Conjuntos de Bases Mutuamente No Sesgadas y Sus Aplicaciones

Ariel Martín Bendersky

Tesis de Licenciatura en Ciencias Físicas
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

Diciembre de 2006

TEMA: Conjuntos de bases mutuamente no sesgadas y sus aplicaciones

ALUMNO: Ariel Martín Bendersky **L.U.N:** 133/01

LUGAR DE TRABAJO: Departamento de Física, Facultad de Ciencias Exactas y Naturales, U.B.A.

DIRECTOR DEL TRABAJO: Dr. Juan Pablo Paz

FECHA DE INICIO: Diciembre de 2005

FECHA DE FINALIZACIÓN: Diciembre de 2006

FECHA DE EXAMEN:

INFORME FINAL APROBADO POR:

Autor

Director

Profesor de Tesis de Licenciatura

Resumen

Las bases mutuamente no sesgadas constituyen, en computación cuántica, una herramienta fundamental para aplicaciones que van desde la tomografía de estados cuánticos hasta la medición de la fidelidad media de implementaciones de algoritmos cuánticos, pasando por los espacios de fases discretos. En el presente trabajo se estudiaron, en primer lugar, dichos conjuntos de bases junto con sus propiedades. Se obtuvo la cantidad de conjuntos de bases mutuamente no sesgadas que existen para sistemas de hasta 5 qubits. Luego, en relación con las funciones de Wigner y la representación de los estados en espacios de fases discretos se demostró que no todo conjunto de bases mutuamente no sesgadas es adecuado para la construcción de un espacio de fases consistente. Se analizaron, además, medidas de la fidelidad media de algoritmos cuánticos que requieren, para su estimación, de los conjuntos de bases mutuamente no sesgadas. Además se presentó una definición del peso de un conjunto de errores en un canal cuántico, que permite determinar el tipo de código de corrección de errores necesario para que un circuito cuántico alcance una fidelidad dada. Asímismo, se presentaron circuitos eficientes para la medición de dicho peso, lo que constituye una herramienta fundamental para toda implementación de algoritmos cuánticos.

Índice general

Capítulo 1

Introducción

La computación cuántica [1], que consiste en el aprovechamiento de las propiedades de sistemas cuánticos para la realización de computos, se ha convertido en los últimos años en el candidato ideal para la próxima revolución tecnológica en lo que hace a la computación. Si bien existen aún grandes dificultades técnicas para su realización, la teoría ya se encuentra en un estadío en el que permite afirmar lo antes mencionado. Por tal motivo, y por su utilidad para la simulación de sistemas cuánticos, se ha convertido en un tema de gran interés de la comunidad física, que dedica grandes esfuerzos a su estudio.

Dentro de éste marco de la computación cuántica, una herramienta que ha ido ganando terreno recientemente en virtud de sus aplicaciones al análisis de estados cuánticos e implementación de algoritmos cuánticos, es la constituída por los conjuntos de bases mutuamente no sesgadas [2][3][4][5][6][7][8]. Dichos conjuntos son conocidos desde los orígenes de la mecánica cuántica, cuando Heisenberg introdujo su proncipio de incertidumbre. En él afirmaba que al determinar la posición de una partícular se destruía toda la información sobre el momento, y viceversa. Es de la generalización de esta noción de complementariedad a sistemas de dimensión discreta que surgen los conjuntos de bases mutuamente no sesgadas.

Cada una de las bases de dicho conjunto tiene, entre otras, la propiedad de proporcionar información completamente distinta a la que proporcionan las demás. No sorprende que sea en esa propiedad que se encuentre su virtud en lo que hace a la tomografía de estados cuánticos, como mostraron Wootters y Fields en [9], puesto que mediciones en bases no sesgadas proporcionarían información completamente distinta unas de otras. Además, por razones similares, los conjuntos de bases mutuamente no sesgadas se encuntran relacionados con la definición de espacios de fases discretos

[6][10][11][12][13][14]. Asímismo, las mediciones de fidelidad de implementaciones de algoritmos cuánticos se valen de la propiedad de ausencia de sesgo para obtener una caracterización completa de la fidelidad antes mencionada [15].

Se estudiaron, en el marco del presente trabajo, dichos conjuntos de bases y algunas aplicaciones que resultan de gran interés para la computación cuántica. En el capítulo 2 se introducen los conjuntos de bases mutuamente no sesgadas, junto con propiedades de los mismos. Luego, mediante el formalismo de estabilizadores[16] se muestra una forma de caracterizar dichos conjuntos para sistemas de qubits, es decir, sistemas cuyo espacio de estados es de dimensión 2^n (ver apéndice A para una descripción más detallada), y mediante la utilización de operadores de Pauli generalizados se construyen algunos de éstos conjuntos y se establece un método mediante el cual generarlos para sistemas de qubits de tamaño arbitrario. Por último, en dicho capítulo, se presentan circuitos eficientes para el cambio de base entre dos bases de un conjunto de bases mutuamente no sesgadas dado, que requieren del orden de n^2 compuertas cuánticas para sistemas de n qubits, y n^3 operaciones clásicas para su generación.

Luego, en el capítulo 3 se da una introducción a las funciones de Wigner para sistemas continuos y discretos y, en particular, se muestra la relación estrecha que existe entre una de las posibles definiciones de espacio de fases discreto y los conjuntos de bases mutuamente no sesgadas. Además, se obtiene analíticamente la cantidad de funciones de Wigner no equivalentes que pueden definirse.

A partir de los capítulos 2 y 3 quedan planteados problemas que hacen a la relación entre las propiedades de los espacios de fases discretos y las bases mutuamente no sesgadas. En particular, en el capítulo 4 se establece la relación entre los elementos generadores de un cuerpo finito y las bases mutuamente no sesgadas. Se demuestra, además, que existen conjuntos de bases mutuamente no sesgadas que no son adecuados para definir un espacio de fases consistente, puesto que la cantidad de conjuntos de bases mutuamente no sesgadas es muy superior a la cantidad de espacios de fases que pueden definirse para sistemas de cinco qubits en adelante. Se presenta, por último, un breve repaso por problemas abiertos relativos a los conjuntos de bases mutuamente no sesgadas.

En el capítulo 5 se estudia el uso de los conjuntos de bases mutuamente no sesgadas para la determinación de la fidelidad con la que se implementa un dado algortimo cuántico. Se define, además, una nueva medida del peso de un conjunto de errores en un canal ruidoso, que permite determinar qué tipo de corrección de errores se debe utilizar para obtener la implementación

de un algoritmo cuántico con una fidelidad requerida dada. Ésto último constituye un compañero ideal para los códigos de corrección de errores, en tanto que permite, previo a la implementación del código, determinar el tipo de corrección necesaria. Se presentan, además, circuitos eficientes para la medición de la fidelidad media y del peso de un conjunto de errores.

Capítulo 2

Bases mutuamente no sesgadas

Se denominan *bases mutuamente no sesgadas*[2][3][4][5][6][7] de un espacio de Hilbert $\mathcal{H}$ a un conjunto de bases ortonormales del espacio tales que, si se prepara el sistema en un estado de una de las bases y se lo mide en otra, la probabilidad de obtener cada resultado distinto es la misma. Dichas bases, para sistemas de dimensión discreta, son la extensión natural de los operadores continuos p y q en los que, al medir uno, se destruye toda la información acerca del otro.

Para sistemas de dimensión finita es posible generalizar esas nociones de complementariedad. Por ejemplo, para un sistema de dimensión 2, los autoestados de las matrices de Pauli resultan ser bases no sesgadas. La medición del observable asociado a alguna de ellas destruye toda la información de las demás.

El estudio de este tipo de conjuntos de bases se ha convertido, recientemente, en un tema de gran importancia para el procesamiento cuántico de la información puesto que, siendo que las mediciones en las distintas bases del conjunto aportan información tan distinta sobre el estado del sistema, dichas bases resulten de gran utilidad a la hora de realizar tomografía de estados cuánticos[14], mediciones de fidelidad de canales cuánticos[15], criptografía cuántica[17] y otras aplicaciones que resultan de interés.

En éste capítulo se dará la definición de dichos conjuntos de bases y se estudiarán métodos para la generación de conjuntos de bases mutuamente no sesgadas. Se presentará, además, un nuevo algoritmo clásico para construir circuitos cuánticos eficientes para pasar de una base a otra de un conjunto dado, que requieren del orden de n^2 compuertas cuánticas, con n el número de qubits, y n^3 recursos clásicos para su generación.

2.1. Definición del objeto de estudio

Es necesario, para comenzar a hablar de los conjuntos de bases mutuamente no sesgadas, definir el objeto de estudio de manera precisa.

Al considerar un espacio de Hilbert $\mathcal{H}$ de dimensión $\dim(\mathcal{H}) = d$, y distintas bases ortonormales $B_\kappa = \{|\psi_i^\kappa\rangle, i = 1, ..., d\}$ tales que $\langle\psi_i^\kappa|\,\psi_j^\kappa\rangle = \delta_{i,j}$, se dirá que el conjunto de bases $\{B_\kappa, \kappa = 1, 2, ...m\}$ es un conjunto de m bases mutuamente no sesgadas si se cumple que:

$$|\langle\psi_i^\kappa|\,\psi_j^{\kappa'}\rangle|^2 = \frac{1}{d} \tag{2.1}$$

para todo $\kappa \neq \kappa'$, y para todo i y todo j.

Es decir, si se prepara un sistema en el estado $|\psi_i^\kappa\rangle$ y se mide en la base $B_{\kappa'}$, todos los posibles resultados ocurrirán con la misma probabilidad $1/d$. En otras palabras, dado un estado de una de las bases, no hay un sesgo en favor de ninguno de los estados de otra de las bases del conjunto.

Un ejemplo de conjunto de bases mutuamente no sesgadas para un espacio de Hilbert de dimensión 2, son las bases de autoestados de los operadores de Pauli definidos como:

$$\begin{aligned}
\sigma_x &= \sigma_1 = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
\sigma_y &= \sigma_2 = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\
\sigma_z &= \sigma_3 = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\
1 &= \sigma_0 = 1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}
\end{aligned} \tag{2.2}$$

cuyas bases de autoestados son:

$$\begin{aligned}
B_Z &= \{|0\rangle, |1\rangle\} \\
B_X &= \left\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\} \\
B_Y &= \left\{\frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle)\right\}
\end{aligned} \tag{2.3}$$

Como es sabido, al preparar un sistema de spin 1/2 en un autoestado de X, la probabilidad de medir cada uno de los dos resultados de Y o de Z es 1/2. Y esa propiedad se mantiene si se intercambian los roles de los operadores de Pauli X, Y y Z. Es decir, son bases mutuamente no sesgadas.

Debido a la propiedad (2.1), cada estado de una base es una combinación lineal de *todos* los estados de otra base no sesgada dada, en la que todos los coeficientes de la combinación lineal tienen igual amplitud. Es decir, si $\kappa \neq \kappa'$, resulta que:

$$\left|\psi_i^{\kappa'}\right\rangle = \frac{1}{\sqrt{d}} \sum_{j=1}^{d} \exp\left(i\theta_{i,j}^{\kappa'\kappa}\right) \left|\psi_j^{\kappa}\right\rangle \tag{2.4}$$

Por lo tanto, para definir un conjunto de m bases mutuamente no sesgadas, sería necesario especificar una de las bases y dar a conocer $m \times d \times (d-1)$ fases. Es por eso que resulta poco conveniente utilizar los vectores del espacio de Hilbert para trabajar con este tipo de conjuntos, y es de utilidad introducir el formalismo de estabilizadores puesto que permite, como se verá en la sección 2.2, definir una base de un conjunto de bases mutuamente no sesgadas de n qubits a partir de n operadores, en lugar de $m \times 2^n \times (2^n - 1)$ fases.

Existen, al respecto de la existencia de conjuntos de bases mutuamente no sesgadas, algunos resultados importantes y otras preguntas abiertas:

- No existen, para ningún sistema de dimensión d, conjuntos de más de $d+1$ bases mutuamente no sesgadas [18].
- Cuando la dimensión del sistema es $d = p^n$ con p primo, existe al menos un conjunto de $d+1$ bases mutuamente no sesgadas. Pueden encontrarse demostraciones distintas de dicho resultado en [7] y [6].
- No se sabe si para cualquier dimensión existen conjuntos de $d+1$ bases mutuamente no sesgadas. Se cree (hay evidencia numérica) que para dimensión 6 existen conjuntos de a lo sumo 3 bases mutuamente no sesgadas [19].

2.2. El formalismo de estabilizadores

Durante su estudio de los códigos cuánticos de corrección de errores, Daniel Gottesman desarrollo el formalismo de estabilizadores[16][20][21].

Si bien la motivación de Gottesman era esa, su formalismo tomó mucha relevancia en el campo del procesamiento de la información cuántica, y se ha

utilizado en gran cantidad de aplicaciones. Una de las aplicaciones en las que resulta de suma utilidad es el estudio de los conjuntos de bases mutuamente no sesgadas.

En esta sección, se mostrarán algunos resultados de dicho formalismo que resultarán de utilidad en lo sucesivo.

2.2.1. El grupo estabilizador

Al trabajar con el formalismo de estabilizadores, se deja de describir a los estados mediante vectores en un espacio de Hilbert y se comienza a dar una descripción a partir de operadores unitarios que tienen al estado en cuestión como autovector, y sus respectivos autovalores, que sólo pueden ser $+1$ y -1. Esto tiene la ventaja de dar una descripción más eficiente de los estados, ya que sólo se requieren n operadores para estados de n qubits, en lugar de $2^n - 1$ números complejos. Si bien suele hablarse, en la literatura, de que los estabilizadores de un estado son operadores unitarios que tienen a dicho estado como autovector de autovalor $+1$, en este trabajo se relajará la última condición permitiendo autovalores -1 para hacerlo más apropiado para el estudio de bases.

Se dice, entonces, que un cierto estado $|\psi\rangle$ es estabilizado por un operador unitario S si vale que:

$$S|\psi\rangle = \pm|\psi\rangle \tag{2.5}$$

Se desprenden de esta relación tres consecuencias fundamentales del formalismo estabilizador:

1. Si S estabiliza a $|\psi\rangle$, entonces S^{-1} también lo estabiliza.

2. El operador identidad estabiliza a todos los estados.

3. Si S_1 y S_2 estabilizan a $|\psi\rangle$, entonces $S_1 S_2$ también lo estabiliza.

de donde se concluye que el conjunto de los estabilizadores de un estado dado $|\psi\rangle$ es un grupo. Dicho grupo se denomina *grupo estabilizador*.

Una consecuencia importante que surge de la relajación del requerimiento sobre los autovalores asociados a un estabilizador de un estado dado, permitiendo que dicho valor pueda ser también -1, es que el estado asociado a un grupo estabilizador no es único. De hecho, el operador de Pauli Z estabiliza tanto a $|0\rangle$ como a $|1\rangle$; la diferencia radica en los autovalores. Sin embargo, lejos de ser una dificultad, dicha propiedad será fundamental en la aplicación del formalismo a conjuntos de bases.

El grupo estabilizador y las bases

Para aplicar el formalismo de estabilizadores a conjuntos de bases mutuamente no sesgadas, resulta necesario imponer algunas restricciones adicionales al grupo estabilizador.

Si se elije un grupo estabilizador abeliano, existirá una base de autoestados común a todos los operadores del grupo. Si se suma a ese requerimiento que *todos* los autovalores de los operadores del grupo sean ± 1, se tendrá que el grupo será estabilizador de todos los vectores de dicha base común.

Si, además, el espacio de Hilbert del sistema tiene dimensión 2^n, entonces el grupo estabilizador estará generado por n operadores. Y puesto que cada estado está asociado a un autovalor ± 1 para cada uno de los n generadores del grupo estabilizador, y que hay exactamente 2^n conjuntos de n valores ± 1, se tendrá que esa base común es única, y que recorriendo los autovalores se recorren los vectores de la base.

Un ejemplo sería, en el caso de dos qubits, la elección como generadores del grupo estabilizador de los operadores de Pauli generalizados $X \otimes X$ y $Z \otimes Z$, donde se entiende que el primer operador del producto tensorial actúa sobre el primer qubit, y el segundo sobre el segundo (Para una descripción más detallada de los operadores de Pauli generalizados, ver Apéndice B). En la tabla 2.1 se puede observar que, dependiendo de los autovalores que se asignen a cada uno de los generadores del grupo, el autovector asociado será uno distinto de los estados de la denominada base de Bell.

Autovalor de $X \otimes X$	Autovalor de $Z \otimes Z$	Estado
+1	+1	$2^{-1/2}\left(\|00\rangle + \|11\rangle\right)$
+1	-1	$2^{-1/2}\left(\|01\rangle + \|10\rangle\right)$
-1	+1	$2^{-1/2}\left(\|00\rangle - \|11\rangle\right)$
-1	-1	$2^{-1/2}\left(\|01\rangle - \|10\rangle\right)$

Tabla 2.1: *Eligiendo como generadores del grupo estabilizador abeliano los operadores de Pauli generalizados $X \otimes X$ y $Z \otimes Z$ se obtiene como base asociada la base de Bell.*

2.3. Utilizando operadores de Pauli generalizados

Como se ha visto, un grupo abeliano de operadores unitarios determina una base del espacio de Hilbert. En particular, si la dimensión del espacio de Hilbert es 2^n, un grupo que admita n generadores independientes será suficiente para determinar unívocamente dicha base. Sin embargo, todo esto

se refiere a una única base, dejando de lado todo el estudio de conjuntos de bases mutuamente no sesgadas. Se estudiarán, en lo que queda del capítulo, conjuntos de bases mutuamente no sesgadas en dimensión 2^n mediante el formalismo de los estabilizadores.

Para retomar los conjuntos de bases mutuamente no sesgadas en dimensión 2^n, resulta conveniente utilizar los operadores de Pauli generalizados (ver Apéndice B). Se demostrará a continuación que, de existir, una partición de los $2^{2n} - 1$ operadores de Pauli generalizados en $2^n + 1$ grupos abelianos de $2^n - 1$ operadores cada uno[1], induce un conjunto de $2^n + 1$ bases mutuamente no sesgadas.

Teorema 2.3.1. *Sea $G_1, G_2, ...G_{2^n+1}$ una partición del conjunto $\mathcal{P}_n$ de todos los operadores de Pauli generalizados de dimensión n (a excepción de la identidad), tal que cada uno de los G_i forma un grupo abeliano. Entonces las bases estabilizadas por cada uno de los G_i forman un conjunto de bases mutuamente no sesgadas.*

Demostración. En primer lugar, nótese que no existen conjuntos conmutativos de más de $2^n - 1$ operadores de Pauli generalizados. Por lo tanto, puesto que hay en total $2^{2n} - 1$ operadores de Pauli que deben particionarse en $2^n + 1$ conjuntos, cada conjunto contendrá exáctamente $2^n - 1$ operadores de Pauli.

Ya fue demostrado en la sección 2.2 que cada uno de los conjuntos de $2^n - 1$ operadores conmutativos da lugar a una base única del espacio de Hilbert (recordemos que los $2^n - 1$ operadores del grupo son generados por n operadores independientes y sus productos, dejando de lado a la identidad). Falta probar que, si se particionan los operadores de Pauli generalizados en $2^n + 1$ grupos abelianos, no habrá sesgo entre las bases asociadas a cada uno de los grupos estabilizadores.

Para eso, recordemos que dos operadores de Pauli generalizados pueden conmutar o anticonmutar (ver Apéndice B). Por lo tanto, cada operador de Pauli que no forme parte de un grupo abeliano de $2^n - 1$ operadores de Pauli, anticonmutará con al menos uno de los que sí pertenecen al grupo. Consideremos, ahora, dos de esos grupos:

[1]Se considera al contar la cantidad de operadores del grupo sólo los operadores de Pauli generalizados únicos, dejándose de lado aquellos que difieren de un operador de Pauli generalizado en una fase. Formalmente, cada grupo estabilizador posee infinitos operadores que pueden ser agrupados en $2^n - 1$ clases de equivalencia definidas a partir de un operador y aquellos operadores que difieren del primero en una fase. Pero se consignan, al mencionar la cantidad de operadores de un grupo, el número de clases de operadores o, rquivalentemente, el número de operadores de Pauli generalizados que pertenecen al grupo, sin contar la identidad.

$$\begin{aligned} G_r &= \left\{1, P_1^r, ..., P_{2^n-1}^r\right\} \\ G_s &= \left\{1, P_1^s, ..., P_{2^n-1}^s\right\} \end{aligned} \tag{2.6}$$

Veremos, para mostrar que no hay sesgo, que si se prepara el sistema en un estado $|\psi_1^r\rangle$ de la base inducida por G_r, y se mide cualquier operador de G_s, el valor medio de la medición es 0. En efecto, el valor medio de la medición es:

$$\langle P_i^s \rangle_{|\psi_1^r\rangle} = \mathrm{Tr}\left(|\psi_1^r\rangle \langle\psi_1^r| P_i^s\right) \tag{2.7}$$

Pero existe un operador P_j^r tal que ese estado $|\psi_1^r\rangle$ es autoestado de autovalor ± 1 y tal que P_j^r anticonmuta con P_i^s, luego:

$$\begin{aligned} \langle P_i^s \rangle_{|\psi_1^r\rangle} &= \mathrm{Tr}\left(P_j^r |\psi_1^r\rangle \langle\psi_1^r| P_j^r P_i^s\right) \\ &= -\mathrm{Tr}\left(P_j^r |\psi_1^r\rangle \langle\psi_1^r| P_i^s P_j^r\right) \\ &= -\mathrm{Tr}\left(|\psi_1^r\rangle \langle\psi_1^r| P_i^s\right) \\ &= -\langle P_i^s \rangle_{|\psi_1^r\rangle} = 0 \end{aligned} \tag{2.8}$$

Lo que concluye la demostración de que una partición de los operadores de Pauli generalizados en $2^n + 1$ grupos abelianos de $2^n - 1$ operadores cada uno induce un conjunto de $2^n + 1$ bases mutuamente no sesgadas. Se verá en el capítulo 3 que dicha partición siempre existe para sistemas de qubits. □

Asímismo, quedará claro en el capítulo 3 que si la dimensión del sistema es $d = p^k$, con p primo y k entero, existen conjuntos de $p^k + 1$ bases mutuamente no sesgadas construidas mediante la partición de conjuntos de operadores análogos a los de Pauli generalizados.

2.3.1. Ejemplos

Para el caso de un qubit, la partición es trivial. Se trata de dividir los $2^{2\times 1} - 1 = 3$ operadores de Pauli generalizados (X, Y y Z) en $2^1 + 1 = 3$ conjuntos de $2^1 - 1 = 1$ operador y la identidad. La solución es trivial:

$$\begin{aligned} G_1 &= \{1, X\} \\ G_2 &= \{1, Y\} \\ G_3 &= \{1, Z\} \end{aligned} \tag{2.9}$$

Y las bases mutuamente no sesgadas son las del ejemplo mostrado en la ecuación (2.3).

No es tan sencillo, en cambio, el caso de dos qubits, pero aún es posible armar una partición manualmente, separando los 15 operadores de Pauli generalizados en 5 conjuntos de 3 operadores conmutativos cada uno, y la identidad:

$$\begin{aligned} G_1 &= \{1\otimes 1, X\otimes 1, 1\otimes X, X\otimes X\} \\ G_2 &= \{1\otimes 1, Z\otimes 1, 1\otimes Z, Z\otimes Z\} \\ G_3 &= \{1\otimes 1, Y\otimes 1, 1\otimes Y, Y\otimes Y\} \\ G_4 &= \{1\otimes 1, X\otimes Y, Y\otimes Z, Z\otimes X\} \\ G_5 &= \{1\otimes 1, Y\otimes X, Z\otimes Y, X\otimes Z\} \end{aligned} \tag{2.10}$$

en este caso, además, es posible notar que en cada uno de los grupos sólo se pueden elegir dos operadores, y que el tercero queda automáticamente determinado por el producto de los otros dos. Es por este motivo que los generadores del grupo determinan completamente al mismo, siendo siempre tantos como el número n de qubits.

Es posible, como siempre, encontrar los estados asociados a cada uno de los grupos de la ecuación (2.10) como aquellos que son autoestados simultáneos de los cuatro operadores de cada grupo. Sin embargo, puesto que todos los estados son autoestados de la identidad, y que cada autoestado de los dos primeros operadores no triviales es también autoestado de su producto, alcanza con diagonalizar simultáneamente dos operadores que actúan sobre un espacio de Hilbert de dimensión 4.

2.4. Matrices binarias y bases mutuamente no sesgadas

Como fue mostrado por Bandyopadhyay, Boykin, Roychowdhury y Vatan en [7], existe una relación entre los conjuntos de bases mutuamente no sesgadas en dimensión 2^n y las matrices bianrias simétricas de $n\times n$. Se mostrará en esta sección dicha relación, demostrándose que existe una conexión de ida y vuelta entre dichas matrices y los conjuntos de bases mutuamente no sesgadas.

Se trata, al igual que en la sección anterior, de particionar los operadores de Pauli generalizados. Sin embargo, se agregará la restricción de particionar todos los Paulis generalizados, a excepción de aquellos que están conformados sólo por operadores Z e identidades en los distintos qubits (*grupo de operadores Z* de aquí en adelante), y aquellos formados por X e identidades

(*grupo de operadores* X de aquí en más). Estos dos grupos de operadores X y de operadores Z tienen $2^n - 1$ operadores cada uno y son abelianos, por lo tanto cada uno de ellos define una base y ambas bases son no sesgadas. Además, cualquier otro operador puede escribirse, a menos de una fase irrelevante para el formalismo de los estabilizadores, como un producto de un operador de cada grupo (por ejemplo, el operador $X \otimes Z \otimes 1 \otimes Y$ puede escribirse, a menos de una fase que no tiene importancia, como el producto entre $X \otimes 1 \otimes 1 \otimes X$ y $1 \otimes Z \otimes 1 \otimes Z$). De esta forma, el problema de encontrar las $2^n + 1$ bases mutuamente no sesgadas se reduce a utilizar la base estabilizada por los operadores Z, la estabilizada por los X, y particionar el resto de los operadores de Pauli generalizados en $2^n - 1$ grupos abelianos de $2^n - 1$ operadores cada uno.

En general, cada operador de Pauli generalizado puede escribirse, a menos de un signo que no reviste importancia como:

$$T(\vec{q}, \vec{p}) \equiv X^{\vec{q}} Z^{\vec{p}} e^{\frac{\pi i \vec{q} \cdot \vec{p}}{2}} = \left(\bigotimes_i X_i^{q_i} \right) \cdot \left(\bigotimes_j Z_j^{p_j} \right) e^{\frac{\pi i \vec{q} \cdot \vec{p}}{2}} \tag{2.11}$$

donde $\vec{p}$ y $\vec{q}$ son vectores fila binarios de dimensión n igual al número de qubits, sobre los que todas las operaciones son módulo 2. Es decir, cada operador de Pauli generalizado está unívocamente determinado por los vectores $\vec{p}$ y $\vec{q}$.

