UNIVERSIDAD DE GUADALAJARA

Centro Universitario de Ciencias Exactas e Ingenerías

División de Ciencias Básicas

Funciones de Wigner en el Espacio de Fase Discreto

Tesis
que para obtener el título de

Matemático

presenta

Ernesto Camacho Ramírez

Director: Dr. Andrés García Sandoval

Guadalajara, Jal., julio 2023

Dictamen 765/2023
Código 210466504

C. Ernesto Camacho Ramírez
Egresado de la carrera de Licenciado en Matemáticas
Presente

Hacemos de su conocimiento el resultado en el Dictamen emitido por el Comité de Titulación de la Licenciatura en Matemáticas, con relación a su solicitud de aprobación de modalidad y opción de titulación, conforme al Reglamento General de Titulación de la Universidad de Guadalajara:

Artículo 14, **Tesis, Tesina e Informes**
Opción I, **Tesis**
Con el título: ***"Funciones de Wigner en el Espacio de Fase Discreto".***

El Comité emite el siguiente resolutivo:

PROPUESTA APROBADA

Quedando asentada en el acta de la sesión con fecha 30 de mayo de 2023, con el número 3/2023, que éste Comité designa al Dr. Andrés García Sandoval como Director del trabajo. Asimismo, se le otorga el plazo de un año a partir de 31 de mayo de 2023, la cual es su fecha de aprobación para concluir su proceso de titulación.

El presente Dictamen deberá aparecer en el trabajo de titulación antes mencionado.

ATENTAMENTE
"Piensa y Trabaja"
"2023, Año del fomento a la formación integral con una Red de Centros y Sistemas Multitemáticos"
Guadalajara, Jal. a 02 de junio de 2023

Mtra. María Elena Olivares Pérez
PRESIDENTE DEL COMITÉ DE TITULACIÓN

UNIVERSIDAD DE GUADALAJARA
PIENSA Y TRABAJA
COMITÉ DE TITULACIÓN
LICENCIATURA EN MATEMÁTICAS

Comprobante Académico

El Comité de Titulación de la carrera de **Licenciado en Matemáticas**, hace constar que:

Ernesto Camacho Ramírez
Código 210466504

Egresado del plan semestral modular sistema de créditos, ha cumplido con los requisitos académicos para obtener el grado de **Matemático**, como lo marca el resolutivo Décimo Cuarto del Dictamen I/2012/388. La modalidad y opción que le han sido aprobadas, se indican en la siguiente tabla:

Artículo 9. Desempeño Académico Sobresaliente		I. Excelencia Académica
		II. Titulación por Promedio
Artículo 10. Exámenes		I. Examen Global Teórico-Práctico
		II. Examen Global Teórico
		III. Examen General de Certificación Profesional
		IV. Examen de Capacitación Profesional
Artículo 11. Producción de Materiales Educativos		I. Guías Comentadas o Ilustradas
		II. Producción de Materiales Educativos
		III. Paquete Didáctico
Artículo 12. Investigación y Estudios de Posgrado		I. Cursos de Maestría o Doctorado en IES de reconocido prestigio
		III. Seminario de Investigación
		IV. Seminario de Titulación
		V. Diseño o Rediseño de Equipos, Aparatos, Maquinaria, Proceso o Sistema de computación y/o Informática
Artículo 14. Tesis, Tesina e Informes	X	I. Tesis
		II. Tesina
		III. Informe de Prácticas Profesionales

El Comité de Titulación ha designado a los profesores Dr. Andrés García Sandoval, Mtra. María Cristina Muela López, Dr. Iván Fernando Valtierra Carranza y Dr. Juan Jesús Díaz Guevara para realizar la ceremonia de titulación.

ATENTAMENTE
"Piensa y Trabaja"
"2023, Año del fomento a la formación integral con una Red de Centros y Sistemas Multitemáticos"
Guadalajara, Jal. a 02 de junio de 2023

UNIVERSIDAD DE GUADALAJARA
PIENSA Y TRABAJA
COMITÉ DE TITULACIÓN
LICENCIATURA EN MATEMÁTICAS

MTRA. MARÍA ELENA OLIVARES PÉREZ
PRESIDENTE DEL COMITÉ DE TITULACIÓN

H. COMITÉ DE TITULACIÓN
LICENCIATURA EN MATEMÁTICAS
PRESENTE

Guadalajara, Jal., a 17 de julio de 2023

Por medio del presente nos permitimos informar a ustedes que los académicos asignados por el H. Comité de Titulación de la Licenciatura en Matemáticas, después de haber revisado el manuscrito del proyecto de tesis titulado:

"Funciones de Wigner en el Espacio de Fase Discreto"

desarrollado por el estudiante ERNESTO CAMACHO RAMIREZ (210466504), han tenido a bien aprobar su impresión, trabajo que defenderá el alumno para obtener el grado de Licenciado en Matemáticas.

Sin más por el momento, nos despedimos de ustedes, enviándoles un cordial saludo.

A T E N T A M E N T E

Dr. Andrés García Sandoval

Mtra. María Cristina Muela López

Dr. Iván Fernando Valtierra Carranza

Dr. Juan Jesús Díaz Guevara

Índice general

0.1. Introducción

El número de elementos de un conjunto general de operadores cuánticos unitarios sobre estados de n-qudit generalmente crece exponencialmente con n. Una excepción importante a ésta regla involucra el conjunto de operadores de Clifford, que actúan sobre estados estabilizadores. Los operadores de Clifford son los operadores que normalizan el grupo de Pauli, y los estados estabilizadores son los eigenestados simultáneos de un subconjunto maximal de operadores de Pauli conmutativos. Éstos estados juegan un papel importante en la corrección de errores cuánticos [1] y son cerrados bajo la acción de las compuertas de Clifford. La simulación eficiente de dichos sistemas con una computadora clásica se demostró con el algoritmo tableau de Aaronson y Gottesman [2, 1] para qubits ($d = 2$). La busqueda de un explicación de por qué un algoritmo tan eficiente es posible para la simulación de circuitos de Clifford ha sido un objeto de mucho estudio [3, 4, 5]. El progreso reciente ha sido resultado del trabajo de Wooters [6], Eisert [5], Gross [7] y Emerson [4], quienes han formulado una nueva perspectiva basada en los espacios de fase discretos de estados y operadores en espacios de Hilbert finitos, utilizando funciones discretas de Wigner. La función de Wigner en el caso continuo surge de vincular la mecánica cuántica con la mecánica clásica estadística, mediante el espacio de fase. Las funciones de Wigner nos dan una representación alternativa de estados de sistemas cuánticos, por medio de *cuasi-distribuciones* sobre el espacio de fase. Éstas funciones no son distribuciones probabílisticas verdaderas ya que pueden tomar valores negativos, y ésta negatividad ha sido vinculada con la no-localidad. La generalización a sistemas discretos a tomado distintas formas a traves de los años, cada una con ventajas y desventajas. Para una clase particular de funciones de Wigner discretas, se ha demostrado que los estados estabilizadores son análogos discretos a los estados Gaussianos en sistemas continuos [7], en el sentido de que tienen funciones de Wigner no-negativas. Por otro lado se ha demostrado que los operadores de Clifford son mapeos definidos positivos, ésto implica que los circuitos de Clifford son simulables eficientemente en computadores clásicas.

En este trabajo, buscamos construir de una manera explícita, a los operadores *puntuales de fase* discretos (núcleos de la transformación de Wigner) para qubits y qutrits. En particular, desarrollamos la construcción *estándar* siguiendo la metodología de Gibbons y Wootters [6], y como contribución del trabajo, buscamos una construcción *no estándar* de los núcleos por medio de bases no equivalentes (bajo transformaciones unitarias) a las bases de la construcción estándar. La motivación para realizar éste trabajo es que los núcleos de la construcción no estándar preservan las propiedades de la construcción estándar por lo tanto pueden ser utilizados para definir una función de Wigner. En particular, preservan la propiedad tomográfica, la cual permite expresar la función de Wigner de cualquier estado como una combinación lineal de probabilidades observadas. La inequivalencia de las construcciones conduce a la *posibilidad* de encontrar estados no estabilizadores con funciones de Wigner no-negativas, lo que contrasta con resultados previos para el caso discreto [7, 8, 9].

Capítulo 1

Preliminares

La función de Wigner es una función sobre el espacio de fase que nos brinda una representación alternativa de los sistemas cuánticos. Dicha función es la parte esencial de una formulación completa de la teoría de la mecánica cuántica sobre el espacio de fase. Inicialmente solo se consideraban sistemas de dimensión infinita en donde las variables de posición y de momentum del sistema toman valores de $\mathbb{R}^n$. Alrededor de los años 80's se hicieron múltiples intentos de generalizar el concepto de la función de Wigner a sistemas de dimensión finita. Para los sistemas continuos resulta que la función de Wigner es prácticamente única en el sentido de que posee la propiedad tomográfica [10], pero para sistemas discretos no hay una función de Wigner única, e incluso hay distintas construcciones con distintas propiedades. Esencialmente existen dos versiones básicas, una que imita la construcción de la versión continua de una manera muy natural y otra construcción que se basa en las propiedades que satisface la versión continua. En éste trabajo adoptamos la segunda construcción, la cual se debe a Wootters. La razón principal para ésta elección es que nos brinda una metodología que se puede aplicar para una construcción alternativa de la función Wigner.

Para poder estudiar la función de Wigner discreta es necesario presentar la función en el caso continuo. Para ésto requerimos un conocimiento básico de la mecánica cuántica. A diferencia de la mecánica clásica, la teoría cuántica es naturalmente probabilística y sus formulaciones matemáticas son bastante distintas. En la mecánica clásica, cuando se fija un estado de un sistema físico, el valor especificado por un observable (algo se puede medir del sistema) está completamente determinado. En la mecánica cuántica ésto ya no es cierto, los observables solo nos brindan distribuciones probabilísticas de los posibles valores. La siguiente sección introduce los conceptos básicos de la mecánica cuántica que necesitaremos para formular las funciones de Wigner en el caso continuo y discreto. El apéndice (A.1) puede ser consultado para repasar el concepto del espacio de fase en la mecánica clásica de manera introductoria.

1.1. La mecánica cuántica

La teoría cuántica ha tomado distintas direcciones despues de su concepción en los años viente y existen distintas formulaciones matematicamente equivalentes que surgieron despues de las teorias iniciales de Schrödinger (mecánica de ondas) y de Heisenberg (mecánica matricial). La más común hoy en dia es la formulación en el espacio de Hilbert, la cual fue desarrollada de manera rigurosa por Von Neumann en 1932. La segunda formulación más común, especialmente en la teoría cuantica de

campos, es la formulación de la integral de trayectoria de Feynman desarrollada en 1948. Otra formulación, de particular interés para nuestro trabajo, es la formulación en el espacio de fase, que tiene sus inicios en 1932 por Wigner, pero que solo fue desarrollada como una descripción completa de la mecánica cuántica despues de la segunda guerra mundial.

En cualquiera de las formulaciones, la mecánica cuántica como toda teoría física, permite el cálculo del comportamiento y las propiedades de sistemas físicos. Dado un sistema físico, se definen los *observables* como las cantidades que podemos medir sobre el sistema, por ejemplo la temperatura de algún cuerpo. En la formulación de Schrödinger, a los sistemas físicos se le asocia un espacio de Hilbert separable. Los observables físicos son representados por los operadores auto-adjuntos definidos en algún subespacio del espacio de Hilbert. El estado de un sistema representa toda la información del sistema en algún momento y está dado por operadores auto-adjuntos que satisfacen ciertas condiciones adicionales. Cuando no hay incertidumbre sobre el estado en el que está el sistema, podemos representar el estado por un vector del espacio de Hilbert, y decimos que el sistema está en un estado puro.

El ejemplo físico básico es el de una partícula moviendose en un espacio Euclideano. El espacio de Hilbert asociado a éste sistema generalmente es el espacio de las funciones cuadráticamente integrables $L^2(\mathbb{R}^n)$. Los estados puros del sistema son los elementos de éste espacio y el operador correspondiente al observable de la posición de la partícula es el operador que multiplica una función por la coordenada. La mecánica cuántica nos dice que no podemos predecir la posición exacta de una partícula en un estado arbitrario, lo único que podemos hacer es obtener la *probabilidad* de encontrar a la partícula en algún subconjunto de $\mathbb{R}^n$. Estadísticamente, nos interesa obtener el *valor esperado* de la posición de la partícula en un estado en específico, así como el valor esperado de otros operadores de interés como lo son la energía del sistema, el momentum, el momentum angular, entre otros. La mecánica cúantica nos permite estudiar los sistemas y sus observables de manera probabilística y también nos permite describir su evolución temporal por medio de la ecuación de Schrödinger.

1.1.1. Postulados de la mecánica cuántica

Comencemos definiendo los conceptos y algunos de los postulados que necesitaremos de la mecánica cuántica. Existen múltiples versiones de los postulados, dependiendo del rigor matemático con el cual se planea trabajar. Para ésta sección adaptamos las definiciones del libro de Brian Hall [11].

Postulado 1. *A cada sistema cúantico le corresponde un espacio de Hilbert $\mathcal{H}$. Los estados del sistema son todos los operadores lineales $\rho : \mathcal{H} \to \mathcal{H}$, definidos-positivos y de traza finita, tales que* $\mathrm{Tr}(\rho) = 1$.

Un estado cuántico ρ se dice *puro*, is existe un elemento $\psi \in \mathcal{H}$, tal que para todo $\alpha \in \mathcal{H}$ se cumple

$$\rho(\alpha) = \frac{\langle \psi | \alpha \rangle}{\langle \psi | \psi \rangle} \psi,$$

donde $\langle \cdot | \cdot \rangle$ es el producto interno del espacio de Hilbert en cuestion. De ésta manera, cuando hablemos de un estado puro, podremos referirnos a un elemento $\psi \in \mathcal{H}$, algo que casi siempre sucede en la literatura física.

Postulado 2. *A cada observable físico, A, sobre el espacio de fase clásico, le corresponde un observable cuántico representado por un operador auto-adjunto del espacio de Hilbert,*

$$\hat{A} : \mathcal{D}_{\hat{A}} \to \mathcal{H} \, .$$

Los operadores auto-adjuntos representan a los observables físicos como por ejemplo la energía, posición, momentum y momentum angular. Pero también pueden representar observables que no tienen un análogo clásico. Por ejemplo pueden representar los grados de libertad de un sistema *spin* mediante un espacio de dimensión finita. La matemática se vuelve más sencilla en el caso finito ya que no se tiene que lidiar con las sutilezas del continuo. Por ésta razón, muchos de los tratados sobre la *teoría de la medición cuántica* generalmente se hacen en el caso finito, evitando las cuestiones delicadas pertinentes a la convergencia, cuestiones de acotamiento y del dominio del operador, etc. Muchos problemas surgen del ignorar éstos detalles y se pueden tratar rigurosamente con la teoría espectral, pero dada la naturaleza de éste trabajo, podemos prescindir de ellos ya que nuestro estudio será sobre sistemas finitos.

