

# Funciones de Wigner discretas y estados estabilizadores en computación cuántica

Cecilia Cormick

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

Agosto de 2005

**TEMA:** Funciones de Wigner discretas y estados estabilizadores en  
computación cuántica

**ALUMNA:** Cecilia Cormick

**L.U.N:** 304/00

**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:** Agosto 2004

**FECHA DE FINALIZACIÓN:** Agosto 2005

**FECHA DE EXAMEN:**

**INFORME FINAL APROBADO POR:**

---

Autor

---

Director

---

Profesor de Tesis de Licenciatura

# Resumen

Los estados estabilizadores juegan roles clave en la computación cuántica; constituyen un recurso esencial en el modelo de computación cuántica basada en la medición [1] y en la construcción de códigos de corrección de errores [2]. En esta tesis se estudia la representación de los estados estabilizadores en el espacio de fases. Para ello se utiliza la función de Wigner discreta definida en [3, 4], y se proponen variantes de esta definición más apropiadas para algunos de los problemas considerados. En cualquiera de estas construcciones de la función de Wigner, las líneas del espacio de fases resultan asociadas a un conjunto de estados estabilizadores, pero la asociación entre cada línea y un dado estado puede variar dando lugar a una clase de posibles funciones de Wigner. En este trabajo se muestra que los únicos estados cuya función de Wigner es no negativa para cualquier definición en esta clase son las combinaciones estadísticas de los estados estabilizadores asociados a las líneas, demostrando así una conjetura presentada en [5]. Se estudia también la representación en el espacio de fases de la interferencia en una superposición coherente de estados estabilizadores, concluyendo que en general esta interferencia tiende a desparramarse en todo el espacio de fases, incluso en las regiones correspondientes a los estados superpuestos. Por último, se analiza un sistema de qubits en un estado estabilizador que sufre efectos de decoherencia, hallando tiempos críticos de pérdida de entrelazamiento y mostrando el modo en que la decoherencia se manifiesta en la función de Wigner del estado.

# Índice general

<b>1. Introducción</b>	<b>6</b>
<b>2. Computación cuántica: el modelo de circuitos y el basado en la medición</b>	<b>9</b>
2.1. El modelo de circuitos . . . . .	12
2.1.1. El modelo de circuitos de la computación clásica (muuy breve) . . . . .	12
2.1.2. La versión cuántica del modelo de circuitos . . . . .	12
2.2. Los operadores de Pauli generalizados . . . . .	15
2.3. El formalismo de estabilizadores . . . . .	17
2.3.1. Qué es un grupo estabilizador . . . . .	17
2.3.2. Los estados estabilizadores . . . . .	18
2.3.3. El grupo de Clifford, y el Teorema de Knill-Gottesman	19
2.3.4. Algunos ejemplos de estados estabilizadores . . . . .	20
2.4. Los estados-grafo . . . . .	21
2.5. Computación cuántica basada en la medición . . . . .	22
2.6. Cómo es que este modelo es equivalente al de circuitos . . . . .	24
<b>3. Funciones de Wigner discretas utilizando cuerpos finitos</b>	<b>31</b>
3.1. La función de Wigner en el espacio de fases continuo . . . . .	33
3.2. Funciones de Wigner para sistemas de qubits usando cuerpos finitos . . . . .	35
3.2.1. El espacio de fases y los cuerpos de Galois . . . . .	35
3.2.2. La generalización de la función de Wigner a dimensión discreta $d = p^n$ . . . . .	39
3.2.3. La condición de covariancia frente a traslaciones, y sus consecuencias . . . . .	40
3.2.4. La elección de la grilla cuántica . . . . .	46
3.2.5. Representación de algunos estados sencillos . . . . .	46
3.2.6. Los operadores de punto . . . . .	47

3.2.7.	Función de Wigner de estados estabilizadores . . . . .	49
3.2.8.	Funciones de Wigner a medida para los estados-grafo .	50
<b>4.</b>	<b>Positividad de la función de Wigner discreta</b>	<b>54</b>
4.1.	Caracterización de los estados con función de Wigner no negativa en toda grilla cuántica . . . . .	55
4.2.	Operadores que preservan la positividad total de la función de Wigner . . . . .	58
4.2.1.	Los operadores de Pauli . . . . .	59
4.2.2.	El operador de squeezing . . . . .	59
4.2.3.	Transformada discreta de Fourier . . . . .	60
<b>5.</b>	<b>La interferencia en la función de Wigner</b>	<b>64</b>
5.1.	La interferencia en la definición redundante de la función de Wigner . . . . .	65
5.2.	La función de Wigner discreta de una superposición de estados estabilizadores . . . . .	66
5.3.	Superposiciones de estados de la base computacional . . . . .	68
5.3.1.	El caso de dos qubits . . . . .	70
5.3.2.	Tres qubits, o más . . . . .	71
5.3.3.	Comportamiento promedio de la interferencia . . . . .	72
5.4.	Un último ejemplo: el código perfecto . . . . .	74
<b>6.</b>	<b>El efecto de la decoherencia en estados cluster</b>	<b>81</b>
6.1.	El modelo de decoherencia . . . . .	82
6.2.	Pérdida del entrelazamiento entre vecinos en un estado-grafo	83
6.3.	El tiempo de pérdida de entrelazamiento en algunos casos particulares . . . . .	86
6.3.1.	Ruido individual sobre cada qubit . . . . .	87
6.3.2.	Ruido correlacionado entre un qubit y todos sus vecinos	89
6.3.3.	Ruido correlacionado sobre pares de vecinos . . . . .	90
6.4.	El efecto de la decoherencia en la función de Wigner . . . . .	92
<b>7.</b>	<b>Conclusiones</b>	<b>97</b>
	<b>Muchas gracias a</b>	<b>99</b>
	<b>Bibliografía</b>	<b>100</b>

# Capítulo 1

## Introducción

Desde la aparición de las computadoras en los años '50, se han dedicado continuos esfuerzos para hacerlas, al mismo tiempo, más potentes y más pequeñas. Al cabo de muchos años de evolución en ambos sentidos, el proceso de disminución del tamaño parece estar acercándose al límite en que la naturaleza cuántica de los componentes de la computadora comienza a manifestarse. Este hecho, que implica un entorpecimiento en el desarrollo de la computación clásica, también abre las puertas a nuevas posibilidades en la construcción de computadoras que incorporen en su funcionamiento las propiedades cuánticas en cuestión.

Esta transformación es más que la adaptación de los algoritmos existentes a la aparición del comportamiento cuántico en la computadora: la mecánica cuántica proporciona una visión diferente de la información y su procesamiento. La utilización de sistemas cuánticos para computar permite la explotación de nuevos recursos, como el paralelismo cuántico y el entrelazamiento, gracias a los cuales es posible resolver en forma más eficiente problemas importantes como lo son el de factorización de números grandes (por su relación con la encriptación con clave pública) [6], y el de búsqueda en una base de datos desordenada [7, 8].

Desde el punto de vista de la física, el aprovechamiento de las propiedades cuánticas en la realización de cómputos promete mejorar notablemente la capacidad de simulación de sistemas físicos complejos, como conjuntos de un gran número de spins interactuantes. La simulación de esta clase de problemas en una computadora clásica es ineficiente, ya que en la medida en que aumenta la cantidad de componentes del sistema, el número de coeficientes necesarios para describir el estado crece exponencialmente, y por lo tanto también lo hace el tiempo de cómputo. Tal como lo señaló Feynman a principios de los '80 [9], esta dificultad puede ser superada si la

simulación se realiza procesando y almacenando información en un sistema también cuántico: para simular la dinámica de un sistema de  $n$  spines, es necesario un número exponencial de bits, y sin embargo los propios  $n$  spines pueden simularse a sí mismos eficientemente. La búsqueda de mecanismos para implementar “cómputos cuánticos”, entonces, es de enorme interés para el estudio de sistemas cuánticos de grandes dimensiones.

En los modelos más usuales de computación cuántica, la información se encuentra almacenada en el estado de un sistema de partículas con espacios de Hilbert de dimensión 2; a estos subsistemas se los llama “qubits”. El objetivo de esta tesis es el estudio de la representación en el espacio de fases del estado de este sistema, y de su evolución. El foco de este estudio está puesto en los llamados “estados estabilizadores” del sistema de qubits, que forman un conjunto de estados de especial importancia para la computación cuántica.

La organización del trabajo es la siguiente: en el capítulo 2 se presenta un resumen del modelo de circuitos de la computación cuántica, y de un modelo más reciente, llamado “irreversible” o “basado en la medición”. En este capítulo se define la notación a utilizar en lo sucesivo, y se presentan el formalismo de estabilizadores, la clase de estados estabilizadores, y, entre éstos, el conjunto de los llamados “estados-grafo” que son un ingrediente fundamental en el modelo basado en la medición. El capítulo concluye con una descripción de las razones por las que los dos modelos presentados son equivalentes.

En el capítulo 3 se introducen las funciones de Wigner como herramienta para representar el estado de un sistema cuántico en el espacio de fases; en primer lugar se muestra la definición de la función de Wigner para una partícula en una dimensión, y luego se discute la generalización de esta definición al caso de sistemas con dimensiones discretas. Para un sistema de qubits, se construye una función de Wigner en un espacio de fases cuyas coordenadas son elementos de un cuerpo finito, y se muestra de qué manera esta elección de coordenadas repercute en las propiedades de la función de Wigner. En particular, los conjuntos de líneas paralelas en el espacio de fases resultan asociados a bases conjugadas del espacio de Hilbert que están formadas por estados estabilizadores. Según se muestra, el procedimiento utilizado para la construcción de la función de Wigner no conduce a una única definición de esta función, sino a un conjunto de posibles definiciones, correspondientes a las diferentes “grillas cuánticas”, o asociaciones entre líneas del espacio de fases y estados del espacio de Hilbert.

En el capítulo 4 se estudia el conjunto de estados cuya función de Wigner es positiva para todas las posibles grillas cuánticas, y se demuestra que

este conjunto está formado por combinaciones estadísticas de los estados estabilizadores asociados a las líneas en el espacio de fases. A continuación se muestran algunos operadores que preservan este conjunto de estados, y se analiza el modo en que su aplicación transforma la función de Wigner.

En el capítulo 6 se considera un estado-grafo bajo el efecto de la decoherencia, y se calcula el tiempo para el cual se pierde el entrelazamiento entre vecinos. El interés de este problema radica en que este entrelazamiento es esencial para poder llevar a cabo un cómputo cuántico en el modelo basado en la medición. Al final del capítulo, se muestra la evolución del sistema en el espacio de fases.

Finalmente, el capítulo 7 contiene una revisión de los problemas estudiados a lo largo de la tesis y de otros, aún abiertos, relacionados con ellos.



## Capítulo 2

# Computación cuántica: el modelo de circuitos y el basado en la medición

Existen en la actualidad varios modelos de computación cuántica, de los cuales el más conocido es el modelo de circuitos, o modelo estándar de la computación cuántica. Todos los modelos existentes hasta el momento son equivalentes, en el sentido de que cualquier cómputo definido en un cierto modelo puede ser simulado eficientemente (esto es, con un número de recursos polinomial) en cualquiera de los otros. Sin embargo, existen diferencias conceptuales entre los distintos modelos y cada uno permite una perspectiva diferente no sólo de la implementación física de un cómputo cuántico sino también respecto del origen del poder computacional del sistema cuántico utilizado.

En cualquiera de los modelos conocidos, el resultado del cómputo se extrae realizando una serie de mediciones sobre el estado final de un sistema físico que obedece a las leyes de la mecánica cuántica. En el caso más sencillo, este sistema es una colección de subsistemas con espacios de Hilbert de dimensión 2, llamados “qubits”. Una base ortonormal arbitraria del espacio de Hilbert de cada qubit,  $B = \{|0\rangle, |1\rangle\}$  constituye la “base computacional” para cada qubit, en tanto que la base computacional para un sistema compuesto por un número  $n$  de qubits está formada por estados producto de los distintos qubits, de la forma:

$$|\vec{k}\rangle = |k_1\rangle \otimes |k_2\rangle \otimes \dots \otimes |k_n\rangle = |k_1, k_2, \dots, k_n\rangle \quad (2.1)$$

donde  $\vec{k}$  es una  $n$ -upla binaria.

En el modelo estándar, el esquema de implementación de un cómputo

es el siguiente: preparación de un conjunto de  $n$  qubits en un estado arbitrario conocido, aplicación de una secuencia predeterminada de operadores unitarios sobre los qubits, y medición en la base computacional sobre el estado final. Un conjunto de compuertas universales, cuya combinación en la forma apropiada permite generar una evolución arbitraria del sistema de qubits, puede formarse utilizando sólo operadores que actúan sobre uno o dos qubits a la vez. Este esquema básico puede enriquecerse incorporando qubits auxiliares, mediciones intermedias, evolución no unitaria, etc. [10]

Entre los modelos de computación cuántica alternativos al de circuitos se encuentran los llamados modelos basados en la medición [1, 11, 12]. En ellos se parte de un estado entrelazado del sistema de qubits, sobre el que se realizan secuencias ordenadas de mediciones de a un qubit en bases arbitrarias; el resultado del cómputo se obtiene de la última secuencia de mediciones. A causa del rol fundamental de la evolución no unitaria del sistema provocada por las mediciones, y del hecho de que éstas “consumen” a lo largo del cómputo el entrelazamiento inicial, estos modelos son también llamados “irreversibles” o “de un sentido” (*one-way*). Otros modelos basados en la medición incorporan también mediciones que involucran más de un qubit como mecanismo entrelazante.

El modelo de circuitos de la computación cuántica es esencialmente la generalización a un sistema cuántico del modelo clásico de circuitos; las propiedades del sistema permiten explotar el “paralelismo cuántico”, el entrelazamiento y la interferencia para realizar cálculos en tiempos que aventajan a las computadoras clásicas. Éste es el modelo original de la computación cuántica, y fue creado por David Deutsch [13], quien en 1985 dio el puntapié inicial en la búsqueda de algoritmos cuánticos con el algoritmo de Deutsch [14], que fue luego generalizado por Deutsch y Jozsa en 1992 [15]. Fue también Deutsch quien encontró la primer compuerta cuántica universal en 1989 [13]. En el marco del modelo de circuitos se desarrolló la computación cuántica a partir de los algoritmos de factorización de Shor en 1994 [6] y de búsqueda de Grover en 1995 [7, 8], que demostraron que existen problemas de interés computacional que pueden resolverse en forma más eficiente usando la mecánica cuántica.

Los modelos de computación cuántica basados en la medición surgieron a partir de un trabajo de Raussendorf y Briegel en el año 2000 [1]. Su equivalencia con el modelo original de computación cuántica no resultaba evidente en un principio; en el 2004, Childs, Leung y Nielsen [16] publicaron un modo de implementar eficientemente en el modelo *one-way* cualquier cómputo definido en forma de circuito, y viceversa, identificando una variante del proceso de teleportación como el procedimiento fundamental subyacente en

el modelo basado en la medición. La equivalencia entre los dos modelos se debe esencialmente al hecho de que, en el modelo de circuitos, es posible efectuar todas las interacciones entre qubits necesarias como primer paso en el cómputo; y más notable es que esto puede realizarse de antemano en forma independiente del cálculo a realizar, ya que las interacciones indeseadas pueden luego “deshacerse” por medio de mediciones en las bases apropiadas. El estado resultante, que ya contiene todas las posibles interacciones, y sobre el que sólo resta efectuar operaciones separadas en cada qubit, constituye entonces un punto de partida universal para cualquier cómputo en el modelo basado en la medición.

La aparición del modelo basado en la medición desafió la concepción tradicional respecto de la computación cuántica, en la cual la realización de mediciones individuales sobre los qubits destruye el paralelismo cuántico, que debe ser preservado hasta el fin del cómputo. La propuesta de Raussendorf y Briegel, por lo tanto, dio lugar a una nueva visión del origen de la capacidad de realizar computación cuántica relevante, y de los recursos básicos necesarios para ella. Por otra parte, las diferencias en la implementación del cómputo abrieron nuevas posibilidades en la búsqueda de sistemas físicos y dispositivos experimentales para la construcción de computadoras cuánticas.

El objetivo de este capítulo es presentar una revisión de algunos aspectos básicos de los modelos de circuitos y basados en la medición, definiendo además la notación a utilizar en lo sucesivo. En particular, se introducirán las clases de estados estabilizadores y estados-grafo, que constituyen el recurso fundamental de la computación cuántica en los modelos *one-way*. Los estados estabilizadores tienen, además, especial importancia en la construcción de códigos cuánticos de corrección de errores y en una definición reciente, propuesta por Wootters, de la función de Wigner de un sistema de qubits (que se detalla en el capítulo 3, y cuyo estudio es el tema central de este trabajo).

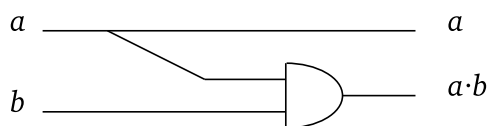
El capítulo está organizado de la siguiente manera: en primer lugar se repasarán algunos de los elementos fundamentales del modelo de circuitos de la computación cuántica. A continuación, se introducirán los llamados operadores de Pauli generalizados (que tienen un rol protagónico a lo largo de toda esta tesis); a partir de estos operadores se presentará el formalismo de estabilizadores, que a su vez se utilizará para definir las clases de estados estabilizadores y estados-grafo. Se mostrarán los pasos esenciales en la implementación de un cómputo en el modelo basado en la medición y se mostrará por qué los dos modelos presentados son equivalentes. Estas últimas secciones son de tipo monográfico, y pretenden explicar los aspectos

principales del modelo basado en la medición, entre ellos la aparición de los estados-grafo como recurso crucial para el cómputo, desde la perspectiva del modelo de circuitos.

## 2.1. El modelo de circuitos

### 2.1.1. El modelo de circuitos de la computación clásica (muuy breve)

En el modelo clásico de circuitos, un cómputo se representa como una combinación de cables y compuertas; cada cable conduce un bit de información, y las compuertas son funciones de la forma  $f : \{0, 1\}^j \rightarrow \{0, 1\}^k$  cuya entrada y salida están asociadas a los valores de los bits en los cables que entran y salen de las compuertas. Por ejemplo, el circuito que se muestra en la Figura 2.1 copia el primer bit y luego aplica la operación lógica *AND* sobre el segundo y el tercer bit. Si el estado inicial de los bits está dado por una 2-upla binaria  $(a, b)$ , la salida del circuito corresponde a dos bits cuyos valores son  $(a, a \cdot b)$ . Una introducción a este tema con vistas al modelo de circuitos de la computación cuántica se puede encontrar en el Capítulo 3 del libro de Nielsen y Chuang [10], y en el 6 de Preskill [17].

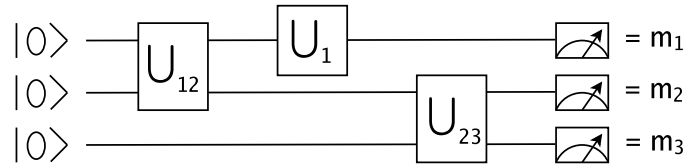


**Figura 2.1:** Representación de un cómputo en el modelo (clásico) de circuitos. El tiempo transcurre hacia la derecha; cada línea horizontal continua transporta un bit de información. Sobre los bits se aplican compuertas que evalúan funciones de la forma  $f : \{0, 1\}^j \rightarrow \{0, 1\}^k$  cuya entrada y salida están asociadas a los valores de los bits en los cables que entran y salen de las compuertas. En este caso, el circuito crea una copia del primer bit ( $f(a) = (a, a)$ ) y luego aplica una compuerta *AND* ( $f(a, b) = a \cdot b$ ) sobre los bits 2 y 3.

### 2.1.2. La versión cuántica del modelo de circuitos

El modelo de circuitos es el modelo original de la computación cuántica, y se asemeja al modelo de circuitos clásico, pero el sistema físico en el que se almacena la información y se implementan los cálculos exhibe propiedades cuánticas, de modo que su estado en cada instante es una superposición coherente de los estados que forman la base computacional.

En este modelo, se parte de un conjunto de qubits inicializados en un estado fácil de preparar (típicamente el  $|\vec{0}\rangle$ ), sobre los cuales se aplican compuertas que producen la evolución de los qubits. Estas compuertas son operadores unitarios que actúan sobre uno o dos qubits a la vez. Al concluir la secuencia de compuertas se mide el estado resultante en la base computacional, con lo que concluye el cálculo. Un esquema de este procedimiento se muestra en la Figura 2.2.



**Figura 2.2:** Representación de un cómputo cuántico en el modelo de circuitos. El tiempo transcurre hacia la derecha, cada línea horizontal continua corresponde a un qubit. Los qubits son inicializados en el estado  $|\vec{0}\rangle$ . A continuación se aplica una secuencia predefinida de compuertas que producen la evolución unitaria del sistema. El cómputo termina con una medición de los qubits en la base computacional, cuyos resultados se indican a la derecha del gráfico.

Un conjunto de compuertas es universal para la computación cuántica si mediante la composición de dichas compuertas es posible aproximar, con precisión arbitraria, cualquier operador unitario sobre el sistema de qubits. Un posible conjunto universal es el formado por todas las operaciones unitarias sobre un qubit y la compuerta entrelazante de dos qubits *CNOT* [18]; cualquier operador unitario puede descomponerse (en forma exacta) como un producto de compuertas en este conjunto (aunque el número de compuertas que es necesario componer para generar una evolución arbitraria es exponencial en el número de qubits en el sistema).

Los operadores unitarios sobre un qubit son (a menos de una fase global) de la forma:

$$U = R_{(\hat{n},\phi)} = e^{-\frac{i\phi\hat{n}\cdot\vec{\sigma}}{2}} \quad (2.2)$$

con  $\hat{n}$  un versor en  $\mathbb{R}^3$  y  $\hat{n}\cdot\vec{\sigma} = n_1\sigma_1 + n_2\sigma_2 + n_3\sigma_3$ , donde  $\sigma_1 = X$ ,  $\sigma_2 = Y$ ,  $\sigma_3 = Z$  son las matrices de Pauli (para simplificar la notación donde sea conveniente se usará también  $\sigma_0 = I$ ). Para el caso en que el qubit es una partícula de spin 1/2, el operador  $R_{(\hat{n},\phi)}$  corresponde a una rotación en torno del eje  $\hat{n}$  en un ángulo  $\phi$ . Entre los operadores unitarios de esta forma se encuentran (en algunos casos, a menos de una fase global) la identidad ( $I$ ), las matrices de Pauli ( $X$ ,  $Y$ ,  $Z$ ), el Hadamard ( $H$ ) y el operador de fase ( $P$ ).

La representación matricial de estos operadores en la base computacional es la siguiente:

$$\begin{aligned} X &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & Y &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} & Z &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ I &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & H &= \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} & P &= \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \end{aligned} \quad (2.3)$$

La compuerta  $CNOT$  (negación controlada) corresponde a una interacción entre dos qubits, y aplica un  $NOT$  (la matriz de Pauli  $X$ ) sobre el qubit objetivo si el estado del qubit de control es  $|1\rangle$ , y la identidad si el estado del qubit de control es  $|0\rangle$ , según:

$$CNOT_{(1,2)}|k_1, k_2\rangle = |k_1, k_2 \oplus k_1\rangle \quad (2.4)$$

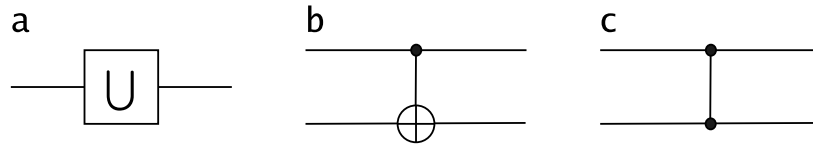
donde el primer qubit es el control y el segundo, el objetivo.

Un conjunto equivalente de compuertas universales, de utilización frecuente en el marco de la preparación de los estados-grafo y de la simulación de circuitos cuánticos en los modelos *one-way*, es el formado por todas las compuertas unitarias de un qubit y la compuerta de dos qubits llamada “fase controlada” ( $CZ$ ), que corresponde a la aplicación controlada del operador de Pauli  $Z$  sobre el qubit objetivo:

$$CZ_{(1,2)}|k_1, k_2\rangle = (-1)^{k_1 k_2} |k_1, k_2\rangle \quad (2.5)$$

A diferencia del  $CNOT$ , la compuerta  $CZ$  actúa en forma simétrica sobre los dos qubits.

La representación gráfica de los operadores presentados se muestra en la Figura 2.3.



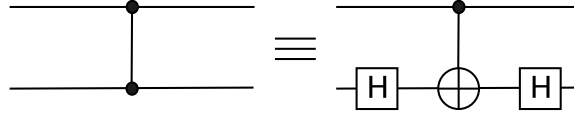
**Figura 2.3:** Representación de las compuertas unitarias: a)  $U$  (rotación sobre un qubit), b)  $CNOT$  ( $X$  controlado), c)  $CZ$  ( $Z$  controlado).

Dado que el operador  $H$  proporciona el cambio de la base de autoestados de  $Z$  a la de  $X$ , la compuerta  $CZ$  puede obtenerse combinando  $CNOT$  y  $H$

en la forma:

$$CZ_{(1,2)} = H_{(2)}CNOT_{(1,2)}H_{(2)} \quad (2.6)$$

Esta propiedad se muestra gráficamente en la Figura 2.4.



**Figura 2.4:** La compuerta  $CZ$  puede obtenerse a partir de la combinación de compuertas  $CNOT$  y  $H$ .

De acuerdo a lo comentado previamente, cualquier evolución del sistema de qubits puede obtenerse en forma exacta a través de la composición de operadores unitarios arbitrarios sobre un qubit y compuertas de dos qubits  $CNOT$  o  $CZ$ . Sin embargo, la aproximación de cualquier operador unitario con precisión arbitraria puede realizarse con un conjunto mucho más restringido de compuertas; un conjunto estándar de compuertas universales es el compuesto por  $CNOT$ ,  $H$ , y el operador  $T = R_{(\hat{z}, \pi/4)}$ . Esto es porque cualquier operación sobre un qubit puede aproximarse con precisión arbitraria por medio de las compuertas  $H$  y  $T$  (la eficiencia de esta aproximación se discute, haciendo uso del teorema de Solovay-Kitaev, en el capítulo 4 del libro de Nielsen y Chuang [10]).

## 2.2. Los operadores de Pauli generalizados

Las matrices de Pauli  $\{\sigma_i, i = 1, 2, 3\}$  forman un conjunto de generadores para todas las evoluciones posibles de un qubit (de la forma de (2.2)), y satisfacen las siguientes (muy conocidas) propiedades:

1. Son hermíticas.
2. Sus autovalores son  $\pm 1$ .
3. Tienen traza nula.
4. El producto de dos matrices de Pauli es, a menos de una fase global, otra matriz de Pauli, o la identidad ( $\sigma_0$ ):

$$\sigma_j \sigma_k = i \epsilon_{jkl} \sigma_l + \delta_{jk} \sigma_0 \quad (2.7)$$

donde  $j, k, l$  van de 1 a 3 y  $\epsilon_{jkl}$  es el tensor de Levi-Civita.

5. Las matrices de Pauli conmutan o anticonmutan:

$$\{\sigma_i, \sigma_j\} = 0 \quad \text{si } i \neq j \quad (2.8)$$

donde  $i, j$  van de 1 a 3 (y obviamente si  $i = j$  las matrices conmutan).

6. Utilizando las reglas para el producto de matrices de Pauli y sabiendo que tienen traza nula, puede verse que el conjunto formado por las matrices de Pauli y la identidad es ortogonal en el producto de Schmidt:

$$\text{Tr}(\sigma_j \sigma_k) = 2\delta_{jk} \quad (2.9)$$

donde  $j, k$  van de 0 a 3. Por lo tanto,  $\{\sigma_i, i = 0, \dots, 3\}$  es una base para el desarrollo de cualquier operador hermítico de  $2 \times 2$ .

Los operadores de Pauli generalizados son operadores unitarios  $\pm \sigma_{\vec{a}, \vec{b}}$  que corresponden, a menos de un signo, a la aplicación de una matriz de Pauli sobre cada uno de los qubits en el sistema, en la forma:

$$\sigma_{\vec{a}, \vec{b}} = \prod_{i=1}^n X_{(i)}^{a_i} Z_{(i)}^{b_i} e^{i\frac{\pi}{2} a_i b_i} = X^{\vec{a}} Z^{\vec{b}} e^{i\frac{\pi}{2} \vec{a} \cdot \vec{b}} \quad (2.10)$$

donde  $\vec{a}, \vec{b}$  son dos  $n$ -uplas binarias que indican qué matriz de Pauli  $\sigma_i$  se aplica sobre cada uno de los qubits (los subíndices entre paréntesis indican el qubit sobre el que actúa cada operador).

A partir de las propiedades de las matrices de Pauli es fácil deducir que los operadores de Pauli generalizados satisfacen:

1. Son hermíticos.
2. Sus autovalores son  $\pm 1$ .
3. Tienen traza nula, excepto por  $\sigma_{\vec{0}, \vec{0}} = I$ , que tiene traza  $2^n$ .
4. El producto de dos operadores de Pauli generalizados es otro operador de este conjunto (a menos de una fase global  $\pm 1, \pm i$ ).
5. Los operadores de Pauli generalizados conmutan o anticonmutan:

$$\sigma_{\vec{a}, \vec{b}} \sigma_{\vec{c}, \vec{d}} = (-1)^{\vec{a} \cdot \vec{d} - \vec{c} \cdot \vec{b}} \sigma_{\vec{c}, \vec{d}} \sigma_{\vec{a}, \vec{b}} \quad (2.11)$$

de donde se obtienen las condiciones:

$$[\sigma_{\vec{a}, \vec{b}}, \sigma_{\vec{c}, \vec{d}}] = 0 \quad \text{si } \vec{a} \cdot \vec{d} - \vec{c} \cdot \vec{b} = 0 \pmod{2} \quad (2.12)$$

$$\{\sigma_{\vec{a}, \vec{b}}, \sigma_{\vec{c}, \vec{d}}\} = 0 \quad \text{si } \vec{a} \cdot \vec{d} - \vec{c} \cdot \vec{b} = 1 \pmod{2} \quad (2.13)$$



6. Son ortogonales en el producto de Schmidt:

$$\text{Tr}(\sigma_{\vec{a},\vec{b}} \sigma_{\vec{c},\vec{d}}) = 2^n \delta(\vec{a} - \vec{c}) \delta(\vec{b} - \vec{d}) \quad (2.14)$$

Por lo tanto, los operadores de Pauli generalizados forman una base para el desarrollo de cualquier operador hermítico de  $2^n \times 2^n$ .

## 2.3. El formalismo de estabilizadores

El formalismo de estabilizadores fue desarrollado por Daniel Gottesman, en el marco del estudio de códigos cuánticos de corrección de errores [2]. La idea básica de estos códigos es proteger la información contenida en un qubit a través de su codificación en el estado de un grupo de qubits; de esta forma, los estados lógicos aceptables son un subespacio de dimensión 2 dentro del espacio de Hilbert del grupo de qubits, y los errores en el cómputo son detectados cuando el estado del sistema se “escapa” de este subespacio. El formalismo de estabilizadores permite caracterizar el subespacio de estados lógicos como el formado por aquellos estados que son autoestados con autovalor 1 de un cierto conjunto de operadores de Pauli, que se llama el “estabilizador” del código. En [19, 20] se pueden encontrar introducciones al formalismo de estabilizadores y su uso en códigos de corrección de errores.

Las aplicaciones del formalismo creado por Gottesman van más allá de la corrección de errores: su utilización permite la simulación eficiente en una computadora clásica de la evolución de un sistema de qubits a lo largo de un cómputo contenido en el tipo de circuitos llamados “circuitos estabilizadores”, lo que puede ser de utilidad para testear el correcto funcionamiento de una potencial computadora cuántica. Este formalismo también facilita notablemente la descripción de los llamados “estados-grafo” y “estados cluster”, que son el recurso fundamental para la computación cuántica basada en la medición.

Algunas de las definiciones que aparecen en esta sección son distintas de las de los trabajos originales sobre el formalismo de estabilizadores. Las versiones que se muestran acá se corresponden con las de [21].

### 2.3.1. Qué es un grupo estabilizador

Dado un estado  $|\psi\rangle$ , se dice que  $|\psi\rangle$  es estabilizado por un operador unitario  $S$  si se verifica:

$$S|\psi\rangle = |\psi\rangle \quad (2.15)$$

o sea, si  $|\psi\rangle$  es un autoestado de  $S$  con autovalor 1. Es claro que si  $S$  estabiliza a  $|\psi\rangle$  también  $S^{-1}$  lo hará, y que si dos operadores  $S_1, S_2$  estabilizan a

$|\psi\rangle$  también lo hace el producto de los mismos. Además, la identidad estabiliza a cualquier estado  $|\psi\rangle$ . Por lo tanto, para cada estado  $|\psi\rangle$  el conjunto de operadores unitarios que lo estabilizan es un grupo, llamado “grupo estabilizador de  $|\psi\rangle$ ” o simplemente “estabilizador de  $|\psi\rangle$ ”. Este grupo se notará en la forma  $S_\psi$ .