A partir de los operadores $\vec{p}$ y $\vec{q}$ es posible determinar propiedades de los correspondientes operadores de Pauli generalizados, así como de las bases estabilizadas por los mismos.

Propiedad 2.4.1. *Dos operadores $T(\vec{q}_1, \vec{p}_1)$ y $T(\vec{q}_2, \vec{p}_2)$ conmutan sí y sólo sí se cumple que el producto simpléctico se anula. Es decir:*

$$\vec{q}_1 \cdot \vec{p}_2 - \vec{q}_2 \cdot \vec{p}_1 = 0 \tag{2.12}$$

siendo todas las operaciones realizadas módulo 2.

Propiedad 2.4.2. *Dados dos operadores $T(\vec{q}_1, \vec{p}_1)$ y $T(\vec{q}_2, \vec{p}_2)$ pertenecientes al grupo estabilizador de una base no sesgada con aquella estabilizada por los operadores X y aquella estabilizada por los Z, vale que $\vec{q_1} \neq \vec{q_2}$ y $\vec{p_1} \neq \vec{p_2}$.*

Demostración. Supongamos que esto no es así, y que $q_1 = q_2$ y $p_1 \neq p_2$. Puesto que los estabilizadores forman un grupo, también el operador $X^{\vec{q_1}+\vec{q_2}} Z^{\vec{p_1}+\vec{p_2}}$ es parte del grupo estabilizador en cuestión.

Sin embargo, debido a que las operaciones entre vectores son módulo 2 y que $q_1 = q_2$, dicho operador es $Z^{\vec{p_1}+\vec{p_2}}$. Pero puesto que la base es

no sesgada con aquella estabilizada por los operadores Z, ese operador no puede pertenecer al grupo en cuestión. Por lo tanto, necesariamente vale que $q_1 \neq q_2$. Análogamente se demuestra que $p_1 \neq p_2$. □

A partir de las propiedades anteriores pueden probarse los siguientes teoremas, que establecen una relación entre los vectores $\vec{q}$ y $\vec{p}$ que forman un estabilizador dado:

Teorema 2.4.1. *Para todo grupo estabilizador que estabiliza a una base no sesgada con las bases estabilizadas por los operadores X y Z, respectivamente, existe una matriz binaria S simétrica y no singular de $n \times n$, con n el número de qubits, tal que el grupo estabilizador está compuesto por los operadores $T(\vec{q}, \vec{q}S)$.*

Demostración. En efecto, puesto que el grupo estabilizador tiene $2^n - 1$ operadores de Pauli generalizados, y que, de acuerdo con la propiedad 2.4.2, no hay dos que tengan el mismo vector $\vec{q}$, entonces habrá un operador de Pauli con cada vector $\vec{q}$ no nulo. En particular, perteneceran al grupo operadores de la forma $T\left(\vec{e_j}, \vec{p}_{\vec{e_j}}\right)$ con $\vec{e_j}$ los vectores de la base canónica.

Cualquier otro operador tendrá en su coordenada $\vec{q}$ una combinación lineal de los vectores canónicos $\vec{q} = \sum_j x_j \vec{e_j}$, con $x_j \in \{0, 1\}$. Pero puesto que los operadores de un estabilizador conforman un grupo, se tiene que también pertenece al grupo estabilizador el operador:

$$\prod_j \left(T\left(\vec{e_j}, \vec{p}_{\vec{e_j}}\right)\right)^{x_j} \propto T\left(\sum_j x_j \vec{e_j}, \sum_j x_j \vec{p}_{\vec{e_j}}\right) \tag{2.13}$$

Ésta igualdad muestra que hay una relación lineal entre los vectores $\vec{q}$ y $\vec{p}$. Por lo tanto existe una matriz S tal que los operadores de Pauli que pertenecen al grupo estabilizador son todos, a menos de una fase, de la forma $T(\vec{q}, \vec{q}S)$. Además, dicha matriz es no singular, porque el grupo no admite ningún operador con el vector nulo como coordenada $\vec{p}$ (tales operadores forman parte del grupo de los operadores X).

Falta ver, para terminar la demostración, que dicha matriz es simétrica. Pero eso se consigue imponiendo la conmutación entre todos los operadores del grupo. De acuerdo con la propiedad 2.4.1, eso es equivalente a:

$$\vec{q_i} S^\dagger \vec{q_j}^\dagger - \vec{q_j} S^\dagger \vec{q_i}^\dagger = 0 \tag{2.14}$$

para todo i y para todo j. Eso es equivalente a pedir que la matriz S sea simétrica, con lo que concluye la demostración. □

Teorema 2.4.2. *Dada una matriz S binaria simétrica con* $\det S = 1$*, los operadores $T(\vec{q}, \vec{q}S)$ forman un grupo estabilizador de una base no sesgada con las bases estabilizadas por los operadores X y Z.*

Demostración. Sólo hay que ver que los operadores de la forma $T(\vec{q}, \vec{q}S)$ conmutan, y que ninguno es un operador X o Z.

Que ninguno es un operador X o Z es simple. Ya que la matriz S es no singular, la única forma de que el vector $\vec{q}S$ sea nulo es que el vector $\vec{q}$ lo sea. Por lo tanto el único operador de esa forma que pertenece al grupo de las X o de las Z es la identidad.

Falta ver que todos conmutan. A partir de la propiedad 2.4.1, dos operadores $T(\vec{q_1}, \vec{q_1}S)$ y $T(\vec{q_2}, \vec{q_2}S)$ conmutan si y sólo si:

$$0 = \vec{q_1}S^\dagger\vec{q_2} - \vec{q_2}S^\dagger\vec{q_1} \tag{2.15}$$

Pero eso es cierto ya que $S = S^\dagger$, y con eso concluye la demostración. □

Los teoremas 2.4.1 y 2.4.2 permiten relacionar cada una de las bases de un conjunto de bases mutuamente no sesgadas con una matriz simétrica binaria no singular. El teorema que se demuestra a continuación va más allá, al dar una relación entre conjuntos de bases mutuamente no sesgadas y conjuntos de matrices binarias simétricas no singulares.

Teorema 2.4.3. *Todo conjunto de k bases mutuamente no sesgadas tales que el grupo estabilizador de una de las bases contiene a todos los operadores X y el estabilizador de otra de las bases contiene a todos los operadores Z, tiene asociado un conjunto de $k-2$ matrices de $n \times n$ binarias $\{S_1, S_2, ..., S_{k-2}\}$ tales que:*

1. $S_\alpha = S_\alpha^\dagger \ \forall\alpha$
2. $\det(S_\alpha) = 1 \ \forall\alpha$
3. $\det(S_\alpha - S_\beta) = 1 \ \forall\alpha \neq \beta$

estando los grupos estabilizadores de las $k-2$ bases restantes generados por los operadores $X^{\vec{q}_i}Z^{\vec{q}_i S_\alpha}$, donde el índice α recorre las distintas bases.

Vale también la recíproca. Todo conjunto de $k-2$ matrices binarias simétricas con las propiedades enunciadas tiene asociado, de igual forma, un conjunto de k bases mutuamente no sesgadas.

Demostración. Las dos primeras propiedades salen directo del teorema 2.4.1. Sólo falta ver que la tercera propiedad es equivalente a que no se repitan operadores de Pauli generalizados de un grupo a otro.

Dicha condición es equivalente a pedir que el operador con coordenada $\vec{q}$ de un conjunto no tenga la misma coordenada $\vec{p}$ que aquel de coordenada $\vec{q}$ de otro conjunto. Eso es:

$$\vec{q}S_\alpha - \vec{q}S_\beta \neq 0 \quad \forall \vec{q} \tag{2.16}$$

Pero eso es equivalente a pedir que $\det(S_\alpha - S_\beta) = 1 \ \forall \alpha \neq \beta$, que es la propiedad 3 del enunciado, con lo que queda demostrado el teorema. □

Éste último teorema es de suma utilidad, puesto que permite trabajar con las particiones de los operadores de Pauli como conjuntos (cada matriz representa un conjunto de operadores de Pauli generalizados), y no operador por operador, lo que facilita enormemente la tarea de buscar conjuntos de bases mutuamente no sesgadas.

Una pregunta que surge es acerca de la cantidad de conjuntos de bases mutuamente no sesgadas que existen. Dicho problema será más estudiado en el capítulo 4, sin embargo, ya pueden darse argumentos por los cuales el número de conjuntos de bases mutuamente no sesgadas crece rápidamente con el número de qubits.

Llamemos $W(n)$ a la cantidad de matrices binarias simétricas de $n \times n$ con determinante no nulo. Dicha cantidad es igual a la cantidad de bases que son no sesgadas con las dos prefijadas (no necesariamente no sesgadas entre ellas). Dicha cantidad se puede obtener analíticamente[22] como:

$$W(n) = \prod_{j=1}^{n} \left[2^j - \mathrm{Imp}(j)\right] \tag{2.17}$$

donde Imp (j) vale 1 si j es impar, y 0 si es par.

De esta forma se tiene que:

$$\begin{aligned} W(1) &= 1 \\ W(2) &= W(1) * 4 = 4 \\ W(3) &= W(2) * 7 = 28 \\ W(4) &= W(3) * 16 = 448 \\ W(5) &= W(4) * 31 = 13888 \end{aligned} \tag{2.18}$$

Este crecimiento más que exponencial en el número de qubits da un indicio respecto del gran crecimiento (mayor que exponencial) que se esperaría del número de conjuntos de bases mutuamente no sesgadas con el número de qubits, puesto que puede esperarse que el número de conjuntos de bases tenga un crecimiento, en algún sentido, combinatorio en $W(n)$. Pero éste problema será tratado en mayor detalle en el capítulo 4.

Ejemplos

En primer término, para el caso de 2 qubits existen, de acuerdo a la ecuación (2.18), 4 matrices binarias simétricas de 2×2 no singulares. Estas son:

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; A_2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}; A_3 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}; A_4 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{2.19}$$

Para completar las cinco bases mutuamente no sesgadas se deben elegir tres de éstas matrices tales que el determinante de su diferencia sea 1. Notemos que $\det(A_4 + A_1) = \det(A_4 + A_2) = \det(A_4 + A_3) = 0$. Por lo tanto, la matriz A_4 no puede generar nunca el grupo estabilizador de un conjunto de cinco bases mutuamente no sesgadas que incluyan a aquellas estabilizadas por los operadores X y Z respectivamente. Puede verse también que, si se toman las matrices $A_!$, A_2 y A_3, sí vale que el determinante de cualquier suma es 1, con lo que cumplen las tres condiciones enunciadas. Es decir, las tres matrices correspondientes a un conjunto de cinco bases mutuamente no sesgadas son:

$$S_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; S_2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}; S_3 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \tag{2.20}$$

Veamos ahora los grupos estabilizadores correspondientes a los cinco conjuntos de bases mutuamente no sesgadas. Se considerará la igualdad entre operadores a menos de una fase que sigue sin tener relevancia:

$$\begin{aligned} G_1 &= \{1 \otimes 1, X \otimes 1, 1 \otimes X, X \otimes X\} \\ G_2 &= \{1 \otimes 1, Z \otimes 1, 1 \otimes Z, Z \otimes Z\} \\ G_3 &= \left\{X^{\vec{q}} Z^{\vec{q}S_1}; \forall \vec{q}\right\} = \{1 \otimes 1, Y \otimes 1, 1 \otimes Y, Y \otimes Y\} \\ G_4 &= \left\{X^{\vec{q}} Z^{\vec{q}S_2}; \forall \vec{q}\right\} = \{1 \otimes 1, X \otimes Z, Z \otimes Y, Y \otimes X\} \\ G_5 &= \left\{X^{\vec{q}} Z^{\vec{q}S_3}; \forall \vec{q}\right\} = \{1 \otimes 1, Z \otimes X, Y \otimes Z, X \otimes Y\} \end{aligned} \tag{2.21}$$

Éstos grupos estabilizadores son los mismos del ejemplo (2.10). Puede verse, además, que no existe otra partición de los operadores de Pauli generalizados en grupos abelianos que tenga en un grupo todos los operadores X y en otro todos los Z, puesto que de existir, la elección entra las matrices A_i de las matrices S_i realizada no sería única, como de hecho lo fue.

En tres qubits no resulta tan simple. Vemos en (2.18) que hay 28 matrices simétricas binarias no singulares de 3×3, de las que hay que elegir 7 tales que las diferencias de a pares tampoco sean singulares. La dificultad no sólo radica en la mayor cantidad de matrices entre las que se puede optar, sino en el hecho de que ya no será única la elección, sino que existirán varios conjuntos de 9 bases mutuamente no sesgadas, como se verá en el capítulo 4. Un posible conjunto de 7 matrices es:

$$S_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad S_2 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \quad S_3 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

$$S_4 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad S_5 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \quad S_6 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix} \tag{2.22}$$

$$S_7 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

A partir de las matrices, al igual que en el caso de dos qubits, pueden generarse los grupos estabilizadores de cada una de las siete bases que completan el conjunto de nueve bases mutuamente no sesgadas.

2.5. Circuitos eficientes de cambio de base

Una manera muy utilizada de representar algoritmos cuánticos, es mediante los circuitos cuánticos. Descripciones detalladas sobre el modelo de computación cuántica basada en circuitos pueden encontrarse en [1] y [23].

En esta sección se mostrará que existen circuitos eficientes para pasar de una base a otra de un conjunto de bases mutuamente no sesgadas de los estudiados en la sección 2.4, en dimensión 2^n. La eficiencia de dichos circuitos radica en que son necesarios recursos del orden de n^2 para implementarlos, y orden n^3 de recursos clásicos para determinarlos. Para mostrar la existencia de los circuitos, se presentará un algoritmo nuevo que permite, a una computadora clásica, generar el circuito de cambio de base entre las correspondientes a dos grupos estabilizadores de Pauli dados. Para un enfoque distinto de la construcción de circuitos de cambio de base, en el contexto de los códigos de corrección de errores, ver [24].

En primer término se definirán tres transformaciones unitarias que, además de los operadores de Pauli, serán utilizadas para la construcción de los circuitos en cuestión. Luego, mediante la aplicación sucesiva de dichas compuertas cuánticas, se construirán los circuitos requeridos.

2.5.1. Compuertas cuánticas a utilizar

La transformada de Hadamard

La transformada de Hadamard H actúa sobre un qubit de la base computacional como:

$$\begin{aligned} H|0\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ H|1\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned} \tag{2.23}$$

Puede mostrarse, además, que $H^\dagger = H = H^{-1}$, es decir, que es una transformación unitaria y hermítica.

Circuitalmente, se ilustra dicha transformación como se muestra en la figura 2.1.

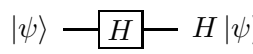

Figura 2.1: *Representación circuital de la transformada de Hadamard.*

Una particularidad fundamental de ésta transformación es la forma en que actúa sobre los operadores de Pauli, como se ve en las ecuaciones (2.24), (2.25) y (2.26). La representación circuital de dichas igualdades puede verse en la figura 2.2.

$$HXH = Z \tag{2.24}$$

$$HZH = X \tag{2.25}$$

$$HYH = -Y \tag{2.26}$$

Es decir, pasa de la base de autoestados de X a la de Z, y viceversa.

Operador de fase

La transformada de Hadamard permite convertir operadores X en Z y viceversa; sin embargo, para poder realizar transformaciones más complejas, es necesario incluir al operador Y, invariante a menos de una fase frente a H, en las transformaciones. Para ello se utiliza el operador de fase T definido como:

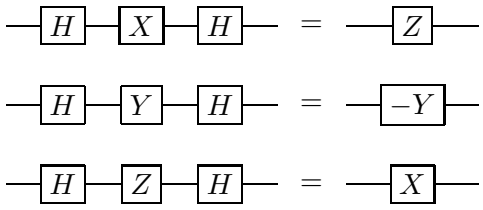

Figura 2.2: *Modo en el que actúa el operador de Hadamard sobre los operadores de Pauli.*

$$\begin{aligned} T|0\rangle &= |0\rangle \\ T|1\rangle &= i|1\rangle \end{aligned} \tag{2.27}$$

En la figura 2.3 puede verse la representación circuital del operador T.

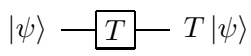

Figura 2.3: *Representación circuital del operador de fase.*

En éste caso, resultarán de importancia las equivalencias dadas en la figura 2.4.

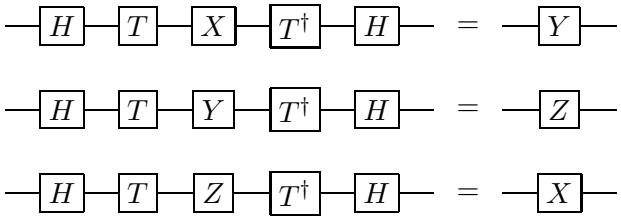

Figura 2.4: *El operador T, en conjunto con H, permite moverse cíclicamente por los operadores de Pauli.*

La compuerta C-Not

La compuerta C-Not, también llamada control-not, es un negador controlado cuántico. Dicha compuerta será la única que se utilizará en este trabajo que haga interactuar dos qubits y será, por tanto, la responsable de modificar las propiedades de entrelazamiento de los estados.

En la figura 2.5 se muestra el resultado de la aplicación de la compuerta C-Not sobre una base del espacio de dos qubits, con lo que queda completamente definido el operador.

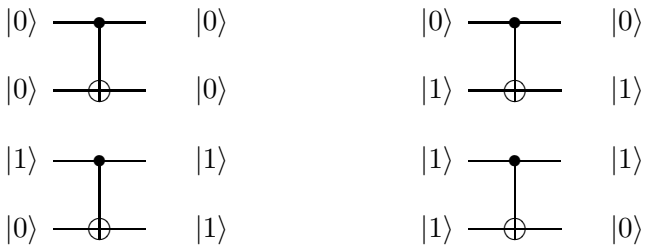

Figura 2.5: *La compuerta C-Not y su accionar sobre una base del espacio de Hilbert de dos qubits.*

Una característica importante de la compuerta C-Not es que puede ser utlizada para construir una compuerta de intercambio entre dos qubits, combinando tres C-Not de la forma ilustrada en la figura 2.6.

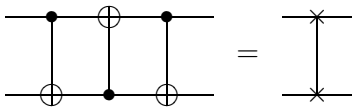

Figura 2.6: *Las compuertas C-Not se pueden combinar para intercambiar la información de dos qubits.*

Obedece, además, las reglas de conmutación con los operadores de Pauli que se ilustran en las figuras 2.7 y 2.8.

2.5.2. Construcción de los circuitos

En primer término, es importante notar que si es posible construir eficientemente circuitos que lleven cualquier base estabilizada por operadores de Pauli generalizados a aquella estabilizada por los operadores Z, entonces será posible construir circuitos que lleven de cualquier base estabilizada por un conjunto de operadores de Pauli a cualquier otra base estabilizada por otro conjunto de operadores de Pauli, combinando dos de estos circuitos. Se trata, por lo tanto, de encontrar circuitos para pasar de cualquier base estabilizada por operadores de Pauli a la base estabilizada por los operadores Z.

Para llevar a cabo la construcción del circuito de cambio de base de la estabilizada por $\left\{X^{\vec{q}}Z^{\vec{q}S}, \forall \vec{q}\right\}$ a la base estabilizada por $\left\{Z^{\vec{q}}, \forall \vec{q}\right\}$, resulta conveniente comenzar por construir una transformación unitaria $\tilde{U}$ que convierta un autovector de $X^{\vec{1}}Z^{\vec{1}S}$ en un autovector de $Z^{\vec{1}}$ de igual autovalor, donde $\vec{1}$ es el vector bianrio de dimensión n que tiene un 1 en la primera

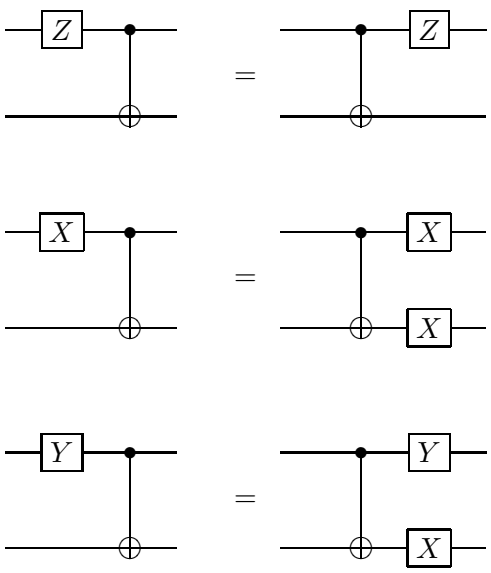

Figura 2.7: *Reglas de conmutación de la compuerta C-Not con operadores de Pauli en el qubit de control.*

componente y ceros en las demás. Es decir, encontrar una transformación unitaria $\tilde{U}$ tal que se verifique la siguiente implicación:

$$\begin{aligned} X^{\vec{1}} Z^{\vec{1}S} |\psi\rangle &= \lambda |\psi\rangle \\ \Longrightarrow Z^{\vec{1}} \tilde{U} |\psi\rangle &= \lambda \tilde{U} |\psi\rangle \end{aligned} \tag{2.28}$$

Equivalentemente, $Z^{\vec{1}} = \tilde{U} X^{\vec{1}} Z^{\vec{1}S} \tilde{U}^\dagger$. Por lo tanto, se construirá una operador $\tilde{U}$ que actúe convirtiendo por conjugación (es decir, multiplicando a izquierda por $\tilde{U}$ y a derecha por $\tilde{U}^\dagger$) un operador de Pauli dado en el operador $Z^{\vec{1}}$,

Para conseguir dicha transformación es necesario, en primer lugar, convertir al operador en cuestión en un operador formado sólo por Z e identidades. Esto puede conseguirse aplicando, por conjugación, transformaciones de Hadamard y operadores de fase a los qubits individuales:

$$\bigotimes_{j=1}^{n} R_j \left[\vec{1}_j, \left(\vec{1}S \right)_j \right] \tag{2.29}$$

donde el subíndice j indica el qubit sobre el que actúa la operación, y R_j

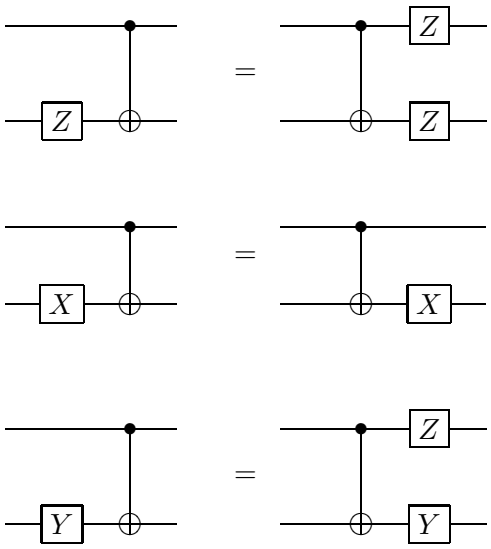

Figura 2.8: *Reglas de conmutación de la compuerta C-Not con operadores de Pauli en el qubit de objetivo.*

está dada por:

$$\begin{array}{rcl} R_j\left(0,0\right) & = & 1_j \\ R_j\left(1,0\right) & = & H_j \\ R_j\left(0,1\right) & = & 1_j \\ R_j\left(1,1\right) & = & H_j T_j^{\dagger} \end{array} \tag{2.30}$$

Supongamos, a modo de ejemplo, que se intenta construir una transformación unitaria V que convierta al operador $X\otimes 1\otimes X\otimes Z\otimes Y$ en el operador $Z\otimes 1\otimes Z\otimes Z\otimes Z$. Es decir, $V\left(X\otimes 1\otimes X\otimes Z\otimes Y\right)V^{\dagger}=Z\otimes 1\otimes Z\otimes Z\otimes Z$. De acuerdo a las ecuaciones (2.29) y (2.30), el operador V estaría dado por:

$$V = H\otimes 1\otimes 1\otimes 1\otimes HT^{\dagger} \tag{2.31}$$

que, considerando la representación circuital mostrada en la figura 2.9 de $VX\otimes 1\otimes X\otimes Z\otimes YV^{\dagger}$ y las identidades exhibidas en las figuras 2.4 y 2.2, es igual a $Z\otimes 1\otimes Z\otimes Z\otimes Z$.

Luego debe aplicarse alguna transformación que convierta todos los operadores Z en identidades, a excepción del operador del primer qubit, que debe permanecer Z. Esto puede conseguirse aplicando un C-Not con control en cada uno de los qubits que no tienen a la identidad y objetivo en el primero:

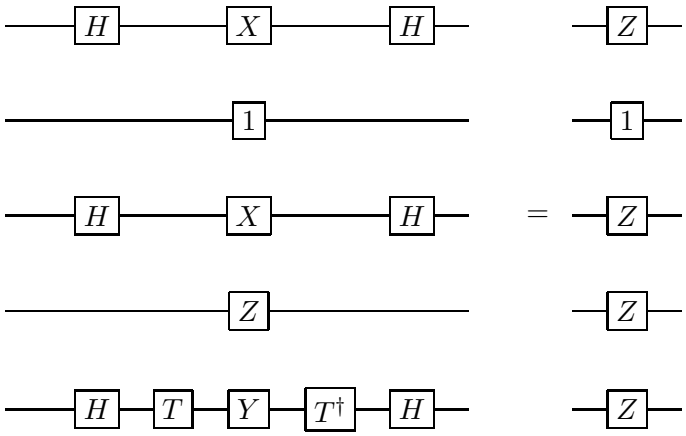

Figura 2.9: *Un operador de Pauli generalizado puede convertirse, mediante la aplicación de transformaciones de sólo un qubit, en un producto de operadores Z e identidades.*

$$\prod_{j=2}^{n} \left(\mathrm{C-Not}\left(j,1\right)\right)^{\left(1-\delta_{\vec{1}_j,0}\delta_{\left(\vec{1}S\right)_j,0}\right)} \tag{2.32}$$

donde el exponente da cuenta de que sólo se realiza el $\mathrm{C-Not}$ utilizando los qubits que no tienen una identidad.

