E} \otimes I$ . Es decir que se aplica  $\mathcal{E}$  en el subsistema  $A$  y se mantiene el subsistema  $B$  inalterado. Cualquier operador de Pauli distinto de la identidad actuando en el primer qubit anticonmuta con alguno de los operadores  $X^A X^B$  o  $Z^A Z^B$ . Veamos que las propiedades de conmutación con  $X^A X^B$  y  $Z^A Z^B$  determinan unívocamente un operador de Pauli en el subsistema  $A$ . En la siguiente tabla, se indica con 1 los casos de conmutación y con  $-1$  los casos de anticonmutación.

Operador en $A$	$X^A X^B$	$Z^A Z^B$
$I$	1	1
$X$	1	-1
$Z$	-1	1
$Y$	-1	-1

Si se miden los operadores  $X^A X^B$  y  $Z^A Z^B$  sobre  $\rho' = (\mathcal{E} \otimes I(|\phi^+\rangle \langle\phi^+|))$ , puede usarse la tabla de manera inversa para decidir a que operador de Pauli atribuir la acción en el sistema

A. A continuación, vemos como se identifica el operador  $Z^A$  a partir de medir sobre el estado final los autovalores  $-1$  y  $1$  para los observables  $X^A X^B$  y  $Z^A Z^B$  respectivamente.

$$\begin{aligned} & \text{tr} (X^A X^B Z^A |\phi^+\rangle \langle\phi^+| Z^A) \\ &= -1 \text{tr} (Z^A X^A X^B |\phi^+\rangle \langle\phi^+| Z^A) \\ &= -1 \text{tr} (|\phi^+\rangle \langle\phi^+|) = -1 \end{aligned}$$

$$\begin{aligned} & \text{tr} (Z^A Z^B Z^A |\phi^+\rangle \langle\phi^+| Z^A) \\ &= \text{tr} (Z^A Z^A Z^B |\phi^+\rangle \langle\phi^+| Z^A) \\ &= \text{tr} (|\phi^+\rangle \langle\phi^+|) = 1 \end{aligned}$$

Una medición de estos dos operadores es equivalente a una medición completa en la base de Bell. Los cuatro estados de Bell son:

$$\begin{aligned} |\phi^\pm\rangle &= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \\ |\psi^\pm\rangle &= \frac{1}{\sqrt{2}}(|10\rangle \pm |01\rangle) \end{aligned}$$

Entonces, los cuatro operadores de proyección correspondientes son:

$$\begin{aligned} P_0 &= |\phi^+\rangle \langle\phi^+| \\ P_1 &= |\psi^+\rangle \langle\psi^+| \\ P_2 &= |\phi^-\rangle \langle\phi^-| \\ P_3 &= |\psi^-\rangle \langle\psi^-| \end{aligned}$$

En particular, tenemos que  $Z^A Z^B = P_0 - P_1 + P_2 - P_3$  y  $X^A X^B = P_0 + P_1 - P_2 - P_3$ . Es decir que medir los observables  $Z^A Z^B$  y  $X^A X^B$  es equivalente a realizar una medición proyectiva completa sobre la base de Bell. Finalmente tenemos que cada estado de Bell observado a la salida corresponde a un operador de Pauli actuando en el sistema principal  $p_m = \text{tr} (P_m \rho') = \chi_{mm}$ . Esto significa que con una sola medición proyectiva completa de ensamble pueden caracterizarse simultáneamente los cuatro coeficientes diagonales de la matriz  $\chi$ . Las probabilidades de medir cada uno de los estados de Bell, se corresponden con los respectivos coeficientes diagonales de la matriz  $\chi$  del operador  $\mathcal{E}$ .

### 3.4.2. Condición de preservar traza en la base de Pauli

El método propuesto aprovechará de manera óptima la propiedad de preservar trazas (9) del canal  $\mathcal{E}$ .

$$\sum_{mn} \chi_{mn} E_n^\dagger E_m = I$$

En el caso de una base con buenas propiedades como los operadores de Pauli, esta condición puede expresarse explícitamente como:

$$\begin{aligned}
\chi_{00} + \chi_{11} + \chi_{22} + \chi_{33} &= 1 && \text{(Coeficiente de } I\text{)} \\
\chi_{01} + \chi_{10} - i\chi_{23} + i\chi_{32} &= 0 && \text{(Coeficiente de } X\text{)} \\
\chi_{02} + \chi_{20} - i\chi_{31} + i\chi_{13} &= 0 && \text{(Coeficiente de } Y\text{)} \\
\chi_{03} + \chi_{30} - i\chi_{12} + i\chi_{21} &= 0 && \text{(Coeficiente de } Z\text{)}
\end{aligned}$$

Utilizando que la matriz  $\chi$  es hermítica, podemos escribir esto de manera más compacta:

$$\begin{aligned}
\text{tr}(\chi) &= 1 \\
\text{Re}(\chi_{01}) &= \text{Im}(\chi_{32}) \\
\text{Re}(\chi_{02}) &= \text{Im}(\chi_{13}) \\
\text{Re}(\chi_{03}) &= \text{Im}(\chi_{21})
\end{aligned}$$

El experimento anteriormente mencionado permite caracterizar las 4 poblaciones (4 coeficientes reales). Veamos como es posible diseñar otros experimentos que permitan obtener 2 coeficientes complejos de la matriz  $\chi$ , (4 coeficientes reales de los cuales solo 3 independientes).

### 3.4.3. Medición de coeficientes no diagonales (coherencias)

La medición de elementos no diagonales de  $\chi$  (coherencias), comienza con la preparación de estados entrelazados (pero no máximamente) del tipo  $|\psi\rangle = \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle$  donde se pide  $|\alpha| \neq |\beta|$  y  $\alpha, \beta \neq 0$  además de la normalización  $|\alpha|^2 + |\beta|^2 = 1$ . Esto implica un estado inicial:

$$\rho = |\alpha|^2 |00\rangle\langle 00| + \alpha\beta^* |00\rangle\langle 11| + \beta\alpha^* |11\rangle\langle 00| + |\beta|^2 |11\rangle\langle 11|$$

Luego, al igual que para la medición de poblaciones, se hace pasar al estado por el canal  $\mathcal{E} \otimes I$ . A esta altura tenemos un estado de la forma:

$$\rho' = |\alpha|^2 \mathcal{E}(|0\rangle\langle 0|) \otimes |0\rangle\langle 0| + \alpha\beta^* \mathcal{E}(|0\rangle\langle 1|) \otimes |0\rangle\langle 1| + \beta\alpha^* \mathcal{E}(|1\rangle\langle 0|) \otimes |1\rangle\langle 0| + |\beta|^2 \mathcal{E}(|1\rangle\langle 1|) \otimes |1\rangle\langle 1|$$

La primer medición a realizar es del estabilizador  $Z^A Z^B$ , del estado inicial. Al medir solamente este operador, se preserva la coherencia entre los operadores  $X$  e  $I$  y entre los operadores  $Y$  y  $Z$ . La medición del operador  $Z^A Z^B$  equivale a proyectar sobre los subespacios  $P_\phi = |\phi^+\rangle\langle\phi^+| + |\phi^-\rangle\langle\phi^-|$  y  $P_\psi = |\psi^+\rangle\langle\psi^+| + |\psi^-\rangle\langle\psi^-|$ . La probabilidad de que el resultado de la medición arroje  $+1$  es  $\text{tr}(P_\phi \rho') = \chi_{00} + \chi_{33} + 2(|\alpha|^2 - |\beta|^2)\text{Re}(\chi_{03})$ . De manera complementaria, la probabilidad de que el resultado de la medición sea  $-1$  es  $\text{tr}(P_\psi \rho') = \chi_{11} + \chi_{22} + 2(|\alpha|^2 - |\beta|^2)\text{Im}(\chi_{12})$ . Como ya hemos descripto como obtener los coeficientes diagonales, esta medición permite despejar  $\text{Re}(\chi_{03})$  e  $\text{Im}(\chi_{12})$  que en realidad

son uno el opuesto del otro. De aquí la motivación de  $|\alpha| \neq |\beta|$ . Los estados posibles luego de la medición son:

$$\begin{aligned}\rho_\phi &= \frac{P_\phi \rho' P_\phi}{\text{tr}(P_\phi \rho')} \\ \rho_\psi &= \frac{P_\psi \rho' P_\psi}{\text{tr}(P_\psi \rho')}\end{aligned}$$

Podemos desarrollar explícitamente expansiones para estos estados mediante:

$$\begin{aligned}\rho_\phi \text{tr}(P_\phi \rho') &= |\alpha|^2 (\chi_{00} + \chi_{33} + 2\text{Re}(\chi_{03})) |00\rangle \langle 00| \\ &+ \alpha\beta^* (\chi_{00} - \chi_{33} + 2i\text{Im}(\chi_{03})) |00\rangle \langle 11| \\ &+ \beta\alpha^* (\chi_{00} - \chi_{33} - 2i\text{Im}(\chi_{03})) |11\rangle \langle 00| \\ &+ |\beta|^2 (\chi_{00} + \chi_{33} - 2\text{Re}(\chi_{03})) |11\rangle \langle 11| \\ \rho_\psi \text{tr}(P_\psi \rho') &= |\alpha|^2 (\chi_{11} + \chi_{22} + 2\text{Im}(\chi_{12})) |10\rangle \langle 10| \\ &+ \alpha\beta^* (\chi_{11} - \chi_{22} + 2i\text{Re}(\chi_{12})) |10\rangle \langle 01| \\ &+ \beta\alpha^* (\chi_{11} - \chi_{22} - 2i\text{Re}(\chi_{12})) |01\rangle \langle 10| \\ &+ |\beta|^2 (\chi_{11} + \chi_{22} - 2\text{Im}(\chi_{12})) |01\rangle \langle 01|\end{aligned}$$

Por último, se mide  $X^A X^B$  sobre los estados resultantes. Esto permitirá despejar  $\text{Im}(\chi_{03})$  así como  $\text{Re}(\chi_{12})$ . Efectivamente, tenemos:

$$\begin{aligned}\text{tr}(X^A X^B \rho_\phi) &= \frac{2\text{Re}(\alpha\beta^*)(\chi_{00} - \chi_{33}) - 2\text{Im}(\alpha\beta^*)\text{Im}(\chi_{03})}{\text{tr}(P_\phi \rho')} \\ \text{tr}(X^A X^B \rho_\psi) &= \frac{2\text{Re}(\alpha\beta^*)(\chi_{11} - \chi_{22}) - 2\text{Im}(\alpha\beta^*)\text{Re}(\chi_{12})}{\text{tr}(P_\psi \rho')}\end{aligned}$$

De aquí la motivación  $\alpha \neq 0$  y  $\beta \neq 0$ . Surge la condición adicional  $\alpha\beta^* \notin \mathbb{R}$  que no se menciona explícitamente en la publicación original del método. Notemos que con este proceso pueden caracterizarse completamente  $\chi_{03}$  y  $\chi_{12}$ . La medición sucesiva de los operadores  $Z^A Z^B$  y  $X^A X^B$  es equivalente a una medición completa en la base de Bell, ya que estos dos operadores conmutan y son diagonalizados simultáneamente por esta base.

Para medir los restantes coeficientes alcanza con preparar distintos estados iniciales entrelazados (superposición de un par de estados de Bell). Para medir  $\chi_{01}$  y  $\chi_{23}$  puede prepararse un estado inicial entrelazado  $\alpha |++\rangle + \beta |--\rangle$ . Este es un estado, cuyo único estabilizador es  $X^A X^B$ , puede escribirse también como una superposición de  $|\phi^+\rangle$  y  $|\psi^+\rangle$ . Luego de hacer pasar al estado por el canal  $\mathcal{E} \otimes I$ , se hace una medición completa en la base de Bell, al igual que en los otros casos. En este caso, la interpretación de la medición se hace de otra manera. Podemos pensar que primero se mide el estabilizador  $X^A X^B$  y luego el normalizador  $Y^A Y^B$ . Finalmente, para medir  $\chi_{02}$  y  $\chi_{13}$  se prepara un estado puro como  $\alpha |++i\rangle + \beta |--i\rangle$ . Nuevamente, se realiza una medición proyectiva completa en la base de Bell, cuya interpretación consiste en medir “primero” el estabilizador  $Y^A Y^B$  y luego el normalizador  $Z^A Z^B$ .

#### 3.4.4. Medición en sistemas de $N$ qubits

La propuesta original de Mohseni y Lidar parece utilizar muy fuertemente el hecho de trabajar sobre un sistema de un qubit [ML06]. No obstante, presentan una extensión del método a sistemas de  $p$  niveles para el caso de  $p$  primo [ML07]. Señalan también que es posible aplicar el método para caracterizar un canal que actúa sobre  $N$  subsistemas. Las mediciones necesarias son productos tensoriales de las mediciones correspondientes a la caracterización de procesos en cada subsistema. En el caso de qubits, la matriz  $\chi$  representará el peso de productos tensoriales de operadores de Pauli de un qubit.

A diferencia de AAPT, el método que proponen no requiere hacer ninguna tomografía completa de estados. Podemos entonces analizar si es posible caracterizar selectivamente algunos coeficientes tomográficos sin la necesidad de realizar el conjunto completo de experimentos necesario para una tomografía completa. En el primer artículo, presentan una descripción del método para dinámicas en 1 qubit. En el caso de querer caracterizar un coeficiente diagonal, solo se requiere medir la probabilidad correspondiente a un solo estado final en un solo experimento. Esto significa que para caracterizar un coeficiente diagonal en  $N$  subsistemas, solo se requiere caracterizar la probabilidad de un estado final en un experimento. En el caso de querer caracterizar un coeficiente no diagonal en un canal que actúa sobre un único qubit, se requiere:

- Un experimento para caracterizar los coeficientes diagonales correspondientes. Es decir que si se quiere caracterizar el coeficiente  $\chi_{mn}$ , primero se deben caracterizar los coeficientes  $\chi_{mm}$  y  $\chi_{nn}$ . Para ello, alcanza con medir las probabilidades de dos estados finales en el experimento que caracteriza elementos diagonales.
- Un experimento adicional, en el que nuevamente se precisan conocer las probabilidades correspondientes a dos estados finales.

A partir de estos 2 experimentos, se puede obtener completamente el coeficiente deseado. El problema, es que para caracterizar un coeficiente que es no diagonal en  $N$  subsistemas, se requerirán entonces  $2^N$  experimentos. De cada uno de estos experimentos, se requerirá caracterizar las probabilidades de  $2^N$  de las salidas posibles. Esto significa que el método de DCQD no resulta eficiente para selectivamente caracterizar coeficientes tomográficos no diagonales en un sistema con un gran número de qubits  $N$ . El caso de un coeficiente general, no requerirá tantos experimentos como un coeficiente no diagonal en todas las componentes. Un coeficiente típico, tendrá una acción diagonal en aproximadamente uno de cada cuatro subsistemas. Esto hace que el costo de realizar el algoritmo para obtener un coeficiente típico se reduzca un poco sin dejar de ser exponencial.

#### 3.4.5. Resumen y perspectivas

El método DCQD es considerado por algunos, una modificación de AAPT. Quienes mantienen esta opinión, argumentan que preparar un estado inicial extendido con una ancila y

hacer tomografía sobre el resultado es de alguna manera equivalente a preparar muchos estados iniciales y realizar una única medición sobre los resultados obtenidos [Zim06]. De hecho, este método mantiene las ventajas y desventajas de AAPT, como poder codificar información en un espacio de Hilbert más grande y necesitar un canal auxiliar de igual tamaño que mantenga una fidelidad<sup>5</sup> máxima a través del tiempo y/o el espacio. Sin embargo, éste método agrega muchos ingredientes no están sugeridos en AAPT. Por un lado, muestra que elegir una base para la representación  $\chi$ , puede ser muy ventajoso para el diseño de un algoritmo tomográfico. En efecto, muestran como la base de Pauli y el formalismo de estabilizadores permiten una extracción directa de errores responsables de ciertas transiciones. En efecto, es gracias a esta astucia que los coeficientes diagonales  $\chi_{mm}$  se vuelven observables directamente como probabilidades de distintos estados finales. Aunque no sea mencionado en el artículo, esto permite la estimación simultánea de todos los coeficientes diagonales de la matriz  $\chi$  como probabilidades de los resultados de un único experimento. Dicho de otra manera, esto permite estimar cualquier coeficiente diagonal con precisión  $\epsilon$  realizando tan solo  $O(\epsilon^{-2})$  mediciones en un mismo experimento. No obstante la necesidad de un canal auxiliar limpio y la imposibilidad de hacer tomografía selectiva sobre coeficientes no diagonales eficientemente todavía da lugar a progresos significativos en el área de tomografía de procesos cuánticos.

### 3.5. Caracterización de procesos ruidosos simetrizados

El primer método que explícitamente reduce el número de experimentos tomográficos necesarios de exponencial a polinomial es SCNQP *Symmetrized Characterization of Noisy Quantum Processes* [ESM<sup>+</sup>07, SMKE07]. El método se basa en dos observaciones esenciales. La primera observación, es la necesidad de reducir el número de parámetros a estimar a un número polinomial en  $N$ , agrupándolos según algún criterio. Proponen pues simetrizar el proceso bajo consideración para reducir el número de parámetros independientes a una cantidad polinomial. Esto requiere identificar los parámetros de interés y la simetrización asociada a estos. La segunda observación o más bien, el logro, es la posibilidad de implementar eficientemente las simetrizaciones necesarias. La propuesta hace énfasis en el objetivo específico de dar una caracterización tomográfica que permita estudiar la aplicabilidad de códigos correctores de errores conocidos. En particular, se concentran en dar una presentación para la clase de códigos que permiten corregir errores que afecten simultáneamente hasta  $t$  qubits. Un código que permite corregir errores simultáneos en hasta  $t$  qubits se denomina de distancia  $2t + 1$ , ya que significa que para pasar de un estado del código a otro se requiere un operador con peso de Hamming (ver Peso de Hamming) mayor o igual a  $2t + 1$ . Los coeficientes tomográficos adquiridos deberán distinguir pues entre la posibilidad de que se introduzcan errores en más de  $t$  qubits y que se introduzcan errores en hasta  $t$  qubits. La probabilidad de esta última corresponde a la aplicación exitosa de un código corrector de

---

<sup>5</sup>Aquí, se entiende por fidelidad, la calidad con la cual un canal preserva un estado cuántico.

errores de distancia  $2t + 1$ .

Supongamos que se quiere aplicar un código corrector de errores al canal  $\mathcal{E}$  y se parte de una representación  $\chi$  del mismo. Los códigos correctores de errores discretizan el conjunto de errores posibles. Típicamente, colapsan cualquier evolución a una evolución de Pauli. Es por eso, que es conveniente tomar la la representación  $\chi$  utilizando el mismo conjunto de operadores. En este caso, volveremos a usar la base de operadores de Pauli como venimos haciendo. Como el canal solo nos interesa a efectos de aplicar un código corrector de errores, solo nos interesa la parte diagonal de la representación  $\chi$ . Es decir, a los efectos de aplicar un código corrector de errores, tener un canal  $\mathcal{E}(\rho) = \sum_{mn} \chi_{mn} P_m \rho P_n$  es equivalente a tener el canal  $\mathcal{E}_{\text{Pauli}}(\rho) = \sum_m \chi_{mm} P_m \rho P_m$ . Podemos construir el canal  $\mathcal{E}_{\text{Pauli}}$  aplicando un twirl de Pauli (ver Twirl finito). Esto es justamente, elegir al azar un operador  $P_r$  de entre los  $4^N$  operadores de Pauli, aplicarlo al estado inicial  $\rho$  aplicar el canal  $\mathcal{E}$  al estado resultante y finalmente aplicar el inverso del primer operador aplicado (como los Paulis son hermíticos unitarios es el mismo operador). El canal resultante puede describirse como:

$$\mathcal{E}_{\text{Pauli}}(\rho) = \sum_{mn} \chi_{mn} 4^{-N} \sum_r P_r P_m P_r \rho P_r P_n P_r \quad (23)$$

Como cualquier par de operadores de Pauli conmuta o anticonmuta, podemos escribir  $P_m P_r = (-1)^{m,r} P_r P_m$ . Usando esta notación, podemos escribir:

$$\mathcal{E}_{\text{Pauli}}(\rho) = \sum_{mn} \chi_{mn} 4^{-N} \sum_r (-1)^{m,r} (-1)^{n,r} P_m \rho P_n \quad (24)$$

Una propiedad que tiene este conmutador es que si  $P_m$  es distinto de la identidad,  $(-1)^{m,r}$  vale 1 para exactamente la mitad de los índices posibles  $r$  y  $-1$  para la otra mitad. Si llamamos  $P_{m+n}$  al operador de Pauli obtenido de  $P_m P_n$ , su propiedad de conmutación puede ser obtenida como:  $P_m P_n P_r = (-1)^{m,r} (-1)^{n,r} P_r P_m P_n = .$  Estas dos observaciones, nos permiten decir que:

$$\sum_r (-1)^{m,r} (-1)^{n,r} = 4^N \delta_{m,n}. \quad (25)$$

Finalmente, combinar las dos ecuaciones anteriores nos lleva al resultado buscado:

$$\mathcal{E}_{\text{Pauli}}(\rho) = \sum_m \chi_{mm} P_m \rho P_m \quad (26)$$

Resumiendo, el resultado de aplicar un twirl de Pauli a un canal arbitrario  $\mathcal{E}$  es un canal de Pauli  $\mathcal{E}_{\text{Pauli}}$  cuya representación  $\chi$  en la base de Pauli puede obtenerse del original anulando los elementos no diagonales.

Ahora, el objetivo de la tomografía será decidir con que probabilidad fracasará o tendrá éxito un código corrector de hasta  $t$  errores. Es por esto que el método tomográfico no necesita distinguir entre distintos operadores de Pauli con el mismo peso de Hamming (ver. peso de Hamming). En particular, no se precisa distinguir entre los errores  $X, Y, Z$ . En segunda

instancia, no se precisa distinguir en que posiciones se producen errores si no solo cuantos son. Veremos como la simetrización permite tratar de igual manera todos los errores que consideramos equivalentes. (Fig. 1).

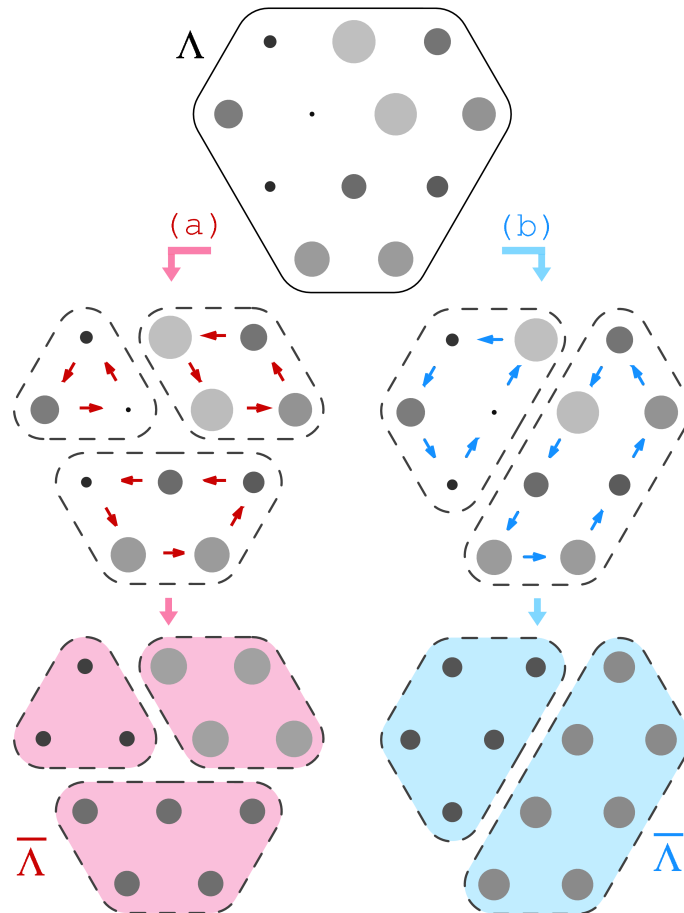


Figura 1: Aquí se muestra como una vez identificadas las clases de equivalencia se aplica un twirl o simetrización cuyo efecto es promediar los pesos de los coeficientes dentro de cada clase. El gráfico ilustra como elegir distintos criterios (a, b) para separar en clases resulta en distintas simetrizaciones. Imagen tomada de [ESM<sup>+</sup>07].

Un twirl de Clifford es un twirl finito al igual que el twirl de Pauli pero en este caso, utilizando el conjunto de operadores de Clifford (ver apéndice A.2). C. Dankert et al. [DCEL06] muestran como realizar un twirl de Clifford logra uniformizar entre los pesos correspondientes a todos los operadores de Pauli distintos a la identidad. Esta simetrización que realizan en su primer artículo resulta demasiado fuerte, ya que solo distingue la identidad de los demás operadores de Pauli distintos de la identidad. Con esta propuesta, se logra dar un algoritmo que estime la fidelidad media (ver fidelidad media) de un proceso  $\mathcal{E}$  de manera

eficiente. Mostraremos como resultados posteriores [ESM<sup>+</sup>07] permitieron superar dificultades importantes. Por un lado, se utilizaba una implementación aproximada para el Clifford twirl para reducir la complejidad en la cantidad de compuertas cuánticas necesarias. Por otra parte, el único parametro del canal original que sobrevive esta simetrización tan fuerte es la fidelidad media. La descripción de como realizar un Clifford twirl exacto en el caso de un qubit es uno de los ingredientes que puede entenderse mejor en este primer artículo y sirve para dar una descripción de SCNQP. Primero, veamos que para un qubit, existe un operador del grupo de Clifford que cicla entre los operadores de Pauli  $\{X, Y, Z\}$  y los distingue solo de la identidad. En este caso, se trata del operador  $R$  (Sec.A.2) y sus tres potencias:  $\{I, R, R^2\}$ . Estos operadores pertenecen al grupo de Clifford, y su acción por conjugación es:

$$RIR^\dagger = I \quad ; \quad RXR^\dagger = Z \quad ; \quad RYR^\dagger = X \quad ; \quad RZR^\dagger = Y \quad (27)$$

Con lo cual, conjugar con probabilidad  $\frac{1}{3}$  con cada uno de los operadores  $\{I, R, R^2\}$ , promedia los coeficientes diagonales correspondientes a todos los operadores de Pauli distintos de la identidad. Esto es, la simetrización que falta luego de un twirl de Pauli para completar un twirl de Clifford sobre un qubit. Si lo aplicamos sobre los  $N$  subsistemas, promedia los pesos de distintos operadores de Pauli cuya descomposición tensorial tienen identidades en exactamente las mismas posiciones. Sin embargo, aplicar un twirl de Clifford sobre cada uno de los qubits independientemente  $\mathcal{C}_1^{\otimes N}$  es distinto a aplicar un twirl de Clifford sobre  $N$  qubits  $\mathcal{C}_N$ . Podemos ilustrar la diferencia para un canal que actúa sobre 2 qubits. En el primer caso  $\mathcal{C}_1^{\otimes 2}$ , los cuatro grupos dentro de los cuales se promedian los pesos de los operadores son:  $\{II\}$ ,  $\{XI, YI, ZI\}$ ,  $\{IX, IY, IZ\}$  y  $\{XX, XY, XZ, YX, YY, YZ, ZX, ZY, ZZ\}$ . En el segundo caso  $\mathcal{C}_2$ , hay solo dos grupos  $\{II\}$  y un segundo grupo con los restantes 15 operadores distintos de la identidad.