Dados dos estados  $|\psi\rangle, |\phi\rangle$ , se verifica que  $|\psi\rangle \neq |\phi\rangle \Rightarrow S_\psi \neq S_\phi$  (donde se considera que dos estados son iguales si sólo difieren en una fase global). De esta forma, el grupo estabilizador caracteriza completamente a un estado puro. Si  $|\psi\rangle$  tiene estabilizador  $S_\psi$ , entonces al transformar el estado aplicando una operación unitaria  $U$ , el nuevo grupo estabilizador se obtiene en la forma:

$$\begin{aligned} |\psi\rangle &\rightarrow |\phi\rangle = U|\psi\rangle \\ S \in S_\psi &\rightarrow USU^\dagger \in S_\phi \end{aligned} \quad (2.16)$$

Cada estado es estabilizado por un conjunto de infinitos operadores, ya que si  $S$  es un estabilizador del estado también lo será cualquier operador de la forma  $S^x$  con  $x \in \mathbb{R}$ . Por ejemplo, en el caso de 1 qubit el estado  $|0\rangle$  es estabilizado por todos los operadores de la forma  $|0\rangle\langle 0| + e^{i\phi}|1\rangle\langle 1|$ ; sin embargo, para determinar unívocamente el estado alcanza con dar un elemento (no trivial) del estabilizador, por ejemplo, el operador  $Z$ .

La caracterización de un estado puro de  $n$  qubits a través de su estabilizador requiere de, al menos, una matriz unitaria (por ejemplo, el operador  $2|\psi\rangle\langle\psi| - I$  estabiliza al estado  $|\psi\rangle$  y tiene autovalor  $-1$  para cualquier estado ortogonal a él). Pero una matriz unitaria arbitraria depende de  $2^{2n}$  parámetros reales, o sea que la determinación del estado por su estabilizador no es, en general, más eficiente que su desarrollo en una base dada.

### 2.3.2. Los estados estabilizadores

Es posible definir clases de estados con descripción eficiente en términos de sus estabilizadores, a partir de la restricción de los operadores que pueden pertenecer al grupo estabilizador. En particular, la clase de “estados estabilizadores” de un sistema de  $n$  qubits se define como el conjunto de estados que son estabilizados por exactamente  $2^n$  operadores de Pauli generalizados  $\pm \sigma_{\vec{a}, \vec{b}}$  (contando la identidad). Si un estado pertenece a esta clase, para describirlo por medio de su estabilizador alcanza con indicar los  $n$  generadores del grupo formado por los  $2^n$  operadores de Pauli que lo estabilizan. Por ejemplo, el estado  $|\vec{0}\rangle$  es (a menos de una fase) el único estado que es estabilizado por el operador de Pauli  $Z$  en cualquier qubit. Esto es porque, en el espacio de Hilbert de dimensión  $2^n$ , los estados estabilizados por cualquier operador de Pauli no trivial forman un subespacio de dimensión  $2^{n-1}$ ; al

ir agregando operadores de Pauli independientes al grupo estabilizador la dimensión del subespacio se achica a la mitad en cada paso. De esta forma, un conjunto de  $n$  generadores independientes selecciona un subespacio de dimensión 1, o sea, un único estado (a menos de la norma y la fase global).

A diferencia de una matriz unitaria arbitraria, para la que se necesita un número exponencial de coeficientes, cada uno de los  $n$  generadores es determinado por las dos  $n$ -uplas binarias  $\vec{a}$ ,  $\vec{b}$  y el signo. Por lo tanto, se precisan  $(4n + 1)$  bits para cada generador, y  $(4n^2 + n)$  bits para la caracterización completa del estado. Esto muestra que los estados en esta clase tienen una descripción eficiente utilizando el formalismo de estabilizadores.

Si se tienen dos operadores de Pauli  $S_1, S_2$  que anticonmutan, resulta  $\{S_1, S_2\}|\psi\rangle = 0$  para cualquier estado  $|\psi\rangle$ . Por lo tanto, para que dos operadores de Pauli tengan un autoestado común deben conmutar (dado que sus autovalores son no nulos). Entonces, para cada estado estabilizador los operadores de Pauli que lo estabilizan forman un grupo abeliano.

Como los operadores de Pauli generalizados forman una base para los operadores hermíticos, la matriz densidad de un estado estabilizador  $|\psi\rangle$  puede escribirse como combinación lineal de operadores de Pauli. Si  $S_\psi$  es generado por los operadores de Pauli  $\{S_1, \dots, S_n\}$ , la expansión de la matriz densidad contiene únicamente los operadores que estabilizan el estado, en la forma:

$$|\psi\rangle\langle\psi| = \frac{1}{2^n} \sum_{\sigma \in S_\psi} \sigma = \frac{1}{2^n} \prod_{i=1}^n (I + S_i) \quad (2.17)$$

donde en la primera expresión la suma es sobre los  $2^n$  operadores de Pauli generalizados que estabilizan a  $|\psi\rangle$ , mientras que en la segunda el producto es sólo sobre los  $n$  generadores del grupo estabilizador.

### 2.3.3. El grupo de Clifford, y el Teorema de Knill-Gottesman

Dado un estado estabilizador  $|\psi\rangle$  cuyo grupo estabilizador es generado por  $\{S_1, \dots, S_n\}$ , al aplicar sobre  $|\psi\rangle$  un operador unitario  $U$  se obtiene un nuevo estado cuyo estabilizador es generado por  $\{US_1U^\dagger, \dots, US_nU^\dagger\}$ . Si  $US_iU^\dagger$  es un operador de Pauli generalizado (para  $i = 1, \dots, n$ ), entonces el nuevo estado también pertenece a la clase de estados estabilizadores. Aquellos operadores unitarios que mapean todos los estados estabilizadores en otros (o, equivalentemente, todos los operadores de Pauli en otros) conforman el grupo de Clifford. Todos los operadores en este grupo pueden obtenerse componiendo las compuertas  $H$ ,  $CNOT$ , y  $P$ , a menos de una fase global. En particular, cualquier estado estabilizador puede obtenerse a partir del  $|\vec{0}\rangle$  utilizando sólo operadores de Clifford [21].

No sólo los estados estabilizadores tienen una descripción eficiente utilizando este formalismo, sino que, además, el resultado de la aplicación de una compuerta de Clifford sobre un estado estabilizador es otro estado estabilizador que puede calcularse eficientemente. O sea, la evolución de un conjunto de qubits que se prepara en un estado estabilizador y sobre el que se aplican compuertas pertenecientes al grupo de Clifford es simulable eficientemente en una computadora clásica. También la medición de un estado estabilizador en la base computacional puede ser simulada eficientemente utilizando este formalismo, de forma que cualquier cómputo cuántico que conste de: preparación de un estado estabilizador inicial (en particular el  $|\vec{0}\rangle$ ), aplicación de compuertas de Clifford, y medición en la base computacional, puede ser simulado eficientemente en una computadora clásica, y por lo tanto estos recursos no son suficientes para realizar computación cuántica relevante. Este resultado se conoce como el Teorema de Knill-Gottesman, y los circuitos de la forma descrita se llaman “circuitos estabilizadores” [2, 19].

### 2.3.4. Algunos ejemplos de estados estabilizadores

Entre los estados estabilizadores se encuentran algunos estados conocidos, como los de la base computacional, los estados de Bell y los GHZ. El estado  $|\vec{k}\rangle$  de la base computacional tiene un grupo estabilizador generado por  $\{(-1)^{k_1} Z_{(1)}, \dots, (-1)^{k_n} Z_{(n)}\}$ . Los estados de Bell, que son los estados de dos qubits máximamente entrelazados de la forma:

$$|\phi_{\pm}\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2} \quad (2.18)$$

$$|\psi_{\pm}\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2} \quad (2.19)$$

son estabilizados por productos de operadores de Pauli de la forma  $\pm X_{(1)}X_{(2)}$ ,  $\pm Z_{(1)}Z_{(2)}$ . El estado GHZ de  $n$  qubits

$$|GHZ\rangle = (|00\dots 0\rangle + |11\dots 1\rangle)/\sqrt{2} \quad (2.20)$$

debe su nombre a Greenberger, Horne y Zeilinger [22], y es llamado también “estado tipo gato de Schrödinger” (por consistir en una superposición coherente de dos estados “antagónicos” –vida y muerte del gato– de un sistema compuesto por muchos subsistemas). Este estado es estabilizado por el operador  $X_{(1)}X_{(2)}\dots X_{(n)}$  y todos los productos de la forma  $Z_{(i)}Z_{(j)}$ .

## 2.4. Los estados-grafo

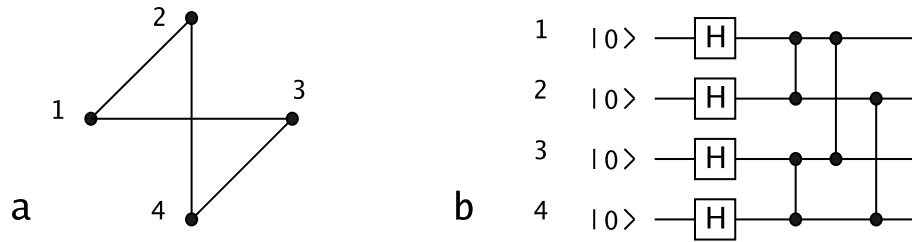
Entre los estados estabilizadores, un subconjunto de particular interés para la computación cuántica es el de los llamados “estados-grafo” [23].

Este tipo de estados juega un rol central en los modelos de computación cuántica basados en la medición, en los que el poder computacional surge del entrelazamiento entre qubits presente en el estado-grafo, que es el punto de partida para el cálculo.

Cada estado-grafo se define a partir de un grafo asociado; un dado grafo  $G$  está compuesto por un conjunto  $V$  de  $n$  vértices, y una matriz binaria  $\Gamma$  que determina las relaciones de vecindad entre ellos:  $\Gamma_{i,j}$  vale 1 si los vértices  $i, j$  son vecinos, y 0 si no. El estado-grafo  $|G\rangle$  asociado a  $G$  se prepara en la siguiente forma:

1. Se toman  $n$  qubits en el estado  $|0\rangle$ .
2. Se aplica una compuerta  $H$  sobre cada uno de ellos; el estado final de cada qubit es autoestado de la matriz de Pauli  $X$  con autovalor  $+1$ , y se notará  $|+\rangle$ .
3. Se realizan compuertas  $CZ$  entre todos los pares de qubits correspondientes a vértices vecinos en el grafo; este paso produce el entrelazamiento entre los qubits. Es importante notar que todas las compuertas  $CZ$  conmutan entre sí, de modo que no es necesario especificar el orden en que deben ser aplicadas.

El proceso descrito define, para cada grafo  $G$ , el estado-grafo asociado  $|G\rangle$ . En la Figura 2.5 se muestra el circuito que prepara el estado-grafo asociado a un grafo de 4 vértices.



**Figura 2.5:** a) Grafo de 4 vértices; b) Circuito de preparación de su estado-grafo asociado.

Dado que el estado asociado a un grafo dado se obtiene aplicando una sucesión de compuertas del grupo de Clifford a un conjunto de qubits cuyo estado inicial es el  $|\vec{0}\rangle$ , el estado-grafo es un estado estabilizador. Por lo tanto, es posible definirlo no a partir de su proceso de preparación sino en términos de su grupo estabilizador. Utilizando el estabilizador del estado inicial, que

es el generado por  $Z$  en cada qubit, y la ecuación (2.16) para hallar el nuevo grupo estabilizador al cabo de cada paso en el proceso de preparación, puede obtenerse el estabilizador del estado-grafo, que es generado por los operadores de Pauli que aplican  $X$  sobre un vértice y  $Z$  sobre todos sus vecinos, o sea:

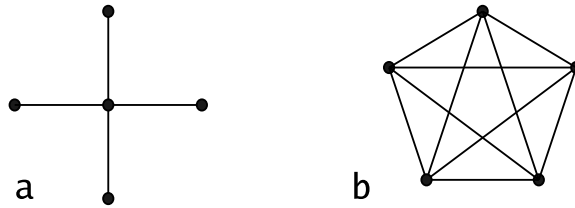
$$S_G = \langle S_1, \dots, S_n \rangle \quad \text{con} \quad S_i = X_{(i)} \prod_j Z_{(j)}^{\Gamma_{i,j}}. \quad (2.21)$$

Utilizando la ecuación (2.17) y reordenando los operadores de Pauli se puede obtener para la matriz densidad de un estado-grafo la expresión:

$$|G\rangle\langle G| = \frac{1}{2^n} \sum_{\vec{a}} \sigma_{\vec{a}, \Gamma \vec{a}} \quad (2.22)$$

donde la suma es sobre todas las  $n$ -uplas binarias  $\vec{a}$ .

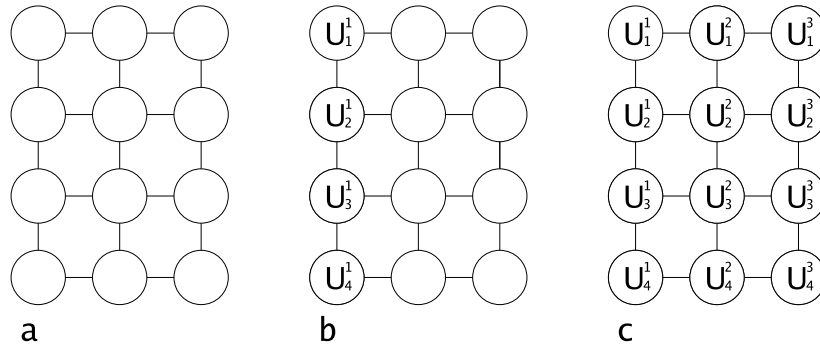
Un tipo de estado-grafo particularmente relevante para la computación cuántica basada en la medición es el de los llamados “estados cluster”, que corresponden a grafos de redes cúbicas en dimensión  $D$ . Un estado cluster de dos o más dimensiones proporciona el principal recurso para la computación cuántica universal en el modelo basado en la medición. Otro ejemplo lo proporcionan los estados  $|GHZ\rangle$ , que pueden obtenerse aplicando operaciones unitarias locales (o sea, sobre un qubit a la vez) sobre los estados-grafo en que todos los vértices son vecinos entre sí o todos son vecinos de un vértice central (ver Figura 2.6). Más generalmente, cualquier estado estabilizador es localmente equivalente a un estado-grafo, esto es, es el resultado de aplicar un conjunto de operaciones unitarias de un qubit sobre los componentes de un estado-grafo [23, 24].



**Figura 2.6:** Los estados  $|GHZ\rangle = (|00\dots 0\rangle + |11\dots 1\rangle)/\sqrt{2}$  pueden obtenerse aplicando rotaciones de a un qubit sobre los estados-grafo correspondientes a: a) el grafo en que todos los vértices son vecinos de un vértice central; b) el grafo en que todos son vecinos entre sí.

## 2.5. Computación cuántica basada en la medición

Los estados-grafo constituyen el recurso básico en el modelo original de computación cuántica basada en la medición [1]. En este modelo, la implementación de cualquier cómputo cuántico consiste en la preparación de un estado-grafo, seguida por una secuencia ordenada de mediciones en bases arbitrarias de los qubits, donde cada medición sólo involucra a uno de los qubits pero la base en que se mide depende de los resultados de mediciones previas (realimentación clásica). Cualquier cómputo definido en el modelo de circuitos con  $n$  qubits y  $m$  pasos temporales puede realizarse siguiendo este procedimiento sobre un estado cluster de dimensión 2 y tamaño  $\mathcal{O}(n \times m)$ . Un esquema de un cálculo dentro de este modelo se muestra en la Figura 2.7.



**Figura 2.7:** Representación esquemática de un cómputo en el modelo basado en la medición. a) El cómputo comienza con la preparación de un estado cluster; cada círculo representa un qubit y las líneas que los unen indican relaciones de vecindad. b) Los qubits de la primera hilera son medidos en bases arbitrarias  $B_U = \{U^\dagger|0\rangle, U^\dagger|1\rangle\}$ . c) Al final del cálculo, todos los qubits han sido medidos, y el resultado del cómputo se obtiene de la última secuencia de mediciones.

El punto de partida para el cómputo es un estado cluster (cuyo tamaño depende del cálculo a realizar); el entrelazamiento presente en este estado inicial es la fuente del poder computacional en este modelo. Una vez preparado este estado, los qubits en la primera hilera del cluster son medidos en cualquier orden, cada uno de ellos en una base arbitraria  $B_U = \{U^\dagger|0\rangle, U^\dagger|1\rangle\}$ . Como resultado de este proceso, los qubits medidos se desentrelazan, y el estado en que queda el resto de los qubits depende de las bases en que se realizaron las mediciones y de los resultados de las mismas. De esta manera, la información sobre el cálculo se “propaga” a lo largo de las sucesivas hileras

de qubits, y el proceso concluye al medir la última de ellas. Las bases en que se miden los qubits en una dada hilera dependen de los resultados de las mediciones previas, en una forma que puede ser calculada eficientemente por una computadora clásica. Los recursos necesarios para la realización de un cómputo en este modelo son, por lo tanto, el estado cluster inicial y la capacidad de realizar mediciones de un qubit en bases arbitrarias que dependen de los resultados previamente almacenados.

## 2.6. Cómo es que este modelo es equivalente al de circuitos

La equivalencia entre el modelo de computación cuántica basado en la medición y el modelo de circuitos fue demostrada por Childs, Leung y Nielsen [16], a través de la presentación de un procedimiento para simular eficientemente en cada uno de los dos modelos cualquier cómputo definido en el otro. En esta sección se resumen las ideas básicas de este trabajo.

En primer lugar, es fácil ver que cualquier cómputo en el modelo irreversible es simulable eficientemente en el modelo de circuitos: la preparación de un cluster de dos dimensiones y tamaño  $n \times m$  puede realizarse en el modelo de circuitos según el procedimiento explicado en la sección 2.4, usando  $n$  qubits preparados en el estado  $|\vec{0}\rangle$  sobre los que se aplican  $n$  operadores de Hadamard y un número  $\mathcal{O}(nm)$  de compuertas  $CZ$ . A continuación se realiza una secuencia de rotaciones individuales sobre los qubits y mediciones en la base computacional; si el cómputo requiere de la medición de un qubit en la base  $B_U = \{U^\dagger|0\rangle, U^\dagger|1\rangle\}$ , esto corresponde simplemente a la aplicación de la compuerta de rotación  $U$  seguida de una medición en la base computacional. Las rotaciones y mediciones deben hacerse alternadamente, esto es: en primer lugar se realizan las rotaciones y mediciones necesarias sobre los qubits correspondientes a la primer hilera; en función de los resultados de esta ronda de mediciones se aplican las rotaciones sobre los qubits en la segunda hilera, etc.

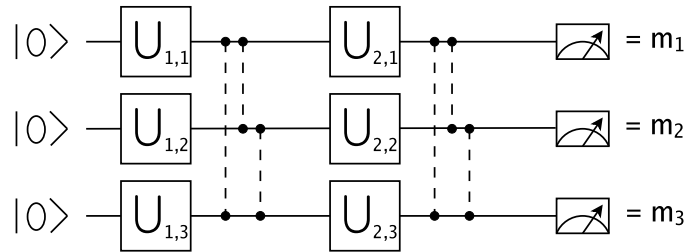
Para ver que, por otra parte, cualquier cómputo en el modelo de circuitos es simulable eficientemente en el modelo basado en la medición, es necesario convencerse de que:

1. Es posible escribir cualquier circuito como una repetición de la siguiente secuencia de operaciones: aplicación de compuertas  $CZ$  opcionales, rotaciones individuales, y teleportación del estado de los qubits a otros qubits, sobre los que se repite la secuencia.



2. El circuito desarrollado en esta forma puede modificarse de modo de aplicar todas las interacciones entre qubits (en forma de compuertas  $CZ$ ) al principio del cómputo.
3. Es posible efectuar interacciones de más, que luego pueden deshacerse de ser necesario, de manera que las compuertas  $CZ$  que se apliquen al principio del cómputo sean independientes del cálculo que se quiere realizar.

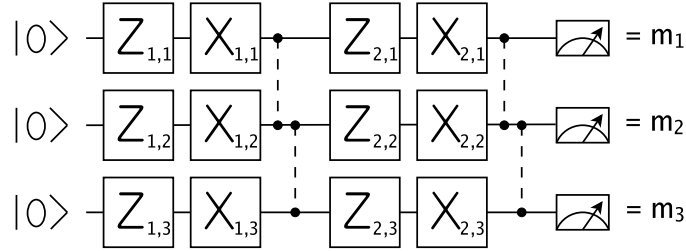
A continuación se mostrará cómo cualquier circuito puede ser reescrito de acuerdo a estas indicaciones, de modo de llevarlo a la forma de un cómputo en el modelo basado en la medición. En primer lugar, cada circuito puede pensarse como una repetición de una ronda de compuertas arbitrarias de un qubit seguida por una ronda de compuertas  $CZ$  entre pares de qubits a elección; al cabo de un cierto número de repeticiones el cálculo termina al medir los qubits en la base computacional. Este esquema se muestra en la Figura 2.8.



**Figura 2.8:** Representación de un cómputo en el modelo de circuitos. El cómputo está formado por la repetición de una secuencia compuesta por una ronda de compuertas arbitrarias de un qubit y una ronda de compuertas  $CZ$  entre pares de qubits a elección (el carácter opcional de esta compuerta  $CZ$  se indica dibujándola con una línea punteada). Al terminar el cálculo los qubits son medidos en la base computacional.

Componiendo compuertas  $CZ$  y  $H$  es posible armar la compuerta  $SWAP$ , que intercambia el estado de dos qubits; entonces, no es necesaria la capacidad de aplicar compuertas  $CZ$  entre cualquier par de qubits en el sistema, sino que alcanza con poder aplicar las compuertas de la forma  $CZ_{(i,i+1)}$  con  $i = 1, \dots, n - 1$ . Por otra parte, cualquier operador de rotación de un qubit puede descomponerse en la forma:  $U = Z_{\theta_3} X_{\theta_2} Z_{\theta_1}$ , donde  $Z_{\theta}$  y  $X_{\theta}$  son rotaciones en un ángulo  $\theta$  en torno de los ejes  $\hat{z}$  y  $\hat{x}$ , respectivamente. Entonces, cualquier circuito puede escribirse como una repetición de una secuencia de rotaciones en torno de  $\hat{z}$ , una de rotaciones en torno de  $\hat{x}$ , otra de  $\hat{z}$  y una

ronda de  $CZ$  opcionales. Como además las compuertas  $Z_\theta$  conmutan con las  $CZ$ , se pueden juntar las últimas  $Z_\theta$  de cada secuencia con las primeras de la secuencia siguiente. O sea, cualquier circuito puede descomponerse como la repetición de una secuencia formada por: una ronda de compuertas tipo  $Z_\theta$ , una de compuertas  $X_\theta$ , y una de  $CZ$  opcionales. Esta descomposición se muestra en la Figura 2.9.

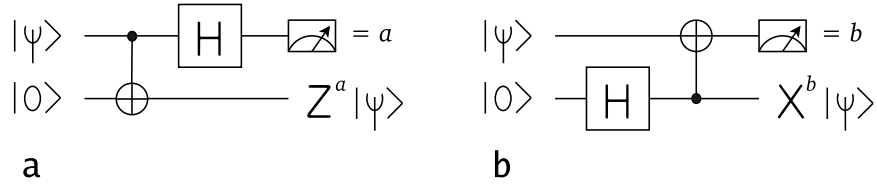


**Figura 2.9:** Un cómputo en el modelo de circuitos puede descomponerse como una repetición de una secuencia compuesta por una ronda de rotaciones en ángulos arbitrarios en torno del eje  $\hat{z}$  ( $Z_{i,j}$ ), otra en torno del eje  $\hat{x}$  ( $X_{i,j}$ ), y una ronda de compuertas  $CZ$  opcionales entre pares de qubits vecinos (dibujadas con línea punteada). Al terminar el cálculo los qubits son medidos en la base computacional.

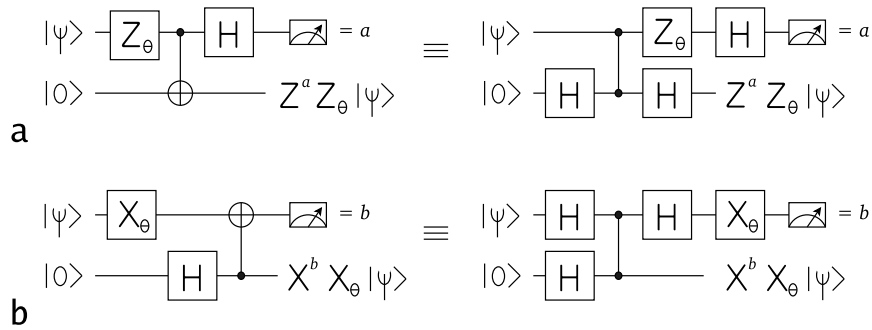
Como siguiente paso en la “conversión” del circuito al modelo *one-way*, luego de cada compuerta tipo  $X_\theta$  o  $Z_\theta$  se teleporta el qubit sobre el cual se aplicó la compuerta, utilizando los circuitos de “teleportación  $X$ ” y “teleportación  $Z$ ” que se muestran en las Figuras 2.10 a y b (aunque en realidad la palabra “teleportación” no describe correctamente la situación ya que en estos esquemas hay una interacción directa entre el qubit original y el destinatario del estado). Estos circuitos transfieren el estado de un qubit a otro a menos de un error de Pauli conocido a través del resultado de la medición sobre el primer qubit.

Para que las compuertas  $X_\theta$  y  $Z_\theta$  conmuten con los errores de Pauli y la interacción que aparecen en el circuito pseudo-teleportador, se aplica teleportación tipo  $X$  luego de las compuertas  $X_\theta$  y tipo  $Z$  luego de las  $Z_\theta$ . Utilizando además el hecho de que la compuerta  $CNOT$  se puede obtener combinando  $CZ$  y  $H$  (Figura 2.4), las compuertas  $X_\theta$  y  $Z_\theta$  seguidas de pseudo-teleportación se reescriben según se muestra en la Figura 2.11.

El circuito escrito como una repetición de compuertas  $Z_\theta$ ,  $X_\theta$ , y  $CZ$  opcionales (según se lo muestra en la Figura 2.9) se modifica, entonces, teleportando cada qubit luego de aplicarle una compuerta  $X_\theta$  o  $Z_\theta$ , como se indica en la Figura 2.11; el resultado se muestra en la Figura 2.12.



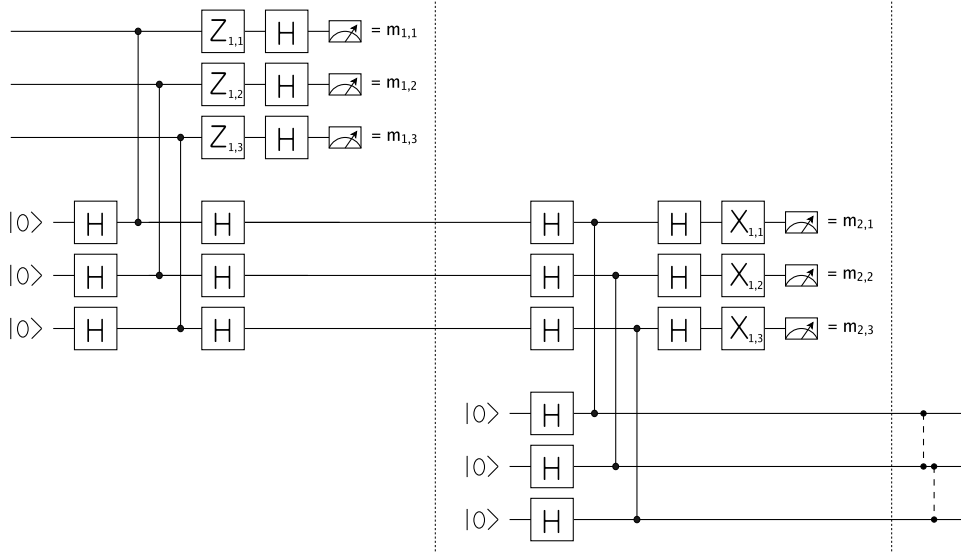
**Figura 2.10:** Circuitos de pseudo-teleportación. a) La “teleportación  $Z$ ” transfiere el estado del qubit original al del segundo qubit, a menos de un error de Pauli conocido  $Z^a$  (que depende del resultado de la medición sobre el primer qubit). b) La “teleportación  $X$ ” tiene el mismo resultado, ahora a menos de un error de Pauli conocido  $X^b$ .



**Figura 2.11:** Las compuertas  $Z_\theta$  (a) y  $X_\theta$  (b) se reescriben incorporando una teleportación luego de la aplicación de la compuerta. Luego se conmutan con la interacción entre qubits  $CNOT$  del circuito de teleportación, y finalmente se obtiene el  $CNOT$  como composición de  $CZ$  y  $H$ .

La medición final en la base computacional sobre cada qubit, precedida por las compuertas de rotación  $X_\theta$  o  $Z_\theta$  y  $H$ , puede interpretarse como una medición en una base rotada (esto se distingue en el gráfico con una doble línea de contorno del “aparato de medición”); por otra parte, usando que  $H^2 = I$  y que  $H|0\rangle = |+\rangle$ , se puede simplificar el esquema de la figura anterior en la forma que se muestra en la Figura 2.13.

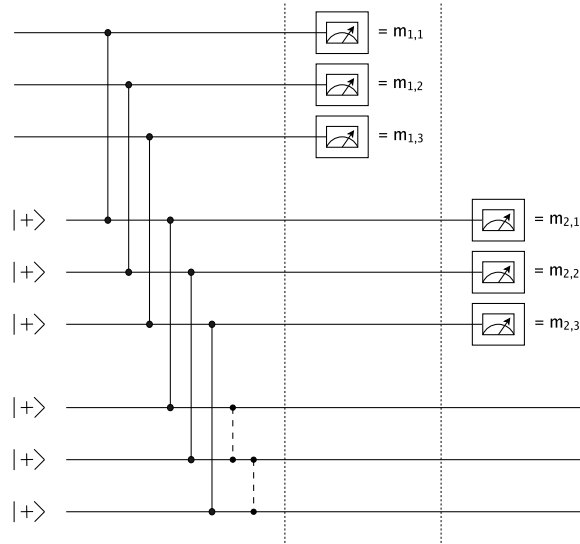
En esta última versión del circuito, el cómputo queda claramente separado en dos etapas diferentes: todas las interacciones están concentradas al inicio del cómputo, y producen un estado-grafo. Luego se realizan secuencias de mediciones en bases rotadas, sobre cada qubit por separado; en cada secuencia se miden los qubits asociados a una cierta hilera del grafo. El estado-grafo que se prepara depende del cómputo a través de su tamaño, pero también a causa de las compuertas  $CZ$  opcionales: el grafo asociado



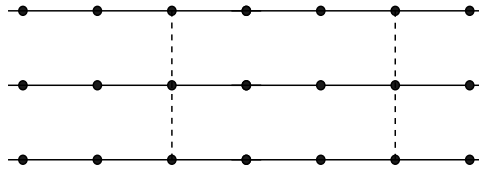
**Figura 2.12:** Un cómputo en el modelo de circuitos puede descomponerse como una repetición de una secuencia compuesta por una ronda de rotaciones  $Z_{i,j}$ , otra de  $X_{i,j}$ , y una ronda de compuertas  $CZ$  opcionales entre pares de qubits vecinos (dibujadas con línea punteada). Luego de cada compuerta de rotación se teleporta el estado a otro qubit. Las líneas verticales punteadas separan las tres etapas en cada secuencia.

es igual a un grafo tipo cluster de dos dimensiones en el que algunas de las uniones están borradas (ver Figura 2.14).

Por otra parte, quedan pendientes los errores de Pauli cometidos al teleportar: si todas las mediciones obtienen 0 como resultado, entonces el estado se teleporta exitosamente en cada paso, pero en caso contrario aparecen errores de Pauli de forma conocida. El modo en que se puede lidiar con esta dificultad es simplemente arrastrando estos errores, y eligiendo en qué base realizar cada medición de modo de ir cancelando los errores a medida que es necesario. Por ejemplo, supongamos que se tiene un qubit cuyo estado debería ser  $|\psi\rangle$ , y se quiere aplicar sobre éste una compuerta  $X_\theta$ , para obtener el estado  $|\psi'\rangle = X_\theta|\psi\rangle$ . Pero este qubit tiene un error de Pauli de forma  $X^a$ , de modo que el estado es en realidad  $X^a|\psi\rangle$ . El estado deseado puede obtenerse a menos del mismo error de Pauli, ya que la compuerta  $X_\theta$  conmuta con el error, y entonces el estado luego de aplicarla será  $X^a|\psi'\rangle$ . Si en cambio el error de Pauli es tipo  $Z^b$ , se tiene que  $X_\theta Z^b = Z^b X_{(-1)^b\theta}$ , de modo que en lugar de aplicar la compuerta  $X_\theta$  hay que aplicar  $X_{(-1)^b\theta}$ , para obtener el estado deseado a menos del error de Pauli conocido  $Z^b$ . Como los errores de



**Figura 2.13:** Un cómputo en el modelo de circuitos puede descomponerse en una primera etapa de preparación de un estado-grafo, seguida de una secuencia de mediciones en bases arbitrarias sobre cada qubit separadamente; las secuencias se muestran separadas por líneas punteadas. Las compuertas  $CZ$  marcadas con línea punteada son opcionales.



**Figura 2.14:** Un cómputo en el modelo de circuitos puede descomponerse en una primera etapa de preparación de un estado-grafo, seguida de una secuencia de mediciones en bases arbitrarias sobre cada qubit separadamente. El estado-grafo inicial depende del cálculo a realizar a través de su tamaño y de la presencia de las compuertas  $CZ$  opcionales, y es igual a un estado tipo cluster de dos dimensiones con algunas uniones borradas.