Continuando con el ejemplo de 2.9, puede verse dicha transformación en la figura 2.10. La operación completa para convertir un Pauli que no posee una identidad en el primer qubit del grupo estabilizador en el operador Z del primer qubit es, entonces:

$$\tilde{U} = \prod_{j=2}^{n} \left(\mathrm{C-Not}\left(j,1\right)\right)^{\left(1-\delta_{\vec{1}_j,0}\delta_{\left(\vec{1}S\right)_j,0}\right)} \bigotimes_{j=1}^{n} R_j \left[\vec{1}_j, \left(\vec{1}S\right)_j\right] \tag{2.33}$$

Sin embargo, el problema no se resuelve aquí; al convertir un cierto operador del estabilizador original en un operador Z sobre el primer qubit, el resto de los operadores del estabilizador también se transforman. Pero puesto que la transformación $\tilde{U}$ conserva la característica abeliana del grupo, se obtendrá luego de la transformación, un grupo abeliano estabilizador al cual pertenece el operador Z del primer qubit. Se debe, en éste punto, determinar generadores de dicho grupo abeliano. Para eso, se deben tomar los n generadores O_j del grupo, y transformarlos como $\tilde{U}O_j\tilde{U}^\dagger$. Determinar el resultado de dicha transformación, puesto que los O_j son operadores de Pauli y $\tilde{U}$ está compuesta por rotaciones entre los operadores de Pauli y

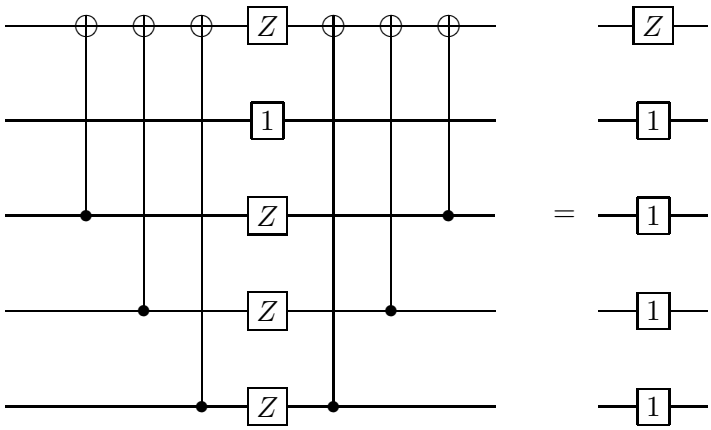

Figura 2.10: *Mediante la aplicación de compuertas C-Not puede llevarse un producto de operadores Z a un operador Z en el primer qubit.*

compuertas $\mathrm{C-Not}$ es eficiente, mediante las reglas de conmutación ya presentadas. Se requiere, para cada generador, del orden de n operaciones clásicas para determinar el resultado; es decir, n^2 operaciones para ver como transforma el grupo estailizador.

Dicho grupo estabilizador transformado poseerá operadores con identidades y Z en el primer qubit, cualquier otra opción violaría la propiedad abeliana del grupo. Por lo tanto existirá un subgrupo con identidades en el primer qubit que es simple de encontrar: se debe, a cada generador que no posee una identidad en el primer qubit, multiplicarlo por Z_1, donde el subíndice indica el qubit sobre el que actúa el operador en cuestión. Y debido a que Z_1 también pertenece al grupo, el resultado será un generador del grupo con una identidad en el primer qubit. Sobre ese subgrupo que actúa sobre los últimos $n-1$ qubits, se repite el procedimiento para convertir un autoestado de uno de los operadores en autoestado de Z_2, y así sucesivamente hasta convertir a todos los generadores en operadores Z.

De esta forma, con n operadores unitarios como el descripto anteriormente, cada uno utilizando del orden de n compuertas cuánticas, se lleva un grupo estabilizador arbitrario al grupo de las Z. Es decir, se requieren del orden de n^2 operaciones fundamentales. Los recursos clásicos necesarios son del orden de n^3, puesto que para cada uno de los n circuitos que llevan un operador de los generadores a un operador Z en el primer qubit, se deben propagar n generadores por el circuito, requiriendo n operaciones clásicas cada uno; es decir n^3 operaciones clásicas para determinar el circuito.

Algoritmo de construcción del circuito de cambio de base

Se puede describir el algoritmo de construcción del circuito de cambio de base de manera recursiva mediante el algoritmo que se incluye a continuación. De acuerdo a las consideraciones anteriores:

- El procedimiento para generar el circuito recibe como parámetros la lista de generadores del grupo estabilizador y el primer qubit k.
-
  - Seleccionar algún generador $X^{\vec{q}}Z^{\vec{p}}$ que no tenga la identidad en el qubit k.
  - Rotar todos los qubits hasta convertir el generador en cuestión en Z e identidades. Requiere del orden de n operaciones clásicas determinar las rotaciones correspondientes:

$$\bigotimes_{j=k}^{n} R_j\left(q_j, p_j\right) \tag{2.34}$$

  - Aplicar $\mathrm{C-Not}$ con control en cada qubit distinto del k que no tiene la identidad, y objetivo en el qubit k:

$$\prod_{j=k+1}^{n} \left(\mathrm{C-Not}\left(j,k\right)\right)^{\left(1-\delta_{q_j,0}\delta_{p_j,0}\right)} \tag{2.35}$$

  - Propagar los $n-1$ generadores restantes por el circuito descripto en los items anteriores. Requiere del orden de n^2 operaciones clásicas.
  - Multiplicar aquellos generadores que tienen al operador Z en el qubit k por Z_k.
  - Todos los generadores tienen una identidad en el primer qubit. Si $k \neq n$, llamar al procedimiento de generación del circuito con el grupo de generadores para los qubits $k+1$ al n y con $k+1$ como el primer qubit.

Una aclaración importante sobre el algoritmo es que, para comenzar, se debe generar la lista de generadores asociados a la matriz S y llamar al procedimiento con dicha lista y $k = 1$. No es conveniente que el procedimiento recursivo reciba como parámetro a la matriz S, porque podría suceder que alguno de los subgrupos de menor cantidad de qubits con los que se realice el llamado recursivo posea operadores Z, para los que no hay matriz S asociada.

Ejemplo

Supongamos que se quiere convertir el grupo estabilizador G en aquel estabilizado por los operadores Z, donde G está generado por:

$$G = \{X \otimes Z \otimes 1, Z \otimes Y \otimes Z, 1 \otimes Z \otimes Y\} \tag{2.36}$$

Notemos que alcanza con dar 3 operadores, puesto que los demás son productos de ellos.

Dice el algoritmo anterior que, en primer lugar, debe tomarse el operador $X \otimes Z \otimes 1$ y aplicar las tranformaciones correspondientes para llevar cada qubit a operadores Z para luego, mediante compuertas C-Not, llevar el operador a un operador Z sobre el primer qubit. Las rotaciones son simples, sólo aplicar H al primer qubit. En la figura 2.11 puede verse el circuito parcial.

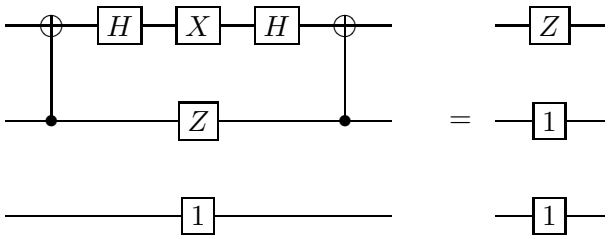

Figura 2.11: *Primera etapa del circuito de cambio de base.*

El problema que surge es que el circuito de 2.11 también modifica los demás operadores del estabilizador. Luego de aplicado el circuito, el estabilizador se convierte en:

$$G' = \{Z \otimes 1 \otimes 1, 1 \otimes Y \otimes Z, 1 \otimes Z \otimes Y\} \tag{2.37}$$

La segunda etapa del algoritmo debe tomar el operador $1 \otimes Y \otimes Z$ y transformarlo, mediante $\tilde{\tilde{U}}$, de la misma forma; pero puesto que dicho operador sólo aparece una vez realizada la transformación $\tilde{U}$ como imagen del operador $Z \otimes Y \otimes Z$, debe implementarse luego de ésta. Los pasos son los mismos, en primer lugar transformar la Y del segundo qubit en Z, y luego mediante un C-Not convertir la Z del tercero en una identidad, como se ve en la figura 2.12.

Es importante notar que ésta segunda etapa no afecta al primer qubit, por lo que lo conseguido con la primera de llevar el primer operador a una Z sobre el primer qubit se mantiene, mientras que se consigue, además, que el segundo operador se convierta en una Z del segundo qubit.

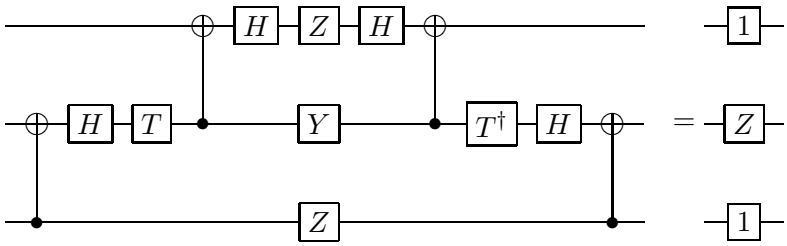

Figura 2.12: *Segunda etapa del circuito de cambio de base.*

Nuevamente, esta modificación actúa sobre el tercer operador, por lo que nuevamente hay que ver como queda dicho operador luego de la segunda etapa. El grupo estabilizador queda, luego de la segunda etapa:

$$G'' = \{Z \otimes 1 \otimes 1, 1 \otimes Z \otimes 1, 1 \otimes 1 \otimes Y\} \tag{2.38}$$

Debe, para corregirse el tercer operador, aplicar una tranformación al tercer qubit. Dicho circuito se puede observar en la figura 2.13.

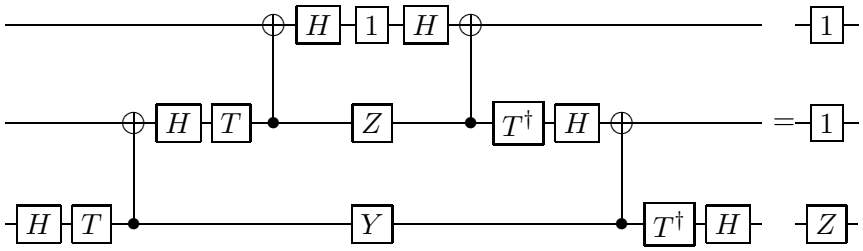

Figura 2.13: *Tercera etapa del circuito de cambio de base.*

Por lo tanto, el circuito al que entra un autoestado del estabilizador G y sale un autoestado del grupo estabilizador de operadores Z es el ilustrado en la figura 2.14.

2.6. Conclusiones parciales

Se presentaron en este capítulo los conjuntos de bases mutuamente no sesgadas. Dichas bases surgen como una generalización de los observables conjugados en sistemas continuos, como la posición y el momento, al caso de sistemas discretos. Resultan de importancia, entre otros motivos, porque permiten definir un espacio de fases, como se verá en el capítulo 3, y sirven

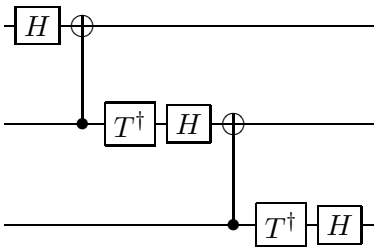

Figura 2.14: *Circuito de cambio de base. Convierte un autoestado del grupo estabilizador G en uno del grupo estabilizado por los operadores Z.*

para medir la fidelidad de un circuito cuántico, como se mostrará en el capítulo 5.

Se mostró, además, que los conjuntos de bases mutuamente no sesgadas pueden obtenerse mediante particiones de los operadores de Pauli generalizados en conjuntos abelianos, y que existe una relación de uno a uno entre dichas particiones y conjuntos de matrices simétricas S_i tales que $\det S_i = 1$ y $\det(S_i + S_j) = 1 - \delta_{ij}$, para todo i y para todo j.

Por último, se obtuvo un algoritmo novedoso que permite a una computadora clásica construir un circuito de cambio de base entre dos bases no sesgadas. Dicha construcción se realiza a partir de los estabilizadores correspondientes a cada una de las dos bases, y requiere del orden n^3 operaciones clásicas para determinar el circuito cuántico en cuestión. El circuito cuántico de cambio de base así generado emplea del orden de n^2 rotaciones de un qubit y compuertas $\mathrm{C-Not}$.

Capítulo 3

Las funciones de Wigner

El estado de un sistema cuántico, ya sea puro o mixto, puede representarse mediante su operador densidad ρ. Sin embargo, existe un formalismo que permite estudiar un sistema a partir de un símil de distribución de probabilidad en el espacio de fases que resulta de gran utilidad en distintos problemas de procesamiento cuántico de la información. Dicha pseudodistribución de probabilidad se denomina *función de Wigner*.

Existen distintos tipos de funciones de Wigner. El primero fue el presentado por Wigner en 1932 [25], en el que introducía la distribución que hoy lleva su nombre para sistemas cuyo espacio de Hilbert de estados tiene dimensión infinita (en particular, sistemas continuos cuyo espacio de fases se encuentra definido por las variables de posición y momento).

Asimismo, hay distintas definiciones no equivalentes de la función de Wigner para sistemas con espacio de estados de dimensión finita d. Una de ellas se vale de un espacio de fases de $2d \times 2d$ [26][27][10][13]. Otra, que será estudiada en detalle en el presente capítulo, utiliza cuerpos finitos para definir un espacio de fases de $d \times d$ para sistemas de dimensión $d = p^n$, con p primo [14][12][6][2][23].

En este capítulo se presenta la función de Wigner definida sobre una grilla de $d \times d$ para sistemas de dimensión $d = p^n$. Se presenta, además, un conteo original de la cantidad de funciones de Wigner no equivalentes de este tipo que pueden definirse.

Los resultados aquí mostrados resultarán de utilidad en los capítulos posteriores. En especial para la obtención de algunos resultados relacionados con la fidelidad de un algoritmo cuántico, en el capítulo 5.

3.1. La función de Wigner para sistemas continuos

La primera de las distintas funciones de Wigner antes mencionadas es la correspondiente a una partícula que se mueve en una dimensión. Este sistema, cuyo espacio de Hilbert de estados es continuo, puede representarse mediante un espacio de fases continuo cuyas coordenadas son la posición de la partícula Q y su momento P.

La función de Wigner definida sobre ese espacio de fases debe poseer, fundamentalmente, la propiedad de dar, al ser integrada sobre la recta $aQ + bP = c$, la probabilidad de medir el valor c al observable $aQ + bP$. Es en ese sentido que se dice que *la función de Wigner se comporta de manera similar a una distribución de probabilidad*, siendo la principal diferencia con dichas distribuciones la cualidad que tiene la función de Wigner de poder tomar valores negativos, como se verá a continuación.

Se define la función de Wigner en un punto del espacio de fases como:

$$W(q,p) = \frac{1}{\pi\hbar}\int_{-\infty}^{+\infty} \langle q-x|\,\rho\,|q+x\rangle\, e^{\frac{i2px}{\hbar}}\,dx \tag{3.1}$$

A partir de dicha definición, se pueden verificar varias propiedades fundamentales requeridas.

3.1.1. Propiedades de las funciones de Wigner continuas

1. La función de Wigner es real.

2. El producto interno entre dos estados puede computarse a partir de sus respectivas funciones de Wigner mediante la siguiente fórmula:

$$\mathrm{Tr}\,(\rho_1\rho_2) = 2\pi\hbar\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} W_1(q,p)\,W_2(q,p)\,dqdp \tag{3.2}$$

3. Si se integra la función de Wigner sobre la franja delimitada por las rectas $aQ + bP = c$ y $aQ + bP = d$, se obtiene la probabilidad de obtener un resultado comprendido entre c y d al medir el observable $aQ + bP$.

Es interesante, y resultará más aún para el caso discreto, reescribir la expresión (3.1) de la forma:

$$W(q,p) = \mathrm{Tr}\,(\rho A(q,p)) \tag{3.3}$$

donde los operadores $A(q,p)$ se denominan operadores de punto, y están dados por

$$A(q,p) = \frac{1}{\pi\hbar}\int_{-\infty}^{\infty} |q+x\rangle\langle q-x| \, e^{\frac{i2px}{\hbar}} dx \tag{3.4}$$

De ésta forma, el valor de la función de Wigner en un punto dado queda asociado al valor medio del operador de punto correspondiente. Además, los operadores de punto poseen las siguientes propiedades:

1. Son hermíticos. Es decir, $A(q,p) = A^{\dagger}(q,p)$. De aquí se desprende inmediatamente que la función de Wigner es real, puesto que es el valor medio de un operador hermítico.

2. Vale que $\mathrm{Tr}\left(A(q,p)\right) = \frac{1}{2\pi\hbar}$.

3. Son ortogonales en el producto interno de Schmidt:

$$\mathrm{Tr}\left(A(q,p)\, A\left(q',p'\right)\right) = \begin{cases} \frac{1}{2\pi\hbar} & p = p', q = q' \\ \\ 0 & \text{Otro caso} \end{cases} \tag{3.5}$$

4. Son una base completa del espacio de operadores hermíticos. Cumplen la relación de completitud:

$$1 = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} A(q,p)\, dq\, dp \tag{3.6}$$

Es posible, a partir de las propiedades antes enunciadas, mostrar que, así como puede calcularse la función de Wigner a partir de la matriz densidad como se hace en (3.3), puede calcularse la matriz densidad a partir de la función de Wigner:

$$\rho = 2\pi\hbar\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} W(q,p)\, A(q,p)\; dq\, dp \tag{3.7}$$

Asímismo, teniendo en cuenta que los operadores de traslación en posición y momento están definidos como

$$T(q,p) = e^{\left(-\frac{i}{\hbar}(qP-pQ)\right)} = e^{-\frac{iqP}{\hbar}} e^{-\frac{ipQ}{\hbar}} e^{-\frac{ipq}{2\hbar}} \tag{3.8}$$

resulta conveniente escribir los operadores de punto en término del operador de paridad o reflexión R, definido como $R|q\rangle = |-q\rangle$ y dichos operadores, en la forma:

$$A(q,p) = \frac{1}{\pi\hbar} T(q,p)\, RT^{\dagger}(q,p) \tag{3.9}$$

Esto es, los operadores de punto son traslaciones en momento y posición del operador de reflexión. Dicha relación, en tanto que $A(0,0) = \frac{1}{\pi\hbar}R$, muestra que la función de Wigner es covariante frente a traslaciones; trasladar un estado en el espacio de Hilbert es equivalente a realizar una traslación en el espacio de fases, y resulta de suma importancia en lo que a la interpretación de la función de Wigner respecta.

3.2. La función de Wigner de $d \times d$ para sistemas de dimensión 2^n

Un tipo de generalización de las funciones de Wigner continuas a espacios de Hilbert de dimensión finita surge a partir de la generalización directa del espacio de fases y algunas de sus propiedades geométricas. Se debe definir sobre una grilla discreta la noción de línea, para luego asociar a cada línea un proyector adecuado sobre el espacio de Hilbert y, de esta forma, asignando valores correspondientes a cada punto de la grilla, conservar la propiedad de la función de Wigner de dar, al integrar sobre una línea, la probabilidad de obtener un resultado dado en una medición correspondiente a un conjunto de rectas paralelas.

En primer término, es menester definir adecuadamente el espacio de fases, la grilla sobre la que se definirá la función de Wigner. Resulta natural, cuando el sistema tiene dimensión finita d, definir una grilla de $d \times d$ puntos, etiquetados en cada eje por valores de q y p entre 0 y $d-1$.

El problema surge a la hora de definir la noción de línea sobre esa grilla, junto con la idea de paralelismo. La generalización del caso continuo parece ser directa, pero no lo es tanto. Uno estaría tentado a definir las líneas como los conjuntos de puntos (q,p) que satisfacen que $aq + bp = c$, con $a, b, c \in \mathbb{Z}$ fijos, y utilizando aritmética módulo d. Sin embargo, salta a la vista que no todas las líneas así definidas tienen igual cantidad de puntos. Se puede ver, por ejemplo, que en dimensión $d = 4$ la línea $q + 2p = 1$ tiene 4 puntos, y $2q + 2p = 0$ tiene 8.

Sin embargo, éste problema da una idea acerca de un camino a seguir para sortear las dificultades. Es importante notar que, si la dimensión del sistema es $d = p$, con p un número primo, entonces todas las líneas definidas mediante el uso de aritmética módulo d tendrán d puntos. Más aún, al igual que en el caso continuo se respetará la noción de paralelismo. Las líneas $aq + bp = c_1$ y $aq + bp = c_2$ no tendrán ningún punto en común, a menos que $c_1 = c_2$; es decir, son paralelas. No sólo eso sino que, adicionalmente, se respetará la noción continua y euclidiana que dice que dos líneas no paralelas

se cruzarán en exactamente un punto.

En este esquema, y en dimensión prima, habrá $d + 1$ conjuntos de d líneas paralelas. Cada conjunto se denomina *estriación*. En la figura 3.1 se muestran las estriaciones para un sistema de dimensión 3.

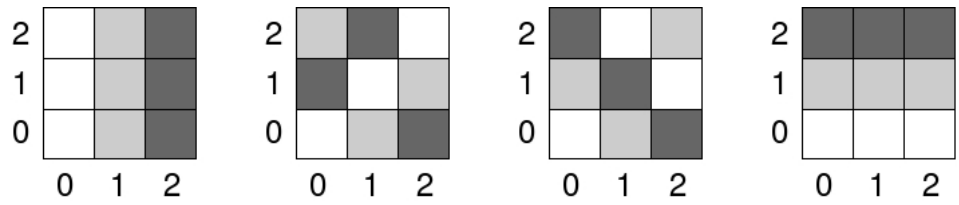

Figura 3.1: *Los cuatro conjuntos de líneas paralelas (estriaciones) en el espacio de fases de un sistema de dimensión* 3.

Que la suma y el producto módulo d en dimensión prima den estriaciones cuyo comportamiento coincide con el de las líneas definidas en el caso continuo, es debido a que el producto y la suma módulo d son operaciones cerradas en el conjunto de números enteros entre 0 y $d - 1$ e invertibles. En otras palabras, los números enteros entre 0 y $d - 1$ forman un cuerpo finito y es debido a ello que las líneas tienen las mismas propiedades que las definidas en el caso continuo:

1. Dados dos puntos distintos existe una única línea que pasa por ambos.
2. Dos líneas son paralelas o se cortan en exactamente un punto.
3. Dado un punto y una estriación, existe una única línea de esa estriación que pasa por dicho punto.
4. Todas las líneas tienen la misma cantidad de puntos, y dicha cantidad es igual a d.

Al trabajar en una dimensión d compuesta, ocurre que no todos los números tienen inverso multiplicativo módulo d, por lo que no todas las líneas tienen igual cantidad de puntos. Sin embargo, si la dimensión es una potencia de un primo, es decir $d = p^n$, entonces se pueden construir estriaciones con las propiedades deseadas apelando a la teoría de los cuerpos finitos, o cuerpos de Galois.

3.2.1. Los cuerpos finitos

De acuerdo con la teoría de Galois, existe un cuerpo finito con d elementos si y sólo si d es un primo o una potencia de un primo; es decir, $d = p^n$.

Más aún, puede probarse que todos los cuerpos finitos de igual dimensión son isomorfos. Además, puesto que en los cuerpos finitos existe el inverso multiplicativo, constituyen la teoría matemática ideal para generalizar el espacio de fases anteriormente esbozado.

Los números enteros del 0 al $d-1$, junto con la suma y el producto módulo d conforman, cuando d es primo, un cuerpo finito; el cuerpo finito mencionado más arriba llamado $GF(d)$. En cambio, si la dimensión es $d = p^n$, con p primo y n entero, también puede construirse el cuerpo $GF(d)$, pero sus elementos no son números enteros sino polinomios con coeficientes en $GF(p)$.

El primer paso para construir el cuerpo finito consiste en encontrar un polinomio de grado n irreducible con coeficientes en $GF(p)$, y que no divida a ningún polinomio de la forma $1 + x^m$, con $m \in \mathbb{N}, m < d-1$. Dicho polinomio $P(x)$ se denomina *polinomio primitivo* del cuerpo $GF(d)$. Luego se considera un elemento ω tal que $P(\omega) = 0$, que no es necesario encontrar explícitamente, y al que se llamará *elemento generador*. Finalmente, el cuerpo $GF(d)$ estará dado por el conjunto $\left\{0, 1, \omega, ..., \omega^{d-2}\right\}$. Es decir, por ω y todas sus potencias.

Una propiedad importante del elemento generador del cuerpo $GF(d)$ es que sus potencias son cíclicas; es decir, $\omega^{d-1} = 1$. De allí que se haya mencionado que *todas* las potencias de ω conforman el cuerpo finito. Además, puesto que todos los elementos del cuerpo están dados por ω y sus potencias, y que por definición $P(\omega) = 0$, cualquier elemento x del cuerpo podrá escribirse como:

$$x = \sum_{j=0}^{n-1} x_j \omega^j \tag{3.10}$$

donde los coeficientes x_j son números enteros comprendidos entre 0 y $p-1$, y todas las operaciones aritméticas entre los números enteros se realizan módulo p. Es importante notar que el cuerpo finito, a partir de la expansión (3.10) tiene exactamente d elementos, como era requerido.

De ésta forma, y para definir con mayor precisión el cuerpo finito, se pueden definir adecuadamente la suma y el producto de elementos del cuerpo. La suma de dos elementos del cuerpo corresponderá a la suma de los respectivos coeficientes de los elementos escritos en la forma (3.10), realizada módulo p. El producto, en tanto, corresponderá al producto de los polinomios en ω definidos en (3.10), donde los coeficientes serán computados módulo p y las potencias de ω serán reducidas a potencias de ω con exponentes entre 0 y $n-1$ mediante el polinomio primitivo.

Se denominará al desarrollo de la ecuación (3.10) expansión en la base canónica, siendo la base canónica $B_\omega = \left\{\epsilon_0 = \omega^0 = 1, ..., \epsilon_{n-1} = \omega^{n-1}\right\}$. Además, se define la base dual $\tilde{B_\omega} = \{\tilde{\epsilon_0}, ..., \tilde{\epsilon_{n-1}}\}$ como aquella tal que $\mathrm{tr}\left(\epsilon_i \tilde{\epsilon_j}\right) = \delta_i j$, donde debe entenderse que la traza es tomada sobre $GF\left(d\right)$, y su resultado en un número entero entre 0 y $p-1$.

Ejemplo - El cuerpo $GF\left(8\right)$

Para la construcción del cuerpo $GF\left(8\right) = GF\left(2^3\right)$, es requisito encontrar, en primer lugar, un polinomio primitivo. Dicho polinomio $P\left(x\right)$ debe tener, como se mencionó anteriormente, las siguientes propiedades:

1. Poseer coeficientes en $GF\left(2\right)$. Es decir, 0 o 1.
2. Ser irreducible.
3. No dividir a ningún polinomio de la forma $1 + x^m$, con $m < 2^3 - 1$.

Puede verse que existen dos polinomios que verifican las tres propiedades, por lo que debe elegirse uno. Uno de ellos es $P\left(x\right) = 1 + x + x^3$. Se considera ahora un elemento ω tal que $P\left(\omega\right) = 0$. Es importante notar que no es necesario encontrar explícitamente dicho elemento, sino que basta con saber que existe dentro del cuerpo finito que se va a construir.