El proceso de medición consiste de la prueba o manipulación de un sistema físico para obtener un valor númerico. En la mecánica cuántica, dichas predicciones son probabilísticas de manera natural. A pesar de las cuestiones filosóficas que aun no se resuelven rotúndamente sobre todo en la cuestión de la medición, experimentalmente es un éxito. El precepto que seguiremos para obtener la información probabilística del sistema está dada por el postulado de la medición:

Postulado 3. *Si un sistema cuántico está en un estado descrito por un vector unitario $\psi \in \mathcal{H}$, entonces el valor esperado de un observable A, con operador correspondiente $\hat{A}$, satisface*

$$\langle \hat{A} \rangle_{\psi} := \langle \psi | \hat{A} \psi \rangle \, ,$$

De manera general, dado un estado ρ, el valor esperado de un observable A está dado por

$$\mathrm{Tr}\left(\hat{A}\rho\right) = \mathrm{Tr}\left(\rho\hat{A}\right) ,$$

donde Tr *es la traza del operador.*

Los valores que pueden tomar los observables cuánticos pertenecen al *espectro* del operador. En la literatura física es común que se consideren a los elementos del espectro como los eigenvalores del operador, pero el espectro generalmente es mucho más grande. En cuanto al postulado de medición, ésto nos dice que a la hora de hacer una medición de un observable en un estado cuántico ψ, mediremos un elemento del espectro y el estado colapsa a una 'eigenfunción' correspondiente a dicho valor. En el caso finito, las cuestiones matemáticas se vuelven más simples porque el espectro de los operadores auto-adjuntos *sí* es el conjunto de eigenvalores del operador. Por el momento nos enfocamos en sistemas cuánticos finitos para poder estudiar un poco más fondo el concepto de la medición.

1.2. En dimensión finita

El ejemplo clásico es el del *spin* de una partícula, la cual toma una cantidad de valores finitos. El ejemplo físico más sencillo es el de las partículas de spin-1/2, en éste caso el spin solo toma dos valores, y se dice que la partícula es de 2-niveles. Para una

partícula de d-niveles, el espacio de Hilbert correspondiente es $\mathcal{H} = \mathbb{C}^d$. Para el caso finito, adoptaremos por completo a la notación (maquinaria) de P. A. M. Dirac, pues es una manera fácil de hacer cálculos y de expresar a los operadores de los observables y aquellos correspondientes a los estados puros. En ésta notación, los estados puros ψ del sistema cuántico, se denotan con un *ket*, $|\psi\rangle$. A cada ket, le corresponde un funcional lineal llamado *bra*, $\langle\psi|$, el cual se define por su acción:

$$(\langle\psi|)(|\phi\rangle) := \langle\psi|\phi\rangle\,.$$

Utilizando el bra, para todo estado puro $|\psi\rangle$ podemos formar un operador de rango uno, que resulta ser la proyección Π_ψ al subespacio generado por $|\psi\rangle$, dicho operador está formado por el producto tensorial de $|\psi\rangle$ con su dual:

$$|\psi\rangle\langle\psi| := \Pi_\psi = |\psi\rangle \otimes \langle\psi|\,. \tag{1.1}$$

Su acción sobre algun elemento del espacio de Hilbert se expresa de manera muy natural utilizando la notación de Dirac:

$$(|\psi\rangle\langle\psi|)\,|\phi\rangle = \langle\psi|\phi\rangle\,|\psi\rangle\,.$$

Dado que los observables son operadores auto-adjuntos, sus eigenestados forman una base ortonormal del espacio de Hilbert. En particular las proyecciones de cada elemento de la base ortonormal son auto-adjuntos. En general los operadores auto-adjuntos satisfacen las siguientes propiedades:

Proposición 1. *Si A es un operador auto-adjunto entonces:*

1. *Sus eigenvalores son reales.*
2. *Sus eigenestados son ortogonales.*
3. *Existe una base ortonormal del espacio de Hilbert que consiste de los eigenestados del operador (normalizados).*

1.2.1. Medidas proyectivas

La idea básica de la teoría de medición consiste en el hecho de que podemos elegir *cualquier* base ortonormal del espacio de Hilbert $\mathcal{H}$ y observar en que estado de la base se encuentra nuestro sistema cuántico. Al hacer la medición siempre encontraremos uno de los estados de dicha base, y, utilizando el postulado de la medición (3), podemos calcular la probabilidad de observar una de las posibles mediciones. Una medición de éste tipo se conoce como *medición de Von Neumann* ó medición proyectiva. Existen otros tipos de mediciones que generalizan éste concepto, como las POVMs (medidas de operadores positivos), pero la construcción de la función de Wigner está basada en las medidas proyectivas así que no será necesario estudiar esas alternativas para éste trabajo.

La regla que asigna una probabilidad al evento de observar un valor específico de los posibles se conoce como la *regla de Born*. Si tenemos un operador auto-adjunto, sus eigenvectores y eigenvalores forman un conjunto de posibles mediciones. Denotemos por m el resultado correspondiente al eigenestado $|\phi_m\rangle$. Entonces la regla de Born nos dice que la probabilidad de observar a m está dada por la norma cuadrada de la proyección

del vector $|\psi\rangle$ hacia el subespacio generado por el vector $|\phi_m\rangle$, i.e., si Π_m representa dicha proyección, entonces:

$$p(m) = \|\Pi_m |\psi\rangle\|^2 = \langle\psi|\Pi_m^* \Pi_m|\psi\rangle = \langle\psi|\Pi_m|\psi\rangle . \tag{1.2}$$

La última igualdad se sigue de que las proyecciones son idempotentes y auto-adjuntos. En otras palabras, la probabilidad de obtener m en una medición corresponde al valor esperado de la proyección Π_m en el estado $|\psi\rangle$. Utilizando cualquier base ortonormal $\{|\varphi_n\rangle\}$, podemos expresar a la regla de Born en términos de la traza para un estado puro $|\psi\rangle$ de la siguiente manera:

$$\begin{aligned} p(m) &= \langle\psi|\Pi_m|\psi\rangle && (1.3)\\ &= \sum_n \langle\psi|\varphi_n\rangle \langle\varphi_n|\Pi_m|\psi\rangle && (1.4)\\ &= \sum_n \langle\varphi_n|\Pi_m|\psi\rangle \langle\psi|\varphi_n\rangle && (1.5)\\ &= \mathrm{Tr}\left(|\psi\rangle \langle\psi| \Pi_m\right). && (1.6) \end{aligned}$$

Para proyecciones de rango uno, es decir operadores de que proyectan a subespacios unidimensionales, es fácil observar que la probabilidad de la medición m, $p(m)$, es igual a los coeficientes de la expansión del estado en la base de medición, ya que podemos expresar la proyección como $\Pi_m = |m\rangle \langle m|$ y así:

$$\begin{aligned} p(m) &= \langle\psi|\Pi_m|\psi\rangle && (1.7)\\ &= \langle\psi|m\rangle \langle m|\psi\rangle && (1.8)\\ &= \overline{\langle m|\psi\rangle} \langle m|\psi\rangle && (1.9)\\ &= |\langle m|\psi\rangle|^2 . && (1.10) \end{aligned}$$

Una *medida proyectiva* es un conjunto de proyecciones que proyectan hacia subespacios ortogonales y cuya suma es igual al operador identidad. Los eigenvectores de operadores auto-adjuntos forman una medida proyectiva. Es evidente que la suma de las probabilidades debe ser igual a 1 para una medida proyectiva, ya que la suma de las proyecciones nos da la identidad, y los estados cuánticos puros son de norma unitaria por el primer postulado:

$$\sum_m p(m) = \sum_m \langle\psi|\Pi_m|\psi\rangle = \langle\psi| \left(\sum_m \Pi_m\right) |\psi\rangle = \langle\psi|I|\psi\rangle = 1. \tag{1.11}$$

Hasta ahorita hemos expuesto los mecanismos de la medición para estados puros. Éstos corresponden a la posesión de la información completa del sistema, algo generalmente no es el caso. Ahora supongamos que no se conoce con certeza en que estado está el sistema. Lo único que sabemos es que el sistema está preparado en el estado $|\psi_k\rangle$ con probabilidad p_k de una colección de posibles estados $\{(p_k, |\psi_k\rangle)\}$, de tal modo que $\sum_k p_k = 1$. Con ésto podemos darle un significado al uso de operadores para describir estados cuánticos como lo hicimos en el primero postulado.

Definición 1. *Si el conjunto $\{(p_k, |\psi_k\rangle)\}$ corresponde a un estado mixto, entonces definimos al operador de densidad como*

$$\rho = \sum_k p_k |\psi_k\rangle \langle\psi_k| . \tag{1.12}$$

Proposición 2. *Un operador ρ es el operador de densidad asociado a conjunto estadístico $\{(p_k, |\psi_k\rangle)\}$ si y solo si es auto-adjunto, positivo y de traza unitaria.*

Resulta que la correspondencia entre conjuntos estadísticos y operadores de densidad no es única. Distintos conjuntos estadísticos nos llevan al mismo operador de densidad. Por lo tanto tienen los mismos valores esperados para cualquier observable y en efecto son indistinguibles. Es por ésto que el operador de densidad es la generalización más natural de un estado cuántico, en lugar de simplemente los vectores unitarios del espacio de Hilbert. Es común confundir el significado de la superposición de estados cuánticos y una mezcla de estados. Para ganar intuición, podemos considerar el ejemplo de una mezcla de dos estados. Ésta mezcla describe nuestra *falta de conocimiento*, el sistema realmente se encuentra en uno de los dos, solo que no sabemos cual es. En cambio, una superposición de estados, el sistema *no* se encuentra en uno de los dos específicamente, sino que el estado se encuentra en ambos a la vez (o en ninguno dependiendo de la filosofía que uno adopte).

Para operadores de densidad, la regla de Born se expresa naturalmente como el valor esperado de la proyección Π_m en el estado ρ:

$$p(m) = \mathrm{Tr}\left(\rho \Pi_m\right). \tag{1.13}$$

1.2.2. Tomografía cuántica y MUBs

En la mecánica cuántica, el estado de un sistema cuántico no puede ser observado ni puede ser determinado completamente de manera experimental. Dado que una sola medición no es suficiente para obtener la información necesaria para reconstruir el estado cuántico, y dado que la medición afecta el estado, se vuelve imposible obtener el resto de la información con mediciones subsiguientes [12]. Pero si tenemos un conjunto (ensamble) de sistemas *identicamente* preparados, la noción de la determinación del estado mediante mediciones cobra sentido, ya que se puede, en principio, identificar el estado en que se *prepara* el sistema cuántico. A ésto se le conoce como *tomografía cuántica*.

El uso de las bases mutuamente insesgadas (MUBs) ha sido impulsado principalmente por la busqueda de métodos óptimos de reconstrucción de estados. Kanat [13] menciona que las bases mutuamente insesgadas fueron estudiadas por primera vez por Schwinger en 1960, pero no fueron definidas y ejemplificadas hasta 1987 por parte de Wootters y Fields [6]. En dicho trabajo Wootters y Fields investigan la determinación de estados óptima y llegan a la conclusión de que sí se puede encontrar un conjunto de $d+1$ bases mutuamente insesgadas para un espacio de Hilbert $\mathcal{H}$ de dimensión d, entonces las mediciones correspondientes a esas bases proveen una manera óptima de determinar el operador de densidad de un ensamble de estados, en el sentido de que el error estadístico es minimizado. Además demuestran que la cantidad máxima de MUBs para un sistema de dimensión d es precisamente $d+1$ y nos dan una manera de cálcular las bases explícitamente.

La caracteristica de ser mutuamente insesgados es una relación entre distintas bases ortogonales del espacio de Hilbert, y se define de la siguiente manera.

Definición 2. *Sea $\mathcal{H} = \mathbb{C}^d$, decimos que dos bases ortonormales $\mathcal{B}_0 = \{|\psi_i\rangle\}$ y $\mathcal{B}_1 = \{|\phi_j\rangle\}$ son mutuamente insesgadas si*

$$|\langle\psi_i|\phi_j\rangle|^2 = \frac{1}{d}, \tag{1.14}$$

para cualesquiera i y j.

Dado que tenemos una preferencia por expresar estados cuánticos por medio de operadores de densidad, es útil notar que podemos expresar ésta noción de ser mutuamente insesgado en términos de las proyecciones. Si Π_i es el operador que proyecta al subespacio generado por $|\psi_i\rangle$ y Π_j el que proyecta hacia $|\phi_j\rangle$, entonces dos bases son mutuamente insesgadas si

$$\mathrm{Tr}\left(\Pi_i \Pi_j\right) = \frac{1}{d}, \tag{1.15}$$

para todo i y j. El ejemplo más básico es para un qubit, donde el sistema cuántico es modelado por el espacio $\mathcal{H} = \mathbb{C}^2$. Un cálculo directo prueba que las siguientes bases son mutuamente insesgadas:

$$\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}, \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}, \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix} \right\}. \tag{1.16}$$

Éstas son las bases a las que se refiera Kanat, pues Schwinger identificó que son los eigenestados de operadores que son *complementarios* [14]. Son complementarios en el sentido de que la información que obtenemos al medir en un base no nos aporta nada en cuanto a los resultados de la medición en alguna otra base.

Hemos mencionado el problema de la determinación de estados cuánticos múltiples veces, enseguida hacemos ésto más claro. El problema de la determinación de estados, ó de tomografía cuántica es el problema de determinar la matriz de densidad[1] correspondiente a un ensamble de sistemas d-dimensionales preparados de manera idéntica. Para un sistema de dimensión d, la matriz de densidad está totalmente determinada por $d^2 - 1$ parámetros reales. Una medición en una base de un subconjunto del ensamble nos genera solamente $d - 1$ números reales independientes, ya que la regla de Born nos dice que su suma debe ser la unidad. Se sigue que requerimos *al menos* $d + 1$ distintas mediciones para recuperar el estado cuántico. Se ha demostrado que si uno puede obtener $d + 1$ MUBs, entonces las mediciones en éstas bases son suficientes para determinar la matriz de densidad. No es necesario que las bases sean mutuamente insesgadas para recuperar el estado, pero si lo son, nos brindan una manera óptima en el siguiente sentido: como no podemos hacer una cantidad infinita de experimentos, estamos sujetos al error estadístico que se introduce, i.e., no podremos recuperar las probabilidades con precisión exacta. Wootters y Fields establecen ésta noción de error estadístico de manera precisa y prueban que las mediciones hechas con MUBs son óptimas en el sentido de que minimizan el error estadístico.

Otro aspecto fundamental de las MUBs para nuestro trabajo, es que en general no son únicas, en el sentido de que para ciertas dimensiones existen bases que no son unitariamente equivalentes.

Definición 3. *Sea B_k la matriz cuyas columnas corresponden a elementos de una base $\mathcal{B}_k$ de un conjunto de MUBs $\mathcal{B}$. Decimos que dos conjuntos de MUBs,*

$$\mathcal{B} = \{B_0, \ldots, B_k\} \quad y \quad \mathcal{B}' = \{B'_0, \ldots, B'_k\},$$

son equivalentes si existe una transformación unitaria U de $\mathbb{C}^d$ tal que

$$\{B'_0, \ldots, B'_k\} = \{UB_0, \ldots, UB_k\}, \tag{1.17}$$

[1] En la literatura física generalmente se utilizan los términos matriz de densidad y operador de densidad para referirse al mismo objeto, nosotros hacemos el ligero incapie en que la matriz de densidad es la representación matricial del operador de densidad en alguna base.

donde el orden no se preserva necesariamente.

Calderbank, Cameron, Kantor y Seidel demostraron la existencia de varias bases mutuamente insesagadas que no son equivalentes [15], i.e., tales que *no* existe una transformación unitaria que satisface la definición anterior. Ésto lo hacen a partir de la inequivalencia de unas estructuras llamadas *coberturas simplécticas*, las cuales veremos en el capítulo cuatro.

Nuestro interés en las MUBs para éste trabajo es que surgen de manera natural a la hora de asignar una estructura cuántica al espacio de fase discreto para la construcción de una función de Wigner discreta. Antes de continuar con ese tema es necesario introducir el concepto de la función de Wigner. A pesar de que la mayoría de éste trabajo se centra en sistemas finitos, nos será útil repasar sistemas continuos ó dimensión infinita, ya que la función de Wigner originalmente se introdujo para el uso en esos sistemas cuánticos.