Pauli en cada paso dependen del resultado de las mediciones en los circuitos de pseudoteleportación, es necesario mantener el orden correcto entre las distintas mediciones, de modo de ir acomodando las bases para compensar los errores.

Por último, queda por resolver la dependencia del estado-grafo con los  $CZ$  opcionales: el modo de ver que el estado-grafo correspondiente a un cluster de dos dimensiones sirve para realizar cualquier cómputo es notando

que es posible realizar compuertas en exceso, y luego deshacerlas. Esto es porque si se mide un qubit de un estado-grafo en la base computacional, el estado resultante es el que corresponde a un estado-grafo igual al anterior pero en el que se borró el vértice correspondiente al qubit medido (a menos de compuertas  $Z$  en los vecinos del qubit medido, pero esto sólo introduce otro error de Pauli conocido). Para implementar las compuertas  $CZ$  opcionales, entonces, es necesario introducir en el grafo vértices auxiliares que actúen como intermediarios en las interacciones entre qubits de la misma hilera: si estos qubits intermediarios son medidos en la base computacional simplemente desaparecen del grafo, mientras que si se los mide en la base  $X$  el resultado es un grafo con la interacción aplicada (los detalles de este procedimiento, y del modo de tratar a los errores de Pauli, se pueden encontrar en el paper de Childs, Leung y Nielsen [16]). El costo de la universalidad del estado inicial es, por lo tanto, el agregado de los qubits intermediarios. La conveniencia de pagar este precio depende del mecanismo utilizado para la generación del estado-grafo: si la disposición experimental favorece una dada geometría, por ejemplo si se tiene un sistema de spines colocados en una red bidimensional, entonces puede que lo más conveniente sea preparar el estado cluster y luego borrar los qubits innecesarios; en caso contrario, lo más económico es preparar directamente el estado-grafo que contenga sólo las interacciones requeridas para el cómputo.

## Capítulo 3

# Funciones de Wigner discretas utilizando cuerpos finitos

Las funciones de Wigner constituyen una herramienta para estudiar sistemas cuánticos a través de su representación en un espacio de fases, en forma alternativa a la representación de los estados como vectores de un espacio de Hilbert [25, 26]. La formulación original de la función de Wigner, aplicable únicamente a sistemas con dimensión continua, fue posteriormente generalizada con el objetivo de incorporar la descripción de estados de spin, o de partículas cuyos grados de libertad de posición y momento se encuentran discretizados [27, 28, 29, 30, 3].

En [30], Wootters presenta una función de Wigner que para sistemas con dimensión discreta prima  $d$  usa como espacio de fases una grilla de  $d \times d$  puntos, y cuya extensión a sistemas con dimensiones discretas no primas requiere de un espacio de fases que es un producto cartesiano de los espacios correspondientes a los factores primos de  $d$ . O sea, se trata a cualquier sistema de dimensión no prima a través de su descomposición en subsistemas de dimensión prima. Este tratamiento no resulta apropiado para dimensiones grandes arbitrarias, porque la visualización de la función de Wigner es difícil, y también la comparación del límite semiclásico con el caso continuo.

Como alternativa, es posible definir funciones de Wigner para dimensión discreta  $d$  utilizando como espacio de fases una sola grilla de  $d \times d$  puntos cuando  $d$  es impar [31], mientras que, cuando la dimensión  $d$  es par, para conservar las propiedades de la función de Wigner original es necesaria una grilla de  $2d \times 2d$  puntos [32]. En este caso, se introducen redundancias en

la representación en el espacio de fases, y es posible recuperar toda la información sobre el estado a partir de un subconjunto de  $d \times d$  puntos. Esta particularidad se traduce en la aparición de efectos de interferencia de un estado consigo mismo, o “imágenes fantasma”.

Más recientemente, Wootters propuso una formulación de la función de Wigner en un espacio de  $d \times d$  puntos que se aplica a sistemas cuya dimensión  $d$  es una potencia entera de un número primo [33]. En esta definición, presentada y analizada con más detalle en [3], se rotulan las coordenadas del espacio de fases con elementos del cuerpo finito  $GF(d)$ , dotando al espacio de fases de propiedades geométricas muy similares a las del caso continuo. A partir del uso de estas propiedades en la construcción de la función de Wigner, es posible encontrar relaciones con problemas como el de la reconstrucción tomográfica del estado o la existencia de bases del espacio de Hilbert mutuamente “no sesgadas” o “conjugadas” [34]. Dado que en computación cuántica se trata con sistemas de dimensión  $d = 2^n$ , esta definición de la función de Wigner podría ser de utilidad para el análisis de problemas en esta área (en [4] se estudian la representación de códigos de corrección de errores y la resolución del *mean king problem* por medio de esta función de Wigner).

A lo largo de este capítulo se presentará la función de Wigner original, definida para un sistema cuyo espacio de estados es un continuo, y la generalización propuesta en [3] para sistemas con espacios de Hilbert cuya dimensión es una potencia entera de un número primo (en especial el caso  $d = 2^n$ ). Para esto, será necesario introducir previamente el espacio de fases utilizado, y algunos conceptos relacionados con los cuerpos de Galois, cuyos elementos rotulan las coordenadas del espacio de fases. Siguiendo los pasos desarrollados en [3, 4], la construcción de la función de Wigner discreta se realizará a partir de la imposición de un conjunto de propiedades que son esenciales en la función de Wigner continua; en este procedimiento cumplen un rol fundamental los operadores de Pauli, identificados con las traslaciones en el espacio de fases. Se mostrará que las líneas del espacio de fases están asociadas a estados estabilizadores del sistema de qubits; más precisamente, los conjuntos de líneas paralelas están asociados a bases ortonormales del espacio de Hilbert formadas por estados estabilizadores, y estas bases resultan ser mutuamente no sesgadas. Una vez completa la definición de la función de Wigner, se darán ejemplos de representaciones en el espacio de fases de distintos estados de un sistema de qubits. Finalmente, se presentará un mecanismo para construir funciones de Wigner alternativas, que pueden resultar convenientes en el estudio de problemas relacionados con estados-grafo.



### 3.1. La función de Wigner en el espacio de fases continuo

La definición original de la función de Wigner  $W$  permite describir el estado de una partícula que se mueve en una dimensión; el espacio de fases de este sistema es un plano con coordenadas reales de posición ( $q$ ) y momento ( $p$ ), y  $W$  es una función que toma valores reales en este plano, proporcionando un modo de representar el estado de la partícula en su espacio de fases [26]. Esta representación es ideal para la comparación del comportamiento de un sistema clásico con su análogo cuantizado, a través del estudio de las diferencias entre la función de Wigner y la distribución clásica de probabilidad. Para cada estado, la función de Wigner contiene toda la información que pueda obtenerse por medio de la matriz densidad, y viceversa; ambas representaciones son equivalentes.

Una de las propiedades cruciales de la función de Wigner es que al integrar sus valores a lo largo de las rectas en el espacio de fases es posible calcular distribuciones de probabilidad; en particular, la integral a lo largo de las líneas verticales (con  $q$  constante) permite obtener la densidad de probabilidad para una medición de la posición, e integrar sobre  $q$  para un valor de  $p$  constante permite hallar la densidad de probabilidad de los momentos. Sin embargo, la función de Wigner no puede interpretarse como una densidad de probabilidad para cada punto del espacio de fases porque no es definida positiva; por ejemplo, la función de Wigner de una superposición coherente de paquetes gaussianos en el espacio de fases contiene términos de interferencia que oscilan tomando valores positivos y negativos.

Para el sistema descrito, la función de Wigner se define a partir de la matriz densidad en la forma:

$$W(q, p) = \frac{1}{\pi\hbar} \int \langle q-x | \rho | q+x \rangle e^{2ipx/\hbar} dx \quad (3.1)$$

donde  $\{|x\rangle, x \in \mathbb{R}\}$  es la base de autoestados de posición; la función  $W$  así definida satisface las siguientes propiedades:

1.  $W(q, p)$  es una función real.
2. El producto interno entre dos estados puede calcularse utilizando sus funciones de Wigner, según:

$$\text{Tr}(\rho_1 \rho_2) = 2\pi\hbar \int \int W_1(q, p) W_2(q, p) dq dp \quad (3.2)$$

3. La integral de la función de Wigner sobre la franja del espacio de fases rodeada por las líneas de ecuaciones  $aq+bp = c_1$  y  $aq+bp = c_2$  es igual

a la probabilidad de obtener un resultado entre  $c_1$  y  $c_2$  en una medición del observable  $aQ + bP$  donde  $Q$  y  $P$  son los operadores de posición y momento respectivamente. Una consecuencia de esta propiedad es que  $W(q, p)$  está normalizada, esto es, su integral sobre todo el espacio de fases vale 1.

La expresión (3.1) puede reescribirse en términos de los llamados “operadores de punto”  $A(q, p)$ , en la forma:

$$W(q, p) = \text{Tr}(\rho A(q, p)) \quad (3.3)$$

con

$$A(q, p) = \frac{1}{\pi\hbar} \int |q+x\rangle\langle q-x| e^{2ipx/\hbar} dx \quad (3.4)$$

Los operadores  $A(q, p)$  son hermíticos, tienen traza  $1/(2\pi\hbar)$  y forman una base ortogonal para el espacio de operadores hermíticos. En particular, la expansión de la matriz densidad en esta base está dada por:

$$\rho = 2\pi\hbar \int W(q, p) A(q, p) dq dp \quad (3.5)$$

es decir, la función de Wigner proporciona los coeficientes en el desarrollo de  $\rho$  en términos de los operadores de punto.

Una expresión alternativa para los operadores  $A(q, p)$  los relaciona con el operador de reflexión  $R$  (que opera en la base de posición en la forma  $R|x\rangle = |-x\rangle$ ), según:

$$A(q, p) = \frac{1}{\pi\hbar} T(q, p) R T(q, p) \quad (3.6)$$

donde  $T(q, p) = e^{-(i/\hbar)(qP - pQ)}$  es el operador de traslación en  $(q, p)$  en el espacio de Hilbert. O sea, los operadores de punto corresponden a operadores de reflexión trasladados, cuyo valor de expectación está dado por la función de Wigner. Esto muestra que todos los operadores de punto se relacionan a través de traslaciones, en la forma:

$$A(q, p) = T(q, p) A(0, 0) T^\dagger(q, p) \quad (3.7)$$

(donde  $A(0, 0)$  es proporcional al operador de reflexión  $R$ ). Como consecuencia, la función de Wigner es covariante frente a traslaciones, o sea, si se traslada el estado en el espacio de Hilbert aplicando un operador  $T(q, p)$ , su función de Wigner se traslada a su vez en el espacio de fases.

## 3.2. Funciones de Wigner para sistemas de qubits usando cuerpos finitos

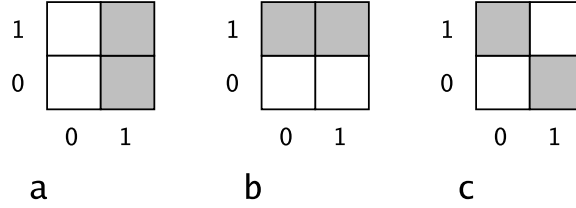
### 3.2.1. El espacio de fases y los cuerpos de Galois

Para definir la función de Wigner en un sistema de dimensión discreta, en primer lugar es necesario definir un espacio de fases apropiado. En analogía con la función de Wigner continua, en este espacio de fases hay que definir líneas, y cada una de estas líneas debe estar asociada a algún proyector en el espacio de Hilbert del sistema; de esta forma es posible imponer las propiedades tomográficas de la función de Wigner continua en el caso discreto, esto es, se puede pedir que la suma de los valores a lo largo de cada línea esté asociada a la probabilidad de obtener un cierto resultado en una dada medición.

#### Por qué el caso de dimensión prima es especial

Si se tiene un sistema con dimensión  $d$  entera finita, la elección más natural para el espacio de fases es una grilla con  $d \times d$  puntos, donde las coordenadas, que se identifican con la posición y el momento, son números de 0 a  $d - 1$ . A continuación es necesario definir las líneas en esta grilla. En el caso continuo, en que las coordenadas son números reales, las líneas corresponden a conjuntos de puntos  $(q, p)$  que son soluciones de ecuaciones lineales de la forma  $aq + bp = c$ , donde  $a, b, c \in \mathbb{R}$  y  $a, b$  no pueden ser los dos cero. Traduciendo esta definición al caso discreto, las líneas serían los conjuntos de puntos  $(q, p)$  que satisfacen ecuaciones  $aq + bp = c$ , donde ahora  $a, b, c$  son números enteros. Es fácil ver que para que esta definición tenga sentido la suma y el producto no pueden ser los mismos que los definidos para los números enteros: la ecuación  $q + p = 0$ , por ejemplo, sólo tendría una solución (el origen) así que correspondería a un punto y no a una línea. En cambio, es posible definir las líneas como soluciones a ecuaciones lineales donde las operaciones son módulo  $d$ . En la Figura 3.1 se muestran el espacio de fases y todas las líneas en él, agrupadas en conjuntos de líneas paralelas, o “estriaciones”, para el caso  $d = 2$ , correspondiente a 1 qubit.

Cuando  $d$  es un número primo, los números enteros de 0 a  $d - 1$  forman un cuerpo finito, de modo que la suma y el producto módulo  $d$  son operaciones cerradas en este conjunto de elementos, y además son inversibles (excepto la multiplicación por cero). A consecuencia de esto las líneas tienen propiedades similares a las de las rectas en el plano  $\mathbb{R}^2$ : dados dos puntos existe una única línea que los une; dos líneas o son paralelas (esto es, los cocientes entre  $a$  y



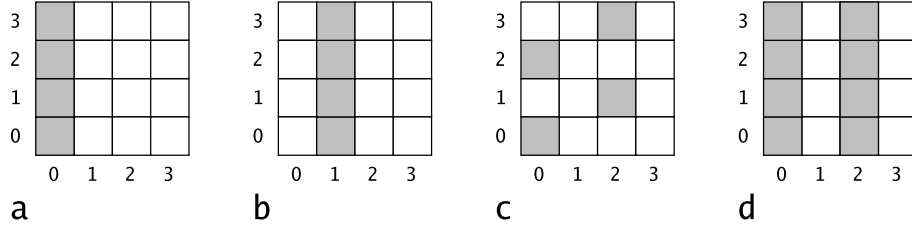
**Figura 3.1:** El espacio de fases para un sistema de dimensión 2; las coordenadas se rotulan con los números 0, 1; las líneas son los conjuntos de puntos  $(q, p)$  que son soluciones de ecuaciones  $aq + bp = c$ , donde la suma y el producto son módulo 2. En total hay 6 líneas, agrupadas en tres estriaciones o conjuntos de líneas paralelas: a) la estriación vertical, con líneas de la forma  $q = c$ ; b) la estriación horizontal, con las líneas  $p = c$ ; c) la estriación diagonal, formada por las líneas  $q + p = c$ . El valor  $c = 0$  se muestra en blanco, y  $c = 1$  en gris.

$b$  son iguales) o se cortan en exactamente un punto; dados un punto y una línea que no lo contiene existe una única paralela que pasa por ese punto; dos líneas paralelas distintas no comparten ningún punto; todas las líneas tienen la misma cantidad ( $d$ ) de puntos.

Cuando la dimensión no es prima, el producto módulo  $d$  no es inversible: por ejemplo, si  $d = 4$  se tiene que  $2 \cdot 2 = 0$ , o sea, el número 2 no tiene inverso multiplicativo. Entonces, las líneas ya no tienen las bonitas propiedades del caso en que la dimensión es prima: no existe una noción clara de paralelismo, y no todas las líneas tienen igual cantidad de puntos (ver Figura 3.2). Esto no es una dificultad insalvable, y de hecho existen definiciones de la función de Wigner donde las líneas están definidas de esta forma. Sin embargo, las propiedades geométricas del espacio de fases influyen en la construcción de la función de Wigner, y algunas propiedades deseables se pierden al usar aritmética módulo  $d$  para dimensiones no primas.

### La alternativa de usar cuerpos de Galois

Cuando el sistema cuántico estudiado tiene dimensión  $d$  igual a una potencia entera de un primo  $p$  ( $d = p^n$ ), existe un cuerpo finito con  $d$  elementos, llamado cuerpo de Galois ( $GF(d)$ ) [35]. Si  $d$  es un número primo, los elementos del cuerpo son los números de 0 a  $d - 1$ , con la suma y el producto definidos módulo  $d$ . Cuando  $d = p^n$  los elementos del cuerpo  $GF(d)$  se definen a partir de los de  $GF(p)$ . En primer lugar, es necesario encontrar un polinomio  $P(x)$  con coeficientes en  $GF(p)$ , de grado  $n$ , irreducible y que no sea factor de ningún polinomio de la forma  $1 + x^m$  con  $m < p^n - 1$ . Un poli-



**Figura 3.2:** El espacio de fases para un sistema de dimensión 4; las coordenadas se rotulan con los números de 0 a 3; las líneas son los conjuntos de puntos  $(q, p)$  que son soluciones de ecuaciones  $aq + bp = c$ , donde la suma y el producto son módulo 4. A causa de que el producto no es inversible, las líneas no tienen las propiedades de las rectas en el plano  $\mathbb{R}^2$ . a) La línea  $q = 0$ ; b) La línea  $q = 1$ , no comparte ningún punto con la anterior; c) la línea  $q + 2p = 0$ , comparte dos puntos con la primera y ninguno con la segunda; d) la línea  $2q = 0$ , tiene el doble de puntos que las anteriores.

nomio con estas propiedades se llama el “polinomio primitivo” del cuerpo  $GF(d)$ . Una vez hallado un polinomio primitivo, se inventa un elemento  $\omega$  que satisface  $P(\omega) = 0$ , al que se llama “elemento generador” del cuerpo. Con esto es posible construir el cuerpo  $GF(d)$ : sus elementos son el cero y todas las potencias del elemento generador:  $\{0, 1, \omega, \dots, \omega^{d-2}\}$ , y se verifica que  $\omega^{d-1} = \omega^0 = 1$ , o sea que las potencias de  $\omega$  son cíclicas.

Alternativamente, sabiendo que  $P(\omega) = 0$  pueden escribirse todos los elementos del cuerpo como combinaciones lineales de la forma:

$$x = \sum_{j=0}^{n-1} x_j \omega^j \quad (3.8)$$

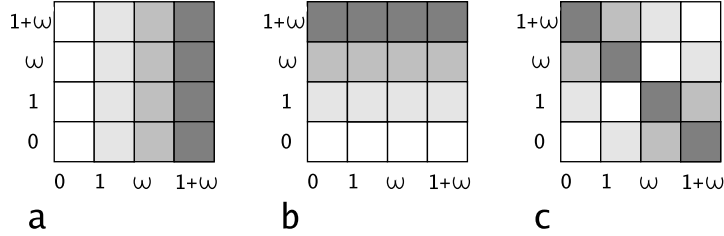
donde  $x_j$  es un número de 0 a  $p - 1$ . La suma de los elementos es módulo  $p$  en los coeficientes  $x_j$ ; el producto de elementos del cuerpo está determinado por la condición de que  $P(\omega) = 0$ , y de que el producto de dos coeficientes es módulo  $p$ . En total, hay  $d$  elementos en el cuerpo (correspondientes a todas las posibles elecciones de coeficientes  $x_j$ , o todas las potencias de  $\omega$  más el cero).

Por ejemplo, para el caso de dos qubits el único polinomio primitivo posible es  $P(x) = x^2 + x + 1$ ; entonces, el elemento generador  $\omega$  satisface  $P(\omega) = \omega^2 + \omega + 1 = 0$ , o sea  $\omega^2 = 1 + \omega$ ; puede verse que  $\omega^3 = \omega(1 + \omega) = \omega + (1 + \omega) = 1$ . El cuerpo tiene en total 4 elementos:  $\{0, 1, \omega, 1 + \omega\}$ .

Los elementos en la ecuación 3.8 están desarrollados en la “base canónica” del cuerpo,  $B_\omega = \{e_0, \dots, e_{n-1}\}$ , con  $e_j = \omega^j$ . La llamada “base dual”  $\tilde{B}_\omega = \{\tilde{e}_0, \dots, \tilde{e}_{n-1}\}$  es la compuesta por los elementos  $\tilde{e}_j$  que verifican

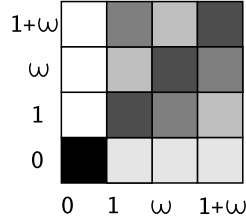
$\text{tr}(e_i \tilde{e}_j) = \delta_{ij}$ . La notación de traza con minúscula refiere a la traza definida en el cuerpo  $GF(d)$ , que es una operación lineal que toma valores entre 0 y  $p - 1$ .

Si elegimos como coordenadas  $(q, p)$  del espacio de fases a los elementos de  $GF(d)$  (ordenados como sucesivas potencias de  $\omega$ ), y definimos las líneas como los conjuntos de puntos  $(q, p)$  que satisfacen ecuaciones  $aq + bp = c$  donde  $a, b, c \in GF(d)$  y  $a, b$  no son los dos cero, entonces la estructura del cuerpo garantiza que las líneas definidas satisfacen todas las propiedades enunciadas para el caso de dimensión prima. Para cada elección de los parámetros  $a, b$ , es posible obtener un conjunto de  $d$  líneas paralelas variando  $c$ ; esta colección de líneas contiene a todos los puntos y constituye una estriación del espacio de fases. Variando los parámetros  $a, b$  es posible obtener  $d + 1$  estriaciones diferentes. En la Figura 3.3 se muestra el espacio de fases para un sistema de dos qubits, con los puntos repartidos en tres estriaciones diferentes.



**Figura 3.3:** El espacio de fases con coordenadas rotuladas utilizando elementos de  $GF(4)$  para un sistema de dos qubits, con sus puntos repartidos en tres estriaciones diferentes: a) la estriación vertical, correspondiente a líneas de la forma  $q = c$ ; b) la estriación horizontal, con las líneas  $p = c$ ; c) la estriación diagonal “principal”, conteniendo las líneas de ecuación  $q + p = c$ .

En lo sucesivo, los puntos del espacio de fases se indicarán con letras griegas  $\alpha, \beta$ , etc, en la forma  $\alpha = (q_\alpha, p_\alpha)$ . Las estriaciones se rotularán con un índice  $\kappa$ , usando la notación  $\lambda^{(\kappa)}$  para una línea  $\lambda$  que pertenece a la estriación  $\kappa$ ,  $\lambda_\alpha^{(\kappa)}$  para la línea en la estriación  $\kappa$  que pasa por el punto  $\alpha$ , y  $\lambda_{\alpha, \beta}$  para la línea que une los puntos  $\alpha$  y  $\beta$ . Las líneas que pasan por el origen,  $\lambda_{0, \alpha}$  (con  $\alpha \neq 0$ ), son los “rayos” del espacio de fases; en cada una de las estriaciones hay un rayo. En la Figura 3.4 se muestran todos los rayos para el caso de 2 qubits.



**Figura 3.4:** Los rayos en el espacio de fases con coordenadas rotuladas utilizando elementos de  $GF(4)$  para un sistema de dos qubits. Cada rayo se indica con un tono de gris diferente. Hay un rayo por cada estriación, y todos los rayos se intersecan en el origen.

### 3.2.2. La generalización de la función de Wigner a dimensión discreta $d = p^n$

Las propiedades de la función de Wigner para sistemas continuos pueden traducirse al caso discreto en la forma:

1.  $W(\alpha)$  es una función real.
2. El producto interno entre dos estados puede calcularse utilizando sus funciones de Wigner según:

$$\text{Tr}(\rho_1 \rho_2) \sim \sum_{\alpha} W_1(\alpha) W_2(\alpha) \quad (3.9)$$

donde  $\sim$  indica una igualdad a menos de un factor constante.

3. La suma de los valores de la función de Wigner a lo largo de una línea cualquiera  $\lambda$  en el espacio de fases debe ser igual a la probabilidad de obtener en una medición el resultado correspondiente a un cierto proyector  $P(\lambda)$  asociado a esa línea ( $P(\lambda)$  opera en el espacio de Hilbert):

$$\sum_{\alpha \in \lambda} W(\alpha) = \text{Tr}(\rho P(\lambda)) = p_{\lambda} \quad (3.10)$$

Considerando el estado totalmente mixto,  $\rho = 1/d I$ , la condición (3.10) implica que la suma sobre cualquier línea  $\lambda$  de los valores de  $W$  para este estado debe ser igual a  $1/d$ . A causa de las propiedades geométricas de las líneas, para que esto se verifique la función de Wigner de este estado debe tener un valor de  $1/d^2$  para todos los puntos del espacio de fases. Si se aplica la propiedad (3.9) para el producto de este estado consigo mismo,

puede verse que la constante de proporcionalidad debe ser igual a  $d$ , o sea que:

$$\text{Tr}(\rho_1\rho_2) = d \sum_{\alpha} W_1(\alpha)W_2(\alpha) \quad (3.11)$$

Aplicando ahora esta propiedad para el producto interno entre el estado totalmente mixto y otro estado arbitrario, es posible recuperar la condición de normalización de la función de Wigner, en la forma:

$$\sum_{\alpha} W(\alpha) = 1. \quad (3.12)$$

Para que valgan simultáneamente las propiedades de normalización (3.12) y de probabilidades (3.10) es necesario que la suma de los proyectores asociados a las  $d$  líneas de una dada estriación sea igual a la identidad; para esto, las  $d$  líneas en cada estriación deben estar asociadas a  $d$  vectores ortonormales en el espacio de Hilbert.

Usando las propiedades geométricas del espacio de fases y la condición de normalización es posible invertir la condición (3.10) y obtener una expresión para el valor de la función de Wigner en cada punto en función de las probabilidades asociadas a las distintas líneas:

$$W(\alpha) = \frac{1}{d} \left\{ \sum_{\kappa} \text{Tr}(\rho P(\lambda_{\alpha}^{(\kappa)})) - 1 \right\} = \frac{1}{d} \left\{ \sum_{\kappa} p_{\lambda_{\alpha}^{(\kappa)}} - 1 \right\} \quad (3.13)$$

El valor de la función de Wigner en un punto dado, entonces, depende de las probabilidades para los proyectores asociados a todas las líneas (una de cada estriación) que pasan por ese punto.

### 3.2.3. La condición de covariancia frente a traslaciones, y sus consecuencias

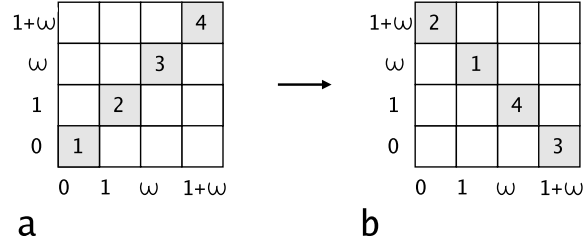
También por analogía con la función de Wigner continua, se requiere de la función de Wigner discreta que sea covariante frente a traslaciones, esto es, que al aplicar sobre un estado una traslación en el espacio de Hilbert su nueva función de Wigner corresponda a una traslación en el espacio de fases de la función de Wigner inicial.

#### La definición de las traslaciones

Las traslaciones en el espacio de fases son operaciones  $\mathcal{T}_{\beta}$  que actúan sobre un punto  $\alpha$  en la forma:  $\mathcal{T}_{\beta} \alpha = \alpha + \beta$ , donde la suma de puntos se define como:  $\alpha + \beta = (q_{\alpha} + q_{\beta}, p_{\alpha} + p_{\beta})$ . Al aplicar una traslación sobre los puntos de una línea, se obtiene una línea paralela, o sea, en la misma



estriación que la línea original; partiendo del rayo de una dada estriación, pueden obtenerse todas las líneas paralelas a él aplicando traslaciones. En la Figura 3.5 se muestra el efecto de aplicar una traslación  $\mathcal{T}_{(1,\omega)}$  sobre los puntos del rayo diagonal principal. La composición de dos traslaciones es siempre otra traslación. Para el caso de un sistema de qubits, como los coeficientes en la expansión (3.8) se suman módulo 2, la composición de cualquier traslación consigo misma es igual a la identidad.



**Figura 3.5:** Las traslaciones en el espacio de fases son operadores  $\mathcal{T}_\beta$  que mapean cada línea en otra (o la misma) en la misma estriación. a) El rayo diagonal principal. b) El resultado luego de aplicar la traslación  $\mathcal{T}_{(1,\omega)}$  es otra línea “paralela” a la anterior.

Estas traslaciones en el espacio de fases deben asociarse a traslaciones en el espacio de Hilbert, que pueden definirse como operadores de Pauli generalizados. El caso en que  $p$  es un número primo impar puede tratarse en forma similar al de un sistema compuesto por qubits, con operadores de Pauli generalizados a la dimensión requerida. De ahora en adelante el desarrollo se refiere sólo a sistemas de qubits, para los que los operadores de traslación se definen en la forma:

$$T(\vec{q}, \vec{p}) = \sigma_{\vec{q}, \vec{p}} = X^{\vec{q}} Z^{\vec{p}} e^{i\frac{\pi}{2} \vec{q} \cdot \vec{p}} \quad (3.14)$$

Las propiedades de los operadores de Pauli se describen en la sección 2.2. Al igual que ocurre con las traslaciones en el espacio de fases, el cuadrado de una traslación en el espacio de Hilbert es igual a la identidad. Además, la composición de traslaciones es otra traslación, pero a menos de una fase  $(\pm 1, \pm i)$ ; en consecuencia, a diferencia de lo que sucede con las traslaciones en el espacio de fases, las traslaciones en el espacio de Hilbert pueden conmutar o anticonmutar.

## Consecuencias de imponer la covariancia

Para relacionar las traslaciones  $\mathcal{T}_{(q,p)}$  en el espacio de fases con las traslaciones  $T(\vec{q}, \vec{p})$  en el espacio de Hilbert es necesario establecer una relación entre los elementos  $(q, p)$  del cuerpo  $GF(d)$  y las  $n$ -uplas  $(\vec{q}, \vec{p})$ . Una vez determinada esta relación, la condición de covariancia frente a traslaciones implica que la asociación entre líneas del espacio de fases y proyectores debe satisfacer:

$$P(\mathcal{T}_{(q,p)} \lambda) = T(\vec{q}, \vec{p})P(\lambda)T^\dagger(\vec{q}, \vec{p}) \quad (3.15)$$

para toda línea  $\lambda$  y para cualquier traslación  $\mathcal{T}_{(q,p)}$ . Esto quiere decir que al trasladar una línea del espacio de fases se obtiene otra línea cuyo proyector asociado corresponde a una traslación en el espacio de Hilbert del proyector de la línea original.

Consideremos una estriación cualquiera, cuyas líneas son de la forma  $aq + bp = c$  con  $a, b$  fijos y  $c \in GF(d)$ . Estas líneas son invariantes frente a traslaciones de la forma  $\mathcal{T}_{(b\omega^j, a\omega^j)}$ , para cualquier  $j = 0, \dots, d-2$ . Los puntos  $(b\omega^j, a\omega^j)$ , unidos al  $(0, 0)$ , forman el rayo de esta estriación (ya que todos estos puntos satisfacen la ecuación  $aq + bp = 0$ ). La condición de covariancia (3.15) implica que los proyectores correspondientes a las líneas en esta estriación deben ser autoestados del conjunto de traslaciones en el espacio de Hilbert asociadas a las traslaciones  $\mathcal{T}_{(b\omega^j, a\omega^j)}$  en el espacio de fases. Esto es, las  $d$  líneas en esta estriación tienen que estar asociadas a la base ortonormal del espacio de Hilbert compuesta por los autoestados comunes de los operadores  $T(\vec{q}, \vec{p})$  correspondientes a puntos  $(b\omega^j, a\omega^j)$  en el rayo de la estriación. Y para que esto sea posible, los  $d-1$  operadores de esta forma deben conmutar.

En resumen:

1. Para cada punto  $(q, p)$  en el espacio de fases existe una traslación en el espacio de fases  $\mathcal{T}_{(q,p)}$ , que está asociada a una traslación  $T(\vec{q}, \vec{p})$  en el espacio de Hilbert; los operadores de traslación en el espacio de Hilbert son los operadores de Pauli generalizados.
2. El conjunto de  $d$  puntos en cada rayo debe estar asociado a un conjunto de  $d$  operadores de Pauli que conmutan (el origen corresponde a la identidad).
3. Cada estriación está asociada a una base ortonormal de autoestados comunes de los operadores de Pauli correspondientes al rayo de esa estriación.

Dado que hay  $d + 1$  rayos, los  $d^2 - 1$  operadores de Pauli  $T(\vec{q}, \vec{p})$  no triviales quedan agrupados en  $d + 1$  conjuntos, cada uno conteniendo  $d - 1$  operadores que conmutan. Usando las propiedades de las matrices de Pauli es posible demostrar que las  $d + 1$  bases asociadas a estos  $d + 1$  conjuntos resultan ser mutuamente conjugadas, o sea, verifican:

$$\text{Tr}\left(P(\lambda^{(\kappa)})P(\lambda^{(\kappa')})\right) = \frac{1}{d} \quad \forall \kappa \neq \kappa' \quad (3.16)$$

Esto es, las bases son mutuamente conjugadas si cada estado en una de las bases puede escribirse como una superposición de los  $d$  estados de cualquiera de las otras bases, en que los  $d$  coeficientes son iguales en módulo. Equivalentemente, si sobre un estado de una de las bases se realiza una medición que proyecta sobre cualquiera de las otras bases, todos los resultados tienen igual probabilidad [34].