Una forma alternativa de indexar los operadores de Pauli que será de utilidad para este protocolo es mediante tres índices  $P_{w, \nu_w, \mathbf{i}_w}$ . El primero,  $w \in \{0, \dots, N\}$  sera el número de factores distintos de la identidad en la descomposición tensorial del operador  $P_{w, \nu_w, \mathbf{i}_w}$  (i.e. el peso de Hamming del operador). El segundo,  $\nu_w \in \{1, \dots, \binom{N}{w}\}$  sera un índice de permutación que codifica en que posiciones se encuentran los factores identidad y en cuales los factores distintos de la identidad. El tercero,  $\mathbf{i}_w = \{i_1, \dots, i_w\}$  es un vector de  $w$  componentes donde los valores posibles para una componente  $i_k$  pueden ser 1, 2, o 3 e indican si el  $k$ -ésimo factor distinto de la identidad es  $X, Y$  o  $Z$ . Esta forma de indexar resulta conveniente porque se ajusta a la simetría percibida por los códigos correctores de errores. Efectivamente, que un código corrector de distancia  $2t + 1$  pueda corregir la acción de un cierto error de Pauli solo dependerá de que el primer índice  $w$  sea menor o igual que  $t$ .

Aplicar el twirl  $\mathcal{C}_1^{\otimes N}$  ya mencionado, mezcla los coeficientes con distinto  $\mathbf{i}_w$  pero con el mismo  $w$  y  $\nu_w$ . En efecto, si escribimos a los  $\chi_{mm}$  como  $a_{w, \nu_w, \mathbf{i}_w}$  tenemos:

$$\sum_{w, \nu_w, \mathbf{i}_w} a_{w, \nu_w, \mathbf{i}_w} 3^{-N} \sum_{\mathbf{j}=1}^{3^N} R^{-\mathbf{j}} P_{w, \nu_w, \mathbf{i}_w} R^{\mathbf{j}} \rho R^{-\mathbf{j}} P_{w, \nu_w, \mathbf{i}_w} R^{\mathbf{j}} = \sum_{w, \nu_w, \mathbf{i}_w} r_{w, \nu_w} P_{w, \nu_w, \mathbf{i}_w} \rho P_{w, \nu_w, \mathbf{i}_w} \quad (28)$$

donde  $\mathbf{j}$  es un vector de  $N$  componentes en  $\{0, 1, 2\}$  que indican que potencia de  $R$  se aplica en cada subsistema y  $r_{w,\nu_w} = 3^{-w} \sum_{\mathbf{i}_w} a_{w,\nu_w,\mathbf{i}_w}$ .

Para completar la simetrización buscada, es necesario promediar además sobre los coeficientes con distinto  $\nu_w$  pero igual  $w$ . Una forma de hacer esto es mediante un twirl que aplique una permutación aleatoria  $\pi_s$  sobre los qubits iniciales e invertirla antes de la medición final.

$$\sum_{w,\nu_w,\mathbf{i}_w} \sum_{\pi_s=1}^{N!} r_{w,\nu_w} \pi_s^{-1} P_{w,\nu_w,\mathbf{i}_w} \pi_s \rho \pi_s^{-1} P_{w,\nu_w,\mathbf{i}_w} \pi_s = \sum_{w,\nu_w,\mathbf{i}_w} p_w 3^{-w} \binom{N}{w}^{-1} P_{w,\nu_w,\mathbf{i}_w} \rho P_{w,\nu_w,\mathbf{i}_w} \quad (29)$$

donde  $p_w = 3^w \sum_{\nu_w} r_{w,\nu_w} = \sum_{\nu_w,\mathbf{i}_w} a_{w,\nu_w,\mathbf{i}_w}$ . Es decir que  $p_w$  representa la probabilidad de que ocurra un error de Pauli con peso de Hamming  $w$ .

En el mismo artículo original, se propone una alternativa que puede ser más eficiente y logra un efecto equivalente. Esta consiste en empezar el experimento con un estado invariante ante permutaciones de qubits (i.e.  $|0\rangle = |0\rangle^N$ ) y hacer una medida sobre la base computacional  $|l\rangle$  que resulta en una cadena de  $N$  bits,  $l \in \{0, 1\}^N$ . Si la información que utilizamos de  $l$  no depende de las posiciones de los 0s y los 1s, esto simula la permutación de qubits en el resultado final. Es decir, solo se distingue a los estados finales  $|l\rangle$  mediante el peso de Hamming  $h \in 0, \dots, N$  de la cadena de bits asociada  $l$ . Notemos que no todos los operadores de Pauli alteran el estado final. En efecto, el operador  $Z$  conmuta con el estado inicial con lo que no provoca ninguna alteración. Los factores que podremos observar son pues únicamente  $X$  e  $Y$ . Por lo tanto, la probabilidad  $u_h$  de obtener una cadena  $l$  con  $h$  unos en la medición final esta dada por:

$$u_h = \sum_{w=h}^N R_{hw} p_w \quad (30)$$

La suma empieza en  $w = h$  pues si hay menos de  $h$  operadores distintos de la identidad, es imposible que haya  $h$  que sean además distintos de  $Z$ . Los coeficientes  $R_{hw} = \binom{w}{h} \frac{2^h}{3^w}$  representan la proporción de operadores de Pauli con  $w$  factores distintos de la identidad que tienen exactamente  $w - h$  factores  $Z$  (es decir  $h$  factores en total entre  $X$  e  $Y$ ). La relación entre  $\vec{u}$  y  $\vec{p}$ , esta dada pues por una matriz diagonal superior no singular, por lo que en principio, es posible despejar los valores de los  $p_w$  eficientemente a partir de los observables  $u_h$ . Un problema al que no se responde en este trabajo es la sensibilidad exponencial en  $w$  que se necesita en los experimentos para estimar  $p_w$ . Por ejemplo, para estimar  $p_N$ , tenemos:

$$p_N = \left(\frac{3}{2}\right)^N u_N \quad (31)$$

Por suerte, para decidir si un canal es apto para aplicar un código corrector de errores, solo se necesita los coeficientes  $p_w$  con  $w$  pequeño, ya que se espera que la cantidad de errores a corregir sea pequeña. En este caso, los  $p_w$  con  $w < l$  pueden estimarse con  $O\left(\left(\frac{3}{2}\right)^l\right)$  experimentos.

En la presentación de este método, también se proponen observables alternativos y una alteración que hace al protocolo accesibles para sistemas físicos como resonancia magnética, donde la preparación aproximada de estados puros no es escaleable con el número de qubits. Lamentablemente, no se repetirá el desarrollo de estos resultados.

### 3.5.1. Resumen y perspectivas

Este método nos muestra como la simetrización permite extraer información sobre el canal sin la necesidad de realizar una tomografía completa. Fue utilizando estas técnicas que por primera vez se demostró la posibilidad de estimar parámetros de un canal tales como la fidelidad utilizando recursos polinomiales en  $N$ . Sugiere que la simetrización/twirl que conviene utilizar depende de los parámetros que se desean estimar. También muestra que la simetrización de un proceso mediante un twirl y la variación de estados iniciales y mediciones son dos maneras distintas de ver la misma herramienta. El twirl utiliza diseños simétricos sobre el espacio de los unitarios mientras que la variación de estados iniciales y finales busca diseños de estados invariantes ante alguna simetría. En particular, se vio como fue posible eliminar por completo un twirl de permutación arrancando con un estado invariante y transformando la permutación final en una permutación virtual luego de la medición.

En resumen, el método requiere de tan solo  $O(N)$  compuertas de un qubit aplicadas con profundidad constante. Permite estimar parámetros como la fidelidad y las probabilidades  $p_w$  de que ocurran errores de Pauli con peso de Hamming  $w \leq l$  con una precisión  $\epsilon$  realizando tan solo  $O\left(\left(\frac{3}{2}\right)^l \epsilon^{-2}\right)$  experimentos independientes.

## 3.6. Comparación y nuevas metas

En esta sección, hemos hecho un repaso de los principales métodos existentes de tomografía de procesos cuánticos. Los primeros dos métodos presentados, SQPT y AAPT, dan recetas generales de como realizar una tomografía de proceso, y por su generalidad, pierden de vista algunas posibles optimizaciones que buscaremos encontrar. De SCNQP, tomaremos la idea de introducir aleatoriedad para implementar una simetrización y así poder estimar parámetros de interés. Como mejora, buscaremos tener más flexibilidad en cuanto a los parámetros accesibles de canal. De DCQD, tomaremos la idea de utilizar estados y mediciones que permitan dar una interpretación simple a los operadores utilizados en la representación  $\chi$ . Para poder tener alguna ventaja sobre este método, buscaremos no utilizar sistemas auxiliares (o minimizar el tamaño del mismo). También resultaría una mejora importante garantizar métodos selectivos eficientes para coeficientes no diagonales.

## 4. Tomografía selectiva de procesos cuánticos

El mayor problema con el que se encuentra la tomografía de procesos cuánticos es la enorme cantidad de parámetros que precisa estimar. Esta dificultad, aparentemente irremediable puede ser salvada mediante la selección de un subconjunto de coeficientes a estimar. No obstante, en los métodos tradicionales de tomografía de procesos (SQPT, AAPT y en algún grado también DCQD) todos o muchos de los coeficientes tomográficos de  $\chi$  pueden estar relacionados de manera compleja con cada una de las probabilidades estimadas experimentalmente. Es necesario pues, idear nuevos métodos tomográficos que permitan estimar selectivamente algunos coeficientes permitiendo una correspondiente reducción del número de experimentos necesarios.

En esta sección presentamos la *tomografía selectiva de procesos*, un método capaz de medir selectivamente coeficientes de la matriz  $\chi$  con muy pocos recursos. Primero, daremos condiciones necesarias y condiciones deseables sobre la base de operadores utilizada en la representación  $\chi$  para que esta permita la estimación selectiva de coeficientes. En segundo lugar, mostramos como es posible obtener información de un canal observando su efecto promedio (integrado) sobre todo el espacio de Hilbert. Como siguiente paso, utilizamos estos resultados para mostrar como pueden diseñarse estimadores para cualquier coeficiente de la matriz  $\chi$ . Luego, se dan representaciones circuitales de estos estimadores, confirmando la existencia de una estimación experimental físicamente viable. Se enumeran luego los distintos métodos disponibles para la evaluación de las integrales como fidelidades y se describe con detalle cada proceso experimental resultante.

### 4.1. Una base de operadores conveniente

Como veremos, no cualquier base de operadores permite una medición sencilla de los coeficientes  $\chi$ . Es importante sin embargo tratar de reducir a un mínimo las propiedades requeridas sobre la base de operadores  $\{E_m\}$ , ya que el resultado final resultará más general mientras menos se exija de la misma. Es por ello que separamos condiciones absolutamente necesarias de condiciones deseables. Las primeras resultan indispensables para la aplicabilidad de cualquiera de nuestros resultados de tomografía selectiva. Las restantes, permiten importantes optimizaciones, motivando el uso de bases que se adecúen siempre que esto sea posible.

#### Condiciones necesarias

- Los operadores de la base deberán ser unitarios:

$$E_m E_m^\dagger = I$$

Esta condición es necesaria para poder implementar tanto los operadores como sus inversas físicamente. La condición significa que corresponden a una evolución temporal bajo algún Hamiltoniano.

- Los operadores de la base deberán ser ortonormales:

$$\text{tr} (E_m E_n^\dagger) = D \delta_{mn}$$

Esta condición es esencial para que la tomografía resultante pueda estimar un coeficiente seleccionado de manera directa. Sin ella, resultaría un álgebra mucho más complicada y, más importante aun, no permitiría estimar un coeficiente tomográfico independientemente de los demás. Notamos también que gracias al factor  $D$ , es consistente con la primera condición.

### Condiciones deseables

Cuando se desarrolló el método de tomografía selectiva, se utilizaron inicialmente los operadores de Pauli como base para la descripción  $\chi$ . Se observa que las siguientes propiedades hacen de los operadores de Pauli una base privilegiada para realizar optimizaciones.

- Es deseable que los operadores  $\{E_m\}$  admitan una descomposición como producto tensorial.

$$E_m = E_m^{(1)} \otimes E_m^{(2)} \otimes \dots \otimes E_m^{(N)}$$

La motivación de esta condición, es garantizar una implementación directa y eficiente. Los operadores  $E_m$  podrán expresarse como la aplicación en paralelo de operadores más simples en los distintos subsistemas. La factorización también permite obtener implementaciones de los operadores  $E_m$  controlados y anticontrolados (ver apéndice A.3).

- El grupo generalizado de operadores de Heisenberg-Weyl (ver apéndice 6.1) y en particular, el grupo de operadores de Pauli generalizados, cumplen con todas las condiciones anteriores y además, satisfacen dos propiedades adicionales que permitirán mejoras sustanciales sobre el algoritmo tomográfico.

1. Forman un grupo a menos de fases numéricas (i.e.  $E_m E_n = e^{i\theta_{m,n}} E_{m \cdot n}$ ).
2. Forman un *conjunto máximamente conmutativo de unitarios ortogonales* (ver definición 5.7), condición necesaria y suficiente para definir un conjunto maximal de bases mutuamente no sesgadas [BBRV02]. Esto quedará claro luego de la lectura de la sección 5 y particularmente la subsección 5.4. Por el momento, basta aclarar que no se espera tener  $D^2$  operadores ortogonales que conmuten (esto es imposible), si no que el conjunto de operadores pueda partitionarse en un numero mínimo subconjuntos conmutativos.

## 4.2. Algunos promedios sobre el espacio de Hilbert

A continuación, veremos como un canal puede caracterizarse completamente por propiedades globales. Es decir, podemos describir un canal completamente a partir de coeficientes que resultan de hacer promedios sobre todo el espacio de Hilbert. Más aun, estos promedios tienen grado 2 en bras y en kets con lo que en virtud de los resultados que presentaremos en la sección 5.4 podrán ser calculados mediante el uso de 2-diseños (ver 2-diseños).

Podemos empezar por la fidelidad media de un canal  $\mathcal{E}$ , que puede ser expresada como[Nie02]:

$$\overline{F}(\mathcal{E}) \equiv \int_{F-S} \langle \psi | \mathcal{E}(|\psi\rangle \langle \psi|) |\psi\rangle d|\psi\rangle = \int \text{tr}(P_\psi \mathcal{E}(P_\psi)) dP_\psi \quad (32)$$

Aquí, el proyector  $P_\psi$  representa el estado puro  $|\psi\rangle \langle \psi|$  y las integrales se realizan utilizando la medida de Fubini-Study sobre el espacio de Hilbert (ver Medida de Fubini-Study). Así como el diferencial de área sobre la esfera unidad es la única medida invariante ante rotaciones, la medida de Fubini-Study es la única medida sobre los estados puros invariante ante transformaciones unitarias (respectivamente conjugación por unitarios en el caso de los proyectores puros). Por otra parte, la condición de normalización de la medida de Fubini-Study esta dada por

$$\int_{F-S} 1 d|\psi\rangle = 1 \quad (33)$$

A partir de ahora, omitiremos el subíndice  $F-S$ , y se asumirá que las integrales sobre estados puros  $|\psi\rangle$  o proyectores puros  $P_\psi$  se realizan utilizando esta medida. Presentamos la expresión de la derecha para mostrar explícitamente que las integrales no dependen de la fase del estado, y puede tomarse la integral en el espacio de matrices densidad correspondiente a estados puros. Un resultado interesante que sustenta esta notación, es que las integrales de términos que no tengan igual cantidad de factores  $|\psi\rangle$  que  $\langle \psi|$  se anulan.

El parámetro  $\overline{F}(\mathcal{E})$  se utiliza como estimador de la bondad de canales de comunicación cuánticos y memorias cuánticas. También veremos que puede utilizarse para estimar cuan buena es la implementación  $\Sigma_U$  de un operador unitario  $U$  asumiendo que se dispone de una implementación perfecta de la operación inversa  $U^\dagger$ . La estimación de este parámetro ha sido hasta hace poco tiempo el caballito de batalla de quienes promueven el uso de estados aleatorios en tomografía cuántica [DCEL06, Dan05, EAZ05]. Veremos como, en genral, los estados aleatorios resultan adecuados para la estimación de cantidades definidas como promedios sobre los estados puros del espacio de Hilbert.

Cualquier polinomio homogéneo de grado 2 en los kets y grado 2 en los bras promediado sobre el espacio de Hilbert, puede escribirse como una combinación lineal de términos con el siguiente aspecto [Dan05]:

$$\int \langle \psi | E_1 P_\psi E_2 |\psi\rangle d|\psi\rangle = \frac{\text{tr}(E_1) \text{tr}(E_2) + \text{tr}(E_1 E_2)}{D(D+1)} \quad (34)$$

No es casualidad que estos sean justamente el tipo de términos que aparece cuando se desea evaluar la fidelidad media de un canal en representación  $\chi$ .

En particular, si se toma una base de operadores  $\{E_m\}$  tales que  $E_0 = I$  y  $\text{tr}(E_n E_m^\dagger) = D\delta_{mn}$ , tenemos que:

$$\int \langle \psi | E_m P_\psi E_n^\dagger | \psi \rangle d|\psi\rangle = \frac{D\delta_{m,0}\delta_{n,0} + \delta_{m,n}}{D+1} \quad (35)$$

Dado un canal  $\mathcal{E}$  cuya representación  $\chi$  esté dada por  $\mathcal{E}(\rho) = \sum_{mn} \chi_{mn} E_m \rho E_n^\dagger$ , podemos desarrollar la expresión para su fidelidad media como:

$$\begin{aligned} \bar{F}(\mathcal{E}) &\equiv \int \langle \psi | \mathcal{E}(P_\psi) | \psi \rangle d|\psi\rangle \\ &= \int \langle \psi | \sum_{mn} \chi_{mn} E_m P_\psi E_n^\dagger | \psi \rangle d|\psi\rangle \\ &= \sum_{mn} \chi_{mn} \frac{D\delta_{m,0}\delta_{n,0} + \delta_{m,n}}{D+1} \\ &= \frac{D\chi_{00} + \sum_m \chi_{mm}}{D+1} \end{aligned}$$

Si además,  $\mathcal{E}$  preserva trazas (Ec. 9), como hemos supuesto una base  $\{E_m\}$  de operadores ortonormales, la diagonal de la matriz  $\chi$  es una distribución de probabilidades (Ec. 10). Podemos entonces concluir que  $\sum_m \chi_{mm} = 1$ . Con lo cual, tenemos la siguiente relación sencilla entre la fidelidad media y  $\chi_{00}$ .

$$\bar{F}(\mathcal{E}) = \frac{D\chi_{00} + 1}{D+1} \quad (36)$$

De aquí, que puede usarse el resultado del experimento para estimar  $\chi_{00}$  como

$$\frac{(D+1)\bar{F}(\mathcal{E}) - 1}{D} = \chi_{00} \quad (37)$$

**Corolario 4.1.** De  $\bar{F}(\mathcal{E}) = \frac{D\chi_{00}+1}{D+1}$ , se desprende que sin importar que tan buena o mala es una operación, la fidelidad media no puede ser menor que  $\frac{1}{D+1}$ . Podemos expresar esto como:  $\bar{F}(\mathcal{E}) \in [\frac{1}{D+1}, 1]$ .

En particular, un operador unitario  $U$  debe tener traza 0 para minimizar su fidelidad media. Aun así, tiene fidelidad máxima para los  $D$  estados  $|\psi\rangle$  de la base ortonormal que diagonaliza a  $U$ . Es por ello que el estudio de la fidelidad media de  $U$  no puede limitarse a una base preseleccionada. Debe pues considerarse un conjunto más amplio de estados para el estudio de fidelidades.

Es natural preguntarse si es posible estimar otros coeficientes diagonales de  $\chi$ . Una respuesta inmediata a esto, surge de medir la fidelidad media del superoperador  $\mathcal{E}_s \equiv \rho \rightarrow \mathcal{E}(E_s^\dagger \rho E_s)$ . Para su construcción, solo es necesario contar con  $\mathcal{E}$  y una implementación perfecta del operador  $E_s^\dagger$ . Luego se utiliza la técnica preferida para medir la fidelidad media del canal modificado  $\mathcal{E}_s$ . El efecto de este canal esta descrito por:

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

Nuevamente, podemos expresar la fidelidad media de  $\mathcal{E}_s$  como:

$$\begin{aligned} \overline{F}(\mathcal{E}_s(P_\psi)) &\equiv \int \langle \psi | \mathcal{E}_s(P_\psi) | \psi \rangle d|\psi\rangle \\ &= \sum_{mn} \chi_{mn} \int \langle \psi | E_m E_s^\dagger P_\psi E_s E_n^\dagger | \psi \rangle d|\psi\rangle \\ &= \sum_{mn} \chi_{mn} \frac{\text{tr}(E_m E_s^\dagger) \text{tr}(E_s E_n^\dagger) + \text{tr}(E_m E_s^\dagger E_s E_n^\dagger)}{D(D+1)} \\ &= \frac{D^2 \chi_{ss} + \sum_{mn} \chi_{mn} \text{tr}(E_m E_s^\dagger E_s E_n^\dagger)}{D(D+1)} \\ &= \frac{D^2 \chi_{ss} + \text{tr}(\mathcal{E}(E_s^\dagger E_s))}{D(D+1)} \\ &= \frac{D^2 \chi_{ss} + \text{tr}(E_s^\dagger E_s)}{D(D+1)} \\ &= \frac{D \chi_{ss} + \delta_{ss}}{D+1} \\ &= \frac{D \chi_{ss} + 1}{D+1} \end{aligned}$$

Para justificar la simplificación de  $\text{tr}(\mathcal{E}(E_s^\dagger E_s)) = \text{tr}(E_s^\dagger E_s)$ , utilizamos que el superoperador  $\mathcal{E}$  preserva trazas (Ec. 9). Ahora, si  $E_s$  es unitario, podemos interpretar este resultado como *gate fidelity*, la fidelidad con la que  $\mathcal{E}$  implementa una compuerta  $E_s$ . Estará dada por  $\overline{F}(E_s, \mathcal{E}) = \overline{F}(\mathcal{E}_s) = \frac{D \chi_{ss} + 1}{D+1}$  y se encontrará siempre entre  $\frac{1}{D+1}$  y 1. Más aun, es importante notar que dado un canal  $\mathcal{E}$ , el coeficiente diagonal  $\chi_{ss}$  correspondiente al operador  $E_s$  tiene el mismo valor siempre y cuando la base de operadores utilizada para la representación  $\chi$  sea ortogonales e incluya a  $E_s$ . Notamos que tampoco es necesaria la condición  $E_0 = \mathbb{1}$  ya que no se utiliza en la derivación.

Pueden extraerse con el mismo concepto coeficientes no diagonales de la representación  $\chi$  de  $\mathcal{E}$ . Veamos que el siguiente promedio nos aporta información sobre el coeficiente  $\chi_{mn}$ .

$$\int \langle \psi | \mathcal{E}(E_m^\dagger P_\psi E_n) | \psi \rangle d|\psi\rangle = \frac{D \chi_{mn} + \delta_{mn}}{D+1} \quad (38)$$

Esta es una generalización bastante directa de la fórmula utilizada para expresar los coeficientes diagonales como promedios. La derivación es totalmente análoga salvo que el último paso introduce una  $\delta_{mn}$  que no admite reducción como con  $\delta_{ss} = 1$ .

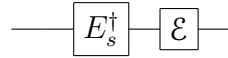
No obstante, es imposible encontrar una relación tan directa entre los coeficientes  $\chi_{mn}$  no diagonales y un observable físico, ya que en general, estos coeficientes son números complejos.

### 4.3. Representación circuital

Nuestro enfoque en esta sección se concentrará en la construcción de circuitos que contengan a  $\mathcal{E}$  y permitan caracterizar los distintos coeficientes de su matriz  $\chi$ . Para la construcción de los circuitos, asumimos operadores  $E_s$  unitarios para permitir su implementación. Nos contentaremos con construir circuitos cuya fidelidad media determine un coeficiente de  $\chi$ . Hay varias propuestas eficientes para la medición de fidelidades medias que se mostrarán en la próxima subsección (Sec 4.5).

#### 4.3.1. Circuito para coeficientes diagonales de chi

Los circuitos para la medición de coeficientes diagonales de  $\chi$  ya fueron sugeridos en la sección anterior. Siempre que los operadores  $E_s$  sean unitarios, se puede dar una implementación física de los mismos.



Recordemos que en los circuitos cuánticos el tiempo avanza de izquierda a derecha. Así pues, implementamos el canal  $\mathcal{E}_s$  cuya fidelidad nos proporciona  $\overline{F}(\mathcal{E}_s) = \frac{D\chi_{ss}+1}{D+1}$ .

Algo importante a notar, es que conmutar la aplicación de  $\mathcal{E}$  y  $E_s^\dagger$ , proporciona un canal con la misma fidelidad. Este nuevo canal, esta descrito por:

$$\rho \rightarrow \sum_{mn} \chi_{mn} E_s^\dagger E_m \rho E_n^\dagger E_s$$

A quantum circuit diagram consisting of two boxes connected in series. The first box is labeled  $\mathcal{E}$  and the second box is labeled  $E_s^\dagger$ . The circuit starts with a horizontal line entering the first box from the left and exits to the right, then continues into the second box and exits to the right.

De manera análoga a casos anteriores, podemos llegar a que su fidelidad esta dada por:

$$\sum_{mn} \chi_{mn} \frac{\text{tr}(E_s^\dagger E_m) \text{tr}(E_n^\dagger E_s) + \text{tr}(E_s^\dagger E_m E_n^\dagger E_s)}{D(D+1)}$$

Como la traza es cíclica tenemos que:

$$\text{tr}(E_s^\dagger E_m E_n^\dagger E_s) = \text{tr}(E_s E_s^\dagger E_m E_n^\dagger)$$

Como estamos considerando solo  $E_s$  unitarios, tenemos pues:

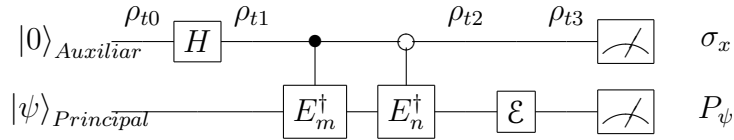
$$\text{tr}(E_s^\dagger E_m E_n^\dagger E_s) = \text{tr}(E_m E_n^\dagger)$$

A partir de aquí, la misma derivación que se utilizó para el circuito anterior nos permite llegar a la misma expresión  $\frac{D\chi_{ss}+1}{D+1}$  para la fidelidad media.

### 4.3.2. Circuito para coeficientes no diagonales de chi

A continuación, mostramos como pueden estimarse coeficientes no diagonales de la matriz  $\chi$  a partir de las fidelidades de circuitos que utilizan al superoperador  $\mathcal{E}$ . Un aspecto que deberemos tener en cuenta, para la medición de coeficientes no diagonales, es que estos son por lo general, números complejos. En el caso ideal, deberíamos encontrar un observable asociado a la parte real y otro a la parte imaginaria. Más aun, incluso las partes reales y partes imaginarias de los  $\chi_{mn}$  pueden ser tanto positivas como negativas, por lo que si la estimación se realiza en términos de fidelidades, debería ser un estimador basado en diferencia de fidelidades.

Presentamos a continuación un esquema tomográfico que nos permitirá estimar cualquier coeficiente seleccionado de  $\chi$ .



En este caso, lo que se busca medir es una diferencia de fidelidades en el sistema principal. Más concretamente, el estimador que nos proporcionará información sobre  $\chi_{mn}$  es diferencia de fidelidades medias del sistema principal, condicionales a cada autoestado de polarización en el qubit auxiliar.