1.2.3. Sistemas continuos

En sistemas continuos, los dos operadores fundamentales de la mecánica cuántica son los operadores de posición y de momentum. En particular pensemos en el sistema de una partícula moviendose sobre la recta real $\mathbb{R}$. El espacio de Hilbert es el espacio de las funciones cuadráticamente integrables, $L^2(\mathbb{R})$. Si $\psi \in L^2(\mathbb{R})$ es un vector unitario, entonces $|\psi|^2$ puede ser interpretado como la densidad de probabilidad de la posición de la partícula en el estado ψ, es decir, que la probabilidad de que la partícula se encuentre en el subconjunto $B \subset \mathbb{R}$ es $\int_B |\psi|^2$. A partir de ésto es posible definir los operadores de posición y de momentum que satisfacen ésta propiedad:

Definición 4. *El operador de posición $\hat{X}$ se define como*

$$\hat{X}\psi(x) = x\psi(x),$$

donde $\psi \in L^2(\mathbb{R})$ es tal que $x\psi \in L^2(\mathbb{R})$.

Notemos que no existen estados $\psi \in L^2(\mathbb{R})$ para los cuales el operador $\hat{X}$ toma valores definitivos. Las "eigenfunciones" de $\hat{X}$ nisiquiera son funciones, sino *deltas de Dirac* $\delta_{x_0}(x) = \delta(x - x_0)$. Éstas se pueden considerar como un conjunto de "estados idealizados" y que forman una "base ortonormal continua" del espacio de Hilbert en el siguiente sentido:

$$\langle \delta_{x_1} | \delta_{x_2} \rangle = \int \delta(x - x_1)\delta(x - x_2)\, dx = \delta(x_1 - x_2),$$
$$f = \int f(x)\delta_x\, dx = \int \langle f|\delta_x\rangle\, \delta_x\, dx,$$

donde las integrales se interpretan en el sentido de las distribuciones de Schwartz. La teoría de distribuciones aporta una manera de hacer riguroso los cálculos con los deltas de Dirac por medio del triplete de Gel'fand [16]. Por otro lado, la teoría espectral de los operadores auto-adjuntos nos brinda una manera de hacer riguroso toda la maquinaria matemática necesaria para hacer los cálculos sin recurrir a la distribuciones. A pesar de ésto, generalmente se opta por utilizar la maquinaria de Dirac sin cuidar el rigor con la finalidad de facilitar los cálculos. Dado que éstos detalles no aparecen en el caso finito, nosotros no seremos muy rigurosos a la hora de introducir a la función de Wigner en el caso continuo y generalmente optaremos por usar las convenciones físicas.

Es común trabajar con la *función de onda* correspondiente a un estado ψ, ésto es una representación del estado ψ en términos de la posición. La función de onda se define como

$$\psi(x) = \langle x|\psi\rangle\,, \tag{1.18}$$

donde el $x \in \mathbb{R}$ del lado izquierdo es un "eigenvalor" y del lado derecho es un "eigenestado" del operador de posición. Por otro lado, podemos definir el operador que corresponde al momentum clásico de la siguiente manera:

Definición 5. *El operador de momentum $\hat{P}$ se define como*

$$\hat{P}\psi(x) = -i\frac{\partial}{\partial x}\psi,$$

donde $\psi \in L^2(\mathbb{R})$ es tal que

El operador de momentum también tiene un espectro continuo por lo cual es necesario introducir estados generalizados para poder hacer cálculos. Además, de manera análoga al operador de posición, podemos expresar un estado ψ en términos del momentum mediante

$$\psi(p) = \langle p|\psi\rangle\,, \tag{1.19}$$

donde de nuevo p representa los eigenestados de $\hat{P}$. Notemos que las funciones $\psi(x)$ y $\psi(p)$ son dos representaciones del *mismo* estado ψ. La transformación de Fourier conecta a la función de posición $\psi(x)$ con la del momentum $\psi(p)$ de la siguiente manera:

$$\psi(x) = \frac{1}{\sqrt{2\pi\hbar}}\int_{\mathbb{R}} \psi(p)e^{ixp/\hbar}\,dp, \tag{1.20}$$

donde $\hbar$ es la constante de Planck. Ésta relación es una de las razones por la cual se les llama a las *variables* de posición y momentum, *variables conjugadas*.

Los estados mixtos se expresan de una manera análoga al caso finito. Definimos un estado mixto como un conjunto de pares $\{(\lambda_j, \psi_j)\}_{j\in\mathbb{N}}$ donde cada $\psi_j \in L^2(\mathbb{R}^n)$ es un estado puro y $0 \leq \lambda_j \leq 1$ es una probabilidad clásica, es decir, $\sum_j \lambda_j = 1$.

Definición 6. *Un estado cuántico es el conjunto de pares $(\lambda_j, \psi_j) \in [0,1]\times L^2(\mathbb{R}^n)$, indexado por un conjunto discreto F donde $\|\psi_j\|_{L^2(\mathbb{R}^n)} = 1$ para todo $j \in F$ y $\sum_{j\in F}\lambda_j = 1$. El operador lineal $\hat{\rho}$ sobre $L^2(\mathbb{R}^n)$ definido por*

$$\hat{\rho}\psi = \sum_{j\in F}\lambda_j\Pi_{\psi_j}\psi = \sum_{j\in F}\lambda_j\,\langle\psi|\psi_j\rangle\,\psi_j, \tag{1.21}$$

es el operador de densidad asociado al estado.

El operador de densidad definido de ésta manera es auto-adjunto, semi-definido positivo, y es de clase de traza con $\mathrm{Tr}(\hat{\rho}) = 1$, por lo tanto cumple con el primer postulado de la mecánica cuántica. El espectro de un operador de densidad $\hat{\rho}$ sobre $L^2(\mathbb{R}^n)$ es discreto y consiste de números no negativos tales que $\lambda_1 \geq \lambda_2 \geq \ldots \geq 0$, y $\lim_{j\to\infty}\lambda_j = 0$ (en el caso en que F es infinito).

El postulado de la medición nos dice que podemos calcular el valor esperado de un observable cuántico A, en un estado cuántico ρ de la siguiente manera:

$$\langle\hat{A}\rangle = \mathrm{Tr}(\hat{A}\rho). \tag{1.22}$$

También podemos calcular las probabilidades de observar un valor específico de una medición de un observable, éstos valores son elementos del espectro del observable en cuestión. Como mencionamos antes, el espectro del un observable generalmente es más grande que su conjunto de eigenestados. Aún así, podemos trabajar con la idea de eigenestados generalizados para poder hacer los cálculos de manera análoga como lo hicimos en el caso finito. De hecho la función de onda en la representación de la posición nos da precisamente la probabilidad de medir la posición en un punto x para un estado que modela la posición de una partícula. Sucede lo mismo con la función de onda en representación del momentum.

La no conmutatividad de los operadores de posición y de momentum tiene consecuencias profundas en la teoría de la medición. El principio de incertidumbre nos dice que no podemos medir de manera simultánea la posición y momentum de una partícula con precisión (ni siquiera en teoría). Del repaso de la mecánica clásica en el apéndice (A.1), sabemos que mediante el uso del espacio de fase, podemos representar a los estados de un sistema físico por puntos en el plano $\mathbb{R}^2$. En la mecánica clásica sí es posible, en teoría, medir la posición y el momentum de una partícula en cualquier momento. Por lo tanto tiene sentido representar al estado de un sistema como un punto en el plano. La evolución temporal del sistema forma trayectorias en el plano de acuerdo a las leyes de movimiento. En el caso cuántico el principio de incertidumbre no nos permite localizar el estado en un espacio de fase. Pero, no todo está perdido, hay maneras de vincular éstos dos conceptos por medio de las cuasi-distribuciones, y en particular la función de Wigner.

Capítulo 2

Función de Wigner

2.1. Mecánica cuántica en el espacio de fase

En éste capítulo introducimos el concepto de la función de Wigner y la formulación de la mecánica cuántica en el espacio de fase. El principio de la incertidumbre hace que la noción de un espacio de fase análogo al de la mecánica clásica, sea problemático para la teoría cuántica. Ésto se debe a que la posición y el momentum de una partícula no se pueden medir de manera simultánea. Aún así existen funciones que se *asemejan* a distribuciones probabilísticas sobre el espacio de fase, llamadas funciones de distribución cuasi-probabilísticas, las cuales son útiles de manera práctica, además de vincular de cierta manera a la mecánica clásica y la cuántica. Ésto sucede porque dichas cuasi-distribuciones nos permiten calcular los valores esperados de los operadores cuánticos de manera muy similar a los promedios clásicos de la mecánica estadística. La primera y la que estudiamos en éste trabajo es la función de Wigner.

La función de Wigner tiene una larga historia que inicia con un artículo publicado por Eugene P. Wigner en 1932 [17] sobre correcciones cuánticas del equilibrio termodinámico. La idea principal de Wigner fue introducir una cuasi-distribución que le permite calcular valores esperados cuánticos de una manera análoga a los valores esperados de la mecánica estadística. Para el caso de una función ψ cuadráticamente integrable, la expresión que expuso Wigner originalmente (para un sistema de una dimensión) es:

$$W_\psi(x,p) = \frac{1}{\hbar\pi}\int_{\mathbb{R}} \overline{\psi}(x+y)\psi(x-y)e^{\frac{2i}{\hbar}py}\,dy. \tag{2.1}$$

En el caso de un estado cuántico puro, la función $W_\psi(x,p)$ representa al estado ψ de manera análoga a una densidad probabilística sobre el espacio de fase. Wigner partió de la mecánica estadística clásica, en donde la evolución del sistema puede ser estudiado de manera probabilística mediante la ecuación de Liouville, la cual nos brinda una distribución sobre el espacio de fase. Su idea fue construir una distribución que nos permita hacer los mismos cálculos probabilísticos de la mecánica cuántica que se pueden hacer con la formulación en el espacio de Hilbert.

Unos años antes de la publicación de Wigner, Hermann Weyl formuló una manera de mapear observables clásicos a observables cuánticos, lo cual se conoce como la *cuantización de Weyl* [18]. Debido a la no conmutatividad de los operadores canónicos $\hat{X}$ y $\hat{P}$, la cuantización de un observable clásico no es única y es necesario introducir un orden específico, la cuantización de Weyl es un caso específico. Weyl utilizó la transformación de Fourier para producir operadores correspondientes a ciertas funciones de

x y p en el espacio de fase que satisfacen algunas condiciones de regularidad. Existe una relación directa entre los mapeos de Weyl y de Wigner y nos es útil introducir el mapeo de Weyl primero.

Utilizando las transformaciones de Wigner y de Weyl, Enrique Moyal y Groenewold formularon de manera independiente, una descripción *completa* de la mecánica cuántica en el espacio de fase [19]. Ésta tercera formulación de la mecánica cuántica, ha sido muy útil en muchas ramas de la física, particularmente en la óptica cuántica [20]. En éste trabajo no daremos un resumen de ésta formulación, en caso de que el lector esté interesado, le invitamos a consultar los trabajos de Moyal [21] y de Groenwold [22].

2.2. La transformación de Wigner-Weyl

En ésta sección vamos definir la transformación de Wigner para estados puros, los cuales serán elementos de $L^2(\mathbb{R})$, para posteriormente definir la función de Wigner de un estado cuántico arbitrario. Para iniciar, introducimos el concepto de la cuantización de Weyl porque de ésta forma surgen de manera muy natural varios de los objetos que aparecen en las definiciones de la función de Wigner, independientemente si el sistema es continuo o discreto.

Recordemos la motivación de la sección anterior. Consideremos un conjunto de partículas que se mueven en un espacio $\mathbb{R}^n$. La ecuación de Liouville rige la evolución temporal de una función de distribución en el espacio de fase del conjunto de partículas. La solución de dicha ecuación nos brinda una densidad probabilística y dado un observable clásico $A : \mathbb{R}^{2n} \to \mathbb{R}$, que depende de la posición x y del momentum p de una partícula, podemos calcular el valor esperado del observable como una integral sobre el espacio de fase

$$\mathbb{E}[A] = \iint A(x,p)F(x,p)\,dx\,dp, \tag{2.2}$$

donde F es la densidad de probabilidad de Liouville. La densidad F contiene toda la información probabilística del *conjunto* de partículas, es decir del sistema. La intención es poder calcular valores esperados de observables cuánticos de manera análoga, es decir, mediante una integración en el espacio de fase, en donde la densidad que obtenemos representa a algún estado cuántico:

$$\mathrm{Tr}\left(\hat{\rho}\hat{A}\right) = \iint A(x,p)W(x,p)\,dx\,dp, \tag{2.3}$$

La función $W : \mathbb{R}^{2n} \to \mathbb{R}$ que actúa como una distribución probabilística será precisamente la transformación de Wigner de un estado cuántico. Desafortunadamente no es una distribución verdadera, pues puede tomar valores negativos (de aquí proviene el nombre de *cuasi*-distribución). Sin embargo, nos permite calcular los valores esperados de los operadores cuánticos y otras cantidades probabilísticas como las densidades de la posición y momentum de la partícula, dándonos una representación de nuestro estado cuántico completo pero distinto.

Notemos que la definición (2.1) es una transformación integral de una función $\psi \in L^2(\mathbb{R}^n)$. Para poder definir la transformación de un estado cuántico $\hat{\rho}$, tendremos que tomar algunos pasos previos. En particular, primero introducimos el concepto de *cuantización*, lo cual es un proceso inverso que nos permite pasar de un observable clásico definido en el espacio de fase a un operador cuántico definido en el espacio de Hilbert correspondiente.

2.2.1. La transformación de Weyl

El problema de la cuantización consiste en encontrar una correspondencia entre funciones sobre el espacio de fase $\mathbb{R}^{2n}$ y operadores auto-adjuntos sobre $L^2(\mathbb{R}^n)$, tales que las propiedades de los observables clásicos se reflejen lo más posible en sus correspondientes operadores cuánticos, en una manera consistente con la interpretación probabilística de la mecánica cuántica. Dada la no conmutatividad de los operadores de posición y de momentum, no hay una correspondencia única, por lo tanto se restringe el mapeo de una manera ad-hoc, buscando satisfacer ciertas propiedades razonables. Por ejemplo es deseable que las funciones coordenadas de posición y de momentum x_j y p_j correspondan a los operadores $\hat{X}_j$ y $\hat{P}_j$, así como el operador correspondiente a la función constante 1 debe ser el operador identidad, entre otros. A pesar de que no hay un manera única de cuantizar observables clásicos, existe una que es más *natural*, conocida como la cuantización de Weyl.

La idea de la cuantización de Weyl, es la siguiente: consideramos un observable clásico $A : \mathbb{R}^{2n} \to \mathbb{R}$, comunmente llamado *símbolo* en el análisis armónico y en la óptica cuántica. Lo podemos expresar mediante la transformación de Fourier inversa:

$$A(x,p) = \frac{1}{(2\pi\hbar)^n} \int_{\mathbb{R}^{2n}} \mathcal{F}A(\xi,\eta) e^{\frac{i}{\hbar}(\xi x + \eta p)}\, d\xi\, d\eta, \tag{2.4}$$

donde $\mathcal{F}A$ es la transformada de Fourier de A. Enseguida reemplazamos de manera *formal* a las variables x y p por los operadores $\hat{X}$ y $\hat{P}$[1], para obtener al operador $\hat{A}$ correspondiente:

$$\hat{A}(\hat{X},\hat{P}) = \frac{1}{(2\pi\hbar)^n} \int_{\mathbb{R}^{2n}} \mathcal{F}A(\xi,\eta) e^{\frac{i}{\hbar}(\xi \hat{X} + \eta \hat{P})}\, d\xi\, d\eta. \tag{2.5}$$

Para darle un sentido riguroso a la integral es necesario pedir ciertas condiciones de regularidad a la función A. En la literatura matemática generalmente se comienza por definir la transformación de Weyl sobre el espacio de las funciones rápidamente decrecientes $\mathcal{S}(\mathbb{R}^{2n}) \subset L^2(\mathbb{R}^{2n})$ y luego se extiende a las funciones cuadraticamente integrables y por dualidad a las distribuciones templadas $\mathcal{S}'(\mathbb{R}^{2n})$. Evitaremos hablar de éstos detalles importantes para no extender el tema incesesariamente. El operador exponencial que aparece en el integrando de (2.5) se conoce como el operador característico de Moyal (ó operador característico de Weyl).