Dado ese elemento, es posible escribir todos los elementos del cuerpo en la forma (3.10), usando que ω es raíz de $P\left(x\right)$; es decir, utilizando que $-\omega^3 = \omega^3 = 1 + \omega$, donde se invirtió el signo de ω^3 utilizando las propiedades de la suma en $GF\left(2\right)$. Dado esto, es posible construir los ocho elementos del cuerpo, y se ve que el noveno elemento es nuevamente la identidad:

- 0
- $\omega^0 = 1$
- $\omega^1 = \omega$
- $\omega^2 = \omega^2$
- $\omega^3 = 1 + \omega$
- $\omega^4 = \omega\omega^3 = \omega + \omega^2$
- $\omega^5 = \omega\omega^4 = \omega^2 + \omega^3 = \omega^2 + \omega + 1$
- $\omega^6 = \omega\omega^5 = \omega^3 + \omega^2 + \omega = \omega^2 + 1$
- Comienzan a repetirse cíclicamente: $\omega^7 = \omega\omega^6 = \omega^3 + \omega = 1 = \omega^0$

Puede verse, asímismo, que todos los elementos no nulos son combinaciones lineales en $GF\left(2\right)$ de los elementos 1, ω y ω^2. No sólo eso, sino que toda combinación lineal de dichos elementos es un elemento del cuerpo. Es por ello que cada elemento del cuerpo puede notarse como los coeficientes de la expansión en la base $\left\{1, \omega, \omega^2\right\}$, quedando en éste caso representado cada elemento por un vector fila binario de dimensión 3.

Representación matricial del elemento generador del cuerpo finito

Los elementos del cuerpo finito pueden representarse como vectores fila binarios de n componentes. Además, los elementos del cuerpo finito tienen un orden establecido, según la potencia de ω. Por otra parte, puesto que todos los elementos del grupo son combinaciones lineales de n elementos, y que la regla para pasar de uno al siguiente en aquel orden es lineal (el siguiente, en dicho orden, de una suma es igual a la suma de los siguientes), existe una matriz M que recorre los vectores correspondientes a los elementos del cuerpo finito en el mismo orden en el que se encuentran como potencias del elemento generador. Dicha matriz se denomina matriz compañera del polinomio característico.

Volviendo al ejemplo de $GF\left(8\right)$, puede escribirse el desarrollo en la base canónica de los elementos del cuerpo como:

$$GF\left(8\right) = \left\{ \begin{array}{c} \left(0 \quad 0 \quad 0\right), \left(1 \quad 0 \quad 0\right), \left(0 \quad 1 \quad 0\right), \left(0 \quad 0 \quad 1\right), \\ \left(1 \quad 1 \quad 0\right), \left(0 \quad 1 \quad 1\right), \left(1 \quad 1 \quad 1\right), \left(1 \quad 0 \quad 1\right) \end{array} \right\} \tag{3.11}$$

Puede verse que, a excepción del elemento nulo, la matriz

$$M = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \tag{3.12}$$

recorre los elementos del cuerpo. Esto es, al ser multiplicada por izquierda por un vector correspondiente a algún elemento del cuerpo finito, el resultado del producto es el elemento siguiente, y dicho producto es cíclico. Esto puede resumirse en la siguiente identificación entre elementos del cuerpo y vectores:

$$\omega^k \longrightarrow \left(1 \quad 0 \quad 0\right) M^k \tag{3.13}$$

Vale notar que, para una cantidad de qubits arbitraria, si el polinomio primitivo está dado por $P\left(x\right) = r_0 + r_1 x + r_2 x^2 + ... + r_{n-1} x^{n-1} + x^n$, entonces la matriz compañera será:

$$M = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & & & & & 1 \\ r_0 & r_1 & r_2 & \cdots & & r_{n-1} \end{pmatrix} \tag{3.14}$$

Dicha matriz tiene la propiedad de recuperar el polinomio primitivo, en tanto que $P(x) = \det(M - 1x)$. Esto, y el teorema de Hamilton-Cayley, muestran que $P(M) = 0$. Por lo tanto M *es* un elemento generador del cuerpo finito en representación matricial.

La matriz M, como representación matricial del cuerpo finito, posee la propiedad de ser autopotente, al igual que el elemento ω. Es decir, $M^{2^n} = M$.

Además, puesto que las potencias de M forman un grupo cíclico, y siendo que todos los grupos cíclicos son isomorfos, cualquier matriz binaria M tal que $M^{2^n} = M$ y $M^k \neq M$ con $1 < k < 2^n$, servirá de elemento generador del cuerpo finito.

3.2.2. La estructura del espacio de fases

Etiquetando los ejes con los elementos del cuerpo finito y definiendo las líneas como aquellos puntos (q, p) que verifican que $aq + bp = c$, pero con $a, b, c, q, p \in GF(d)$, se obtienen líneas que, si bien su distribución sobre el espacio no evoca a las líneas módulo d, poseen las siguientes propiedades:

1. Todas las líneas poseen d puntos.
2. Las líneas $aq + bp = c_1$ y $aq + bp = c_2$ con $c_1 \neq c_2$ no poseen puntos en común. Dichas líneas se denominan paralelas.
3. Las líneas que no son paralelas tiene un único punto en común.

Puede verse que existen $d+1$ estriaciones (La ecuación de la línea puede llevarse a la forma $q + bp = c$. De ésta forma hay d estriaciones, una para cada posible valor de b. Además, se tiene la estriación $p = c$. De ahí las $d + 1$ estriaciones.), cada una compuesta por d líneas paralelas, como era requerido. Se notará $\lambda^{(\kappa)}_{(q,p)}$ a la línea de la estriación κ que pasa por el punto (q, p). Asímismo, se llamrá *rayo* de la estriación κ a la línea $\lambda^{(\kappa)}_{(0,0)}$.

Los rayos tendrán importancia por distintos motivos. En primer lugar, puesto que los rayos correspondientes a todas las estriaciones pasan por el origen, y que dados dos puntos del espacio de fases existe una única línea que pasa por ambos, todo punto del espacio de fases será atravesado por

exactamente un rayo, a excepción del origen que estará atravesado por todos los rayos. Más aún, todas las líneas de una dada estriación podrán construirse a partir de traslaciones del rayo correspondiente, y serán invariantes frente a las mismas traslaciones que dicho rayo. Por otra parte, como se ve en la figura 3.2, donde se ilustran los rayos para un sistema de dimensión 8, estos rayos sí poseen una representación geométrica sencilla.

ω^6	9	3	4	5	6	7	8	2
ω^5	9	4	5	6	7	8	2	3
ω^4	9	5	6	7	8	2	3	4
ω^3	9	6	7	8	2	3	4	5
ω^2	9	7	8	2	3	4	5	6
ω	9	8	2	3	4	5	6	7
1	9	2	3	4	5	6	7	8
0		1	1	1	1	1	1	1
	0	1	ω	ω^2	ω^3	ω^4	ω^5	ω^6

Figura 3.2: *Los nueve rayos correspondientes a un espacio de fases de dimensión 8. Los puntos correspondientes a cada rayo se identifican con un número, correspondiendo cada número a una estriación. El origen es el único punto que pertenece a todos los rayos. Puede verse, asímismo, su sencilla distribución geométrica.*

3.2.3. La función de Wigner en dimensión $d = p^n$.

Se buscará, dada la estructura del espacio de fases descripta anteriormente, una función de Wigner que posea propiedades similares a aquellas establecidas para el caso continuo:

- La función de Wigner $W(q,p)$ es real.
- Puede computarse el producto interno entre dos estados ρ_1 y ρ_2 a partir de sus respectivas funciones de Wigner como:

$$\mathrm{Tr}\left(\rho_1\rho_2\right) \propto \sum_{q,p} W_1(q,p)\, W_2(q,p) \tag{3.15}$$

- La función de Wigner debe cumplir el rol de pseudodistribución de probabilidad; es decir, la suma de dicha función sobre los puntos pertenecientes a una dada línea $\lambda^{(\kappa)}_{(q,p)}$ debe ser igual a la probabilidad p_λ de obtener, al realizar la medición asociada al observable κ, el valor correspondiente a dicha línea. Es decir, dado el proyector $P(\lambda)$

asociado a la línea λ, tiene que cumplirse que:

$$\sum_{(p,q)\in\lambda} W(\alpha) = \mathrm{Tr}\left(\rho P(\lambda)\right) = p_\lambda \tag{3.16}$$

Es conveniente comenzar por un estado cuya función de Wigner pueda determinarse a partir de las propiedades anteriores, aún sin definir con precisión dicha función. Ese estado es el totalmente mixto, $\rho = 1/d$. Por la ecuación (3.16), es necesario que la suma sobre cualquier línea sea, para un estado máximamente mixto, $1/d$. Además, para que esto se verifique para cualquier línea de cualquier estriación, y debido a la estructura del espacio de fases, puede probarse que la única solución es que la función de Wigner sea igual a $1/d^2$ en todos los puntos.

De la misma forma, tomando $\rho = 1/d$, y utilizando la ecuación (3.15), se obtiene:

$$\mathrm{Tr}\left(\rho^2\right) = \frac{1}{d} \propto \sum_{q,p} \frac{1}{d^4} = \frac{1}{d^2} \tag{3.17}$$

con lo que la proporcionalidad de (3.15) se convierte en una igualdad mediante el factor d correspondiente:

$$\mathrm{Tr}\left(\rho_1\rho_2\right) = d\sum_{q,p} W_1(q,p)\, W_2(q,p) \tag{3.18}$$

Además, mediante la ecuación (3.18) aplicada al estado máximamente mixto y otro operador densidad ρ arbitrario, y recordando que la traza de los operadores densidad es 1, se obtiene la condición de normalización correspondiente a una pseudodistribución de probabilidad, como es la función de Wigner:

$$\sum_{q,p} W(q,p) = 1 \tag{3.19}$$

Por último, es importante notar que puede obtenerse la función de Wigner en un punto mediante mediciones de los observables correspondientes a todas las estriaciones. Si se quiere obtener el valor de la función de Wigner en un punto (q,p) dado, y se suma sobre todas las estriaciones la probabilidad de obtener el resultado correspondiente a la línea que pasa por (q,p), se estará sumando una vez el valor de la función de Wigner en todos los puntos, a excepción del punto (q,p), cuya función de Wigner estará sumada $d+1$ veces. Por lo tanto, y dada la condición de normalización, si se resta 1 a la suma de todas las probabilidades mencionadas, se obtendrá la función de Wigner:

$$W(q,p) = \frac{1}{d}\left[-1 + \sum_{\kappa} \mathrm{Tr}\left(\rho P\left(\lambda^{(\kappa)}_{(q,p)}\right)\right)\right] \tag{3.20}$$

donde $P\left(\lambda^{(\kappa)}_{(q,p)}\right)$ es el proyector asociado a la línea de la estriación κ que pasa por el punto (q,p).

Esto muestra que, en principio, no será simple la medición de la función de Wigner en un punto, en tanto que implica medir los observables correspondientes a todas las estriaciones, es decir, una cantidad de observables exponencial en el número de qubits.

3.2.4. La covariancia frente a las traslaciones

Al igual que en el caso continuo, una de las propiedades fundamentales que relaciona el espacio de fases con el de Hilbert es la covariancia frente a las traslaciones; es decir, las traslaciones en el espacio de Hilbert tienen que tener sus contrapartidas en el espacio de fases. Resulta necesario, por lo tanto, definir las traslaciones en ambos espacios para luego establecer una conexión entre ambas.

Para asociar las traslaciones en el espacio de fases con traslaciones en el espacio de Hilbert, es necesario imponer una condición sobre los proyectores correspondientes a cada línea. Se pedirá que el proyector de una línea λ', que es una cierta traslación de una línea λ en el espacio de fases, corresponda a trasladar en el espacio de Hilbert el proyector asociado a λ. Es decir:

$$P\left(\lambda'\right) = T\left(\vec{q},\vec{p}\right) P\left(\lambda\right) T^{\dagger}\left(\vec{q},\vec{p}\right) \tag{3.21}$$

donde $\lambda' = \mathcal{T}_{(q,p)}\lambda$, y la relación vale para toda línea λ y para todo par (q,p). Se interpretará, además, que q y p son elementos del cuerpo finito, con $\vec{q}$ y $\vec{p}$ vectores asociados a cada uno de esos estados de una forma que se verá más adelante. Además, los operadores $\mathcal{T}\left(q,p\right)$ corresponderán a traslaciones en el espacio de fases, cuya traslación correspondiente en el espacio de Hilbert se notará $T\left(\vec{q},\vec{p}\right)$.

Se definen los operadores de traslación en el espacio de fases $\mathcal{T}_{(q',p')}$ como aquellos que trasladan un punto una cantidad (q',p'). Es decir:

$$\mathcal{T}_{(q',p')}\left(q,p\right) = \left(q+q', p+p'\right) \tag{3.22}$$

Cuando una misma traslación actúa sobre todos los puntos de una línea, se obtiene otra línea perteneciente a la misma estriación. En la figura 3.3 puede verse una línea del espacio de fases $GF\left(8\right)$ antes y después de aplicada

una traslación. En particular, a partir del rayo de una estriación y traslaciones, pueden obtenerse todas las líneas de esa estriación. Y puesto que el rayo es una línea que pasa por el origen, las traslaciones correspondientes para llevar el rayo a una línea dada de su misma estriación serán todas aquellas que la trasladen una cantidad igual a alguno de los puntos pertenecientes a la línea en cuestión.

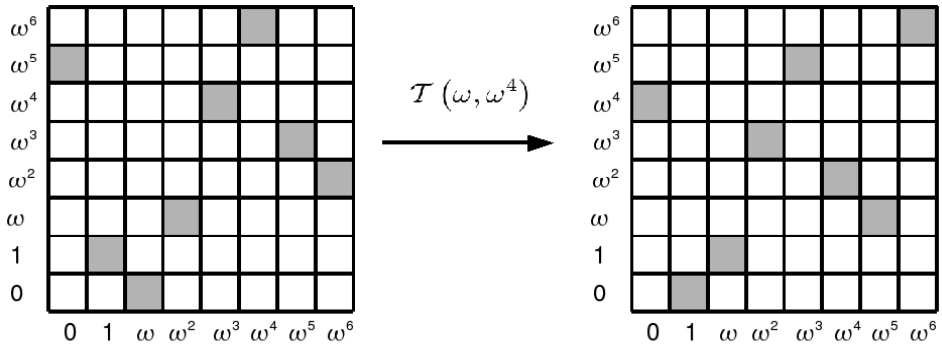

Figura 3.3: *Traslación de la línea $q + \omega^3 p = \omega$, definida mediante el polinomio primitivo $P(x) = 1 + x + x^3$, por el operador $\mathcal{T}\left(\omega, \omega^4\right)$. Puede observarse que, si bien no tienen el aspecto familiar de las líneas definidas módulo 8, ambas rectas poseen igual cantidad de puntos y no poseen puntos en común por ser paralelas.*

Las traslaciones así definidas poseen algunas propiedades análogas al caso continuo y otras particulares del caso discreto. En primer término, la composición de dos traslaciones es otra traslación cuya cantidad trasladada es la suma de ambas:

$$\mathcal{T}_{(q_1,p_1)}\left(\mathcal{T}_{(q_2,p_2)}(q,p)\right) = \mathcal{T}_{(q_1+q_2,p_1+p_2)}(q,p) \tag{3.23}$$

En segundo lugar, cuando la dimensión del sistema es 2^n, puesto que los coeficientes de las expansiones de los elementos del cuerpo se suman módulo 2, la aplicación de una misma traslación dos veces es igual a la identidad.

En éste tipo de sistema, las traslaciones en el espacio de Hilbert se definen, a menos de una fase, como operadores de Pauli generalizados (ver Apéndice B). De ésta forma, una traslación en el espacio de Hilbert estará dada por un operador:

$$T(\vec{q}, \vec{p}) = X^{\vec{q}} Z^{\vec{p}} e^{\frac{\pi i \vec{q}\cdot\vec{p}}{2}} \tag{3.24}$$

Puede verse que el cuadrado de una traslación es la identidad, propiedad que debía verse reflejada por la definición de las traslaciones dadas para el espacio de Hilbert. De igual forma, la composición de dos traslaciones

es una traslación pero, a diferencia de las traslaciones en el espacio de fases, puede ocurrir que aparezca una fase adicional. Esto ocurre porque los operadores de Pauli generalizados pueden conmutar o anticonmutar, y esas anticonmutaciones tendrán particular importancia al ver qué conjunto de traslaciones deja invariante a cada estriación, así como los correspondientes estados asociados a las líneas.

Relación entre estriaciones y conjuntos de bases mutuamente no sesgadas

Cada línea de cada estriación del espacio de fases será invariante frente a cierto conjunto de traslaciones; en particular, frente a aquellas que trasladan un punto del rayo de la estriación correspondiente sobre otro punto del mismo rayo. Dicha invariancia tendrá aparejada, de acuerdo a la covariancia traslacional, una invariancia de algunos estados del espacio de Hilbert frente a ciertas traslaciones. Eso impondrá condiciones sobre los estados líneas que permitirán, como se verá a continuación, relacionar el espacio de fases discreto con las bases mutuamente no sesgadas definidas en el capítulo 2. En efecto, se mostrará que los estados correspondientes a líneas de una estriación son una base, y que las bases correspondientes a distintas estriaciones son no sesgadas.

En primer término, veamos frente a qué operadores son invariantes las líneas de una estriación, mediante la propiedad que se enuncia a continuación:

Propiedad 3.2.1. *Las líneas de una estriación κ son invariantes frente a una traslación $\mathcal{T}_{(q',p')}$ si y sólo si el punto (q',p') pertenece al rayo de la estriación κ.*

Demostración. En primer lugar, se demostrará la primera implicación: si el punto (q',p') pertenece al rayo de la estriación κ, entonces toda línea de dicha estriación es invariante frente a la traslación $\mathcal{T}_{(q',p')}$.

En efecto, la estriación κ corresponde a todas las líneas cuyos puntos son de la forma $aq+bp=c$, con a y b fijos (dependen de κ), y c recorriendo las distintas líneas de la estriación. El rayo de dicha estriación corresponde a la línea con $c=0$. Sea (q',p') un punto del rayo en cuestión, y sea un punto (q,p) perteneciente a la línea $aq+bp=c$, con algún c dado. Se tiene que:

$$\mathcal{T}_{(q',p')}\,(q,p) = \left(q+q', p+p'\right) \tag{3.25}$$

Pero puesto que el punto (q',p') pertenece al rayo, vale que:

$$a\left(q+q'\right)+b\left(p+p'\right)=aq+bp+\left(aq'+bp'\right)=aq+bp=c \tag{3.26}$$

Por lo que la traslación transforma un punto de una línea c en otro de la misma línea c. Es decir, toda línea de la estriación κ en invariante frente a traslaciones en cantidades correspondientes a puntos del rayo κ.

Falta ver la implicación inversa. Sí todas las líneas de κ son invariantes frente a una traslación $\mathcal{T}_{(q',p')}$, entonces (q',p') pertenece al rayo. En efecto, supongamos que la traslación convierte a un punto (p,q) en otro de la misma línea:

$$c=aq+bp=a\left(q+q'\right)+b\left(p+p'\right) \tag{3.27}$$

Por lo que ocurre que $aq'+bp'=0$, y queda demostrada la propiedad. □

Recordando la relación de covariancia (3.21) y la definición de los operadores de traslación en el espacio de Hilbert (3.24), y apelando a la propiedad 3.2.1, se obtiene que el estado asociado a una línea $aq+bp=c$ será invariante frente a los operadores de traslación

$$T\left(\vec{q'},\vec{p'}\right)=X^{\vec{q'}}Z^{\vec{p'}}e^{\frac{\pi i\vec{q'}\cdot\vec{p'}}{2}} \tag{3.28}$$

con $aq'+bp'=0$. Es decir, será autoestado común de un conjunto de $d-1$ operadores de Pauli generalizados. Pero para que sea autoestado común de todos ellos, necesariamente serán conmutativos. Tenemos entonces los siguientes resultados:

- Los estados línea de cada estriación se encuentran estabilizados por $d-1$ operadores de Pauli generalizados.
- Estados correspondientes a estriaciones distintas no poseen ningún estabilizador en común, puesto que los rayos sólo se cruzan en el origen.
- Hay $d+1$ estriaciones.

Por lo tanto, apelando a lo visto en la sección 2.3, los estados línea asociados a cada estriación forman una base del estado de Hilbert, y las bases correspondientes a las diferentes estriaciones son mutuamente no sesgadas.

El hecho de que todos los operadores de traslación del espacio de Hilbert asociados a puntos de un mismo rayo conmuten, impone una condición respecto de la representación del cuerpo finito que se utilizará para indexar cada eje del espacio de fases.

Asociación entre elementos del cuerpo finito y vectores fila binarios

Se debe, por último, asociar los elementos del cuerpo finito con los que se indexan los ejes del espacio de fases con vectores fila binarios que serán los vectores $\vec{q}$ y $\vec{p}$ antes mencionados. Dicha asociación debe conservar la estructura del cuerpo finito, en tanto que si la suma de dos elementos del cuerpo dan otro dado, entonces la suma de sus vectores asociados deben dar el vector asociado a la suma. Esto se debe a que se quiere conseguir que una composición de dos traslaciones en el espacio de fases tenga asociada en el espacio de Hilbert la composición de las dos traslaciones asociadas a las correspondientes traslaciones del espacio de fases; esto es, conservar la covariancia frente a traslaciones. Además, por las razones expuestas anteriormente, los operadores de traslación del espacio de Hilbert que estabilizan a una estriación deben ser conmutativos.

Pueden satisfacerse ambas condiciones con una misma solución. Dada una matriz M generadora del cuerpo finito ($M^{2^n} = M$ y $M^k \neq M$ con $1 < k < 2^n$) y su transpuesta $\tilde{M}$, se pueden construir $d+1$ conjuntos de $d-1$ operadores de Pauli generalizados que conmutan. Dichos conjuntos están dados por:

$$G_{(\vec{b},\vec{a})} = \left\{ T\left(\vec{b}M^j, \vec{a}\tilde{M}^j\right), \quad 0 \leq j \leq d-2 \right\} \tag{3.29}$$

con $\vec{a}$ y $\vec{b}$ vectores binarios de n componentes.

En primer lugar, puede verificarse que los operadores pertenecientes a un mismo conjunto conmutan. En efecto, para ver que esto es así, alcanza con tomar el producto simpléctico entre ambos:

$$\vec{b}M^j M^k \vec{a}^\dagger - \vec{b}M^k M^j \vec{a}^\dagger = \vec{b}M^{j+k}\vec{a}^\dagger - \vec{b}M^{j+k}\vec{a}^\dagger = 0 \tag{3.30}$$

La segunda propiedad buscada, respecto de la estructura del cuerpo, se satisface automáticamente por ser M un elemento generador del cuerpo finito en representación matricial.

La asociación entre elementos del cuerpo finito y vectores para etiquetar los ejes del espacio finito se vuelve trivial:

$$\begin{array}{rclcrcl} q_j & = & \omega^j & \longrightarrow & \vec{q_j} & = & \vec{1}M^j \\ p_j & = & \omega^j & \longrightarrow & \vec{p_j} & = & \vec{1}\tilde{M}^j \end{array} \tag{3.31}$$

donde $\vec{1}$ es un vector binario que posee un 1 en la primera posición y 0 en las demás.

De esta forma se tiene que las traslaciones que dejan invariante una cierta estriación son aquellas que corresponden a traslaciones $T(\vec{q},\vec{p})$, con el punto $(\vec{q},\vec{p})$ ubicado sobre el rayo correspondiente a la estriación en cuestión.

Ejemplo - Espacio de fases de un sistema de 3 qubits

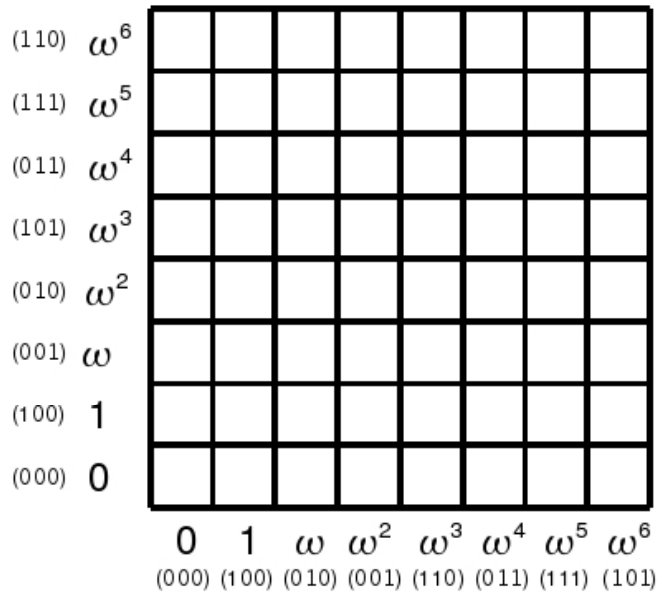

Figura 3.4: *El espacio de fases de un sistema de* 3 *qubits. La coordenada* $\vec{q}$ *es recorrida por la matriz* M*, mientras que la* $\vec{p}$ *es recorrida por* $\tilde{M}$*.*

El espacio de fases para un sistema de tres qubits cuya matriz generadora del cuerpo es la misma dada en el ejemplo (3.12) quedará representado por la grilla ilustrada en la figura 3.4, en la que se observa cada elemento de los ejes representado por ω^j y su respectiva representación vectorial.

Encontrar el grupo estabilizador para cada estriación resulta sencillo a partir de la figura 3.4. Por ejemplo, si resultara de interés encontrar el grupo estabilizador de la estriación cuyo rayo pasa por el punto $(\omega, 1)$, bastaría con recorrer los puntos de dicho rayo (recordando que el rayo está formado por puntos distribuidos sobre una línea oblicua, en el sentido euclidiano) y construir los operadores del grupo estabilizador de la forma que se observa en la tabla 3.1.

Sin embargo, queda claro en el ejemplo que, si bien la elección del elemento generador del cuerpo finito en representación matricial establece el grupo estabilizador asociado a cada estriación, no queda todavía establecido el estado correspondiente a cada línea de la estriación, sino, apenas, la base

Vector $\vec{q}$	Vector $\vec{p}$	Traslación $X^{\vec{q}}Z^{\vec{p}}$
$(0 \quad 1 \quad 0)$	$(1 \quad 0 \quad 0)$	$Z \otimes X \otimes 1$
$(0 \quad 0 \quad 1)$	$(0 \quad 0 \quad 1)$	$1 \otimes 1 \otimes Y$
$(1 \quad 1 \quad 0)$	$(0 \quad 1 \quad 0)$	$X \otimes Y \otimes 1$
$(0 \quad 1 \quad 1)$	$(1 \quad 0 \quad 1)$	$Z \otimes X \otimes Y$
$(1 \quad 1 \quad 1)$	$(0 \quad 1 \quad 1)$	$X \otimes Y \otimes Y$
$(1 \quad 0 \quad 1)$	$(1 \quad 1 \quad 1)$	$Y \otimes Z \otimes Y$
$(1 \quad 0 \quad 0)$	$(1 \quad 1 \quad 0)$	$Y \otimes Z \otimes 1$

Tabla 3.1: *Recorriendo los puntos del rayo correspondiente a una dada estriación y tomando las coordenadas en su representación como vectores binarios, la construcción del grupo estabilizador asociado a la base correspondiente a una estriación resulta trivial.*

asociada a dicha estriación. La elección del estado que corresponde a cada línea, o elección de la *grilla cuántica*, será tratada a continuación, quedando de esa forma concluida la definición de la función de Wigner.