Damos a continuación una descripción del estado del sistema en los distintos pasos del proceso. El estado inicial del sistema, puede expresarse como:

$$\rho_{t0} = |0\rangle \langle 0| \otimes P_\psi$$

Luego de aplicar la compuerta de Hadamard  $H$  (ver ecuación (83) de apéndice por más propiedades) en el qubit auxiliar, obtenemos:

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

$$\rho_{t1} = H |0\rangle \langle 0| H^\dagger \otimes P_\psi$$

$$\rho_{t1} = \frac{1}{2} (|0\rangle \langle 0| + |0\rangle \langle 1| + |1\rangle \langle 0| + |1\rangle \langle 1|) \otimes P_\psi$$

Luego de aplicar  $E_n^\dagger$  de manera controlada y  $E_m^\dagger$  complemento-controlada, el estado resultante queda entrelazado para obtener:

$$\rho_{t2} = \frac{1}{2} \left[ |0\rangle \langle 0| \otimes E_n^\dagger P_\psi E_n + |0\rangle \langle 1| \otimes E_n^\dagger P_\psi E_m + |1\rangle \langle 0| \otimes E_m^\dagger P_\psi E_n + |1\rangle \langle 1| \otimes E_m^\dagger P_\psi E_m \right]$$

Luego de aplicar el mapa  $\mathcal{E}$  sobre el sistema principal, obtenemos el estado:

$$\rho_{t3} = \sum_{m'n'} \frac{\chi_{m'n'}}{2} \left[ |0\rangle \langle 0| \otimes E_{m'} E_n^\dagger P_\psi E_n E_{n'}^\dagger + |0\rangle \langle 1| \otimes E_{m'} E_n^\dagger P_\psi E_m E_{n'}^\dagger + |1\rangle \langle 0| \otimes E_{m'} E_m^\dagger P_\psi E_n E_{n'}^\dagger + |1\rangle \langle 1| \otimes E_{m'} E_m^\dagger P_\psi E_m E_{n'}^\dagger \right]$$

El observable a medir es:  $\sigma_x \otimes P_\psi$ , donde  $\sigma_x$  vale 1 si el qubit auxiliar esta polarizado en el sentido de  $X$  y  $-1$  si esta polarizado en sentido contrario. Por otra parte, la medición de  $P_\psi$  resultará 1 si se mide supervivencia del estado inicial, y 0 en caso contrario.

Otra forma de interpretar esto, es la medición condicional de  $\sigma_x$ , solo en el caso de supervivencia de  $P_\psi$ . Con lo cual, en un primer paso, tomamos la traza parcial del sistema principal con respecto a  $P_\psi$ . Obtenemos así, una densidad reducida para el qubit auxiliar que es igual a:

$$\rho_{aux} = \sum_{m'n'} \frac{\chi_{m'n'}}{2} \left[ \begin{array}{l} |0\rangle \langle 0| \text{tr} \left( E_{m'} E_n^\dagger P_\psi E_n E_{n'}^\dagger P_\psi \right) + |0\rangle \langle 1| \text{tr} \left( E_{m'} E_n^\dagger P_\psi E_m E_{n'}^\dagger P_\psi \right) + \\ |1\rangle \langle 0| \text{tr} \left( E_{m'} E_m^\dagger P_\psi E_n E_{n'}^\dagger P_\psi \right) + |1\rangle \langle 1| \text{tr} \left( E_{m'} E_m^\dagger P_\psi E_m E_{n'}^\dagger P_\psi \right) \end{array} \right]$$

Ahora, por la ecuación 34, cuando tomamos el promedio sobre  $P_\psi$  con distribución uniforme sobre la medida de Fubini-Study o sobre un 2-diseño de estados, obtenemos:

$$\overline{\rho_{aux}} = \sum_{m'n'} \frac{\chi_{m'n'}}{2D(D+1)} \left[ \begin{array}{l} |0\rangle \langle 0| \left( \text{tr} \left( E_{m'} E_n^\dagger \right) \text{tr} \left( E_n E_{n'}^\dagger \right) + \text{tr} \left( E_{m'} E_n^\dagger E_n E_{n'}^\dagger \right) \right) + \\ |0\rangle \langle 1| \left( \text{tr} \left( E_{m'} E_n^\dagger \right) \text{tr} \left( E_m E_{n'}^\dagger \right) + \text{tr} \left( E_{m'} E_n^\dagger E_m E_{n'}^\dagger \right) \right) + \\ |1\rangle \langle 0| \left( \text{tr} \left( E_{m'} E_m^\dagger \right) \text{tr} \left( E_n E_{n'}^\dagger \right) + \text{tr} \left( E_{m'} E_m^\dagger E_n E_{n'}^\dagger \right) \right) + \\ |1\rangle \langle 1| \left( \text{tr} \left( E_{m'} E_m^\dagger \right) \text{tr} \left( E_m E_{n'}^\dagger \right) + \text{tr} \left( E_{m'} E_m^\dagger E_m E_{n'}^\dagger \right) \right) \end{array} \right]$$

Podemos hacer la simplificación  $\text{tr} \left( E_m E_n^\dagger \right) = D\delta_{mn}$  utilizando que los  $E_k$  son ortogonales. También es posible usar que el canal  $\mathcal{E}$  conserva trazas para simplificar los términos de la derecha.

$$\overline{\rho_{aux}} = \sum_{m'n'} \frac{\chi_{m'n'}}{2D(D+1)} \left[ \begin{array}{l} |0\rangle \langle 0| D^2 \delta_{m'n} \delta_{nn'} + \\ |0\rangle \langle 1| D^2 \delta_{m'n} \delta_{mn'} + \\ |1\rangle \langle 0| D^2 \delta_{m'm} \delta_{nn'} + \\ |1\rangle \langle 1| D^2 \delta_{m'm} \delta_{mn'} \end{array} \right] + \frac{1}{2D(D+1)} \left[ \begin{array}{l} |0\rangle \langle 0| \text{tr} \left( E_n^\dagger E_n \right) + \\ |0\rangle \langle 1| \text{tr} \left( E_n^\dagger E_m \right) + \\ |1\rangle \langle 0| \text{tr} \left( E_m^\dagger E_n \right) + \\ |1\rangle \langle 1| \text{tr} \left( E_m^\dagger E_m \right) \end{array} \right]$$

Utilizando nuevamente la ortonormalidad de los operadores y las sumas sobre  $\delta$  de Kronecker, podemos reducir la expresión derecha a:

$$\overline{\rho_{aux}} = \frac{1}{2D(D+1)} \left[ \begin{array}{l} |0\rangle \langle 0| (D^2 \chi_{nn} + D) + |0\rangle \langle 1| (D^2 \chi_{nm} + D\delta_{nm}) + \\ |1\rangle \langle 0| (D^2 \chi_{mn} + D\delta_{mn}) + |1\rangle \langle 1| (D^2 \chi_{mm} + D) \end{array} \right]$$

Simplificando un factor  $D$  podemos dar la matriz  $\overline{\rho_{aux}}$  explícitamente como:

$$\overline{\rho_{aux}} = \frac{1}{2(D+1)} \begin{pmatrix} D\chi_{nn} + 1 & D\chi_{nm} + \delta_{nm} \\ D\chi_{mn} + \delta_{mn} & D\chi_{mm} + 1 \end{pmatrix} \quad (39)$$

Ahora veamos que la información sobre  $\chi_{mn}$  se encuentra codificada en la polarización horizontal (ejes  $X$  e  $Y$ ) del qubit auxiliar en  $\rho_{aux}$ .

Para ver esto, podemos escribir  $\overline{\rho_{aux}}$  en términos de las matrices de Pauli  $\mathbb{1}, \sigma_x, \sigma_y, \sigma_z$ .

$$\overline{\rho_{aux}} = \frac{D(\chi_{nn} + \chi_{mm}) + 2}{4(D+1)} \mathbb{1} + \frac{D\text{Re}(\chi_{mn}) + \delta_{mn}}{2(D+1)} \sigma_x + \frac{D\text{Im}(\chi_{mn})}{2(D+1)} \sigma_y + \frac{D(\chi_{nn} - \chi_{mm})}{4(D+1)} \sigma_z$$

La fidelidad media del canal principal, esta dada por la traza de  $\overline{\rho_{aux}}$ :

$$\frac{D\frac{\chi_{nn} + \chi_{mm}}{2} + 1}{D+1}$$

Condicional a esta supervivencia en el canal principal, podemos medir la parte real y la parte imaginaria de  $\chi_{mn}$  a través de los observables  $\sigma_x$  y  $\sigma_y$  sobre el qubit auxiliar.

Por ejemplo, la polarización en  $x$ , dada por  $\overline{\rho_{aux}}\sigma_x$ , nos proporciona la información suficiente para reconstruir  $\text{Re}(x_{mn})$ .

$$\text{tr}(\overline{\rho_{aux}}\sigma_x) = \frac{D\text{Re}(x_{mn}) + \delta_{mn}}{D+1}$$

Ya que despejando explícitamente, tenemos:

$$\text{Re}(x_{mn}) = \frac{(D+1)\text{tr}(\overline{\rho_{aux}}\sigma_x) - \delta_{mn}}{D}$$

Si en cambio medimos la polarización del qubit auxiliar en el eje  $y$ , obtenemos:

$$\text{tr}(\overline{\rho_{aux}}\sigma_y) = \frac{D\text{Im}(x_{mn})}{D+1}$$

El segundo estimador de interés nos provee pues la parte imaginaria del coeficiente  $\chi_{mn}$ .

$$\text{Im}(x_{mn}) = \frac{(D+1)\text{tr}(\overline{\rho_{aux}}\sigma_y)}{D}$$

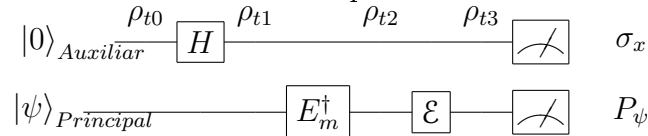
Por último, medir  $\sigma_z$  nos da información acerca de la diferencia  $\chi_{nn} - \chi_{mm}$ .

$$\chi_{nn} - \chi_{mm} = \frac{2(D+1)\text{tr}(\overline{\rho_{aux}}\sigma_z)}{D}$$

Notamos que si,  $m = n$ , el qubit auxiliar se encuentra en un estado totalmente polarizado en el eje  $X$ :

$$\overline{\rho_{aux}} = \left[ \begin{array}{c} \frac{d\chi_{mm}+1}{2(d+1)} \sigma_x + \\ \frac{d\chi_{mm}+1}{2(d+1)} \mathbb{1} \end{array} \right]$$

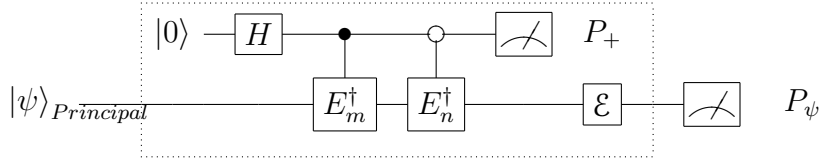
El resultado solo depende de la probabilidad de supervivencia en el sistema principal. Una manera de ver esto, es mediante el circuito equivalente:



Aquí, el sistema principal resulta desacoplado del auxiliar debido a que se realiza la misma operación independientemente del valor del qubit auxiliar (ver apéndice A.3). Recuperamos pues los resultados en la subsección anterior para la medición de coeficientes diagonales.

#### 4.4. Estimadores en términos de fidelidades

La polarización en el qubit auxiliar puede pensarse como:  $\sigma_x = P_+ - P_-$ . Podemos considerar la fidelidad media del sistema principal en un canal en el que solo se consideran los experimentos en los que el qubit auxiliar termine en el estado  $|+\rangle$ , Utilizando este resultado, las cantidades necesarias para estimar  $\text{Re}(\chi_{mn})$  o  $\text{Im}(\chi_{mn})$  pueden estimarse como la diferencia entre dos fidelidades medias, donde el canal se define haciendo poselección sobre las mediciones en el sistema auxiliar. En el rectángulo delimitado por la línea de puntos del siguiente circuito, se representa un canal  $\mathcal{E}_{mn+}$  con poselección al que se le debe medir la fidelidad.



Análogamente, se definen los canales  $\mathcal{E}_{mn-}$ ,  $\mathcal{E}_{mn,+i}$  y  $\mathcal{E}_{mn,-i}$  de acuerdo a poselecciones sobre la polarización de qubit auxiliar. Esto nos muestra que podemos expresar los coeficientes  $\chi_{mn}$  en términos de mediciones de fidelidades.

$$\text{Re}(\chi_{mn}) = \frac{(D+1)(\overline{F}(\mathcal{E}_{mn+}) - \overline{F}(\mathcal{E}_{mn-})) - \delta_{mn}}{D} \quad (40)$$

$$\text{Im}(\chi_{mn}) = \frac{(D+1)(\overline{F}(\mathcal{E}_{mn,+i}) - \overline{F}(\mathcal{E}_{mn,-i}))}{D} \quad (41)$$

$$(42)$$

#### 4.5. Medición de fidelidad

El resultado principal de esta sección ha sido reducir el problema de medir coeficientes arbitrarios de la matriz  $\chi$  de un canal a la medición de fidelidades medias. A continuación mencionamos algunas posibles respuestas al problema de medir fidelidades.

##### 4.5.1. Utilizar DCQD o SCNQP para medir fidelidades medias

El método tomográfico DCQD permite medir selectivamente cualquier coeficiente diagonal. En particular, puede utilizarse para medir el coeficiente  $\chi_{00}$  que determina la fidelidad del proceso. Aunque esta propuesta parece no tener mucho sentido, la combinación propuesta, aplicada sobre los canales  $\chi_{mn\pm}$  y  $\chi_{mn\pm i}$ , permite medir de manera eficiente coeficientes no diagonales  $\chi_{mn}$  del proceso original.

En el caso de SCNQP, este permite medir eficientemente la fidelidad de un proceso. Aplicándolo sobre las modificaciones propuestas del proceso original, también permitirá la estimación eficiente de cualquier otro coeficiente de la matriz  $\chi$  original.

### 4.5.2. Usar 2-diseños de estados para medir fidelidades medias

Las mediciones cuánticas son de naturaleza inherentemente probabilística. Consideremos por ejemplo, preparar un estado  $|\psi\rangle$ , luego dejarlo evolucionar bajo un operador  $\mathcal{E}$  y finalmente medir si sigue en el mismo estado. Cada medición de este tipo puede resultar en dos posibilidades, 1 si el sistema se encuentra finalmente en  $|\psi\rangle$  y 0 si el sistema no se encuentra en  $|\psi\rangle$  (se encontrará pues en  $|\psi\rangle^\perp$ ). Si realizamos un gran número de mediciones promediando los valores obtenidos, llegamos a un buen estimador  $p$  de  $\langle\psi|\mathcal{E}(P_\psi)|\psi\rangle$ .

Una vez comprendido esto, podemos argumentar, que es posible introducir aleatoriedad en el experimento más allá de la propia aleatoriedad inherente a la medición. Por ejemplo, dada la siguiente formula para la fidelidad media de un mapa  $\mathcal{E}$ :

$$\overline{F}(\mathcal{E}) \equiv \int \langle\psi|\mathcal{E}(P_\psi)|\psi\rangle d|\psi\rangle$$

Una lectura posible de esta formula puede decirnos que para calcular la fidelidad media de un mapa  $\mathcal{E}$ , es necesario promediar la probabilidad de supervivencia de todos los estados puros posibles  $|\psi\rangle$  en el espacio de Hilbert en el que actúa. Esta lectura es difícil, si no imposible de llevar a la práctica. Otra lectura posible es que la fidelidad media del operador  $\mathcal{E}$  esta dada por medir la probabilidad de supervivencia de un estado puro generado al azar con una distribución uniforme sobre la medida de Fubini-Study. De esta manera, la receta para medir la fidelidad media se vuelve más simple:

1. Preparar un estado puro al azar  $\psi$ .
2. Aplicar el mapa  $\mathcal{E}$  al estado preparado.
3. Medir si el estado final es el mismo que el preparado.
4. Promediar los resultados de las  $M$  mediciones así realizadas.

$$|\psi\rangle \text{ --- } \boxed{\mathcal{E}} \text{ --- } \boxed{\text{A}} \quad P_\psi$$

Donde  $|\psi\rangle$  se toma aleatoriamente entre estados puros.

El valor resultante es un estimador no sesgado de la fidelidad  $\overline{F}$  con varianza  $2\overline{F}(1-\overline{F})/M < 1/2M$ . Esta receta tan simple de enunciar, puede resultar difícil de llevar a la práctica. Los problemas que se encuentran para la implementación corresponden a los pasos 1 y 3 de la misma.

Por un lado, la generación de un estado aleatorio uniformemente distribuido corresponde a tener un sistema en equilibrio térmico a temperatura infinita<sup>6</sup>. Sin embargo, esta posibilidad, no nos permite conocer el estado sin hacer una medición destructiva sobre el mismo. Es por ello que tampoco podremos medir la probabilidad de supervivencia del mismo ya que no

<sup>6</sup>Temperatura muy grande con respecto a las diferencias energéticas de los distintos estados accesibles

sabremos de que estado se trata. Analizaremos esta propuesta con más detalle una vez que hayamos presentado las herramientas necesarias para que este camino resulte viable.

Es por eso que las implementaciones de tomografía de procesos cuánticos (TPC) hasta el momento, requieren preparar distintos estados iniciales de manera controlada. Y luego medir en cada caso la probabilidad de supervivencia y/o transición del estado preparado. Nuevamente, estamos en problemas, ya que la complejidad de la preparación controlada de un estado puro arbitrario en un sistema de dimensión  $D$ , crece polinomialmente con  $D$ , es decir exponencialmente con el número  $N$  de subsistemas.

Notemos que dado un canal  $\mathcal{E}$ , la fidelidad de estado es un polinomio homogéneo de grado 2 en  $|\psi\rangle$  y en  $\langle\psi|$ . Existen conjuntos finitos de estados sobre los cuales el valor medio de estos polinomios es igual al promedio sobre todo el espacio de Hilbert. Estos conjuntos de estados se denominan 2-diseños y su utilidad para medir fidelidades fue señalada en la tesis de maestría de Christoph Dankert [Dan05]. Por el momento, solo precisamos saber que podemos limitar el sorteo de estados iniciales a un conjunto finito de estados  $X$  (un 2-diseño de estados) en lugar de sortear sobre el conjunto completo de estados puros.

$$|\psi\rangle \text{---} \boxed{\mathcal{E}} \text{---} \boxed{\text{A}} \quad P_\psi$$

Donde  $|\psi\rangle$  se toma aleatoriamente de  $X$ .

La varianza del estimador luego de  $M$  mediciones independientes será de  $\frac{2\overline{F}(\mathcal{E})(1-\overline{F}(\mathcal{E}))}{M}$ .

Otra posibilidad, es medir la probabilidad de supervivencia  $\langle\psi| \mathcal{E}(P_\psi) |\psi\rangle$  para cada estado  $|\psi\rangle$  en el 2-diseño  $X$  de manera exacta y el promedio de estos valores nos dará el resultado preciso esperado.

$$\overline{F}(\mathcal{E}) = \frac{1}{|X|} \sum_{|\psi\rangle \in X} \langle\psi| \mathcal{E}(P_\psi) |\psi\rangle$$

Lamentablemente  $X$  contiene una cantidad exponencial de estados (como mínimo  $D^2$ ) por lo que esta última propuesta deja de ser viable para  $N$  grande.

Ahora bien, la pregunta que debemos hacernos ahora es:

*“¿Es posible obtener de manera eficiente los estados pertenecientes a un 2-diseño?”*

Este problema ha sido estudiado por Christoph Dankert en su tesis de Maestría [Dan05] y retomado por Ariel Bendersky en su tesis de licenciatura [Ben06]. Ambos estudian el uso de bases mutuamente no sesgadas como 2-diseños para la medición de la fidelidades. Tanto en la tesis de Dankert [Dan05] como en la de Bendersky [Ben06] se muestra como se pueden construir circuitos cuánticos para generar elementos arbitrarios de un conjunto maximal de bases mutuamente no sesgadas utilizando  $O(N^2)$  compuertas. En la sección 5 presentaremos las propiedades de los 2-diseños y su relación con las bases mutuamente no sesgadas. Con esta base, daremos en la sección 6 una definición explícita de un 2-diseño de estados que permite una construcción eficiente <sup>7</sup> para la construcción de cada estado. La crítica que admite esta

---

<sup>7</sup>Se requeriran  $O(N^3)$  operaciones clásicas y un circuito con  $O(N^2)$  compuertas cuánticas elementales.

propuesta, es que se precisa realizar un gran número de operaciones  $O(N^2)$  con una fidelidad total más alta que la del proceso que se busca caracterizar.

C. Dankert, J. Emerson y et al. proponen, tanto en la tesis de maestría del primero [Dan05] como en un artículo posterior [DCEL06], el uso de 2-diseños aproximados de operadores unitarios para la medición de fidelidades. Muestran como un 2-diseño de operadores unitarios  $X_U$ , induce, al aplicarse sobre cualquier estado  $|\psi_0\rangle$  un 2-diseño de estados  $X$ . Proponen utilizar un circuito con  $O(N \log(1/\epsilon))$  compuertas y profundidad  $O(\log(N) \log(\epsilon))$  para inducir una distribución de estados que muestra una distancia  $\epsilon + 1/4^N$  de un 2-diseño de estados para un sistema de  $N$  qubits. Tomando la perspectiva de simetrización del canal, llegan a la conclusión de que con un número de experimentos independiente de  $D$  utilizando este circuito, pueden estimar la fidelidad media con un error  $\delta > 1/4^N$ .

## 5. $t$ -diseños y Bases Mutuamente no Sesgadas

### 5.1. Introducción a los $t$ -diseños

Un polinomio  $p$  es homogéneo de grado  $t$  en las variables  $x_1, x_2, \dots, x_n$  si  $p(\lambda x_1, \lambda x_2, \dots, \lambda x_n) = \lambda^t p(x_1, x_2, \dots, x_n)$ . Equivalentemente, cada monomio que lo compone, tiene exactamente  $t$  factores pertenecientes a  $\{x_1, \dots, x_n\}$ .

Para introducir la noción de  $t$ -diseños y desarrollar una intuición de cómo funcionan, consideremos los polinomios  $p(x) = ax + b$  de grado 1 en una sola variable con dominio en  $[-1, 1]$ . En este caso, es fácil ver que:

$$\int_0^1 p(x) dx = \frac{1}{2}a + b = p\left(\frac{1}{2}\right)$$

En el caso de polinomios  $p(x) = ax^2 + bx + c$  de grado 2, podemos con un razonamiento similar, obtener:

$$\int_0^1 p(x) dx = \frac{1}{3}a + \frac{1}{2}b + c = \frac{p\left(\frac{1}{2} + \frac{1}{\sqrt{12}}\right) + p\left(\frac{1}{2} - \frac{1}{\sqrt{12}}\right)}{2}$$

Esto nos muestra que para evaluar la integral de un polinomio, nos alcanza con evaluar al mismo sobre un número finito de puntos y tomar el promedio sobre estos. Sin embargo, es importante elegir correctamente el conjunto de puntos que se utiliza. Esta técnica tiene gran uso para problemas de integración numérica. Estos problemas toman el nombre de cuadratura o cubatura según se trate respectivamente de integrales en una o múltiples variables. También es posible elegir conjuntos de puntos apropiados cuando la integración se realiza sobre un espacio algo más complejo, como la superficie de una esfera en un espacio de múltiples variables. P. Delsarte [DGS77] fue el primero en estudiar sistemáticamente el problema de integrar polinomios sobre una esfera promediando sobre un subconjunto finito de puntos. A partir de sus trabajos, estos conjuntos de puntos tomaron el nombre de códigos y diseños esféricos.

En el caso de la mecánica cuántica, el espacio de integración pertinente, es el espacio de Hilbert de los estados, y la medida unitariamente invariante que se utiliza para promediar sobre los mismos se llama medida de Fubini-Study. Otra propiedad de las cantidades a promediar, es que siempre aparecen igual cantidad de factores bra como factores ket.

Un  $t$ -diseño de estados cuánticos es pues, un conjunto de estados puros que permite evaluar de forma fiel el valor medio de polinomios de grado  $t$  en las componentes de un bra y grado  $t$  en las componentes del ket correspondiente.

En particular, cualquier conjunto de vectores que forme una base  $\mathcal{B}$  ortonormal del espacio de Hilbert  $\mathcal{H}$  de dimensión  $D$ , constituye un 1-diseño de estados.

$$\int_{F-S} \langle \psi | O | \psi \rangle d|\psi\rangle = \text{tr}(O) = \frac{1}{D} \sum_{|\psi\rangle \in \mathcal{B}} \langle \psi | O | \psi \rangle$$

El término  $\text{tr}(O)$  se obtiene de un cálculo explícito de la integral. A menos de una constante multiplicativa, es el único término posible que es lineal en  $O$  y unitariamente invariante. Notemos que las componentes de  $O$  representan en  $\langle \psi | O | \psi \rangle$  los coeficientes correspondientes a cada uno de los monomios en las componentes de  $\langle \psi |$  y  $|\psi \rangle$ .

Para que el conjunto  $X$  sea un 2-diseño de estados, es necesario y suficiente pedir que se preserven todas las integrales de la forma:

$$\int_{F-S} \langle \psi | O_1 | \psi \rangle \langle \psi | O_2 | \psi \rangle d\psi = \frac{1}{|X|} \sum_{|\psi\rangle \in \mathcal{B}} \langle \psi | O_1 | \psi \rangle \langle \psi | O_2 | \psi \rangle$$

Esto permite expresar cualquier combinación de monómios de grado 2 en los elementos de  $|\psi \rangle$  y grado 2 en los elementos de  $\langle \psi |$ . También puede encontrarse la forma explícita de estas integrales. Se trata de:

$$\int_{F-S} \langle \psi | O_1 | \psi \rangle \langle \psi | O_2 | \psi \rangle d\psi = \frac{\text{tr}(O_1 O_2) + \text{tr}(O_1) \text{tr}(O_2)}{D(D+1)}$$

## 5.2. Cuatro definiciones de $t$ -diseños

En esta subsección damos cuatro maneras equivalentes de definir los  $t$ -diseños de estados, que nos proveen los medios para entenderlos y nos permitirán relacionar los 2-diseños con las bases mutuamente no sesgadas. Imitamos la presentación de Andreas Klappenecker y Martin Rötteler [KR05], quienes demuestran la equivalencia de distintas definiciones de  $t$ -diseños para así llegar a un mayor entendimiento de los mismos.

**Lemma 5.1.** Si integramos sobre la esfera compleja para cualquier vector normalizado  $|\phi\rangle$ , tenemos que:

$$\int |\langle \psi | \phi \rangle|^{2k} d\psi = \frac{1}{\binom{D+k-1}{k}}$$

Demostración: Sin importar de que vector normalizado  $\phi$  se trate, existe un operador unitario  $U$  que mapea  $\phi$  al primer vector de la base canónica,  $U|\phi\rangle = |e_1\rangle$ . Entonces tenemos:

$$\int |\langle \psi | \phi \rangle|^{2k} d\psi = \int |\langle \psi U^\dagger | e_1 \rangle|^{2k} d\psi =$$

Como la integral es unitariamente invariante, esto es equivalente a:

$$\int |\langle \psi | e_1 \rangle|^{2k} d\psi = \int |\psi_1|^{2k} d\psi =$$

Donde  $\psi_1$  se refiere a la primer componente de  $\psi$  en su representación canónica. La proposición 1.4.9 del libro de Rudin [Rud80] permite finalmente evaluar esta integral a:

$$\frac{1}{\binom{D+k-1}{k}}$$

Notamos que en el caso particular,  $k = 0$ , esto señala que la integral esta normalizada. En el caso particular  $k = 1$ , esto puede obtenerse de que la proyección promedio sobre cada uno de  $D$  vectores de una base ortonormal es la misma, y suman  $1 = \psi_1^2 + \psi_2^2 + \dots + \psi_D^2$ .

**Teorema 5.2.** Dado un conjunto finito no vacio  $X$  de estados puros, las siguientes condiciones son equivalentes:

1.  $X$  es un  $t$ -diseño. Es decir que para todo polinomio  $p(|\psi\rangle, \langle\psi|)$  homogeneo de grado  $t$  en las componentes de  $|\psi\rangle$  y homogeneo de grado  $t$  en las componentes de  $\langle\psi|$ , tenemos que:

$$\int p(|\psi\rangle, \langle\psi|) d|\psi\rangle = \frac{1}{|X|} \sum_{|\psi\rangle \in X} p(|\psi\rangle, \langle\psi|)$$

Notemos que tanto en la integral como en la suma, solo se consideran estados  $|\psi\rangle$  normalizados.