Definición 7. *El operador $\hat{M}(\xi,\eta) : L^2(\mathbb{R}^n) \to L^2(\mathbb{R}^n)$ definido como*

$$\hat{M}(\xi,\eta) = e^{\frac{i}{\hbar}(\xi \hat{X} + \eta \hat{P})},$$

se conoce como el operador característico de Moyal (entre otros nombres). Actúa sobre alguna función $\psi \in L^2(\mathbb{R}^n)$ de la siguiente manera:

$$\hat{M}(\xi,\eta)\psi(x) = e^{\frac{i}{2\hbar}\xi\eta} e^{\frac{i}{\hbar}\xi x} \psi(x+\eta). \tag{2.6}$$

Utilizando la definición del operador $\hat{M}(\xi,\eta)$, podemos definir de manera operacional a la transformación de Weyl sobre en subespacio apropiado de $L^2(\mathbb{R}^n)$.

[1] Ésto corresponde con el orden simétrico de Weyl.

Definición 8. *Sea $A \in \mathcal{S}(\mathbb{R}^{2n})$. El operador de Weyl, $\hat{A} = \mathrm{Op}_W(A)$ del símbolo A se define para un $\psi \in \mathcal{S}(\mathbb{R}^n)$ apropiado como*

$$\hat{A}\psi(x) = \frac{1}{(2\pi\hbar)^n} \int_{\mathbb{R}^{2n}} \mathcal{F}A(\xi,\eta)\hat{M}(\xi,\eta)\psi(x)\, d\xi\, d\eta. \tag{2.7}$$

Es más común expresar a la transformación de Weyl en términos del símbolo A directamente, sin recurrir a la transformada de Fourier. Utilizando la definición de $\mathcal{F}$, de manera formal tenemos:

$$\begin{aligned}
\mathrm{Op}_W(A) &= \frac{1}{(2\pi\hbar)^n} \int_{\mathbb{R}^{2n}} \mathcal{F}A(\xi,\eta)\hat{M}(\xi,\eta)\, d\xi\, d\eta \\
&= \frac{1}{(2\pi\hbar)^n} \int_{\mathbb{R}^{2n}} \left(\int_{\mathbb{R}^{2n}} A(x,p) e^{-i(\xi x+\eta p)}\, dx\, dp \right) \hat{M}(\xi,\eta) d\xi\, d\eta \\
&= \frac{1}{(2\pi\hbar)^n} \int_{\mathbb{R}^{2n}} A(x,p) \left(\int_{\mathbb{R}^{2n}} e^{-i(\xi x+\eta p)} \hat{M}(\xi,\eta)\, d\xi\, d\eta \right) dx\, dp \\
&= \frac{1}{(2\pi\hbar)^n} \int_{\mathbb{R}^{2n}} A(x,p)\hat{\Delta}(x,p)\, dx\, dp.
\end{aligned}$$

El la literatura matemática, el operador $\hat{\Delta}(x,p)$ se conoce como el operador de Grossmann-Royer y generalmente se denota $\hat{R}(x,p)$. En la literatura física comunmente es llamado el operador puntual de cuantización o del espacio de fase, ó el núcleo de la transformación de Wigner. Formalmente se puede ver como la transformada de Fourier del operador característico de Weyl $\hat{M}(\xi,\eta)$:

$$\hat{\Delta}(x,p) = \int_{\mathbb{R}^{2n}} e^{-i(\xi x+\eta p)} \hat{M}(\xi,\eta)\, d\xi\, d\eta. \tag{2.8}$$

Resulta que el mismo operador puntual puede ser utilizado para definir la transformación de Wigner, vinculando de manera muy natural a dicha transformación con la transformación de Weyl. Hemos presentado la idea de la cuantización de Weyl para motivar la introducción del operador puntual $\hat{\Delta}$, pero existe otra forma de expresar a los operadores puntuales $\Delta(x,p)$ particularmente iluminadora para nuestros objetivos, por medio de los operadores de Heisenberg-Weyl, conocidos también como los operadores de desplazamiento. Despues de reformular a los operadores puntuales en términos de los operadores de desplazamiento, podremos definir la transformación de Wigner de un estado ψ, en una forma que se preservará a la hora de pasar al caso discreto.

2.2.2. Los operadores puntuales del espacio de fase

Los operadores de Heisenberg-Weyl son muy estudiados en la mecánica cuántica, pues son operadores unitarios sobre $L^2(\mathbb{R}^n)$ que pueden ser utilizados para definir al grupo de Heisenberg y son una representación del grupo de Galilei, las cuales corresponden a traslaciones en el espacio de fase [23].

Definición 9. *El operador de Heisenberg-Weyl $\hat{D}(\xi,\eta)$ se define como*

$$\hat{D}(\xi,\eta)\psi(x) = e^{\frac{i}{\hbar}(\eta x - \frac{1}{2}\eta\xi)}\psi(x-\xi). \tag{2.9}$$

Equivalentemente se puede expresar como

$$\hat{D}(\xi,\eta)\psi(x) = e^{\frac{i}{\hbar}\sigma((\xi,\eta),(\hat{x},\hat{p}))}\psi(x), \tag{2.10}$$

donde $\sigma((x,p),(x',p')) = p\cdot x' - p'\cdot x$, es una forma simpléctica en el espacio de fase.

Proposición 3. *Los operadores de desplazamiento satisfacen las siguientes propiedades. Para todo $\psi, \phi \in L^2(\mathbb{R}^n)$ y $z_0, z_1 \in \mathbb{R}^{2n}$, los operadores $\hat{D}(z_0)$ son:*

1. *Lineales.*
$$\hat{D}(z_0)(\lambda\psi + \mu\phi) = \lambda\hat{D}(z_0)\psi + \mu\hat{D}(z_0)\phi, \quad \lambda, \mu \in \mathbb{C}\,. \tag{2.11}$$

2. *Unitarios.*
$$\hat{D}(z_0)^{-1} = \hat{D}(-z_0) = \hat{D}(z_0)^*. \tag{2.12}$$

3. *Satisfacen la relación de conmutatividad:*
$$\hat{D}(z_0)\hat{D}(z_1) = e^{\frac{i}{\hbar}\sigma(z_0,z_1)}\hat{D}(z_1)\hat{D}(z_0). \tag{2.13}$$

4. *Satisfacen la relación de composición:*
$$\hat{D}(z_0 + z_1) = e^{-\frac{i}{2\hbar}\sigma(z_0,z_1)}\hat{D}(z_0)\hat{D}(z_1). \tag{2.14}$$

Una versión análoga de la proposición (3) volverá a aparecer cuando pasemos a un espacio discreto. Utilizando a los operadores de desplazamiento, ahora definimos el operador de *Grossmann-Royer*, actuando sobre un operador de *paridad* $\hat{\Delta}(0,0)$ bajo la conjugación de un operador de desplazamiento.

Definición 10. *El operador de Grossmann-Royer $\hat{\Delta}(\xi, \eta)$ es el operador*
$$\hat{\Delta}(\xi, \eta) : \mathcal{S}(\mathbb{R}^n) \to \mathcal{S}(\mathbb{R}^n) \tag{2.15}$$
definido por las formulas
$$\hat{\Delta}(0,0)\psi(x) = \psi(-x), \tag{2.16}$$
y
$$\hat{\Delta}(\xi, \eta) = \hat{D}(\xi, \eta)\hat{\Delta}(0,0)\hat{D}(\xi, \eta)^{-1}, \tag{2.17}$$
donde $\hat{D}$ es el operador de Heisenberg-Weyl. El operador de Grossmann-Royer es unitario y es una involución en el espacio de Schwartz. Su acción sobre cualquier función $\psi : \mathbb{R}^n \to \mathbb{C}$ está dado por
$$\hat{\Delta}(\xi, \eta)\psi(x) = e^{\frac{2i}{\hbar}\eta(x-\xi)}\psi(2\xi - x). \tag{2.18}$$

Elegimos la notación $\hat{\Delta}$ porque los operadores de Grossmann-Royer son precisamente los operadores puntuales definidos en la sección anterior. El uso de los operadores puntuales nos dará una expresión bastante sencilla de la función de Wigner de un estado cuántico, y además, muchas de las propiedades interesantes de la función de Wigner se heredan de las siguientes propiedades de los operadores puntuales.

Proposición 4. *Para todo $\psi, \phi \in L^2(\mathbb{R}^n)$ y $z_0, z_1 \in \mathbb{R}^{2n}$, los operadores puntuales $\hat{\Delta}(z_0)$ son:*

1. *Lineales.*

2. *Unitarios.*

3. *Satisfacen la relación de composición:*
$$\hat{\Delta}(z_0)\hat{\Delta}(z_1) = e^{-\frac{2i}{\hbar}\sigma(z_0,z_1)}\hat{\Delta}(2(z_0 - z_1)). \tag{2.19}$$

Para ciertos operadores sobre $\mathcal{H}$, es posible invertir la transformación de Weyl, un ejemplo del proceso que se conoce como *decuantización*. De manera precisa, para un operador que admite una representación integral, podemos construir un símbolo que es integrable en el espacio de fase. Al símbolo obtenido a partir del operador de Weyl se conoce como símbolo de Weyl. Ésto nos dice que existe una correspondencia entre los símbolos cuadracticamente integrables sobre el espacio de fase y una clase de operadores acotados de $L^2(\mathbb{R}^n)$ [24]. Gosson demuestra en partícular, que la transformación de Weyl de una función cuadraticamente integrable corresponde a un operador Hilbert-Schmidt.

Definición 11. *Un operador de Hilbert-Schmidt es un operador acotado $\hat{A} : \mathcal{H} \to \mathcal{H}$ que tiene una norma de Hilbert-Schmidt finita. La norma de Hilbert-Schmidt se define como:*

$$\|\hat{A}\|_{HS}^2 = \sum_{i \in I} \|\hat{A}e_i\|_{\mathcal{H}}^2, \tag{2.20}$$

donde $\{e_i : i \in I\}$ es un base ortonormal del espacio de Hilbert $\mathcal{H}$. En dimensión finita, la norma de Hilbert-Schmidt es idéntica a la norma de Frobenius.

Los operadores de densidad son un ejemplo de operadores Hilbert-Schmidt por lo tanto pueden ser transformados a un símbolo en el espacio de fase. El proceso de la decuantización comunmente se realiza (al menos de manera formal) a través de la siguiente fórmula para un operador de Weyl $\mathrm{Op}_W(A)$:

$$A(x,p) = \mathrm{Tr}\left(\Delta(x,p)\,\mathrm{Op}_W(A)\right). \tag{2.21}$$

Ésta expresión solo tiene sentido riguroso de manera obvia cuando $\mathrm{Op}_W(A)$ tiene traza finita, entre otros requerimientos. De nuevo los operadores de densidad satisfacen los requisitos, por lo que se puede utilizar dicha fórmula para obtener el símbolo correspondiente. Resulta que para un estado cuántico, el símbolo que se obtiene de ésta manera es precisamente la función de Wigner.

Resumiendo ésta sección, hemos introducido a los operadores puntuales por medio de la cuantización de Weyl, y en el camino hemos definido a los operadores de desplazamiento. En la siguiente sección por fin definimos la función de Wigner en la manera en que se usará en el resto del trabajo.

2.3. La transformación de Wigner

Lo que sigue está basado principalmente en los libros de Gosson [25] y de Folland [16], quienes introducen la función de Wigner de manera general, en el contexto del análisis armónico. Nosotros adaptamos el formalismo que ellos emplean en el contexto de la mecánica cuántica.

Definición 12. *La transformación de Wigner es una transformación integral*

$$W : L^2(\mathbb{R}^n) \to L^2(\mathbb{R}^{2n}), \tag{2.22}$$

definida como

$$W(\psi)(x,p) = (2\pi\hbar)^{-n} \int_{\mathbb{R}^n} e^{-\frac{i}{\hbar}p\cdot y}\psi(x+\tfrac{1}{2}y)\overline{\psi(x-\tfrac{1}{2}y)}\,dy, \tag{2.23}$$

para $\psi \in L^2(\mathbb{R}^n)$ y $x, p \in \mathbb{R}^n$.

Denotaremos a la *función de Wigner* de una función ψ por el símbolo W_ψ. Utilizando los operadores puntuales definidos en la sección anterior, se puede demostrar fácilmente que la expresión (2.23) es equivalente a la siguiente expresión.

Definición 13. *Sea $\psi \in \mathcal{S}(\mathbb{R}^n)$ y $\hat{\Delta}(x,p)$ el operador puntual correspondiente al punto (x,p) del espacio de fase. La transformación de Wigner $W : \psi \mapsto W_\psi$ se puede definir como*

$$W(\psi)(x,p) = \frac{1}{(\pi\hbar)^n} \langle \psi | \hat{\Delta}(x,p)\psi \rangle \, . \tag{2.24}$$

La transformación de Wigner satisface varias propiedades interesantes, por ejemplo, para $\psi \in L^2(\mathbb{R}^n)$, es real valuada, acotada y continua. Las demostraciones se pueden encontrar en el libro de Gosson [24].

Proposición 5. *Si $\psi \in L^2(\mathbb{R}^n)$, entonces $W_\psi = \overline{W_\psi}$, por lo tanto W_ψ es real-valuada.*

Proposición 6. *Sean $\psi \in L^2(\mathbb{R}^n)$ y supongamos que su función de Wigner es absolutamente integrable, i.e., $W_\psi \in L^1(\mathbb{R}^{2n})$. Entonces $W_\psi \in L^1(\mathbb{R}^{2n})$ y*

$$\int_{\mathbb{R}^{2n}} W_\psi(x,p)\, dx\, dp = \|\psi\|^2_{L^2(\mathbb{R}^n)}. \tag{2.25}$$

Debido a que los operadores puntuales se obtienen a partir de desplazamientos, la función de Wigner tiene una propiedad a la que se le llama *covarianza bajo traslaciones.*

Proposición 7. *Para todo $\psi \in L^2(\mathbb{R}^n)$ y $z_0 = (x_0, p_0) \in \mathbb{R}^{2n}$ tenemos que*

$$W(\hat{D}(z_0)\psi)(z) = T(z_0)W_\psi(z), \tag{2.26}$$

donde $T(z_0)$ es una traslación en el espacio de fase, $z \mapsto z + z_0$, y sobre funciones definidas en $\mathbb{R}^{2n}$ actúa como $T(z_0)f(z) = f(z - z_0)$.

Ésta propiedad nos dice que un desplazamiento de la función de ψ por el operador $D(z_0)$ en el espacio de Hilbert $L^2(\mathbb{R}^n)$, simplemente corresponde a una traslación de la función de Wigner en el espacio de fase. De hecho, la transformación de Wigner es covariante bajo transformaciones simplécticas debido a que los operadores puntuales lo son [25].