3.2.5. La grilla cuántica

En lo visto anteriormente no fue única la elección del espacio de fases; se eligió arbitrariamente una matriz M con las propiedades deseadas. Sin embargo, dicha decisión no fue única. Existe, además, otro punto en el que se debe hacer una elección. Hemos visto en 3.2.4 como se puede asociar una base, a partir de su grupo estabilizador, con cada estriación del espacio de fases; pero no quedó establecido qué estado de cada base corresponde a cada línea de dicha estriación. Esa asociación entre líneas y estados se denomina grilla cuántica.

Dicha elección no tiene más restricción que la covariancia frente a traslaciones. Por lo tanto, para cada estriación se podrá elegir libremente el estado que corresponde al rayo (simepre y cuando sea un estado de la base asociada a la estriación en cuestión), mientras que los demás estados quedarán asignados a líneas automáticamente, mediante la aplicación de traslaciones al rayo.

Puede verse que existen grillas cuánticas equivalentes entre sí, tales que toda la grilla difiere en una traslación, y otras grillas cuánticas que no son equivalentes entre sí. Veremos a continuación de cuantas maneras no equivalentes pueden definirse las funciones de Wigner y sus respectivas grillas cuánticas.

3.2.6. Cantidad de funciones de Wigner no equivalentes

En ésta sección se realizará un conteo original de las formas no equivalentes de definir la función de Wigner mediante cuerpos finitos. Para ello, es conveniento notar que a lo largo del desarrollo hecho, se tomaron decisiones arbitrarias en tres puntos:

1. La fijación de las bases de operadores X y Z como grupos estabilizadores de la estriación cuyos rayos son horizontal y vertical, respectivamente.

2. La elección de la grilla cuántica.

3. La elección de la matriz M.

El primer punto no será tenido en cuenta. Se estudiarán sólo aquellas funciones de Wigner que verifican ese punto. En cuanto a las demás, pueden obtenerse redefiniendo los operadores X y Z. Luego, multiplicando la cantidad de diferentes elecciones de grilla cuántica por la cantidad de matrices M generadoras del cuerpo finito, se encontrará el número total de definiciones de funciones de Wigner distintas.

Conteo de las grillas cuánticas

Para contar la cantidad de grillas cuánticas, hay que notar que, para cada una de las $d+1$ estriaciones, se puede elegir uno de d estados para colocar en el rayo, y que el resto de la estriación queda, luego, fija por la covariancia traslacional. Por lo tanto hay d^{d+1} grillas distintas. Sin embargo, aquellas que difieren sólo en una traslación, son equivalentes. Puesto que hay d^2-1 traslaciones distintas, hay conjuntos de d^2 grillas cuánticas equivalentes. Por lo tanto hay d^{d-1} grillas cuánticas no equivalentes, para cada matriz M dada.

Conteo de los elementos generadores del cuerpo $GF(2^n)$

En segundo lugar, es necesario realizar el conteo de matrices M distintas que generan el cuerpo finito. Cada matriz M distinta dará lugar a grupos estabilizadores distintos para las estriaciones, por lo que la definición de la función de Wigner será no equivalente para matrices M distintas. La única excepción es que potencias de una matriz M pueden servir como elementos generadores del cuerpo, dando lugar a las mismas bases no sesgadas. Se debe, por lo tanto, tener el cuidado de no considerar como diferentes a dos matrices tales que cada una es potencia de la otra.

Para realizar el conteo, hay que tener en cuenta que el cuerpo finito se puede definir a partir de su base canónica y la regla de generación de elementos ordenados a partir de dicha base. Utilizando la representación como vectores fila de los elementos del cuerpo, basta con tomar una base de los vectores para utilizarla como base canónica, y una regla de generación para, a partir de n elementos consecutivos del cuerpo, generar el siguiente, conservando la estructura cíclica del cuerpo.

La cantidad de formas de elegir una base ordenada del espacio de vectores fila binarios está dada por [28]:

$$\prod_{j=0}^{n-1} \left(2^n - 2^j\right) \tag{3.32}$$

La manera de realizar el conteo es la siguiente. Para construir una base se comienza por elegir el primer vector. La cantidad de formas de elegir el primer vector es $2^n - 1$. El segundo vector de la base, puede ser cualquiera a excepción del ya elegido, es decir, hay $2^n - 2$ vectores posibles. Para los siguientes vectores de la base, se puede tomar cualquier vector que no sea combinación lineal de los ya elegidos. Por lo tanto, el k-ésimo vector de la base se puede seleccionar de $2^n - 2^{k-1}$. De multiplicar los n factores se obtiene la expresión (3.32).

La cantidad de maneras de, a partir de una base, construir el elemento siguiente, es igual al número de polinomios primitivos de grado n sobre $GF(2)$. Esto es porque, como fue expuesto, es el polinomio primitivo el que determina el orden de los elementos escritos en la base canónica. Dicha cantidad, que llamaremos $h(n)$ obedece que [29][30]:

$$h(n) = \frac{\phi\left(2^n - 1\right)}{n} \tag{3.33}$$

donde $\phi(k)$ es la función de Euler, y es igual a la cantidad de números menores que k que son coprimos con k, y se encuentra bien estudiada. Los primeros valores que toma $h(n)$, comenzando por $h(1)$ son: 1, 1, 2, 2, 6, 6, 18, 16, 48, 60, $\cdots$.

Por lo tanto, el número total de matrices M generadoras del cuerpo finito, tales que ninguna es potencia de otra, vendrá dado por el producto entre las formas de elegir una base de la ecuación (3.32), multiplicado por la cantidad de maneras de elegir un polinomio primitivo dada en (3.33). Además, se debe dividir por $2^n - 1$ ya que cualquier rotación cíclica de los vectores del cuerpo tendrá asociada la misma matriz M. De esta forma, la cantidad $b(n)$ de matrices distintas que pueden utilizarse para generar el cuerpo es:

$$b(n) = \frac{\phi(2^n - 1)\prod_{j=0}^{n-1}\left(2^n - 2^j\right)}{n(2^n - 1)} \tag{3.34}$$

Falta, a esta cantidad, descontar las matrices que son potencias de otras y también son generadoras. Para cada matriz hay una cantidad de matrices que son potencias de ella. Dicha cantidad es igual a la cantidad de números coprimos con $2^n - 1$ y menores que $2^n - 1$, puesto que toda potencia distinta de la identidad de una M dada sirve de generadora, a excepción de aquellas que son cíclicas con una potencia menor que 2^n. Las matrices que tienen un ciclo menor son las que corresponden a potencias de M que no son coprimas con $2^n - 1$. Es decir, hay que dividir (3.34) por $\phi(2^n - 1)$. Por lo tanto, la cantidad $B(n)$ de formas no equivalentes de elegir matrices generadoras del cuerpo es:

$$B(n) = \frac{\prod_{j=1}^{n-1}\left(2^n - 2^j\right)}{n} \tag{3.35}$$

Conteo de funciones de Wigner no equivalentes

El número total de funciones de Wigner $G(n)$ que se pueden construir es, entonces, el producto entre la ecuación (3.35) y d^{d-1} correspondiente a las distintas grillas cuánticas posibles. Usando que $d = 2^n$ se obtiene:

$$G(n) = \frac{2^{(n(2^n-1))}\prod_{j=1}^{n-1}\left(2^n - 2^j\right)}{n} \tag{3.36}$$

Dejando de lado lo mencionado acerca de dejar los grupos estabilizadores de las X y de las Z en los ejes horizontal y vertical respectivamente, esa es la cantidad total de funciones de Wigner no equivalentes que pueden definirse.

El crecimiento de esta función, teniendo en cuenta que las d^{d-1} posibles grillas cuánticas crecen con el número de qubits de una manera superior a cualquier exponencial, también será mayor que una exponencial.

3.2.7. Los operadores de punto

Luego de elegir la matriz M y la grilla cuántica, quedan determinados los proyectores asociados a cada línea y, mediante la ecuación (3.20), queda completamente definida la función de Wigner.

Dicha función de Wigner puede, de la misma forma que en el caso continuo, definirse como el valor medio de un operador de punto:

$$W(\vec{q}, \vec{p}) = \mathrm{Tr}\left(\rho A(\vec{q}, \vec{p})\right) \tag{3.37}$$

$$A\left(\vec{q},\vec{p}\right)=\frac{1}{d}\left[-1+\sum_{\kappa}P\left(\lambda_{\left(\vec{q},\vec{p}\right)}^{(\kappa)}\right)\right]=T\left(\vec{q},\vec{p}\right)A\left(0,0\right)T^{\dagger}\left(\vec{q},\vec{p}\right) \tag{3.38}$$

Vale notar que, puesto que ya se estableció el estado de Hilbert correspondiente a cada línea, queda también establecido el proyector asociado a dicha línea, como aquel proyector sobre el estado correspondiente.

También puede verse a partir de la ecuación (3.38), que puesto que la función de Wigner tiene, dentro de los operadores de punto, una suma sobre proyectores de todas las estriaciones, en principio no será simple medir dicha función eficientemente. En efecto, sería necesario, en principio, medir en 2^n+1 bases distintas.

Los operadores de punto poseen propiedades análogas a las de los operadores de punto para sistemas continuos. En primer lugar, vale que tienen traza $1/d$. Además, los operadores de punto forman una base de los operadores hermíticos y, si se permite toamr combinaciones lineales complejas, de los operadores lineales.

Además, son ortogonales en el producto interno de operadores:

$$\mathrm{Tr}\left(A\left(\vec{q},\vec{p}\right)A\left(\vec{q}',\vec{p}'\right)\right)=\frac{1}{d}\delta_{\vec{q},\vec{q}'}\delta_{\vec{p},\vec{p}'} \tag{3.39}$$

Puesto que forman una base ortogonal de los operadores hermíticos, se puede, en particular, escribir al operador densidad ρ como combinación lineal de operadores de punto. El coeficiente de la expansión es proporcional a la función de Wigner definida en (3.37):

$$\rho=d\sum_{\vec{q},\vec{p}}W\left(\vec{q},\vec{p}\right)A\left(\vec{q},\vec{p}\right) \tag{3.40}$$

3.3. Conclusiones parciales

En éste capítulo se presentaron las funciones de Wigner discretas, junto con algunas propiedades de las mismas.

Se encontró, además, una nueva manera de contar las distintas funciones de Wigner no equivalentes que pueden construirse.

Por otra parte, se mostró que las bases asociadas a las distintas estriaciones son mutuamente no sesgadas. Esto marca una íntima relación entre los conjuntos de bases mutuamente no sesgadas y los espacios de fases discretos. En particular, surge la pregunta acerca de si todo conjunto de bases mutuamente no sesgadas sirve para definir un espacio de fases o no. Dicha

pregunta será estudiada en el capítulo siguiente, donde se mostrará que existen conjuntos de bases mutuamente no sesgadas que *no* sirven para construir funciones de Wigner consistentes con la covariancia traslacional. Además, se presentarán algunos problemas abiertos en lo que respecta a los conjuntos de bases mutuamente no sesgadas.

Ante la pregunta acerca de si es necesario realizar tomografía completa del estado para determinar la función de Wigner en un punto, la respuesta es negativa. Puesto que los operadores de punto son hermíticos, podría medirse en la base de autoestados de uno para la determinación de la función en el punto en cuestión. Sin embargo, nada dice esto acerca de la eficiencia de dicha medición.

Al respecto de la medición eficiente de la función de Wigner, existe una definición que sí se puede medir eficientemente. Dicha definición, brevemente introducida en el Apéndice C, es medible eficientemente por ser sus operadores de punto proporcionales a un operador unitario. Sin embargo, en la función de Wigner aquí presentada no ocurre lo mismo. En principio, debido a la definición de los operadores de punto (3.38), sería necesario medir en todas las estriaciones para determinar el valor de la función de Wigner. Pero eso no sólo es ineficiente (se requiere una cantidad exponencial en el número de qubits de mediciones), sino que es equivalente a realizar tomografía completa del estado. Dos enfoques que podrían intentarse en trabajos futuros con el fin de medir la función de Wigner discreta definida mediante cuerpos finitos son:

- Factorización de los operadores de punto en expresiones eficientemente medibles.
- Implementación eficiente, de ser posible, de operadores de cambio de base entre la base de autoestados de los operadores de punto (simepre existe, por ser hermíticos) y la base computacional.

Capítulo 4

Bases no sesgadas y funciones de Wigner

Como fue expuesto en el capítulo 3, la función de Wigner discreta definida en una grilla de $d \times d$, con $d = p^n$ y p un número primo, induce un conjunto de $d+1$ bases mutuamente no sesgadas, estando cada una asociada a los estados linea de cada estriación del espacio de fases.

Por otra parte, en el capítulo 2 mostramos que todos los conjuntos de bases mutuamente no sesgadas pueden obtenerse a partir de conjuntos de matrices binerias simétricas $\{S_1, \cdots, S_k\}$ tales que $\det S_i = 1$ y $\det(S_i - S_j) = 1 - \delta_{ij}$. Surge naturalmente la pregunta: ¿Es posible asociar todo conjunto de bases mutuamente no sesgadas con el correspondiente a las $d+1$ estriaciones de un espacio de fases? En éste capítulo motraremos que la respuesta a esta pregunta es negativa.

Con dicho fin, se comenzará por encontrar la relación entre las bases inducidas por una matriz generadora del cuerpo finito $GF(d)$ y aquellas generadas por conjuntos de matrices simétricas binarias descriptas en la sección 2.4, mostrándose una condición necesaria sobre las matrices binarias simétricas que corresponden a espacios de fases con covariancia traslacional.

En segundo término, se verá que existen conjuntos de bases mutuamente no sesgadas que no pueden ser distribuidas sobre un espacio de fases con covariancia traslacional. Esto se realizará encontrando algún conjunto de bases mutuamente no sesgadas cuyas matrices bianrias simétricas asociadas violan la condición necesaria antes mencionada.

Además, mediante una búsqueda exhaustiva de conjuntos de bases mutuamente no sesgadas y matrices generadoras del cuerpo finito, se encontrará que existe una gran cantidad de conjuntos de bases mutuamente no sesgadas que no corresponden a ningún espacio de fases con covariancia

traslacional.

Por último se hará un breve comentario sobre problemas abiertos relacionados con cuerpos finitos y bases mutuamente no sesgadas.

4.1. Bases mutuamente no sesgadas y cuerpos finitos

Hemos visto que un elemento generador M del cuerpo finito $GF(d)$ genera $d+1$ bases mutuamente no sesgadas. Además, cada conjunto de $d+1$ bases mutuamente no sesgadas tiene asociado un conjunto de matrices simétricas binarias $\{S_1, \cdots, S_{d-1}\}$, incluso las del conjunto de bases mutuamente no sesgadas generado por M. Veremos en ésta sección que la matriz M se relaciona con el conjunto de matrices S_i mediante:

$$S_k = S_1 M^k \tag{4.1}$$

Éste resultado tiene una interpretación geométrica sencilla; supongamos que los operadores correspondientes a un rayo dado son de la forma $T(\vec{q}, \vec{q}S_1)$. Si se desplaza, en el espacio de fases, cada operador hacia su casilla contigua hacia la izquierda, es equivalente a multiplicar la coordenada $\vec{q}$ por la matriz M^{-1}; es decir, los operadores desplazados son de la forma $T\left(\vec{q}M^{-1}, \vec{q}S_2\right)$. Pero en éste conjunto de operadores desplazados, la relación entre las coordenadas es de la forma $\vec{p}' = \vec{q}'S_2M$. Es decir, su matriz S_2 es igual a S_1M. Aplicando sucesivas traslaciones de rayos, se obtiene que todos los conjuntos de operadores estabilizadores de los rayos son de la forma (4.1).

Veamos que esto es así. En la sección 3.2.4, más precisamente en la ecuación (3.29), vimos que los conjuntos de estabilizadores de cada una de las $d+1$ bases no sesgadas construidas a partir de una matriz M generadora del cuerpo finito son de la forma:

$$G_{(\vec{b},\vec{a})} = \left\{ T\left(\vec{b}M^j, \vec{a}\tilde{M}^j\right), \quad 0 \leq j \leq d-2 \right\} \tag{4.2}$$

donde $\vec{a}$ y $\vec{b}$ son vectores fila binarios de n componentes. Vale aclarar que no todos los pares $\left(\vec{b}, \vec{a}\right)$ corresponden a grupos estabilizadores diferentes. En efecto, como las potencias de la matriz M conforman un grupo cíclico, entonces:

$$G_{(\vec{b},\vec{a})} = G_{\left(\vec{b}M^k, \vec{a}\tilde{M}^k\right)} \tag{4.3}$$

donde k es un número entero.

Ésta ambigüedad puede ser salvada tratando por separado a los grupos estabilizadores formados por operadores X y operadores Z (que corresponden, respectivamente, a los casos $\vec{a} = 0$ y $\vec{b} = 0$). En los demás conjuntos, cada vector no nulo $\vec{q}$ tiene que aparecer exactamente una vez en el lugar de la coordenada correspondiente, por lo que puede mostrarse que se obtienen los $d-1$ grupos estabilizadores distintos fijando uno de los dos vectores; por ejemplo, el $\vec{a}$:

$$G_{\vec{b}} = \left\{ T\left(\vec{b}M^j, \vec{1}\tilde{M}^j\right), \quad 0 \leq j \leq d-2 \right\} \tag{4.4}$$

donde $\vec{1}$ es un vector binario que posee un 1 en su primera coordenada, y ceros en las demás, y $\vec{b}$ es un vector binario no nulo.

Además, como fue visto en la sección 2.4, cada uno de esos conjuntos tiene asociada una matriz $S_{\vec{b}}$ binaria, simétrica y no singular, que permite escribir al grupo estabilizador como:

$$G_{\vec{b}} = \left\{ T\left(\vec{q}, \vec{q}S_{\vec{b}}\right), \quad \forall \vec{q} \neq 0 \right\} \tag{4.5}$$

Pero puesto que en estos conjuntos no importa el orden de los elementos, una manera partícular de recorrer los vectores $\vec{q}$ es:

$$G_{\vec{b}} = \left\{ T\left(\vec{b}M^j, \vec{b}M^j S_{\vec{b}}\right), \quad 0 \leq j \leq d-2 \right\} \tag{4.6}$$

Nos interesa, ahora, encontrar la relación que existe entre la matriz M y las matrices $S_{\vec{b}}$ asociadas a las bases mutuamente no sesgadas generadas a partir de M. Comparando (4.6) con (4.4) se obtiene que, para $0 \leq j \leq d-2$, tiene que valer:

$$\vec{1}\tilde{M}^j = \vec{b}M^j S_{\vec{b}} \tag{4.7}$$

Pero puesto que vale, en particular, para $j = 0$, tiene que ser $\vec{b} = \vec{1}S_{\vec{b}}^{-1}$, con lo que la ecuación que debe satisfacer cada matriz $S_{\vec{b}}$ se convierte en:

$$\vec{1}\tilde{M}^j = \vec{1}S_{\vec{b}}^{-1} M^j S_{\vec{b}} \tag{4.8}$$

Vale notar, a esta altura, que la ecuación (4.8) es independiente de $\vec{b}$. Por lo tanto, todas las matrices $S_{\vec{b}}$ tiene que satisfacer la misma ecuación.

Supongamos ahora una matriz $S_{\vec{b}_1}$ fija y $S_{\vec{b}_k}$ otra matriz tales que dan dos de las bases mutuamente no sesgadas. Ambas tienen que satisfacer la ecuación (4.8). Por lo tanto:

$$\begin{aligned} \vec{1}\tilde{M}^j &= \vec{1}S_{\vec{b}_1}^{-1}M^jS_{\vec{b}_1} \\ \vec{1}\tilde{M}^j &= \vec{1}S_{\vec{b}_k}^{-1}M^jS_{\vec{b}_k} \end{aligned} \tag{4.9}$$

Definiendo $V_k = S_{\vec{b}_k}S_{\vec{b}_1}^{-1}$, se tiene que:

$$\vec{1}S_{\vec{b}_1}^{-1}M^jV_k^{-1} = \vec{1}S_{\vec{b}_1}^{-1}V_k^{-1}M^j \tag{4.10}$$

Sabemos que existen al menos 2^n-1 matrices V_k distintas (porque sabemos que existen las matrices S_i), una de las cuales es la identidad, que son soluciones de (4.10). Además, 2^n-1 soluciones V_k triviales a dicho sistema son las 2^n-1 potencias distintas de la matriz M. Si, además, mostramos que la ecuación (4.10) tiene exactamente 2^n-1 soluciones no singulares, sabremos que las potencias de M son las 2^n-1 soluciones buscadas.

Para eso, supongamos que el sistema tiene 2^n soluciones no singulares y veamos que se llega a un absurdo. De haber 2^n soluciones, existirían dos matrices distintas V_i^{-1} y V_j^{-1} tales que la suma $V_i^{-1}+V_j^{-1}$, al ser multiplicada por izquierda por el vector $\vec{1}S_{\vec{b}_1}^{-1}$, daría como resultado el vector nulo. Puede verse que la suma $V_i^{-1}+V_j^{-1}$ satisface:

$$\vec{1}S_{\vec{b}_1}^{-1}M^j\left(V_i^{-1}+V_j^{-1}\right) = \vec{1}S_{\vec{b}_1}^{-1}\left(V_i^{-1}+V_j^{-1}\right)M^j \tag{4.11}$$

Pero por como fueron elegidas V_i^{-1} y V_j^{-1}, el miembro derecho se anula:

$$\vec{1}S_{\vec{b}_1}^{-1}M^j\left(V_i^{-1}+V_j^{-1}\right) = 0 \tag{4.12}$$

Pero, recordando que esta ecuación vale para cualquier j, y que $\vec{1}S_{\vec{b}_1}^{-1}M^j$ recorre todos los vectores, se concluye que $V_i = V_j$, lo que es absurdo. Por lo tanto la ecuación (4.10) tiene exactamente 2^n-1 soluciones no singulares.

En resumen, dada la representación matricial de un elemento M generador del cuerpo finito, y las matrices S_k que generan las mismas bases que aquellas que surgen de las estriaciones del espacio de fases, se tendrá que, ordenando las matrices S_k de manera adecuada, vale la relación:

$$S_k = S_1M^k \tag{4.13}$$

4.1.1. Consecuencias de la relación entre matrices binarias simétricas y generadores del cuerpo finito

Una primera consecuencia de la relación (4.1), es que, dado que las potencias de la matriz M forman un conjunto cerrado frente a la suma, por

ser M un elemento generador de un cuerpo finito, se desprende de (4.1) que el conjunto de matrices S asociado a una matriz M es un conjunto cerrado frente a la suma. En otras palabras, es condición necesaria para que un conjunto de matrices S pueda estar asociado a un espacio de fases covariante frente a traslaciones, que dicho conjunto de matrices sea cerrado frente a la suma.

Otra consecuencia, que permite relacionar una propiedad de la matriz M con las bases que corresponderán a las estriaciones asociadas, es que si una de las bases del conjunto de bases mutuamente no sesgadas es la estabilizada por operadores Y, entonces la matriz M será simétrica. En efecto, la matriz S correspondiente a la base estabilizada por los operadores Y es la matriz identidad, pero de acuerdo a la relación (4.1), si una de las matrices S es la identidad, y puesto que todas las matrices S son simétricas, entonces todas las potencias de M deben ser simétricas. En particular M es una matriz simétrica. Si bien dicha relación es muy específica, sirve para mostras que algunas propiedades de las bases asociadas a estriaciones pueden obtenerse directamente de la matriz M.

4.2. Conjuntos de bases mutuamente no sesgadas no lineales

Hemos visto que cuando se construye un espacio de fases y se pide que las traslaciones sean covariantes, es decir, que cada traslación en el espacio de fases representado esté asociada a una traslación en el espacio de Hilbert correspondiente, cada estriación tiene asociada una base del espacio de Hilbert, y cada estado de la base mencionada del espacio de Hilbert se encuentra asociado a una linea de esa estriación. Además, como fue visto en la sección anterior, las matrices binarias simétricas asociadas a un conjunto de bases mutuamente no sesgadas generado a partir de un elemento generador del cuerpo finito, serán un conjunto cerrado frente a la suma.

Surge, al respecto, la duda acerca de si cualquier conjunto de bases mutuamente no sesgadas corresponde a un espacio de fases o no.

Realizando una búsqueda exhaustiva entre todas las matrices binarias simétricas no singulares, pueden construirse *todos* los conjuntos de bases mutuamente no sesgadas estabilizadas por operadores de Pauli generalizados, siempre y cuando se dejen fijas las bases estabilizadas por los operadores X y Z.

En la tabla 4.1 se muestra la cantidad de conjuntos de bases mutuamente no sesgadas encontrados para distinta cantidad de qubits, junto con la

cantidad de matrices generadoras del cuerpo finito independientes, calculada mediante lo expuesto en la sección 3.2.6.

Número de qubits n	Cantidad de matrices binarias, simétricas y no singulares	Cantidad de matrices generadoras del cuerpo finito	Cantidad de conjuntos de bases mutuamente no sesgadas
1	1	1	1
2	4	1	1
3	28	8	8
4	448	336	336
5	13888	64512	$1,3 \cdot 10^8$

Tabla 4.1: *Conteo de matrices binarias, simétricas y no singulares; matrices generadoras del cuerpo finito; y conjuntos de bases mutuamente no sesgadas.*

Puede observarse que, hasta cuatro qubits, la cantidad de matrices generadoras del cuerpo finito independientes es igual a la cantidad de conjuntos de bases mutuamente no sesgadas. Esto también permite concluir que todos los conjuntos de matrices asociados a conjuntos de bases mutuamente no sesgadas de hasta cuatro qubits, son cerrados frente a la suma, puesto que todos corresponden a matrices generadoras del cuerpo finito.

Sin embargo, aparece un resultado sorprendente en el caso de cinco qubits. Existe una cantidad muy superior de conjuntos de bases mutuamente no sesgadas que de matrices generadoras del cuerpo. Más aún, algunos de los conjuntos de matrices son abiertos frente a la suma.

La existencia de una cantidad mucho mayor de conjuntos de bases mutuamente no sesgadas que de matrices generadoras del cuerpo se puede comprender mediante el conteo de la cantidad de matrices binarias simétricas y no singulares que existen para cada dimensión. Dicha cantidad $\sigma(n)$ puede calcularse[22] mediante la fórmula:

$$\sigma(n) = \prod_{j=1}^{n} \left(2^j - \mathrm{Imp}(j)\right) \tag{4.14}$$

donde la función $\mathrm{Imp}(j)$ es 1 cuando j es impar, y 0 en otro caso.

Por lo tanto vemos que el número de matrices binarias simétricas no singulares crece como una exponencial del cuadrado del número de qubits.