2. Para todo vector del espacio de Hilbert  $|\phi\rangle$  y para todo  $k$  tal que  $0 \leq k \leq t$  vale la igualdad:

$$\frac{1}{|X|} \sum_{|\psi\rangle \in X} |\langle\phi|\psi\rangle|^{2k} = \frac{\langle\phi|\phi\rangle^k}{\binom{D+k-1}{k}}$$

3. Para todo  $k$  tal que  $0 \leq k \leq t$ , el conjunto  $X$  satisface:

$$\frac{1}{|X|^2} \sum_{|\psi\rangle, |\phi\rangle \in X} |\langle\phi|\psi\rangle|^{2k} = \frac{1}{\binom{D+k-1}{k}}$$

4. Los siguientes tensores de rango  $2t$  son equivalentes

$$\frac{1}{|X|} \sum_{|\psi\rangle \in X} |\psi\rangle^{\otimes t} \langle\psi|^{\otimes t} = \int |\psi\rangle^{\otimes t} \langle\psi|^{\otimes t} d|\psi\rangle$$

**Demostración:** Probaremos cíclicamente que cada condición implica la siguiente.

1.  $\Rightarrow$  1+. Si  $X$  es un  $t$ -diseño, entonces  $X$  es un  $k$ -diseño para todo  $k$  tal que  $0 \leq k \leq t$ . Simplemente es necesario observar que si  $p(|\psi\rangle, \langle\psi|)$  es un polinomio homogeneo de grado  $k$  en las componentes de  $|\psi\rangle$  y grado  $k$  en las componentes de  $\langle\psi|$ , entonces puede verse que para los vectores  $|\psi\rangle$  normalizados, el polinomio  $p(|\psi\rangle, \langle\psi|) \times \langle\psi|\psi\rangle^{(t-k)}$  es equivalente a  $p(|\psi\rangle, \langle\psi|)$  y homogeneo de grado  $t$ . Luego, la evaluación de un polinomio homogeneo de grado  $k \leq t$  en un  $t$ -diseño dara correctamente el valor correspondiente a un  $k$ -diseño.

- 1+  $\Rightarrow$  2. Fijado un vector  $\phi$ , tenemos que  $p(|\psi\rangle, \langle\psi|) = |\langle\phi|\psi\rangle|^{2k} = \langle\phi|\psi\rangle^k \langle\psi|\phi\rangle^k$  es un polinomio homogéneo de grado  $k$  en las componentes de  $|\psi\rangle$  y grado  $k$  en las componentes de  $\langle\psi|$ . Luego, la sumatoria en el lado izquierdo de 2. puede pasarse a una integral, que puede evaluarse utilizando (Lemma 5.1) obteniéndose así la expresión dada a la derecha de la igualdad.
2.  $\Rightarrow$  3. Si instanciamos y sumamos la igualdad en 2. sobre todos los  $|\phi\rangle \in X$ , obtenemos la igualdad expresada en 3. multiplicada por  $|X|$ .
3.  $\Rightarrow$  4. Supongamos que la ecuación 3. es válida. Para un vector  $|\psi\rangle$ , denotamos  $|\psi\rangle^{\otimes t}$  al producto tensorial de  $t$  copias de  $|\psi\rangle$  (no se contrae ningún índice). Notemos que  $\langle\psi|\phi\rangle^t = \langle\psi|^{\otimes t}|\phi\rangle^{\otimes t}$ . Consideremos el siguiente tensor de rango  $t, t$ :

$$\xi = \frac{1}{|X|} \sum_{\psi \in X} |\psi\rangle^{\otimes t} \langle\psi|^{\otimes t} - \int |\psi\rangle^{\otimes t} \langle\psi|^{\otimes t} d\psi$$

Podemos evaluar la norma de  $\xi$  como  $\text{tr}(\xi\xi^\dagger) \geq 0$ . Una evaluación explícita proporciona el siguiente resultado:

$$\begin{aligned} \text{tr}(\xi\xi^\dagger) &= \frac{1}{|X|^2} \sum_{\psi, \phi \in X} \langle\phi|\psi\rangle^t \langle\psi|\phi\rangle^t - \int \frac{1}{|X|} \sum_{\phi \in X} \langle\phi|\psi\rangle^t \langle\psi|\phi\rangle^t d\psi \\ &\quad - \frac{1}{|X|} \sum_{\psi \in X} \int \langle\phi|\psi\rangle^t \langle\psi|\phi\rangle^t d\phi + \int \int \langle\phi|\psi\rangle^t \langle\psi|\phi\rangle^t d\psi d\phi \\ &= \frac{1}{|X|^2} \sum_{\psi, \phi \in X} |\langle\phi|\psi\rangle|^{2t} - \frac{1}{|X|} \sum_{\phi \in X} \int |\langle\phi|\psi\rangle|^{2t} d\psi \\ &\quad - \frac{1}{|X|} \sum_{\psi \in X} \int |\langle\phi|\psi\rangle|^{2t} d\phi + \int \int |\langle\phi|\psi\rangle|^{2t} d\psi d\phi \end{aligned}$$

La doble suma vale por hipótesis  $\binom{D+t-1}{t}^{-1}$ . Por el lema (Lema: 5.1), todas las integrales simples también se evalúan a  $\binom{D+t-1}{t}^{-1}$ . La suma está normalizada por el factor  $|X|^{-1}$  y la segunda integral también está normalizada, ya que corresponde a la medida de Fubini-Study. Podemos concluir que como los cuatro términos valen lo mismo, su suma se anula y  $\text{tr}(\xi\xi^\dagger) = 0$ . La única manera de que la norma del tensor hermitico  $\xi$  se anule, es que el mismo tensor se anule,  $\xi = 0$ . Con esto concluimos que:

$$\frac{1}{|X|} \sum_{\psi \in X} |\psi\rangle^{\otimes t} \langle\psi|^{\otimes t} = \int |\psi\rangle^{\otimes t} \langle\psi|^{\otimes t} d\psi$$

4.  $\Rightarrow$  1. Cada una de las componentes del tensor  $|\psi\rangle^{\otimes t} \langle\psi|^{\otimes t}$  es uno de los monomios posibles de grado  $t$  en las componentes de  $|\psi\rangle$  y grado  $t$  en las componentes de  $\langle\psi|$  estando todos

los monomios incluidos con todos los ordenamientos de factores posibles. Con lo cual, la definición 4. implica que promediar sobre la medida de Fubini-Study y promediar sobre el conjunto  $X$  es equivalente para cualquier monomio homogéneo de grado  $t, t$ . Luego, por linealidad, el valor medio sobre  $X$  de cualquier polinomio homogéneo de grado  $t, t$  da el valor correcto correspondiente a la integral de Fubini-Study. Es decir que  $X$  cumple con la definición 1. de  $t$ -diseño de estados.

**Q.E.D.**

El cuarto paso (3.  $\Rightarrow$  4.) de la demostración anterior, puede generalizarse a una desigualdad que toma el nombre de cota de Welch. Esta desigualdad fue derivada por L. Welch en un artículo de 1974 [Wel74] en el que buscaba acotar que tan pequeña podían ser las correlaciones mutuas de un conjunto de señales.

**Corolario 5.3.** Cota de Welch: Para todo conjunto de estados normalizados  $X$ , vale que:

$$\frac{1}{|X|^2} \sum_{\psi, \phi \in X} |\langle \phi | \psi \rangle|^{2k} \geq \frac{1}{\binom{D+k-1}{k}}$$

**Demostración:** Si utilizamos un conjunto  $X$  tal que

$$\frac{1}{|X|^2} \sum_{\psi, \phi \in X} |\langle \phi | \psi \rangle|^{2k} < \frac{1}{\binom{D+k-1}{k}}$$

en la construcción del tensor hermítico  $\xi$  de la demostración anterior, este tendrá norma negativa. Absurdo, que surge de suponer que se puede violar la desigualdad de Welch. **Q.E.D.**

### 5.3. Bases mutuamente no sesgadas (MUBs)

Las bases mutuamente no sesgadas (MUBs)<sup>8</sup>, representan una posible realización del principio de complementariedad. Este principio, fue introducido por Bohr [KR05, Boh28] en 1928. El ejemplo más conocido de complementariedad, es entre el momento y posición de una partícula cuántica. Si medimos el impulso de una partícula cuya posición está “bien definida”, el valor obtenido no nos proporcionará absolutamente ninguna información acerca del estado original de la misma, ya que todos los impulsos resultan en este caso igualmente probables. Análogamente, si medimos la posición  $x$  de una partícula cuyo impulso  $p$  está bien definido, tampoco obtenemos información sobre el estado original de la partícula, ya que todas las posiciones resultan igualmente probables. Esto puede expresarse mediante la siguiente relación entre los autoestados de impulso y de posición.

$$\int e^{\frac{ipx}{\hbar}} |x\rangle dx = |p\rangle \tag{43}$$

---

<sup>8</sup>Del inglés *mutually unbiased basis*.

Donde  $|x\rangle$  es un autovector de  $X$  con autovalor  $x$ ,  $|p\rangle$  un autovector de  $P$  con autovalor  $p$ . Diremos pues, que dos bases ortonormales  $\mathcal{B}_1$  y  $\mathcal{B}_2$  son mutuamente no sesgadas, si al hacer una medición proyectiva en la base  $\mathcal{B}_2$  de cualquier autoestado de  $\mathcal{B}_1$ , se obtienen todos los resultados posibles con igual probabilidad. La noción de complementaridad también tiene sentido en espacios de dimensión finita, donde el manejo de los espacios de Hilbert requiere de menos sutileza matemáticas. En este caso, podemos dar una definición compacta y simétrica de que dos bases sean mutuamente no sesgadas.

**Definición 5.4.** Dadas dos bases ortonormales  $\mathcal{B}_1 = \{|\psi_i\rangle, i = 1 \dots D\}$  y  $\mathcal{B}_2 = \{|\phi_i\rangle, i = 1 \dots D\}$  del espacio de Hilbert de dimensión  $D$ . Se dice que son mutuamente no sesgadas si y solo si:

$$\forall i, j \quad |\langle \psi_i | \phi_j \rangle|^2 = \frac{1}{D} \quad (44)$$

Los autoestados de polarización en los ejes ortogonales  $X$  y  $Z$  de una partícula de espín  $\frac{1}{2}$  proporcionan el ejemplo más sencillo de este concepto en un espacio de Hilbert de dimensión 2. Como se mostró en el experimento de Stern-Gerlach, medir la polarización de una partícula en el eje  $X$ , implica máxima incerteza para la polarización en el eje perpendicular  $Z$ . La primer medición de la experiencia, colapsa la partícula a un autoestado de polarización en  $X$  mientras que la segunda obtiene con probabilidad  $1/2$  cada una de las dos polarizaciones posibles en el eje  $Z$ . Los observables  $X$  y  $Z$  se llaman pues observables complementarios.

Gran parte de la bibliografía dedicada a las bases mutuamente no sesgadas trata el tema de construir conjuntos maximales de bases mutuamente no sesgadas dos a dos en espacios de dimensión finita  $D$ . Un resultado conocido es que bajo ninguna circunstancia pueden encontrarse más de  $D+1$  bases mutuamente no sesgadas. Daremos una demostración de este hecho basada en la cota de Welch (Corolario 5.3). Pero primero, mostraremos un resultado que relaciona las bases mutuamente no sesgadas con los 2-diseños y resulta fundamental para nuestro trabajo.

**Corolario 5.5.** Si consideramos un espacio de Hilbert finito de dimensión  $D$ , las siguientes afirmaciones son validas.

- a Existen como máximo  $D+1$  bases mutuamente no sesgadas.
- b Los estados pertenecientes a un conjunto de  $D+1$  bases mutuamente no sesgadas forma un 2-diseño de estados.

**Demostración:** Sea  $X$  el conjunto de los  $B \times D$  estados pertenecientes a  $B$  bases mutuamente no sesgadas en un espacio de Hilbert de dimensión  $D$ . Podemos evaluar explícitamente la suma correspondiente a la tercer definición de 2-diseño ( $k=2$ ), que también aparece en la cota de Welch. En ella obtenemos:

$$\frac{1}{|X|^2} \sum_{\psi, \phi \in X} |\langle \phi | \psi \rangle|^{2k} = \frac{1}{(D \times B)^2} \left( DB \times 1^k + DB \times D(B-1) \times \left(\frac{1}{D}\right)^k \right) \quad (45)$$

Hay  $D \times B$  vectores, cuyo producto interno con si mismos resulta 1. Hay  $(D \times B) \times (D \times (B-1))$  productos internos entre pares de vectores de distintas bases mutuamente no sesgadas, cuyo producto interno tiene norma  $\frac{1}{\sqrt{D}}$ . El resultado de los restante productos internos es 0.

Si tomamos  $k = 2$  y simplificamos la expresión de la derecha obtenemos:  $\frac{D+B-1}{D^2B}$ . Veamos qué podemos deducir a partir de su cota inferior de Welch,  $\frac{2}{D(D+1)}$ .

$$\begin{aligned} \frac{D+B-1}{D^2B} &\geq \frac{2}{D(D+1)} \\ (D+B-1)(D+1) &\geq 2DB \\ D^2 + D + BD + B - D - 1 &\geq 2DB \\ D^2 + B - 1 &\geq DB \\ (D-1)(D+1) &\geq (D-1)B \\ (D+1) &\geq B \end{aligned}$$

Esto significa que el número  $B$  de bases mutuamente no sesgadas esta acotado por  $D + 1$ . También significa que cuando  $B = D + 1$  se satura la cota de Welch, cumpliendose para  $X$  la tercera definición de 2-diseño. **Q.E.D.**

Para el caso en el que  $D$  es una potencia de un número primo, (i.e.  $D = p^N$  con  $p$  primo) se conocen construcciones explícitas que alcanzan la cota máxima de  $D + 1$  bases mutuamente no sesgadas. Esto incluye los espacios de Hilbert correspondientes a sistemas de qubits, donde  $D = 2^N$ . Por otra parte, no hay resultados concluyentes acerca del máximo número de bases mutuamente no sesgadas en una dimensión  $D$  que no sea potencia de primo. No se conoce ninguna construcción de  $D + 1$  bases no sesgadas en estos espacios, ni siquiera para  $D = 6$ . Más aun, búsquedas basadas en minimización numérica parecen indicar la no existencia de tales conjuntos de bases [BH07].

En el caso del espacio de Hilbert de dimensión 2, pueden encontrarse 3 bases mutuamente no sesgadas correspondientes a autovectores de polarizaciones en 3 ejes perpendiculares arbitrarios. Físicamente, este resultado se basa en el hecho de que un espín  $1/2$  totalmente polarizado en un eje, no tiene ninguna polarización en los ejes perpendiculares. Este es el máximo número de bases mutuamente no sesgadas que pueden construirse en esta dimensión. El ejemplo más simple que puede darse de MUBs es pues en dimensión 2, y se trata de las bases compuestas por los autovectores de los operadores de Pauli  $X, Y, Z$ . Estos autovectores pueden expresarse en la base canónica (base de autovectores de  $Z$ ) como:

<i>Operador</i>	$X$	$Y$	$Z$
$Ov = v$	$\frac{ 0\rangle+ 1\rangle}{\sqrt{2}}$	$\frac{ 0\rangle+i 1\rangle}{\sqrt{2}}$	$ 1\rangle$
$Ov = -v$	$\frac{ 0\rangle- 1\rangle}{\sqrt{2}}$	$\frac{ 0\rangle-i 1\rangle}{\sqrt{2}}$	$ 0\rangle$

En esta tabla, ya se ve como los vectores de las distintas bases pueden definirse como autovectores de operadores de Pauli, con autovalores 1 y  $-1$ .

Una de las razones por la cual las bases mutuamente no sesgadas han generado tanto entusiasmo, es por las propiedades que poseen a nivel de información cuántica. Esto puede ilustrarse con dos propiedades que resultan contrapuestas, ya que las MUBs permiten maximizar la información extraída en esquemas de tomografía cuántica y minimizar la pérdida de información en criptografía cuántica.

- **Tomografía:** Ya en 1960 J. Schwinger [J.S60] conocía que se podía reconstruir completamente una matriz densidad  $\rho$  a partir de la medición de los observables  $\sigma_x$ ,  $\sigma_y$  y  $\sigma_z$  y propuso una generalización a dimensiones finitas de conjuntos completos de observables unitarios complementarios. Como los operadores  $X, Y$  y  $Z$  son complementarios dos a dos, la reconstrucción resultante produce una incerteza mínima. En 1981, I. D. Ivanovic [Ivo81] obtuvo un resultado general que será de profunda influencia para el presente trabajo. Consideró el problema de determinar la matriz densidad de un estado desconocido  $\rho$  perteneciente a un espacio de dimensión  $D$  utilizando la menor cantidad de mediciones proyectivas. En su trabajo, estas mediciones corresponden a la diagonalización de observables no degenerados<sup>9</sup> y prueba que es posible hacer tomografía completa de la matriz densidad  $\rho$  a partir de  $D + 1$  observables no degenerados. Esta cantidad es óptima, ya que la descripción de la matriz densidad  $\rho$  requiere  $D^2 - 1$  parámetros independientes, y cada medición completa proporciona  $D - 1$  parámetros independientes. Además, se obtienen los mejores resultados tomográficos cuando no hay duplicación de información, esto es, si las bases correspondientes son mutuamente no sesgadas, (observables complementarios).
- **Criptografía:** El protocolo BB84, busca acordar un código secreto entre dos participantes. El primer participante prepara qubits en autoestados de polarización de  $X$  o  $Y$  y los envía al segundo confiando en que por más que sean interceptados, nadie más sabe en que eje están polarizados, haciendo imposible medirlos sin arriesgar destruir la información que portan. Por otra parte, el receptor puede a posteriori recibir públicamente la base de preparación que debe utilizar para medir. Este debe además, elegir al azar algunos de los qubits y medirlos públicamente para controlar que concuerden con los enviados. Esto le permite asegurarse con alta probabilidad que los qubits no estén siendo medidos por terceros antes de su recepción.

No obstante, en situaciones realistas con un ambiente, los qubits sufren ruido en el canal y los efectos de un observador no deseado pueden quedar camuflados en este ruido. Para un qubit, los observables  $X, Y$  y  $Z$  que diagonalizan a bases mutuamente no sesgadas son también complementarios. Esto permite diseñar un protocolo similar pero con mejor resistencia frente a ruido llamado "protocolo de seis estados". En general, los protocolos de criptografía cuántica permiten optimizar la resistencia frente al ruido y ataques cuando utilizan conjuntos maximales de bases mutuamente no sesgadas.

---

<sup>9</sup>Un observable se dice degenerado si admite ser diagonalizado por distintas bases ortonormales. Entonces, un observable sera no degenerado si y solo si, todos sus autovalores tiene multiplicidad uno.

## 5.4. MUBs y bases maximales de unitarios conmutativos

En esta subsección, mostramos la conexión existente entre las bases mutuamente no sesgadas y conjuntos de bases ortogonales máximamente conmutativas de operadores unitarios. Esta relación, nos permitirá, dar una construcción explícita y eficiente de un conjunto de bases mutuamente no sesgadas (Sec. 6). Los resultados principales de esta subsección fueron presentados por primera vez por Somshubhro Bandyopadhyay et. al. [BBRV02]. Por brevedad, diferimos las demostraciones correspondientes al apéndice B.1 sugiriendo al lector interesado una lectura en paralelo.

**Lemma 5.6.** Existen como máximo  $D$  operadores conmutativos ortogonales no nulos.

**Definición 5.7.** Sea  $\mathcal{M} = \{E_0 = \mathbb{1}, \dots, E_{D^2-1}\}$  un conjunto de  $D^2$  matrices unitarias ortogonales. Diremos que  $\mathcal{M}$  es una base maximal de unitarios conmutativos si puede partitionarse como:

$$\mathcal{M} = \{\mathbb{1}\} \cup \mathcal{S}_0 \cup \dots \cup \mathcal{S}_D$$

Donde los  $\mathcal{S}_i$  son conjuntos disjuntos, cada uno compuesto por de  $D - 1$  matrices que conmutan entre si.

El origen del nombre proviene de que por el lema anterior  $\{\mathbb{1}\} \cup \mathcal{S}_i$  forma un conjunto maximal de  $D$  matrices conmutativas.

**Teorema 5.8.** Si  $\mathcal{M} = \{\mathbb{1}\} \cup \mathcal{S}_0 \cup \dots \cup \mathcal{S}_D$  es un conjunto maximal de unitarios conmutativos ortogonales, entonces las  $D+1$  bases ortogonales  $\mathcal{B}_0, \dots, \mathcal{B}_D$  que diagonalizan respectivamente a los conjuntos de matrices  $\mathcal{S}_0, \dots, \mathcal{S}_D$ , forman un conjunto de  $D + 1$  bases mutuamente no sesgadas.

Por una demostración, referirse al apéndice B.1, donde se adapta la demostración original del artículo de Bandyopadhyay et. al.[BBRV02]. En dicho artículo, también se prueba la condición reciproca que se enuncia en el siguiente teorema.

**Teorema 5.9.** Sean  $\mathcal{B}_1, \dots, \mathcal{B}_m$  un conjunto de  $m$  bases mutuamente no sesgadas del espacio de Hilbert de dimensión  $D$ . Entonces existen  $m$  conjuntos disjuntos de matrices unitarias  $\mathcal{S}_1, \dots, \mathcal{S}_m$ , tales que todas las matrices en  $\{I\} \cup \mathcal{S}_1 \cup \dots \cup \mathcal{S}_m$  son ortogonales de a pares. Y para cada  $j$ , las  $D$  matrices en  $\{I\} \cup \mathcal{S}_j$  conmutan.

Notar que de aquí tambien se puede obtener como corolario que existen a lo sumo  $D + 1$  bases mutuamente no sesgadas en dimensión  $D$ . Estos teoremas constituyen un resultado importante, pues reducen la busqueda de bases mutuamente no sesgadas a la busqueda de conjuntos maximales de unitarios conmutativos ortogonales. En particular, en la siguiente sección, combinaremos este resultado con el formalismo de estabilizadores para lograr una novedosa construcción eficiente de bases mutuamente no sesgadas.

## 6. Bases mutuamente no sesgadas eficientes

Si llamamos  $|\psi_{J,k}\rangle$  al  $k$ -ésimo elemento de la  $J$ -ésima base de un conjunto de bases mutuamente no sesgadas, tenemos que, por la misma definición de MUBs 5.4 pueden relacionarse por:

$$|\psi_{J,k}\rangle = \frac{1}{\sqrt{D}} \sum_{k'=1}^{k'} \exp(i\theta_{J,J',k,k'}) |\psi_{J',k'}\rangle \quad (46)$$

Las fases  $\theta$  proveen una manera frontal de describir las bases mutuamente no sesgadas. El problema surge del enorme número de parámetros necesario para describir un conjunto maximal de MUBs. Hay  $D + 1$  bases mutuamente no sesgadas, cada una definida por  $D$  vectores que a la vez requieren de  $D$  coordenadas para ubicarlos en el espacio de Hilbert. Si tomamos la primer base como la base canónica, todavía precisamos  $D^3$  parámetros reales para la descripción de un conjunto maximal de MUBs. Si  $D = p^N$ , el numero de parametros resulta exponencial en  $N$ . El panorama no muestra mucha esperanza para la existencia de una descripción eficiente de algún conjunto maximal de MUBs. Dedicaremos este capítulo a eliminar estas tres exponencialidades y mostrar que existe una descripción eficiente para conjuntos maximales de bases mutuamente no sesgadas.

### 6.1. Operadores de Heisenberg-Weyl generalizados

Los operadores de Heisenberg-Weyl son una de las posible extensiones de los operadores de Pauli, a dimensiones  $D \neq 2$ . Es decir que los operadores actuan sobre un espacio de Hilbert de dimensión  $D$ . Se trata del grupo de operadores generado por:

$$X : |j\rangle \rightarrow |j + 1 \pmod{D}\rangle \quad Z : |j\rangle \rightarrow \omega^j |j\rangle$$

Donde  $\omega = e^{2\pi i/D}$ . Es decir que el grupo de Heisenberg-Weyl se refiere al conjunto de operadores que puede obtenerse mediante multiplicacion sucesiva de generadores. Consideraremos equivalentes operadores que sean iguales a menos de una fase global, ya que tendran la misma acción por conjugación. Los operadores resultantes son unitarios y ortogonales pero no hermíticos (solo en el caso  $D = 2$  se recuperan los operadores hermíticos de Pauli).

Un caso particularmente interesante, es cuando  $D = p$  es un número primo. En tal caso, todos los operadores  $O$  del grupo exepctuando la identidad tienen orden  $p^{10}$ .

En este trabajo, utilizamos el nombre “Grupo de Heisenberg-Weyl Generalizado” para referirnos al grupo compuesto de productos tensoriales de  $N$  operadores del grupo de Heisenberg-Weyl de tamaño  $p$  (con  $p$  primo). Así, estos operadores pueden identificarse como actuando sobre  $N$  subsistemas, cada uno con un espacio de Hilbert de dimensión  $p$ . Se construye así un conjunto de  $p^{2N}$  operadores ortogonales y unitarios, los cuales son todos de orden  $p$  exceptuando la identidad. Estos operadores forman un conjunto maximamente conmutativo de unitarios ortogonales.

<sup>10</sup>Un operador  $O$  tiene orden  $p \in \mathbb{N}$  si  $p$  es el menor natural tal que  $O^p = \mathbb{1}$ .

## 6.2. Formalismo de estabilizadores

El primer paso consiste en describir a los estados  $|\psi_{J,\mathbf{k}}\rangle$  de las MUBs mediante el formalismo de estabilizadores. La teoría de estabilizadores fue diseñada por Daniel Gottesman durante su tesis doctoral en 1997 [Got97] como herramienta para describir códigos correctores de errores y computación cuántica resistente a fallas. Desde entonces, se ha convertido en una herramienta casi omnipresente en el campo de información cuántica. Se utilizará en lo que sigue para la descripción de bases mutuamente no sesgadas.

Al trabajar con el formalismo de estabilizadores, se deja de describir al estado mediante un vector en el espacio de Hilbert. En su lugar, se enumeran los operadores que lo tienen como autovector y los autovalores correspondientes. Motivados por el teorema 5.8, consideraremos solo los  $D^2$  operadores del grupo de Heisenberg-Weyl generalizado. Eligiendo las fases globales apropiadamente, los autovalores correspondientes solo pueden tomar los valores  $\omega^m$  donde  $\omega = e^{\frac{2\pi i}{p}}$  y  $m \in \{0, \dots, p-1\}$ . En particular, solo consideraremos vectores que sean autoestados para subconjuntos maximales de  $D$  operadores conmutativos. Estos conjuntos de  $D$  operadores conmutativos pueden diagonalizarse simultáneamente definiendo así bases ortonormales de  $D$  estados. Cada subconjunto de  $D$  operadores conmutativos forma un subgrupo a menos de fases y cada subgrupo posee  $N$  generadores  $\{J_0, \dots, J_{N-1}\}$  de orden  $p$ . Cualquier elemento del grupo estabilizador puede ser escrito, a menos de una fase como un producto de potencias de estos generadores:

$$E_{J,\mathbf{q}} = J_0^{q_0} \times J_1^{q_1} \dots \times J_{N-1}^{q_{N-1}} \quad (47)$$

Donde  $\mathbf{q} = (q_0, q_1, \dots, q_{N-1})$  es un vector compuesto de  $N$  componentes pertenecientes a  $\mathbb{Z}_p$ . También se pueden enumerar los vectores que diagonalizan de modo que  $J_m |\psi_{J,\mathbf{k}}\rangle = \omega^{k_i} |\psi_{J,\mathbf{k}}\rangle$ . Con esta definición, podemos describir la aplicación de un operador  $E_{J,\mathbf{q}}$  del subgrupo  $J$  sobre el vector  $|\psi_{J,\mathbf{k}}\rangle$  de la base estabilizada  $\mathcal{B}_J$  como:

$$E_{J,\mathbf{q}} |\psi_{J,\mathbf{k}}\rangle = \omega^{\mathbf{q}\cdot\mathbf{k}} |\psi_{J,\mathbf{k}}\rangle \quad (48)$$

Donde en el producto interno  $(\cdot)$  se toman todas las operaciones en el cuerpo  $\mathbb{Z}_p$ . Usando esta notación, la descripción de una base ortonormal  $\mathcal{B}_J$  requiere enumerar  $N$  generadores de un subgrupo de Heisenberg-Weyl generalizado en lugar de describir  $D$  vectores en un espacio de Hilbert de dimensión  $D$ .