Por otro lado, las siguientes propiedades justifican la utilidad de la función de Wigner, pues nos brindan una manera de dar la interpretación probabilística requerida de la mecánica cuántica.

Proposición 8. *La norma de la función de Wigner es proporcional a la norma de la función ψ:*

$$\|W_\psi\|_{L^2(\mathbb{R}^{2n})} = (2\pi\hbar)^{-n/2}\|\psi\|_{L^2(\mathbb{R}^n)}. \tag{2.27}$$

Proposición 9. *Supongamos que $\psi \in L^1(\mathbb{R}^n) \cap L^2(\mathbb{R}^n)$. Entonces*

$$\int_{\mathbb{R}^n} W_\psi(x,p)\, dp = |\psi(x)|^2, \quad \int_{\mathbb{R}^n} W_\psi(x,p)\, dx = |(\mathcal{F}\psi)(p)|^2. \tag{2.28}$$

La proposición (9) es una de las propiedades más importantes de la función de Wigner. Ésta propiedad nos dice que al integrar sobre el eje del momentum p, obtenemos la densidad de la función de onda en la representación de la posición. Similarmente, si integramos sobre el eje de la posición x, obtenemos la densidad de probabilidad de

la transformada de Fourier de la función de onda, es decir de la función de onda en el espacio del momentum. Resulta que ésto es un caso particular de una propiedad más general de la función de Wigner: integrando sobre franjas rectas en el espacio de fase nos dará la probabilidad de medir una clase de operadores en ciertos estados. Investigaremos ésta propiedad con más detalle más adelante pues es parte crucial a la hora de hacer la construcción discreta.

Por el momento solo hemos definido la función de Wigner para funciones cuadráticamente integrables. Recordemos de la sección preliminar, que los estados cuánticos puros se identifican con proyecciones ortogonales Π_ψ hacía el rayo $\mathbb{C}\,\psi = \{\lambda\psi : \lambda \in \mathbb{C}\}$ donde $\psi \in \mathcal{H}$. Utilizando la expresión de la transformación de Weyl en términos del núcleo integral de un operador, es fácil probar que la proyección ortogonal Π_ψ sobre el rayo $\mathbb{C}\,\psi$ es el operador de Weyl cuyo símbolo π_ψ está dado por la transformación de Wigner de ψ, i.e.,

$$\pi_\psi = (2\pi\hbar)^n W_\psi, \quad \text{donde } \operatorname{Op}_W(\pi_\psi) = \Pi_\psi. \tag{2.29}$$

Con ésto podemos identificar un estado cuántico puro ψ con su función de Wigner y vice-versa, ya que la función de Wigner contiene la misma información que el estado cuántico, solo en una representación en el espacio de fase. Utilizando los operadores puntuales, de la ecuación (2.24) podemos ver que la función de Wigner de un estado puro no es nada más que el valor esperado del operador puntual en el estado ψ.

Ahora consideremos un estado mixto $\{(\psi_j, p_j)\}$, el cual sabemos que se puede identificar con el operador dado por la suma de proyecciones ortogonales:

$$\rho = \sum_j p_j \Pi_j, \tag{2.30}$$

conocido como el operador de densidad. Dada la expresión del operador de densidad como una serie convergente de proyecciones ortogonales, es natural *definir* la función de Wigner de un operador de densidad como

$$W_\rho := \sum_j p_j W_{\psi_j}, \tag{2.31}$$

donde los ψ_j son los estados puros que conforman el estado mixto. La serie W_ρ converge en $L^2(\mathbb{R}^{2n})$ y

$$W_\rho \in L^2(\mathbb{R}^{2n}) \cap L^\infty(\mathbb{R}^{2n}). \tag{2.32}$$

A pesar de lo natural que es la definición anterior, no es la definición predominante en la literatura física. Ésto se debe a que su uso está limitado a estados cuánticos, y en general nos interesa calcular la transformación de Wigner de operadores (adecuados) arbitrarios. En su lugar, podemos expresar la función de Wigner como el valor esperado del operador puntual en el estado mixto, por medio de la traza.

Definición 14. *Sea ρ un operador de densidad correspondiente a un estado cuántico. La función de Wigner del estado ρ está dada por:*

$$W_\rho(x,p) = \frac{1}{2\pi\hbar} \operatorname{Tr}\left(\rho\hat{\Delta}(x,p)\right). \tag{2.33}$$

Notemos que ésta definición se reduce a la definición (2.24) para un estado puro, ya que el operador de densidad correspondiente a un estado ψ es simplemente la proyección $|\psi\rangle\langle\psi|$.

Recordemos que una motivación inicial para la definición de la distribución de Wigner es poder calcular valores esperados de observables cuánticos mediante integrales en el espacio de fase. Considerando un operador de Weyl $\hat{A} = \mathrm{Op}_W(A)$ de un símbolo A, podemos utilizar la transformación de Wigner para calcular el valor esperado de $\hat{A}$ en un estado ψ al integrar el producto de A con W_ψ sobre todo el espacio de fase.

Proposición 10. *Sea $A \in \mathcal{S}(\mathbb{R}^{2n})$. Entonces el valor esperado de $\hat{A} = \mathrm{Op}_W(A)$ en el estado ψ es*

$$\langle \hat{A} \rangle_\psi = \int_{\mathbb{R}^{2n}} A(x,p) W_\psi(x,p)\, dx\, dp. \tag{2.34}$$

Ésta propiedad se conoce como la propiedad de *traslape* en literatura física. Gosson menciona que muchas veces se *define* la transformación de Wigner W mediante el producto interno anterior. No es necesario limitarnos a valores esperados de observables en estados cuánticos, para operadores de Weyl que son de Hilbert-Schmidt, podemos calcular su traslape de una manera análoga a (10):

Proposición 11. *Sean $\hat{A} = \mathrm{Op}_W(a)$ y $\hat{B} = \mathrm{Op}_W(b)$ operadores de Hilbert-Schmidt. Entonces*

$$\mathrm{Tr}\left(\hat{A}\hat{B}\right) = \mathrm{Tr}\left(\hat{B}\hat{A}\right) = \frac{1}{(2\pi\hbar)^n} \int_{\mathbb{R}^{2n}} a(z) b(z)\, dz. \tag{2.35}$$

En la siguiente sección mostramos un ejemplo sencillo de la función de Wigner para darnos una idea intuitiva de lo que representa en el espacio de fase. Despues vamos a resumir las propiedades interesantes de la distribución de Wigner de una manera más informal, incluyendo las que hemos visto en ésta sección. Ésto lo hacemos con la finalidad de extraer las propiedades que nos interesan preservar a la hora de definir una función de Wigner discreta.

Ejemplo 1. *Como ejemplo consideraremos el oscilador armónico de una partícula en una dimensión. El oscilador armónico es un modelo muy importante en un gran número de áreas de la física. El Hamiltoniano asociado a éste sistema es*

$$\hat{H} = \frac{\hat{p}^2}{2m} + \frac{m\omega^2}{2}\hat{x}^2, \tag{2.36}$$

donde m y ω son constantes positivas. El espectro del Hamiltoniano es discreto y resolviendo la ecuación independiente del tiempo obtenemos los eigenvalores y los eigenvectores. Introduciendo una constante para simplificar los cálculos

$$a = \sqrt{\frac{\hbar}{m\omega}},$$

obtenemos los niveles de energía

$$E_n = \hbar\omega\left(n + \frac{1}{2}\right), \quad n = 0, 1, 2, \ldots \tag{2.37}$$

con sus correspondientes eigenvectores

$$\psi_n(x) = \frac{1}{\sqrt{2^n n! a\sqrt{\pi}}} e^{-x^2/2a^2} H_n(x), \quad n = 0, 1, 2, \ldots \tag{2.38}$$

donde $H_n(x)$ es el n-ésimo polinomio Hermite. Como $H_0(x) = 1$, el estado "de piso" ψ_0 está dado por

$$\psi_0(x) = \frac{1}{\sqrt{a\sqrt{\pi}}} e^{-x^2/(2a^2)}.$$

Utilizando la definición (2.1), la función de Wigner para el estado ψ_0 está dado por

$$\begin{aligned}(W\psi_0)(x,p) &= \frac{1}{2\pi\hbar}\int_{\mathbb{R}} e^{-\frac{i}{\hbar}py}\psi(x+\tfrac{1}{2}y)\overline{\psi(x-\tfrac{1}{2}y)}\,dy \\ &= \frac{1}{2\pi\hbar}\int_{\mathbb{R}} e^{-\frac{i}{\hbar}py}\frac{1}{a\sqrt{\pi}}\exp\left(-\frac{x^2}{a^2}-\frac{y^2}{4a^2}\right)dy \\ &= \frac{1}{\pi\hbar}\exp\left(-\frac{a^2p^2}{\hbar^2}\right)\exp\left(-\frac{x^2}{a^2}\right).\end{aligned}$$

Se puede demostrar que la función de Wigner correspondiente al n-ésimo eigenestado del oscilador armónico se puede expresar en términos del n-ésimo polinomio de Laguerre [20],

$$(W\psi_n)(x,p) = \frac{(-1)^n}{\pi}\exp\left[-\left(\frac{x}{a}\right)^2-\left(\frac{ap}{\hbar}\right)^2\right]L_n\left[2\left(\frac{x}{a}\right)^2+2\left(\frac{ap}{\hbar}\right)^2\right]. \tag{2.39}$$

La figura (2.1) muestra la gráfica en el espacio de fase de las funciones de Wigner correspondientes a los estados ψ_3 y ψ_7. Notamos el incremento de oscilaciones de un estado a otro y la presencia de valores negativos.

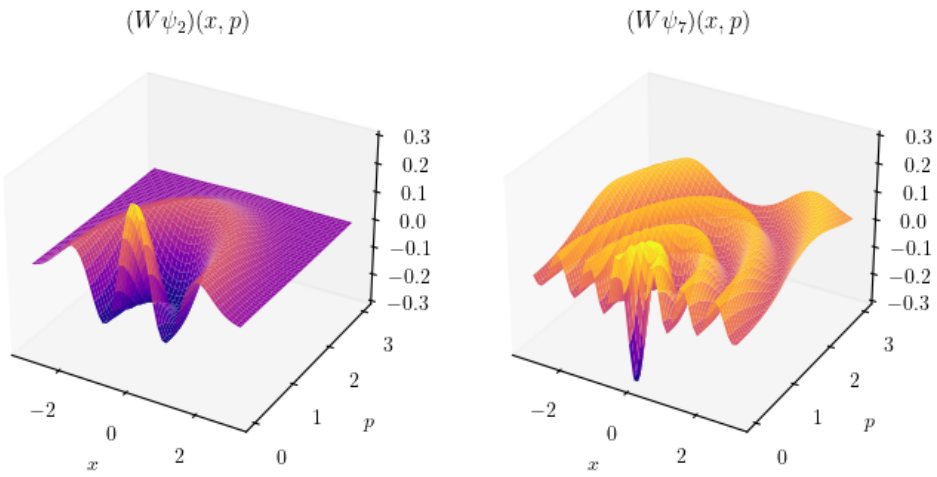


Figura 2.1: Funciones de Wigner de los estados ψ_3 y ψ_7 del oscilador armónico, con $\hbar = 1$ y $\omega = 1$.

2.3.1. La correspondencia de Stratonovich-Weyl y la propiedad tomográfica

Al inicio de éste capítulo mencionamos que existen diversas cuasi-distribuciones en el espacio de fase, las cuales son usadas para formar distintas representaciones de

la mecánica cuántica. Algunas se pueden obtener a partir de las distintas maneras de extender la correspondencia de Wigner-Weyl entre funciones sobre $\mathbb{R}^{2n}$ y operadores sobre $L^2(\mathbb{R}^n)$, a grupos de Lie que actúan sobre un espacio homogéneo[2]. Éstas distribuciones están relacionadas por algo que se conoce como la *correspondencia de Stratonovich-Weyl*, las cuales son un conjunto de propiedades o criterios razonables que una cuasi-distribución sobre un espacio de fase arbitrario debería satisfacer [26].

La idea básica es la siguiente[3]. Sea G un grupo de Lie y π una representación unitaria de G sobre el espacio de Hilbert $\mathcal{H}$. Sea $\mathcal{M}$ un G-espacio homogéneo y sea μ una medida G-invariante sobre $\mathcal{M}$. La correspondencia de Stratonovich-Weyl es un isomorfismo W del espacio de operadores sobre $\mathcal{H}$ al espacio de funciones sobre $\mathcal{M}$ que satisface las siguientes propiedades:

1. W mapea al operador de identidad de $\mathcal{H}$ a la función constante 1.

2. La función $W(A^*)$ es el conjugado complejo de $W(A)$.

3. W satisface la propiedad de covarianza:

$$W\left(\pi(g)A\pi(g)^{-1}\right)(u) = W(A)\left(g^{-1}u\right). \tag{2.40}$$

4. W satisface la propiedad de la traza:

$$\int_{\mathcal{M}} W(A)(u)W(B)(u)\,d\mu(u) = \mathrm{Tr}(AB), \tag{2.41}$$

para dos operadores A y B.

Notemos que la correspondencia de Weyl es un caso particular de la correspondencia de Stratonovich-Weyl. En éste caso G es el grupo de Heisenberg actuando sobre $\mathbb{R}^{2n}$ y π es la representación del grupo de Heisenberg, i.e., los operadores de Heisenberg-Weyl. El isomorfismo es la transformación de Wigner (equivalentemente, la transformación de Weyl), la cual satisface los criterios como hemos visto en la sección anterior.

Los criterios de Stratonovich-Weyl pueden ser expresados en términos de un *núcleo* integral, el cual es una función Ω de $\mathcal{M}$ al espacio de operadores de $\mathcal{H}$, tal que:

1. $\Omega(u)$ es auto-adjunto.

2. $\Omega(u)$ es de traza unitaria.

3. El núcleo satisface una propiedad de covarianza:

$$\pi(g)\Omega(u)\pi(g)^{-1} = \Omega(gu), \tag{2.42}$$

para todo $g \in G$.

4. Satisface la ecuación:

$$\int_{\mathcal{M}} \mathrm{Tr}\left(\Omega(u)\Omega(v)\right)\Omega(v)\,d\mu(v) = \Omega(u). \tag{2.43}$$

[2]Dentro de la teoría de grupos de Lie, formalmente un espacio homogéneo es una variedad $\mathcal{M}$ con una acción lisa y transitiva dada por un grupo de Lie G.

[3]Los detalles no son importantes para nuestros objetivos, por lo cual hemos asumido inecesario definir a los objetos que aperecen enseguida.

En nuestro caso, el núcleo está dado por los operadores puntuales $\hat{\Delta}(x,p)$. En el siguiente capítulo definiremos la función de Wigner para sistemas discretos, y seremos guiados por versiones análogas de las propiedades de Stratonovich-Weyl para la función de Wigner y para los operadores puntuales.

Ahora, existen algunas propiedades de la función de Wigner que la distingue de otras cuasi-distribuciones. En particular, satisface una a la que Wootters [6] le llama *propiedad proyectiva*.

Proposición 12. *Si W_ρ es la función de Wigner de un estado ρ, entonces podemos considerar la integral de W_ρ sobre una franja infinita delimitada por dos rectas paralelas $ax+bp=c_1$ y $ax+bp=c_2$. Resulta que la integral es igual a la probabilidad de que se observe un valor entre c_1 y c_2 del observable $a\hat{X}+b\hat{P}$.*

Ésta propiedad proyectiva se puede expresar en términos de los operadores puntuales. Las siguientes expresiones son formales e ignoramos los detalles de rigor que pudieran presentarse.