Puede verse, además, que la cantidad de matrices generadoras del cuerpo finito también crece de manera acotada por una exponencial del cuadrado del número de qubits. Sin embargo, la cantidad de conjuntos de bases no sesgadas es de esperar que sea, en algún sentido que no pudo aún ser determinado, combinatoria en el número de matrices binarias simétricas no singulares. Por lo tanto, en ese mismo sentido, es de esperar que la cantidad de conjuntos de bases mutuamente no sesgadas crezca como una combinatoria en el número de matrices generadoras del cuerpo finito, y de ahí la gran divergencia que aparece en el caso de cinco qubits y que, es de esperar, será mayor para más qubits, aunque no pudo ser computado numéricamente por razones de recursos de computo. Si bien esto no es una demostración, sirve como argumento en favor de los resultados obtenidos.

4.3. Problemas abiertos

Hemos visto que, para un sistema de dimensión $d = 2^n$, puede definirse un espacio de fases de $d \times d$ mediante la utilización de cuerpos finitos y que, mediante la asociación covariante entre lineas y estados queda definido un conjunto de bases mutuamente no sesgadas. Además, todo el desarrollo realizado puede generalizarse para dimensión $d = p^n$. Puede verse, por lo tanto, que existen conjuntos de $d+1$ bases mutuamente no sesgadas siempre que la dimensión del sistema es $d = p^n$..

Sin embargo, poco se sabe acerca de la cantidad de bases mutuamente no sesgadas que existen para un espacio de dimensión distinta a la potencia de un primo. Un problema que aparentemente se encuentra relacionado con el de encontrar bases mutuamente no sesgadas en dimensión d, es el de encontrar conjuntos de cuadrados latinos de $d \times d$ mutuamente ortogonales. Un cuadrado latino de $d \times d$ es una grilla de $d \times d$ en la que en cada sitio de la grilla se encuentra un número natural entre 1 y d, inclusive, tal que ningún número aparece dos veces en la misma fila ni dos veces en la misma columna[1].

Se dice, además, que dos cuadrados latinos son ortogonales si al construir una grilla de $d \times d$ que en cada casilla contiene los pares ordenados correspondientes a la misma casilla de cada uno de los dos cuadrados latinos en cuestión, cada par ordenado aparece exactamente una vez. En la figura 4.1 se puede observar un par de cuadrados latinos ortogonales.

La relación con las bases mutuamente no sesgadas salta a la vista. Un

[1] Un tipo de cuadrado latino que ha tomado cierta popularidad recientemente es el de los sudokus.

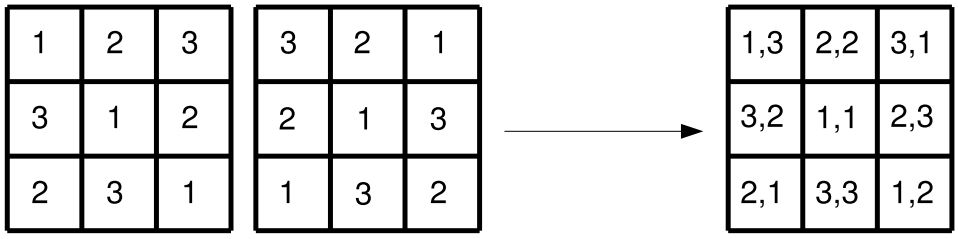

Figura 4.1: *Dos cuadrados latinos ortogonales. En cada cuadrado latino de $d \times d$ aparecen los números del* 1 *al d exactamente una vez cada uno por fila y por columna. Dos cuadrados latinos se dicen ortogonales, como en la figura de la derecha, si al tomar los pares ordenados correspondientes a cada uno de los cuadrados latinos en cuestión, cada par ordenado posible aparece exactamente una vez.*

conjunto de cuadrados latinos mutuamente ortogonales tiene las mismas propiedades geométricas que las lineas en los cuerpos finitos. Sin embargo, los cuadrados latinos mutuamente ortogonales no están limitados a dimensiones que sean potencias de primos, sino que se pueden buscar para cualquier tamaño.

Entonces, está abierto el problema acerca de si, utilizando cuadrados latinos mutuamente ortogonales, junto con los cuadrados correspondientes a lineas horizontales y verticales, podrá definirse un espacio de fases para cualquier dimensión d y, con él, conjuntos de bases mutuamente no sesgadas. O al menos por éste camino se podría determinar para qué dimensiones d es factible realizar esto. Es interesante citar un resultado sorprendente de Gaston Tarry del año 1901 que dice que, para dimensión 6, la mínima dimensión que no es la potencia de un primo, no existen cuadrados latinos ortogonales. Dicho resultado ya había sido conjeturado por Euler más de un siglos antes. Es por esto que no se puede construir un espacio de fases con más de tres estriaciones. Asímismo, se conjetura que para dimensión 10 no se pueden encontrar más de dos cuadrados latinos mutuamente ortogonales, y que para dimensión 12 se pueden encontrar conjuntos de cinco, pero no se sabe si hay de más. Queda en evidencia, por tanto, la ventaja de trabajar con dimensiones que sean potencias de un número primo, puesto que en los casos en los que no lo son, no existe, al menos en los casos estudiados de cuadrados latinos mutuamente ortogonales, manera de definir $d+1$ estriaciones geométricamente viables.

Una propiedad interesante es que todo conjunto de cuadrados latinos mutuamente ortogonales, es de a lo sumo $d-1$ elementos. Esto, sumado al hecho de que todo espacio de fases definido mediante cuerpos finitos tiene asociado un cuadrado latino por cada linea que no sea horizontal o vertical,

demuestra que no se pueden encontrar conjuntos de lineas que sean no sesgadas con todas las de un espacio de fases dado. Más aún, está demostrado que, en dimensión d no puede haber más de $d+1$ bases mutuamente no sesgadas[4].

Existen, además, varias conjeturas y preguntas aún abiertas al respecto, tres de las cuales se enuncian a continuación:

1. Conjetura de Zauner[19]: El mayor número de bases mutuamente no sesgadas para sistemas de dimensión 6 es 3.

2. ¿Existen conjuntos de $d+1$ bases mutuamente no sesgadas para cualquier dimensión d?

3. ¿Tiende a infinito el máximo número de bases no sesgadas, cuando tiende a infinito la dimensión del sistema?

A pesar del gran esfuerzo empleado para responderlas, Poco se sabe aún al respecto. Incluso con mentes geniales como la de Euler dedicando esfuerzo a problemas sobre cuadrados latinos mutuamente ortogonales, es poco lo que se sabe acerca de dichos conjuntos de cuadrados latinos para dimensiones distintas a la potencia de un primo que, aparentemente, tienen una íntima relación con los conjuntos de bases mutuamente no sesgadas.

4.4. Conclusiones parciales

En este capítulo se encontró la relación que existe entre los conjuntos de bases mutuamente no sesgadas asociados a un elemento generador M de un cuerpo finito, con aquellos generados a partir de matrices simétricas binarias. A partir de dicha relación se encontró que las matrices simétricas binarias asociadas a las bases correspondientes a un conjunto de estriaciones forman un conjunto cerrado frente a la suma.

Se encontró, luego, que existen conjuntos de bases mutuamente no sesgadas que no pueden utilizarse para la construcción de un espacio de fases.

Por último, se comentó brevemente acerca de resultados y conjeturas respecto de la relación entre espacios de fases, bases no sesgadas y cuadrados latinos ortogonales.

Capítulo 5

Fidelidad media y caracterización de canales cuánticos

Una aplicación importante de los conjuntos de bases mutuamente no sesgadas, es la medición de la fidelidad media de un circuito cuántico, estudiada por Christoph Dankert en [15].

La fidelidad media es, básicamente, una medida de la distancia entre un algoritmo cuántico y su implementación real, ruidosa y defectuosa. Resulta de gran importancia puesto que permite, entre otras cosas, determinar si son necesarios cambios a la implementación o códigos de corrección de errores [16][20][21] para convertir una implementación mala de un algoritmo en una aceptable. Para tener una caracterización correcta de la distancia, se debe, de alguna manera, obtener una fidelidad promedio sobre todos los estados posibles del estado de Hilbert del sistema.

En el presente capítulo se introducirá el concepto de fidelidad media, presentado por Dankert en [15], mostrando un resultado que relaciona dicha fidelidad con las bases mutuamente no sesgadas.

Luego se presentará una manera de determinar el peso que tiene un conjunto de errores en la implementación de un algoritmo cuántico. Dicho peso sirve para determinar el tipo de código de corrección de errores necesario para mejorar un circuito sin la necesidad de implementario, y constituye, por lo tanto, una herramienta de suma importancia para la implementación de algoritmos cuánticos. Permite, además, dar una caracterización más fidedigna del canal cuántico sobre el que se está trabajando.

5.1. Fidelidad media

La fidelidad media se utiliza para caracterizar la diferencia entre la operación unitaria que uno quiere implementar, y la operación cuántica que realmente hace. Ambas pueden diferir por ruido en el canal sobre el que se la implementa, o errores de la implementación en sí.

Para definir la fidelidad media de un circuito cuántico, se debe distinguir entre un algoritmo cuántico, dado por una operación unitaria U, y su implementación defectuosa. Es decir, si se tiene un algoritmo cuántico U unitario que actúa sobre un estado $|\psi\rangle$, entonces su implementación Σ_U será tal que actuando sobre un operador densidad ρ dará:

$$\Sigma_U(\rho) = \sum_k A_k \rho A_K^\dagger \tag{5.1}$$

Dicha implemetación Σ_U puede diferir del algoritmo cuántico U, puesto que tanto el canal sobre el que se implementa el algoritmo como la implementación en sí, pueden ser defectuosos. Los operadores A_k se denominan operadores de Kraus, y obedecen que $\sum_k A_k^\dagger A_k = 1$. Vale notar que, en caso de tener una implementación perfecta, habrá un único operador de Kraus $A_0 = U$.

Se define, entonces, la fidelidad para un estado $|\psi\rangle$ de un proceso cuántico U con implementación Σ_U como:

$$F_{|\psi\rangle}(U, \Sigma_U) = \langle\psi| U^\dagger \Sigma_U (|\psi\rangle\langle\psi|) U |\psi\rangle \tag{5.2}$$

Es decir, como el solapamiento entre el estado evolucionado exactamente con U y aquel evolucionado con su implementación defectuosa Σ_U.

Sin embargo, dicha definición sólo da cuenta de la fidelidad de la implementación para un estado de entrada dado. Pero puesto que la fidelidad puede depender fuertemente del estado de entrada, es conveniente definir algún tipo de promedio sobre todos los posibles estados. Para realizar ese promedio sobre todos los estados de un espacio de Hilbert dado es necesario definir una medida en dicho espacio. Esto se puede hacer utilizando la medida de Fubini-Study, y será definido en la próxima sección. Por lo pronto, aún sin una definición precisa de dicha medida, se define la fidelidad media de un algoritmo U con implementación Σ_U como:

$$\overline{F}(U, \Sigma_U) = \int_{F-S} F_{|\psi\rangle}(U, \Sigma_U)\, d|\psi\rangle \tag{5.3}$$

Equivalentemente, mediante la definición (5.2) puede verse que:

$$\overline{F}\left(U,\Sigma_U\right)=\int_{F-S}\langle\psi|\,U^{\dagger}\Sigma_U\left(|\psi\rangle\,\langle\psi|\right)U\,|\psi\rangle\,d\,|\psi\rangle \tag{5.4}$$

No está de más notar que se estará promediando sólo sobre los estados de entrada puros, dejando de lado los mixtos.

5.2. Las integrales en la medida de Fubini-Study

La integral en la medida de Fubini-Study permite integrar sobre todos los estados de un espacio de Hilbert. Es conveniente, para introducirla, referir al caso de un qubit. Es ese caso, el estado puro más general puede representarse en la denominada esfera de Bloch:

$$|\psi\rangle=\cos\theta\,|0\rangle+e^{i\varphi}\sin\theta\,|1\rangle \tag{5.5}$$

donde $\theta\in[0,\pi)$ y $\varphi\in[0,2\pi)$. Es decir, todo estado puro está distribuido sobre una esfera de radio 1.

Se define, entonces, la integral sobre la medida de Fubini-Studi para un sistema de un qubit como la integral sobre la esfera de Bloch; es decir:

$$d\,|\psi\rangle=\sin\theta d\theta d\varphi \tag{5.6}$$

En otras palabras, la variable θ recorre un semicírculo, manteniendo la norma del estado en 1, y la variable φ es la encargada de darle al estado las fases correspondientes.

Cuando el espacio de Hilbert tiene dimensión 2^n, la integral no tiene una representación geométrica tan sencilla. Sin embargo puede verse que, para mantener el estado con norma 1, se debe realizar una integral sobre 2^n-1 variables angulares que definen la superficie de una parte de una esfera de dimensión 2^n. Mientras que, puesto que los estados están definidos a menos de una fase global, debe integrarse sobre 2^n-1 variables de fase.

Sin embargo, la forma explícita del diferencial con el que se integra en la medida de Fubini-Study no reviste mayor importancia para el presente trabajo. Sólo es necesario definirla a partir de algunas propiedades.

Más formalmente, un espacio de Hilbert de dimensión n es un espacio proyectivo complejo CP^{n-1}. Esto es equivalente a decir que los estados puros de un sistema cuántico son rayos (vectores de norma 1), y que una fase global no afecta al estado del sistema. O, en otras palabras, que cada estado del espacio de Hilbert está representado por una n-upla de números complejos

no nula, y multiplicar todos los elementos de la n-upla por un mismo número complejo no nulo no modifica el estado.

Por ser el espacio de Hilbert un espacio proyectivo complejo, como está probado para todo espacio proyectivo complejo, existe una única medida invariante unitaria denominada medida de Fubini-Study. Las integrales sobre dicha medida se notan como:

$$\int_{F-S} f\left(|\psi\rangle\right) d\,|\psi\rangle \tag{5.7}$$

Resumiendo, existe una integral sobre el espacio de Hilbert denominada integral en la medida de Fubini-Study con la propiedad de ser invariante frente a transformaciones unitarias. Esto es:

$$\int_{F-S} f\left(U\,|\psi\rangle\right)\, d\,|\psi\rangle = \int_{F-S} f\left(|\psi\rangle\right)\, d\,|\psi\rangle \tag{5.8}$$

donde U es un operador unitario arbitrario.

Además, se utilizará la normalización:

$$\int_{F-S} 1\, d\,|\psi\rangle = 1 \tag{5.9}$$

5.3. Fidelidad media y bases mutuamente no sesgadas

Repasaremos en esta sección algunos resultados obtenidos por Dankert en [15], que serán de utilidad para comprender, luego, su circuito propuesto para la determinación de dicha fidelidad, y para mostrar un circuito alternativo para dicha determinación que, a diferencia del propuesto por Dankert, no requiere de ningún tipo de registro clásico.

5.3.1. Resultados previos

Un primer resultado obtenido en [15], muestra que cierto tipo de integrales en la medida de Fubini-Study pueden ser reducidas al cálculo de trazas. Dicho resultado es de suma importancia, en tanto que permite llevar una integral sobre infinitos estados a un conjunto de sumas sobre una cantidad finita de estados, como son las trazas sobre espacios de Hilbert de dimensión finita.

El resultado en cuestión dice que si M y N son operadores lineales, vale que:

$$\int_{F-S} \langle\psi| M |\psi\rangle \langle\psi| N |\psi\rangle \, d|\psi\rangle = \frac{1}{d(d+1)} (\mathrm{Tr}M\mathrm{Tr}N + \mathrm{Tr}MN) \quad (5.10)$$

es decir, se convierte la integral sobre el espacio de Hilbert en el cálculo de tres trazas.

A partir del resultado (5.10), puede llegarse a un teorema que relaciona las integrales del tipo de las mostradas en (5.10) con sumas sobre vectores de conjuntos de bases mutuamente no sesgadas. Esto permitirá, además de llegar a un resultado de suma importancia en lo sucesivo, utilizar las herramientas desarrolladas en el capítulo 3.

Teorema 5.3.1. *Sea un sistema de dimensión 2^n, un conjunto de $2^n + 1$ bases mutuamente no sesgadas $B_\kappa = \{|\psi_i^\kappa\rangle, i = 1, ..., d\}$ y dos operadores lineales M y N. Entonces vale que:*

$$\int_{F-S} \langle\psi| M |\psi\rangle \langle\psi| N |\psi\rangle \, d|\psi\rangle = \frac{1}{d(d+1)} \sum_{\kappa=1}^{d+1} \sum_{i=1}^{d} \langle\psi_i^\kappa| M |\psi_i^\kappa\rangle \langle\psi_i^\kappa| N |\psi_i^\kappa\rangle \quad (5.11)$$

Demostración. En primer lugar es necesario notar que, así como los operadores de punto definidos en (3.38) sirven de base para desarrollar cualquier operador hermítico (como por ejemplo la matriz densidad, en cuyo caso se obtiene como coeficientes del desarrollo a la función de Wigner evaluada en cada punto) también sirven para desarrollar cualquier operador lineal, con la única salvedad que los coeficientes obtenidos ya no serán necesariamente reales.

Dichos operadores de punto se pueden generalizar levemente sin el requerimiento de la covariancia traslacional. De esta forma se pueden construir operadores de punto aun cuando las bases mutuamente no sesgadas no puedan utilizarse para construir un espacio de fases covariante. Para ello, a la hora de elegir la grilla cuántica, se sigue asociando una base a cada estriación, pero se asigna cualquier estado de la base a cada línea. Con ésta asignación de proyectores a las líneas, se pueden definir los operadores de punto como en (3.38):

$$A(\alpha) = \frac{1}{d} \left[-1 + \sum_{\kappa} P\left(\lambda_{(\alpha)}^{(\kappa)}\right) \right] \quad (5.12)$$

donde α es un punto, y $P\left(\lambda_{(\alpha)}^{(\kappa)}\right)$ es el proyector asociado al punto de la estriación κ que pasa por α.

De esta forma, los operadores M y N de (5.10) admiten desarrollos de la forma:

$$M = d \sum_{\alpha} \mu(\alpha) A(\alpha) \tag{5.13}$$

$$N = d \sum_{\alpha} \nu(\alpha) A(\alpha) \tag{5.14}$$

donde μ y ν son funciones complejas del punto en el espacio de fases.

Además, utilizando la ecuación (3.18), se obtienen los siguientes resultados:

$$\mathrm{Tr}(MN) = d \sum_{\alpha} \mu(\alpha) \nu(\alpha) \tag{5.15}$$

$$\mathrm{Tr}(M) = \sum_{\alpha} \mu(\alpha) \tag{5.16}$$

$$\mathrm{Tr}(N) = \sum_{\alpha} \nu(\alpha) \tag{5.17}$$

Consideremos, ahora, la suma:

$$\frac{1}{d(d+1)} \sum_{\kappa=1}^{d+1} \sum_{i=1}^{d} \langle \psi_i^{\kappa} | M | \psi_i^{\kappa} \rangle \langle \psi_i^{\kappa} | N | \psi_i^{\kappa} \rangle \tag{5.18}$$

donde κ recorre las estriaciones del espacio de fases sobre el que están definidos los operadores de punto utilizados para la expansión de M y N, e i recorre los estados lineas de esa estriación; es decir, se recorren todos los estados del conjunto de bases mutuamente no sesgadas asociado al espacio de fases.

Reemplazando las expansiones de M y N y usando que $\langle \psi_i^{\kappa} | A(\alpha) | \psi_i^{\kappa} \rangle$ vale $1/d$ cuando el punto α pertenece a la linea i de la estriación κ, se obtiene que la expresión (5.18) es igual al miembro derecho de la (5.10), con lo que queda demostrado un resultado fundamental; en las integrales del tipo de las de la ecuación (5.10), integrar sobre la medida de Fubini-Study y promediar sobre los estados de un conjunto de $2^n + 1$ bases mutuamente no sesgadas da el mismo resultado. □

5.3.2. La memoria cuántica

Una memoria cuántica es un algoritmo cuántico cuya operación unitaria es la identidad; es decir, un algoritmo que no hace nada más que devolver a la salida el mismo estado que se colocó a la entrada.

En ese caso, la expresión (5.4) se reduce a:

$$\overline{F}\left(U,\Sigma_1\right)=\int_{F-S}\left\langle\psi\right|\Sigma_1\left(\left|\psi\right\rangle\left\langle\psi\right|\right)\left|\psi\right\rangle d\left|\psi\right\rangle \tag{5.19}$$

Pero de acuerdo con la ecuación (5.10) y la expansión de Σ_1 en operadores de Kraus, se obtiene:

$$\overline{F}\left(U,\Sigma_1\right)=\frac{1}{d\left(d+1\right)}\left(d+\sum_k\left|\mathrm{Tr}A_k\right|^2\right) \tag{5.20}$$

Además, como los operadores de Pauli generalizados son una base del espacio de los operadores lineales sobre el espacio de Hilbert, entonces cada uno de los operadores de Kraus admite un desarrollo como combinación lineal de operadores de Pauli generalizados:

$$A_k=\sum_j\alpha_j^{(k)}P_j \tag{5.21}$$

donde P_j recorre, con el subíndice j, los operadores de Pauli generalizados.

Luego:

$$\overline{F}\left(U,\Sigma_1\right)=\frac{1}{d+1}+\frac{1}{d\left(d+1\right)}\sum_j\sum_{j'}\sum_k\alpha_j^{(k)}\alpha_{j'}^{(k)*}\mathrm{Tr}P_j\mathrm{Tr}P_{j'} \tag{5.22}$$

Sin embargo, todos los operadores de Pauli generalizados, a excepción de la identidad, tienen traza nula; por dicho motivo sólo sobrevive a la suma sobre j y j' aquel valor j_0 tal que $P_{j_0}=1$. Y, puesto que la traza de la identidad es d, se obtiene:

$$\overline{F}\left(U,\Sigma_1\right)=\frac{1}{d+1}\left(1+d\sum_k\left|\alpha_{j_0}^{(k)}\right|^2\right) \tag{5.23}$$

Éste resultado puede interpretarse de la siguiente manera: la fidelidad media de una memoria da cuenta de qué tanto tiene de identidad el desarrollo en operadores de Kraus de su implementación.

Cuando no se trata de memorias, la fidelidad media da cuenta de cuánto tiene del algoritmo original la implementación dada.

5.3.3. Medición de la fidelidad media

Retomando la medición de la fidelidad media, se desea encontrar un circuito capaz de determinarla para un dado canal cuántico. En primer lugar, puesto que la fidelidad media es una suerte de distancia entre el algoritmo real y su implementación, resulta necesario para construir un circuito que la

determine, poder implementar de manera exacta al algoritmo como punto de partida para la comparación con la implementación defectuosa. Por ejemplo, en el caso $U = 1$, la fidelidad media provee una caracterización de las fuentes de ruido (o interacciones externas no controladas) a las que está sometido el sistema, por lo que para la determinación de la fidelidad se requiere de un canal sin ruido, o en su defecto de una implementación limpia de la identidad.

Recordemos que, de acuerdo con la definición (5.4), la fidelidad media de una implementación Σ_U de un algoritmo cuántico U está dada por:

$$\overline{F}\left(U, \Sigma_U\right) = \int_{F-S} \langle\psi| U^\dagger \Sigma_U \left(|\psi\rangle \langle\psi|\right) U |\psi\rangle \, d|\psi\rangle \tag{5.24}$$

Reemplazando Σ_U Por su expansión en operadores de Kraus (5.1), e intercambiando el orden de la suma y la integral de Fubini-Study se obtiene que la fidelidad media puede escribirse como:

$$\overline{F}\left(U, \Sigma_U\right) = \sum_k \int_{F-S} \langle\psi| U^\dagger A_k |\psi\rangle \langle\psi| A_k^\dagger U |\psi\rangle \, d|\psi\rangle \tag{5.25}$$

Pero puede verse que la integral que queda es de la forma de las presentadas en (5.11), con $M = U^\dagger A_k$ y $N = A_k^\dagger U$. Por lo tanto, realizar la integral es igual a promediar sobre los 2^n estados de cada una de las $2^n + 1$ bases mutuamente no sesgadas de un conjunto dado. Reemplazando la suma por el promedio mencionado, e intercambiando el orden de la suma en k y la suma sobre los estados de las bases no sesgadas, se obtiene que:

$$\overline{F}\left(U, \Sigma_U\right) = \frac{1}{d\left(d+1\right)} \sum_{\kappa=1}^{d+1} \sum_{i=1}^{d} \langle\psi_i^\kappa| U^\dagger \Sigma_U \left(|\psi_i^\kappa\rangle \langle\psi_i^\kappa|\right) U |\psi_i^\kappa\rangle \tag{5.26}$$

En otras palabras, la fidelidad media de la implementación de un algoritmo cuántico U es igual al promedio de las fidelidades para los $d\left(d+1\right)$ estados de un conjunto de $d+1$ bases mutuamente no sesgadas:

$$\overline{F}\left(U, \Sigma_U\right) = \frac{1}{d\left(d+1\right)} \sum_{\kappa=1}^{d+1} \sum_{i=1}^{d} F_{|\psi_i^\kappa\rangle}\left(U, \Sigma_U\right) \tag{5.27}$$

Esta última ecuación es la que sienta las bases para el desarrollo de circuitos cuánticos capaces de medir la fidelidad de una implementación dada de un circuito cuántico.

5.4. Circuitos para la medición de la fidelidad media

Para la construcción de circuitos que permitan medir la fidelidad media de un canal cuántico ruidoso Σ_U, es importante ver que, de acuerdo con la ecuación (5.27), la fidelidad media es un promedio de fidelidades sobre los estados que conforman un conjunto de bases mutuamente no sesgadas.

Se presenta un primer circuito introducido por Dankert en [15], seguido de una variante del mismo desarrollada como parte de éste trabajo de tesis que elimina la necesidad de canales clásicos, reemplazándolos por estados mixtos.

5.4.1. Primer circuito

Recordando la expresión (5.2) para la fidelidad sobre un estado dado

$$F_{|\psi\rangle}\left(U, \Sigma_U\right) = \langle\psi| U^\dagger \Sigma_U \left(|\psi\rangle \langle\psi|\right) U |\psi\rangle \tag{5.28}$$

puede interpretarse la fidelidad sobre un estado como la probabilidad de, dado el sistema en el estado $|\psi\rangle$ en cuestión, volver a medir dicho estado luego de la aplicación de Σ_U seguida de $U^\dagger$. Es decir, la probabilidad de que, al evolucionar un sistema con la implementación defectuosa y evolucionar hacia atrás con la implementación perfecta, nada cambie.

Es decir, dado un estado $|\psi_i^\kappa\rangle$, la fidelidad para ese estado puede obtenerse mediante el circuito de la figura 5.1.

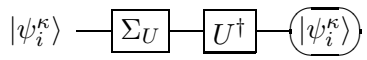

Figura 5.1: *Para medir la fidelidad de una implementación defectuosa Σ_U de un algoritmo cuántico U para un estado $|\psi_i^\kappa\rangle$, se debe evolucionar el estado con la implementación defectuosa, evolucionar hacia atrás con una implementación perfecta, y medir, a la salida, la probabilidad de obtener el mismo estado con el que se entró al circuito.*

Equivalentemente, conociendo un circuito V_i^κ cuya acción sobre el estado $|0\rangle$ de la base computacional sea transformarlo en el estado $|\psi_i^\kappa\rangle$, podría implementarse el circuito de la figura 5.1 de manera levemente más complicada, pero dejando de manera explícita el proceso de preparación del estado $|\psi_i^\kappa\rangle$ y el de medición, como se ilustra en la figura 5.2.