### Cómo se construyen los conjuntos de operadores de Pauli que conmutan

Para seguir adelante en la construcción es necesario determinar una relación entre los puntos  $(q, p)$  y las  $n$ -uplas  $(\vec{q}, \vec{p})$  en forma tal que los operadores  $T(\vec{q}, \vec{p})$  asociados a cada rayo conmuten. A partir de una matriz binaria  $M$ , es posible construir conjuntos de  $d - 1$  operadores de Pauli que conmutan, dados por:

$$S_{(\vec{b}, \vec{a})} = \left\{ T(\vec{b}M^j, \vec{a}\widetilde{M}^j) \quad j = 0, 1, \dots, d - 2 \right\}, \quad (3.17)$$

donde  $\widetilde{M}$  es la transpuesta de  $M$ , y  $\vec{a}$ ,  $\vec{b}$  son  $n$ -uplas binarias (fijas para cada uno de los conjuntos). Para cualquier matriz  $M$ , los operadores en  $S_{(\vec{b}, \vec{a})}$  conmutan; para que, agregando la identidad (y a menos de un signo  $\pm 1$ ), formen un grupo con  $d$  elementos distintos, la matriz  $M$  debe ser el elemento generador de una representación matricial de  $GF(d)$ . Las razones se explican a continuación:

En primer lugar, si se tienen dos operadores en  $S_{(\vec{b}, \vec{a})}$ , su producto es de la forma:

$$T(\vec{b}M^j, \vec{a}\widetilde{M}^j) T(\vec{b}M^{j'}, \vec{a}\widetilde{M}^{j'}) \sim T(\vec{b}(M^j + M^{j'}), \vec{a}(\widetilde{M}^j + \widetilde{M}^{j'})) \quad (3.18)$$

donde  $\sim$  indica que el resultado es a menos de una fase global. Para que, para cualquier elección de las  $n$ -uplas  $\vec{a}$ ,  $\vec{b}$ , el producto de dos operadores distintos en  $S_{(\vec{b}, \vec{a})}$  pertenezca también al conjunto, es necesario que  $M$  sea tal que para cualquier par de enteros distintos  $j, j'$  entre 0 y  $d - 2$ , exista un

tercer entero  $j''$  (diferente de los anteriores, y en el mismo rango), tal que  $M^j + M^{j'} = M^{j''}$  (y por lo tanto también  $\widetilde{M}^j + \widetilde{M}^{j'} = \widetilde{M}^{j''}$ ).

Para que además todos los elementos en cada conjunto sean no triviales y no se repitan, las sucesivas potencias  $M^j$  con  $j = 0, \dots, d-2$  deben ser matrices no nulas y diferentes entre sí.

Supongamos que  $M$  satisface estos requisitos; veamos que entonces resulta  $M^{d-1} = I$ . En primer lugar, para cualquier  $j$  entre 0 y  $d-3$ , existe algún  $k$  entre 0 y  $d-2$  tal que:

$$M^j + M^{d-2} = M^k \quad (3.19)$$

Como todas las matrices en esa expresión son no nulas,  $k$  no puede ser igual a  $j$  ni a  $d-2$ . Se puede concluir entonces que entre 0 y  $d-3$  existen dos números  $k, j$  diferentes tales que:

$$M^{d-2} = M^k + M^j \quad (3.20)$$

Multiplicando esa expresión por  $M$  se tiene que:

$$M^{d-1} = M^{k+1} + M^{j+1} = M^l \quad (3.21)$$

con  $l$  entre 0 y  $d-2$  (donde se usa que  $k+1$  y  $j+1$  están entre 0 y  $d-2$ ). Si  $l \neq 0$ , se tiene que:

$$M^{d-1} + M^l = (M^{d-2} + M^{l-1})M = 0 \quad (3.22)$$

pero como existe un  $m$  entre 0 y  $d-3$  tal que  $M^{d-2} + M^{l-1} = M^m$ , entonces esto quiere decir que:

$$M^m M = M^{m+1} = 0 \quad (3.23)$$

o sea, que la potencia  $(m+1)$ -ésima de  $M$  es nula; como  $m+1$  está entre 1 y  $d-2$ , esto contradice las hipótesis anteriores y por lo tanto debe ser  $l = 0$ , o sea que:

$$M^{d-1} = M^0 = I \quad (3.24)$$

Resumiendo, se tiene que para que los conjuntos  $S_{(\vec{b}, \vec{a})}$  contengan cada uno  $d-1$  operadores de Pauli que conmutan distintos y no triviales, la matriz  $M$  involucrada en la construcción tiene que ser tal que los elementos  $\{0, M^0, M^1, \dots, M^{d-2}\}$  se comporten como los elementos del cuerpo  $GF(d)$ , o sea,  $M$  debe ser un elemento generador para la representación matricial del cuerpo.

## La asociación entre estriaciones y bases del espacio de Hilbert

Si se tiene una matriz  $M$  con las propiedades descritas, es posible asociar cada rayo a un conjunto de operadores de Pauli que conmutan, mapeando las coordenadas de los puntos en un mismo rayo a  $n$ -uplas en la forma:

$$q = b\omega^j \rightarrow \vec{q} = \vec{b}M^j, \quad (3.25)$$

$$p = a\omega^j \rightarrow \vec{p} = \vec{a}\widetilde{M}^j. \quad (3.26)$$

Por simplicidad conviene elegir la asociación entre  $a$  y  $\vec{a}$ ,  $b$  y  $\vec{b}$  de forma tal que  $a = b = 1$  se corresponda con  $\vec{a} = \vec{b} = \vec{1}$ , donde  $\vec{1} = (1, 0, \dots, 0)$  (la asociación resultante entre estriaciones y bases no depende de esta elección). De esta manera, para los puntos con coordenadas no nulas se tiene:

$$q_j = \omega^j \rightarrow \vec{q}_j = \vec{1}M^j, \quad (3.27)$$

$$p_j = \omega^j \rightarrow \vec{p}_j = \vec{1}\widetilde{M}^j. \quad (3.28)$$

Las únicas  $n$ -uplas restantes son las compuestas por  $n$  ceros, que naturalmente se asocian a las coordenadas  $q$ ,  $p$  nulas.

En definitiva, una estriación con líneas de la forma  $aq + bp = 0$  queda asociada a la base ortonormal de autoestados del conjunto de operadores de Pauli  $T(\vec{b}M^j, \vec{a}\widetilde{M}^j)$ . De este modo, la estriación vertical ( $b = 0$ ) queda asociada a la base de autoestados de los operadores  $T(\vec{0}, \vec{p})$ , que es la base computacional, en tanto que la estriación horizontal ( $a = 0$ ) corresponde a los autoestados de los operadores  $T(\vec{q}, \vec{0})$  (la “base  $X$ ”). Las estriaciones oblicuas resultan asociadas a bases de autoestados de operadores de Pauli que son productos de  $X$ s y  $Z$ s.

Una de las opciones para la matriz  $M$ , que se usará de aquí en adelante, es la llamada “matriz compañera” del polinomio primitivo del cuerpo [4]. Para esta elección, las componentes de la  $n$ -upla  $\vec{q}$  asociada al elemento  $q$  son las de la expansión de  $q$  en la base canónica del cuerpo, o sea, la  $n$ -upla  $\vec{1}M^j$  está formada por los coeficientes del desarrollo de  $\omega^j$  en la base canónica  $B_\omega$ . Para las coordenadas de momento, se utilizan las componentes de  $p$  en una base múltiplo de la base dual  $\widetilde{B}_\omega$ , o sea, la  $n$ -upla  $\vec{1}\widetilde{M}^j$  contiene los coeficientes de la expansión de  $\omega^j$  en esta base. Si el polinomio primitivo es de la forma  $P_n(x) = 1 + r_1x + r_2x^2 + \dots + x^n$ , su matriz compañera es la siguiente:

$$M = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 1 & r_1 & r_2 & \dots & r_{n-1} \end{pmatrix} \quad (3.29)$$

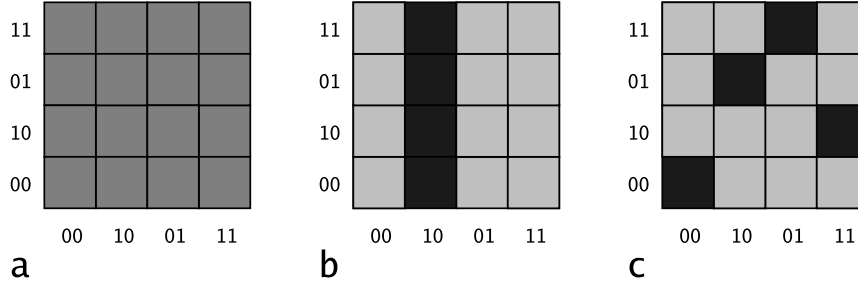
### 3.2.4. La elección de la grilla cuántica

Establecida de esta manera la relación entre cada estriación del espacio de fases y una base del espacio de Hilbert, queda por definir cuál de los estados en cada base corresponde a cada una de las líneas en su estriación asociada. Dada una cierta estriación, al rayo en ella se le puede asignar cualquiera de los  $d$  estados en la base correspondiente, pero una vez hecha esta elección la condición de covariancia traslacional determina cuáles son los estados asociados a las demás líneas en la misma estriación. Dado que hay  $d + 1$  estriaciones, el número total de asociaciones posibles entre líneas y estados es  $d^{d+1}$ . Cada una de ellas constituye una “grilla cuántica”, y conduce a una definición diferente de la función de Wigner. Cada asociación es equivalente a otras  $d^2 - 1$ , que difieren de ella en sólo una traslación; por lo tanto, hay  $d^{d-1}$  grillas cuánticas no equivalentes [3]. Un modo conveniente de restringir las equivalencias consiste en fijar los estados en las estriaciones horizontal y vertical de tal forma que las  $n$ -uplas asociadas a las coordenadas de cada línea correspondan a los autovalores para las matrices de Pauli  $X$  o  $Z$ , respectivamente, sobre cada qubit; por ejemplo, la línea vertical con  $\vec{q} = (1, 0, \dots, 0)$  tendría autovalor  $-1$  para  $Z_{(1)}$  y  $+1$  para  $Z$  sobre los otros qubits. Esto equivale a establecer que el rayo de la estriación horizontal (vertical) tiene autovalor  $+1$  para la aplicación de  $X$  ( $Z$ ), sobre cualquier qubit. Impuesta esta condición, las  $d^{d-1}$  grillas cuánticas que la satisfacen son no equivalentes, y corresponden a todas las posibles elecciones de estados para los rayos oblicuos.

### 3.2.5. Representación de algunos estados sencillos

Para una dada elección de grilla cuántica, la definición de la función de Wigner (3.13) permite calcular fácilmente la representación en el espacio de fases de algunos estados sencillos (ver Figura 3.6). Por ejemplo, como ya se mencionó en la subsección 3.2.2, la función de Wigner para el estado totalmente mixto corresponde a una distribución uniforme, tomando para todos los puntos el valor de  $1/d^2$ . Para los estados que están asociados a alguna de las líneas del espacio de fases, la representación es particularmente simple: usando el hecho de que las bases asociadas a las diferentes estriaciones son mutuamente conjugadas (3.16), puede verse que la función de Wigner de un estado asociado a una línea vale  $1/d$  en todos los puntos de la línea, y 0 fuera de ella.

Es conveniente observar que los estados asociados a las líneas son estados estabilizadores, ya que son autoestados de un conjunto de  $d$  operadores de



**Figura 3.6:** La representación en el espacio de fases con coordenadas en  $GF(d)$  de algunos estados sencillos. El negro corresponde a valores positivos y el blanco, a negativos. a) El estado máximamente mixto corresponde a una distribución uniforme con valor  $1/d^2$ . b) y c) Los estados asociados a líneas del espacio de fases tienen funciones de Wigner que son nulas fuera de las líneas correspondientes, y valen  $1/d$  sobre ellas.

Pauli generalizados. Entonces, hemos identificado un conjunto de estados estabilizadores cuya representación en el espacio de fases es particularmente sencilla. Sin embargo, es fácil notar que hay estados estabilizadores que no corresponden a ninguna línea en el espacio de fases (en el caso de dos qubits, los estados de Bell proporcionan un ejemplo); estos estados estabilizadores en general no tienen una representación simple en términos de su función de Wigner.

### 3.2.6. Los operadores de punto

Una vez elegida una dada grilla cuántica, la condición (3.13) determina completamente la función de Wigner. Al igual que en el caso continuo, la función de Wigner puede interpretarse como el conjunto de valores de expectación para los operadores de punto, definidos según:

$$W(\alpha) = \text{Tr}(\rho A(\alpha)) \quad (3.30)$$

$$A(\alpha) = \frac{1}{d} \left\{ \sum_{\kappa} P(\lambda_{\alpha}^{(\kappa)}) - I \right\} = T(\alpha) A(0) T(\alpha) \quad (3.31)$$

donde en la última igualdad se hace uso de la condición de covariancia frente a traslaciones, y se incorpora en la notación la relación entre puntos del espacio de fases y  $n$ -uplas, esto es,  $T(\alpha) \equiv T(\vec{q}_{\alpha}, \vec{p}_{\alpha})$ .

Estos operadores de punto tienen traza  $1/d$  y, al igual que los del caso continuo, forman una base ortogonal para el espacio de operadores hermíticos,

con su producto interno dado por:

$$\text{Tr}\left(A(\vec{q}, \vec{p}) A(\vec{q}', \vec{p}')\right) = \frac{1}{d} \delta(\vec{q} - \vec{q}') \delta(\vec{p} - \vec{p}') \quad (3.32)$$

Por lo tanto, a partir de la ecuación (3.30) puede obtenerse  $\rho$  en términos de los operadores de punto:

$$\rho = d \sum_{\alpha} W(\alpha) A(\alpha) \quad (3.33)$$

En forma similar, los operadores de traslación pueden escribirse en términos de los operadores de punto, y viceversa. Los coeficientes en este desarrollo están dados por el producto:

$$\begin{aligned} \text{Tr}\left(A(\alpha)T(\beta)\right) &= \text{Tr}\left(T(\alpha)A(0)T(\alpha)T(\beta)\right) = \\ &= (-1)^{\alpha \wedge \beta} \text{Tr}\left(A(0)T(\beta)\right) \end{aligned} \quad (3.34)$$

donde se usa la notación  $\alpha \wedge \beta = \vec{q}_{\alpha} \cdot \vec{p}_{\beta} - \vec{q}_{\beta} \cdot \vec{p}_{\alpha}$ , y la ecuación para conmutar operadores de traslación (2.11). Definiendo un conjunto de constantes dependientes de la grilla cuántica  $f_{\beta} = d \text{Tr}\left(A(0)T(\beta)\right)$  resulta:

$$\text{Tr}\left(A(\alpha)T(\beta)\right) = \frac{(-1)^{\alpha \wedge \beta}}{d} f_{\beta} \quad (3.35)$$

Con lo cual el desarrollo de los operadores de punto en términos de las traslaciones está dado por:

$$A(\alpha) = \frac{1}{d^2} \sum_{\beta} (-1)^{\alpha \wedge \beta} f_{\beta} T(\beta) \quad (3.36)$$

donde se usa también la ecuación (2.14) para la traza de un producto de operadores de Pauli.

El cálculo de las constantes  $f_{\beta}$  puede realizarse de la siguiente manera: para  $\beta = 0$ , la ecuación 3.35 implica  $f_0 = 1$  (porque la traza de  $A(0)$  vale  $1/d$ ); para  $\beta \neq 0$ , se tiene el estado asociado al rayo que pasa por el punto  $\beta$ ,  $P(\lambda_{0,\beta})$ , que es autoestado del operador de traslación  $T(\beta)$  con autovalor:

$$\text{Tr}\left(P(\lambda_{0,\beta})T(\beta)\right) = \sum_{\alpha \in \lambda_{0,\beta}} \text{Tr}\left(A(\alpha)T(\beta)\right) = \sum_{\alpha \in \lambda_{0,\beta}} \frac{(-1)^{\alpha \wedge \beta}}{d} f_{\beta} \quad (3.37)$$

donde se usa la expansión (3.33) del estado  $P(\lambda_{0,\beta})$  en términos de los operadores de punto y el hecho de que la función de Wigner del proyector asociado a una línea toma un valor de  $1/d$  sobre la línea y es nula fuera de



ella. Dado que la suma es sobre puntos  $\alpha$  que están en el mismo rayo que  $\beta$ , los operadores  $T(\alpha)$  y  $T(\beta)$  conmutan, y entonces resulta  $\alpha \wedge \beta = 0 \pmod{2}$ ; por lo tanto:

$$\mathrm{Tr}\left(P(\lambda_{0,\beta})T(\beta)\right) = \sum_{\alpha \in \lambda_{0,\beta}} \frac{1}{d} f_\beta = f_\beta \quad (3.38)$$

O sea, las constantes  $f_\beta$  corresponden a los autovalores de los estados asociados a los rayos, y determinan la grilla cuántica en forma redundante, ya que para cada rayo sólo es necesario indicar  $n$  autovalores (las  $f_\beta$  no son independientes).

### 3.2.7. Función de Wigner de estados estabilizadores

De acuerdo a lo enunciado en la sección 2.3, dado un estado estabilizador  $\rho$  existen  $d$  operadores de Pauli generalizados  $T(\mu)$  que conmutan tales que:

$$T(\mu)\rho = g_\mu\rho, \quad g_\mu = \pm 1 \quad (3.39)$$

Por brevedad, se usará la notación  $\mu \in S$  para indicar un punto  $\mu$  del espacio de fases tal que  $g_\mu T(\mu)$  estabiliza al estado  $\rho$ . La matriz densidad puede desarrollarse en términos de sus estabilizadores según (2.17):

$$\rho = \frac{1}{d} \sum_{\mu \in S} g_\mu T(\mu) \quad (3.40)$$

Utilizando esta expresión, la definición de la función de Wigner en términos de los operadores de punto (3.30) y el desarrollo de éstos en función de las traslaciones (3.36), puede obtenerse para la función de Wigner de  $\rho$ :

$$\begin{aligned} W(\alpha) &= \frac{1}{d^3} \sum_{\beta} \sum_{\mu \in S} (-1)^{\alpha \wedge \beta} f_\beta g_\mu \mathrm{Tr}\left(T(\mu)T(\beta)\right) = \\ &= \frac{1}{d^2} \sum_{\mu \in S} (-1)^{\alpha \wedge \mu} f_\mu g_\mu \end{aligned} \quad (3.41)$$

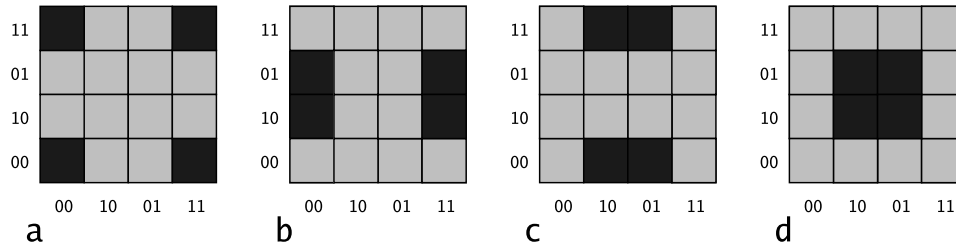
Dado un punto  $\alpha \in S$ , resulta  $\alpha \wedge \mu = 0 \forall \mu \in S$  (ya que los operadores de traslación asociados a los puntos  $\alpha$  y  $\mu$  estabilizan a  $\rho$ , y entonces deben conmutar); por lo tanto la función de Wigner en  $\alpha$  resulta igual a:

$$W(\alpha) = \frac{1}{d^2} \sum_{\mu \in S} f_\mu g_\mu, \quad \forall \alpha \in S \quad (3.42)$$

de donde se ve que el valor de la función de Wigner es el mismo en cualquier punto  $\alpha \in S$ . Esto es necesario ya que el estado es autoestado de las traslaciones  $T(\mu)$  con  $\mu \in S$ , así que su función de Wigner debe ser invariante frente a las traslaciones asociadas  $\mathcal{T}_\mu$  en el espacio de fases.

Una representación particularmente conveniente del estado  $\rho$  en el espacio de fases se obtiene si se elige la grilla cuántica de forma tal que se verifique  $f_\mu = g_\mu \forall \mu \in S$ . En este caso la función de Wigner toma un valor igual a  $1/d$  en todos los puntos  $\alpha \in S$ , mientras que para cualquier otro punto  $\alpha \notin S$  la función de Wigner se anula, ya que la mitad de los estabilizadores de  $\rho$  conmuta con  $T(\alpha)$  (o sea,  $\alpha \wedge \mu = 0$ ) y la otra mitad anticonmuta ( $\alpha \wedge \mu = 1$ ).

En la Figura 3.7 se muestra la representación, para esta elección de grilla cuántica, del estado de Bell  $|\phi_+\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)$ , y de los demás estados de Bell obtenidos a partir de éste mediante traslaciones. El estado de Bell  $|\phi_+\rangle$  es estabilizado por los operadores  $Z_{(1)}Z_{(2)}$ ,  $X_{(1)}X_{(2)}$ , y sus productos. Los puntos  $\mu \in S$  son, por lo tanto:  $(00, 00)$  –el origen–,  $(00, 11)$  – el producto de  $Z$ s–,  $(11, 00)$  – el producto de  $X$ s– y  $(11, 11)$  – el producto de  $Y$ s, o sea  $X$ s y  $Z$ s. Estos puntos corresponden a las “esquinas” del espacio de fases. Para la elección “conveniente” de la grilla cuántica, la función de Wigner de  $|\phi_+\rangle$  valdrá  $1/4$  en estas esquinas y 0 en el resto de los puntos.



**Figura 3.7:** La representación de los estados de Bell en la grilla cuántica “conveniente” para el estado  $|\phi_+\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)$ . El gris corresponde al valor cero de la función de Wigner, y el negro a  $1/4$ . a) El estado  $|\phi_+\rangle$ ; a causa de la grilla cuántica elegida, su función de Wigner es distinta de cero sólo en los puntos asociados a los operadores en su estabilizador. Las representaciones de los demás estados de Bell pueden obtenerse trasladando  $|\phi_+\rangle$ , según: b)  $|\phi_-\rangle = Z_{(1)}|\phi_+\rangle$ ; c)  $|\psi_+\rangle = X_{(1)}|\phi_+\rangle$ ; d)  $|\psi_-\rangle = Z_{(1)}X_{(1)}|\phi_+\rangle$ . Los estados de Bell son autoestados de los operadores  $Z_{(1)}Z_{(2)}$  y  $X_{(1)}X_{(2)}$ ; por lo tanto, sus funciones de Wigner son invariantes frente a las traslaciones asociadas en el espacio de fases (cuyas acciones sobre la función de Wigner corresponden a reflexiones respecto de los ejes horizontal y vertical en medio del espacio de fases).

### 3.2.8. Funciones de Wigner a medida para los estados-grafo

Un paso esencial en la definición de la función de Wigner es la elección de operadores de traslación en el espacio de Hilbert y su identificación con

operadores de traslación en el espacio de fases. Las bases asociadas a cada estriación resultan determinadas por la elección de los operadores de Pauli y de la relación entre los elementos del cuerpo de Galois  $(q, p)$  y las  $n$ -uplas  $(\vec{q}, \vec{p})$ . Al elegir los operadores de traslación como operadores de Pauli de la forma  $T(\vec{q}, \vec{p}) = \sigma_{\vec{q}, \vec{p}}$ , las traslaciones verticales se identifican con productos tensoriales de operadores  $Z$ , las horizontales con productos de operadores  $X$ , y las oblicuas con productos que contienen  $Z$ s y  $X$ s. En consecuencia, la estriación vertical queda asociada a la base computacional, la horizontal a la base  $X$ , y las oblicuas a bases de estados estabilizadores que son conjugadas a las anteriores. Esta elección de los operadores de traslación, entonces, garantiza que las estriaciones horizontal y vertical están asociadas a bases separables del espacio de Hilbert, compuestas por estados producto de los distintos qubits.

Sin embargo, existen otras elecciones posibles para los operadores de traslación  $T(\vec{q}, \vec{p})$  que también permiten construir una función de Wigner covariante frente a las traslaciones. En particular, si en lugar del conjunto de operadores  $X_{(i)}$  y  $Z_{(i)}$  se eligen otros operadores de Pauli  $X'_i$  y  $Z'_i$  con las mismas relaciones de conmutación y anticonmutación que los anteriores (donde el operador  $i$ -ésimo no necesariamente actúa sólo sobre el qubit  $i$ ), pueden definirse las traslaciones en el espacio de Hilbert en la forma:

$$T'(\vec{q}, \vec{p}) = \prod_{i=1}^n X_i'^{q_i} Z_i'^{p_i} e^{i\frac{\pi}{2}q_i p_i} = X'^{\vec{q}} Z'^{\vec{p}} e^{i\frac{\pi}{2}\vec{q}\vec{p}} \quad (3.43)$$

En este caso, la construcción de las bases asociadas a las distintas estriaciones, y de la función de Wigner a partir de ellas, puede realizarse en la misma forma que antes; cada estriación quedará asociada a una base diferente del espacio de Hilbert, y las distintas bases seguirán siendo mutuamente conjugadas. Existe por lo tanto una enorme libertad en la definición de la función de Wigner, pero por supuesto no todas las elecciones posibles serán convenientes para analizar problemas de computación cuántica. Por ejemplo, la base computacional es una base “privilegiada” y en general será conveniente asociarla a las líneas verticales. Sin embargo, para las líneas horizontales puede ser mejor elegir alguna otra base en lugar de la  $X$ .

Un ejemplo lo proporcionan los problemas relacionados con un dado estado-grafo; el estado-grafo se define en la forma explicada en la sección 2.4, y su estabilizador es generado por los operadores  $S_i$  que aplican  $X$  sobre el vértice  $i$ -ésimo y  $Z$  sobre todos sus vecinos. Es posible definir los

operadores  $X'_i$  y  $Z'_i$  en la forma:

$$X'_i = S_i = X_{(i)} \prod_j Z_{(j)}^{\Gamma_{i,j}} \quad (3.44)$$

$$Z'_i = Z_{(i)} \quad (3.45)$$

Estos operadores tienen las relaciones de conmutación y anticonmutación deseadas, y por lo tanto se pueden usar para construir las traslaciones en la forma (3.43). Las distintas estriaciones en el espacio de fases se relacionarán ahora con otras bases. En particular la base vertical seguirá siendo la base computacional, pero la horizontal ahora estará compuesta por los autoestados comunes a los operadores  $S_i$ ; el rayo horizontal será el estado-grafo, y las otras líneas horizontales serán los autoestados de los  $S_i$  con autovalores distintos. Estas otras líneas horizontales pueden obtenerse aplicando traslaciones verticales sobre el rayo, o sea aplicando operadores  $Z$  sobre los distintos qubits en el estado-grafo.

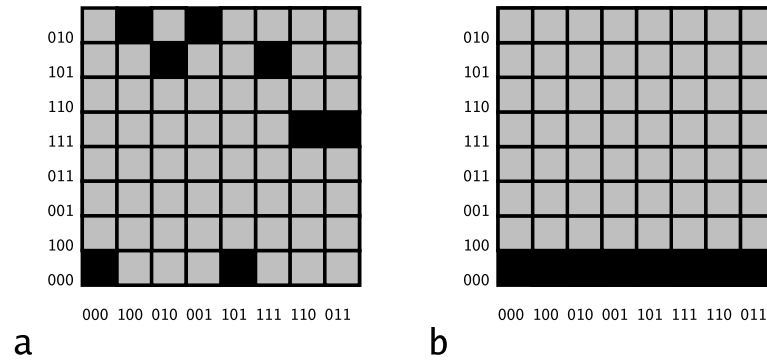
En términos de los nuevos operadores de traslación, la función de Wigner puede escribirse en la forma:

$$W'(\alpha) = \text{Tr}(\rho A'(\alpha)) \quad (3.46)$$

$$A'(\alpha) = \frac{1}{d^2} \sum_{\beta} (-1)^{\alpha \wedge \beta} f_{\beta} T'(\beta) \quad (3.47)$$

(donde también las constantes  $f_{\beta}$  deben ser redefinidas, como autovalores de las nuevas traslaciones).

Como ejemplo, consideremos el estado-grafo asociado a una cadena lineal de tres qubits. Este estado es estabilizado por los operadores de Pauli  $X_{(1)}Z_{(2)}$ ,  $Z_{(1)}X_{(2)}Z_{(3)}$ ,  $Z_{(2)}X_{(3)}$ , y sus productos. Como se indica en la subsección 3.2.7, en la definición estándar de la función de Wigner usando cuerpos de Galois es posible elegir una grilla cuántica tal que la función de Wigner del estado valga  $1/d$  en los puntos asociados a su estabilizador, y se anule en el resto de los puntos. La función de Wigner que resulta se muestra en la Figura 3.8.a. Alternativamente, es posible redefinir la función de Wigner en la forma explicada en esta sección, de modo que las traslaciones horizontales estén asociadas a los estabilizadores del grafo. Con esta elección, el estado-grafo es el proyector asociado al rayo horizontal, y por lo tanto su función de Wigner vale  $1/d$  sobre este rayo, y es nula en los otros puntos. Esta versión de la función de Wigner se muestra en la Figura 3.8.b.



**Figura 3.8:** La representación del estado-grafo asociado a una cadena lineal de tres qubits, para dos definiciones diferentes de la función de Wigner. En los puntos en gris, la función de Wigner tiene valor cero, y en los negros vale  $1/8$ . a) En la definición usual usando cuerpos de Galois, es posible elegir una grilla cuántica “conveniente” de forma tal que la función de Wigner sólo es no nula en los puntos asociados al estabilizador del estado-grafo. b) Si se redefinen las traslaciones horizontales, identificándolas con los estabilizadores del estado-grafo, éste resulta asociado al rayo horizontal, y su función de Wigner sólo es no nula en los puntos pertenecientes a ese rayo. En ambos casos, la función de Wigner es invariante frente a las traslaciones que estabilizan al estado; en la Figura a, estas traslaciones son oblicuas, mientras que en la b son horizontales.

## Capítulo 4

# Positividad de la función de Wigner discreta

De acuerdo a lo comentado en la sección 3.1, la función de Wigner continua, aún a pesar de conducir a las probabilidades marginales correctas, no puede ser interpretada como una densidad de probabilidad a raíz de que puede tomar valores negativos. De hecho, estos valores negativos de la función de Wigner son típicos de las interferencias en los estados cuánticos, sugiriendo cierta “clasicidad” de los estados cuyas funciones de Wigner son positivas. Al superponer paquetes gaussianos en el espacio de fases, por ejemplo, aparecen términos de interferencia que toman valores negativos cuando la superposición es coherente, y en cambio en una superposición estadística no hay efectos de interferencia y la función de Wigner es no negativa.

Las distintas funciones de Wigner propuestas para el caso discreto tampoco son definidas positivas; el conjunto de estados con funciones de Wigner positivas depende de la función de Wigner elegida. Si se estudian sistemas con dimensión  $d = p^n$  en un espacio de fases con coordenadas en el cuerpo  $GF(d)$ , no existe una única definición de la función de Wigner sino clases de posibles funciones, donde las distintas definiciones corresponden a distintas elecciones de los operadores de traslación y de la grilla cuántica. Para cada definición de las traslaciones, los estados cuya función de Wigner es no negativa para cualquier grilla cuántica tienen una caracterización sencilla: todos ellos son combinaciones estadísticas de los estados estabilizadores asociados a las distintas líneas del espacio de fases. Esta propiedad de la función de Wigner discreta definida utilizando cuerpos de Galois fue conjeturada por E. Galvao [5] y demostrada como parte del trabajo de esta tesis.

En este capítulo se estudiará, entonces, el conjunto de estados cuya función de Wigner es no negativa para cualquier elección de la grilla cuántica,

y se demostrará la “conjetura de Galvao”, que establece que este conjunto está formado por todas las combinaciones convexas de los proyectores asociados a las líneas en el espacio de fases. A continuación, se mostrarán algunos operadores unitarios que mapean estados en este conjunto en otros estados del mismo conjunto, preservando la propiedad de no negatividad de la función de Wigner en cualquier grilla cuántica. Los resultados de este capítulo se encuentran también en [36].

#### 4.1. Caracterización de los estados con función de Wigner no negativa en toda grilla cuántica

En lo sucesivo se llamará “totalmente positiva” a la función de Wigner de un estado cuando es no negativa en toda grilla cuántica. A lo largo de este capítulo, se considerará fija la elección del operador de Pauli generalizado identificado con cada traslación  $T(\vec{q}, \vec{p})$  en el espacio de Hilbert. Entonces, las diferentes grillas cuánticas corresponden a las mismas asociaciones entre estricciones y bases del espacio de Hilbert, pero distintas asociaciones entre cada uno de los rayos y un estado de la base correspondiente. El objetivo de esta sección es demostrar que, para una elección determinada de los operadores de traslación, un estado tiene función de Wigner totalmente positiva si y sólo si su matriz densidad es una combinación convexa de los proyectores  $P(\lambda)$  asociados a las  $d(d+1)$  líneas en el espacio de fases, o sea, si y sólo si es una combinación lineal de estos proyectores de la forma:

$$\rho = \sum_{\lambda} c_{\lambda} P(\lambda) \quad (4.1)$$

donde todos los coeficientes  $c_{\lambda}$  son no negativos.