Proposición 13. *Para todo $x,p\in\mathbb{R}^n$ los operadores puntuales $\hat{\Delta}(x,p)$ satisfacen las siguientes propiedades:*

1. *Son "ortogonales" en el siguiente sentido:*

$$\mathrm{Tr}\left(\hat{\Delta}(x,p)\hat{\Delta}(x',p')\right)=\frac{1}{2\pi}\delta(x-x')\delta(p-p'). \tag{2.44}$$

2. *Integrando el operador puntual $\hat{\Delta}(x,p)$ sobre una recta $ax+bq=l$ en el espacio de fase nos brinda una proyección correspondiente al eigenestado de $a\hat{X}+b\hat{P}$ con eigenvalor l:*

$$\int_{\mathbb{R}^2}\hat{\Delta}(x,p)\delta(ax+bq-l)\,dx\,dp=\Pi_l. \tag{2.45}$$

La noción de un producto de deltas no tiene mucho sentido, pero la expresión análoga para el caso discreto está bien definida. La segunda propiedad nos dice que integrando el operador puntual sobre una linea en el espacio de fase, obtenemos una proyección. Como consecuencia, integrando la función de Wigner sobre una recta obtenemos una "densidad marginal" en la dirección de la linea recta. Ésto es una generalización de las densidades de posición y de momentum y se ha demostrado que imponiendo ésta propiedad a una cuasi-distibución adecuada del espacio de fase, se obtiene la distribución de Wigner, en otras palabras, ésta restricción adicional la vuelve única entre las cuasi-distribuciones [10]. Si tenemos un conjunto completo de éstas "marginales generalizadas", es decir, para todas las direcciones, podemos recuperar la distribución conjunta sobre todo el espacio en un proceso de tomografía cuántica.

Definición 15. *Dado un conjunto completo de densidades marginales, es posible recuperar la función de Wigner. A ésta propiedad se le conoce como la propiedad tomográfica de la función de Wigner.*

El término *completo* tiene un significado más preciso, pero no trivial, corresponde a una cantidad mínima de densidades marginales requeridas para la construcción completa del *tomograma* [27]. La representación tomográfica de estados cuánticos está basada en la transformación de Radon de la función de Wigner [28]. En la tomografía

convencional (la tomografía médica), se recolectan datos en forma de densidades marginales. En el plano, una marginal es la proyección de una función sobre el plano en la *dirección* indicada por un ángulo. La colección de marginales para distintos ángulos es la *transformación de Radon* de dicha función[4]. En el contexto de la mecánica cuántica tenemos la siguiente definición.

Definición 16. *La transformación de Radon $\mathcal{R}_\rho$ de una función de Wigner W_ρ de un estado ρ, está dada por*

$$\mathcal{R}_\rho\,(X,\mu,\nu) = \int_{\mathbb{R}^2} W_\rho(x,p)\delta(X-\mu x-\nu p)\,dx\,dp. \tag{2.46}$$

La transformación de Radon es invertible (bajo ciertas condiciones):

$$W_\rho(x,p) = \frac{1}{2\pi\hbar}\int_{\mathbb{R}^3} \mathcal{R}_\rho(X,\mu,\nu)e^{\frac{i}{\hbar}(X-\mu x-\nu p)}\,dX\,d\mu\,d\nu. \tag{2.47}$$

Experimentalmente se mide la transformación de Radón por medio de un proceso llamado el *método homodino*[5]. Al obtener una aproximación adecuada del tomograma, se invierte la transformación de Radon para obtener la función de Wigner. Como ya sabemos, la función de Wigner es un representación completa del estado cuántico asi que solo queda decidir si hacer mecánica cuántica en el espacio de fase o recuperar el operador de densidad y trabajar en el espacio de Hilbert. Ésto concluye el proceso de la tomografía cuántica.

A parte de versiones discretas de las propiedades de Stratonovich-Weyl, la propiedad tomográfica será fundamental en la construcción de una función de Wigner discreta bajo la metodología de Wootters. Dicha construcción será el contenido del siguiente capítulo.

[4]Resulta que las mediciones utilizadas son "mutuamente conjugadas" en el sentido de que los eigenestados de los operadores $a\hat{X}+b\hat{p}$ nos brindan una distribución uniforme del valor de $a'\hat{x}+b'\hat{p}$ siempre y cuando los vectores (a,b) y (a',b') sean en distintas direcciones. Notemos la similitud con el procedimiento de la determinación de estados mediante mediciones con bases mutuamente insesgadas.

[5]La palabra *homodino* se refiere a una comparación entre una luz que se mide contra una luz de referencia de la misma frecuencia.

Capítulo 3

Funciones de Wigner en el Espacio Fase Discreto

Durante las últimas decadas han existido múltiples intentos de generalizar la función de Wigner a sistemas cuánticos de dimensión finita. Parte fundamental de ésta generalización es la definición adecuada del espacio de fase discreto. Para un sistema de dimensión d, la mayoría de construcciones emplean una malla de tamaño $d \times d$ e intentan definir una función de Wigner evaluada en cada punto α de la malla. Como menciona Gross [29], parece que existen dos caminos claros en la construcción de la versión discreta: un camino intenta definir la función de Wigner discreta de una manera análoga a la versión continua, i.e., identificando el espacio de fase discreto con las variables de posición y de momentum, construyendo los operadores de desplazamiento y luego los puntuales, para luego definir la función por medio del valor esperado del operador puntual en el estado cuántico. La ventaja de éste camino es que la definición discreta asemeja lo más posible al caso continuo y a sus a interpretaciones. Ésta versión se puede encontrar en los trabajos de Klimov, Sanches-Soto [30], Paz [31], Vourdas [32], Gross [29], etc. El segundo camino dominante es el que intenta definir la función discreta a partir de la preservación de las propiedades más importantes del caso continuo, en particular la propiedad tomográfica. Ésta versión se debe a Wootters [33] y la idea es identificar una *estructura cuántica* al espacio de fase discreto, la cual permite que la función de Wigner exprese las mismas propiedades que la versión continua. Los operadores de desplazamiento y los puntuales vuelven a aparecer, pero se introduce un tipo de arbitrariedad y de flexbilidad, perdiendo la unicidad pero admitiendo una construcción alternativa. Además, ésta segunda metodología expone una relación directa con la construcción de bases mutuamente insesgadas.

Se sabe que el número máximo de bases mutuamente insesgados para un sistema cuántico de dimensión d es $d+1$, y en particular si la dimensión es una potencia de un número primo, entonces siempre se puede alcanzar la cantidad máxima [33]. Parece que aun es un problema abierto identificar la cantidad máxima para dimensiones que no son potencias de números primos. La construcción de Wootters requiere de la construcción explícita de las $d+1$ MUBs para la definición de los operadores puntuales y como consecuencia la definición de la función de Wigner. Ésto es una consecuencia natural de exigir que la función discreta satisfaga las mismas propiedades tomográficas que satisface la versión continua. Por éstas razones nuestro trabajo se basa en la metodología de Wootters.

3.1. Construcción de Wootters

En su artículo del 2004 [33], Wootters y Gibbons comienzan notando que la función de Wigner en sistemas continuos puede ser obtenida al exigir una estructura cuántica al espacio de fase. Ésta estructura corresponde a la asignación de estados cuánticos a rectas en el espacio de fase, de tal manera que las integrales sobre éstas rectas o franjas de rectas nos dan la probabilidad de observar el sistema en el estado correspondiente, tal como se mencionó en la sección anterior. Con ésta asignación, es posible recuperar los operadores puntuales y así construir la función de Wigner para un estado arbitrario ρ. Wootters y Gibbons intentan definir una versión discreta siguiendo éstos pasos, cuidando que la construcción preserve otras propiedades de la versión continua. Resulta que su método introduce cierto tipo de arbitrariedad por lo que acaban definiendo distintas clase de funciones discretas.

Evidentemente hay una relación directa entre la geometría del espacio de fase y la estructura cuántica por asignar. Por lo tanto requerimos trabajar con un espacio de fase que tenga la suficiente estructura geométrica como para definir rectas en el espacio con las propiedades usuales que conocemos del plano Euclideano. Por ejemplo debemos poder definir rectas paralelas y se debe cumplir que dos rectas no paralelas solo se intersecten en un solo punto. Si d es la dimensión del espacio de Hilbert en cuestión, es natural intentar definir el espacio de fase como la malla $\mathbb{Z}_d \times \mathbb{Z}_d$. Pero si d no es un número primo, $\mathbb{Z}_d$ solo es un anillo y resulta que el espacio $\mathbb{Z}_d \times \mathbb{Z}_d$ no tiene la estructura geométrica necesaria, por ejemplo no es dificil encontrar ejemplos de rectas no paralelas que se intersectan en más de un solo punto. En el caso en que $d = p$ es un número primo, la estructura algebráica $\mathbb{Z}_p$ es un campo y aquí sí se puede definir un espacio de fase $\mathbb{Z}_p \times \mathbb{Z}_p$ con las propiedades deseadas. Además de los campos $\mathbb{Z}_p$, también podemos obtener campos de orden p^n donde p es primo, por medio de la extension de Galois $\mathrm{GF}(p^n)$. La restricción a espacios de Hilbert dimensión p^n sí es limitante, pero Wootters hace la observación que su método es válido para el importante caso de un sistema de n qubits. Por lo tanto su metodología es directamente aplicable a los modelos de la computación e información cuántica.

El método consiste en darle una estructura cuántica al espacio de fase discreto $\mathbb{F} \oplus \mathbb{F}$ asignando un estado cuántico a cada linea del espacio. Ésta asignación debe satisfacer varias propiedades y aquellas que las satisfacen se llaman, *'mallas cuánticas'*. Cada malla cuántica define una versión de la función de Wigner, pero es posible hacer una clasificación en clases de equivalencia para reducir un poco la arbitrariedad. La asignación particular de estados cuánticos a las rectas de conjuntos de rectas paralelas resultan ser bases ortonormales del espacio de Hilbert y además son mutuamente insesgadas respecto a otros conjuntos de rectas paralelas.

Para comenzar, recordemos las propiedades de la función de Wigner del caso continuo que se deseamos perservar en el caso discreto, las primeras tres son las propiedades de Stratonovich-Weyl y la cuarta es la propiedad tomográfica de la función de Wigner:

Proposición 14. *Sea ρ un operador de densidad y W_ρ su función de Wigner.*

1. *W_ρ es covariante bajo traslaciones.*
2. *Los operadores puntuales forman una base ortonormal respecto al producto interno de Hilbert-Schmidt para el espacio de operadores sobre $\mathcal{H}$.*
3. *W_ρ es real y la integral sobre todo el espacio de fase es igual a 1.*

4. *La integral de W_ρ sobre una recta $ax+bp=c$ nos brinda la probabilidad de medir el valor c del operador $a\hat{X}+b\hat{P}$.*

Recordemos que éstas propiedades pueden ser demostradas a partir de las propiedades análogas de los operadores puntuales. En el caso continuo la propiedad proyectiva está relacionada directamente con los operadores $a\hat{X}+b\hat{P}$, en el caso discreto ésto ya no es el caso. De hecho, la asignación de un significado físico a los ejes del plano discreto es algo arbitrario. Como veremos más adelante, elegimos una base ortonormal arbitraria la cual se asigna al "eje horizontal". La base asignada al "eje vertical" será mutuamente insesgada a la horizontal, preservando de algun modo ésta idea de complementariedad. Eligiendo las bases correctamente para el resto de las rectas del espacio nos permitirá reconstruir un estado cuántico por medio de probabilidades medidas, tal como sucede en la tomografía cuántica en el caso continuo. Por otro lado, la propiedad de ser covariante bajo traslaciones surge naturalmente a partir de las propiedades de los operadores de desplazamiento y éstos son clave en la construcción de las bases.

3.1.1. La geometría del espacio de fase discreto

El espacio de fase discreto será un espacio vectorial de dos dimensiones sobre un campo finito $\mathbb{F}$, donde los puntos serán etiquetados con los elementos $(x,p)\in\mathbb{F}\oplus\mathbb{F}$. Por convención, consideramos el punto $(0,0)$ como el origen de nuestra malla de $d\times d$ elementos, ubicado en la parte inferior izquierda. La construcción de Wootters y Gibbons permite identificar el eje horizontal con los eigenvectores de una clase de operadores y el eje vertical con otra clase de operadores, ésto a su vez nos permite darle cierta interpretación física, aunque la asignación no es naturalmente única. Por ejemplo si consideramos un sistema cuántico de dos partículas con spin-1/2, entonces el espacio de Hilbert correspondiente es $\mathcal{H}=\mathbb{C}^2\otimes\mathbb{C}^2$, y el espacio de fase discreto sería una malla de 4×4 elementos. Salvo isomorfismos, el campo finito de cuatro elementos es único y lo identificamos con la extensión de Galois $\mathrm{GF}\left(2^2\right)$. Los elementos de la malla serán indexados por los elementos de éste campo:

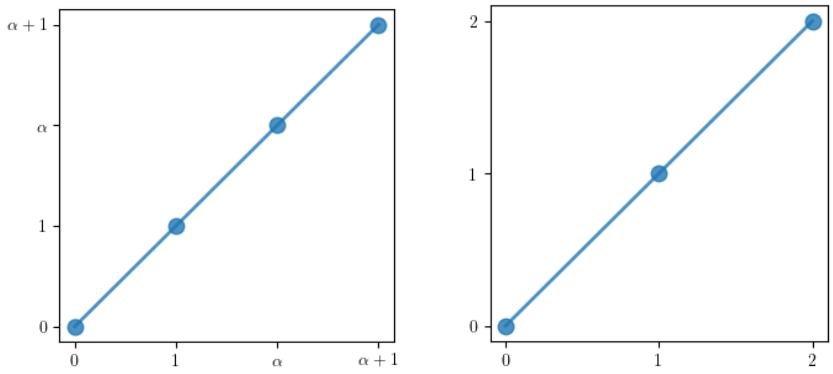
$$\mathbb{F}=\mathrm{GF}\left(2^2\right)=\{0,1,\alpha,\alpha+1\}.$$

En caso de un sistema que no es compuesto, por ejemplo una partícula de tres niveles, $\mathcal{H}=\mathbb{C}^3$, el espacio de fase discreto es una malla de 3×3 en donde los elementos de la malla son indexados simplemente con los enteros módulo 3, $\mathbb{F}=\mathbb{Z}_3=\{0,1,2\}$. La figura (3.1) muestra el espacio de fase de éstos dos ejemplos, y se muestra la linea recta parametrizada como

$$\lambda=\{(s,s):s\in\mathbb{F}\},$$

la cual corresponde con la noción de un rayo diagonal en el plano Euclideano. De manera general, una *recta* en el espacio de fase es el conjunto de puntos que satisfacen la ecuación $ax+bp=c$ donde a,b y c son elementos del campo finito. Dos rectas paralelas son iguales si solo difieren en el valor de c. No es dificil probar que dada una recta λ y un punto α que no pertenece a la recta existe una única recta paralela a λ que contiene a α. Similarmente, dos rectas que no son paralelas solo se intersectan en un solo punto. Existen $d(d+1)$ rectas en el espacio de fase y el conjunto de éstas rectas se particiona en $d+1$ conjuntos de d rectas paralelas. A cada conjunto de d rectas paralelas, se le conoce como un *estría*.

Para ejemplificar un conjunto completo de estrías de un espacio de fase discreto, consideremos un campo finito de ocho elementos. En éste caso el espacio de fase es el



(a) $\mathbb{F} \oplus \mathbb{F}$ donde $\mathbb{F} = \mathrm{GF}(2^2)$. (b) $\mathbb{F} \oplus \mathbb{F}$ donde $\mathbb{F} = \mathbb{Z}_3$.