Cada operador de Heisenberg-Weyl generalizado puede recibir una representación compacta mediante dos vectores, cada uno con  $N$  componentes en  $\mathbb{Z}_p$ .

$$T(\mathbf{p}, \mathbf{q}) \equiv X^{\mathbf{p}} Z^{\mathbf{q}} e^{\frac{i\pi \mathbf{p}\cdot\mathbf{q}}{p}} = \otimes_{m=0}^{N-1} X_m^{p_m} Z_m^{q_m} e^{\frac{i\pi p_m q_m}{p}} \quad (49)$$

Donde  $\mathbf{p}$  y  $\mathbf{q}$  son vectores en  $\mathbb{Z}_p^N$ . Se denomina a esta descripción de los operadores del grupo como forma canónica de un operador. Cada vez que consideramos un operador  $E_m$  del grupo, podemos pensar que el índice  $m$  se descompone en dos vectores, cada uno de  $N$  componentes en  $\mathbb{Z}_p$ .

Con esta notación, la descripción de una base ortonormal estabilizada requiere de  $2N \times N$  números en  $Z_p$ .

**Ejemplo 6.1.** Si estamos considerando un sistema de 8 qubits, estos son algunos operadores representados por la notación  $T(\cdot, \cdot)$ :

$$\begin{aligned} I \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I &= T(00000000, 00000000) \\ X \otimes X \otimes I \otimes I \otimes I \otimes I \otimes Z \otimes I &= T(11000000, 00000010) \\ I \otimes X \otimes Y \otimes Z \otimes X \otimes X \otimes X \otimes Y &= T(01101111, 00110001) \end{aligned}$$

Las propiedades de conmutación de los operadores del grupo generalizado de Heisenberg-Weyl están dadas por:

$$T(\mathbf{p}_1, \mathbf{q}_1)T(\mathbf{p}_2, \mathbf{q}_2) = e^{\frac{2\pi i}{p}(\mathbf{p}_2 \cdot \mathbf{q}_1 - \mathbf{p}_1 \cdot \mathbf{q}_2)}T(\mathbf{p}_2, \mathbf{q}_2)T(\mathbf{p}_1, \mathbf{q}_1) \quad (50)$$

**Lemma 6.2.** En particular, la condición de conmutación entre dos operadores  $T(\mathbf{p}_1, \mathbf{q}_1)$  y  $T(\mathbf{p}_2, \mathbf{q}_2)$  esta dada por:

$$\mathbf{p}_2 \cdot \mathbf{q}_1 = \mathbf{p}_1 \cdot \mathbf{q}_2$$

Vemos que en términos de las representaciones canónicas de los operadores  $T(\mathbf{p}_1, \mathbf{q}_1)$  y  $T(\mathbf{p}_2, \mathbf{q}_2)$ , el coeficiente de conmutación solo depende del producto simpléctico  $\mathbf{p}_2 \cdot \mathbf{q}_1 - \mathbf{p}_1 \cdot \mathbf{q}_2$ .

**Ejemplo 6.3.** La base de Bell (presentada en la sección 3.4.1) es un ejemplo de base estabilizada por operadores de Pauli generalizados. Los operadores de Pauli generalizados  $XX$  y  $ZZ$  conmutan. En efecto, el primero puede ser escrito como  $T(11, 00)$  y el segundo como  $T(00, 11)$ . Como son independientes, son los generadores de un subgrupo conmutativo de cuatro elementos.

$$\{E_{\text{Bell},00} = II, E_{\text{Bell},10} = XX, E_{\text{Bell},01} = ZZ, E_{\text{Bell},11} = -YY\}$$

Notemos que el operador  $E_{\text{Bell},11}$  muestra una diferencia de signo con respecto a  $T(11, 11) = YY$ . Es decir que por más que los operadores  $T(11, 00)$  y  $T(00, 11)$  conmuten, esto no significa que su producto sea  $T(11, 11)$  ya que puede surgir una diferencia de una fase. La base de estados  $|\psi\rangle$  estabilizados por estos operadores es precisamente la base de Bell, y puede enumerarse según sus autovalores respecto a  $XX$  y a  $ZZ$  como:

	$XX  \psi\rangle =  \psi\rangle$	$XX  \psi\rangle = - \psi\rangle$	
$ZZ  \psi\rangle =  \psi\rangle$	$ \psi_{\text{Bell},00}\rangle = \frac{1}{\sqrt{2}}( 00\rangle +  11\rangle)$	$ \psi_{\text{Bell},01}\rangle = \frac{1}{\sqrt{2}}( 00\rangle -  11\rangle)$	(51)
$ZZ  \psi\rangle = - \psi\rangle$	$ \psi_{\text{Bell},10}\rangle = \frac{1}{\sqrt{2}}( 01\rangle +  10\rangle)$	$ \psi_{\text{Bell},11}\rangle = \frac{1}{\sqrt{2}}( 01\rangle -  10\rangle)$	

Podemos comprobar como una vez que se enumeran los operadores del estabilizador y vectores de la base estabilizada de esta manera vale la ecuación (48) que describe los autovalores correspondientes.

$$-YY \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = E_{\text{Bell},11} |\psi_{\text{Bell},11}\rangle = (-1)^{11 \cdot 11} \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

La ecuación (Ec. 48), describe como actúa un operador del conjunto estabilizador sobre un vector de la base. El siguiente lema, nos permitirá estudiar el efecto de un operador de Heisenberg-Weyl arbitrario sobre un vector definido a partir del formalismo de estabilizadores.

**Lemma 6.4.** Si los operadores  $E_1$  y  $E_2$  tienen una relación de conmutación/anticommutación definida  $E_1 E_2 = c E_2 E_1$  y  $|\psi\rangle$  es un autovector del operador  $E_1$  con autovalor  $\lambda$  (i.e.  $E_1 |\psi\rangle = \lambda |\psi\rangle$ ), entonces  $E_2 |\psi\rangle$  también es autovector de  $E_1$ , con autovalor  $c\lambda$ .

**Demostración:** Aplicando la condición de conmutación sobre el vector  $|\psi\rangle$  obtenemos:

$$E_1 E_2 |\psi\rangle = c E_2 E_1 |\psi\rangle = c E_2 \lambda |\psi\rangle = c \lambda (E_2 |\psi\rangle)$$

**Q.E.D.**

Esto significa que un operadores con relaciones de anticonmutación bien definidas, respecto de todos los operadores de un estabilizador envía vectores de la base estabilizada a vectores de la base estabilizada. En el caso de un operador  $E_m$  en el grupo de Heisenberg-Weyl y una base arbitraria estabilizada por  $D$  operadores del grupo, tenemos.

$$E_m |\psi_{J,\mathbf{k}}\rangle \in \mathcal{B}_J \quad (52)$$

**Definición 6.5.** Definimos el vector de conmutación  $\mathbf{c}$  de un operador de Heisenberg-Weyl  $E$  con respecto a una base estabilizada  $\mathcal{B}_J$ , como un vector  $\mathbf{c} = (c_0, \dots, c_{N-1})$  de  $N$  componentes en  $\mathbb{Z}_p$  donde cada  $c_m$  esta definido tal que:

$$J_m E = e^{\frac{2\pi i c_m}{p}} E J_m$$

Notar que este vector no depende de las fases con la que se defina  $E$  y los generadores del grupo estabilizador de  $\mathcal{B}_J$ .

Utilizando la definición de los estados  $|\psi_{J,\mathbf{k}}\rangle$  (Ec. 48) y el lema 6.4, podemos describir la acción sobre los vectores  $|\psi_{J,\mathbf{k}}\rangle \in \mathcal{B}_J$  de un unitario  $E$ . Si  $\mathbf{c}$  es el vector de conmutación de  $E$  respecto a la base  $\mathcal{B}_J$  la acción puede describirse por:

$$E |\psi_{J,\mathbf{k}}\rangle \cong |\psi_{J,\mathbf{k}+\mathbf{c}}\rangle \quad (53)$$

Donde  $\cong$  indica igualdad módulo una fase.

### 6.3. Cuerpos finitos y polinomio primitivo

La teoría de Galois indica que existe un cuerpo finito con exactamente  $D$  elementos si y solo si  $D$  es una potencia de un número primo  $p$ . Esto nos provee de una de las construcciones posibles para los estabilizadores de las bases mutuamente no sesgadas. Existe un único cuerpo finito con  $D = p^N$  elementos a menos de isomorfismos y se lo denomina  $\mathbb{F}_{p^N}$ . Cuando  $D = p$  es un número primo, las operaciones de suma y producto del cuerpo son las operaciones usuales de la aritmética modulo  $p$  con lo cual  $\mathbb{Z}_p \equiv \mathbb{F}_p$ .

Para dar una definición explícita del cuerpo  $\mathbb{F}_D$ , primero debemos encontrar un polinomio mónico e irreducible<sup>11</sup>  $P(x)$  de grado  $N$ , con coeficientes en  $\mathbb{Z}_p$  y que no divida a ningún polinomio de la forma  $1 + x^m$  con  $0 < m < D - 1$ . El polinomio  $P(x)$  toma el nombre de polinomio primitivo de  $\mathbb{F}_D$ . Para muchos casos, estos polinomios pueden encontrarse tabulados, pero también existen algoritmos eficientes  $O(N^2)$  para encontrarlos [DPGM92]. Luego, se considera una raíz  $\omega$  de  $P(x)$  en  $\mathbb{F}_D$  a la que llamaremos elemento generador. No se precisa encontrar explícitamente esta raíz, pero en términos de ella, los elementos de  $\mathbb{F}_D$  son precisamente el 0 y todas las potencias de  $\omega$  (i.e.  $\{0, 1, \omega, \omega^2, \dots, \omega^{D-2}\}$ ). Esto se debe a que  $\omega^{D-1} = 1$  y que  $\omega^{m_1} \neq \omega^{m_2}$  para  $0 < m_1 < m_2 < D$ . Otra alternativa para escribir a los elementos de  $\mathbb{F}_D$  es en un espacio vectorial de  $N$  componentes sobre  $\mathbb{Z}_p$ . Esto corresponde a describir a cada elemento  $\mathbf{x}$  del grupo en una base canónica.

$$\mathbf{x} = \sum_{j=0}^{N-1} x_j \omega^j \quad (54)$$

En esta representación, identificamos los vectores canónicos.

$$\epsilon_0 = 1 = \omega^0 \quad , \quad \dots \quad , \quad \epsilon_{N-1} = \omega^{N-1} \quad (55)$$

De aquí, obtenemos que la operación de suma de los elementos del cuerpo  $\mathbb{F}_D$  está dada por la suma de los vectores  $\mathbf{x}$  componente a componente en  $\mathbb{Z}_p$ . Para la operación de producto, se toman las componentes de  $\mathbf{x}$  como coeficientes de un polinomio y se utiliza el producto usual de polinomios en  $\omega$  con coeficientes en  $\mathbb{Z}_p$ . Como resultado de tomar productos, pueden surgir polinomios con potencias de  $\omega$  con grado mayor o igual que  $N$ . Estos deben reducirse a polinomios de grado menor que  $N$  restando un múltiplo conveniente de  $P(\omega)$  (que se anula por definición). Así como el cuerpo  $\mathbb{Z}_p$  es el cuerpo finito que toma las operaciones de  $\mathbb{Z}$  módulo  $p$ , el cuerpo finito  $\mathbb{F}_{p^N}$ , puede definirse tomando la suma y multiplicación de polinomios con coeficientes en  $\mathbb{Z}_p$  y tomando los resultados módulo  $P(x)$ .

**Ejemplo 6.6.** El primer paso para construir el cuerpo finito  $\mathbb{F}_4 = \mathbb{F}_{2^2}$ , consiste en encontrar un polinomio mónico irreducible de grado 2 con coeficientes en  $\mathbb{Z}_2$ . En este caso, el único

---

<sup>11</sup>Se dice que un polinomio  $P(x)$  es irreducible si no admite ninguna factorización no trivial en polinomios con coeficientes en  $\mathbb{Z}_p$ . Es decir que 1 y  $P(x)$  son sus únicos divisores a menos de una constante multiplicativa en  $\mathbb{Z}_p$ .

polinomio posible es:  $P(x) = 1 + x + x^2$ . Utilizando este polinomio, los elementos del cuerpo pueden enumerarse como:

- $0$
- $\omega^0 = 1$
- $\omega^1 = \omega$
- $\omega^2 = 1 + \omega$
- $\omega^{3+r} = \omega^r$

La tabla de adición de las potencias de  $\omega$  puede darse como:

$+$	$0$	$\omega^0$	$\omega^1$	$\omega^2$
$0$	$0$	$\omega^0$	$\omega^1$	$\omega^2$
$\omega^0$	$\omega^0$	$0$	$\omega^2$	$\omega^1$
$\omega^1$	$\omega^1$	$\omega^2$	$0$	$\omega^0$
$\omega^2$	$\omega^2$	$\omega^1$	$\omega^0$	$0$

**Ejemplo 6.7.** Para construir el cuerpo finito  $\mathbb{F}_8$ , un polinomio primitivo posible es:  $P(x) = 1 + x^2 + x^3$ . Las potencias de  $\omega$ , pueden entonces reducirse como:

- $0 = 0$
- $\omega^0 = 1$
- $\omega^1 = \omega$
- $\omega^2 = \omega^2$
- $\omega^3 = 1 + \omega$
- $\omega^4 = \omega + \omega^2$
- $\omega^5 = \omega^2 + \omega + 1$
- $\omega^6 = \omega^2 + 1$
- $\omega^{7+r} = \omega^r$

## 6.4. Matriz compañera

Si escribimos a los elementos de  $\mathbb{F}_D$  como vectores columna de  $N$  componentes en  $\mathbb{Z}_p$ , existe una matriz  $M$  de  $N \times N$ , con elementos en  $\mathbb{Z}_p$  cuya acción sobre los vectores corresponde a la multiplicación por  $\omega$  en  $\mathbb{F}_D$ . En efecto, esta matriz se denomina matriz compañera del polinomio primitivo. Esta matriz, junto con la suma y multiplicación de matrices de  $N \times N$  con coeficientes en  $\mathbb{Z}_p$  genera el cuerpo finito  $\mathbb{F}_{p^N}$  como subconjuntos de las mismas. Veamos que su acción sobre vectores determina unívocamente la forma que  $M$  debe tener. Para  $0 \leq j < N - 1$ , tenemos que  $M\epsilon_j = \epsilon_{j+1}$  puesto que  $\omega\omega^j = \omega^{j+1}$  puede expresarse como versor directamente. Esto corresponde a una diagonal de unos justo abajo de la diagonal principal y ceros en las demás posiciones de las primeras  $N - 1$  columnas. En el caso de  $M\epsilon_{N-1}$ , tenemos que el vector resultante debe representar a  $\omega^N$ , que no tiene un versor correspondiente. Tomamos pues el resto de  $x^N$  en la división por  $P(x)$  para obtener la representación correspondiente a  $\omega^N$ . Sin pérdida de generalidad, podemos asumir que el polinomio primitivo puede expresarse como  $P(x) = a_0 + a_1x + a_2x^2 + \dots + a_{N-1}x^{N-1} + x^N$ . Donde los coeficientes  $a_0, \dots, a_{N-1}$  pertenecen a  $\mathbb{Z}_p$ . Por definición de  $\omega$  como raíz de  $P(x)$ ,

tenemos que  $P(\omega) = 0$ . Por lo tanto, podemos reducir  $\omega^N = \omega^N - P(\omega)$  que puede darse explícitamente  $-a_0 - a_1\omega - a_2\omega^2 - \dots - a_{N-1}\omega^{N-1}$ . Entonces la  $m$ -ésima componente de la última columna contiene el coeficiente  $-a_m$ . En particular, el polinomio característico de la matriz  $M$ , es precisamente  $\det(xI - M) = P(x)$ . Por el teorema de Hamilton-Cayley, esto significa que  $P(M) = 0$ , por lo que  $M$  es un generador del cuerpo finito en representación matricial. Es decir, que  $M$  tiene todas las propiedades antes atribuidas a  $\omega$ . En particular, tenemos que las potencias de  $M$  no se repiten hasta  $M^{D-1} = I$ .

**Ejemplo 6.8.** La matriz compañera para el polinomio primitivo  $P(x) = 1 + x + x^2$  del cuerpo  $\mathbb{F}_4$  es:

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

**Ejemplo 6.9.** La matriz compañera del polinomio primitivo  $P(x) = 1 + x + x^3$  del cuerpo finito  $\mathbb{F}_8$  esta dada por:

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

## 6.5. Aplicación a MUBs estabilizadas

El resultado principal de esta subsección es una manera de separar a todos los operadores de Heisenberg-Weyl en  $D + 1$  subgrupos conmutativos cuyo único elemento compartido es la identidad. En particular, no sera necesario contar con una definición especial para cada uno de los grupos estabilizadores permitiendo una definición polinomial de los mismos.

Como  $M^k \epsilon_0$  es el representante de  $\omega^k$  como vector, tenemos que si  $\mathbf{x}$  no es el vector nulo,  $\{M^k \mathbf{x} : 0 < k < D\}$  es el conjunto de todos los vectores no nulos en  $\mathbb{Z}_p^N$ . Por simetría, la matriz transpuesta  $M^T$  tiene la misma propiedad con la aplicación a derecha.

**Teorema 6.10.** Sean  $G_Z$  y  $G_{\mathbf{J}}$  con  $\mathbf{J} \in \mathbb{Z}_p^N$  dados por:

$$G_Z = \{T(\mathbf{0}, M^q \mathbf{1}) : 0 < q < D\} \quad (56)$$

$$G_{\mathbf{J}} = \{T(M^q \mathbf{1}, (M^T)^q \mathbf{J}) : 0 < q < D\} \quad (57)$$

Los subconjuntos de operadores  $G_Z$  y  $G_{\mathbf{J}}$  particionan a los operadores de Heisenberg-Weyl distintos de la identidad en  $D + 1$  conjuntos de  $D - 1$  operadores conmutativos.

**Demostración:** Trivialmente los operadores de  $G_Z$  son todos distintos y conmutan entre sí. Para ver que los operadores de  $G_{\mathbf{J}}$  también conmutan, utilizamos la condición de conmutación (Lema 6.2). Vemos que la condición necesaria y suficiente para la conmutación de  $T(M^q \mathbf{1}, (M^T)^q \mathbf{J})$  y  $T(M^k \mathbf{1}, (M^T)^k \mathbf{J})$  se satisface trivialmente:

$$\mathbf{J}^T M^k M^q \mathbf{1} = \mathbf{J}^T M^q M^k \mathbf{1}$$

Además, como  $M^q \mathbf{1}$  recorre todos los vectores no nulos, los elementos de  $G_{\mathbf{J}}$  son distintos. Trivialmente,  $G_Z$  es disjunto con los demás  $G_{\mathbf{J}}$ . Supongamos que  $G_{\mathbf{J}}$  y  $G_{\mathbf{K}}$  comparten un elemento. En efecto, para que compartan un elemento, precisamos que los dos argumentos de  $T(\cdot)$  coincidan. Para que coincida la primer componente necesitamos que los elementos sean descriptos por el mismo  $q$ . Esto nos lleva a que la única posibilidad de solapamiento es:

$$(M^T)^q \mathbf{J} = (M^T)^q \mathbf{K}$$

Pero como la matriz  $M$  y por lo tanto  $M^T$  es no singular, podemos multiplicar a izquierda por la inversa obteniendo  $\mathbf{J} = \mathbf{K}$ . **Q.E.D.**

A partir de este momento, los índices de base serán o bien un vector  $\mathbf{J} \in \mathbb{Z}_p^N$  o bien la letra  $Z$ .

**Corolario 6.11.** Las bases estabilizadas por los grupos estabilizadores  $G_Z$  y  $G_{\mathbf{J}}$  con  $\mathbf{J} \in \mathbb{Z}_p^N$  forman un conjunto maximal de  $D + 1$  bases mutuamente no sesgadas.

Podemos elegir los generadores de los  $D + 1$  estabilizadores como:

$$Z_m = T(\mathbf{0}, M^m \mathbf{1}) : 0 \leq m < N \quad (58)$$

$$\mathbf{J}_m = T(M^m \mathbf{1}, (M^T)^m \mathbf{J}) : 0 \leq m < N \quad (59)$$

Con esta definición,  $E_{Z,\mathbf{q}} = T(\mathbf{0}, \mathbf{q})$  y  $E_{\mathbf{J},\mathbf{q}} = T(\mathbf{q}, \sum_{m=0}^{N-1} q_m (M^T)^m \mathbf{J})$  donde  $q_m$  es la  $m$ -ésima componente de  $\mathbf{q}$  y la suma y producto de vectores se realiza en  $\mathbb{Z}_p$ . El operador  $\mathbb{1}$  podrá representarse como  $E_{Z,\mathbf{0}}$  y tendrá otras  $D$  representaciones como  $E_{\mathbf{J},\mathbf{0}}$ . Es interesante observar, que la relación de conmutación con la base canónica es ahora muy simple.

$$E_{Z,\mathbf{p}} E_{\mathbf{J},\mathbf{q}} = e^{\frac{2\pi i \mathbf{p} \cdot \mathbf{q}}{p}} E_{\mathbf{J},\mathbf{q}} E_{Z,\mathbf{p}} \quad (60)$$

Esto significa que el vector de conmutación del operador  $E_{\mathbf{J},\mathbf{q}}$  con respecto a la base computacional  $\mathcal{B}_Z$  es precisamente  $\mathbf{q}$ .

**Ejemplo 6.12.** En el caso de dos qubit tenemos dos generadores por base que definen completamente el subgrupo estabilizador. Usaremos la matriz  $M$  del ejemplo 6.8 para encontrar los generadores de las 5 bases mutuamente no sesgadas. La base  $X$  siempre estará entre las bases estabilizadas correspondiendo esta a  $\mathbf{J} = \mathbf{0}$ . En este caso, tenemos que  $M = M^T$ , condición necesaria y suficiente para que la base  $Y$  esté entre las estabilizadas, correspondiendo esta siempre al vector  $\mathbf{1}$ . Para la base correspondiente a  $\mathbf{J} = 10$  tenemos que los estabilizadores serán:

$$T(10, (M^T)^0 01) = X \otimes Z \text{ y } T(01, (M^T)^1 01) = Z \otimes Y$$

La base estabilizada por estos operadores toma el nombre de base de Belle.

Nombre	$\mathbf{J}$	$E_{\mathbf{J},10}$	$E_{\mathbf{J},01}$
Base $Z$		$Z \otimes I$	$I \otimes Z$
Base $X$	00	$X \otimes I$	$I \otimes X$
Base $Y$	10	$Y \otimes I$	$I \otimes Y$
Belle	01	$X \otimes Z$	$Z \otimes Y$
Beau	11	$Y \otimes Z$	$Z \otimes X$

También se muestra gráficamente, como los subgrupos generados forman una partición de los operadores de Pauli de 2 qubits en la figura 2.

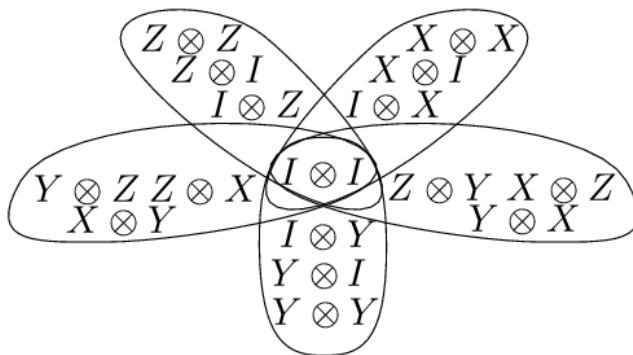


Figura 2: Grupos estabilizadores para 5 bases de 2 qubits.

## 6.6. Construcción del estado $|\psi_{\mathbf{J},\mathbf{k}}\rangle$

En esta subsección presentaremos la secuencia de pasos necesaria para construir un estado arbitrario  $|\psi_{\mathbf{J},\mathbf{k}}\rangle$  del conjunto de bases mutuamente no sesgadas propuesto y analizamos la complejidad algorítmica de cada paso. Supondremos que estamos trabajando con  $N$  subsistemas y que ya disponemos del polinomio primitivo  $P(x)$ . Este polinomio solo precisa calcularse una vez, en el momento que se decide trabajar con sistemas de dimensión  $p^N$ . El primer paso es preparar el estado  $|\psi_{\mathbf{Z},\mathbf{0}}\rangle$  o un estado arbitrario pero conocido de la base computacional. Luego se construye el estado  $|\psi_{\mathbf{Z},\mathbf{k}}\rangle$  aplicando  $X^{\mathbf{k}}$ . Finalmente, es necesario aplicar un cambio de base de la base  $Z$  o computacional a la base  $\mathbf{J}$ .

Será necesario, para poder obtener un circuito de cambio de base, conocer los generadores del estabilizador que definen la base  $\mathbf{J}$ . Es decir, es necesario calcular los siguientes  $N$  operadores.

$$\mathbf{J}_m = T(M^m \mathbf{1}, (M^T)^m \mathbf{J}) : 0 \leq m < N$$

La multiplicación de  $M$  o  $M^T$  por un vector, puede lograrse en  $O(N)$  operaciones. A partir de esto, los estabilizadores pueden calcularse sucesivamente requiriendo un total de  $O(N^2)$  operaciones elementales para calcularlos a todos.

En su tesis de licenciatura, Ariel Bendersky [Ben06] muestra como es posible construir circuitos de cambio de base estabilizadas de  $N$  qubits. Dados los  $N$  generadores de los respectivos subgrupo estabilizadores, presenta un algoritmo clásico de complejidad  $O(N^3)$  que permite construir un circuito cuántico de cambio de base. El circuito cuántico así obtenido está compuesto de  $O(N^2)$  rotaciones de un qubit y compuertas C-Not. Este es el circuito que debe ser aplicado sobre el estado  $|\psi_{Z,\mathbf{k}}\rangle$  para obtener el estado  $|\psi_{J,\mathbf{k}}\rangle$ .

## 7. Tomografía diagonal de procesos cuánticos

Hasta ahora, el esquema tomográfico que hemos presentado, consiste en medir supervivencia de un estado para poder realizar la caracterización de los elementos de matriz de  $\chi$ . Sin embargo, cada vez que preparamos un estado  $|\psi\rangle$  y medimos su probabilidad de supervivencia desperdiciamos toda la información que permanece en el subespacio correspondiente a  $|\psi\rangle^\perp$  cuando la medición de supervivencia resulta negativa. En principio, es posible distinguir entre  $p^N$  resultados finales mediante el uso de  $N$  mediciones  $p$ -arias. En el caso de qubits,  $2^N$  resultados a partir de  $N$  mediciones binarias. Hasta el momento, solo estamos extrayendo información de uno de estos  $2^N$  resultados finales, y desperdiciando la información extraíble de distinguir entre los  $2^N - 1$  resultados restantes.

En esta sección, presentaremos un método que permite aprovechar de manera óptima toda la información contenida en los estados finales en el caso que se utilicen para la tomografía las bases no sesgadas estabilizadas por la base de operadores de la representación  $\chi$ . Como primer paso, estudiaremos que operadores  $E_m$  aportan a la probabilidad de cada uno de los estados finales. A partir del resultado obtenido, mostraremos como se puede estimar uno o todos los coeficientes diagonales de  $\chi$  a partir de preparación y medición de estados de las MUBs asociadas. Por último, mostraremos como una buena representación de los datos experimentales puede responder de manera eficiente preguntas interesantes sobre los coeficientes diagonales  $\chi_{mm}$ .