En primer lugar, es fácil ver que las combinaciones convexas de proyectores  $P(\lambda)$  tienen funciones de Wigner totalmente positivas. De acuerdo a lo explicado en la subsección 3.2.5, los estados asociados a líneas del espacio de fases tienen funciones de Wigner no negativas (que valen  $1/d$  sobre la línea, y cero fuera). Estos estados son los mismos en todas las posibles grillas cuánticas, y aunque la identificación de cada estado con una dada línea depende de la grilla cuántica, la positividad se verifica para cualquiera de las asociaciones posibles. Dado que la función de Wigner (3.13) es lineal frente a combinaciones lineales de matrices densidad, un estado que es combinación convexa de los proyectores asociados a las distintas líneas tiene también una función de Wigner no negativa, cualquiera sea la grilla cuántica elegida.

A continuación, se demostrará la afirmación recíproca: los únicos estados con función de Wigner totalmente positiva son las combinaciones convexas

de los proyectores asociados a líneas. Estos proyectores forman un conjunto linealmente dependiente, ya que la suma de todos los proyectores en cualquiera de las bases es igual a la identidad. Como se hace notar en la subsección 3.2.6, el conjunto de los  $d$  operadores de punto  $A(\alpha)$  forma una base para las matrices hermíticas de  $d \times d$ . A su vez, los operadores  $A(\alpha)$  son combinaciones lineales de operadores de proyección  $P(\lambda)$  (en la ecuación (3.31) puede reemplazarse la identidad por cualquier suma de proyectores en la misma base). Por lo tanto, cualquier estado  $\rho$  puede descomponerse en términos de los proyectores  $P(\lambda)$  en la forma (4.1), con coeficientes reales que pueden ser negativos. Como la suma sobre los proyectores de cualquier estriación es igual a la identidad, el conjunto de proyectores  $P(\lambda)$  es sobre-completo y la descomposición (4.1) no es única: dadas dos estriaciones  $\kappa_1$  y  $\kappa_2$ , es posible redefinir todos los coeficientes asociados a líneas en dichas estriaciones en la forma:

$$\begin{cases} c(\lambda^{(\kappa_1)}) & \rightarrow c(\lambda^{(\kappa_1)}) + x \\ c(\lambda^{(\kappa_2)}) & \rightarrow c(\lambda^{(\kappa_2)}) - x \end{cases} \quad (4.2)$$

con  $x$  cualquier número real, obteniendo una expansión distinta para el mismo estado.

La condición de traza 1 para  $\rho$  se traduce en:

$$\sum_{\lambda} c(\lambda) = 1 \quad (4.3)$$

Insertando la expresión (4.1) en la función de Wigner dada por (3.13), se tiene:

$$W(\alpha) = \frac{1}{d} \left\{ \sum_{\kappa} \sum_{\lambda'} c(\lambda') \operatorname{Tr} \left( P(\lambda') P(\lambda_{\alpha}^{(\kappa)}) \right) - 1 \right\} \quad (4.4)$$

Usando el hecho de que las bases son mutuamente no sesgadas, resulta que si  $\lambda'$  no está en la estriación  $\kappa$ -ésima, entonces:

$$\operatorname{Tr} \left( P(\lambda') P(\lambda_{\alpha}^{(\kappa)}) \right) = \frac{1}{d} \quad \forall \lambda' \notin \{\lambda^{(\kappa)}\} \quad (4.5)$$

mientras que porque las bases son ortonormales, se tiene que si  $\lambda'$  está en la estriación  $\kappa$ -ésima se tiene:

$$\operatorname{Tr} \left( P(\lambda') P(\lambda_{\alpha}^{(\kappa)}) \right) = \begin{cases} 1, & \text{si } \lambda' = \lambda_{\alpha}^{(\kappa)} \\ 0, & \text{si } \lambda' \neq \lambda_{\alpha}^{(\kappa)} \end{cases} \quad (4.6)$$



Por lo tanto, la condición de que la función de Wigner de  $\rho$  sea no negativa en todo punto es equivalente a:

$$\begin{aligned} \sum_{\kappa} \left\{ c(\lambda_{\alpha}^{(\kappa)}) + \sum_{\lambda' \notin \{\lambda^{(\kappa)}\}} \frac{c(\lambda')}{d} \right\} &= \\ &= \sum_{\kappa} c(\lambda_{\alpha}^{(\kappa)}) + \sum_{\kappa} \sum_{\lambda' \notin \{\lambda^{(\kappa)}\}} \frac{c(\lambda')}{d} \geq 1 \quad \forall \alpha \end{aligned} \quad (4.7)$$

En la segunda sumatoria, el coeficiente de cada línea  $\lambda'$  del espacio de fases aparece en la suma  $d$  veces, con lo cual la ecuación puede reescribirse en la forma:

$$\sum_{\kappa} c(\lambda_{\alpha}^{(\kappa)}) + d \sum_{\lambda'} \frac{c(\lambda')}{d} \geq 1 \quad \forall \alpha \quad (4.8)$$

Utilizando la normalización de  $\rho$  (4.3), se obtiene:

$$\sum_{\kappa} c(\lambda_{\alpha}^{(\kappa)}) \geq 0 \quad \forall \alpha \quad (4.9)$$

Esta condición debe verificarse para cualquier grilla cuántica, o sea, para cualquier asociación entre el rayo de cada estriación y un estado de la base correspondiente. Esto quiere decir que la última desigualdad debe valer para cualquier suma de  $d + 1$  coeficientes asociados a  $d + 1$  proyectores, con tal de que se tome uno de cada una de las bases. En particular, pueden elegirse los menores coeficientes de cada estriación,  $c_{min}^{(\kappa)}$ , para los que se verifica:

$$\sum_{\kappa} c_{min}^{(\kappa)} \geq 0 \quad (4.10)$$

Si existen estriaciones en las que el menor coeficiente es negativo, entonces claramente por la condición anterior debe existir al menos una en la que el menor coeficiente sea positivo. Separando las estriaciones según este criterio, y llamando  $\kappa_-$  a aquéllas en las que el coeficiente mínimo es negativo y  $\kappa_+$  a las restantes, se tiene:

$$\sum_{\kappa_+} c_{min}^{(\kappa)} \geq \sum_{\kappa_-} |c_{min}^{(\kappa)}| \quad (4.11)$$

Esto implica que en cada una de las estriaciones en las que el menor coeficiente sea menor que cero pueden incrementarse todos los coeficientes en la forma:

$$c(\lambda^{(\kappa)}) \rightarrow c(\lambda^{(\kappa)}) - c_{min}^{(\kappa)} \quad (4.12)$$

y simultáneamente restar a los coeficientes de las otras estriaciones lo necesario para compensar el incremento anterior, de modo de obtener una expansión distinta para el mismo estado, conteniendo sólo coeficientes no negativos. Un modo explícito de llegar a una nueva expansión de la forma deseada es el siguiente: se define una cantidad no negativa  $x$  dada por:

$$x = \frac{1}{d+1} \sum_{\kappa} c_{\min}^{(\kappa)} \quad (4.13)$$

y luego se redefinen los coeficientes de todas las estriaciones según:

$$c^{(\kappa)} \rightarrow c'^{(\kappa)} = c^{(\kappa)} - c_{\min}^{(\kappa)} + x \quad (4.14)$$

De esta forma, a todos los coeficientes en una misma estriación se les suma la misma cantidad, y la suma de todos los coeficientes mantiene su valor, con lo cual la ecuación (4.14) proporciona un desarrollo alternativo para  $\rho$ . Dicho desarrollo sólo contiene coeficientes no negativos y puede por lo tanto interpretarse en términos de una combinación probabilística de los proyectores  $P(\lambda)$ . Con esto queda demostrada la conjetura.

En conclusión, los únicos estados cuyas funciones de Wigner son no negativas en cualquier grilla cuántica son las combinaciones convexas de los proyectores asociados a las líneas. Los únicos estados puros en este conjunto, por lo tanto, son los propios proyectores  $P(\lambda)$ . Estos proyectores son estados estabilizadores, lo cual muestra que los únicos estados puros con función de Wigner totalmente positiva son estados estabilizadores. Sin embargo, como ya se mencionó anteriormente (en 3.2.4), existen estados estabilizadores que no están asociados a líneas, y que por lo tanto tienen función de Wigner negativa en alguna grilla cuántica.

## 4.2. Operadores que preservan la positividad total de la función de Wigner

Por otra parte, puede definirse el conjunto de operadores unitarios que preservan la propiedad de positividad total de la función de Wigner. Estos operadores son aquéllos que mapean cada uno de los proyectores  $P(\lambda)$  en otro  $P(\lambda')$ . Recientemente, Gottesman demostró que un operador con esta propiedad necesariamente pertenece al grupo de Clifford [36]. Teniendo en cuenta que los proyectores  $P(\lambda)$  son estados estabilizadores, este resultado implica que una evolución unitaria que parte de un estado puro con función de Wigner totalmente positiva y preserva la positividad total, siempre es un proceso que se inicia en un estado estabilizador sobre el que se aplican

solamente compuertas de Clifford. Por lo tanto, cualquier evolución unitaria restringida a estados puros con funciones de Wigner totalmente positivas es simulable eficientemente en una computadora clásica utilizando el formalismo de estabilizadores.

El conjunto de operadores que preservan la positividad total de la función de Wigner para toda grilla cuántica es, entonces, un subgrupo del grupo de Clifford. Sin embargo, la caracterización completa de este subgrupo es un problema aún no resuelto. Para la definición de la función de Wigner descrita en la sección 3.2 (tomando los operadores de traslación en la forma usual,  $T(\vec{q}, \vec{p}) = \sigma_{\vec{q}, \vec{p}}$ ) a continuación se muestran algunos operadores que preservan la positividad total, y se analiza su acción en el espacio de Hilbert y el de fases.

#### 4.2.1. Los operadores de Pauli

Los operadores de Pauli generalizados, a causa de la condición de covariancia frente a traslaciones, mapean cada estado asociado a una línea en otro asociado a otra línea (o la misma) de la misma estriación. Esto implica que los operadores de traslación preservan la positividad total de la función de Wigner. También como consecuencia de la covariancia, bajo la acción de un operador de Pauli la función de Wigner de un estado se transforma como un flujo en el espacio de fases, esto es, cada operador de punto es mapeado en otro (con el mapa dado por la traslación en el espacio de fases asociada a ese operador de Pauli). El hecho de que los operadores de Pauli actúen como flujos en el espacio de fases es independiente de la grilla cuántica elegida, con lo cual estos operadores preservan además la positividad de la función de Wigner para cualquier grilla cuántica particular.

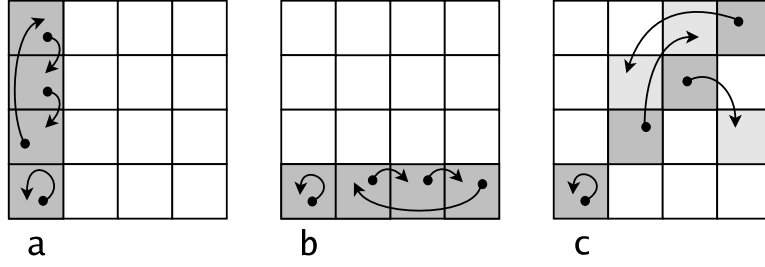
#### 4.2.2. El operador de squeezing

La operación de squeezing en el espacio de fases corresponde a un mapa  $u_s$  que actúa en la forma:

$$u_s(q, p) = (q\omega, p\omega^{-1}) \quad (4.15)$$

Esta operación mapea las estriaciones horizontal y vertical en sí mismas, y recorre cíclicamente todas las estriaciones oblicuas (ver Figura 4.1). En [4] se define un operador unitario  $U_s$  perteneciente al grupo de Clifford cuya acción sobre los operadores de traslación es análoga a la de una operación de squeezing:

$$U_s T(\vec{q}, \vec{p}) U_s^\dagger = \pm T(\vec{q}M, \vec{p}\widetilde{M}^{-1}) \quad (4.16)$$



**Figura 4.1:** El operador de squeezing  $u_s$  transforma los puntos del espacio de fases en la forma  $u_s(q, p) = (q\omega, p\omega^{-1})$ . La aplicación de la transformación  $u_s$  mapea las estriaciones horizontal y vertical en sí mismas, y recorre cíclicamente las estriaciones oblicuas. Es posible definir un operador  $U_s$  que actúa en el espacio de Hilbert cuyo efecto sobre los operadores de traslación  $T(\vec{q}, \vec{p})$  es análogo al de  $u_s$ , a menos de un signo. En la figura se muestra (a menos de un signo) el efecto de  $U_s$  sobre los operadores de traslación asociados a puntos en los rayos: a) vertical; b) horizontal; c) diagonal principal.

Este operador proporciona una manera de restringir el número de grillas cuánticas, consistente en imponer sobre la función de Wigner la condición adicional de covariancia frente a  $u_s$ , equivalente a:

$$P(u_s\lambda) = U_s P(\lambda) U_s^\dagger \quad (4.17)$$

Utilizando esta covariancia adicional, el número de posibles grillas cuánticas se reduce a  $d$ , ya que la única libertad reside en la elección del estado para uno de los rayos oblicuos, y las condiciones de covariancia determinan los estados que deben asociarse a todas las otras líneas [4].

El operador de squeezing en el espacio de Hilbert  $U_s$  mapea cada línea del espacio de fases en otra, independientemente de la grilla cuántica elegida. Por lo tanto,  $U_s$  preserva la positividad total de la función de Wigner. En el caso particular en que la grilla cuántica elegida es covariante frente a la operación de squeezing,  $U_s$  mapea cada operador de punto en otro, de modo tal que al aplicar  $U_s$  sobre un estado su función de Wigner se transforma como un flujo en el espacio de fases. En este caso, entonces,  $U_s$  preserva además la positividad de la función de Wigner para estados cuya función de Wigner es positiva en esa grilla cuántica particular pero no en todas las grillas cuánticas posibles.

### 4.2.3. Transformada discreta de Fourier

En la definición más usual de la función de Wigner discreta, con aritmética módulo  $d$  (o  $2d$ , si  $d$  es par), las líneas horizontales y verticales, asociadas

a los autoestados de posición y momento, se relacionan a través de una transformada de Fourier discreta. Para el espacio de fases con coordenadas en el cuerpo de Galois, también es posible definir una transformada discreta de Fourier que relacione las estriaciones horizontal y vertical [37], y que tiene además la propiedad de mapear todos los proyectores  $P(\lambda)$  en otros, de modo que preserve la positividad total de la función de Wigner. Esta transformada es la siguiente:

$$F = \frac{1}{\sqrt{d}} \sum_{\vec{a}, \vec{b}} (-1)^{(\vec{a}C) \cdot \vec{b}} |\vec{a}\rangle \langle \vec{b}| \quad (4.18)$$

donde la suma es sobre todas las  $n$ -uplas binarias  $\vec{a}$ ,  $\vec{b}$ , y  $C$  es la matriz que realiza el cambio de base de las  $n$ -uplas asociadas a la posición a las asociadas al momento:

$$\vec{p}_j = \vec{q}_j C \quad \forall j \quad (4.19)$$

La matriz  $C$  puede encontrarse fácilmente teniendo en cuenta que para los primeros valores de  $j$  ( $j = 0, 1, \dots, n-1$ ) las  $n$ -uplas  $\vec{q}_j = \vec{1}M^j$  son los versores canónicos, o sea,  $(\vec{1}M^j)_i = \delta_{j+1,i}$ . A partir de esto, se ve que la fila  $(j+1)$ -ésima de la matriz  $C$  está dada por las componentes de la  $n$ -upla de momentos  $\vec{p}_j = \vec{1}\widetilde{M}^j$ .

La transformada de Fourier discreta definida es equivalente a una composición de una transformada de Hadamard  $F_H$  y un cambio de base  $F_C$ , en la forma:

$$F = F_C F_H \quad (4.20)$$

$$F_H = \frac{1}{\sqrt{d}} \sum_{\vec{a}, \vec{b}} (-1)^{\vec{a} \cdot \vec{b}} |\vec{a}\rangle \langle \vec{b}| \quad (4.21)$$

$$F_C = \sum_{\vec{x}} |\vec{x}\rangle \langle \vec{x}C| \quad (4.22)$$

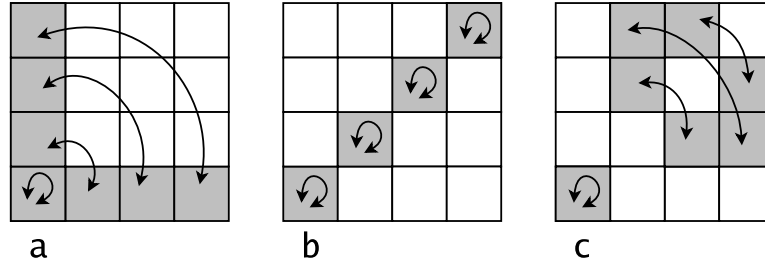
La transformada de Hadamard consiste simplemente en la aplicación de la compuerta  $H$  sobre cada qubit. El cambio de base puede implementarse usando compuertas  $CNOT$ . Si la base asociada a las coordenadas de posición es igual a la base de momentos,  $F$  es igual a la transformada de Hadamard (esto ocurre en el caso de dos qubits).

El efecto de la transformada de Fourier sobre los operadores de traslación es de la forma:

$$FT(\vec{q}_j, \vec{p}_k)F^\dagger = \pm T(\vec{q}_k, \vec{p}_j) \quad (4.23)$$

lo cual corresponde, a menos de un signo, a una reflexión respecto de la diagonal principal ( $k = j$ ) de los operadores de traslación asociados a los

distintos puntos del espacio de fases (ver Figura 4.2). Al aplicar esta transformada, las bases asociadas a las distintas estriaciones son mapeadas unas en otras de a pares, excepto por la base asociada a la estriación cuyo rayo es el eje de reflexión; esta base, correspondiente a los autoestados de los operadores de Pauli de la forma  $T(\vec{q}_j, \vec{p}_j)$ , es mapeada en sí misma.



**Figura 4.2:** La transformada discreta de Fourier  $F$  mapea los operadores de traslación  $T(\vec{q}_j, \vec{p}_k)$  en  $\pm T(\vec{q}_k, \vec{p}_j)$ ; este efecto corresponde, a menos de un signo, a una reflexión de los operadores respecto del eje diagonal principal del espacio de fases. a)  $F$  intercambia los operadores de traslación en los rayos vertical y horizontal; b)  $F$  sólo produce cambios de signo al actuar sobre los operadores de traslación asociados a puntos en el rayo diagonal principal; c) los operadores de traslación en los rayos de las estriaciones restantes son intercambiados, a menos de un signo.

Por analogía con el caso del operador de squeezing, la acción de  $F$  sobre los operadores de traslación y sobre las bases asociadas a las  $d + 1$  estriaciones sugiere que  $F$  podría actuar sobre los estados asociados a las líneas intercambiándolos de forma tal que la aplicación de  $F$  sobre un estado se traduzca en una reflexión de su función de Wigner, tal vez para algunas grillas cuánticas particulares. Para que esto ocurra, el estado asociado al rayo correspondiente al eje de reflexión debe ser mapeado en sí mismo por  $F$ . Para ello, tiene que ser un autoestado común de  $F$  y los operadores de Pauli de la forma  $T(\vec{q}_j, \vec{p}_j)$ . Sin embargo, algunos de estos operadores anticonmutan con  $F$ , y tanto las traslaciones como  $F$  tienen autovalores no nulos (por ser operadores unitarios); por lo tanto, no es posible hallar un autoestado común a todos ellos. En conclusión, no es posible elegir una grilla cuántica tal que la acción de  $F$  sobre el estado corresponda a una reflexión de su función de Wigner.

De hecho, con argumentos similares es posible mostrar que no existe ninguna grilla cuántica para la cual el efecto de  $F$  pueda traducirse en una transformación de la función de Wigner como un flujo en el espacio de fases. Esto es porque para que la función de Wigner se transforme como un flujo

cada operador de punto debe ser mapeado en otro. Para esto, los estados asociados a las  $d + 1$  líneas que se cruzan en cada punto deben ser mapeados en otros estados asociados a líneas que también se crucen en un solo punto. Dado que  $F$  intercambia el rayo vertical con el horizontal, los otros rayos deben ser también mapeados en rayos (de modo que la intersección de las  $d + 1$  líneas siga siendo el origen). En particular, como  $F$  mapea en sí misma la estriación asociada a la diagonal principal, nuevamente se tiene que el rayo en dicha estriación debe permanecer invariante frente a  $F$ , lo cual de acuerdo a lo discutido en el párrafo anterior no es posible.

Por lo tanto,  $F$  proporciona un ejemplo de un operador que preserva la positividad total de la función de Wigner pero que no puede ser interpretado en términos de un flujo en el espacio de fases para ninguna grilla cuántica, y que entonces no puede ser asociado fácilmente a ningún operador clásico de evolución.

## Capítulo 5

# La interferencia en la función de Wigner

La identificación de regiones de interferencia en el espacio de fases suele ser un punto clave en el estudio de sistemas físicos por medio de la función de Wigner. Los términos oscilatorios asociados a la interferencia permiten distinguir superposiciones coherentes de combinaciones estadísticas, de modo que pueden estudiarse procesos de decoherencia observando la desaparición de las oscilaciones. En problemas semiclásicos, la principal diferencia entre la distribución de probabilidad para el sistema clásico y la pseudoprobabilidad dada por la función de Wigner para el sistema cuantizado suelen ser las oscilaciones dadas por la interferencia, que determinan cuándo el sistema cuántico se comporta en forma similar al clásico, y cuándo no.

En el área de la computación cuántica, el estudio de la interferencia en una superposición coherente de estados puede ser de interés para representar códigos de corrección de errores en el espacio de fases: un código que guarda un qubit de información en el estado de un grupo de qubits tiene como subespacio de estados permitidos el conjunto de superposiciones de los estados lógicos  $|0\rangle_L$  y  $|1\rangle_L$ .

En este capítulo se estudiará la representación en el espacio de fases de una superposición coherente de dos estados de un sistema de qubits, utilizando la función de Wigner en el espacio de fases con coordenadas en el cuerpo  $GF(d)$ . Se mostrará que en esta definición la interferencia tiende a desparramarse por todo el espacio de fases, a diferencia de lo que ocurre en la definición de la función de Wigner continua, y en sus generalizaciones con aritmética módulo  $d$  o  $2d$ .

Sin embargo, el comportamiento de la interferencia depende fuertemente de la grilla cuántica elegida. Al superponer dos estados asociados a líneas

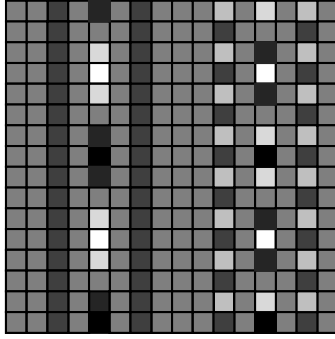


en el espacio de fases, siempre es posible elegir una grilla cuántica en la que la representación en el espacio de fases se asemeja a la del caso continuo, y está compuesta por las líneas que interfieren y términos oscilatorios intermedios. Pero hay muchas más grillas en las que la interferencia ocupa todo el espacio de fases, superponiéndose incluso con las líneas originales. Para sistemas de dos y tres qubits, se mostrará que no hay ninguna elección posible de grilla cuántica en la que la interferencia no se superponga con las líneas interfirientes para elecciones arbitrarias de estas líneas. Para superposiciones de estados de la base computacional, tomando grillas cuánticas al azar se verá que, a medida que aumenta la cantidad de qubits en el sistema, la interferencia tiende a desparramarse cada vez más, y a tomar valores más pequeños. Esto dificulta la identificación de las propiedades del estado a partir de su representación gráfica. Sin embargo, en algunos problemas se puede fijar una grilla cuántica en la que el comportamiento de la interferencia se asemeja al del caso continuo: como ejemplo, se estudiará la función de Wigner del código “perfecto” de 5 qubits [38].

## 5.1. La interferencia en la definición redundante de la función de Wigner

Como ya se ha mencionado, la representación del estado de un sistema de qubits en el espacio de fases cuyas coordenadas son números enteros de 0 a  $d$  no conserva algunas de las propiedades de la función de Wigner original, que pueden recuperarse utilizando aritmética módulo  $2d$ , al costo de agrandar el espacio de fases introduciendo redundancias en la representación. En esta definición de la función de Wigner [39], la superposición de dos estados tiene una representación en el espacio de fases en que los efectos de interferencia corresponden a franjas oscilantes en medio de los estados que interfieren. En este sentido, se asemeja a la función de Wigner continua, excepto por la aparición de las “imágenes fantasma” o “autointerferencias” (que son una consecuencia de la redundancia).

Como ejemplo, en la Figura 5.1 se muestra la representación de una superposición de dos estados de la base computacional; se observan franjas verticales de valor constante en las posiciones de los estados originales, y franjas oscilantes correspondientes a los efectos de interferencia de cada estado consigo mismo y con el otro. Las franjas de interferencia entre los dos estados se encuentran en medio de los dos (a causa de la periodicidad en el espacio de fases hay dos “puntos medios”) y oscilan en forma más lenta cuanto más cercanos se encuentran los estados que interfieren.



**Figura 5.1:** Representación a través de la función de Wigner redundante de una superposición coherente de dos estados de la base computacional; se observan franjas verticales de valor constante en las posiciones de los estados originales, y franjas oscilantes correspondientes a los efectos de interferencia de cada estado consigo mismo y con el otro.

## 5.2. La función de Wigner discreta de una superposición de estados estabilizadores

En el espacio de fases con coordenadas en el cuerpo  $GF(2^n)$ , los efectos de interferencia entre dos estados tienen en general una forma mucho más complicada. En este capítulo se estudiarán superposiciones coherentes de estados estabilizadores, y en particular el caso de estados de la base computacional (que es prácticamente igual al caso un poco más general de superposición de cualquier par de estados asociados a líneas de una misma estriación).

Dados dos estados  $|\psi_1\rangle$  y  $|\psi_2\rangle$  con funciones de Wigner  $W_1(\alpha)$  y  $W_2(\alpha)$ , la función de Wigner del estado  $|\psi\rangle = a|\psi_1\rangle + b|\psi_2\rangle$  está dada por:

$$\begin{aligned} W(\alpha) &= |a|^2 W_1(\alpha) + |b|^2 W_2(\alpha) + ab^* \langle \psi_2 | A(\alpha) | \psi_1 \rangle + a^* b \langle \psi_1 | A(\alpha) | \psi_2 \rangle = \\ &= |a|^2 W_1(\alpha) + |b|^2 W_2(\alpha) + 2\mathcal{R}e\{ab^* \langle \psi_2 | A(\alpha) | \psi_1 \rangle\} \end{aligned} \quad (5.1)$$

Es decir, la función de Wigner del estado superposición es una suma de las funciones de los estados originales (con sus respectivos pesos) y una parte de interferencia dada por los elementos de matriz de los operadores de punto entre los estados superpuestos. En el caso en que  $|\psi_1\rangle$  es un estado estabilizador,

$$\rho_1 = \frac{1}{d} \sum_{\mu \in S} g_\mu T(\mu) \quad (5.2)$$

y  $|\psi_2\rangle$  corresponde a una traslación de  $|\psi_1\rangle$ ,  $|\psi_2\rangle = T(\gamma)|\psi_1\rangle$ , para la parte

de interferencia se tiene:

$$\langle \psi_2 | A(\alpha) | \psi_1 \rangle = \langle \psi_1 | T(\gamma) A(\alpha) | \psi_1 \rangle = \text{Tr} \left( \rho_1 T(\gamma) A(\alpha) \right) \quad (5.3)$$

Reemplazando la expansión de  $\rho_1$  en términos de sus estabilizadores (5.2) y la de los operadores de punto en función de las traslaciones (3.36), resulta:

$$\langle \psi_2 | A(\alpha) | \psi_1 \rangle = \frac{1}{d^3} \sum_{\beta} \sum_{\mu \in S} g_{\mu} f_{\beta} (-1)^{\alpha \wedge \beta} \text{Tr} \left( T(\mu) T(\gamma) T(\beta) \right) \quad (5.4)$$

A causa de la ortogonalidad de los operadores de Pauli, las únicas contribuciones no nulas corresponden a puntos  $\beta = \gamma + \mu$ , por lo que se obtiene:

$$\langle \psi_2 | A(\alpha) | \psi_1 \rangle = \frac{1}{d^3} \sum_{\mu \in S} g_{\mu} f_{\gamma + \mu} (-1)^{\alpha \wedge (\gamma + \mu)} \text{Tr} \left( T(\mu) T(\gamma) T(\gamma + \mu) \right) \quad (5.5)$$

El valor de la traza en esta última ecuación depende de los puntos  $\gamma$  y  $\mu$  en cuestión, ya que  $T(\alpha + \beta) = \pm T(\alpha) T(\beta)$ . El signo  $\pm 1$  surge como consecuencia de que, en el cálculo de las coordenadas del punto  $\alpha + \beta$ , la suma de las  $n$ -uplas asociadas a las coordenadas de los puntos  $\alpha$  y  $\beta$  es módulo 2, mientras que en la fase que hace hermíticos a los operadores de traslación (3.14) la suma de  $n$ -uplas es módulo 4. Partiendo de:

$$T(\alpha + \beta) = X^{\vec{q}_{\alpha} + \vec{q}_{\beta}} Z^{\vec{p}_{\alpha} + \vec{p}_{\beta}} e^{i \frac{\pi}{2} (\vec{q}_{\alpha} \oplus \vec{q}_{\beta}) \cdot (\vec{p}_{\alpha} \oplus \vec{p}_{\beta})} \quad (5.6)$$

donde  $\vec{a} \oplus \vec{b}$  indica que la suma de  $n$ -uplas es módulo 2, y definiendo

$$x_{\alpha\beta} = \sum_{i=1}^n (\vec{q}_{\alpha} + \vec{q}_{\beta})_i (\vec{p}_{\alpha})_i (\vec{p}_{\beta})_i + (\vec{p}_{\alpha} + \vec{p}_{\beta})_i (\vec{q}_{\alpha})_i (\vec{q}_{\beta})_i \quad (5.7)$$

resulta:

$$T(\alpha + \beta) = T(\alpha) T(\beta) e^{i \frac{\pi}{2} \alpha \wedge \beta} (-1)^{x_{\alpha\beta}} \quad (5.8)$$

Insertando este resultado en la ecuación (5.5), se tiene:

$$\langle \psi_2 | A(\alpha) | \psi_1 \rangle = \frac{1}{d^2} \sum_{\mu \in S} g_{\mu} f_{\gamma + \mu} (-1)^{\alpha \wedge (\gamma + \mu)} e^{i \frac{\pi}{2} \gamma \wedge \mu} (-1)^{x_{\gamma\mu}} \quad (5.9)$$

de donde se ve que la parte de interferencia depende de cuáles son los estados superpuestos (a través de los valores de  $\mu$  en la sumatoria, de los autovalores  $g_{\mu}$  y del desplazamiento relativo  $\gamma$ ) y también de la grilla cuántica, a causa del factor  $f_{\gamma + \mu}$ .

### 5.3. Superposiciones de estados de la base computacional

Como caso particular, se considerarán estados de la base computacional:  $|\psi_1\rangle = |\vec{0}\rangle$  y  $|\psi_2\rangle = |\vec{m}\rangle$  ( $T(\gamma) = T(\vec{m}, \vec{0}) = X^{\vec{m}}$ ). Las funciones de Wigner de los estados que interfieren son líneas verticales ubicadas en  $\vec{q} = \vec{0}$  y  $\vec{q} = \vec{m}$ . Los estabilizadores de  $|\psi_1\rangle$  son los operadores de la forma  $Z^{\vec{k}}$ ; por lo tanto, de la ecuación (5.7) puede verse que para  $\mu \in S$  resulta  $x_{\gamma\mu} = 0$ . El término de interferencia puede calcularse a partir de (5.9) según:

$$\begin{aligned} \langle \vec{m} | A(\vec{q}, \vec{p}) | \vec{0} \rangle &= \frac{1}{d^2} \sum_{\vec{k}} g_{(\vec{0}, \vec{k})} f_{(\vec{m}, \vec{k})} (-1)^{\vec{q} \cdot \vec{k} - \vec{m} \cdot \vec{p}} e^{i \frac{\pi}{2} \vec{m} \cdot \vec{k}} = \\ &= \frac{(-1)^{\vec{m} \cdot \vec{p}}}{d^2} \sum_{\vec{k}} f_{(\vec{m}, \vec{k})} (-1)^{\vec{q} \cdot \vec{k}} e^{i \frac{\pi}{2} \vec{m} \cdot \vec{k}} \end{aligned} \quad (5.10)$$

De acuerdo a esta expresión, la parte de interferencia depende de las coordenadas de posición y momento en forma separable. La dependencia con el momento corresponde a una oscilación en la dirección vertical: para un dado valor de  $\vec{q}$ , el módulo de la interferencia es constante y el signo depende de  $(-1)^{\vec{m} \cdot \vec{p}}$ , de manera que la suma del término de interferencia a lo largo de cualquier línea vertical se anula. El factor que es función de la coordenada de posición es de la forma:

$$F(\vec{q}) = \sum_{\vec{k}} f_{(\vec{m}, \vec{k})} (-1)^{\vec{q} \cdot \vec{k}} e^{i \frac{\pi}{2} \vec{m} \cdot \vec{k}} \quad (5.11)$$

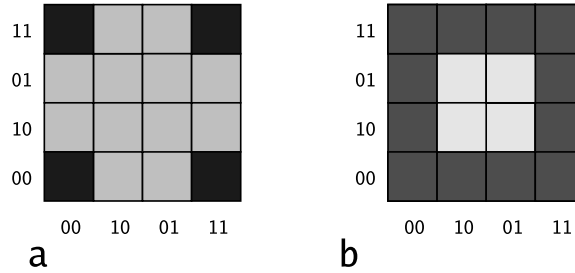
$F(\vec{q})$  depende del desplazamiento relativo  $\vec{m}$  y también de la grilla cuántica elegida, y verifica:

$$F(\vec{q} + \vec{m}) = \sum_{\vec{k}} f_{(\vec{m}, \vec{k})} (-1)^{(\vec{q} + \vec{m}) \cdot \vec{k}} e^{i \frac{\pi}{2} \vec{m} \cdot \vec{k}} = F(\vec{q})^* \quad (5.12)$$

En general, para una grilla cuántica arbitraria, la parte de interferencia tendrá valores no nulos en cualquier coordenada  $\vec{q}$ . Para dos estados fijos  $|\vec{0}\rangle$  y  $|\vec{m}\rangle$ , siempre es posible imponer sobre la grilla cuántica la condición de que la suma en  $F(\vec{q})$  sea totalmente constructiva en algún valor de  $\vec{q}$  a elección. En este caso, la suma será también totalmente constructiva en  $\vec{q} + \vec{m}$ , y en cambio en cualquier otro valor de  $\vec{q}$  los distintos términos se cancelarán (este procedimiento se muestra en una situación parecida en la sección 5.4). La función de Wigner que se obtiene de esta manera está compuesta por las líneas verticales originales, y dos líneas verticales oscilantes. Sin embargo, si para los estados  $|\vec{0}\rangle$  y  $|\vec{m}\rangle$  se elige una grilla con esta propiedad, al elegir

otro par de estados  $|\vec{0}\rangle$  y  $|\vec{m}'\rangle$  la función de Wigner ya no tendrá, en general, la misma forma.