Figura 3.1: Dos espacios de fase discretos para sistemas de distinta dimensión, señalando el rayo diagonal $y = x$.

espacio vectorial $\mathbb{F} \oplus \mathbb{F}$ donde $\mathbb{F} = \mathrm{GF}\left(2^3\right)$ es una extensión de Galois del campo primo $\mathbb{Z}_2$ de grado $n = 3$. De acuerdo al apéndice (A.2), para construir a $\mathbb{F}$ solo debemos elegir un polinomio irreducible $f(x)$ con coeficientes en $\mathbb{Z}_2$ de grado $n = 3$ y adjuntarle una raíz α del polinomio al campo primo. Equivalentemente podemos tomar el cociente del anillo de polinomios $\mathbb{Z}_2[x]$ con el ideal generado por el polinomio irreducible:

$$\mathbb{F} = \mathbb{Z}_2(\alpha) \cong \mathbb{Z}_2[x]/\langle f(x)\rangle. \tag{3.1}$$

Sea $f(x) = x^3 + x^2 + 1$ tal polinomio irreducible y α una raíz primitiva[1]. Entonces el campo finito $\mathbb{F}$ está dado por el conjunto

$$\mathbb{F} = \{0, 1, \alpha, \alpha^2, \alpha + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1, \alpha^2 + 1\}, \tag{3.2}$$

con sus correspondientes operaciones de suma y mutliplicación. Las rectas verticales estarán dadas por los conjuntos $\{(x, y) : y \in \mathbb{F}\}$ donde fijamos el elemento x para cada recta vertical. El resto de las rectas pueden ser parametrizadas como $\{(x, mx + c) : m, c \in \mathbb{F}\}$. La figura (3.2) muestra todas las estrías de éste espacio de fase. Otro aspecto importante inicial en la metodología de Wootters es la noción de las traslaciones en el espacio de fase. En el caso discreto no existen traslaciones infinitesimales, pero podemos definir una traslación como la suma de un vector a los puntos del espacio de fase. Si $(a, b) \in \mathbb{F} \oplus \mathbb{F}$, entonces la traslación $\mathcal{T}(a, b)$ se define simplemente como

$$[\mathcal{T}(a, b)](c, d) = (a + c, b + d), \quad \text{para todo } (c, d) \in \mathbb{F} \oplus \mathbb{F}\,. \tag{3.3}$$

Se sigue inmediatamente que la composición de traslaciones en el espacio de fase discreto se rige bajo la siguiente regla. Para todo $(a, b), (c, d) \in \mathbb{F} \oplus \mathbb{F}$ tenemos que

$$\mathcal{T}(a, b) \circ \mathcal{T}(c, d) = \mathcal{T}(a + c, b + d). \tag{3.4}$$

La metodología de Wootters inicia haciendo una correspondencia entre las traslaciones en el espacio de fase con operadores en el espacio de Hilbert, de manera análoga al caso continuo. En el artículo original, no mencionan las representaciones unitarias del grupo

[1] Todos los polinomios elegidos en éste trabajo son los de Conway

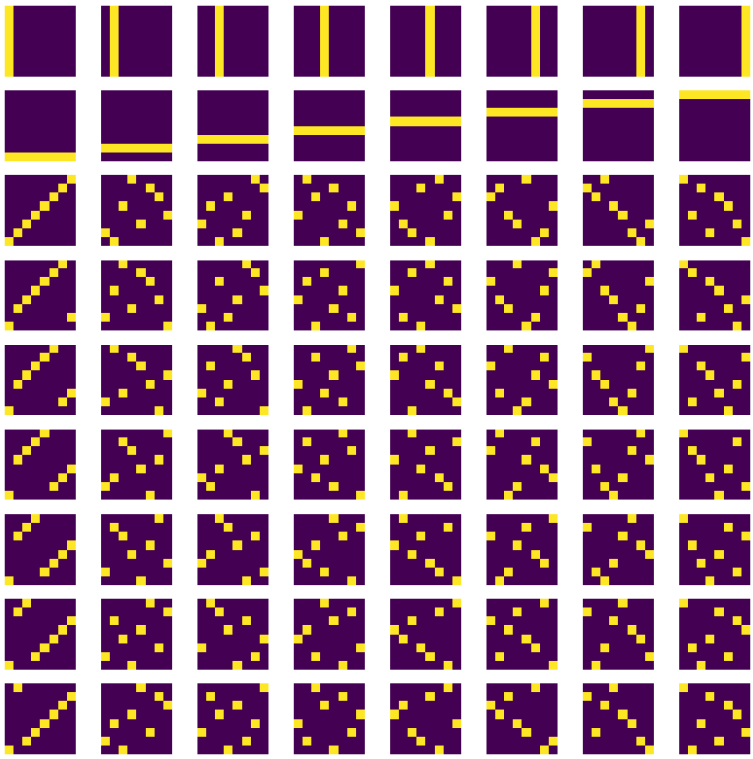


Figura 3.2: Las nueve estrías del espacio de fase sobre el campo $\mathbb{F} = \mathrm{GF}\left(2^3\right)$. La primera columna consta de los rayos y el resto de las columnas representan las traslaciones paralelas de cada rayo.

de traslaciones a la hora de definir a los operadores de desplazamiento, ya que para asignar la malla cuántica no es necesario utilizar a toda la representación pues las fases globales se ignoran. Para ver una construcción más fiel al caso continuo recomendamos ver el trabajo de Vourdas [32].

3.1.2. Asignación de la estructura cuántica

Para vincular el sistema cuántico con nuestro espacio de fase discreto, la clave del método Wootters y Gibbons es asignar un estado cuántico a cada una de las $d(d+1)$ lineas rectas del espacio de fase. De aquí en adelante consideramos un sistema cuántico modelado por un espacio de Hilbert de dimensión $d = p^n$ donde p es un número primo. Éste método es aplicable de manera natural a sistemas compuestos de n subsistemas de dimensión p:

$$\mathcal{H}^{\otimes n} = \mathcal{H} \otimes \cdots \otimes \mathcal{H}, \quad \text{donde } \dim \mathcal{H} = p. \tag{3.5}$$

Sea Q la malla cuántica, la cual asigna una proyección ortogonal correspondiente a un estado puro $Q(\lambda)$, a cada recta λ y que satisface ciertas propiedades. La primera propiedad que debe satisfacer la malla cuántica es la propiedad de ser covariante bajo traslaciones, para ésto, debemos definir una versión discreta de los operadores de Heisenberg-Weyl $\hat{D}(x,p)$ para cada $(x,p) \in \mathbb{F} \oplus \mathbb{F}$. De ésta manera a cada traslación en el espacio de fase discreto le corresponderá un operador unitario en el espacio de Hilbert. Éstos operadores deben tener una regla de composición que preserve de algún modo la composición de traslaciones en el espacio de fase.

Como mencionamos en la sección anterior, Wootters et al no mencionan a los operadores de Heisenberg-Weyl como comunmente se hace en el caso continuo. En su lugar, construyen a los operadores de desplazamiento de una manera ad-hoc, enfocándose en sistemas de dimensión prima, en donde el espacio de fase discreto es simplemente el campo finito $\mathbb{F} = \mathbb{Z}_p$, y luego utilizando el producto tensorial para obtener los operadores para dimensiones compuestas. Por el momento seguimos éste camino. Comenzamos por definir a dos operadores básicos, correspondientes a traslaciones horizontales y verticales de una unidad. A la traslación horizontal del espacio de fase $\mathcal{T}(1,0)$ y la traslación vertical $\mathcal{T}(0,1)$ les asociamos los operadores unitarios X y Z definidos de la siguiente manera:

Definición 17. *Sea $\{|k\rangle : k \in \mathbb{Z}_p\}$ una base ortonormal del espacio de Hilbert $\mathcal{H}$ correspondiente a un subsistema (generalmente usaremos la base estándar). Etiquetamos a los vectores con los elementos del campo primo. Entonces definimos los operadores X y Z como*

$$X\,|k\rangle = |k+1\rangle\,, \tag{3.6}$$

$$Z\,|k\rangle = \omega^k\,|k\rangle\,, \tag{3.7}$$

donde $\omega = e^{2\pi i/p}$ y donde la suma dentro de los kets se hace módulo p, i.e., la suma es la del campo finito $\mathbb{Z}_p$.

El uso de los números del campo primo como etiquetas implica una estructura cíclica a las potencias del operador X y comunmente se le llama el operador *shift* porque en el caso continuo representan cambios en la posición. Similarmente el operador Z se le conoce como el operador *boost* porque en el caso continuo representa un empuje en términos del momentum. Podemos expresar a éstos operadores en la base estándar de la siguiente manera:

$$X = \sum_{k\in\mathbb{Z}_p} |k+1\rangle\langle k|\,, \quad Z = \sum_{k\in\mathbb{Z}_p} \omega^k\,|k\rangle\langle k|\,. \tag{3.8}$$

Es fácil probar las siguientes propiedades de los operadores X y Z:

Proposición 15. *Sea $|k\rangle$ un elemento de la base estándar y $a, b \in \mathbb{F}$, entonces*

1. *$X^a\,|k\rangle = |k+a\rangle$ y $Z^b\,|k\rangle = \omega^{bk}\,|k\rangle$.*
2. *$X^p = Z^p = 1$, $X^a Z^b = \omega^{-ab} Z^b X^a$, y $\mathrm{Tr}(X) = \mathrm{Tr}(Z) = 0$.*

Ejemplo 2. *En el caso de dimensión $p = 2$, los monomios de X y Z son elementos del grupo de Pauli. En particular las matrices X y Z son simplemente las matrices de Pauli σ_x y σ_z:*

$$X = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

La matriz Z es diagonal en la base estándar por lo tanto sus eigenvectores son simplemente los elementos $|k\rangle$. La matriz X es diagonal respecto a la siguiente base:

$$|\tilde{j}\rangle = \frac{1}{\sqrt{p}} \sum_{k\in\mathbb{Z}_p} \omega^{jk}\,|k\rangle\,,$$

donde la tilde se usa para distingir ésta base de la base estándar. Notemos que ésta última expresión parece una transformación de Fourier de la base computacional. De hecho Vourdas y otros autores definen una transformación de Fourier finita a partir de los caracteres aditivos χ del campo finito y construyen una segunda base del espacio de Hilbert mediante su aplicación. De ésta manera obtienen dos bases "Fourier conjugables" y las asocian con la noción de posición (base computacional) y momentum (base obtenida por la transformación de Fourier) en el espacio de fase discreto. A pesar de ésto Klimov et al. hacen la observación que debido a la arbitrariedad de las bases, la analogía con la posición y momentum en el espacio de fase discreto es un poco forzada [34]. Otra propiedad interesante de éstas dos bases surge del siguiente cálculo:

$$\langle m|\tilde{j}\rangle = \frac{1}{\sqrt{p}} \sum_{k\in\mathbb{Z}_p} \omega^{jk} \langle m|k\rangle = \frac{1}{\sqrt{p}}\omega^{jm}, \tag{3.9}$$

por lo tanto $\left|\langle m|\tilde{j}\rangle\right|^2 = \frac{1}{p}$. En otras palabras, las bases $|k\rangle$ y $|\tilde{j}\rangle$ son mutuamente insesgadas. Más adelante construiremos más bases a partir de subconjuntos de los operadores de desplazamiento y para sistemas con dimensión p^n, todas éstas bases serán mutuamente insesgadas.

Los operadores de desplazamiento están en correspondencia con las traslaciones del espacio de fase discreto. Sean $a, b \in \mathbb{F}$, utilizando la proposición (15) naturalmente definimos a los operadores de desplazamiento correspondientes a una traslación $\mathcal{T}(a, b)$ como

$$D(a, b) = X^a Z^b, \tag{3.10}$$

cuya acción sobre los elementos de la base estándar es

$$D(a, b)\,|k\rangle = X^a Z^b\,|k\rangle = X^a \omega^{bk}\,|k\rangle = \omega^{bk}\,|k + a\rangle\,.$$

Recordemos que para todo $(a, b), (c, d) \in \mathbb{F} \oplus \mathbb{F}$, las traslaciones satisfacen la regla de composición en (3.4), similarmente, los operadores de desplazamiento satisfacen la siguiente propiedad de composición:

$$\begin{aligned} D(a, b)D(c, d) &= \left(X^a Z^b\right)\left(X^c Z^d\right) && (3.11)\\ &= \omega^{cb} X^a X^c Z^b Z^d && (3.12)\\ &= \omega^{cb} X^{a+c} Z^{b+d} && (3.13)\\ &= \omega^{cb} D(a + c, b + d). && (3.14) \end{aligned}$$

Por lo tanto, salvo una fase global, la composición de los operadores $D(a, b)$ es análoga a la de las traslaciones en el espacio de fase.

Hasta ahorita solo hemos trabajado con sistemas de dimensión prima. En el siguiente capítulo se definirán los operadores X y Z para sistemas de dimensión p^n, en donde la base ortonormal elegida se etiqueta con elementos de la extensión de Galois. Mediante el uso de bases del campo finito, se pueden factorizar los operadores de desplazamiento y de sus eigenvectores. Wootters y Gibbons deciden trabajar de una manera inversa, ellos definen los operadores de desplazamiento para sistemas de dimensión p^n *directamente* del producto tensorial de monomios de X y Z para los subsistemas de dimensión p. Ésto involucra la elección de una base en el campo finito, lo cual introduce cierta arbitrariedad. La asociación del punto $(a, b) \in \mathbb{F} \oplus \mathbb{F}$ con el operador correspondiente del espacio $\mathcal{H}^{\otimes n}$ depende de la expansión de a y de b en bases de la extensión de

Galois. Recordemos que la extensión de Galois $\mathrm{GF}(p^n)$ se puede ver como un espacio vectorial de dimensión n sobre el campo primo $\mathbb{Z}_p$. Eligiendo una base de la extensión $\{b_1, \ldots, b_n\} \subset \mathrm{GF}(p^n)$, podemos expresar a todo elemento $a \in \mathbb{F}$ como la combinación lineal:

$$a = \sum_{i=1}^{n} c_i b_i, \quad \text{donde } c_i \in \mathbb{Z}_p\,.$$

De igual manera, debemos elegir una base dual a la base del campo finito. Recordemos del apéndice (A.2) que una base dual es tal que

$$\mathrm{tr}(b_i \tilde{b}_j) = \delta_{ij},$$

y que en muchas ocasiones podemos encontrar una base *auto-dual*, algo que es conveniente a la hora de hacer los cálculos. Dada la base y la base dual, Wootters y Gibbons definen a los operadores de desplazamiento correspondientes a traslaciones arbitrarias $\mathcal{T}(a, b)$, como productos tensoriales de monomios de los operadores unitarios X y Z, donde las potencias están dadas por los coeficientes de la expansión de a en la base y de b en la base dual:

Definición 18. *Sean $a_1, \ldots, a_n$ los coeficientes de a en la base del campo y $b_1, \ldots, b_n$ los coeficientes de b en la base dual. Entonces definimos al operador de desplazamiento como*

$$D(a, b) = X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_n} Z^{b_n}. \tag{3.15}$$

A pesar de la aribtrariedad que ésto introduce, podemos ver que hay una correspondencia natural con las traslaciones *básicas* del espacio de fase discreto, en el sentido de que si una traslación por el vector (a, b) solo tiene los i-ésimos componentes de a y b no nulos, entonces el operador de desplazamiento solo actúa sobre el i-ésimo subsistema. Los operadores satisfacen varias propiedades interesantes, por ejemplo, forman una base del espacio de operadores lineales de $\mathcal{H}$.