### 7.1. Dando significado a otros estados finales

Se puede estimar el coeficiente  $\chi_{mm}$  de  $\mathcal{E}$  a partir de la fidelidad del siguiente circuito.

$$|\psi\rangle \quad \text{---} \boxed{\mathcal{E}} \text{---} \boxed{E_m^\dagger} \text{---} \boxed{\text{---}} \quad P_\psi$$

Donde  $|\psi\rangle$  se toma aleatoriamente de un 2-diseño  $X$ .

Si bien se ha permutado la aplicación de  $\mathcal{E}$  y la de  $E_m^\dagger(\cdot)E_m$ , con respecto a los circuitos propuestos en la sección 4, este reordenamiento resulta equivalente en lo que respecta a mediciones de fidelidad media. Es posible asimilar el unitario  $E_m^\dagger$  a la medición y eliminarlo del bloque central del circuito.

$$|\psi\rangle \quad \text{---} \boxed{\mathcal{E}} \text{---} \boxed{\text{---}} \quad E_m P_\psi E_m^\dagger$$

Esta nueva representación permite cambiar levemente levemente nuestra visión acerca del circuito. Este circuito mide pues que tan “parecidos” son los resultados de aplicar  $\mathcal{E}$  a  $P_\psi$  con respecto a aplicar  $E_m$  por conjugación a  $P_\psi$ . Si se promedia sobre  $P_\psi$ , esto es precisamente la fidelidad de compuerta  $\overline{F}(\mathcal{E}, E_m)$ ,<sup>12</sup> más conocida como *gate fidelity*.

<sup>12</sup>Referirse al glosario por una definición de fidelidad de compuerta.

Ahora bien, si tomamos como base de operadores  $\{E_n\}$  para la representación  $\chi$  al grupo de Heisenberg-Weyl, y tomamos el conjunto de bases mutuamente no sesgadas asociado, es posible obtener ciertas equivalencias. Recordando de la ecuación 52, tenemos que los operadores de Heisenberg-Weyl preservan bases.

$$\forall m E_m |\psi_{J,\mathbf{k}}\rangle \in \mathcal{B}_J$$

Luego, sin importar cual de las fidelidades de compuerta  $\overline{F}(\mathcal{E}, E_m) = \overline{F}(\mathcal{E}_m)$  se desea medir, ni con que estado  $|\psi_{J,\mathbf{k}}\rangle$  se empezó, hay un estado  $|\psi_{J,\mathbf{k}'}\rangle$  de la base  $\mathcal{B}_J$  tal que su medición a la salida es equivalente a medir  $|\psi_{J,\mathbf{k}}\rangle$  en el circuito  $\mathcal{E}_m$ .

$$|\psi_{J,\mathbf{k}}\rangle \langle\psi_{J,\mathbf{k}}| \text{ --- } \boxed{\mathcal{E}} \text{ --- } \boxed{\text{A}} \quad \mathcal{B}_J$$

El índice  $\mathbf{k}'$  que debemos considerar, dependerá tanto de  $\mathbf{k}$ , de  $J$  como de  $E_m$ . Si  $\mathbf{c}$  es el vector de conmutación (Definición 6.5) de  $E_m$  respecto a la base  $J$ , tendremos que  $\mathbf{k}' = \mathbf{k} + \mathbf{c}$ .

**Ejemplo 7.1.** Consideremos un sistema de un qubit y estudiemos la acción de  $X$  sobre los elementos de las distintas bases. En la base computacional, tenemos:

$$X |0\rangle \langle 0| X = |1\rangle \langle 1| \quad X |1\rangle \langle 1| X = |0\rangle \langle 0|$$

Es decir que  $X$  intercambia los autoestados del operador  $Z$ . Análogamente,  $X$  intercambia los autoestados del operador  $Y$ . Por último  $X$  actúa como la identidad sobre sus propios autoestados manteniendolos constantes. Utilizando la notación de la sección anterior, las transiciones que aportan positivamente al medir la fidelidad con la que el canal  $\mathcal{E}$  implementa el operador  $X$ , son:

$$\begin{aligned} |\psi_{X,0}\rangle &\rightarrow |\psi_{X,0}\rangle & |\psi_{X,1}\rangle &\rightarrow |\psi_{X,1}\rangle \\ |\psi_{Y,0}\rangle &\rightarrow |\psi_{Y,1}\rangle & |\psi_{Y,1}\rangle &\rightarrow |\psi_{Y,0}\rangle \\ |\psi_{Z,0}\rangle &\rightarrow |\psi_{Z,1}\rangle & |\psi_{Z,1}\rangle &\rightarrow |\psi_{Z,0}\rangle \end{aligned}$$

Hay dos transiciones a contar por cada una de las bases, precisamente una por cada estado inicial. La receta para estimar  $\overline{F}(\mathcal{E}, X)$  será pues:

- Elegir al azar uno de los seis estados  $|\psi_{J,k}\rangle$ , donde  $J \in \{X, Y, Z\}$  y  $k \in \{0, 1\}$ .
- Aplicar el canal  $\mathcal{E}$  sobre este estado inicial.
- Hacer una medición completa en la misma base de la preparación.
- Considerar el resultado como 1 si se observa la transición esperada según la tabla correspondiente a  $X$  y como 0 en caso contrario.
- Promediar los resultados obtenidos.

El hecho importante de este ejemplo, es que todo el proceso cuántico no depende de la compuerta  $X$ . Solo los últimos dos pasos muestran una dependencia respecto a este operador y pueden realizarse clásicamente en un momento posterior a la medición.

Luego, concluimos que si realizamos una medición completa en la base  $\mathcal{B}_J$ , cada vez que aplicamos el canal a uno de los estados de la base  $\mathcal{B}_J$ , y luego seleccionamos clásicamente la salida apropiada podemos estimar la fidelidad con la que  $\mathcal{E}$  implementa cualquiera de los operadores de Heisenberg-Weyl. Lo sorprendente de esto, es que cada medición se realiza en una base predeterminada (solo depende del estado inicial), y da información para la estimación de  $D^2$  coeficientes diagonales de  $\chi$ .

## 7.2. Medición simultanea de todos los coeficientes $\chi_{mm}$

También podemos proponer un método para estimar simultaneamente todas las *gate fidelities* de  $\mathcal{E}$  respecto a los  $D^2$  operadores de Heisenberg-Weyl. Primero, se inician  $D^2$  contadores  $\mathbf{C}[\mathbf{m}]$ , uno para cada operador  $E_m$  del grupo de Heisenberg-Weyl. Se realizan  $M$  mediciones con este protocolo:

1. Se elige al azar  $\mathcal{B}_J$  una base de las presentadas en el corolario 6.11 y se prepara con distribución uniforme un estado  $|\psi_{J,\mathbf{k}}\rangle$  de la misma. La preparación del estado sigue el procedimiento indicado en la sección 6.6.
2. Se deja actuar al superoperador  $\mathcal{E}$  sobre el estado  $P_{J,\mathbf{k}}$ .
3. Se realiza una medición completa en la base  $\mathcal{B}_J$  obteniendo como resultado  $|\psi_{J,\mathbf{k}'}\rangle$ . Para realizar esta medición, primero se realiza un cambio de base a la base computacional, operación inversa a la utilizada para la preparación de los estados de  $\mathcal{B}_J$ . Allí se realiza una medición completa factorizada en mediciones locales en cada uno de los  $N$  subsistemas obteniendo de cada una los respectivos componentes de  $\mathbf{k}'$ .
4. Se incrementan en uno los contadores  $\mathbf{C}[\mathbf{m}]$  para todos los  $m$  tales que  $|\langle\psi_{J,\mathbf{k}'}|E_m|\psi_{J,\mathbf{k}}\rangle| = 1$ . Esto implica incrementar un total de  $D$  contadores en cada medición. Estos son los operadores  $E_m$  con vector de conmutación  $\mathbf{k}' - \mathbf{k}$  respecto a la base  $\mathcal{B}_J$ .

Ahora  $\frac{\mathbf{C}[\mathbf{m}]}{M}$  es un estimador no sesgado de la fidelidad media  $\overline{F}_m = \overline{F}(\mathcal{E}, E_m)$  con la que  $\mathcal{E}$  implementa  $E_m$ . La varianza de este estimador esta dada por  $\frac{2\overline{F}_m(1-\overline{F}_m)}{M} \leq \frac{1}{2M}$ . Se desprende inmediatamente que  $\frac{(D+1)\mathbf{C}[\mathbf{m}]/M-1}{D}$  es un estimador de  $\chi_{mm}$  y su desviación estándar es menor que:  $\frac{D+1}{D\sqrt{2M}}$ . Este método de estimación, garantiza automáticamente que los elementos diagonales de  $\chi$  sumen 1 en total.

Un aspecto no trivial de este protocolo tomográfico, es como saber que  $\mathbf{C}[\mathbf{m}]$  deben incrementarse al final de cada experimento. Supongamos que las base  $\mathcal{B}_J$  es distinta de la base computacional  $\mathcal{B}_Z$ . Tenemos que:  $E_m |\psi_{J,\mathbf{k}}\rangle \cong |\psi_{J,\mathbf{k}'}\rangle$ , si y solo si el vector de conmutación

de  $E_m$  respecto a la base  $\mathcal{B}_J$  es  $\mathbf{k}' - \mathbf{k}$ . Puede verse a partir de la ecuación 60 que el vector de conmutación de un operador  $E_{Z,\mathbf{q}}$  con respecto a la base  $\mathcal{B}_J$  es precisamente  $-\mathbf{q}$ . Entonces, uno de los operadores  $E_m$  con la condición de conmutación requerida puede darse con la representación canónica  $E_m = T(\mathbf{0}, \mathbf{k} - \mathbf{k}')$ . Para obtener los demás  $E_m$  con el mismo vector de conmutación respecto a  $\mathcal{B}_J$ , solo es necesario multiplicar este operador por los estabilizadores de la base  $\mathcal{B}_J$ . Los  $D^2$  estabilizadores de la base  $\mathcal{B}_J$  son por definición, los únicos operadores del grupo de Heisenberg-Weyl que tienen vector de conmutación  $\mathbf{0}$  respecto de esta base. Como vimos en la sección 6.6, las representaciones canónicas  $T(\mathbf{p}_m, \mathbf{q}_m)$  de los  $N$  generadores  $\mathbf{J}_m$  con  $0 \leq m < N$  del este estabilizador de la base  $\mathcal{B}_J$  pueden obtenerse realizando  $O(N^2)$  operaciones clásicas. No obstante deben incrementarse los contadores correspondientes a  $D$  operadores, con lo cual, por más de que obtengamos cada uno en un tiempo  $O(N)$ , necesitaremos tiempo  $O(ND)$  para incrementar todos los índices  $\mathcal{C}[\mathbf{m}]$  que correspondan. Más aun, una representación frontal de  $\mathcal{C}[\mathbf{m}]$  requiere  $D^2$  unidades de memoria, una por cada valor de  $m$ .

Si el experimento se llevó a cabo en la base computacional  $\mathcal{B}_z$  el procedimiento para determinar los operadores resulta análogo. Parte de que el operador  $T(\mathbf{k}' - \mathbf{k}, \mathbf{0})$  del estabilizador de la base  $X$  tiene el vector de conmutación buscado. Luego, la representación canónica de todos los operadores con el vector de conmutación buscado puede darse explícitamente como  $T(\mathbf{k}' - \mathbf{k}, \mathbf{q})$ , donde  $\mathbf{q}$  es un vector arbitrario.

Tanto la inicialización de los coeficientes  $\mathcal{C}[\mathbf{m}]$  a 0 como la obtención de estimadores de los  $\chi_{mm}$  a partir de los  $\mathcal{C}[\mathbf{m}]$ , requieren una cantidad de operaciones y espacio de almacenamiento ambos proporcionales a  $D^2$ . Esta es la complejidad más alta presente en el algoritmo y resulta inherente a la representación de los coeficientes  $\chi_{mm}$  que se busca obtener. El algoritmo no podrá pues bajar de complejidad mientras se use esta representación.

### 7.3. Mejorar el procesamiento clásico de mediciones

En la subsección anterior, vimos que a partir de un conjunto de  $M$  mediciones proyectivas completas es posible extraer información acerca de los  $D^2$  coeficientes diagonales  $\chi_{mm}$ . La cantidad de mediciones que realizamos es  $M$ . La cantidad de bits de información que aporta cada medición es  $N \log_2(p)$ . Por lo tanto, el resultado de las mediciones puede ser almacenado por completo utilizando  $O(MN \log_2(p))$  bits. Por un lado, esto impone una aparente contradicción, pues indica que la mayoría de los estimadores  $\chi_{mm}$  no se está estimando ni un bit de información. Por otra parte, nos indica que insistir en utilizar una representación directa para los coeficientes  $\chi_{mm}$  con un requerimiento de almacenamiento exponencial en  $N$  resulta altamente ineficiente siempre que  $MN \log_2(p) \ll D^2$ . Veamos pues, que es posible almacenar los resultados de todas y cada una de las mediciones y realizar consultas sobre los mismos de manera eficiente. La manera de almacenar estos resultados, es directamente, mediante dos índices vectoriales. El índice  $Z$  o  $\mathbf{J}$ , de la base  $\mathcal{B}_J$  que se utilizó para la preparación y medición. Esto requiere un bit para indicar si se trata de la base  $Z$  o de una base  $\mathbf{J}$  y  $N \log_2(p)$  bits para determinar el vector  $\mathbf{J}$  en caso que corresponda. También se

precisa almacenar el resultado experimental mediante la diferencia entre los vectores  $\mathbf{k}'$  y  $\mathbf{k}$  que indexan al estado medido y al preparado respectivamente. Se llamará  $\mathbf{e} = \mathbf{k}' - \mathbf{k}$ , a la diferencia entre los vectores  $\mathbf{k}'$  y  $\mathbf{k}$ . Puede representarse pues al experimento con la tupla  $(J, \mathbf{e})$  que requiere de tan solo  $2N \log_2(p) + 1$  bits.

Será esencial para continuar recordar que en el caso del conjunto de MUBs definido en el corolario 6.11 disponemos de un algoritmo  $O(N^2)$  para dar la representación canónica de los  $N$  generadores del grupo estabilizador de  $\mathcal{B}_J$ .

### 7.3.1. Estimar un $\chi_{mm}$

Estimar el peso de un  $\chi_{mm}$  particular a partir del conjunto de los  $M$  experimentos obtenidos puede lograrse eficientemente. Cada experimento se considera independientemente, y se considera el número  $C[m]$  de experimentos que admiten  $E_m |\psi_{J,\mathbf{k}}\rangle \langle \psi_{J,\mathbf{k}}| E_m^\dagger = |\psi_{J,\mathbf{k}'}\rangle \langle \psi_{J,\mathbf{k}'}|$ . Un experimento  $(J, \mathbf{e})$  admite a  $E_m = T(\mathbf{q}, \mathbf{p})$  como causante, si y solo si, el vector de conmutación de  $E_m$  con los generadores del grupo estabilizador de  $\mathcal{B}_J$  es precisamente  $\mathbf{e}$ . Si puede darse la expresión canónica para el  $i$ -ésimo generador del estabilizador de  $\mathcal{B}_J$  como  $J_i = T(\mathbf{q}_i, \mathbf{p}_i)$ . Esta condición se reduce a comprobar  $e_i = \mathbf{q} \cdot \mathbf{p}_i - \mathbf{p} \cdot \mathbf{q}_i$  para cada  $0 \leq i < N$ . Tanto la construcción de la representación canónica de los  $N$  generadores como la verificación de que el vector de conmutación sea el esperado requieren de  $O(N^2)$  operaciones. Entonces, la complejidad para estimar a  $\chi_{mm}$  a partir de  $M$  experimentos cuánticos es de  $O(N^2 M)$  operaciones clásicas.

### 7.3.2. Detectar y medir todos los $\chi_{mm}$ grandes

Una pregunta interesante que se puede buscar responder con el extracto experimental es: *¿Cuales son los  $m$  correspondientes a los  $\chi_{mm}$  más grandes?*. Sorprendentemente, veremos que si es posible dar una respuesta eficiente a esta pregunta siempre y cuando haya unos pocos  $\chi_{mm}$  con valores altos. Este es justamente el caso que puede remediarse con el uso de códigos correctores de errores. Una situación particular que se adapta a esta descripción, se da cuando la probabilidad correspondiente a cada error decrece exponencialmente con el peso de Hamming del mismo. En el caso de sistemas de qubits con esta distribución de errores, los operadores de Pauli con peso de Hamming bajo, como la identidad, errores de un qubit, errores de 2 qubits, etc. serán detectados y estimados. No obstante, la propuesta es general y no requiere ningún *ansatz* acerca de los coeficientes grandes, permitiendo la posibilidad de que nos sorprendan operadores  $E_m$  con coeficientes  $\chi_{mm}$  inesperadamente altos.

Una condición necesaria pero no suficiente para que el estimador de un determinado  $\chi_{mm}$  se encuentre entre los más grandes es  $\mathcal{C}[\mathbf{m}] \geq 2$ . En efecto, ya con un experimento, hay una cantidad exponencial de  $E_m$  para los cuales  $\mathcal{C}[\mathbf{m}] \geq 1$ . Mientras que la cantidad de operadores  $E_m$  tales que  $\mathcal{C}[\mathbf{m}] \geq 2$  es polinomial en  $M$ , estando acotada por  $\binom{M}{2}$ .<sup>13</sup> Veamos

<sup>13</sup>Adoptamos a partir de aquí, la hipótesis de que en los  $M$  experimentos, no se repiten las bases  $J$ . Esta hipótesis se satisface casi automáticamente siempre que  $M^2 \ll D$ .

que podemos determinar eficientemente los  $E_m$  tales que  $\mathbb{C}[\mathbf{m}] > 2$ .

Primero, veamos que dos experimentos  $(J, \mathbf{e})$  y  $(J', \mathbf{e}')$  tales que  $J \neq J'$  admiten exactamente un  $E_m$  común. Si los operadores  $J_i : 0 \leq i < N$  son los generadores del grupo estabilizador de la base  $\mathcal{B}_J$  y  $J'_i : 0 \leq i < N$  son los generadores del grupo estabilizador de la base  $\mathcal{B}_{J'}$  las condiciones sobre  $E_m$  son:

$$\begin{aligned} J_i E_m &= \omega^{e_i} E_m J_i \\ J'_i E_m &= \omega^{e'_i} E_m J'_i \end{aligned} \quad (61)$$

Donde aquí,  $\omega$  es la raíz de orden  $p$  de la unidad. Esto es equivalente a decir que  $\mathbf{e}$  y  $\mathbf{e}'$  son los vectores de conmutación de  $E_m$  respecto a las bases  $\mathcal{B}_J$  y  $\mathcal{B}_{J'}$  respectivamente.

Como  $\mathcal{B}_J$  y  $\mathcal{B}_{J'}$  son bases mutuamente no sesgadas estabilizadas por operadores de Heisenberg-Weyl, cualquier  $E_m$  puede escribirse, a menos de una fase como:

$$E_m \cong \prod_{i=0}^{N-1} J_i^{q_i} \times \prod_{i=0}^{N-1} J'_i{}^{q'_i} \quad (62)$$

La forma canónica  $E_m = T(\mathbf{q}, \mathbf{q}')$ , representa un caso particular de esta definición donde  $\mathcal{B}_J = \mathcal{B}_X = \mathcal{B}_0$  y  $\mathcal{B}_{J'} = \mathcal{B}_Z$ . Una vez obtenidos los vectores  $\mathbf{q}$  y  $\mathbf{q}'$  se puede obtener la representación canónica de  $E_m$  con tan solo  $O(N^2)$  operaciones. El procedimiento para obtenerla consiste en realizar una sustitución directa de los valores de  $\mathbf{q}$ ,  $\mathbf{q}'$  y las representaciones canónicas de los generadores  $J_i$  y  $J'_i$  en la ecuación 62.

Veamos entonces como podemos obtener los vectores  $\mathbf{q}$  y  $\mathbf{q}'$  de (Ec. 62). Podemos a partir de las representaciones canónicas de los generadores  $J_i$  y  $J'_i$  obtener una matriz de conmutación  $C$  con  $N \times N$  componentes en  $\mathbb{Z}_p$ .

$$J_i J'_j = \omega^{C_{i,j}} J'_j J_i \quad (63)$$

O, de manera equivalente:

$$J'_i J_j = \omega^{-C_{j,i}} J_j J'_i \quad (64)$$

La matriz de conmutación  $C$  entre dos bases  $\mathcal{B}_J$  y  $\mathcal{B}_{J'}$  contiene a todos los vectores de conmutación de los generadores  $J_i$  respecto de los generadores  $J'_j$ . Obtenerla, requiere calcular  $N^2$  productos simplécticos sumando un total de  $O(N^3)$  operaciones. Si ahora remplazamos la definición de  $E_m$  (Ec. 62) en (Ec. 61) utilizando que los estabilizadores de una misma base conmutan y la matriz de conmutación  $C$ , obtenemos:

$$\begin{aligned} \forall i \ e_i &= \sum_{j=0}^{N-1} C_{i,j} q'_j \\ \forall i \ e'_i &= \sum_{j=0}^{N-1} -C_{j,i} q_j \end{aligned} \quad (65)$$

Alternativamente, esto puede expresarse en forma matricial como:

$$\begin{aligned} \mathbf{e} &= C \mathbf{q}' \\ \mathbf{e}' &= -C^T \mathbf{q} \end{aligned} \quad (66)$$

Como  $C$  es una matriz de  $N \times N$ , calcular su inversa  $C^{-1}$  requiere de  $O(N^3)$  operaciones. Notemos que aquí no es necesario ni posible utilizar los métodos usuales de inversión para números reales. Por un lado, en  $\mathbb{Z}_p$  no existe la noción de solución aproximada. Por otra parte, no hay riesgo de que la matriz sea mal condicionada. Es posible entonces obtener  $\mathbf{q}$  y  $\mathbf{q}'$  como:

$$\begin{aligned}\mathbf{q}' &= C^{-1}\mathbf{e} \\ \mathbf{q} &= -C^{-1T}\mathbf{e}'\end{aligned}\tag{67}$$

con un costo total de  $O(N^3)$  operaciones.

Si se consideran todos los pares de experimentos realizados en distintas bases, el procedimiento mostrado permitirá obtener a lo sumo  $\binom{M}{2}$  operadores  $E_m$  tales que  $C[m] \geq 2$ . Obtener todos los  $m$  tales que  $\mathfrak{C}[m] \geq 2$  requiere con nuestro método,  $O(M^2N^3)$ , donde la mayor complejidad reside en la obtención e inversión de  $\binom{M}{2}$  matrices de conmutación  $C$ .

Como ya vimos, el cálculo de cada  $\mathfrak{C}[m]$  requiere de  $O(MN^2)$  operaciones. Como puede haber a lo sumo  $\binom{M}{2}$  valores distintos de  $m$  tales que  $\mathfrak{C}[m] \geq 2$ , esto nos mantiene en un total de  $O(M^3 \otimes N^2)$  operaciones para estimarlos a todos. Resumiendo, hay dos partes de la estimación que aportan de manera significativa a la complejidad.

1. Identificar los  $E_m$  tales que haya al menos 2 experimentos cuyo resultado puede ser atribuido al operador  $E_m$ : Requiere  $O(M^2N^3)$  operaciones.
2. Calcular los  $\mathfrak{C}[m]$  correspondientes a estos  $E_m$ : Requiere  $O(M^3 \times N^2)$  operaciones.

La complejidad total de realizar estos dos pasos, puede expresarse de manera compacta como  $O((M+N)^3N^2)$ . Notar que esta complejidad no muestra una dependencia exponencial con  $N$  ni con  $M$ .

Otra opción posible es integrar el proceso de cálculo de  $\mathfrak{C}[m]$  a la fase de identificación. Cada  $E_m$  será identificado  $\frac{\mathfrak{C}[m](\mathfrak{C}[m]-1)}{2}$  veces, con lo cual es posible despejar de aquí el valor de  $\mathfrak{C}[m]$ . Esto requiere el paso adicional de ordenar los  $E_m$  identificados requiriendo  $O(M^2 \log(M))$  operaciones adicionales.

### Medir todos los $\chi_{mm} > \epsilon$

Supongamos que queremos medir todos los  $\chi_{mm}$  que sean mayores que  $\epsilon$  con un error de medición menor que  $\delta$ . Veamos cual es el número de mediciones  $M$  necesario si queremos lograr esto con una probabilidad mayor o igual que  $P$ .

Si definimos  $F_m = \frac{D\chi_{mm}+1}{D+1}$ , podemos recordar que  $\frac{\mathfrak{C}[m]}{M}$  es un estimador no sesgado de  $F_m$  con varianza  $\frac{2F_m(1-F_m)}{M}$ . Si definimos  $\delta' = \frac{D}{D+1}\delta$ , estimar a  $\chi_{mm}$  con un error menor a  $\delta$  resulta equivalente a estimar  $F_m$  con un error menor a  $\delta'$ . Necesitamos pues, que para todos los  $F_m$  estimados valga que:

$$\left| \frac{\mathfrak{C}[m]}{M} - F_m \right| < \delta'\tag{68}$$

Esto es equivalente a:

$$\left(\frac{\mathbf{C}[\mathbf{m}]}{M} - F_m\right)^2 < \delta'^2 \quad (69)$$

Ahora, el valor medio de la expresión de la izquierda es justamente la varianza  $\frac{2F_m(1-F_m)}{M}$  del estimador de  $F_m$ . Con lo cual, la expresión de la izquierda no puede ser mayor o igual que  $\delta'^2$  con una probabilidad mayor a  $\frac{2F_m(1-F_m)}{\delta'^2 M}$ . Entonces, tenemos que:

$$P\left(\left|\frac{(D+1)\mathbf{C}[\mathbf{m}] - M}{DM} - \chi_{mm}\right| > \delta\right) < \frac{2F_m(1-F_m)}{\delta'^2 M} \quad (70)$$

Donde  $\frac{(D+1)\mathbf{C}[\mathbf{m}] - M}{DM}$  es el estimador de  $\chi_{mm}$ . La probabilidad de que alguno este mal estimado esta acotado por la suma de las probabilidades de que cada uno este mal estimado.

$$P(\text{Algún } \chi_{mm} \text{ fue estimado con error mayor que } \delta.) < \sum_{m:\chi_{mm}>\epsilon} \frac{2F_m(1-F_m)}{\delta'^2 M} \quad (71)$$

Acotando  $1 - F_m \leq 1$  y reemplazando  $F_m = \frac{D\chi_{mm}+1}{D+1}$  obtenemos:

$$\sum_{m:\chi_{mm}>\epsilon} \frac{2F_m(1-F_m)}{\delta'^2 M} \leq \sum_{m:\chi_{mm}>\epsilon} \frac{2(D\chi_{mm}+1)}{(D+1)\delta'^2 M} \quad (72)$$

Considerando que los  $\chi_{mm}$  forman una distribución de probabilidades, podemos acotar la suma de cualquier subconjunto de los mismos por 1. Además, vale que puede haber como máximo  $\lfloor \frac{1}{\epsilon} \rfloor$  coeficientes  $\chi_{mm} \geq \epsilon$ . Utilizando esto, podemos eliminar la suma sobre  $m$  y dar la siguiente cota:

$$\sum_{m:\chi_{mm}>\epsilon} \frac{2(D\chi_{mm}+1)}{(D+1)\delta'^2 M} \leq \frac{2(D+\frac{1}{\epsilon})}{(D+1)\delta'^2 M} \quad (73)$$

Podemos expresar  $\delta'$  en términos de  $\delta$ . Obtenemos una condición sobre  $M$  para que con probabilidad  $P$  todos los estimadores de los  $\chi_{mm} \geq \epsilon$  se encuentren estimados con un error menor que  $\epsilon$ .

$$\frac{2(D+\frac{1}{\epsilon})(D+1)}{D^2\delta^2 M} \leq 1 - P \quad (74)$$

En términos de  $M$ , esto puede ser escrito como:

$$M \geq \frac{2(D+\frac{1}{\epsilon})(D+1)}{D^2\delta^2(1-P)} = \frac{2(1+\frac{1}{D\epsilon})(1+\frac{1}{D})}{\delta^2(1-P)} \quad (75)$$

Si consideramos el caso en el que  $D \gg \frac{1}{\epsilon}$  se puede dar una cota aproximada aun más simple para en número  $M$  de experimentos necesarios.

$$M \gtrsim \frac{2}{\delta^2(1-P)} \quad (76)$$

Para que todos los coeficientes  $\chi_{mm} > \epsilon$  sean detectados como coeficientes grandes en la primer parte del algoritmo, debemos pedir además que para los  $\mathbf{C}[\mathbf{m}]$  correspondientes valga  $\mathbf{C}[\mathbf{m}] \geq 2$ . O equivalentemente  $\frac{\mathbf{C}[\mathbf{m}]}{M} \geq \frac{2}{M}$ . Ahora, como ya vimos en (Ec. 68) podemos asumir que:

$$\frac{\mathbf{C}[\mathbf{m}]}{M} \geq F_m - \delta' \geq \frac{D(\epsilon - \delta) + 1}{D + 1} \quad (77)$$

Alcanza pues con pedir que estemos en el caso en que:

$$\frac{D(\epsilon - \delta) + 1}{D + 1} \geq \frac{2}{M} \quad (78)$$

O bien, suponiendo  $\epsilon > \delta$  podemos despejar la siguiente condición para  $M$ :

$$M \geq \frac{2D + 2}{D(\epsilon - \delta) + 1} \quad (79)$$

Como además, tenemos  $\epsilon - \delta < 1$ , esta última condición esta implicada por:

$$M \geq \frac{2}{\epsilon - \delta} \quad (80)$$

Fortaleciendo la hipótesis  $\epsilon > \delta$  a  $\epsilon \geq \delta + \delta^2$ , que sigue siendo muy razonable<sup>14</sup>, tanto la condición (Ec. 75) como su versión simplificada (Ec. 76) implican (Ec. 80), volviéndose irrelevante requerir esta última.