Como ejemplo, consideremos el estado de Bell  $|\phi_+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ . Este estado es una superposición de los estados computacionales  $|00\rangle$  y  $|11\rangle$ , y es autoestado de los operadores de Pauli  $X_{(1)}X_{(2)}$  y  $Z_{(1)}Z_{(2)}$ . Esto implica que su función de Wigner debe ser invariante frente a las traslaciones asociadas en el espacio de fases. En [4] se muestra que, teniendo en cuenta las propiedades de este estado, para distintas grillas cuánticas sólo pueden obtenerse dos representaciones diferentes en el espacio de fases, que se muestran en la Figura 5.2. En una de ellas (que ya apareció en la subsección 3.2.7), la función de Wigner sólo es no nula en los puntos del espacio de fases asociados al estabilizador de  $|\phi_+\rangle$ . En la otra, la función de Wigner es no nula en todos los puntos, y está compuesta por dos líneas constantes y positivas en las posiciones de los estados que interfieren, y dos líneas verticales oscilantes entre ellos. Este ejemplo muestra dos comportamientos diferentes de la interferencia: en el primer caso, se superpone con las líneas originales; en el otro, está restringida a la zona intermedia.



**Figura 5.2:** Las posibles funciones de Wigner para el estado de Bell  $|\phi_+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ , que es una superposición de dos estados de la base computacional. Los tonos oscuros son positivos y los claros, negativos. a) Para algunas elecciones de la grilla cuántica, la función de Wigner sólo es no nula en los puntos de espacio de fases asociados al estabilizador de  $|\phi_+\rangle$ ; en este caso, la interferencia aparece sobre las dos líneas originales, aumentando el valor de la función de Wigner en las esquinas, y anulándolo en los otros puntos. b) En otras grillas cuánticas, la función de Wigner está formada por las líneas superpuestas, más una contribución oscilante de la interferencia que aparece solamente en la región intermedia.

Por comparación con la propuesta redundante para la función de Wigner, se estudiará bajo qué condiciones la interferencia entre los estados  $|\vec{0}\rangle$  y  $|\vec{m}\rangle$  se anula sobre las líneas asociadas a estos estados; si éste es el caso, la función de Wigner de la superposición estará compuesta por dos líneas verticales de

valor constante en las posiciones de los estados interfirientes y oscilaciones verticales en posiciones intermedias. Dada la relación  $F(\vec{q} + \vec{m}) = F(\vec{q})^*$ , la condición para que la parte de interferencia se anule en las dos líneas originales es la misma y está dada por:

$$F(\vec{0}) = \sum_{\vec{k}} f_{(\vec{m}, \vec{k})} e^{i\frac{\pi}{2}\vec{m} \cdot \vec{k}} = 0 \quad (5.13)$$

Para cada valor de  $\vec{m}$ , se tienen dos ecuaciones sobre la grilla cuántica, dadas por las partes real e imaginaria de la ecuación anterior, y en ellas aparecen relaciones entre las  $f_{(\vec{m}, \vec{k})}$  para el valor de  $\vec{m}$  dado. Si se pretende que la condición de interferencia fuera de las líneas originales valga simultáneamente para todos los valores de  $\vec{m}$ , se imponen sobre la grilla cuántica  $2(d-1)$  ecuaciones en total. De las constantes  $f_{(\vec{m}, \vec{k})}$  (con  $\vec{m} \neq \vec{0}$ , y considerando  $f_{(\vec{m}, \vec{0})} = 1 \forall \vec{m}$ ) sólo  $n(d-1)$  son independientes; pueden elegirse como independientes las  $f_{(\vec{m}, \vec{k})}$  correspondientes a las primeras  $n$  posiciones no nulas  $\vec{m}$  y los  $d-1$  posibles valores no nulos de  $\vec{k}$ . Para esta elección, las condiciones de interferencia fuera de las líneas originales son lineales (e independientes) para los primeros  $n$  valores no nulos de  $\vec{m}$ , y no lineales para los  $d-1-n$  valores no nulos restantes.

### 5.3.1. El caso de dos qubits

En el caso de dos qubits, hay tres desplazamientos  $\vec{m}$  posibles entre los estados que interfieren; las condiciones de interferencia fuera de las líneas originales (5.13) para todos los desplazamientos posibles son:

$$\begin{cases} f_{(\vec{q}_0, \vec{0})} + f_{(\vec{q}_0, \vec{p}_1)} + i(f_{(\vec{q}_0, \vec{p}_0)} + f_{(\vec{q}_0, \vec{p}_2)}) & = 0 \\ f_{(\vec{q}_1, \vec{0})} + f_{(\vec{q}_1, \vec{p}_0)} + i(f_{(\vec{q}_1, \vec{p}_1)} + f_{(\vec{q}_1, \vec{p}_2)}) & = 0 \\ f_{(\vec{q}_2, \vec{0})} - f_{(\vec{q}_2, \vec{p}_2)} + i(f_{(\vec{q}_2, \vec{p}_0)} + f_{(\vec{q}_2, \vec{p}_1)}) & = 0 \end{cases} \quad (5.14)$$

Las constantes  $f_{(\vec{q}, \vec{0})}$  son todas iguales a 1; las otras constantes no son independientes, y las  $f_{(\vec{q}_2, \vec{p}_i)}$  pueden obtenerse a partir de las otras  $f$ s en el mismo rayo según:

$$\begin{cases} f_{(\vec{q}_2, \vec{p}_0)} & = -f_{(\vec{q}_0, \vec{p}_1)} f_{(\vec{q}_1, \vec{p}_2)} \\ f_{(\vec{q}_2, \vec{p}_1)} & = -f_{(\vec{q}_0, \vec{p}_2)} f_{(\vec{q}_1, \vec{p}_0)} \\ f_{(\vec{q}_2, \vec{p}_2)} & = f_{(\vec{q}_0, \vec{p}_0)} f_{(\vec{q}_1, \vec{p}_1)} \end{cases} \quad (5.15)$$

Reemplazando estas expresiones en las ecuaciones anteriores, la condición (5.14) para todo desplazamiento relativo  $\vec{m}$  implica que:

$$\begin{cases} f_{(\vec{q}_0, \vec{0})} + f_{(\vec{q}_1, \vec{p}_1)} & = 0 \\ f_{(\vec{q}_0, \vec{p}_0)} f_{(\vec{q}_1, \vec{p}_1)} & = 1 \end{cases} \quad (5.16)$$

lo cual no puede satisfacerse para ninguna elección de  $f_{(\vec{q}_0, \vec{p}_0)}$ ,  $f_{(\vec{q}_1, \vec{p}_1)}$ .

En conclusión, para un sistema de dos qubits, dado un estado formado por una superposición coherente de estados de la base computacional, siempre es posible elegir una grilla cuántica de forma tal que la función de Wigner del estado corresponda a dos líneas verticales constantes en las posiciones de los estados originales, más líneas verticales oscilantes en posiciones intermedias; sin embargo, no existe ninguna grilla cuántica para la cual la función de Wigner tenga esta propiedad para cualquier desplazamiento relativo entre los estados que interfieren (es conveniente notar que, si bien las condiciones estudiadas correspondían a los estados  $|\vec{0}\rangle$  y  $|\vec{m}\rangle$ , aplicando traslaciones sobre los estados de esta forma puede obtenerse cualquier superposición de estados de la base computacional).

### 5.3.2. Tres qubits, o más

Para sistemas con mayor número de qubits, el problema se hace más difícil no sólo porque la cantidad de ecuaciones aumenta exponencialmente, sino porque a la vez aumenta su grado (para dos qubits se pueden tener a lo sumo ecuaciones cuadráticas, para tres qubits cúbicas, etc.). Para el caso de tres qubits se escribieron las relaciones entre las constantes  $f_\beta$  y las condiciones (5.13) para todos los desplazamientos relativos, obteniéndose un sistema de 14 ecuaciones no lineales para las 21 constantes independientes. El problema fue estudiado barriando sobre todas las elecciones posibles y controlando la validez de las ecuaciones, no resultando posible satisfacerlas a todas en ninguno de los casos.

De los cálculos realizados, entonces, se concluye que para sistemas de dos o tres qubits no es posible elegir una grilla cuántica tal que para una superposición arbitraria de estados de la base computacional la parte de interferencia de la función de Wigner se anule sobre las líneas correspondientes a los estados superpuestos. Dados estos resultados, es natural conjeturar que la misma situación se repetirá para sistemas con cualquier cantidad de qubits. Por otra parte, sólo se estudiaron los casos de superposiciones de estados de la base computacional; la condición de interferencia fuera de las líneas para estados en otras estriaciones conduce a conjuntos similares de ecuaciones (con las constantes  $f_\beta$  agrupadas de otras formas, la suma sobre los puntos  $\mu$  asociados al rayo de la estriación que corresponda y con el agregado del signo  $(-1)^{x\gamma\mu}$ ). Por lo tanto, parece razonable suponer que en general no es posible elegir una grilla cuántica tal que la función de Wigner estudiada comparta con la definición redundante la propiedad de que la interferencia ocurre en zonas intermedias a los estados originales, para superposiciones

arbitrarias de dos líneas en la misma estriación. En consecuencia, la representación gráfica del estado dada por la función de Wigner con coordenadas en  $GF(d)$  parece ser de interpretación más difícil que en la definición redundante, a causa de la superposición del patrón de interferencia con las líneas interfirientes.

### 5.3.3. Comportamiento promedio de la interferencia

A continuación, se analizaron las funciones de Wigner de superposiciones de dos estados  $|\vec{0}\rangle$  y  $|\vec{m}\rangle$  de la base computacional utilizando grillas cuánticas elegidas al azar, con el objetivo de encontrar, de ser posible, características comunes en la representación de estos estados, y tendencias en las propiedades “promedio” de sus funciones de Wigner al aumentar el número de qubits.

Para esto, se estudió la parte de los términos de interferencia que depende de la posición, esto es, la función  $F(\vec{q})$  (5.11). Esta función compleja, que depende también de la grilla cuántica elegida y del desplazamiento relativo  $\vec{m}$  entre los estados superpuestos, tiene las siguientes propiedades:

1.  $\mathcal{R}e(F(\vec{q})), \mathcal{I}m(F(\vec{q})) \in \mathbb{N}$ .
2.  $F(\vec{q} + \vec{m}) = F(\vec{q})^*$
3.  $\sum_{\vec{q}} F(\vec{q}) = d$

Para cada valor de  $\vec{m}$ , siempre es posible elegir una grilla cuántica en forma tal que la interferencia aparezca en sólo dos líneas verticales del espacio de fases, separadas entre sí por un desplazamiento  $\vec{m}$ . En este caso, en que la interferencia se halla tan concentrada como es posible, sobre estas dos líneas las partes reales e imaginarias de  $F(\vec{q})$  alcanzan sus máximos valores posibles (en módulo), de  $\pm d/2$ . Sin embargo, la misma grilla cuántica no conservará estas propiedades si se elige otro desplazamiento relativo  $\vec{m}'$ . Y, por otra parte, si se elige una grilla cuántica al azar la probabilidad de que, para un dado  $\vec{m}$ , la interferencia tenga estas características decae rápidamente a medida que crece el número de qubits.

El estudio del comportamiento promedio de la parte de interferencia se realizó eligiendo grillas cuánticas al azar y calculando los valores de  $F(\vec{q})$  para todas las posiciones  $\vec{q}$  y para cada posible desplazamiento  $\vec{m}$ , para sistemas de 2 a 10 qubits. Para cada una de las grillas cuánticas se calcularon las partes reales e imaginarias de  $F(\vec{q})$  para todos los desplazamientos relativos y se las dividió por  $d^2$  para obtener, a menos del signo dependiente de  $\vec{p}$ , el elemento de matriz del operador de punto asociado al valor de la



interferencia (5.10). Tanto para las partes reales como para las imaginarias (por separado) se tomaron los módulos de los valores obtenidos y se buscó el valor máximo, para compararlo con el valor de la función de Wigner sobre las líneas originales.

Para mejorar la caracterización de la interferencia, se calculó además la entropía de las distribuciones. Para esto, se sumaron todos los valores de  $F(\vec{q})$  (siempre en módulo, y siempre separando partes reales e imaginarias) y se los normalizó a 1, de modo de poder interpretarlos como los coeficientes  $\mathcal{P}(\vec{q})$  de una distribución probabilística. La entropía de la distribución se calculó luego en la forma:

$$S = - \sum_{\vec{q}} \mathcal{P}(\vec{q}) \ln(\mathcal{P}(\vec{q})) \quad (5.17)$$

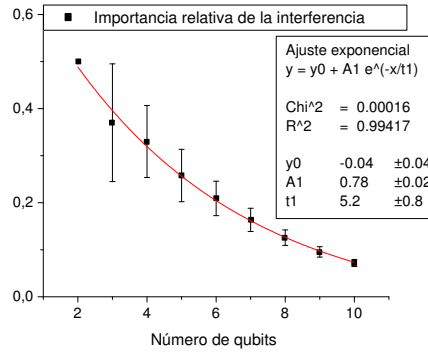
Así definida, la entropía de una distribución concentrada en un único valor de  $\vec{q}$  es igual a cero, mientras que la máxima entropía posible corresponde a una distribución uniforme y vale  $\ln(d)$ . Para poder estudiar más fácilmente el comportamiento de esta cantidad al variar el número de qubits, se definió una entropía normalizada de tal modo que la distribución uniforme corresponda siempre a un valor de 1:

$$\tilde{S} = \frac{S}{\ln(d)} = - \sum_{\vec{q}} \mathcal{P}(\vec{q}) \log_d(\mathcal{P}(\vec{q})) \quad (5.18)$$

Los máximos y entropías fueron calculados para todos los desplazamientos posibles en sistemas de 2 a 10 qubits tomando 50 grillas cuánticas al azar en cada caso. Dado que no se observaron diferencias importantes entre las distintas grillas cuánticas, se promediaron conjuntamente los  $50(d-1)$  resultados obtenidos para los  $d-1$  desplazamientos posibles en las 50 grillas. Los valores obtenidos para las partes reales e imaginarias son iguales teniendo en cuenta sus dispersiones.

Considerando que el valor de la función de Wigner es del orden de  $1/d$  en las líneas asociadas a los estados originales, los máximos hallados fueron multiplicados por  $d$  con el fin de estimar la importancia relativa de la parte de interferencia. De acuerdo a los resultados obtenidos, esta importancia decae a cero a medida que aumenta el número de qubits en el sistema. En la Figura 5.3 se muestra el valor máximo hallado para la interferencia, en promedio y multiplicado por  $d$ , en función del número de qubits, y su ajuste exponencial.

El hecho de que, en general, la importancia relativa de la parte de interferencia decaiga a medida que aumenta el número de qubits tiene como consecuencia que en la representación gráfica del estado la interferencia se



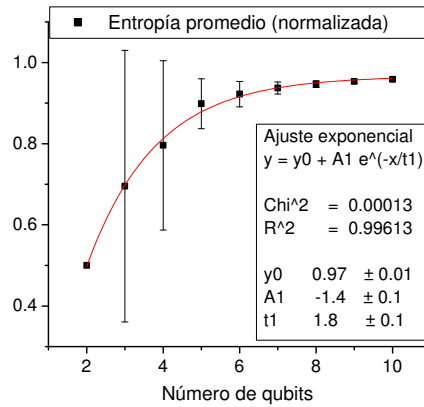
**Figura 5.3:** Decaimiento de la importancia de la interferencia (en promedio) frente a los valores de la función de Wigner en las líneas correspondientes a los estados superpuestos, a medida que aumenta el número de qubits en el sistema. Los valores en el gráfico corresponden a los máximos valores de las partes reales (en módulo) de  $F(\vec{q})$ , multiplicados por  $d$  (ya que la función de Wigner en las líneas originales es de orden  $1/d$ ), y promediados sobre todos los desplazamientos posibles en 50 grillas cuánticas tomadas al azar. Las barras de error están dadas por la desviación estándar. En línea continua se muestra el ajuste exponencial de los datos.

hace cada vez más débil, y por lo tanto se complica la distinción entre superposiciones coherentes y estadísticas (de todos modos, esto podría resolverse usando una relación no lineal entre los valores de la función de Wigner y los tonos de gris asociados).

Para la entropía normalizada, se halló un crecimiento que tiende a saturarse en la medida en que aumenta el número de qubits, es decir, cuanto más grande la dimensión del sistema más uniformemente están distribuidos, en promedio, los valores de  $F(\vec{q})$ . Al aumentar la cantidad de qubits, entonces, la interferencia tiende a ocupar todo el espacio de fases. El ajuste exponencial de la entropía para las partes reales se muestra en la Figura 5.4.

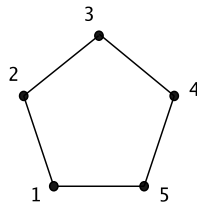
## 5.4. Un último ejemplo: el código perfecto

Para terminar este capítulo, consideremos un ejemplo en el cual la representación de la interferencia en el espacio de fases se parece a la de la función de Wigner continua: el código “perfecto” de corrección de errores de un qubit. Éste proporciona un mecanismo para proteger la información de un qubit a través de su codificación en el estado de un sistema de cinco qubits [38]. El subespacio de estados aceptables en este código es el formado por



**Figura 5.4:** Dependencia de la entropía (normalizada) de la distribución de interferencia con el número de qubits en el sistema. Los resultados corresponden a promedios en un barrido sobre las partes reales de  $F(\vec{q})$  en todos los desplazamientos relativos  $\vec{m}$  en 50 grillas cuánticas elegidas al azar. Las barras de error están dadas por la desviación estándar. En línea continua se muestra el ajuste exponencial de los datos.

las combinaciones de los estados del sistema de cinco qubits  $|0\rangle_L$  y  $|1\rangle_L$  (que serían la versión codificada de los estados de la base computacional de un qubit). Estos estados son estados estabilizadores, y están emparentados con el estado-grafo correspondiente a un anillo de cinco qubits, que se muestra en la Figura 5.5.



**Figura 5.5:** El estado-grafo correspondiente a un anillo de 5 qubits; este estado está emparentado con el código perfecto de corrección de un qubit.

El estabilizador del estado-grafo en cuestión está generado por los operadores de Pauli  $S_i$  que aplican  $X$  sobre el vértice  $i$ -ésimo y  $Z$  sobre sus vecinos, o sea  $S_i = Z_{(i-1)}X_{(i)}Z_{(i+1)}$  (donde los índices son cíclicos de 1 a 5). En el código de corrección de errores considerado, el subespacio de estados admisibles se define como el formado por los estados que son estabilizados

por los operadores  $S_i S_j$ . Se dice entonces que este conjunto de operadores forma el estabilizador del código.

El estado lógico  $|0\rangle_L$  se elige como el estado cuyo estabilizador es generado por los operadores de la forma  $S_i S_j$  y el producto de operadores  $Z$  sobre todos los qubits a la vez. El otro estado de la base computacional codificada,  $|1\rangle_L$ , es estabilizado por los operadores  $S_i S_j$  y por el operador  $-Z_{(1)} \dots Z_{(5)}$ . De esta forma, los dos estados lógicos son estabilizados por los operadores  $S_i S_j$  (y por lo tanto cualquier estado admisible, que es combinación lineal de  $|0\rangle_L$  y  $|1\rangle_L$ ) mientras que el operador que distingue entre los dos estados de la base computacional codificada es  $\tilde{Z} = Z_{(1)} \dots Z_{(5)}$ . El operador que intercambia los dos estados en esta base es el que aplica  $X$  sobre cada qubit, o sea  $\tilde{X} = X_{(1)} \dots X_{(5)}$ , que es igual, a menos de un signo, al producto de los estabilizadores del grafo:  $\tilde{X} = -S_1 \dots S_5$  (todos los operadores  $Z$  se cancelan entre sí al realizar este producto, y el signo aparece al conmutarlos con operadores  $X$ ).

¿Cómo se relaciona el código con el estado-grafo? El estabilizador del estado-grafo es generado por los operadores  $S_i$ ; pero equivalentemente su generador se puede elegir como el conjunto de operadores  $S_i S_j$  (que generan el estabilizador del código), más el operador  $\tilde{X} = -S_1 \dots S_5$ . O sea, el estado-grafo estaría asociado al estado codificado  $|-\rangle_L = (|0\rangle_L - |1\rangle_L)/\sqrt{2}$ .

Todos los estados admisibles en el sistema son combinaciones lineales de  $|0\rangle_L$  y  $|1\rangle_L$ , pero alternativamente se pueden pensar como combinaciones lineales de los estados  $|-\rangle_L$  y  $|+\rangle_L$ , donde el primero es el estado-grafo y el segundo el que se obtiene aplicando  $Z$  sobre todos los qubits en el estado-grafo. Entonces, todos estos estados pueden escribirse en la forma:

$$|\psi\rangle_L = a|-\rangle_L + b|+\rangle_L, \quad \text{con } |a|^2 + |b|^2 = 1 \quad (5.19)$$

En la subsección 3.2.8 se propone una definición de Wigner en la cual los estados-grafo y sus traslaciones tienen una representación particularmente simple, dada por las líneas horizontales en el espacio de fases. En esta definición, las traslaciones horizontales en el espacio de fases están asociadas a los operadores de Pauli  $S_i$  en el estabilizador del grafo, y las verticales a los operadores  $Z_{(i)}$ . El estado-grafo  $|-\rangle_L$  corresponde al rayo horizontal,  $\vec{p} = (0, 0, 0, 0, 0) = \vec{0}$ , mientras que el  $|+\rangle_L$  es la línea horizontal que corresponde al rayo trasladado aplicando  $Z$  sobre todos los qubits, o sea, la línea  $\vec{p} = (1, 1, 1, 1, 1) = \vec{m}$ . Entonces, en esta definición de la función de Wigner todos los estados codificados corresponden a superposiciones de estas dos líneas horizontales.

Con los mismos pasos de antes, pero ahora aplicados a la nueva definición,

se puede ver que la función de Wigner del estado  $|\psi\rangle_L$  está dada por:

$$W'_\psi(\vec{q}, \vec{p}) = |a|^2 W'_-(\vec{q}, \vec{p}) + |b|^2 W'_+(\vec{q}, \vec{p}) + 2W'_{int}(\vec{q}, \vec{p}) \quad (5.20)$$

donde:

$$W'_-(\vec{q}, \vec{p}) = (1/d) \delta(\vec{p}) \quad (5.21)$$

$$W'_+(\vec{q}, \vec{p}) = (1/d) \delta(\vec{p} - \vec{m}) \quad (5.22)$$

$$W'_{int}(\vec{q}, \vec{p}) = (2/d^2) (-1)^{\vec{q} \cdot \vec{m}} \mathcal{R}e \left\{ ab^* \sum_{\vec{x}} (-1)^{\vec{x} \cdot \vec{p}} f'_{(\vec{x}, \vec{m})} e^{-i \frac{\pi}{2} \vec{x} \cdot \vec{m}} \right\} \quad (5.23)$$

donde la sumatoria en la última expresión es sobre todas las  $n$ -uplas binarias  $\vec{x}$ . O sea, la función de Wigner es una superposición de las líneas horizontales asociadas a  $|-\rangle_L$  y  $|+\rangle_L$ , y una parte de interferencia que oscila a lo largo de la dirección horizontal, y que depende fuertemente de la grilla cuántica elegida.

Siempre es posible elegir una grilla cuántica en la que esta función de Wigner tenga una forma bonita, en que la interferencia aparezca sólo en dos líneas horizontales intermedias  $\vec{p}_{int}$  y  $\vec{p}_{int} + \vec{m}$ . Lo que hay que hacer para esto es imponer sobre la grilla cuántica las condiciones:

$$f'_{(\vec{x}, \vec{m})} = \begin{cases} (-1)^{\vec{x} \cdot \vec{p}_{int}} e^{i \frac{\pi}{2} \vec{x} \cdot \vec{m}} & \text{si } \vec{x} \cdot \vec{m} = 0 \pmod{2} \\ -i (-1)^{\vec{x} \cdot \vec{p}_{int}} e^{i \frac{\pi}{2} \vec{x} \cdot \vec{m}} & \text{si } \vec{x} \cdot \vec{m} = 1 \pmod{2} \end{cases} \quad (5.24)$$

Al imponer esas restricciones sobre la grilla cuántica, la sumatoria sobre las  $n$ -uplas  $\vec{x}$  es totalmente constructiva en los valores  $\vec{p} = \vec{p}_{int}$  y  $\vec{p} = \vec{p}_{int} + \vec{m}$ , y se anula en todos los demás casos. La función de Wigner que se obtiene, entonces, es de la forma de (5.20), con la parte de interferencia dada por:

$$W'_{int}(\alpha) = 1/d (-1)^{\vec{q} \cdot \vec{m}} \left\{ \delta(\vec{p} - \vec{p}_{int}) [\mathcal{R}e\{ab^*\} + \mathcal{I}m\{ab^*\}] + \delta(\vec{p} - \vec{p}_{int} - \vec{m}) [\mathcal{R}e\{ab^*\} - \mathcal{I}m\{ab^*\}] \right\} \quad (5.25)$$

Como ejemplo, consideremos los estados de la base computacional codificada: son combinaciones de  $|+\rangle_L$  y  $|-\rangle_L$  de la forma:

$$|0\rangle_L = (|-\rangle_L + |+\rangle_L)/\sqrt{2} \quad (5.26)$$

$$|1\rangle_L = (-|-\rangle_L + |+\rangle_L)/\sqrt{2} \quad (5.27)$$

o sea que sus funciones de Wigner, para esta grilla cuántica, son:

$$W'_0(\alpha) = \{\delta(\vec{p}) + \delta(\vec{p} - \vec{m}) + (-1)^{\vec{q} \cdot \vec{m}} [\delta(\vec{p} - \vec{p}_{int}) + \delta(\vec{p} - \vec{p}_{int} - \vec{m})]\} / (2d) \quad (5.28)$$

$$W'_1(\alpha) = \{\delta(\vec{p}) + \delta(\vec{p} - \vec{m}) - (-1)^{\vec{q} \cdot \vec{m}} [\delta(\vec{p} - \vec{p}_{int}) + \delta(\vec{p} - \vec{p}_{int} - \vec{m})]\} / (2d) \quad (5.29)$$

En la Figura 5.6 se muestra la representación del estado-grafo  $|-\rangle_L$  y el estado de la base computacional codificada  $|0\rangle_L$ .

Como última cosa, veamos que cuando ocurre un error en forma de aplicación de  $X$ ,  $Z$  o  $Y$  sobre un qubit, la operación transforma el estado en uno ortogonal al subespacio de estados codificados, y por lo tanto el error puede ser detectado. Además, los subespacios de estados erróneos son ortogonales entre sí, con lo cual los distintos errores de Pauli de un qubit pueden ser identificados y corregidos. Los errores de Pauli considerados forman una base para todos los errores de un qubit, y por lo tanto la corrección de errores de Pauli de un qubit garantiza la de cualquier error de un qubit [40, 41].

La condición de ortogonalidad entre dos estados con funciones de Wigner  $W'_a(\alpha)$  y  $W'_b(\alpha)$  está dada, de acuerdo a la ecuación (3.11), por:

$$\sum_{\alpha} W'_a(\alpha)W'_b(\alpha) = 0 \quad (5.30)$$

En la definición de la función de Wigner que estamos considerando, y con una grilla cuántica conveniente, todos los estados codificados tienen representaciones en el espacio de fases que consisten de dos líneas horizontales positivas con valores constantes en  $\vec{p} = \vec{0}$  y  $\vec{p} = \vec{m}$ , y dos líneas horizontales oscilantes en  $\vec{p} = \vec{p}_{int}$  y  $\vec{p} = \vec{p}_{int} + \vec{m}$ , donde  $\vec{p}_{int}$  es una  $n$ -upla fija a elección. La suma de los valores sobre una línea oscilante es cero, y la función de Wigner es nula en todos los otros puntos del espacio de fases. La única excepción a esta descripción son los estados  $|-\rangle_L$  y  $|+\rangle_L$ , cuya representación está dada por una única línea horizontal constante.

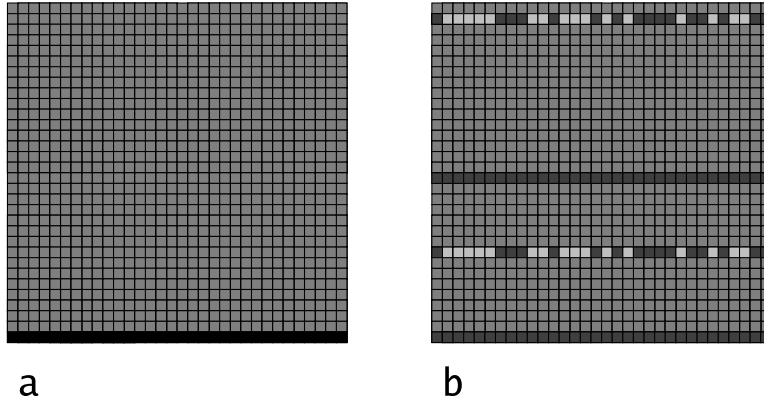
La aplicación de un error de Pauli corresponde a una traslación en el espacio de Hilbert, y por lo tanto produce una traslación de la función de Wigner en el espacio de fases. Para que la función de Wigner de un estado codificado cualquiera, al trasladarla, resulte ortogonal a la de todos los estados codificados, alcanza con que las nuevas líneas horizontales constantes se encuentren en valores de  $\vec{p}$  distintos de  $\vec{0}$  y  $\vec{m}$ , y las nuevas líneas oscilantes no se encuentren en  $\vec{p}_{int}$  o  $\vec{p}_{int} + \vec{m}$ . La superposición de líneas constantes en la función trasladada con líneas oscilantes en la función original (o viceversa) no importa ya que la suma sobre los puntos da cero. Para garantizar la ortogonalidad entre los estados erróneos y los permitidos, entonces, alcanza con ver que las operaciones aplicadas corresponden a traslaciones que modifican las coordenadas  $\vec{p}$  sumándoles una  $n$ -upla que no es  $\vec{0}$  ni  $\vec{m}$ .

Consideremos ahora los distintos errores de Pauli de un qubit. Todos ellos son traslaciones; la parte horizontal de estas traslaciones no nos interesa, ya que es suficiente saber cómo se transforman las coordenadas  $\vec{p}$  de las líneas constantes y oscilantes. Las transformaciones de  $\vec{p}$  para cada uno de los

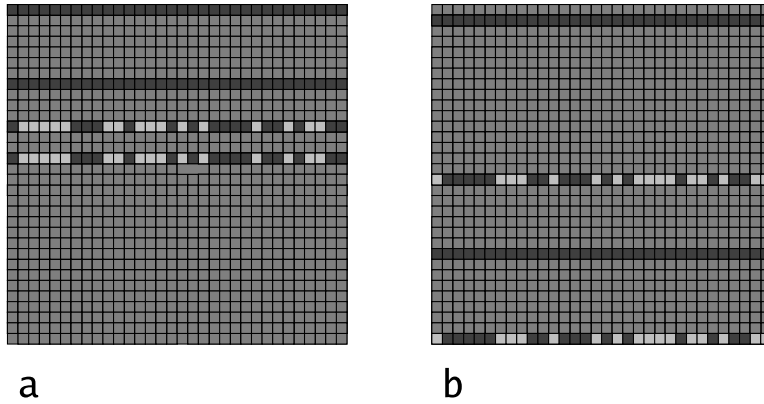
errores de Pauli de un qubit son las siguientes:

1. Error tipo  $Z_{(i)}$ : es una traslación vertical, que actúa sobre  $\vec{p}$  en la forma:  $p_i \rightarrow p_i + 1$ .
2. Error tipo  $X_{(i)}$ : es una traslación oblicua, equivalente a  $S_i Z_{(i-1)} Z_{(i+1)}$ . La parte de traslación vertical transforma las coordenadas  $\vec{p}$  según:  $p_{i-1} \rightarrow p_{i-1} + 1, p_{i+1} \rightarrow p_{i+1} + 1$ .
3. Error tipo  $Y_{(i)}$ : también es una traslación oblicua, ahora equivalente a  $S_i Z_{(i-1)} Z_{(i)} Z_{(i+1)}$ . La parte de traslación vertical transforma  $\vec{p}$  de acuerdo a:  $p_{i-1} \rightarrow p_{i-1} + 1, p_i \rightarrow p_i + 1, p_{i+1} \rightarrow p_{i+1} + 1$ .