Supongamos, por un instante, que se conoce la familia de operadores V_i^κ. Para obtener la fidelidad media se debe, entonces, promediar el circuito 5.2 sobre κ e i. Con dicho fin pueden utilizarse dos canales clásicos que varían

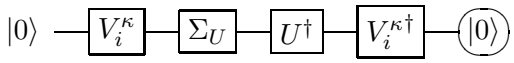

Figura 5.2: *Conociendo un operador V_i^κ que convierta el estado $|0\rangle$ en el $|\psi_i^\kappa\rangle$, puede explicitarse, a partir del circuito de la figura 5.1, el proceso de fabricación del estado y el de medición.*

al azar, uno recorriendo los posibles valores de κ, es decir de 1 a $d+1$, y el otro los valores de i de 1 a d. Dichos canales resultarán responsables de controlar cuál de todos los operadores V debe actuar en el circuito. Con ello aplicado al circuito 5.2, se consigue promediar la fidelidad sobre todos los estados del conjunto de bases mutuamente no sesgadas, con lo que se obtiene, efectivamente, la fidelidad media. En la figura 5.3 se muestra el circuito completo.

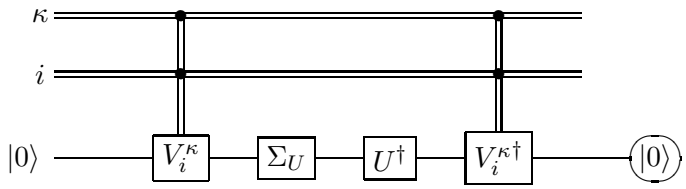

Figura 5.3: *Circuito cuántico para la medición de la fidelidad media. La variable κ recorre los valores del 1 al $d+1$ aleatoriamente para recorrer las bases del conjunto de bases no sesgadas, mientras que i va, también aleatoriamente, del 1 a d para recorrer los estados de dichas bases. La probabilidad de encontrar $|0\rangle$ a la salida corresponde a la fidelidad media de la implementación del circuito cuántico.*

Una primera objeción puede hacerse respecto de las implementaciones de V, ya que si bien se vieron en la sección 2.5 circuitos eficientes para el cambio de base, nada se habló acerca de convertir un estado particular en otro. Sin embargo, si se usa el i para convertir al vector $|0\rangle$ en el vector $|i\rangle$ de la base computacional (Esto se consigue aplicando C-Not, utilizando como control cada qubit del desarrollo binario de i, y como objetivo el qubit correspondiente del canal cuántico), y luego se aplica el cambio de base a la base κ mediante los circuitos desarrollados en la sección 2.5, se obtendrá que el resultado, por tomar i al azar, será un vector tomado al azar de la base κ. Por lo tanto el resultado al recorrer al azar κ e i será la generación aleatoria de todos los vectores de los conjuntos de bases mutuamente no sesgadas.

En resumen, los circuitos para los operadores V se consiguen mediante un número de compuertas C-Not igual a la cantidad de qubits, con control en los bits del registro i y destino en los qubits del canal cuántico del circuito

5.3, seguido del circuito de cambio de base a la base κ mostrado en la sección 2.5.

Se tiene, entonces, un circuito para medir la fidelidad media. La medición consiste en determinar la probabilidad de medir $|0\rangle$ a la salida. Entonces, la cantidad de veces que se debe hacer funcionar el circuito y medir a la salida para obtener la fidelidad media con una desviación estándar ν dada obedece por razones estadísticas que:

$$N \propto \frac{1}{\nu^2} \tag{5.29}$$

donde N es el número de veces que se debe medir.

5.4.2. Segundo circuito

El segundo circuito en cuestión se basa en un resultado de Ekert y colaboradores, en [31]. En ese trabajo probaron que, dados dos sistemas cuyos espacios de Hilbert son idénticos, puede medirse la traza del producto de sus operadores densidad ρ_1 y ρ_2 mediante el circuito de la figura 5.4. La compuerta swap controlada actúa como se muestra en la ecuación (5.30).

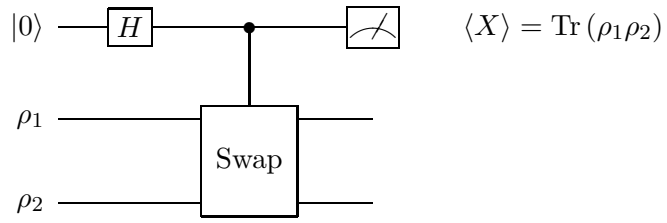

Figura 5.4: *Circuito cuántico para la determinación del producto de dos operadores densidad ρ_1 y ρ_2.*

$$\begin{aligned} \mathrm{C-Swap}\,|0\rangle\,|a\rangle\,|b\rangle &= |0\rangle\,|a\rangle\,|b\rangle \\ \mathrm{C-Swap}\,|1\rangle\,|a\rangle\,|b\rangle &= |1\rangle\,|b\rangle\,|a\rangle \end{aligned} \tag{5.30}$$

Esta idea de un circuito que mida el solapamiento entre dos estados, marca un camino a seguir; midiendo el solapamientro entre el estado evolucionado por la implementación ruidos Σ_U con aquel evolucionado de manera perfecta por U se obtendría la fidelidad. En efecto, el circuito de la figura 5.5 mide la fidelidad de la implementación del algoritmo cuántico U, como se verá a continuación. Es notable, además, que los últimos dos registros del circuito 5.5 pueden ser preparados en sistemas de dimensión $d+1$ y d, respectivamente, como estados máximamente mixtos. En otras palabras,

son registros de ruido. Por ese motivo, no resulta en absoluto complicado conseguir esos estados a la entrada.

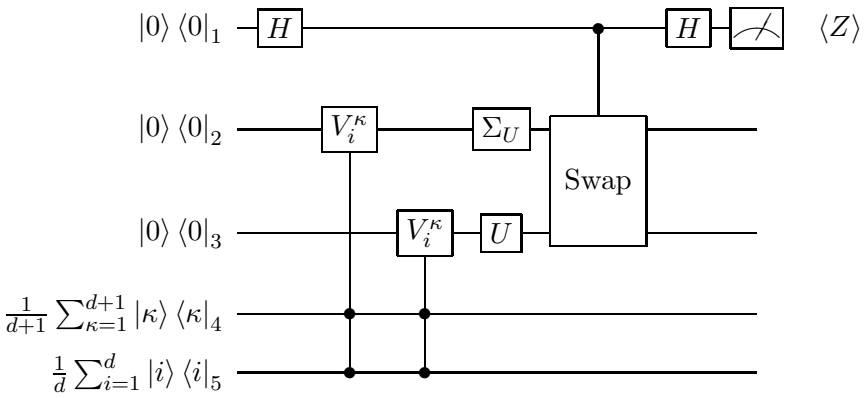

Figura 5.5: *Segundo circuito para la medición de la fidelidad media. Midiendo el valor medio de Z a la salida, se obtiene el valor de la fidelidad media.*

Analizaremos ahora el funcionamiento del circuito 5.5. Para eso llamaremos $\rho_T(t_j)$ al operador densidad de todo el sistema que atraviesa el circuito, luego de realizados j pasos del circuito. De esta forma $\rho_T(t_0)$ es el estado inicial, y $\rho_T(t_6)$ es el estado en el instante anterior a la medición. El estado inicial del circuito está dado por el producto tensorial de los estados individuales, comenzando, de acuerdo al circuito, de arriba hacia abajo:

$$\rho_T(t_0) = \frac{1}{d(d+1)} \sum_{\kappa=1}^{d+1} \sum_{i=1}^{d} |0\rangle\langle 0|_1 \otimes |0\rangle\langle 0|_2 \otimes |0\rangle\langle 0|_3 \otimes |\kappa\rangle\langle\kappa|_4 \otimes |i\rangle\langle i|_5 \quad (5.31)$$

Luego de atravesar todo el circuito, pero previo a la aplicación de la última compuerta de Hadamard, el estado del sistema se convierte en:

$$\begin{aligned}\rho'_T(t_5) = \frac{1}{2d(d+1)} \sum_{k} \sum_{\kappa=1}^{d+1} \sum_{i=1}^{d} \Big(& |0\rangle\langle 0|_1 \otimes A_k |\psi_i^\kappa\rangle\langle\psi_i^\kappa|_2 A_k^\dagger \otimes U|\psi_i^\kappa\rangle\langle\psi_i^\kappa|_3 U^\dagger + \\ & |0\rangle\langle 1|_1 \otimes A_k |\psi_i^\kappa\rangle\langle\psi_i^\kappa|_2 U^\dagger \otimes U|\psi_i^\kappa\rangle\langle\psi_i^\kappa|_3 A_k^\dagger + \\ & |1\rangle\langle 0|_1 \otimes U |\psi_i^\kappa\rangle\langle\psi_i^\kappa|_2 A_k^\dagger \otimes A_k|\psi_i^\kappa\rangle\langle\psi_i^\kappa|_3 U^\dagger + \\ & |1\rangle\langle 1|_1 \otimes U |\psi_i^\kappa\rangle\langle\psi_i^\kappa|_2 U^\dagger \otimes A_k|\psi_i^\kappa\rangle\langle\psi_i^\kappa|_3 A_k^\dagger \Big) \quad (5.32)\end{aligned}$$

donde el primado corresponde a que se tomó traza parcial sobre los últimos dos registros por no ser necesarios para el resto del cálculo.

El último Hadamard seguido por una medición en Z es equivalente a medir en X sin realizar dicha transformación. Por lo tanto, el resultado de la medición que se realiza en el circuito es $\mathrm{Tr}\left(\rho'_T\left(t_5\right)X_1\right)$:

$$\mathrm{Tr}\left(\rho'_T\left(t_5\right)X_1\right)=\frac{1}{2d\left(d+1\right)}\mathrm{Tr}\sum_k\sum_{\kappa=1}^{d+1}\sum_{i=1}^{d}\Big(A_k\left|\psi_i^\kappa\right\rangle\left\langle\psi_i^\kappa\right|_2U^\dagger\otimes U\left|\psi_i^\kappa\right\rangle\left\langle\psi_i^\kappa\right|_3A_k^\dagger+ U\left|\psi_i^\kappa\right\rangle\left\langle\psi_i^\kappa\right|_2A_k^\dagger\otimes A_k\left|\psi_i^\kappa\right\rangle\left\langle\psi_i^\kappa\right|_3U^\dagger\Big) \quad (5.33)$$

Pero puesto que la traza es lineal, y la traza de ambos sumandos dentro del paréntesis es la misma, se obtiene que:

$$\mathrm{Tr}\left(\rho'_T\left(t_5\right)X_1\right)=\frac{1}{d\left(d+1\right)}\mathrm{Tr}\sum_k\sum_{\kappa=1}^{d+1}\sum_{i=1}^{d}\Big(A_k\left|\psi_i^\kappa\right\rangle\left\langle\psi_i^\kappa\right|_2U^\dagger\otimes U\left|\psi_i^\kappa\right\rangle\left\langle\psi_i^\kappa\right|_3A_k^\dagger\Big) \quad (5.34)$$

lo que es igual a

$$\mathrm{Tr}\left(\rho'_T\left(t_5\right)X_1\right)=\frac{1}{d\left(d+1\right)}\sum_{\kappa=1}^{d+1}\sum_{i=1}^{d}\left\langle\psi_i^\kappa\right|U^\dagger\Sigma_U\left(\left|\psi_i^\kappa\right\rangle\left\langle\psi_i^\kappa\right|\right)U\left|\psi_i^\kappa\right\rangle \quad (5.35)$$

que es precisamente la fidelidad media buscada. Por lo tanto, el circuito propuesto mide la fidelidad media.

Respecto de la eficiencia de este circuito, las consideraciones son similares a aquellas del circuito anterior; puesto que el valor medio de una medición de valores aleatorios es la fidelidad media, la cantidad de mediciones necesaria para obtener la fidelidad con una desviación estándar ν obedecerá:

$$N\propto\frac{1}{\nu^2} \quad (5.36)$$

donde N es la cantidad de mediciones necesarias. Como N es independiente del número de qubits, el circuito es eficiente.

5.5. Peso de los operadores de Pauli en canales cuánticos ruidosos

Hemos visto que la fidelidad media da, en el caso de una memoria cuántica, el peso que tiene el operador identidad en el canal cuántico que se está utilizando. Surge entonces la pregunta acerca del peso que tienen los demás operadores de Pauli en dicho canal. A ese problema se dedicará la presente sección.

La determinación del peso de los distintos operadores de Pauli resulta de importancia ya que permite, entre otras cosas, determinar el tipo de corrección de errores necesario para un cierto canal. Por ejemplo, si se detecta que en una memoria tienen mucho peso los operadores de Pauli de un qubit, será necesario utilizar un código de corrección de errores acorde.

Por otra parte, el estudio del peso de los distintos operadores de Pauli de un canal da una caracterización más completa del mismo que sólo el peso de la identidad.

Se presentará la definición del peso de un operador de Pauli en un canal, así como del peso de un conjunto de operadores de Pauli dados. Junto con eso se mostrarán dos circuitos distintos para la medición del peso de un conjunto de operadores de Pauli.

5.5.1. Peso de los operadores de Pauli en un canal cuántico

Como fue mostrado en la sección 5.3.2, el peso Ω_1 de la identidad en un canal cuántico dado es igual a la fidelidad media, y es de la forma:

$$\Omega_1 = \int_{F-S} \langle\psi| \Sigma\left(|\psi\rangle \langle\psi|\right) |\psi\rangle \, d\,|\psi\rangle \tag{5.37}$$

donde $\Sigma(\rho) = \sum_k A_k \rho A_k^\dagger$ es la operación cuántica asociada al canal cuántico en cuestión, y A_k sus operadores de Kraus.

Basado en esto, se define el peso Ω_P de un operador de Pauli P como:

$$\Omega_P = \int_{F-S} \langle\psi| P\Sigma\left(|\psi\rangle \langle\psi|\right) P\,|\psi\rangle \, d\,|\psi\rangle \tag{5.38}$$

La propiedad que se enunciará a continuación sirve para comprender en qué sentido Ω_P corresponde al peso del operador P en el canal.

Propiedad 5.5.1. *Sea un canal cuántico definido por:*

$$\Sigma(\rho) = \sum_k A_k \rho A_k^\dagger \tag{5.39}$$

donde, en el caso más general, cada operador de Kraus A_k es una combinación lineal de operadores de Pauli generalizados:

$$A_k = \sum_P \alpha_P^{(k)} P \tag{5.40}$$

Se cumple que Ω_P definido en (5.38) es tal que:

$$\Omega_P = \frac{1}{d+1}\left(1 + d\sum_k \left|\alpha_P^{(k)}\right|^2\right) \tag{5.41}$$

La demostración de dicha propiedad es similar a la que se da en la sección 5.3.2, utilizando que el cuadrado de cualquier operador de Pauli generalizado es la identidad.

Conociendo el peso de los distintos operadores de Pauli de un canal es posible determinar el tipo de corrección de errores que se debe implementar para que siga funcionando como memoria. En general, resulta conveniente conocer el peso de un conjunto de operadores de Pauli en un canal para determinar el código de corrección de errores adecuado. Por ejemplo, si predominan los operadores de Pauli de un qubit, es necesario corregir errores de un qubit. En la siguiente sección veremos una definición adecuada para el peso de un conjunto de operadores de Pauli dado.

5.5.2. Peso de un conjunto de operadores de Pauli en un canal cuántico

Se quiere conocer el peso $\underline{\Omega}_B$ de un conjunto de operadores de Pauli $B = \{P_1, P_2, \cdots\}$ en un canal cuántico definido por una operación Σ. Para eso, mostraremos que es conveniente definirlo como:

$$\underline{\Omega}_B = \frac{(d+1)\sum_{P' \in B} \Omega_{P'} - \#B}{d} \tag{5.42}$$

donde $\#B$ es el cardinal del conjunto B.

Propiedad 5.5.2. *Sea un canal cuántico definido por una operación $\Sigma(\rho) = \sum_k A_k \rho A_k^\dagger$, donde los operadores de Kraus A_k admiten un desarrollo como combinación lineal de operadores de Pauli:*

$$A_k = \sum_P \alpha_P^{(k)} P \tag{5.43}$$

donde la suma recorre todos los operadores de Pauli, pero se admite que algunos coeficientes sean nulos.

Entonces vale que:

$$\underline{\Omega}_B = 1 - \sum_k \sum_{P' \notin B} \left|\alpha_{P'}^{(k)}\right|^2 \tag{5.44}$$

Demostración. Reemplazando (5.41) en (5.42), y utilizando que $\sum_k A_k^\dagger A_k = 1$ es equivalente a $\sum_k \sum_P \left|\alpha_P^{(k)}\right|^2 = 1$, se obtiene sin complicaciones la ecuación (5.44). □

Es importante notar que cuando el número de qubits se hace grande y el conjunto B posee sólo a la identidad, $\underline{\Omega}_B$ tiende a la fidelidad media de

una memoria. Por lo tanto, esta caracterización del peso de los operadores de Pauli sirve también para determinar la fidelidad de un canal cuántico.

5.5.3. Peso de los errores de Pauli en un algoritmo cuántico

Una extensión natural de lo expuesto anteriormente, consiste en la determinación del peso de ciertos errores de Pauli en un algoritmo cuántico.

Supongamos un algoritmo cuántico U, cuyos operadores de Kraus están dados por:

$$A_k = \sum_P \alpha_P^{(k)} PU \tag{5.45}$$

Es decir, la implementación del algoritmo aplica U y a continuación, con ciertas probabilidades, aplica errores. Resulta de interés, entonces, determinar el peso de cada error de Pauli para poder elegir un código de corrección de errores adecuado.

Con dicho fin se define el peso Ω'_P de un error de Pauli P, en analogía con las ecuaciones (5.38) y (5.4) como:

$$\Omega'_P = \int_{F-S} \langle\psi| U^\dagger P \Sigma_U \left(|\psi\rangle \langle\psi|\right) PU |\psi\rangle \, d|\psi\rangle \tag{5.46}$$

donde el primado corresponde a diferenciar éste Ω'_P de los Ω_P definidos para la memoria cuántica.

Se define, además, el peso de los errores asociados a un conjunto B de operadores de Pauli generalizados, de acuerdo a (5.42) como:

$$\underline{\Omega'}_B = \frac{(d+1)\sum_{P' \in B} \Omega'_{P'} - \#B}{d} \tag{5.47}$$

Puede verse que (5.47) se reduce al caso de la memoria cuántica dado en la sección 5.5.2 cuando $U = 1$. Además, se puede demostrar de manera similar a la expuesta en la sección 5.5.2 que:

$$\underline{\Omega'}_B = 1 - \sum_k \sum_{P' \notin B} \left|\alpha_{P'}^{(k)}\right|^2 \tag{5.48}$$

Se ve en (5.48) que si el conjunto B posee todos los operadores de Pauli que aparecen en los operadores de Kraus, entonces $\underline{\Omega'}_B = 1$. La utilidad, al igual que en el caso de la memoria cuántica, es determinar si corrigiendo ciertos errores de Pauli contenidos en el conjunto B, se consigue acercar $\underline{\Omega'}_B$ a 1 tanto como se requiere para una implementación suficientemente buena de U. De ahí que se puede utilizar para determinar el código de corrección de errores necesario.

5.6. Circuitos para la medición del peso de un conjunto de errores de Pauli

La medición del peso de los errores de Pauli constituye una herramienta de suma importancia, en tanto que permite caracterizar un canal cuántico y determinar un código de corrección de errores [16][20][21] adecuado para la implementación de un algoritmo cuántico U dado.

Es decir, se puede medir el peso de la identidad y si el resultado obtenido no satisface los requerimientos de fidelidad, se repite el procedimiento para un conjunto B que contenga, además de la identidad, a los $3n$ operadores de Pauli de un qubit. Sí al medir el peso de los errores de un qubit junto con la identidad sí se alcanza un valor satisfactorio (suficientemente cercano a 1), eso indica que un código de corrección de errores capaz de corregir errores de un qubit es suficiente. En caso contrario, se puede medir el peso para un conjunto de operadores B que contenga, además de los anteriores, a todos los posibles errores de dos qubits, y así sucesivamente.

Se presentan, con dicho fin, dos circuitos derivados de los presentados en la sección 5.4 para la medición del peso de un conjunto de operadores de Pauli definido en la ecuación (5.47). Vale notar que para el caso de memorias cuánticas, basta con utilizar los mismos circuitos que se mostrarán a continuación con $U = 1$.

5.6.1. Primer circuito

El primer circuito es una generalización directa de aquel presentado en la sección 5.4.1. Es importante notar, en primer lugar, que dada la definición del peso de los errores de la ecuación (5.47), sólo es necesario medir eficientemente el valor de $\sum_{P' \in B} \Omega'_P$, puesto que el resto de los valores involucrados son constantes conocidas, como la dimensión del espacio de Hilbert del sistema, y la cantidad de errores distintos cuyos pesos se desea medir.

El problema se reduce a la medición de $\sum_{P \in B} \Omega'_P$. Pero cada uno de los sumandos Ω'_P de $\sum_{P \in B} \Omega'_P$ es de la forma:

$$\Omega'_P = \int_{F-S} \langle\psi| U^\dagger P \Sigma_U \left(|\psi\rangle \langle\psi|\right) PU |\psi\rangle \; d|\psi\rangle \tag{5.49}$$

Es decir, es una fidelidad media $\overline{F}\left(PU, \Sigma_U\right)$. Y en la sección 5.4.1 fue presentado un circuito para medir fidelidades medias. En efecto, el circuito de la figura 5.6 sirve para medir eficientemente cada uno de los sumandos de Ω'_P.

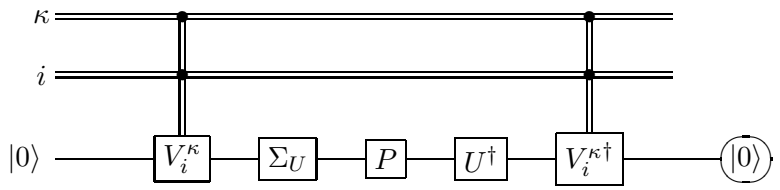

Figura 5.6: *Circuito cuántico para la medición de los sumandos Ω'_P necesarios para la medición de los errores correspondientes a los operadores de Pauli de un conjunto B dado. La variable κ recorre los valores del 1 al $d+1$ aleatoriamente para recorrer las bases del conjunto de bases no sesgadas, mientras que i va, también aleatoriamente, del 1 a d para recorrer los estados de dichas bases. La probabilidad de encontrar $|0\rangle$ a la salida corresponde al sumando Ω'_P.*

Sin embargo, se busca la suma de los distintos Ω'_P sobre todos los operadores P que pertenecen al conjunto B. Resulta sencillo promediar sobre todos ellos mediante una leve variante del circuito 5.6 que incluya un nuevo canal clásico. Dicho canal debe controlar, mediante un valor tomado clásicamente al azar, cual de todos los operadores de Pauli generalizados pertenecientes al conjunto B es el que actúa en cada pasada del circuito. En la figura 5.7 se muestra el circuito en cuestión.

Puesto que se busca la suma, y no el promedio, el circuito tendrá un leve perjuicio en la eficiencia. Obtener una desviación de ν en la suma es equivalente a requerir una desviación de $\nu/\#B$ en el promedio. Por lo tanto, el número N de experimentos necesarios, dada una desviación estándar ν será de la forma:

$$N \propto \left(\frac{\#B}{\nu}\right)^2 \tag{5.50}$$

5.6.2. Segundo circuito

La modificación del circuito dado en la sección 5.4.2 para medir el peso de los errores de un conjunto de operadores de Pauli, se realiza de manera similar a la realizada para el circuito 5.4.1 en la sección anterior. En primer lugar, debe agregarse un nuevo canal que funcione como índice sobre los operadores de Pauli generalizados del conjunto B. Además, debe reemplazarse la aplicación del algoritmo cuántico U por PU, en tanto que, como se ha mostrado en la sección anterior, cada sumando Ω'_P es, en sí mismo, una fidelidad media de un algoritmo PU con implementación Σ_U.

En la figura 5.8 se muestra el circuito que se utiliza para la determinación

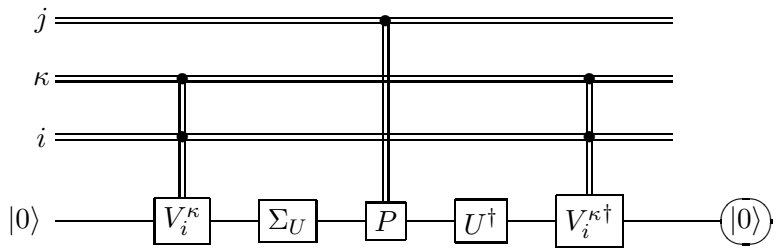

Figura 5.7: *Circuito cuántico para la medición del peso correspondiente a un conjunto de errores de Pauli. Se agrega al circuito 5.6 un registro para recorrer aleatoriamente los operadores del conjunto B. Si bien el circuito no mide el peso sino $\sum_{P'\in B}\Omega'_P/\#B$, puede, a partir de dicha magnitud, computarse sencillamente.*

de $\sum_{P'\in B}\Omega'_P$ y, mediante simples cálculos clásicos, el peso del error, definido en la ecuación (5.47).

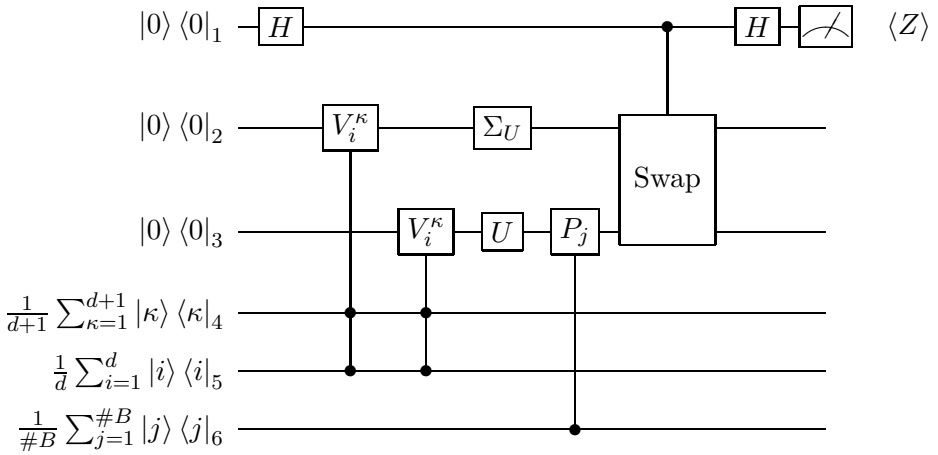

Figura 5.8: *Segundo circuito para la medición del peso de los errores asociados a un conjunto de operadores de Pauli. Midiendo el valor medio de Z a la salida, se obtiene el valor de $\sum_{P'\in B}\Omega'_P/\#B$ mediante el que se salcula el peso de los errores en cuestión. El último canal recorre el índice de los operadores de Pauli generalizados del conjunto B.*

Al igual que en el caso de la fidelidad media, el registro agregado es un registro máximamente mixto, es decir, es un canal de ruido. Esto tiene suma importancia a la hora de producir el estado inicial de dicho canal, en tanto que no consume recursos cuánticos.