### 7.3.3. Eficiencia relativo a $\epsilon$ , $\delta$ , $P$ y $N$

Si  $\delta \ll \epsilon$ , usar el mismo número de mediciones  $M$  en la etapa de detección de coeficientes grandes y la etapa de estimación de los mismos produce dos ineficiencias importantes.

1. El costo computacional clásico de la etapa de detección resultará más grande que el necesario, ya que se esta considerando un  $M$  más grande que el necesario.
2. La etapa de detección detectará como grandes a muchos  $m$  para los cuales  $\chi_{mm} < \epsilon$ . Esto provocará que en la etapa de estimación se estimen más coeficientes que los necesarios aumentando el costo computacional clásico de esta etapa.

La propuesta para salvar este inconveniente es utilizar  $\delta_0 = \epsilon - \epsilon^2$  para la etapa de detección de los coeficientes grandes. Esta propuesta se hace para satisfacer  $\epsilon \geq \delta_0 + \delta_0^2$ . Entonces con  $M_0 = O(\epsilon^{-2}(1 - P')^{-1})$  experimentos, pueden detectarse todos los  $m$  tales que  $\chi_{mm} \geq \epsilon$  con una probabilidad  $P'$ . Al haber separado lógicamente las dos etapas, debe

---

<sup>14</sup>El error con el que se busca estimar los coeficientes es por lo menos un poco más pequeño que los coeficientes que se busca estimar.

tomarse también  $P' = \sqrt{P} \approx \frac{1+P}{2}$ . En este paso, se detectan  $\binom{M_0}{2}$  índices  $m$  que se etiquetan como grandes. Son estos los coeficientes que deben estimarse utilizando el total de las  $M = O(\delta^{-2}(1 - P')^{-1})$  mediciones. La complejidad computacional de la etapa de detección es  $O(M_0^2 N^3)$ , mientras que la complejidad de la de estimación es  $O(M_0^2 M N^2)$ . Podemos finalmente dar la complejidad de las etapas de detección y estimación en términos de la precisión que se espera alcanzar.

1. Detección de coeficientes grandes:  $O(\epsilon^{-4}(1 - P')^{-2} N^3)$
2. Estimación de coeficientes:  $O(\epsilon^{-4} \delta^{-2}(1 - P')^{-3} N^2)$

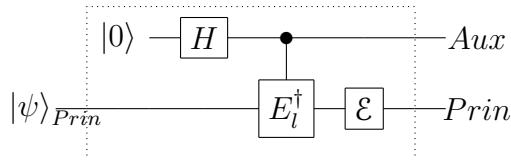
Además, el posprocesamiento clásico necesario para estimar los  $\chi_{mm}$  grandes, no tiene una dependencia exponencial con ninguno de los parámetros involucrados, incluido el número de subsistemas. Esto permite estimar eficientemente los  $\chi_{mm}$  de tamaño significativo.

#### 7.4. Medición simultanea de coeficientes no diagonales de $\chi$

En las subsecciones anteriores, hemos mostrado como es posible estimar de manera eficiente coeficientes diagonales de la matriz  $\chi$ . La idea fundamental que sostiene el método que se presentó es la utilización de un mismo conjunto de experimentos para la medición de cualquiera de los  $\chi_{mm}$ .

En esta sección, veremos que hay conjuntos de coeficientes no diagonales  $\chi_{mn}$ , que de manera análoga pueden obtenerse utilizando un mismo conjunto de experimentos. Más precisamente, para cada  $E_l$  fijo, se podrán estimar simultáneamente los  $\chi_{mn}$  tales que  $E_n^\dagger E_m \cong E_l$ . Donde aquí  $\cong$  indica que puede haber una diferencia de fases. El caso de los coeficientes diagonales  $\chi_{mm}$  pasará a ser un caso particular correspondiente a  $E_l = \mathbb{1}$ , que por algunas simplificaciones resulta más simple de entender y presentar. Una de las razones por la cual debemos tener más cuidado con los coeficientes no diagonales es porque comienza a tener importancia la fase con la que se definieron los operadores  $E_m$ . Dado un superoperador  $\mathcal{E}$ , sus coeficientes diagonales  $\chi_{mm}$  se mantendrán invariantes si en la base de la representación  $\chi$  se cambia el operador  $E_m$  por uno con una fase diferente como  $e^{i\theta} E_m$ . En los coeficientes no diagonales, este cambio en el operador  $E_m$  introducirá un factor de fase de  $e^{-i\theta}$  en los coeficientes  $\chi_{mn}$  y uno de  $e^{i\theta}$  en los coeficientes  $\chi_{nm}$ .

Si definimos a partir de  $\mathcal{E}$  un canal modificado  $\tilde{\mathcal{E}}_l$  mediante el siguiente diagrama.



Gracias al qubit auxiliar que introduce la modificación, los estados resultantes de aplicar este canal pertenecen a un espacio de Hilbert con el doble de dimensión respecto al espacio

de entrada. Imitando el desarrollo presentado en la sección 4 estudiamos la polarización horizontal (ejes  $X$  e  $Y$ ) del qubit auxiliar (cable superior del circuito), condicionada a la transición de un estado tomado al azar,  $|\psi\rangle$  al estado final  $E_n|\psi\rangle$ . Para empezar, tenemos que:

$$\tilde{\mathcal{E}}_l(P_\psi) = \sum_{m',n'} \frac{\chi_{m,n}}{2} \left[ \begin{array}{l} |0\rangle \langle 0| E_{m'} P_\psi E_{n'}^\dagger + |0\rangle \langle 1| E_{m'} P_\psi E_l E_{n'}^\dagger + \\ |1\rangle \langle 0| E_{m'} E_l^\dagger P_\psi E_{n'}^\dagger + |1\rangle \langle 1| E_{m'} E_l^\dagger P_\psi E_l E_{n'}^\dagger \end{array} \right]$$

Ahora, sobre el resultado final, trazamos sobre el sistema principal solo la parte que corresponda al resultado  $E_n P_\psi E_n^\dagger$ .<sup>15</sup> Obtenemos así la matriz densidad correspondiente al qubit auxiliar.

$$\rho_{aux} = \sum_{m',n'} \frac{\chi_{m,n}}{2} \left[ \begin{array}{l} |0\rangle \langle 0| \text{tr} \left( E_{m'} P_\psi E_{n'}^\dagger E_n P_\psi E_n^\dagger \right) + \\ |0\rangle \langle 1| \text{tr} \left( E_{m'} P_\psi E_l E_{n'}^\dagger E_n P_\psi E_n^\dagger \right) + \\ |1\rangle \langle 0| \text{tr} \left( E_{m'} E_l^\dagger P_\psi E_{n'}^\dagger E_n P_\psi E_n^\dagger \right) + \\ |1\rangle \langle 1| \text{tr} \left( E_{m'} E_l^\dagger P_\psi E_l E_{n'}^\dagger E_n P_\psi E_n^\dagger \right) \end{array} \right]$$

Si promediamos sobre todos los estados  $|\psi\rangle$  del dos diseño, podemos utilizar la ecuación 34 y obtener:

$$\overline{\rho_{aux}} = \sum_{m',n'} \frac{\chi_{m,n}}{2D(D+1)} \left[ \begin{array}{l} |0\rangle \langle 0| \left( \text{tr} \left( E_{m'} E_{n'}^\dagger E_n E_n^\dagger \right) + \text{tr} \left( E_{n'}^\dagger E_n \right) \text{tr} \left( E_n^\dagger E_{m'} \right) \right) + \\ |0\rangle \langle 1| \left( \text{tr} \left( E_{m'} E_l E_{n'}^\dagger E_n E_n^\dagger \right) + \text{tr} \left( E_l E_{n'}^\dagger E_n \right) \text{tr} \left( E_n^\dagger E_{m'} \right) \right) + \\ |1\rangle \langle 0| \left( \text{tr} \left( E_{m'} E_l^\dagger E_{n'}^\dagger E_n E_n^\dagger \right) + \text{tr} \left( E_{n'}^\dagger E_n \right) \text{tr} \left( E_n^\dagger E_{m'} E_l^\dagger \right) \right) + \\ |1\rangle \langle 1| \left( \text{tr} \left( E_{m'} E_l^\dagger E_l E_{n'}^\dagger E_n E_n^\dagger \right) + \text{tr} \left( E_l E_{n'}^\dagger E_n \right) \text{tr} \left( E_n^\dagger E_{m'} E_l^\dagger \right) \right) \end{array} \right]$$

Utilizando la unitariedad y ortogonalidad de los operadores en cuestión, podemos simplificar la expresión anterior en:

$$\overline{\rho_{aux}} = \sum_{m',n'} \frac{\chi_{m,n}}{2D(D+1)} \left[ \begin{array}{l} |0\rangle \langle 0| (D\delta_{m',n'} + D^2\delta_{n',n}\delta_{n,m'}) + \\ |0\rangle \langle 1| \left( \text{tr} \left( E_{m'} E_l E_{n'}^\dagger \right) + \text{tr} \left( E_l E_{n'}^\dagger E_n \right) D\delta_{n,m'} \right) + \\ |1\rangle \langle 0| \left( \text{tr} \left( E_{m'} E_l^\dagger E_{n'}^\dagger \right) + D\delta_{n',n} \text{tr} \left( E_n^\dagger E_{m'} E_l^\dagger \right) \right) + \\ |1\rangle \langle 1| \left( \text{tr} \left( E_{m'} E_{n'}^\dagger \right) + \text{tr} \left( E_l E_{n'}^\dagger E_n \right) \text{tr} \left( E_n^\dagger E_{m'} E_l^\dagger \right) \right) \end{array} \right]$$

Existe un único  $E_m$  perteneciente a la base de operadores unitarios ortogonales tal que  $E_m = \theta_m E_n E_l$ , donde  $\theta_m$  es una fase que debemos averiguar. Inmediatamente tenemos también que

<sup>15</sup>Recordemos que si  $|\psi\rangle$  pertenecía a una de las bases mutuamente no sesgadas estabilizadas,  $E_l|\psi\rangle$  también pertenece a la misma base. Dadas las representaciones canónicas de  $E_l$  y del estado estabilizado  $|\psi\rangle$ , la ecuación 53 define la representación canónica de  $E_l|\psi\rangle$ .

$E_m^\dagger = \theta_m^* E_l^\dagger E_n^\dagger$ . En términos de  $E_m$  y  $\theta_m$ , podemos escribir:

$$\overline{\rho_{aux}} = \sum_{m',n'} \frac{\chi_{m,n}}{2D(D+1)} \left[ \begin{array}{l} |0\rangle \langle 0| (D\delta_{m',n'} + D^2\delta_{n',n}\delta_{n,m'}) + \\ |0\rangle \langle 1| \left( \text{tr} \left( E_{m'} E_l E_{n'}^\dagger \right) + D^2\theta_m \delta_{m',n'} \delta_{n,m'} \right) + \\ |1\rangle \langle 0| \left( \text{tr} \left( E_{m'} E_l^\dagger E_{n'}^\dagger \right) + D^2\theta_m^* \delta_{n',n} \delta_{m',m} \right) + \\ |1\rangle \langle 1| \left( \text{tr} \left( E_{m'} E_{n'}^\dagger \right) + D^2\delta_{n',m} \delta_{m',m} \right) \end{array} \right]$$

Finalmente, usando la propiedad de las  $\delta$  en la suma y la hipótesis de que el canal  $\mathcal{E}$  preserva trazas, tenemos:

$$\overline{\rho_{aux}} = \frac{1}{2D(D+1)} \left[ \begin{array}{l} |0\rangle \langle 0| (D + D^2\chi_{n,n}) + \\ |0\rangle \langle 1| (D\delta_{m,n} + D^2\theta_m\chi_{n,m}) + \\ |1\rangle \langle 0| (D\delta_{m,n} + D^2\theta_m^*\chi_{m,n}) + \\ |1\rangle \langle 1| (D + D^2\chi_{m,m}) \end{array} \right]$$

O bien, simplificando un factor  $D$  y reescribiendo  $\overline{\rho_{aux}}$  como matriz, tenemos:

$$\overline{\rho_{aux}} = \frac{1}{2(D+1)} \begin{pmatrix} D\chi_{n,n} + 1 & D\chi_{n,m}\theta_m + \delta_{n,m} \\ D\chi_{m,n}\theta_m^* + \delta_{m,n} & D\chi_{m,m} + 1 \end{pmatrix} \quad (81)$$

Notamos que la ecuación obtenida es completamente análoga a la ecuación 39. Con lo cual, medición de la polarización en los ejes  $X$  e  $Y$  permitirá obtener la parte real y la parte imaginaria de  $\chi_{n,m}\theta_m$ . El único efecto de  $\theta_m$  es rotar los ejes que se utilizan para medir  $\chi_{n,m}$ .

Finalmente, solo nos resta conocer  $\theta_m$  para poder despejar  $\chi_{n,m}$  a partir de  $\chi_{n,m}\theta_m$ . Podemos suponer que disponemos de las representaciones canónicas de  $E_l$  y  $E_n$ . Entonces tenemos:

$$\begin{aligned} E_l &= T(\mathbf{p}_l, \mathbf{q}_l) = X^{\mathbf{p}_l} Z^{\mathbf{q}_l} e^{\frac{i\pi}{p} \mathbf{p}_l \cdot \mathbf{q}_l} \\ E_n &= T(\mathbf{p}_n, \mathbf{q}_n) = X^{\mathbf{p}_n} Z^{\mathbf{q}_n} e^{\frac{i\pi}{p} \mathbf{p}_n \cdot \mathbf{q}_n} \\ E_m &= \theta_m E_n E_l = T(\mathbf{p}_n + \mathbf{p}_l, \mathbf{q}_n + \mathbf{q}_l) \end{aligned}$$

De aquí, podemos despejar:

$$\theta_m = e^{\frac{i\pi}{p} (\mathbf{p}_n \cdot \mathbf{q}_l - \mathbf{p}_l \cdot \mathbf{q}_n)} \quad (82)$$

En particular, si  $E_n$  y  $E_m$  conmutan,  $\theta_m = \pm 1$ .

## 8. Conclusiones

### 8.1. Resumen de resultados

En primera instancia, este trabajo ha dado una presentación general al problema de tomografía de procesos cuánticos. Se han repasado distintos métodos de tomografía de procesos, motivando la adopción de algunas ideas y resaltando los aspectos en los que aun cabe lugar para mejoras.

La primer mejora presentada consiste en permitir la determinación de cualquier coeficiente  $\chi_{mn}$  de la matriz  $\chi$  que representa a un proceso  $\mathcal{E}$  de manera selectiva y eficiente. Nuestra propuesta reduce el problema de estimar coeficientes  $\chi$  a estimar fidelidades de a lo sumo dos canales modificados requiriendo como máximo un qubit auxiliar. El método extiende así propuestas anteriores capaces de estimar la fidelidad dando la posibilidad de estimar cualquier coeficiente. Como tal, la estimación de coeficientes requiere un número de experimentos independiente de la dimensión del sistema. Este método resulta particularmente útil cuando solo se requiere una tomografía parcial del proceso  $\mathcal{E}$  en cuestión, ya que en este caso, los recursos necesarios se vuelven polinomiales en el número de subsistemas.

A nivel de herramientas para estudios de información cuántica, este trabajo resume algunos resultados de utilidad sobre los 2-diseños y particularmente, sobre las bases mutuamente no sesgadas. Como aporte original, se muestra una definición explícita de  $D+1$  bases mutuamente no sesgadas para dimensión  $D = p^N$  estudiando propiedades específicas aprovechables para la tomografía. En base a esta definición, pueden darse construcciones experimentales de estos estados en sistemas de  $N$  qubits utilizando  $O(N^2)$  compuertas cuánticas elementales y  $O(N^3)$  operaciones clásicas.

Por último, se presenta un método novedoso que permite hacer tomografía completa de la parte diagonal de la matriz  $\chi$ . Inspirados ahora también en los trabajos de M. Mohseni y D. A. Lidar [ML06] se decide utilizar un conjunto de bases mutuamente no sesgadas asociado a la base de operadores utilizado para la representación  $\chi$ . En base a esta elección, la acción del operador  $\mathcal{E}$  estudiado respecto a los estados de las MUBs puede recibir una interpretación sencilla que conduce a un método polinomial para estimar todos los coeficientes diagonales de la matriz  $\chi$ . Se hace un estudio detallado de la precisión que permite el método llegando a la conclusión de que el mismo es capaz de detectar y caracterizar completamente los coeficientes de canales de Pauli en el caso que estos resulten tener pocos elementos de tamaño significativo. La información que este método hace disponible es la necesaria y suficiente para definir el código corrector de errores específico que conviene usar para proteger al canal. Se dieron también los primeros pasos para mostrar que las ideas que permiten la estimación simultanea de los coeficientes diagonales, también permiten la estimación simultanea de grupos de coeficientes no diagonales.

Tanto en la estimación selectiva y eficiente de coeficientes no diagonales, como en la estimación simultanea de coeficientes diagonales son aporte novedozos al area de Tomografía Cuántica. Es por ello, que junto a Ariel Bendersky y Juan Pablo Paz, hemos hecho pública

una versión resumida de estos resultados [BPP08].

## 8.2. Perspectivas a futuro

Si todavía queda un punto debil en el método tomográfico que se desarrollo, es la complejidad de los circuitos cuanticos necesarios para la preparación y medición de los estados pertenecientes a las bases mutuamente no sesgadas. Actualmente, se requieren  $O(N^2)$  compuertas para esta tarea. Esto es el mismo orden necesario para realizar tareas complejas como la transformada de Fourier cuántica. Una mejora deseable es reducir la complejidad de los circuitos cuánticos manteniendo las buenas propiedades del método de manera exacta o aproximada. Como la definición de una base general estabilizada requiere de  $O(N^2)$  parámetros, esta dirección no parece muy prometedora, pero por su potencial impacto merece ser estudiada en más profundidad.

Por otra parte, los circuitos cuánticos necesarios ni siquiera están definidos para el caso  $p \neq 2$ , pues hemos hecho uso de un resultado para qubits presentados por A. Benderski [Ben06]. Para generalizar la construcción a otros valores de  $p$ , se precisa contar con una generalización del grupo de Clifford y las correspondientes compuertas cuánticas generadoras del grupo Simpléctico.

El método de tomografía simultanea de coeficientes se encuentra limitado a una base particular de operadores para la representación  $\chi$  del canal  $\mathcal{E}$ . Una pregunta que parece interesante, es si se puede adaptar la base de operadores para la representación  $\chi$  a otra más conveniente en función de algún conocimiento previo del operador  $\mathcal{E}$ . O más interesante aun, elegir la base de operadores y las mediciones a realizar de manera adaptativa en base a los resultados de mediciones anteriores.

Por último, un area de estudio que no debemos pasar por alto es la adaptabilidad del método a ensambles físicos. Los primeros resultados que permiten medir selectivamente cualquier coeficiente de un proceso pueden adaptarse a sistemas de ensamble sin demasiado esfuerzo. Lamentablemente, la tomografía simultanea de coeficientes que se ha presentado en la sección 7, utiliza fuertemente que los resultados de medición son discretos. Esto hace que no haya una interpretación directa cuya validez se extienda a sistemas de ensambles. Por otra parte, se puede buscar como aprovechar la continuidad que ofrecen las mediciones sobre ensamble permitiendo el uso de resultados de concentración de medida.

## A. Operaciones y circuitos cuánticos

### A.1. Operadores de Pauli

Los operadores de Pauli de un qubit son los siguientes. Se incluye la identidad, para que estos operadores formen un grupo (considerando equivalentes operadores que difieren en una fase).

$$\begin{aligned} I = P_0 = \sigma_0 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ X = P_1 = \sigma_1 &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ Y = P_2 = \sigma_2 &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\ Z = P_3 = \sigma_3 &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned}$$

Con esta definición de los operadores de Pauli, vemos que son hermíticos, unitarios y ortogonales.

### A.2. Operadores de Clifford

Los operadores de Clifford son los elementos unitarios pertenecientes al grupo normalizador del grupo de Pauli. Es decir que los operadores de Clifford son aquellos unitarios que preservan el grupo de Pauli por conjugación. El grupo de Clifford para  $n$  qubits (denotado por  $\mathcal{C}_n$ ), es el conjunto de operadores  $U$  tales que:

$$\forall P \in \mathcal{P}_n : UPU^\dagger \in \mathcal{P}_n$$

El grupo de Clifford incluye estrictamente al grupo de operadores de Pauli y el grupo cociente entre los dos se denomina grupo simpléctico (denotado por  $SL$ ). Listamos a continuación algunos elementos del grupo simpléctico que se utilizan en este trabajo. También mostramos su acción por conjugación sobre los operadores de Pauli.

$H$  Compuerta de Hadamard.

$$H = (X + Z)/\sqrt{2} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (83)$$

Una propiedad de el  $H$  es que es su propio inverso (es un operador hermítico). El efecto por conjugación sobre los operadores de Pauli de 1 qubit es:

$$HXH^\dagger = Z \quad ; \quad HYH^\dagger = -Y \quad ; \quad HZH^\dagger = X$$

$S$  Compuerta de fase.

$$S = R(1/4) = |0\rangle\langle 0| + i|1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$$SXS^\dagger = Y \quad ; \quad SYS^\dagger = -X \quad ; \quad SZS^\dagger = Z$$

$R$  El operador  $R = SH$  produce por conjugación un reordenamiento cíclico de los operadores de Pauli distintos a la identidad.

$$R = SH = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}$$

$$RXR^\dagger = Z \quad ; \quad RYR^\dagger = X \quad ; \quad RZR^\dagger = Y$$

CNOT El último operador del grupo de Simplético que mencionaremos es el el operador de negación controlada o CNOT. La representación de esta operación es:

$$\text{CNOT} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10| = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Puede generarse el grupo Simplético disponiendo de los operadores CNOT entre cualquier par de qubits y los operadores  $H$  y  $R$  en cualquier qubit. Si además, se dispone de los operadores de Pauli, se puede generar el grupo completo de Clifford.

### A.3. Operadores controlados

Si  $U$  es una matriz unitaria sobre un espacio de Hilbert de Dimensión  $D$ , pueden definirse operaciones unitarias sobre el espacio de Hilbert de dimensión  $2D$  llamadas  $U$ -controlado y  $U$ -anticontrolado. La representación matricial y circuital de estas operaciones es:

$$\begin{aligned} U\text{-controlado} &= \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix} = \begin{array}{c} \bullet \\ \text{---} \\ \boxed{U} \\ \text{---} \end{array} \\ U\text{-anticontrolado} &= \begin{pmatrix} U & 0 \\ 0 & I \end{pmatrix} = \begin{array}{c} \circ \\ \text{---} \\ \boxed{U} \\ \text{---} \end{array} = \begin{array}{c} \boxed{X} \text{---} \bullet \text{---} \boxed{X} \\ \text{---} \\ \boxed{U} \\ \text{---} \end{array} \end{aligned}$$

Aquí los elementos  $0, I, U$  representan matrices de dimensión  $D \times D$ .

Si  $U$  admite una factorización:

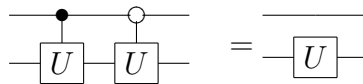
$$U = \prod_{k=1}^m U_k$$

Puede escribirse también:

$$U\text{-controlado} = \prod_{k=1}^m U_k\text{-controlado}$$

Esto es importante para lograr implementaciones eficientes de operadores controlados.

Por la definición misma de operadores controlados y anticontrolados, tenemos que vale la identidad:



## B. Algunas demostraciones

### B.1. MUBs y bases maximales de unitarios conmutativos (Demostraciones)

En este apéndice, se adaptan algunas demostraciones del artículo de Bandyopadhyay et. al [BBRV02] sobre la relación entre bases mutuamente no sesgadas y conjuntos conmutativos de operadores ortogonales y unitarios. La intención es acompañar la sección 5.4 demostrando los resultados que allí se presentan.

**Lemma B.1.** Existen como máximo  $D$  operadores normales conmutativos ortogonales no nulos.

**Demostración:** Supongamos que los operadores  $\{E_1, \dots, E_m\}$  son ortogonales y conmutan entre sí. Entonces, existe una matriz unitaria de cambio de base  $U$  que los lleva simultáneamente a una representación diagonal.

$$\forall i : D_i = UE_iU^\dagger \text{ Donde } D_i \text{ es una matriz diagonal.}$$

Como la rotación  $U$  preserva el producto interno, tenemos:

$$\forall i \neq j : \text{tr} \left( D_i D_j^\dagger \right) = \text{tr} \left( U D_i U^\dagger U D_j^\dagger U^\dagger \right) = \text{tr} \left( E_i E_j^\dagger \right) = 0$$

Entonces, las representaciones como vectores de las matrices diagonales  $D_i$  son ortogonales, y como estos vectores tienen solo  $D$  componentes, concluimos que  $m \leq D$ . **Q.E.D.** La condición de normalidad es necesaria para poder llevar los operadores a una forma diagonal en la demostración, pero el enunciado del lemma es general y correcto incluso sin esta condición.

**Teorema B.2.** Si  $\mathcal{S}_a$  y  $\mathcal{S}_b$  son ambos conjuntos de  $D$  operadores unitarios conmutativos en el espacio de Hilbert de dimensión  $D$  y  $\mathcal{S}_a \cap \mathcal{S}_b = \{\mathbb{1}\}$  y todos los operadores en  $\mathcal{S}_a \cup \mathcal{S}_b$  son ortogonales. Entonces las bases ortonormales  $\mathcal{B}_a$  y  $\mathcal{B}_b$  que diagonalizan respectivamente a los operadores en  $\mathcal{S}_a$  y  $\mathcal{S}_b$  son mutuamente no sesgadas.