O sea, los errores tipo  $Z$  transforman sólo la componente de  $\vec{p}$  correspondiente al qubit en el que ocurrió el error, los errores  $X$  transforman las componentes asociadas a sus vecinos, y los errores  $Y$  cambian las del qubit “erróneo” y las de sus vecinos. Ninguno de estos errores deja  $\vec{p}$  sin cambios, y ninguno altera las cinco componentes de  $\vec{p}$ . En conclusión, los estados erróneos efectivamente son ortogonales a los codificados. Por otra parte, comparando la forma en que actúan los distintos errores considerados es fácil ver que todos los errores conducen a subespacios ortogonales entre sí, y por lo tanto pueden ser distinguidos unos de otros, lo que permite corregirlos. Esto ya no ocurre si se consideran errores sobre más de un qubit. Por ejemplo, un error de dos qubits de la forma  $Z_{(i-1)} Z_{(i+1)}$  produce sobre  $\vec{p}$  el mismo efecto que un error  $X_{(i)}$ , y por lo tanto estos errores no pueden ser distinguidos. En la Figura 5.7 se muestra la función de Wigner luego de que ocurran errores  $Z$  y  $X$  sobre el qubit número 2.



**Figura 5.6:** La representación de estados en el código perfecto, en la definición de la función de Wigner adaptada al estado-grafo correspondiente a un anillo de 5 qubits. a) El estado-grafo, que es el estado  $|-\rangle_L$ , está asociado al rayo horizontal; b) La función de Wigner del estado de la base computacional codificada  $|0\rangle_L$  es una combinación de las líneas asociadas a los estados  $|-\rangle_L$  y  $|+\rangle_L$  y líneas horizontales oscilantes correspondientes a la interferencia entre ellos. Cualquier estado codificado tiene una función de Wigner de esta misma forma.



**Figura 5.7:** La representación de estados erróneos en el código perfecto, en la definición de la función de Wigner adaptada al estado-grafo correspondiente a un anillo de 5 qubits. Se muestra la función de Wigner del estado codificado  $|0\rangle_L$  luego de sufrir errores tipo  $Z$  (Figura a) y tipo  $X$  (Figura b) en el segundo qubit. Por comparación con la Figura 5.6, puede verse que estos estados son ortogonales a cualquier estado codificado.



## Capítulo 6

# El efecto de la decoherencia en estados cluster

Según lo discutido en la sección 2.5, los estados-grafo constituyen el punto de partida para un cómputo cuántico en el modelo basado en la medición. En este capítulo se estudiará el efecto de algunos modelos simples de decoherencia sobre un sistema de  $n$  qubits preparado en un estado-grafo. En particular, se estudiará el tiempo de pérdida del entrelazamiento entre qubits vecinos, siguiendo uno de los procedimientos presentados en [42], aplicándolo a modelos un poco más generales de decoherencia y prestando especial atención al caso en que el estado-grafo es un estado cluster con  $D$  dimensiones. Se observará, en concordancia con los resultados de [42], que la persistencia del entrelazamiento para los modelos estudiados depende fuertemente de la cantidad de vecinos de cada qubit, y no necesariamente del tamaño total del grafo.

En primer lugar, se introducirá el modelo de decoherencia a utilizar, que consiste en la aplicación, con distintas probabilidades, de un conjunto de operadores de Pauli generalizados sobre los qubits en el sistema. Se mostrará el efecto de esta clase de ruido sobre un estado general del sistema de qubits, que luego se especializará para el caso en que el estado inicial es un estado-grafo. Se presentará un criterio para decidir si un par de qubits vecinos en el grafo continúa entrelazado, a través del estudio de la matriz densidad del par de qubits luego de efectuar una medición en la base computacional sobre todos los otros qubits en el sistema. Se calcularán los tiempos de pérdida del entrelazamiento entre vecinos en estados cluster de dimensión  $D$ , para distintos modelos sencillos de decoherencia involucrando ruido individual sobre los qubits o ruido correlacionado sobre grupos de vecinos. Por último, se estudiará la representación en el espacio de fases de la evolución de este

sistema, utilizando la función de Wigner con coordenadas en  $GF(d)$ .

## 6.1. El modelo de decoherencia

El proceso de decoherencia del sistema de qubits como consecuencia de las interacciones no controladas con el entorno se modelará a través de la acción de un superoperador  $\mathcal{L}$  que transforma la matriz densidad del sistema según la ecuación de Lindblad:

$$\frac{\partial \rho}{\partial t} = \mathcal{L}\rho = -i[H, \rho] + \sum_k \left\{ L_k \rho L_k^\dagger - \frac{1}{2} \{L_k^\dagger L_k, \rho\} \right\} \quad (6.1)$$

donde  $H$  es el hamiltoniano del sistema de qubits, y los operadores  $L_\mu$  surgen de la interacción con el entorno (una introducción a este tema se puede encontrar en el capítulo 3 de [17], o el 8 de [10]). La evolución de  $\rho(0)$  a  $\rho(t)$  está dada por un mapa completamente positivo y que preserva la traza de  $\rho$ , en la forma:

$$\rho(t) = e^{\mathcal{L}t} \rho(0) \quad (6.2)$$

En particular, se estudiará el efecto de superoperadores  $\mathcal{L}$  correspondientes a decoherencia pura, esto es,  $H = 0$ , y donde los operadores  $L_\mu$  son operadores de Pauli generalizados:

$$\mathcal{L}\rho = \sum_{\vec{a}, \vec{b}} l_{\vec{a}, \vec{b}} \left\{ \sigma_{\vec{a}, \vec{b}} \rho \sigma_{\vec{a}, \vec{b}}^\dagger - \frac{1}{2} \{ \sigma_{\vec{a}, \vec{b}}^\dagger \sigma_{\vec{a}, \vec{b}}, \rho \} \right\} \quad (6.3)$$

con  $\vec{a}, \vec{b}$  todas las  $n$ -uplas binarias, y  $l_{\vec{a}, \vec{b}} \geq 0$ . Dado que los operadores de Pauli son unitarios, la acción de  $\mathcal{L}$  puede reescribirse en la forma:

$$\mathcal{L}\rho = \sum_{\vec{a}, \vec{b}} l_{\vec{a}, \vec{b}} \left\{ \sigma_{\vec{a}, \vec{b}} \rho \sigma_{\vec{a}, \vec{b}}^\dagger - \rho \right\} \quad (6.4)$$

lo cual a su vez puede reagruparse, redefiniendo los coeficientes, para obtener:

$$\mathcal{L}\rho = \sum_{\vec{a}, \vec{b}} c_{\vec{a}, \vec{b}} \sigma_{\vec{a}, \vec{b}} \rho \sigma_{\vec{a}, \vec{b}}^\dagger \quad (6.5)$$

con

$$\sum_{\vec{a}, \vec{b}} c_{\vec{a}, \vec{b}} = 0 \quad \text{y} \quad c_{\vec{a}, \vec{b}} \geq 0 \quad \forall c_{\vec{a}, \vec{b}} \neq c_{\vec{0}, \vec{0}} \quad (6.6)$$

En este caso, el ruido sobre el sistema se modela a través de la aplicación, con ciertas probabilidades dadas por los coeficientes  $c_{\vec{a}, \vec{b}}$ , de los operadores de

Pauli generalizados  $\sigma_{\vec{a},\vec{b}}$ , de modo que la evolución del sistema corresponde a la suma de todas las posibles evoluciones unitarias de esta forma, pesadas por sus respectivas probabilidades.

Es claro que este tipo de evolución preserva el estado totalmente mixto, proporcional a la identidad, ya que éste no se modifica al aplicarle operadores de Pauli; este estado es autooperador de  $\mathcal{L}$  con autovalor 0. Los demás autooperadores de  $\mathcal{L}$  son los otros operadores de Pauli generalizados, ya que resulta:

$$\mathcal{L} \sigma_{\vec{c},\vec{d}} = \sum_{\vec{a},\vec{b}} c_{\vec{a},\vec{b}} \sigma_{\vec{a},\vec{b}} \sigma_{\vec{c},\vec{d}} \sigma_{\vec{a},\vec{b}}^\dagger = \sum_{\vec{a},\vec{b}} c_{\vec{a},\vec{b}} (-1)^{\vec{a}\cdot\vec{d}+\vec{b}\cdot\vec{c}} \sigma_{\vec{c},\vec{d}} = \lambda_{\vec{c},\vec{d}} \sigma_{\vec{c},\vec{d}} \quad (6.7)$$

Esto es, los operadores de Pauli  $\sigma_{\vec{c},\vec{d}}$  son autooperadores de  $\mathcal{L}$  con autovalores:

$$\lambda_{\vec{c},\vec{d}} = \sum_{\vec{a},\vec{b}} c_{\vec{a},\vec{b}} (-1)^{\vec{a}\cdot\vec{d}+\vec{b}\cdot\vec{c}} \quad (6.8)$$

A causa de que los coeficientes  $c_{\vec{a},\vec{b}}$  positivos aparecen en la suma con distintos signos, mientras que el  $c_{\vec{0},\vec{0}}$  mantiene su signo negativo, los autovalores  $\lambda_{\vec{c},\vec{d}}$  son menores o iguales que cero. En el caso más general, sólo es nulo el autovalor correspondiente a la identidad,  $\lambda_{\vec{0},\vec{0}}$ .

El estado a tiempo  $t$  puede calcularse descomponiendo el estado inicial en términos de las matrices de Pauli, en la forma:

$$\rho(0) = \sum_{\vec{a},\vec{b}} \rho_{\vec{a},\vec{b}} \sigma_{\vec{a},\vec{b}} \quad (6.9)$$

con  $\rho_{\vec{a},\vec{b}} \in \mathbb{R}$ , obteniendo para el estado en un tiempo posterior:

$$\rho(t) = e^{\mathcal{L}t} \sum_{\vec{a},\vec{b}} \rho_{\vec{a},\vec{b}} \sigma_{\vec{a},\vec{b}} = \sum_{\vec{a},\vec{b}} \rho_{\vec{a},\vec{b}} e^{t\lambda_{\vec{a},\vec{b}}} \sigma_{\vec{a},\vec{b}} \quad (6.10)$$

y por lo tanto, en general el estado  $\rho$  bajo la acción de  $\mathcal{L}$  evoluciona tendiendo al estado totalmente mixto.

## 6.2. Pérdida del entrelazamiento entre vecinos en un estado-grafo

Como ya se ha dicho y redicho, el entrelazamiento presente en un estado-grafo proporciona el recurso fundamental para la computación cuántica en el modelo basado en la medición. En este capítulo se estudiará la pérdida de entrelazamiento entre qubits vecinos como consecuencia del proceso de

decoherencia descrito en la sección anterior. Sin embargo, no es claro cómo determinar la persistencia del entrelazamiento entre vecinos cuando éstos a su vez forman parte de un sistema más grande cuyo estado es entrelazado. De hecho, si en el grafo asociado no hay qubits aislados, el estado-grafo no es separable respecto de ninguna partición, y en ese sentido todos los qubits están entrelazados entre sí.

Un modo de distinguir el entrelazamiento entre primeros vecinos en el grafo surge de la siguiente propiedad: si se tiene un estado-grafo y se mide uno de los qubits en la base computacional, el estado final del resto de los qubits es el asociado al grafo que resulta de borrar en el grafo original el vértice medido (a menos de la aplicación de compuertas  $Z$  en los vecinos del vértice borrado). Por lo tanto, si en un estado-grafo se borran, realizando mediciones en la base computacional, todos los vértices menos dos el estado final de los dos qubits restantes será el estado-grafo de dos vértices unidos si los dos qubits son vecinos, y será separable si no lo son (esto no ocurre si los otros qubits se miden en bases arbitrarias). Utilizando esta propiedad, y siguiendo un procedimiento presentado en [42], la permanencia del entrelazamiento entre primeros vecinos se analizará por medio de la matriz densidad  $\rho_{1,2}$  de un par de vecinos luego de haber realizado mediciones en la base computacional sobre todos los otros qubits en el sistema.

De acuerdo al criterio de la transposición parcial, el par de qubits estudiado se encuentra entrelazado si y sólo si la matriz  $(\rho_{1,2})^{tp}$ , que se obtiene transponiendo  $\rho_{1,2}$  respecto de uno solo de los subsistemas, tiene algún autovalor negativo [43].

Dado un cierto estado-grafo inicial  $|G\rangle$ , su matriz densidad puede escribirse en la forma (2.22):

$$\rho(0) = |G\rangle\langle G| = \frac{1}{d} \sum_{\vec{a}} \sigma_{\vec{a}, \Gamma \vec{a}} \quad (6.11)$$

donde  $\Gamma$  es la matriz de vecindad entre qubits. Por lo tanto, bajo la acción de la decoherencia de acuerdo al modelo descrito en la sección pasada, el estado en un tiempo posterior  $t$  está dado por:

$$\rho(t) = \frac{1}{d} \sum_{\vec{a}} \sigma_{\vec{a}, \Gamma \vec{a}} e^{t\lambda_{\vec{a}, \Gamma \vec{a}}} \quad (6.12)$$

Si a un tiempo  $t$  se miden en la base computacional todos los qubits excepto el par  $\{1, 2\}$ , obteniendo resultados  $\{m_3, \dots, m_n\}$ , el estado final

del par de qubits estudiado es:

$$\begin{aligned}\rho_{1,2}(t) &\sim \langle m_3, \dots, m_n | \rho(t) | m_3, \dots, m_n \rangle = \\ &= \frac{1}{d} \sum_{\vec{a}} \langle m_3, \dots, m_n | \sigma_{\vec{a}, \Gamma \vec{a}} | m_3, \dots, m_n \rangle e^{t\lambda_{\vec{a}, \Gamma \vec{a}}} \quad (6.13)\end{aligned}$$

donde  $\sim$  indica una igualdad a menos de la normalización del estado. En esta expresión, los elementos de matriz de los operadores de Pauli que actúan sobre los qubits medidos son de la forma:

$$\langle m_3, \dots, m_n | \prod_{j=3}^n X_{(j)}^{a_j} Z_{(j)}^{b_j} e^{i\frac{\pi}{2} a_j b_j} | m_3, \dots, m_n \rangle \quad \text{con } \vec{b} = \Gamma \vec{a} \quad (6.14)$$

Estos elementos de matriz sólo son no nulos si  $a_j = 0 \forall j = 3, \dots, n$ , y en ese caso se obtiene:

$$\langle m_3, \dots, m_n | \prod_{j=3}^n Z_{(j)}^{b_j} | m_3, \dots, m_n \rangle = \prod_{j=3}^n (-1)^{m_j b_j} \quad \text{con } \vec{b} = \Gamma \vec{a} \quad (6.15)$$

Por lo tanto, para el estado final del par de qubits  $\{1, 2\}$  se tiene:

$$\rho_{1,2}(t) = \frac{1}{4} \sum_{a_1, a_2} (X^{a_1} Z^{b_1})_{(1)} (X^{a_2} Z^{b_2})_{(2)} e^{i\frac{\pi}{2}(a_1 b_1 + a_2 b_2)} (-1)^{\vec{m} \cdot \vec{b}} e^{t\lambda_{\vec{a}, \vec{b}}} \quad (6.16)$$

con  $\vec{a} = (a_1, a_2, 0, \dots, 0)$ ,  $\vec{b} = \Gamma \vec{a}$ ,  $\vec{m} = (0, 0, m_3, \dots, m_n)$ . Desarrollando la suma sobre  $a_1, a_2$  resulta:

$$\begin{aligned}\rho_{1,2}(t) &= \frac{1}{4} \left\{ I + X_{(1)} Z_{(2)}^{\Gamma_{1,2}} (-1)^{\sum_j m_j \Gamma_{j,1}} e^{t\lambda(1,0)} + \right. \\ &\quad + Z_{(1)}^{\Gamma_{1,2}} X_{(2)} (-1)^{\sum_j m_j \Gamma_{j,2}} e^{t\lambda(0,1)} - \\ &\quad \left. - (X Z^{\Gamma_{1,2}})_{(1)} (X Z^{\Gamma_{1,2}})_{(2)} (-1)^{\sum_j m_j (\Gamma_{j,1} + \Gamma_{j,2})} e^{t\lambda(1,1)} \right\} \quad (6.17)\end{aligned}$$

donde se usa la notación  $\lambda(a_1, a_2)$  para indicar el autovalor  $\lambda_{\vec{a}, \vec{b}}$  correspondiente a  $\vec{a} = (a_1, a_2, 0, \dots, 0)$ ,  $\vec{b} = \Gamma \vec{a}$ . En el caso en que los qubits  $\{1, 2\}$  no son vecinos ( $\Gamma_{1,2} = 0$ ), la matriz densidad  $\rho_{1,2}$  luego de la medición es diagonal en la base de autoestados de  $X_{(1)}$  y  $X_{(2)}$ , y el par nunca queda entrelazado. En el caso en que los qubits son vecinos, la matriz densidad está dada por:

$$\begin{aligned}\rho_{1,2}(t) &= \frac{1}{4} \left\{ I + X_{(1)} Z_{(2)} (-1)^{\sum_j m_j \Gamma_{j,1}} e^{t\lambda(1,0)} + \right. \\ &\quad + Z_{(1)} X_{(2)} (-1)^{\sum_j m_j \Gamma_{j,2}} e^{t\lambda(0,1)} - \\ &\quad \left. - (X Z)_{(1)} (X Z)_{(2)} (-1)^{\sum_j m_j (\Gamma_{j,1} + \Gamma_{j,2})} e^{t\lambda(1,1)} \right\} \quad (6.18)\end{aligned}$$

O sea, en el caso en que los qubits sobre los que no se mide son vecinos la matriz densidad de este par luego de la medición es diagonal en una base de autoestados comunes de los operadores  $X_{(1)}Z_{(2)}$  y  $Z_{(1)}X_{(2)}$  (que puede obtenerse de la base de Bell aplicando una compuerta  $H$  sobre cualquiera de los dos qubits). Los autovalores de la matriz densidad  $\rho_{1,2}$  son independientes de los resultados obtenidos en las mediciones de los otros qubits, y resultan siempre no negativos e iguales a:

$$\begin{cases} \alpha_1 &= (1/4)(1 + e^{t\lambda(1,0)} + e^{t\lambda(0,1)} + e^{t\lambda(1,1)}) \\ \alpha_2 &= (1/4)(1 - e^{t\lambda(1,0)} - e^{t\lambda(0,1)} + e^{t\lambda(1,1)}) \\ \alpha_3 &= (1/4)(1 + e^{t\lambda(1,0)} - e^{t\lambda(0,1)} - e^{t\lambda(1,1)}) \\ \alpha_4 &= (1/4)(1 - e^{t\lambda(1,0)} + e^{t\lambda(0,1)} - e^{t\lambda(1,1)}) \end{cases} \quad (6.19)$$

Al trasponer la matriz  $\rho_{1,2}$  respecto de uno de los dos qubits, se obtiene una matriz cuyos autovalores están dados por:

$$\begin{cases} \alpha'_1 &= (1/4)(1 + e^{t\lambda(1,0)} + e^{t\lambda(0,1)} - e^{t\lambda(1,1)}) \\ \alpha'_2 &= (1/4)(1 - e^{t\lambda(1,0)} - e^{t\lambda(0,1)} - e^{t\lambda(1,1)}) \\ \alpha'_3 &= (1/4)(1 + e^{t\lambda(1,0)} - e^{t\lambda(0,1)} + e^{t\lambda(1,1)}) \\ \alpha'_4 &= (1/4)(1 - e^{t\lambda(1,0)} + e^{t\lambda(0,1)} + e^{t\lambda(1,1)}) \end{cases} \quad (6.20)$$

De acuerdo al criterio de la transposición parcial, entonces, el estado de los dos qubits es entrelazado si y sólo si el menor autovalor,  $\alpha'_2$ , es negativo, o sea si  $1 < e^{t\lambda(1,0)} + e^{t\lambda(0,1)} + e^{t\lambda(1,1)}$ . Es claro que para tiempos cortos el estado resulta entrelazado y para tiempos largos, en general, el entrelazamiento desaparece. El tiempo crítico  $t_c$  de pérdida del entrelazamiento, dado por la ecuación:

$$e^{t_c\lambda(1,0)} + e^{t_c\lambda(0,1)} + e^{t_c\lambda(1,1)} = 1 \quad (6.21)$$

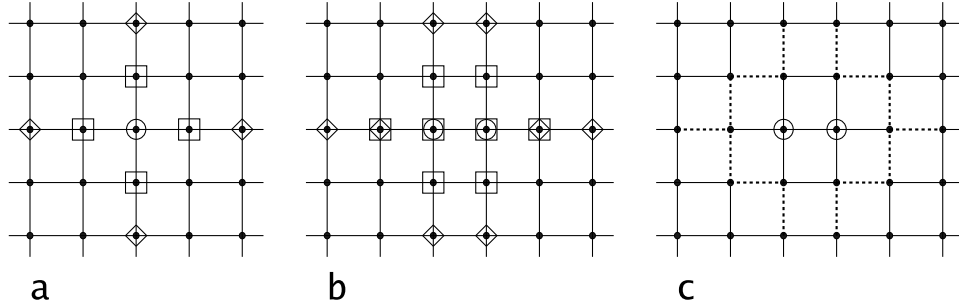
depende de la forma del estado-grafo inicial y de los pesos de los distintos operadores de Pauli en el superoperador  $\mathcal{L}$ .

### 6.3. El tiempo de pérdida de entrelazamiento en algunos casos particulares

A lo largo de esta sección se hallarán los tiempos críticos en que desaparece el entrelazamiento entre los qubits del par estudiado, para distintos pesos de los operadores de Pauli en  $\mathcal{L}$  y distintas geometrías del grafo, especialmente para el caso de estados cluster. Según sea el modelo de decoherencia utilizado, el tiempo crítico puede depender del grado de cada vértice (esto es, el número de vecinos que tiene), de la cantidad de vecinos comunes entre los qubits en el par, u otras propiedades del grafo.

En adelante se llamará  $N_i$  al conjunto de qubits vecinos del vértice  $i$ -ésimo,  $\{i\}$  al conjunto cuyo único elemento es el vértice  $i$ -ésimo, y  $\tilde{N}_i$  al conjunto de vértices  $j$  tales que  $\sum_k \Gamma_{i,k} \Gamma_{j,k} = |N_k \cap N_j| = 1 \pmod{2}$ , o sea, que tienen un número impar de vecinos comunes con el vértice  $i$ , donde se usa  $|A|$  para indicar la cantidad de elementos en el conjunto  $A$ . La unión, intersección y resta de conjuntos se notarán en la forma convencional  $A \cup B$ ,  $A \cap B$ , y  $A - B$  respectivamente, y se usará  $A \oplus B = (A \cup B) - (A \cap B)$ . Dados dos vértices  $i, j$ , se indicará por  $\tilde{N}_{i,j}$  al conjunto de pares de vecinos  $\{k, l\}$  tales que  $k, l \notin \{i, j\}$  y  $\Gamma_{i,k} + \Gamma_{j,k} + \Gamma_{i,l} + \Gamma_{j,l} = 1 \pmod{2}$ , o sea, tales que uno de los vértices  $j, k$  es vecino de  $i$  o de  $j$  y el otro es vecino de los dos o de ninguno (la necesidad de introducir semejantes conjuntos se verá a lo largo de la sección).

En un estado cluster en dimensión  $D$  se tiene, para cualquier vértice  $i$ ,  $|N_i| = |\tilde{N}_i| = 2D$ , y dos vértices vecinos no tienen vecinos comunes. El caso de un cluster de dos dimensiones se muestra en la Figura 6.1.



**Figura 6.1:** Grafo asociado a un cluster de dos dimensiones. a) Se indica con un círculo un dado qubit ( $\{i\}$ ), con un cuadrado sus vecinos ( $N_i$ ) y con un rombo los qubits que comparten con  $i$  un número impar de vecinos ( $\tilde{N}_i$ ). b) Para un par de vecinos  $i, j$  indicados con círculos, se señalan con cuadrados los vértices en  $N_i \cup N_j$ , y con un rombo los vértices en  $\tilde{N}_i \cup \tilde{N}_j$ . c) Para un par de vecinos  $i, j$  marcados con círculos, se indican con líneas punteadas los pares de qubits vecinos en  $\tilde{N}_{i,j}$ , tales que uno de los qubits es vecino de  $i$  o de  $j$  y el otro de ninguno de los dos ( $i, j$  no tienen vecinos comunes).

### 6.3.1. Ruido individual sobre cada qubit

El caso en que el ambiente afecta a cada qubit por separado y a todos por igual fue estudiado en [42], con resultados iguales a los obtenidos en esta sección. Este caso corresponde a una evolución dada por  $\mathcal{L} = \mathcal{L}_1 + \dots + \mathcal{L}_n$ ,

donde cada uno de los  $\mathcal{L}_j$  actúa en la misma forma pero solamente sobre el qubit  $j$ -ésimo, según:

$$\mathcal{L}_j \rho = \sum_{k=0}^3 c_k (\sigma_k)_{(j)} \rho (\sigma_k)_{(j)} \quad (6.22)$$

con  $c_k \geq 0$  para  $k = 1, 2, 3$  y  $\sum_k c_k = 0$ . Utilizando la ecuación (6.8) pueden calcularse los autovalores  $\lambda(a_1, a_2)$ , que están dados por:

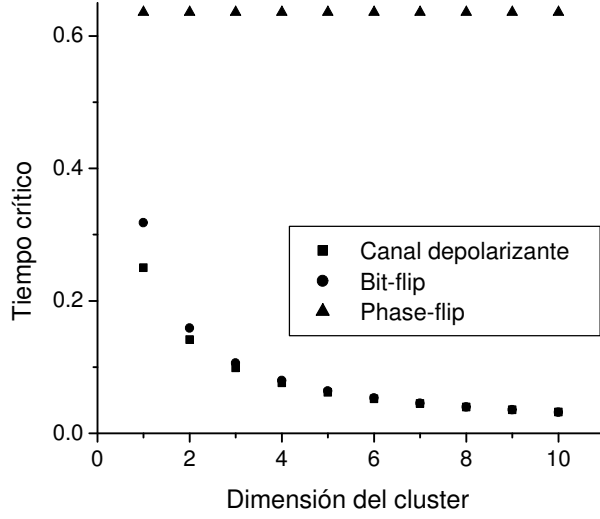
$$\begin{aligned} \lambda(1, 0) &= -2[(c_1 + c_2)|N_1| + (c_2 + c_3)] \\ \lambda(0, 1) &= -2[(c_1 + c_2)|N_2| + (c_2 + c_3)] \\ \lambda(1, 1) &= -2[(c_1 + c_2)|N_1 \oplus N_2| - 2(c_2 - c_3)] \end{aligned}$$

A causa del entrelazamiento entre cada qubit y sus vecinos, el ruido en los vecinos afecta el estado final del par de qubits, y los autovalores son, en general, más negativos cuanto mayor sea el número de vecinos de cada qubit en el par. Como se hace notar en [42], el tiempo de pérdida de entrelazamiento depende de la cantidad de vecinos de los vértices estudiados pero no necesariamente del tamaño del grafo; si la cantidad de qubits en el grafo aumenta sin alterar la cantidad de vecinos (como ocurre, por ejemplo, al agrandar una red cuadrada) el tiempo crítico no varía; algo similar ocurre en cualquier caso en que los operadores en  $\mathcal{L}$  actúan sobre un número finito de qubits independiente del tamaño del grafo.

Para la misma intensidad de ruido, en la Figura 6.2 se muestra el valor de tiempo crítico para estados cluster ( $|N_i| = 2D$ ,  $|N_1 \oplus N_2| = 4D$ ) en función de la dimensionalidad  $D$  del cluster, para ruido correspondiente a los canales depolarizante ( $c_1 = c_2 = c_3 = c/3$ ), “bit-flip” ( $c_1 = c$ ,  $c_2 = c_3 = 0$ ) y desfasante o “phase-flip” ( $c_3 = c$ ,  $c_1 = c_2 = 0$ ).

El canal desfasante tiene la propiedad llamativa de que el tiempo crítico es totalmente independiente de la geometría del grafo. Esto puede entenderse teniendo en cuenta la forma en que actúan los operadores de Pauli sobre un estado-grafo. Dado que el estado es estabilizado por los operadores consistentes en la aplicación simultánea de  $X$  sobre un qubit y  $Z$  sobre todos sus vecinos, la acción del operador  $X_{(j)}$  es igual a la de  $\prod_k Z_{(k)}^{\Gamma_{j,k}}$ . En consecuencia, cualquier ruido de Pauli puede ser descrito usando únicamente productos de operadores  $Z$ , aunque sobre diferentes qubits. La aplicación de un canal individual tipo bit-flip sobre un qubit es igual a un ruido que aplica  $Z$  en forma correlacionada sobre todos los vecinos del qubit, y por esto el efecto del canal depende de la cantidad de vecinos. Algo similar ocurre con el ruido que aplica el operador  $Y$  sobre un qubit, y en cambio el operador  $Z$  actúa en forma independiente del número de vecinos.





**Figura 6.2:** Tiempos críticos de desaparición del entrelazamiento entre pares de vecinos para un modelo de ruido con canales de Pauli independientes e iguales en cada qubit, actuando sobre qubits pertenecientes a un estado cluster. Se muestran los tiempos críticos en función de la dimensión del cluster para los canales depolarizante, desfasante y bit-flip.

### 6.3.2. Ruido correlacionado entre un qubit y todos sus vecinos

El siguiente modelo de ruido contempla la posibilidad de que un cierto canal ruidoso actúe en forma correlacionada sobre cada qubit y sus vecinos, en la forma:  $\mathcal{L} = \mathcal{L}_1 + \dots + \mathcal{L}_n$ , donde  $\mathcal{L}_i$  actúa en la misma forma sobre el qubit  $i$ -ésimo y sobre sus vecinos, según:

$$\mathcal{L}_i \rho = \sum_{k=0}^3 c_k \left[ (\sigma_k)_{(i)} \prod_j (\sigma_k^{\Gamma_{i,j}})_{(j)} \right] \rho \left[ (\sigma_k)_{(i)} \prod_j (\sigma_k^{\Gamma_{i,j}})_{(j)} \right] \quad (6.23)$$

con  $c_k \geq 0$  para  $k = 1, 2, 3$  y  $\sum_k c_k = 0$ . Utilizando la ecuación (6.8) pueden calcularse los autovalores  $\lambda(a_1, a_2)$ :

$$\begin{aligned} \lambda(1, 0) &= -2[c_1|N_1 \oplus \tilde{N}_1| + c_2|\tilde{N}_1 \oplus \{1\}| + c_3(|N_1| + 1)] \\ \lambda(0, 1) &= -2[c_1|N_2 \oplus \tilde{N}_2| + c_2|\tilde{N}_2 \oplus \{2\}| + c_3(|N_2| + 1)] \\ \lambda(1, 1) &= -2[c_1|N_1 \oplus N_2 \oplus \tilde{N}_1 \oplus \tilde{N}_2| + c_2|\{1\} \oplus \{2\} \oplus \tilde{N}_1 \oplus \tilde{N}_2| + \\ &\quad + c_3(|N_1 \oplus N_2| - 2)] \end{aligned}$$

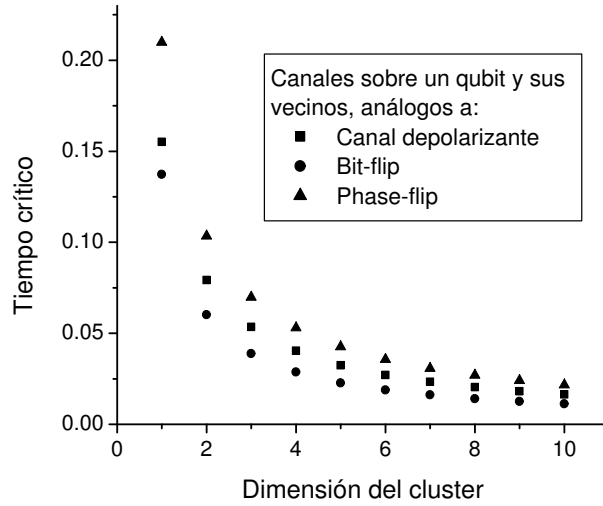
Para la geometría de un estado cluster en dimensión  $D$  se tiene que

$|N_i \oplus \tilde{N}_i| = 4D$ ,  $|\tilde{N}_i \oplus \{i\}| = 2D + 1$ . Además resulta  $|N_i \oplus N_j \oplus \tilde{N}_i \oplus \tilde{N}_j| = 8(D - 1) + 4$ ,  $|\{i\} \oplus \{j\} \oplus \tilde{N}_i \oplus \tilde{N}_j| = 4D + 2$  (ver Figura 6.1.b). Insertando estos datos en las expresiones de los autovalores se obtiene:

$$\lambda(1, 0) = \lambda(0, 1) = -2[(2c_1 + c_2 + c_3)2D + (c_2 + c_3)]$$

$$\lambda(1, 1) = -4[(2c_1 + c_2 + c_3)2D + (-2c_1 + c_2 - c_3)]$$

En la Figura 6.3 se muestra la dependencia del tiempo crítico para los análogos de los canales depolarizante ( $c_1 = c_2 = c_3 = c/3$ ), bit-flip ( $c_1 = c$ ,  $c_2 = c_3 = 0$ ) y phase-flip ( $c_3 = c$ ,  $c_1 = c_2 = 0$ ) en función de la dimensionalidad del cluster.