Puede verse, asímismo, que las consideraciones sobre la eficiencia tomadas para el circuito de la sección 5.6.1 son válidas para este circuito.

5.7. Conclusiones parciales

Se presentó, en este capítulo, la noción de fidelidad media como distancia entre un algoritmo cuántico y su implementación defectuosa, de acuerdo con [15]. Además, se mostró el circuito allí presentado para la determinación de la fidelidad media.

Luego se presentó un circuito nuevo para dicha medición que, a diferencia del de [15] no requiere la utilización de canales clásicos, y que mantiene la eficiencia del primero.

En la segunda parte del capítulo se encontró una manera de generalizar el concepto de fidelidad media para determinar el peso de un conjunto de errores del tipo de los de Pauli en un canal cuántico ruidoso. Dicha generalización permite determinar un código de corrección de errores adecuado, sin la necesidad de implementarlo para medir su fidelidad.

Asímismo, se presentaron dos circuitos que permiten determinar el peso de un conjunto de errores de manera eficiente. Ambos constituyen una herramienta fundamental para la implementación de algoritmos cuánticos.

Ésta parte del trabajo sobre el peso de los errores asociados a un conjunto de operadores de Pauli dado es, probablemente, la más importante del presente trabajo, y constituye un pie de apoyo para investigaciones futuras.

Capítulo 6

Conclusiones

Las bases mutuamente no sesgadas constituyen una herramienta fundamental en varias areas de estudio dentro de la mecánica cuántica. En particular, resultan de suma utilidad en diversas aplicaciones, que van de la tomografía de estados cuánticos, a la medición de la fidelidad de un canal cuántico ruidoso, pasando por la representación de estados en los espacios de fases discretos.

En el capítulo 2 de este trabajo se comenzó por estudiar propiedades de dichos conjuntos de bases para sistemas de qubits. Se mostró que existe una relación estrecha entre los conjuntos de bases mutuamente no sesgadas y las particiones del grupo de Pauli en subgrupos conmutativos máximos, mediante la utilización del formalismo de los estabilizadores. Asimismo, a partir de dicha relación, se encontró que los conjuntos de bases no sesgadas están asociados a conjuntos de matrices binarias, simétricas y no singulares (una por base), tales que la suma de cualquier par no es singular. Además, se formuló un algoritmo eficiente que permite generar circuitos eficientes de cambio de base entre bases de un conjunto de bases no sesgadas. Dicho algoritmo, de complejidad clásica del orden de n^3, genera circuitos que utilizan del orden de n^2 compuertas cuánticas.

Luego, en el capítulo 3 se introdujo una variante de la función de Wigner para sistemas de dimensión p^n, con p primo. Notablemente, esta función de Wigner discreta posee una relación simbiótica con los conjuntos de bases mutuamente no sesgadas del capítulo 2, en tanto que se definen los estados línea a partir de los estados de un conjunto de bases mutuamente no sesgadas. Asímismo, se dejó abierto el problema acerca de algoritmos eficientes para la medición de dicha función de Wigner, para el que se establecieron dos posibles caminos para un futuro trabajo.

Además, se mostró que, si bien para menos de cinco qubits todo conjunto

de bases mutuamente no sesgadas puede utilizarse para definir un espacio de fases, a partir de cinco qubits esto no es cierto, ya que existen conjuntos de bases mutuamente no sesgadas que no se corresponden con ningún espacio de fases con covariancia traslacional. Esto es, conjuntos de bases mutuamente no sesgadas que no son colineales en ningún espacio de fases que se pueda definir.

Por último, a partir de la definición de fidelidad media dada en [15] y el circuito para su medición allí presentado, se encontró un circuito alternativo para dicha tarea. Además, se redefinió la noción de fidelidad media para el caso en el que se desea medir el peso de ciertos errores, en particular. Junto con dicha definición, se encontraron circuitos eficientes para su medición. Esto último constituye una herramienta fundamental, quizás la más importante de las presentadas en éste trabajo, ya que permitiría determinar el tipo de corrección de errores requerido por una implementación defectuosa de un algoritmo cuántico para alcanzar una fidelidad deseada.

Apéndice A

Los qubits y la base computacional

Así como en computación clásica la unidad b;asica de información es el bit, que puede tomar como valores al 0 o al 1, en computación cuántica se define su análogo cuántico denominado *qubit*.

El qubit es, físicamente, cualquier sistema de dos niveles; es decir, un sistema cuyo espacio de Hilbert tiene dimensión 2. Se define, para ese sistema una base de estados $B_2 = \{|0\rangle, |1\rangle\}$ y operadores de Pauli que, en esa base, están dados por las matrices:

$$\begin{aligned} \sigma_x &= \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ \sigma_y &= \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\ \sigma_z &= \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ 1 &= \sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned} \tag{A.1}$$

En otras palabras, la base de estados $B_2 = \{|0\rangle, |1\rangle\}$, o base computacional de un qubit, es la base de autoestados del operador σ_z.

Cuando el sistema está compuesto por n qubits, su espacio de Hilbert tiene dimensión 2^n. Se define, en ese caso, la base computacional B_{2^n} como:

$$B_{2^n} = B_2^{\otimes n} \tag{A.2}$$

Dicha base está compuesta, por lo tanto, por los estados correspondiente a todas las n-uplas binarias. Así, B_4 y B_8 quedan definidas como:

$$\begin{aligned} B_4 &= \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\} \\ B_8 &= \{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\} \end{aligned} \tag{A.3}$$

Puesto que cada n-upla binaria corresponde a un número natural entre 0 y 2^n expresado en base 2, suelen etiquetarse los estados de la base computacional mediante el número decimal correspondiente a la expresión binaria dada en (A.3). De esta forma:

$$B_{2^n} = \{|i\rangle ; 0 \leq i < 2^n\} \tag{A.4}$$

Asímismo, se sobreentiende que el estado $|k\rangle$ debe leerse considerando el resto de la división de k por la dimensión del espacio de Hilbert en cuestión.

La base computacional de n qubits es, entonces, la base de autoestados comunes a todos los operadores formados por productos tensoriales de n operadores σ_z o 1, como los definidos en la ecuación (A.1).

Apéndice B

Los operadores de Pauli generalizados

Las matrices de Pauli, junto con la identidad, exhibidas en la ecuación (A.1) forman una base real de los operadores hermíticos, y una base compleja de todos los operadores lineales. Dichas matrices, fundamentales para los formalismos de la mecánica cuántica y, en particular, de la computación cuántica poseen las siguientes propiedades:

- A excepción de la identidad, tienen traza nula.
- Son matrices hermíticas.
- Cada una, salvo la identidad, posee un autovalor 1 y un autovalor -1.
- Son matrices unitarias.
- El producto de dos de éstas matrices da otra de ellas multiplicada por una fase. Más precisamente:

$$\sigma_j \sigma_k = i\epsilon_{jkl}\sigma_l + \delta_{j,k} \tag{B.1}$$

  donde los subíndices j, k y l pueden tomar valores 1, 2 o 3, y ϵ_{jkl} es el tensor de Levi-Civita.

- Toda matriz de Pauli distinta de la identidad conmuta con la identidad y con sí misma, y anticonmuta con todas las demás matrices de Pauli.
- Además, puede probarse mediante la primera y cuarta propiedad, que las matrices de Pauli junto con la identidad forman un conjunto ortogonal en el producto interno de operadores usual, o de Schmidt:

$$\mathrm{Tr}\left(\sigma_j \sigma_k\right) = 2\delta_{j,k} \tag{B.2}$$

Por lo tanto, y mediante el analisis de la dimensión del espacio vectorial real de los operadores hermíticos y la dimensión del espacio vectorial complejo de operadores lineales, se ve que los operadores de Pauli son una base de ambos espacios.

En computación cuántica, además, suelen notarse las matrices de Pauli como:

$$\begin{aligned} \sigma_0 &= 1 \\ \sigma_1 &= X \\ \sigma_2 &= Y \\ \sigma_3 &= Z \end{aligned} \tag{B.3}$$

Dados dos vectores fila binarios $\vec{a}$ y $\vec{b}$ de dimensión n, se define el operador de Pauli generalizado $\sigma_{\vec{a},\vec{b}}$ como:

$$\sigma_{\vec{a},\vec{b}} = \prod_{i=1}^{n} X_i^{a_i} Z_i^{b_i} e^{i\frac{\pi a_i b_i}{2}} = X^{\vec{a}} Z^{\vec{b}} e^{i\frac{\pi \vec{a}\cdot\vec{b}}{2}} \tag{B.4}$$

donde el subíndice en X y Z se refiere al qubit sobre el que actúa el operador en cuestión.

Es decir, los operadores de Pauli generalizados son operadores que corresponden a un operador de Pauli actuando sobre cada qubit. Se utilizan, en computación cuántica, distintas notaciones para los operadores de Pauli. Dos que se utilizan en el presente trabajo y que quedan claras según el contexto son, una identificando el qubit sobre el que actúa cada operador con un subíndice, como $X_1Y_3Z_2Y_5$. Otra, identificando el qubit sobre el que actúa cada operador por la posición en el producto de operadores. Así, el operador $X \otimes Z \otimes Y \otimes 1 \otimes Y$ es el mismo del ejemplo anterior para un sistema de cinco qubits.

Los operadores de Pauli generalizados poseen, al igual que los operadores de Pauli, ciertas propiedades:

- Son hermíticos.
- Son unitarios.
- Sus autovalores son 1 y -1.
- A excepción de la identidad, poseen traza nula.
- El producto de dos operadores de Pauli generalizados es otro operador de Pauli generalizado, a menos de una fase. El conjunto de operadores de Pauli generalizados con fases conforma un grupo.

- Todo par de operadores de Pauli generalizados conmuta o anticonmuta. En efecto, dos operadores $\sigma_{\vec{a},\vec{b}}$ y $\sigma_{\vec{c},\vec{d}}$ verifican que:

$$\begin{array}{rcl} \left[\sigma_{\vec{a},\vec{b}}, \sigma_{\vec{c},\vec{d}}\right] & = & 0 \qquad \text{si} \quad \vec{a}\cdot\vec{d} - \vec{c}\cdot\vec{b} = 0 \pmod 2 \\ \left\{\sigma_{\vec{a},\vec{b}}, \sigma_{\vec{c},\vec{d}}\right\} & = & 0 \qquad \text{si} \quad \vec{a}\cdot\vec{d} - \vec{c}\cdot\vec{b} = 1 \pmod 2 \end{array} \tag{B.5}$$

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

B.1. Grupos y subgrupos de Pauli

Fue mencionado anteriormente en qué sentido se dice que los operadores de Pauli son un grupo. Estrictamente, son un grupo si se los considera junto con aquellos operadores que tienen, además, una fase ± 1 o $\pm i$. Sin embargo, a lo largo del presente trabajo se omitirá ese detalle y se dirá, por ejemplo, que los operadores X, Y y Z forman un grupo, aunque estrictamente se requiera que haya más operadores en el conjunto.

Apéndice C

La función de Wigner de $2d \times 2d$ para sistemas discretos

Cuando la dimensión del espacio de Hilbert es d, no resulta tan sencillo hablar de un espacio de fases. Existen, al respecto, distintas propuestas de *funciones de Wigner discretas* que, al igual que en el caso continuo, poseen la particularidad de ser pseudodistribuciones de probabilidad.

Una de ellas es la presentada por Bianucci, Miquel, Paz y Saraceno en [26], que resulta extremadamente útil para la visualización e interpretación de estados cuánticos [10]. Asimismo, se conocen para dicha función de Wigner algoritmos eficientes que permiten realizar tomografía cuántica [27], es decir, medir el valor de la función de Wigner en un punto sin necesidad de conocer completamente el estado.

En este apéndice se presenta dicha función de Wigner, junto con algunas propiedades importantes y algoritmos eficientes para su medición, de acuerdo con [27]. No se hará hincapié en detalles, en tanto que es presentada a efectos de ser comparada con la función de Wigner que se dada en la sección 3.2, y no constituye un componente central del presente trabajo.

C.1. El espacio de fases

Una manera de generalizar la noción de espacio de fases obtenida para el caso continuo al discreto, es mediante la introducción de una base y su base conjugada, equivalentes a la posición y el momento del caso continuo, relacionadas ambas por la transformada de Fourier discreta.

Sea, entonces, una base que será considerada la discretización de la base

de posiciones:

$$B_q = \left\{ |j\rangle_q \, ; j = 0, .., d-1 \right\} \tag{C.1}$$

y su base conjugada mediante la transformada discreta de Fourier:

$$B_p = \left\{ |k\rangle_p = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{\frac{2\pi i j k}{d}} |j\rangle_q \, ; k = 0, ..., d-1 \right\} \tag{C.2}$$

A partir de estas bases, es natural pensar los operadores de traslación en posición U como:

$$U^m |j\rangle_q = |j+m\rangle_q \tag{C.3}$$

donde la suma está calculada módulo d.

Asímismo, la traslación en momento V es tal que:

$$V^m |k\rangle_p = |k+m\rangle_p \tag{C.4}$$

Puede mostrarse, además, que la traslación en posición es diagonal en momento y viceversa. Es decir:

$$\begin{aligned} U^m |k\rangle_p &= e^{-\frac{2\pi i m k}{d}} |k\rangle_p \\ V^m |j\rangle_q &= e^{\frac{2\pi i m j}{d}} |j\rangle_q \end{aligned} \tag{C.5}$$

A partir de estos operadores, es posible construir un análogo del operador de traslación continuo para el caso discreto mediante el producto de potencias de U con potencias de V. Pero para mantener la analogía con el caso continuo, que se puede ver en la ecuación (3.8), se debe agregar a dichos operadores una fase adicional:

$$T(q,p) = U^q V^p e^{\frac{i\pi qp}{d}} \tag{C.6}$$

donde se pidió que el espacio de fases tenga area unitaria y que cada estado de los d ortogonales que ocupan todo el espacio ocupe un area $2\pi\hbar$.

Estos operadores obedecen ciertas propiedades requeridas a operadores de traslación:

- La composición de dos traslaciones da una nueva traslación, cuya cantidad trasladada es la suma de ambas, a menos de una fase:

$$T(q_1,p_1)\, T(q_2,p_2) = T(q_1+q_2, p_1+p_2)\, e^{i\pi \frac{p_1 q_2 - q_1 p_2}{d}} \tag{C.7}$$

- El operador conjugado hermítico de una traslación corresponde a una traslación en sentido opuesto:

$$T^{\dagger}(q,p) = T(2d-q, 2d-p) = T(d-q, d-p)(-1)^{N+p+q} \qquad \text{(C.8)}$$

Sobre éste punto son importantes algunas aclaraciones. En primer término notar que la segunda igualdad muestra que, en efecto, sobre una grilla de $d \times d$ (recordemos que los operadores de traslación son cíclicos módulo d), la conjugada hermítica de una traslación corresponde a una traslación en sentido opuesto con, a lo sumo, un signo de diferencia. La primera igualdad, en cambio, afirma que conjugar hermíticamente una traslación da una traslación opuesta en una grilla de $2d \times 2d$. Puede parecer, a primera vista, que ambas igualdades dicen lo mismo al trabajar módulo d; sin embargo, ese signo de diferencia entre ambas sugiere que los operadores de traslación se comportan adecuadamente en una grilla de $2d \times 2d$, siendo ésta la adecuada para describir al espacio de fases. A pesar de eso, como se verá a continuación, bastará con observar un cuadrante de dicha grilla para obtener información completa sobre el estado.

C.2. La función de Wigner discreta

La forma más directa de generalizar la función de Wigner continua al caso discreto, es a partir de la expresión para los operadores de punto dada en (3.9). Con eso, y mediante la definición de las traslaciones discretas, es tentador definir los operadores de punto discretos como:

$$A(q,p) = \frac{2}{d} T(q,p) R T^{\dagger}(q,p) = \frac{1}{d} U^{2q} R V^{-2p} e^{\frac{4\pi i p q}{d}} \qquad \text{(C.9)}$$

donde R es el operador que actúa como $R|j\rangle_q = |d-j\rangle_q$.

Sin embargo, estos operadores tienen el inconveniente de no ser hermíticos, por lo que la función de Wigner definida a partir de ellos no sería real. La solución a este problema es utilizar una grilla de $2d \times 2d$ y los operadores de punto:

$$A(p,q) = \frac{1}{2d} U^{q} R V^{-p} e^{\frac{\pi i q p}{d}} \qquad \text{(C.10)}$$

De ésta forma se obtiene una base de los operadores hermíticos, aunque sobredimensionada, puesto que hay $2d \times 2d = 4d^2$ puntos distintos. Pero esto no representa ningún problema en tanto que la información completa sobre el estado estará contenida en el primer cuadrante, y que la de los otros

tres será redundante debido a que sumar d a cualquiera de las coordenadas, o ambas, da el mismo operador de punto a menos de un signo.

Estos operadores de punto definidos en (C.10) poseen algunas propiedades análogas a las vistas para los operadores de punto del caso continuo. En primer término, son hermíticos, lo que garantiza que la función de Wigner que se definirá sea real. Y, más importante, se recupera una propiedad fundamental de los operadores de punto, el subconjunto de d^2 operadores de punto definidos en el primer cuadrante ($p, q \in \{0, ..., d-1\}$) es ortogonal:

$$\mathrm{Tr}\left(A\left(q,p\right)A\left(q',p'\right)\right) = \frac{1}{4d}\delta_d\left(q'-q\right)\delta_d\left(p'-p\right) \tag{C.11}$$

donde tanto (q,p) como (q',p') pertenecen al primer cuadrante, y la función δ_d es cero en todos los puntos, menos cuando su argumento es congruente a 0 módulo d. Por lo tanto, sí vale ahora que cualquier matriz densidad (y cualquier operador hermítico) puede desarrollarse como combinación lineal de operadores de punto.

La función de Wigner en un punto se define, al igual que en el caso continuo, como el valor medio del operador del punto en cuestión; es decir:

$$W\left(q,p\right) = \mathrm{Tr}\left(A\left(q,p\right)\rho\right) \tag{C.12}$$

Sin embargo, puesto que los operadores de punto son casi cíclicos módulo d (puede haber una diferencia en un signo), también lo será la función de Wigner. Por ese motivo existen distintas maneras de recuperar el estado original a partir de su función de Wigner. Si se considera sólo el primer cuadrante, se tiene que:

$$\rho = 4d\sum_{q,p=0}^{d-1} W\left(q,p\right)A\left(q,p\right) \tag{C.13}$$

en cambio, si se suma sobre toda la grilla, se estará sumando cuatro veces más que en el caso anterior, por lo que se obtiene que:

$$\rho = d\sum_{q,p=0}^{2d-1} W\left(q,p\right)A\left(q,p\right) \tag{C.14}$$

La función de Wigner así definida cumple con dos de las propiedades esperadas para una función de Wigner:

- Es real, puesto que los operadores de punto son hermíticos.

- Vale que el solapamiento de dos estados se obtiene como:

$$\mathrm{Tr}\left(\rho_1\rho_2\right) = N\sum_{q,p=0}^{2d-1} W_1\left(q,p\right)W_2\left(q,p\right) \tag{C.15}$$

Sólo falta ver que sumando sobre lineas la función de Wigner se obtiene la probabilidad de medir un cierto valor a un observable. Equivalentemente, puede mostrarse que la suma de los operadores de punto sobre una linea da un proyector asociado al resultado del observable mencionado. Puede mostrarse, como está realizado en [27] que la suma de los operadores de punto de la forma $n_1p - n_2q = n_3$, donde los coeficientes n_i son números enteros entre 0 y $2d-1$ es un proyector sobre uno de los autoestados del operador de traslación $T\left(n_1,n_2\right)$.

C.3. Medición de la función de Wigner

Veremos ahora el circuito eficiente para medir la función de Wigner en un punto dado presentado en [32]. Si bien dicho circuito es de gran importancia para todos los problemas referidos a espacios de fases discretos, se hará un breve repaso del mismo puesto que, en el presente trabajo, sólo se utilizará para contrastar con el caso de las funciones de Wigner que se presentarán en 3.2.

En el trabajo mencionado, se presenta un circuito que permite medir el valor medio de cualquier operador A unitario. Y, puesto que los operadores de punto pueden construirse mediante traslaciones y reflexiones, son unitarios y pueden medirse mediante el circuito allí presentado. El circuito en cuestión se puede observar en la figura C.1. El operador $\mathrm{Ctrl}-\mathrm{A}$ actúa como $\mathrm{Ctrl}-\mathrm{A}\left|j\right\rangle\left|\psi\right\rangle = \left|j\right\rangle A^j\left|\psi\right\rangle$.

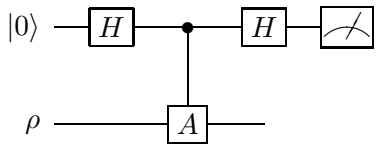

Figura C.1: *Circuito para medir el valor medio de un operador unitario A. Midiendo σ_z se obtiene la parte real, y midiendo σ_y, la imaginaria.*

Sin entrar en detalles sobre el circuito, puesto que el operador de punto definido en (C.10) es proporcional a un operador unitario unitario, puede medirse mediante el circuito de la figura C.1. Puede incluso, como se muestra en [32], modificarse el circuito para elegir el punto a medir mediante registros

cuánticos. Sin embargo, alcanza para el presente trabajo con notar que puede medirse eficientemente la función de Wigner en un punto.

Agradecimientos

Este trabajo, al igual que esta carrera, no hubiera sido posible sin la ayuda de mucha gente. Quiero agradecer:

- a Juan Pablo, por haberme dirigido a lo largo de todo este trabajo, y por haber sido el primer y último docente que tuve en la carrera.
- a Augusto y Cecilia por haber sido excelentes compañeros, y haberme sacado las papas del fuego más de una vez.
- a mis padres, Eduardo y Violeta, por haberme aguantado durante estos años, a pesar de mi ensimismamiento por el estudio.
- a mis hermanos, Pablo y Lila, y mi cuñada, Karina, por todo.
- a mi abuelo, Moishe, el primer científico de la familia. Y a mis abuelos Minda, Samuel y Ana, porque también son parte de este trabajo.
- a mis amigos de siempre. En especial a Lute, Fer y El Tano, por la compañía permanente; a Ale porque, a pesar de la distancia, también estuvo siempre acompañando; a Masa, Mecha y Gabrielito (su primer agradecimiento en un documento público, probablemente); y a todos los gomías.

Bibliografía

[1] Nielsen and Chuang, *Quantum computation and quantum information* (Cambridge University Press, New York, NY, USA, 2000).

[2] G. Bjork, J. L. Romero, A. B. Klimov, and L. L. Sanchez-Soto, Mutually unbiased bases and discrete wigner functions, 2006, arXiv.org:quant-ph/0608173.

[3] J. L. Romero, G. Bjork, A. B. Klimov, and L. L. Sanchez-Soto, On the structure of the sets of mutually unbiased bases for n qubits, 2005, arXiv.org:quant-ph/0508129.

[4] A. Klappenecker and M. Roetteler, Constructions of mutually unbiased bases, 2003, arXiv.org:quant-ph/0309120.

[5] A. O. Pittenger and M. H. Rubin, Linear Algebra and its Applications **390**, 255 (2004), arXiv.org:quant-ph/0308142.

[6] K. S. Gibbons, M. J. Hoffman, and W. K. Wootters, Physical Review A **70**, 062101 (2004), arXiv.org:quant-ph/0401155.

[7] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan, A new proof for the existence of mutually unbiased bases, 2001, arXiv.org:quant-ph/0103162.

[8] I. Bengtsson, Three ways to look at mutually unbiased bases, 2006, arXiv.org:quant-ph/0610216.

[9] W. K. Wootters and B. D. Fields, Annals of Physics **191**, 363 (1989).

[10] C. Miquel, J. P. Paz, and M. Saraceno, Quantum computers in phase space, 2002, arXiv.org:quant-ph/0204149.

[11] W. K. Wootters, Picturing qubits in phase space, 2003, arXiv.org:quant-ph/0306135.

[12] J. P. Paz, A. J. Roncaglia, and M. Saraceno, Physical Review A **72**, 012309 (2005), arXiv.org:quant-ph/0410117.

[13] J. P. Paz, Discrete wigner functions and the phase space representation of quantum teleportation, 2002, arXiv.org:quant-ph/0204150.

[14] W. K. Wootters, Ann. Phys. **176**, 1 (1987).

[15] C. Dankert, *Efficient Simulation of Random Quantum States and Operators* (, 2005), arXiv.org:quant-ph/0512217.

[16] D. Gottesman, Stabilizer codes and quantum error correction, 1997, arXiv.org:quant-ph/9705052.

[17] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Physical Review Letters **88**, 127902 (2002), arXiv.org:quant-ph/0107130.

[18] I. D. Ivonovic, Journal of Physics A Mathematical General **14**, 3241 (1981).

[19] G. Zauner, Quantendesigns – grundzüge einer nichtkommutativen designtheorie, 1999.

[20] D. Gottesman, The heisenberg representation of quantum computers, 1998, arXiv.org:quant-ph/9807006.

[21] D. Gottesman, An introduction to quantum error correction, 2002, arXiv.org:quant-ph/0004072.

[22] R. P. Brent and B. D. McKay, Ars Combinatoria **26A**, 57 (1988).

[23] C. Cormick, Funciones de wigner discretas y estados estabilizadores en computación cuántica, Tesis de Licenciatura, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, 2005.

[24] H. Pringe, Códigos cuánticos de corrección de errores, Tesis de Licenciatura, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, 1997.

[25] E. P. Wigner, Phys. Rev. **40**, 749 (1932).

[26] P. Bianucci, C. Miquel, J. P. Paz, and M. Saraceno, Physics Letters A **297**, 353 (2002), quant-ph/0106091.

[27] J. P. Paz, A. J. Roncaglia, and M. Saraceno, Physical Review A **69**, 032312 (2004), arXiv.org:quant-ph/0310126.

[28] J. P. F. Duvall and I. P. W. Harley, SIAM J. Appl. Math **20**, 374 (1971).

[29] M. Schroeder, *Number Theory in Science and Communication: With Applications in Cryptography, Physics, Digital Information, Computing, and Self-Similarity* (Springer Series in Information Sciences, 1999).

[30] J. S. A.S. Hedayat, Neil J. A. Sloane, *Orthogonal Arrays: Theory and Applications* (Springer Series in Statistics, 1999).

[31] A. K. Ekert *et al.*, Phys. Rev. Lett. **88**, 217901 (2002).

[32] J. P. Paz and A. Roncaglia, A quantum gate array can be programmed to evaluate the expectation value of any operator, 2003, arXiv.org:quant-ph/0306143.