**Demostración:** Para cada  $j \in \{a, b\}$  precisaremos de algunas definiciones y convenciones de nombre. Podemos enumerar los operadores de los cada subconjuntos conmutativo  $\mathcal{S}_j$  como:

$$\mathcal{S}_j = \{E_{j,0}, E_{j,1}, \dots, E_{j,D-1}\} \quad (84)$$

Donde asumimos  $\mathbb{1} = E_{j,0}$ . También podemos enumerar los vectores de la base  $\mathcal{B}_j$  que diagonaliza simultáneamente a los operadores de  $\mathcal{S}_j$  como:

$$\mathcal{B}_j = \{|\psi_{j,0}\rangle, |\psi_{j,1}\rangle, \dots, |\psi_{j,D-1}\rangle\} \quad (85)$$

Ahora definimos  $\lambda_{j,p,k}$  como el autovalor del operador  $E_{j,p}$  vector con respecto al vector  $|\psi_{j,k}\rangle$ . Podemos expandir los operadores en términos de proyectores unidimensionales.

$$E_{j,p} = \sum_{k=0}^{D-1} \lambda_{j,p,k} |\psi_{j,k}\rangle \langle \psi_{j,k}| \quad (86)$$

Como los operadores  $E_{j,p}$  son unitarios, todos los  $\lambda_{j,p,k}$  tienen norma uno. En términos de esta expansión, podemos expresar el producto interno entre operadores del mismo conjunto como:

$$\begin{aligned} \text{tr} \left( E_{j,p} E_{j,q}^\dagger \right) &= \sum_{k,l} \lambda_{j,p,k} \lambda_{j,q,l}^* \text{tr} (|\psi_{j,k}\rangle \langle \psi_{j,k}| |\psi_{j,l}\rangle \langle \psi_{j,l}|) \\ &= \sum_{k,l} \lambda_{j,p,k} \lambda_{j,q,l}^* |\langle \psi_{j,k} | \psi_{j,l} \rangle|^2 \\ &= \sum_{k,l} \lambda_{j,p,k} \lambda_{j,q,l}^* \delta_{k,l} \\ &= \sum_k \lambda_{j,p,k} \lambda_{j,q,k}^* \end{aligned}$$

Sea  $M_j$  la matriz cuadrada de dimensión  $D \times D$  cuyas componentes son:

$$M_j = \begin{pmatrix} \lambda_{j,0,0} & \lambda_{j,0,1} & \cdots & \lambda_{j,0,D-1} \\ \lambda_{j,1,0} & \lambda_{j,1,1} & \cdots & \lambda_{j,1,D-1} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{j,D-1,0} & \lambda_{j,D-1,1} & \cdots & \lambda_{j,D-1,D-1} \end{pmatrix}$$

Como la ortogonalidad de los operadores implica  $\text{tr} \left( E_{j,p} E_{j,q}^\dagger \right) = D \delta_{p,q}$ , tenemos que las filas de la matriz  $M_j$  son ortogonales y todas de norma  $D$ . Entonces, la matriz  $M_j$  es unitaria a menos de un factor de normalización  $\frac{1}{\sqrt{D}}$ . En particular, todas las componentes de la primer fila de  $M_j$  valen 1 como los autovalores de  $\mathbb{1}$ . Por último, definimos la matriz  $G$  de dimensiones  $D \times D$  como la matriz compuesta de los cuadrados de los productos internos de los vectores de la base  $\mathcal{B}_a$  con los de la base  $\mathcal{B}_b$ .

$$G = \begin{pmatrix} \langle \psi_{a,0} | \psi_{b,0} \rangle^2 & \langle \psi_{a,0} | \psi_{b,1} \rangle^2 & \cdots & \langle \psi_{a,0} | \psi_{b,D-1} \rangle^2 \\ \langle \psi_{a,1} | \psi_{b,0} \rangle^2 & \langle \psi_{a,1} | \psi_{b,1} \rangle^2 & \cdots & \langle \psi_{a,1} | \psi_{b,D-1} \rangle^2 \\ \vdots & \vdots & \ddots & \vdots \\ \langle \psi_{a,D-1} | \psi_{b,0} \rangle^2 & \langle \psi_{a,D-1} | \psi_{b,1} \rangle^2 & \cdots & \langle \psi_{a,D-1} | \psi_{b,D-1} \rangle^2 \end{pmatrix}$$

Nuestro objetivo, es precisamente probar que las componentes de  $G$  valen todas  $\frac{1}{D}$ . Ahora

si multiplicamos  $M_a$ ,  $G$  y  $M_b^\dagger$ , obtenemos una matriz cuadrada  $H = M_a G M_b^\dagger$  cuyas componentes son los productos internos entre los operadores de  $\mathcal{S}'_a$  y los de  $\mathcal{S}'_b$ .

$$\begin{aligned}
\text{tr} \left( E_{a,p} E_{b,q}^\dagger \right) &= \text{tr} \left( \sum_{k,l} \lambda_{a,p,k} |\psi_{a,k}\rangle \langle \psi_{a,k}| \lambda_{b,q,l}^* |\psi_{b,l}\rangle \langle \psi_{b,l}| \right) \\
&= \sum_{k,l} \lambda_{a,p,k} \lambda_{b,q,l}^* \text{tr} ( |\psi_{a,k}\rangle \langle \psi_{a,k}| |\psi_{b,l}\rangle \langle \psi_{b,l}| ) \\
&= \sum_{k,l} \lambda_{a,p,k} |\langle \psi_{a,k} | \psi_{b,l} \rangle|^2 \lambda_{b,q,l}^* \\
&= H_{p,q}
\end{aligned}$$

Ahora, por hipótesis, todos estos productos internos se anulan exceptuando uno.

$$\text{tr} \left( E_{a,p} E_{b,q}^\dagger \right) = D \delta_{p,0} \delta_{q,0}$$

Entonces, la representación matricial de  $H$  es:

$$H = \begin{pmatrix} D & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

Ahora podemos despejar  $G$  utilizando que la inversa de  $M_a$  es  $M_a^{-1} = \frac{1}{D} M_a^\dagger$  y la de  $M_b^\dagger$  es  $M_b^{-1\dagger} = \frac{1}{D} M_b$ .

$$G = \frac{1}{D^2} M_a^\dagger H M_b$$

Como  $H$  tiene solo la primer componente no nula, podemos calcular el producto explícitamente obteniendo a partir de la primer columna de  $M_a^\dagger$  y la primer fila de  $M_b$ .

$$G = \frac{1}{D} \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \dots & 1 \end{pmatrix}$$

**Q.E.D.**

Como corolario, podemos deducir la validez del teorema 5.8 de la sección 5.4.

**Teorema B.3.** Dadas dos bases ortonormales mutuamente no sesgadas  $\mathcal{B}_a$  y  $\mathcal{B}_b$ , podemos construir sendos conjuntos de  $D$  operadores unitarios  $\mathcal{S}_a$  y  $\mathcal{S}_b$  que resultan diagonales en las respectivas bases y tales que  $\mathcal{S}_a \cap \mathcal{S}_b = \{\mathbb{1}\}$  y todos los operadores en  $\mathcal{S}_a \cup \mathcal{S}_b$  son ortogonales. Más aun, la construcción de  $\mathcal{S}_a$  solo depende de  $\mathcal{B}_a$  y la de  $\mathcal{S}_b$ , solo depende de  $\mathcal{B}_a$ .

**Demostración:** Volvemos a utilizar la definición de  $\mathcal{B}_j$  para  $j \in \{a, b\}$  como:

$$\mathcal{B}_j = \{|\psi_{j,0}\rangle, |\psi_{j,1}\rangle, \dots, |\psi_{j,D-1}\rangle\} \quad (87)$$

Si definimos también a los conjuntos  $\mathcal{S}_j$ , con  $j \in \{a, b\}$  como:

$$\mathcal{S}_j = \{E_{j,0}, E_{j,1}, \dots, E_{j,D-1}\} \quad (88)$$

Para concretar la construcción de los  $\mathcal{S}_j$ , definimos sus elementos, los operadores  $E_{j,p}$  con  $p \in \{0, \dots, D-1\}$  como:

$$E_{j,p} = \sum_k \omega^{pk} |\psi_{j,k}\rangle \langle \psi_{j,k}| \quad (89)$$

Donde  $\omega = e^{\frac{2\pi i}{D}}$  es una raíz de la unidad de orden  $D$ . Con esta definición, vale automáticamente que  $E_{j,0} = \mathbb{1}$ . Además, los operadores conmutan por construcción y forman un subgrupo con la multiplicación. Usando el desarrollo (Ec. 89), tenemos que el producto interno entre operadores de distintas bases es:

$$\begin{aligned} \text{tr} \left( E_{a,p} E_{b,q}^\dagger \right) &= \sum_{k,l} \omega^{pk} \omega^{-ql} \text{tr} (|\psi_{a,k}\rangle \langle \psi_{a,k}| \psi_{b,l}\rangle \langle \psi_{b,l}|) \\ &= \sum_{k,l} \omega^{pk-ql} |\langle \psi_{a,k} | \psi_{b,l} \rangle|^2 \\ &= \sum_{k,l} \omega^{pk-ql} \frac{1}{D} \\ &= D \delta_{p,0} \delta_{q,0} \end{aligned}$$

Para dos operadores de una misma base, podemos hacer un análisis similar, obteniendo:

$$\begin{aligned} \text{tr} \left( E_{j,p} E_{j,q}^\dagger \right) &= \sum_{k,l} \omega^{pk} \omega^{-ql} \text{tr} (|\psi_{j,k}\rangle \langle \psi_{j,k}| \psi_{j,l}\rangle \langle \psi_{j,l}|) \\ &= \sum_{k,l} \omega^{pk-ql} |\langle \psi_{j,k} | \psi_{j,l} \rangle|^2 \\ &= \sum_{k,l} \omega^{pk-ql} \delta_{k,l} \\ &= \sum_k \omega^{(p-q)k} \\ &= D \delta_{p,q} \end{aligned}$$

La conclusión, es que todos los operadores en  $\mathcal{S}_a \cup \mathcal{S}_b$  son ortonormales (con norma  $D$ ). **Q.E.D.**

Esta demostración puede extenderse de manera trivial al caso de  $m$  bases mutuamente no sesgadas obteniendo como corolario el teorema 5.9 de la sección 5.4.

## Glosario

**Ancila** En el contexto de la computación cuántica, una ancila es un sistema auxiliar que se utiliza para el cómputo. La definición original de la palabra significa criada o sierva.

**Cuerpo** Un cuerpo  $(\mathbb{F}, +, \cdot)$  es un conjunto  $\mathbb{F}$  junto con dos operadores binarios,  $+$  (suma) y  $\cdot$  (producto) tales que:

- $(\mathbb{F}, +)$  es un grupo conmutativo.  $a + b = b + a$
- El operador  $\cdot$  es asociativo.  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- El operador  $\cdot$  distribuye respecto a  $+$ .  $a \cdot (b + c) = a \cdot b + a \cdot c$ .
- Existe un neutro para  $+$  denotado por  $0$ .
- $(\mathbb{F} \setminus \{0\}, \cdot)$  es un grupo conmutativo con elemento neutro  $1 \neq 0$ .
- Si  $a \cdot b = 0$  entonces  $a = 0$  o  $b = 0$ .

Si  $\mathbb{F}$  es finito, decimos que se trata de un cuerpo finito o cuerpo de Galois. Existen algunos resultados importantes sobre cuerpos finitos. El número de elementos de un cuerpo finito debe ser una potencia  $p^N$  de un número primo  $p$ . Dos cuerpos finitos con igual número de elementos son isomorfos. Por convención, estos cuerpos se denotan  $\mathbb{F}_{p^N}$ .

**Descomposición de Schmidt** Supongamos que  $|\psi\rangle$  es un estado puro normalizado del sistema compuesto,  $AB$ .

$$|\psi\rangle \in H_A \otimes H_B$$

Entonces pueden elegirse dos subconjuntos ortonormales  $\{|i_A\rangle\}_{i \in 1 \dots D}$  y  $|i_B\rangle_{i \in 1 \dots D}$  en  $A$  y  $B$  respectivamente, de manera que  $|\psi\rangle$  puede expresarse como:

$$|\psi\rangle = \sum_i s_i |i_A\rangle |i_B\rangle$$

Donde los  $s_i$  son coeficientes reales no negativos satisfaciendo  $\sum_i s_i^2 = 1$ . A esta representación de  $|\psi\rangle$  se la llama descomposición de Schmidt, en honor al matemático Erhard Schmidt. La existencia de una tal representación se desprende de la descomposición en valores singulares de  $|\psi\rangle$ .

Particularmente, si el número de coeficientes  $s_i$  no nulos (rango de Schmidt) en la descomposición de  $|\psi\rangle$  es mayor que 1 significa que  $|\psi\rangle$  es un estado entrelazado.

Como el espacio de operadores (en el que están incluidas estrictamente las matrices densidad) también forman un espacio de Hilbert, puede usarse la descomposición de Schmidt también para las matrices densidad que representan estados mezcla en espacios que se descomponen en dos subsistemas  $A$  y  $B$ . En este caso, las correlaciones clásicas pueden aportar al rango de Schmidt, pudiendo ser este mayor que 1, e incluso maximizarse para estados mezcla no entrelazados.

**Fidelidad media** La fidelidad media es uno de los parámetros que se utilizan para cuantificar la calidad con la que un canal  $\mathcal{E}$  implementa la identidad. Este parámetro se define como el siguiente promedio sobre estados puros:

$$\overline{F}(\mathcal{E}) \equiv \int_{F-S} \langle \psi | \mathcal{E}(|\psi\rangle \langle \psi|) |\psi\rangle d|\psi\rangle = \int_{F-S} \text{tr}(P_\psi \mathcal{E}(P_\psi)) dP_\psi$$

donde  $F - S$  denota que se utiliza la medida de Fubini-Study.

**Fidelidad de compuerta** La *gate fidelity* o fidelidad de compuerta es una generalización de la fidelidad media. En lugar de medir la calidad con la que un canal  $\mathcal{E}$  implementa la identidad, mide la calidad con la que un canal  $\mathcal{E}$  implementa un unitario arbitrario  $U$ . Esta se denota por  $\overline{F}(\mathcal{E}, U)$  y se define como:

$$\overline{F}(\mathcal{E}, U) \equiv \int_{F-S} \langle \psi | U^\dagger \mathcal{E}(|\psi\rangle \langle \psi|) U |\psi\rangle d|\psi\rangle$$

donde  $F - S$  denota que se utiliza la medida de Fubini-Study.

**Grupo de Clifford** El grupo de Clifford  $\mathcal{C}_n$  es el normalizador del grupo de Pauli  $\mathcal{P}_n$  (incluido en el grupo de operadores unitarios). Es decir, es el conjunto de operadores  $U$  tales que:

$$\forall P \in \mathcal{P}_n : U P U^\dagger \in \mathcal{P}_n$$

**Grupo de Heisenberg-Weyl** Es el grupo de operadores generado por:

$$X : |j\rangle \rightarrow |j + 1 \pmod{D}\rangle \quad Z : |j\rangle \rightarrow \omega^j |j\rangle$$

Donde  $\omega = e^{2\pi i/D}$ . Es una generalización de los operadores de Pauli para  $D \neq 2$ . Este grupo tiene un total de  $D^2$  operadores unitarios ortogonales entre si (se consideran equivalentes operadores que se diferencien por solo una fase multiplicativa). Una generalización posible de este grupo, consiste en tomar productos tensoriales de copias iguales del grupo de Heisenberg-Weyl.

**Grupo de Heisenberg-Weyl generalizado** En este trabajo, damos este nombre a cualquier conjunto de operadores que consista de los productos tensoriales de  $N$  operadores de Heisenberg-Weyl correspondientes a una dimensión  $p$  (con  $p$  primo). Bajo esta definición, este conjunto de operadores forma un grupo con  $p^N$  elementos, los cuales tienen todos orden  $p$  exceptuando la identidad.

**Grupo de Pauli generalizado** Es el grupo compuesto por el producto tensorial de operadores de Pauli. Cuando se considera los productos tensoriales de  $n$  operadores de Pauli, el grupo se denota por:  $\mathcal{P}_n$ .

**Grupo Simpléctico** El grupo simplectico  $SL_n$  es el grupo cociente entre el grupo de Clifford  $\mathcal{C}_n$  y el subgrupo de Pauli  $\mathcal{P}_n$ . Los operadores CNOT entre cualquier par de qubits junto con los operadores  $H$  y  $R$  en cualquier qubit son generadores de este grupo.

**Medida de Fubini-Study** La medida de Fubini-Study es una medida sobre el conjunto de estados puros invariente ante transformaciones unitarias.

$$\int_{F-S} f(|\psi\rangle, \langle\psi|) d|\psi\rangle = \int_{F-S} f(U|\psi\rangle, \langle\psi|U^\dagger) d|\psi\rangle =$$

Su importancia esta dada por la necesidad de realizar integración sobre el conjunto de estados puros. En el caso de un qubit, la medida es equivalente a utilizar el diferencial de area de la esfera de Bloch. En general, la condición de normalización de la medida de Fubini-Study esta dada por

$$\int_{F-S} 1 d|\psi\rangle = 1$$

**Normalizador** El normalizador de un subgrupo  $S$  de  $G$  es el conjunto de elementos de  $G$  que preservan el grupo  $S$  por conjugación. Es decir:  $N(S) = \{x \in G : xSx^{-1} = S\}$ . El normalizador de un subgrupo  $S$  es también un subgrupo de  $G$  que debe necesariamente contener a  $S$ .

**Peso de Hamming** Dado un operador de Pauli  $P_m$  que opera sobre  $N$  qubits, su peso de Hamming esta dado por la cantidad de factores distintos de la identidad en su descomposición tensorial  $P_m = P_{m_1} \otimes P_{m_2} \otimes \dots \otimes P_{m_N}$ . Como tal, el peso de Hamming de un operador se encontrara entre 0 y  $N$  siendo la identidad el único operador de Pauli con peso de Hamming 0.

**t-diseño de estados** Es un conjunto finito  $X$  de vectores  $|\psi\rangle$  tal que cualquier polinomio homogéneo de grado  $t$  en las componentes de  $|\psi\rangle$  y homogéneo de grado  $t$  en las componentes de  $\langle\psi|$  satisfice:

$$\int p(|\psi\rangle, \langle\psi|) d|\psi\rangle = \frac{1}{|X|} \sum_{|\psi\rangle \in X} p(|\psi\rangle, \langle\psi|)$$

Una definición alternativa es una distribución de probabilidad  $p_i$  sobre un conjunto de estados cuánticos  $|\phi_i\rangle$  tal que:

$$\int (|\psi\rangle \langle\psi|)^{\otimes t} d\psi = \sum_i p_i (|\phi_i\rangle \langle\phi_i|)^{\otimes t}$$

**Twirl de Haar** Rotación bilateral aleatoria de un mapa. Las posibles rotaciones son unitarios tomados aleatoriamente según la medida de Haar. Un twirl de un mapa  $\Lambda : \mathbb{C}^{D \times D} \rightarrow \mathbb{C}^{D \times D}$  resulta en el operador:

$$X \rightarrow \int_{U(D)} U^\dagger \Lambda(UXU^\dagger) U dU$$

**Twirl finito** Rotación bilateral aleatoria de un mapa, donde las posibles rotaciones se eligen de un conjunto finito de posibilidades  $\{U_k\}$  (con  $K = |\{U_k\}|$ ). Un twirl finito de un mapa  $\Lambda : \mathbb{C}^{D \times D} \rightarrow \mathbb{C}^{D \times D}$  resulta en el operador:

$$X \rightarrow \frac{1}{K} \sum_{k=1}^K U_k^\dagger \Lambda(U_k X U_k^\dagger) U_k$$

**Unital** Se dice que un operador  $O : A \rightarrow B$  es unital si mapea la identidad de  $A$  en la identidad de  $B$ . Típicamente, la evolución de una matriz densidad mediante cualquier operador unitario (acción por conjugación) es unital, ya que envía la identidad en la identidad.

## Índice alfabético

- 2-diseño, 29, 34, 37, 38, 45
- AAPT, *véase* Tomografía de procesos cuánticos asistida por ancila
- Algoritmos randomizados, 1
- Ancila, 14, 16, 80
- Base Beau, 57
- Base Belle, 57
- Base de Bell, 17, 51
- Bases mutuamente no sesgadas, 38, 44, 48
- Códigos correctores de errores, 1, 21
- Códigos esféricos, 40
- Caracterización de procesos ruidosos simetrizados, 21, 36
- Caracterización directa de dinámicas cuánticas, 16, 36
- Complementariedad, 44
- Compuerta  $R$ , 74
- Compuerta CNOT, 74
- Compuerta anticontrolada, 74
- Compuerta controlada, 33, 74
- Compuerta de fase, 74
- Compuerta de Hadamard, 33, 73
- Conjunto máximamente conmutativo de unitarios ortogonales, 28, 48, 55, 76
- Cota de Welch, 44, 45
- Criptografía cuántica, 47
- Cuerpo, 50, 80
- Cuerpo de Galois, *véase* Cuerpo finito
- Cuerpo finito, 53, 80
- DCQD, *véase* Caracterización directa de dinámicas cuánticas
- Definido completamente positivo, 6
- Definido positivo, 6
- Descomposición de Schmidt, 14, 80
- Diseños esféricos, 40
- EAPT, *véase* Tomografía de procesos cuánticos asistida por entrelazamiento
- Elemento generador, 53
- Estabilizadores, 16, 50
- Estados cuánticos aleatorios, 2
- Experimento de Stern-Gerlach, 45
- fault tolerance threshold*, 1
- Fidelidad de compuerta, 59, 81
- Fidelidad de estado, 38
- Fidelidad media, 24, 29, 37, 61, 81
- Gate fidelity*, *véase* *Fidelidad de compuerta* 59
- Grupo de Clifford, 23, 72, 73, 81
- Grupo de Heisenberg-Weyl, 81
- Grupo de Heisenberg-Weyl generalizado, 28, 49, 50, 81
- Grupo de Pauli, 73
- Grupo de Pauli generalizado, 28, 81
- Grupo Simpléctico, 72, 74, 82
- Isomorfismo de Jamiołkowski, 14, 15
- Matriz compañera, 54
- Matriz de conmutación, 64
- Medida de Fubini-Study, 29, 40, 82
- Modelo circuital, 5, 32, 38, 58
- MUBs, *véase* Bases mutuamente no sesgadas, 49, 56, 76
- Números aleatorios, 2
- Normalizador, 19, 82
- Operadores aleatorios, 2
- Operadores de Pauli generalizados, 12
- Orden de un operador, 49
- Peso de Hamming, 21, 22, 63, 82
- Polarización, 12, 35, 36, 70
- Polinomio homogéneo, 40

Polinomio primitivo, 53  
 Proceso cuántico, 5  
 Protocolo de seis estados, 47  
  
 Rango de Schmidt, 80  
 Representación  $\chi$  ( $\chi$ ), 7  
 Representación de Kraus, 6  
 Representación  $\lambda$  ( $\lambda$ ), 9, 13  
  
 SCNQP, *véase* Caracterización de procesos  
           ruidosos simetrizados  
 SQPT, *véase* Tomografía estándar de proce-  
           sos cuánticos  
  
 t-diseño, 40, 41  
 t-diseño de estados, 82  
 Tomografía cuántica de estados, 11, 47  
 Tomografía de procesos cuánticos, 11  
 Tomografía de procesos cuánticos asistida por  
           ancila, 14  
 Tomografía de procesos cuánticos asistida por  
           entrelazamiento, 14  
 Tomografía estándar de procesos cuánticos,  
           13  
 Tomografía selectiva de procesos, 27  
 Twirl de Clifford, 24  
 Twirl de Haar, 82  
 Twirl de Pauli, 22  
 Twirl finito, 83  
  
 Unital, 83  
  
 Vector de conmutación, 52

## Referencias

- [ABJ<sup>+</sup>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. *Physical Review Letters*, 90:193601, 2003.
- [BBRV02] Somshubhro Bandyopadhyay, P. Oscar Boykin, Vwani Roychowdhury, and Farrokh Vatan. A new proof for the existence of mutually unbiased bases. *Algorithmica*, 34:512–528, December 2002.
- [Ben06] Ariel Martín Bendersky. Conjuntos de bases mutuamente no sesgadas y sus aplicaciones. Master’s thesis, Facultad de Ciencias Exactas y Naturales Universidad de Buenos Aires, 2006.
- [BH07] Paul Butterley and William Hall. Numerical evidence for the maximum number of mutually unbiased bases in dimension six, 2007.
- [Boh28] N. Bohr. Das quantenpostulat und die neueren entwicklungen der atomistik. *Naturwissenschaften*, 16:245–257, 1928.
- [BPP08] A. Bendersky, F. Pastawski, and J. P. Paz. Selective Efficient Quantum Process Tomography. *ArXiv e-prints*, 801, January 2008.
- [CN97] I.L. Chuang and M. Nielsen. Prescription for experimental determination of the dynamics of a quantum black box. *J. Modern Optics*, 44:732–744, 1997.
- [Dan05] Christoph Dankert. Efficient simulation of random quantum states and operators. Master’s thesis, University of Waterloo, 2005.
- [DCEL06] Christoph Dankert, Richard Cleve, Joseph Emerson, and Etera Livine. Exact and approximate unitary 2-design: Construction and applications. 2006.
- [DGS77] P. Delsarte, J. M. Goethals, and J. J. Seidel. Spherical codes and designs. *Geometriae Dedicata*, 6, 1977.
- [DPGM92] A. Di Porto, F. Guida, and E. Montolivo. Fast algorithm for finding primitive polynomials over  $\text{gf}(q)$ . *Electronics Letters*, 28:118–120, jan 1992.
- [EAZ05] Joseph Emerson, Robert Alicki, and Karol Zyczkowski. Scalable noise estimation with random unitary operators. *QUANTUM SEMICLASS.OPT.*, 7:S347, 2005.
- [ESM<sup>+</sup>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, 2007.

- [EWS<sup>+</sup>03] Joseph Emerson, Yaakov S. Weinstein, Marcos Saraceno, Seth Lloyd, and David G. Cory. Pseudo-Random Unitary Operators for Quantum Information Processing. *Science*, 302(5653):2098–2100, 2003.
- [Got97] Daniel Gottesman. Stabilizer codes and quantum error correction, 1997.
- [idQ] *Random Number Generation using Quantum Physics*.
- [Ivo81] I. D. Ivonovic. Geometrical description of quantal state determination. *Journal of Physics A Mathematical General*, 14:3241–3245, December 1981.
- [J.S60] J.Schwinger. Unitary operator bases. *Proceedings of the National Academy of Sciences of the United States of America*, 46:570–579, April 1960.
- [Knu97] Donald E. Knuth. *Seminumerical Algorithms*, volume 2 of *The Art of Computer Programming*. Addison-Wesley, Reading, MA, USA, third edition, 1997.
- [KR05] Andreas Klappenecker and Martin Roetteler. Mutually unbiased bases are complex projective 2-designs. In *Proceedings of the IEEE International Symposium on Information Theory*, pages 1740–1744, September 2005.
- [ML06] M. Mohseni and D. A. Lidar. Direct characterization of quantum dynamics. *Physical Review Letters*, 97:170501, 2006.
- [ML07] M. Mohseni and D. A. Lidar. Direct characterization of quantum dynamics: General theory. *Physical Review A*, 75:062331, 2007.
- [NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, October 2000.
- [Nie02] Michael A. Nielsen. A simple formula for the average gate fidelity of a quantum dynamical operation. *Physics Letters A*, 303:249, 2002.
- [Rud80] Walter Rudin. *Function Theory in the Unit Ball of  $\mathbb{C}^n$* . Springer Verlag, 1980.
- [SMKE07] M. Silva, E. Magesan, D. W. Kribs, and J. Emerson. Experimentally scalable protocol for identification of correctable codes. *ArXiv e-prints*, 710, October 2007.
- [Wel74] L. Welch. Lower bounds on the maximum cross correlation of signals. *IEEE Transactions on Information Theory*, 20, May 1974.
- [WF89] W. K. Wootters and B. D. Fields. Optimal state-determination by mutually unbiased measurements. *Annals of Physics*, 191:363–381, may 1989.
- [Zim06] Mario Ziman. Notes on optimality of direct characterisation of quantum dynamics, 2006.