**Figura 6.3:** Tiempos críticos de desaparición del entrelazamiento entre pares de vecinos para un modelo de ruido con canales de Pauli correlacionados sobre cada qubit y todos sus vecinos. El estado inicial del sistema es un estado cluster. Se muestran los tiempos críticos en función de la dimensión del cluster para los canales análogos al depolarizante, desfasante y bit-flip.

### 6.3.3. Ruido correlacionado sobre pares de vecinos

Si el ruido actúa en forma correlacionada sobre pares de qubits vecinos, se tiene  $\mathcal{L} = \sum_{i,j} \mathcal{L}_{i,j}$  donde  $\mathcal{L}_{i,j}$  aplica operadores de Pauli iguales sobre dos qubits vecinos, en la forma:

$$\mathcal{L}_{i,j} \rho = \sum_{k=0}^3 c_k \left[ (\sigma_k)_{(i)} (\sigma_k)_{(j)} \right]^{\Gamma_{i,j}} \rho \left[ (\sigma_k)_{(i)} (\sigma_k)_{(j)} \right]^{\Gamma_{i,j}} \quad (6.24)$$

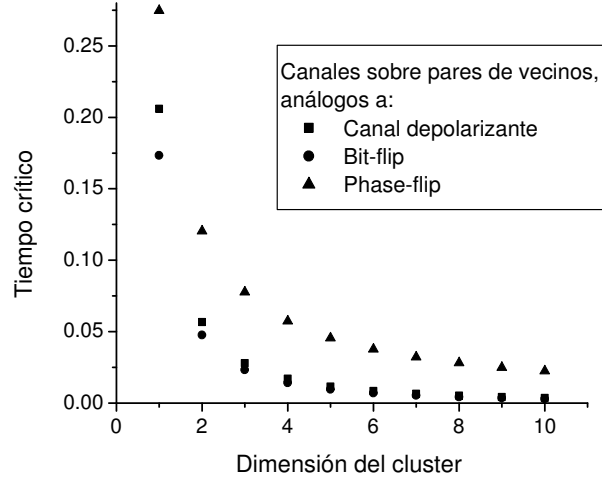
con  $c_k \geq 0$  para  $k = 1, 2, 3$  y  $\sum_k c_k = 0$ . Los autovalores  $\lambda(a_1, a_2)$  están dados por:

$$\begin{aligned}\lambda(1, 0) &= -2[(c_1 + c_3)|N_1| + (c_1 + c_2) \sum_{k \in N_1} |N_k - (\{1\} \cup N_1)|] \\ \lambda(0, 1) &= -2[(c_1 + c_3)|N_2| + (c_1 + c_2) \sum_{k \in N_2} |N_k - (\{2\} \cup N_2)|] \\ \lambda(1, 1) &= -2[(c_1 + c_2)|\tilde{N}_{1,2}| + 2(c_1 - c_2)|N_1 \cap N_2| + (c_2 + c_3)(|N_1| + |N_2| - 2)]\end{aligned}$$

Para un estado cluster de dimensión  $D$ , resulta  $|\tilde{N}_{i,j}| = |N_i| + |N_j| - 2 = 4D - 2$  (ver Figura 6.1.c), y como además los vértices vecinos no tienen vecinos comunes, para cualquier vértice  $k$  vecino de  $i$  es  $|N_k - (\{i\} \cup N_i)| = |N_k - \{i\}| = 2D - 1$ . Los autovalores, entonces, valen:

$$\begin{aligned}\lambda(1, 0) &= \lambda(0, 1) = -4D[(c_1 + c_2)(2D - 1) + (c_1 + c_3)] \\ \lambda(1, 1) &= -4(2D - 1)[c_1 + c_2 + 2c_3]\end{aligned}$$

En la Figura 6.4 se muestra la dependencia del tiempo crítico para los análogos de los canales depolarizante ( $c_1 = c_2 = c_3 = c/3$ ), bit-flip ( $c_1 = c, c_2 = c_3 = 0$ ) y phase-flip ( $c_3 = c, c_1 = c_2 = 0$ ) en función de la dimensionalidad del cluster.



**Figura 6.4:** Tiempos críticos de desaparición del entrelazamiento entre vecinos para un modelo de ruido con canales de Pauli correlacionados actuando sobre pares de qubits vecinos, pertenecientes a un estado cluster. Se muestran los tiempos críticos en función de la dimensión del cluster para los canales análogos al depolarizante, desfasante y bit-flip.

En los tres modelos de ruido, la forma en que varía el tiempo crítico al aumentar la dimensión del cluster puede entenderse como consecuencia de la variación en la probabilidad “efectiva” de la aplicación de ruido sobre los qubits estudiados. Dado que la acción de  $X$  o  $Y$  sobre un qubit es igual a la de un producto de  $Z$ s sobre los qubits vecinos, si la probabilidad de que un canal de ruido tipo  $X$  o  $Y$  actúe sobre un qubit es constante, la probabilidad de que el ruido tipo  $Z$  equivalente afecte a un qubit dado crece como el número de sus vecinos. Por esta razón, el tiempo crítico en el modelo de ruido individual sobre los qubits es independiente de la dimensión del cluster para el canal desfasante, y en cambio decrece aproximadamente como  $D^{-1}$  cuando el canal de ruido es depolarizante o bit-flip.

En forma similar pueden analizarse los dos modelos considerados de ruido correlacionado. En el primer caso, en que el ruido se aplica en forma correlacionada sobre un qubit y todos sus vecinos, el par  $\{1, 2\}$  es afectado por el ruido de tipo  $X$  o  $Y$  centrado en sus segundos vecinos. Sin embargo, la aplicación de ruido sobre qubits que compartan un número par de vecinos con los qubits  $\{1, 2\}$  no tiene efecto sobre ellos (ya que el ruido equivalente aplicaría dos veces la compuerta  $Z$ ). Por esto, los qubits en el par estudiado sólo son afectados por el ruido sobre qubits con los que comparten un número impar de vecinos. En un cluster, este número crece linealmente con la dimensión del cluster (al igual que el número de primeros vecinos), y por esto en este modelo todos los canales de ruido considerados tienen tiempos críticos que disminuyen aproximadamente como  $D^{-1}$ . Por último, en el modelo en que el ruido actúa en forma correlacionada sobre pares de qubits vecinos, nuevamente los qubits  $\{1, 2\}$  son afectados por sus segundos vecinos (excepto en el caso del canal desfasante), pero ahora sin la restricción sobre la paridad del número de vecinos comunes. En consecuencia, los tiempos críticos decaen aproximadamente como  $D^{-2}$  para los canales depolarizante y bit-flip, y como  $D^{-1}$  para el canal desfasante.

## 6.4. El efecto de la decoherencia en la función de Wigner

La evolución del estado-grafo bajo los efectos de la decoherencia puede observarse por medio de las funciones de Wigner discretas definidas en el capítulo 3. Con la elección usual de los operadores de traslación, en la forma  $T(\vec{q}, \vec{p}) = \sigma_{\vec{q}, \vec{p}}$ , haciendo uso de las expresiones (3.30) y (3.36) para obtener la función de Wigner en cada punto, y del desarrollo de la matriz densidad

para todo tiempo dado por (6.12), resulta:

$$W(\vec{q}, \vec{p}, t) = \frac{1}{d^2} \sum_{\vec{a}} (-1)^{\vec{a} \cdot (\vec{p} + \Gamma \vec{q})} f_{(\vec{a}, \Gamma \vec{a})} e^{t\lambda_{\vec{a}, \Gamma \vec{a}}} \quad (6.25)$$

Si se elige una grilla cuántica conveniente para la representación del estado-grafo inicial, es decir una tal que  $f_{(\vec{a}, \Gamma \vec{a})} = 1 \forall \vec{a}$  (los puntos de coordenadas  $(\vec{a}, \Gamma \vec{a})$  son los asociados al estabilizador del grafo), la expresión de la función de Wigner se simplifica aún más, en la forma:

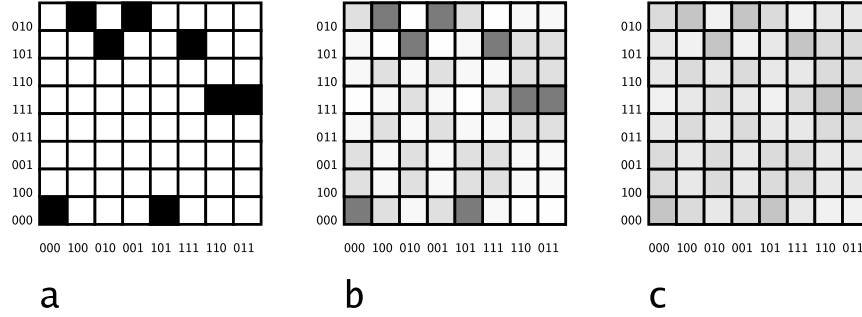
$$W(\vec{q}, \vec{p}, t) = \frac{1}{d^2} \sum_{\vec{a}} (-1)^{\vec{a} \cdot (\vec{p} + \Gamma \vec{q})} e^{t\lambda_{\vec{a}, \Gamma \vec{a}}} \quad (6.26)$$

En el instante inicial esa función corresponde al estado-grafo, y la sumatoria sólo es no nula en los puntos del espacio de fases asociados al estabilizador del estado. En el caso más general, en que todos los autovalores  $\lambda_{\vec{a}, \Gamma \vec{a}}$  son no nulos excepto el  $\lambda_{\vec{0}, \vec{0}}$ , la única contribución a la suma que no decae es la dada por el término  $\vec{a} = 0$ , que corresponde a una distribución uniforme (porque el estado tiende al totalmente mixto).

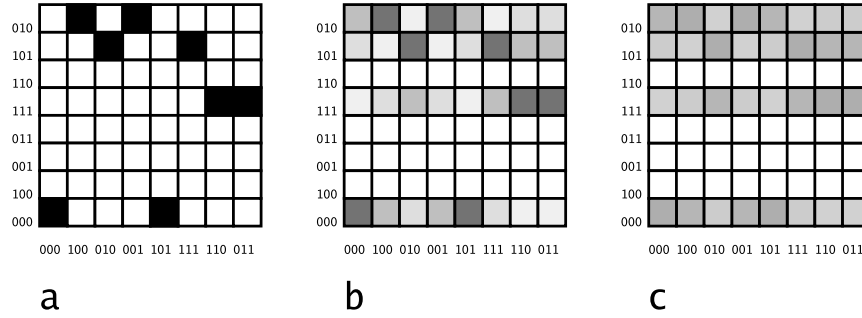
El efecto de un canal de ruido que aplica operadores de Pauli tiene una interpretación sencilla en términos de la función de Wigner del estado. Dado que los operadores de Pauli corresponden a traslaciones en el espacio de fases, el efecto del ruido es superponer las distintas funciones de Wigner obtenidas al trasladar la original, pesadas por las probabilidades asociadas a la aplicación de cada operador de traslación. En consecuencia, bajo la acción de canales desfasantes (o cualquier producto de operadores  $Z$ ) la función de Wigner es “borroneada” en la dirección vertical, mientras que los canales tipo bit-flip tienen un efecto similar en la dirección horizontal. La forma en que evoluciona el estado depende del modelo de ruido considerado y del estado-grafo inicial; en las Figuras 6.5 y 6.6 se muestra la representación en el espacio de fases de tres instantes en la evolución de un sistema de tres qubits cuyo estado inicial es el asociado a una cadena lineal y sobre los que actúan canales independientes de ruido desfasante y bit-flip, respectivamente.

Alternativamente, se puede representar el estado en el espacio de fases usando la función de Wigner “a medida” para el estado-grafo inicial, o sea, con las traslaciones horizontales identificadas con los operadores que estabilizan el estado-grafo. En este caso, el desarrollo del estado inicial en términos de sus estabilizadores (6.11) puede reescribirse en la forma:

$$\rho(0) = \frac{1}{d} \sum_{\vec{a}} \sigma_{\vec{a}, \Gamma \vec{a}} = \frac{1}{d} \sum_{\vec{a}} T'(\vec{a}, \vec{0}) \quad (6.27)$$



**Figura 6.5:** Función de Wigner para un sistema de tres qubits, inicialmente en el estado-grafo asociado a un cluster lineal, que sufren decoherencia en la forma de canales desfasantes independientes. Para aumentar el contraste y dado que la función de Wigner es positiva en la grilla cuántica elegida, el blanco corresponde al valor cero y el negro a  $1/8$ . Se representa el estado en los instantes: a)  $t = 0$ ; b)  $t = 0,25$ ; c)  $t = 0,75$  (el tiempo crítico de pérdida del entrelazamiento entre vecinos es  $t_c \sim 0,44$ ). El ruido desfasante produce traslaciones en la dirección vertical. La función de Wigner del sistema tiende al estado totalmente mixto (distribución uniforme).



**Figura 6.6:** Función de Wigner de un sistema de tres qubits, cuyo estado inicial es el asociado a un cluster lineal, bajo los efectos de canales bit-flip sobre cada qubit. Se muestra la función de Wigner para los instantes: a)  $t = 0$ ; b)  $t = 0,25$ ; c)  $t = 0,75$  (el tiempo de pérdida del entrelazamiento entre primeros vecinos es  $t_c \sim 0,31$ ). El blanco corresponde al valor cero y el negro a  $1/8$ . El ruido, asociado a operadores de traslación horizontales, borrona la función de Wigner en esta dirección. Esta evolución no tiende al estado totalmente mixto, ya que el estado inicial es autoestado (con autovalor 1) del operador  $X_{(1)}X_{(3)}$ , que conmuta con los operadores de ruido. De hecho, el estado tiende a una distribución uniforme sobre las líneas horizontales asociadas al espacio de estados estabilizados por  $X_{(1)}X_{(3)}$ , cuyos puntos tienen coordenadas  $\vec{p}$  tales que  $p_1 + p_3 = 0 \pmod{2}$ .

y el estado a cualquier tiempo posterior está dado por:

$$\rho(t) = \frac{1}{d} \sum_{\vec{a}} T'(\vec{a}, \vec{0}) e^{t\lambda_{\vec{a}, \Gamma \vec{a}}} \quad (6.28)$$

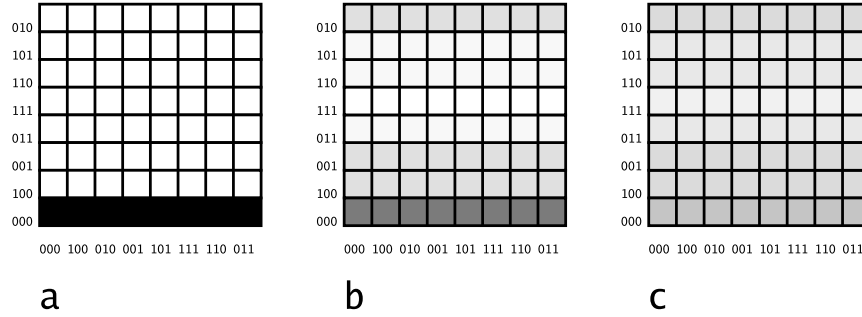
donde los autovalores  $\lambda$  son los mismos de antes, ya que esto no es más que la ecuación (6.12) pero teniendo en cuenta que las traslaciones horizontales son  $T'(\vec{a}, \vec{0}) = \sigma_{\vec{a}, \Gamma \vec{a}}$ .

La función de Wigner se obtiene de la manera usual, pero recordando la redefinición de las traslaciones (y el consiguiente cambio en los proyectores asociados a las líneas, y en los operadores de punto). Para el estado a tiempo  $t$ , con esta nueva definición de la función de Wigner se tiene:

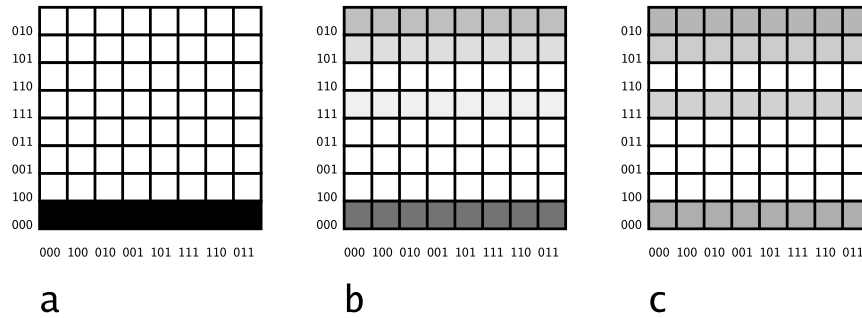
$$W'(\vec{q}, \vec{p}, t) = \frac{1}{d^2} \sum_{\vec{a}} (-1)^{\vec{a} \cdot \vec{p}} e^{t\lambda_{\vec{a}, \Gamma \vec{a}}} \quad (6.29)$$

Esta expresión corresponde a una función de Wigner que no depende de la coordenada horizontal  $\vec{q}$ , lo cual se debe a que para cualquier valor de  $t$  el estado es una superposición estadística de autoestados de los estabilizadores del grafo (con distintos autovalores). Esta invariancia de la función de Wigner frente a la aplicación de traslaciones de la forma  $\sigma_{\vec{a}, \Gamma \vec{a}}$  ya estaba presente en la definición anterior, pero aquí se hace más evidente porque estos operadores ahora corresponden a traslaciones horizontales (las traslaciones oblicuas en el espacio de fases con coordenadas en  $GF(d)$  no son tan fáciles de visualizar).

Para esta definición de las traslaciones, el estado inicial es el rayo horizontal, y el ruido de un canal desfasante corresponde a traslaciones verticales en el espacio de fases (Figura 6.7) mientras que el ruido bit-flip ahora aplica traslaciones oblicuas (Figura 6.8).



**Figura 6.7:** Función de Wigner para un sistema de tres qubits cuyo estado inicial es el estado-grafo asociado a un cluster lineal y que sufren decoherencia en la forma de canales desfasantes independientes. Las traslaciones horizontales se asocian a los estabilizadores del grafo. Para aumentar el contraste y dado que la función de Wigner es positiva en todo instante, el blanco corresponde al valor cero y el negro a  $1/8$ . Las figuras corresponden a los instantes: a)  $t = 0$ ; b)  $t = 0, 25$ ; c)  $t = 0, 75$  (el tiempo crítico es  $t_c \sim 0, 44$ ). El ruido equivale a la aplicación de traslaciones en la dirección vertical. La función de Wigner del sistema tiende al estado totalmente mixto (distribución uniforme).



**Figura 6.8:** Función de Wigner de un sistema de tres qubits que se preparan en el estado asociado a un cluster lineal y evolucionan bajo los efectos de canales bit-flip independientes e iguales sobre cada qubit. El blanco corresponde al valor cero y el negro a  $1/8$ . Las traslaciones horizontales se asocian a los estabilizadores del grafo. Se muestra la función de Wigner para los instantes: a)  $t = 0$ ; b)  $t = 0, 25$ ; c)  $t = 0, 75$  (el tiempo de pérdida del entrelazamiento entre primeros vecinos es  $t_c \sim 0, 31$ ). El ruido produce traslaciones oblicuas en el espacio de fases, que borrarían la función de Wigner. Esta evolución no tiende al estado totalmente mixto, ya que el estado inicial es autoestado (con autovalor 1) del operador  $X_{(1)}X_{(3)}$ , que conmuta con los operadores de ruido. De hecho, el estado tiende a una distribución uniforme sobre las líneas horizontales asociadas al espacio de estados estabilizados por  $S_1S_3 = X_{(1)}X_{(3)}$ , cuyos puntos tienen coordenadas  $\vec{p}$  tales que  $p_1 + p_3 = 0 \pmod{2}$ .



# Capítulo 7

## Conclusiones

A lo largo de esta tesis se han analizado varios problemas relacionados con la representación en el espacio de fases del estado de un sistema de qubits y su evolución, dedicando especial atención a los estados estabilizadores y estados-grafo, por su importancia particular para la computación cuántica.

La utilización de cuerpos de Galois en la construcción del espacio de fases permite dotar a la función de Wigner discreta de algunas propiedades notables, como el hecho de que las distintas estriaciones correspondan a bases mutuamente conjugadas de estados estabilizadores. En contrapartida, la definición de la función de Wigner es bastante más complicada que al usar aritmética módulo  $d$ , o  $2d$ . No existen hasta el momento criterios que permitan seleccionar una única función de Wigner, sino que existe una libertad enorme en la elección de la definición a utilizar en cada caso (y la cantidad de opciones aumenta tremendamente a medida que se agregan qubits al sistema); sin embargo esta multiplicidad de elecciones posibles en algunos casos es una ventaja, ya que permite adaptar la definición de Wigner al problema particular que se quiera estudiar (con el inconveniente de que la comparación de resultados obtenidos con funciones de Wigner diferentes no es sencilla).

La representación de sistemas de qubits por medio de la función de Wigner discreta se analizó para una variedad de problemas: se demostró que el conjunto de estados con función de Wigner totalmente positiva es el de combinaciones estadísticas de los proyectores asociados a líneas en el espacio de fases, y se encontró un conjunto de operadores que preservan la positividad total. Se estudió el comportamiento de la interferencia en el espacio de fases al superponer pares de estados estabilizadores, y en particular pares de estados asociados a líneas en el espacio de fases, observando que en general la interferencia tiende a ocupar todo el espacio de fases, a diferencia de lo

que ocurre en la función de Wigner continua y sus generalizaciones módulo  $d$  o  $2d$ . Por último, se observó el efecto en la función de Wigner de un modelo de decoherencia aplicado a la evolución de un sistema de qubits en un estado-grafo, utilizando el hecho de que el ruido en la forma de operadores de Pauli produce traslaciones en el espacio de fases.

Existen aún muchos problemas abiertos en relación con los estudiados, además del ya mencionado respecto de la búsqueda de una definición única de la función de Wigner con coordenadas en  $GF(d)$ . Entre ellos se encuentran la caracterización de los estados con función de Wigner positiva en cada una de las definiciones posibles, y la del conjunto de operadores que preservan la positividad en cada definición. Respecto del grupo de operadores que preservan la positividad total, se sabe que es un subgrupo del grupo de Clifford, pero no cuáles son exactamente los operadores en este subgrupo. En el estudio de la interferencia, se mostró que para sistemas de dos o tres qubits no es posible evitar, en general, que la interferencia en el espacio de fases se superponga con las líneas asociadas a los estados que interfieren. La extensión de este resultado a casos de más qubits parece una conjetura razonable, pero no ha sido demostrada.

Más allá de los temas tratados en esta tesis, hay una gran variedad de problemas interesantes aún no resueltos relacionados con los estados estabilizadores o las funciones de Wigner discretas. Entre ellos se encuentra el de la existencia de bases mutuamente conjugadas, y su relación con el problema geométrico de la existencia de planos afines [44, 45]. También siguen apareciendo propuestas alternativas para definir la función de Wigner discreta [46]. El estudio de la equivalencia local de estados estabilizadores, del entrelazamiento en estados-grafo o estados estabilizadores, y de su persistencia bajo el efecto de la decoherencia es un área activa de investigación [47, 48]. Respecto de los estados-grafo, su importancia para la computación cuántica tiene mucho que ver con la aparición del modelo *one-way*. A partir de ella surgieron varias propuestas para fabricar estados-grafo, tanto con geometrías de cluster como en versiones más complejas y adaptables al cómputo a realizar en cada caso [49, 50, 51]; la plausibilidad de la construcción de computadoras cuánticas en este modelo (y en cualquier otro) depende de los avances experimentales que se produzcan de aquí en más.

## Muchas gracias a:

- Juan Pablo Paz por dirigirme y querer seguir dirigiéndome, y a Augusto que es el mejor de los compañeros posibles, por socorrerme continuamente, y sin protestar.
- Mis docentes de la carrera y el CBC; sobre todo a Fernando Lombardo, Diego Mazzitelli, Claudio Simeone y Cecilia López, por su (mucho) paciencia y sus (varios y valiosos) consejos.
- Mis compañeros<sup>1</sup> Diana, Flavia, Fer, Ale, León, Leito<sup>2</sup>, Rolo<sup>3</sup> y Wil<sup>4</sup>, por todo lo que me divertí durante la carrera.
- Mis amigos del mundo exterior, Ulises, Lore, Lu, Piki, y especialmente Nanu y Lao, por darme vacaciones en cualquier época del año.
- Padre, madre, hermano y hermanas, la abuela y la Ñata, porque como diría la maestra de Pequeña-Pequeñita, “una pena compartida es media pena, de igual manera que una alegría compartida es una doble alegría” [52].
- Beta, por todas las razones ñoñas imaginables y por otras de índole más práctica, como la ayuda con Linux y la programación y prestarme tu compu muchas horas.

---

<sup>1</sup>El orden en la enumeración es arbitrario! (en serio)

<sup>2</sup>Gracias también por traerme al grupo de cuántica, y por quedarte (nosotros te queremos más, y al fin y al cabo Barcelona ya está llena de argentinos).

<sup>3</sup>Gracias por cursar conmigo pilas de materias, y hacerlas mucho más mejores (diría que no decaiga, pero...)

<sup>4</sup>Gracias muchísimas por presentarme a nuestros amigos del mar, y por las altas dosis de brit-pop.

# Bibliografía

- [1] R. Raussendorf and H. J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86:5188–5191, May 2001.
- [2] Daniel Gottesman. *Stabilizer Codes and Quantum Error Correction*. PhD thesis, California Institute of Technology, 1997. ArXiv e-print quant-ph/9705052.
- [3] Kathleen S. Gibbons, Matthew J. Hoffman, and William K. Wootters. Discrete phase space based on finite fields. *Phys. Rev. A*, 70:062101, 2004.
- [4] J. P. Paz, A. J. Roncaglia, and M. Saraceno. Qubits in phase space: Wigner function approach to quantum error correction and the mean king problem. Arxiv e-print quant-ph/0410117.
- [5] Ernesto F. Galvão. Discrete Wigner functions and quantum computational speedup. *Phys. Rev. A*, 71:042302, April 2005.
- [6] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 124–134. IEEE Press, Los Alamitos, CA, 1994.
- [7] L. Grover. In *Proc. 28th Annual ACM Symposium on the Theory of Computation*, pages 212–219. ACM Press, New York, 1996.
- [8] L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 79(2):325–328, 1997.
- [9] R. P. Feynman. Simulating physics with computers. *Int. J. Theor. Phys.*, 21:467, 1982.
- [10] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, Cambridge, U.K., 2000.

- [11] Daniel Gottesman and Isaac L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402(6760):390–393, November 1999.
- [12] M. A. Nielsen. Universal quantum computation using only projective measurement, quantum memory, and preparation of the 0 state. *Phys. Lett. A*, 308:96, 2003.
- [13] D. Deutsch. Quantum computational networks. *Proc. Roy. Soc. London A*, 425:73, 1989.
- [14] D. Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. *Proc. Roy. Soc. London A*, 400:97, 1985.
- [15] D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. *Proc. Roy. Soc. London A*, 439:553, 1992.
- [16] A. M. Childs, D. W. Leung, and M. A. Nielsen. Unified derivations of measurement-based schemes for quantum computation. ArXiv quant-ph/0404132.
- [17] J. Preskill. Lecture notes for physics 229: Quantum information and computation. <http://www.theory.caltech.edu/people/preskill/ph229>. California Institute of Technology, 1998.
- [18] D. P. DiVincenzo. Two-bit gates are universal for quantum computation. *Phys. Rev. A*, 51(2):1015–1022, February 1995.
- [19] Daniel Gottesman. The Heisenberg representation of quantum computers. In S. P. Corney, R. Delbourgo, and P. D. Jarvis, editors, *Group 22: Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics*, pages 32–43. International Press, Cambridge, MA, 1999. ArXiv e-print quant-ph/9807006.
- [20] D. Gottesman. An introduction to quantum error correction. Proceedings of Symposia in Applied Mathematics. ArXiv e-print quant-ph/0004072, April 2000.
- [21] S. Aaronson and D. Gottesman. Improved simulation of stabilizer circuits. Arxiv e-print quant-ph/0406196.
- [22] D. M. Greenberger, M. A. Horne, and A. Zeilinger. Going beyond Bell’s theorem. In M. Kafatos, editor, *Bell’s Theorem, Quantum Theory, and Conceptions of the Universe*, page 69. Kluwer Academic, Dordrecht, 1989.

- [23] D. Schlingemann and R. F. Werner. Quantum error-correcting codes associated with graphs. *Phys. Rev. A*, 65:012308, 2001.
- [24] D. Schlingemann. Stabilizer codes can be realized as graph codes. *Quant. Inf. Comp.* 2, 4:307–323, 2002.
- [25] E. P. Wigner. On the quantum correction for thermodynamic equilibrium. *Phys. Rev.*, 40(5):749–759, June 1932.
- [26] M. Hillery, R. F. O’Connell, M. O. Scully, and E. P. Wigner. Distribution-functionals in physics - fundamentals. *Phys. Rep.*, 106(3):121–167, 1984.
- [27] J. H. Hannay and M. V. Berry. Quantization of linear maps on a torus – Fresnel diffraction by a periodic grating. *Physica D*, 1(3):267–290, 1980.
- [28] L. Cohen and M. Scully. *Found. Phys.*, 16:295, 1986.
- [29] Richard P. Feynman. Negative probability. In B. J. Hiley and F. David Peat, editors, *Quantum implications: essays in honour of David Bohm*, chapter 13, pages 235–248. Routledge, 1987.
- [30] W. K. Wootters. A Wigner-function formulation for finite-state quantum mechanics. *Annals of Physics*, 176(1):1–21, May 1987.
- [31] O. Cohendet, P. Combe, M. Sirugue, and M. Sirugue-Collin. A stochastic treatment of the dynamics of an integer spin. *J. Phys. A: Math. Gen.*, 21(13):2875–2883, July 1988.
- [32] U. Leonhardt. Quantum-state tomography and discrete Wigner function. *Phys. Rev. Lett.*, 74(21):4101–4105, May 1995.
- [33] W. K. Wootters. Picturing qubits in phase space. *IBM J. Res. Dev.*, 48:99, 2004.
- [34] Jay Lawrence, Caslav Brukner, and Anton Zeilinger. Mutually unbiased binary observable sets on  $N$  qubits. *Phys. Rev. A*, 65:032320, 2002.
- [35] R. Lidl and H. Niederreiter. Introduction to finite fields and their applications. *Cambridge University Press*, 1985.
- [36] C. Cormick, E. Galvão, D. Gottesman, J. P. Paz, and A. Pitterenger. Classicality in discrete wigner functions. Arxiv e-print quant-ph/0506222.

- [37] A. G. Klimov, L. L. Sanchez-Soto, and H. de Guise. Multicomplementary observables via finite Fourier transform. Arxiv e-print quant-ph/0410155.
- [38] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek. Perfect quantum error correction code. *Phys. Rev. Lett.*, 77:198, 1996.
- [39] C. Miquel, J. P. Paz, and M. Saraceno. Quantum computers in phase space. *Phys. Rev. A*, 65(6):062309, June 2002.
- [40] P. W. Shor. Scheme for reducing decoherence in quantum memory. *Phys. Rev. A*, 52:2493–2496, 1995.
- [41] A. M. Steane. Error correcting codes in quantum theory. *Phys. Rev. Lett.*, 77:793–797, 1996.
- [42] M. Hein, W. Dür, and H. J. Briegel. Entanglement properties of multipartite states under the influence of decoherence. Arxiv e-print quant-ph/0408165.
- [43] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: Necessary and sufficient conditions. *Phys. Lett. A*, 223:1–8, November 1996.
- [44] A. Klappenecker and M. Rötteler. Constructions of mutually unbiased bases. *Lecture Notes in Computer Science*, 2948:137–144, 2004.
- [45] Ingemar Bengtsson and Asa Ericsson. Mutually unbiased bases and the complementarity polytope. Arxiv eprint quant-ph/0410120.
- [46] S. Chaturvedi, E. Ercolessi, G. Marmo, G. Morandi, N. Mukunda, and R. Simon. Phase-space descriptions of operators and the wigner distribution in quantum mechanics II. The finite dimensional case. Arxiv e-print quant-ph/0507054.
- [47] S. Bravyi, D. Fattal, and D. Gottesman. GHZ extraction yield for multipartite stabilizer states. Arxiv e-print quant-ph/0504208.
- [48] S. Bandyopadhyay and D. Lidar. Robustness of many-qubit entanglement under general decoherence. Arxiv e-print quant-ph/0408174.
- [49] M. A. Nielsen. Optical quantum computation using cluster states. Arxiv e-print quant-ph/0402005.
- [50] S. C. Benjamin, J. Eisert, and T. M. Stace. Optical generation of matter qubit graph states. Arxiv e-print quant-ph/0506110.

- [51] Q. Chen, J. Cheng, K. Wang, and J. Du. Efficient construction of 2-d cluster states with probabilistic quantum gates. Arxiv e-print quant-ph/0507066.
- [52] F. Delgado Santos. *Aventuras de Pequeña-Pequeñita*. Serie para escuchar y para hablar. Ed. Plus Ultra, 1986.