Definición 19. *Para un espacio de Hilbert de dimensión finita, un operador de Hilbert-Schmidt es un operador tal que $\mathrm{Tr}(AA^*)$ es finito. El producto interno de Hilbert-Schmidt se define como*

$$\langle A, B\rangle_{HS} = \mathrm{Tr}\left(AB^*\right). \tag{3.16}$$

Dado que los operadores de desplazamiento son unitarios, son de Hilbert-Schmidt, pues la traza de la identidad es d. El hecho de que forman una base para los operadores lineales es consecuencia de ser ortogonales bajo el producto de Hilbert-Schmidt.

Proposición 16. *Los operadores de desplazamiento son mutuamente ortogonales respecto al producto de Hilbert-Schmidt en el siguiente sentido:*

$$\mathrm{Tr}\left(D(a, b) D(c, d)^*\right) = d\delta_c^a \delta_d^b. \tag{3.17}$$

Demostración. Para ver ésto primero consideremos el caso de dimensión prima:

$$\mathrm{Tr}\left(D(a, b)\right) = \sum_{k \in \mathbb{Z}_p} \langle k|D(a, b)|k\rangle = \sum_{k \in \mathbb{Z}_p} \langle k|\omega^{bk}|k + a\rangle = \sum_{k \in \mathbb{Z}_p} \omega^{bk} \langle k|k + a\rangle\,. \tag{3.18}$$

Si $a \neq 0$ entonces $\langle k|k + a\rangle = 0$ para todo $k \in \mathbb{Z}_p$. Si $a = 0$ entonces

$$\mathrm{Tr}\left(D(a, b)\right) = \sum_{k \in \mathbb{Z}_p} \omega^{bk},$$

por lo tanto al menos que $a = b = 0$, la traza se anula. Así que

$$\mathrm{Tr}\left(D(a,b)\right) = d\delta_0^a\delta_0^b. \tag{3.19}$$

Por otro lado no es dificil probar que $D(a,b)^* = \omega^{ab}D(-a,-b)$, así que

$$\begin{aligned}\mathrm{Tr}\left(D(a,b)D(c,d)^*\right) &= \mathrm{Tr}\left(\omega^{cd}D(a,b)D(-c,-d)\right) &(3.20)\\ &= \mathrm{Tr}\left(\omega^{cd}\omega^{-cb}D(a-c,b-d)\right) &(3.21)\\ &= \omega^{cd-cb}\,\mathrm{Tr}(D(a-c,b-d)). &(3.22)\end{aligned}$$

De la ecuación (3.19) tenemos que que la traza se anula si $(a,b) \neq (c,d)$, en caso contrario $\omega^{cd-cb} = 1$ y obtenemos el resultado buscado. El caso general se sigue de las propiedades de la traza respecto el producto tensorial. □

Anteriormente mencionamos que el operador Z es diagonal y sus eigenvectores son la base estándar de $\mathbb{C}^p$. Notemos que en el caso de dimensión p^n, los operadores,

$$D(0,b) = Z^{b_1} \otimes \cdots \otimes Z^{b_n},$$

también son diagonales por lo que sus eigenvectores serán la base estándar de $\mathbb{C}^{p^n}$, la cual a su vez se puede factorizar en productos tensoriales de la base estándar de $\mathbb{C}^p$:

$$|k_1\rangle \otimes \cdots \otimes |k_n\rangle\,, \quad k_1,\ldots,k_n \in \mathbb{Z}_p\,.$$

Por otro lado, se puede probar que los operadores de desplazamiento respecto a las traslaciones horizontales son

$$D(a,0) = X^{a_1} \otimes \cdots \otimes X^{a_n},$$

y sus eigenvectores están dados por productos tensoriales de vectores $|\tilde{j}\rangle$.

El concepto de factorización tensorial es muy importante en áreas como la óptica cuántica y en la computación cuántica. A pesar de ésto, la factorización de los operadores desplazamiento y de sus eigenvectores no es una parte fundamental en la construcción de la función de Wigner. En realidad podemos definir una base ortonormal y etiquetarla con elementos de la extensión de Galois $\mathrm{GF}\,(p^n)$ y luego definir los operadores de desplazamiento mediante su acción sobre ésta base. Ésto lo hacemos en el siguiente capítulo para evitar de cierto modo la arbitrariedad que conlleva la introducción de bases del campo finito. Si es necesario factorizar, podemos utilizar una base del campo para mapear elementos entre $\mathbb{C}^{p^n}$ y $(\mathbb{C}^p)^{\otimes n}$ de la siguiente manera

$$|\alpha\rangle \mapsto |\alpha_1\rangle \otimes \cdots \otimes |\alpha_n\rangle\,,$$

donde los $\alpha_1,\ldots,\alpha_n$ son los coeficientes de la expansión de α respecto a la base elegida. Debido a la libertad que tenemos en la elección de la base del campo, la factorización no es única. Klimov et al. [34] muestran que los estados etiquetados con los elementos de la extensión de Galois pueden ser mapeados a estados fisicos con propiedades de factorización distintas, y ésto a su vez tiene consecuencias físicas.

Ejemplo 3. *Éste ejemplo fue tomado de [34] y nos muestra como la factorización tensorial puede depender de las bases del campo finito elegidas. Consideremos un sistema de dos qubits, en el estado*

$$|\psi\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}. \tag{3.23}$$

Utilizando la base $(1, \alpha)$ *obtenemos*

$$|\psi\rangle \mapsto \frac{|0\rangle \otimes |0\rangle + |1\rangle \otimes |0\rangle}{\sqrt{2}} = \frac{(|0\rangle + |1\rangle) \otimes |0\rangle}{\sqrt{2}}, \tag{3.24}$$

mientras que la base (α, α^2) *nos brinda*

$$|\psi\rangle \mapsto \frac{|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle}{\sqrt{2}}. \tag{3.25}$$

Como podemos observar, el primer estado tensorial es factorizable mientras que el segundo no lo es.

3.1.3. Definición de la malla cuántica

Regresando a la construcción de la función de Wigner, vamos a utilizar a los operadores de desplazamiento para definir el requisito de ser covariante bajo traslaciones que le exigimos a la función de Wigner. Recordemos que la función de Wigner dependerá de la malla cuántica Q, la cual es una asignación entre las lineas del espacio de fase discreto y estados cuánticos de $\mathcal{H}$:

$$Q : \mathcal{P}(\mathbb{F} \oplus \mathbb{F}) \to \mathcal{L}(\mathcal{H}). \tag{3.26}$$

Por lo tanto conviene definir una propiedad análoga para la asignación Q. Naturalmente ésto lo logramos al exigir la preservación la estructura cuántica asignada al espacio de fase cuando las lineas son trasladadas, i.e., si trasladamos una linea λ por $\mathcal{T}(a, b)$ entonces el estado cuántico también debe ser "trasladado" pero por los operadores de desplazamiento correspondientes. Formalmente ésto implica que

$$Q(\mathcal{T}(a, b)\lambda) = D(a, b)Q(\lambda)D(a, b)^*. \tag{3.27}$$

Ésto resulta ser un requisito muy fuerte, ya que implica que los operadores correspondientes a las traslaciones que dejan invariantes a las rectas de una estría deben conmutar. Para ver ésto, supongamos que λ es un rayo parametrizado por (sx, sy) donde $s \in \mathbb{F}$. Entonces ésta recta y todas las rectas paralelas a ella son invariantes bajo las traslaciones $\mathcal{T}(tx, ty)$ donde $t \in \mathbb{F}$:

$$\begin{aligned} \mathcal{T}(tx, ty)\lambda &= \{(tx, ty) + (sx, sy) : (sx, sy) \in \lambda\} \\ &= \{((t + s)x, (t + s)y) : t + s \in \mathbb{F}\} \\ &= \lambda. \end{aligned}$$

Por lo tanto la condición (3.27) implica que

$$D(tx, ty)Q(\lambda)D(tx, ty)^* = Q(\mathcal{T}(tx, ty)\lambda) = Q(\lambda),$$

pero como los operadores $D(a, b)$ son unitarios, ésto a su vez significa que

$$D(tx, ty)Q(\lambda) = Q(\lambda)D(tx, ty),$$

i.e., todos los operadores $D(tx, ty)$ con $t \in \mathbb{F}$ conmutan con $Q(\lambda)$. Pero ésto solo sucede si los operadores de desplazamiento $D(tx, ty)$ para (x, y) fijo conmutan entre si. En otras palabras, para que la red cuántica sea covariante bajo traslaciones, los operadores de desplazamiento correspondientes a las traslaciones que dejan las rectas de una estría invariante deben conmutar. Gibbons y Wootters prueban que su definición de $D(a, b)$ satisface éste requisito si y solo si la base en que se expande el vector b es un *múltiplo* de la base dual. Visto desde otro punto de vista, si identificamos el estado cuántico con un vector del espacio de Hilbert, la condición (3.27) implica que $Q(\lambda)$ es un eigenvector de todos los operadores $D(tx, ty)$. Los operadores que son diagonalizables y conmutan entre sí comparten un conjunto completo de eigenvectores. Entonces, dado que los operadores de desplazamiento son diagonalizables, los operadores que corresponden a traslaciones que dejan invariante a una estría en el espacio de fase discreto, son diagonalizables de manera simultánea. Wootters menciona que ésta base es única, por lo que tiene sentido asignar a cada estría su correspondiente base de eigenvectores.

Recordando que los operadores son ortogonales respecto al producto interior de Hilbert Schmidt, el hecho de agrupar a los operadores de desplazamiento en subconjuntos conmutativos nos brinda una de las características más atractivas de la construcción de Wootters de la función de Wigner, que depende del siguiente resultado de Bandyophyay et al. [35]:

Teorema 1 (Bandyophyay et al, teorema 3.2)**.** *Si existe una partición de n^2-1 matrices unitarias mutuamente ortogonales en $d+1$ conjuntos de $d-1$ matrices conmutativas, entonces existen un conjunto de $d+1$ bases mutuamente insesgadas.*

Notemos que la agrupación de los operadores invariantes de cada estría satisface ésta condición, ya que a cada estría le corresponde $d-1$ operadores de desplazamiento (no triviales) y tenemos $d+1$ estrías del espacio de fase discreto en total. Por lo tanto Wootters y Gibbons concluyen que los conjuntos de eigenvectores simultáneaos forman un conjunto de bases mutuamente insesgadas. No detallamos más sobre ésto por el momento porque se estudiará más fondo en el siguiente capítulo.

Hasta ahorita solo se ha asignado una base ortonormal a cada estría. Para definir por completo al mapeo Q debemos identificar a cada linea de cada estría con una proyección ortogonal de un elemento de la base. Resulta que podemos asignar un elemento de la base al rayo λ de la estría de manera *arbitraria*. El resto de la asignación se determina por los mismos operadores de desplazamiento debido a la propiedad de ser covariante bajo traslaciones:

$$Q(\mathcal{T}(x, y)\lambda) = D(x, y)Q(\lambda)D(x, y)^*,$$

ya que se pueden obtener el resto de las rectas de la estría mediante traslaciones en el espacio de fase. Ésto refleja el hecho de que las traslaciones en el espacio de fase discreto no cambian la pendiente de las rectas, por lo tanto al trasladar un recta solo obtendremos otra recta *paralela* a ella, es decir a otro elemento de la estría. Que la malla cuántica sea covariante bajo traslaciones significa que los eigenestados asignados a una estría quedan invariantes bajo los operadores de desplazamiento.

Ejemplo 4. *Consideremos un qutrit. El espacio de Hilbert es $\mathbb{C}^3$ y el espacio de fase discreto es simplemente $\mathbb{Z}_3 \oplus \mathbb{Z}_3$. Como hemos visto anteriormente, el rayo vertical $\lambda = \{(0, u) : u \in \mathbb{Z}_3\}$ es invariante bajo las traslaciones $\mathcal{T}(0, u)$ para todo $u \in \mathbb{Z}_3$. El operador correspondiente es la matriz generalizada de Pauli dada por*

$$D(0, u) = Z^u,$$

cuyos eigenvectores simplemente consiste de la base estándar

$$|0\rangle = \begin{pmatrix}1\\0\\0\end{pmatrix}, \quad |1\rangle = \begin{pmatrix}0\\1\\0\end{pmatrix}, \quad y \quad |2\rangle = \begin{pmatrix}0\\0\\1\end{pmatrix}.$$

Para definir la red cuántica, primero asignamos el eigenestado $|0\rangle\langle 0|$ *al rayo vertical. Si trasladamos a* λ *por cualquier vector* (x, y) *en el espacio de fase discreto, solo obtendremos una recta paralela a* λ*:*

$$\begin{aligned}\mathcal{T}(x,y)\lambda &= \mathcal{T}(x,y)\{(0,u) : u \in \mathbb{Z}_3\} && (3.28)\\ &= \{(x, u+y) : u \in \mathbb{Z}_3\} && (3.29)\\ &= \{(x,s) : s \in \mathbb{Z}_3\} && (3.30)\\ &= \lambda'. && (3.31)\end{aligned}$$

Para que Q *sea covariante bajo traslaciones es necesario que al desplazar el eigenestado* $|0\rangle$ *por el operdaor* $D(x, y)$*, obtengamos otro elemento de la base estándar (salvo una fase). Por definición de los operadores de desplazamiento, ésto siempre sucede (más adelante veremos que el grupo de Pauli deja a las familias de eigenvectores invariantes salvo permutaciones). En éste ejemplo vemos que*

$$\begin{aligned}D(x,y)|0\rangle &= X^x Z^y |0\rangle && (3.32)\\ &= X^x \omega^{x\cdot 0} |0\rangle && (3.33)\\ &= X^x |0\rangle && (3.34)\\ &= |x\rangle. && (3.35)\end{aligned}$$

Volvemos a obtener un elemento de la base estándar. Dado ésto, la malla cuántica Q *debe asignar a la recta paralela* $\mathcal{T}(x, y)\lambda = \lambda'$*, el eigenestado* $|x\rangle$ *para poder preservar ésta propiedad. Es por eso que la elección solo es arbitraria para la primera asignación.*

La definición de la función de Wigner queda totalmente determinada despues de la elegir una malla cuántica. Veamos.

3.1.4. Definición de una función de Wigner

Sea ρ un operador de densidad y W_ρ su función de Wigner por definir. Para preservar la propiedad tomográfica de la función de Wigner en el caso discreto, requerimos que la suma de W_ρ sobre la recta λ, sea la probabilidad de que el sistema cuántico se observe en el estado $Q(\lambda)$. Ésto significa que

$$\sum_{\alpha\in\lambda} W_\rho(\alpha) = \mathrm{Tr}\left(\rho Q(\lambda)\right), \tag{3.36}$$

para toda recta del espacio de fase discreto. Además, requerimos que la suma de W_ρ sobre todo el espacio de fase sea igual a uno para poder considerarlo como una cuasi-distribución. Dado que nuestro espacio de fase es una geometría finita, a traves del punto α pasan exactamente $d + 1$ rectas que cubren a todo el espacio de fase discreto. Entonces si W_ρ satisface la propiedad de normalización, i.e., $\sum_\beta W_\rho(\beta) = 1$, se cumple que

$$\sum_{\lambda\ni\alpha}\left(\sum_{\beta\in\lambda} W_\rho(\beta)\right) = dW_\rho(\alpha) + 1. \tag{3.37}$$

Despejando obtenemos un expresión para $W_\rho(\alpha)$:

$$W_\rho(\alpha) = \frac{1}{d}\left[\sum_{\lambda \ni \alpha}\left(\sum_{\beta\in\lambda} W_\rho(\beta)\right) - 1,\right]$$

y utilizando (3.36) tenemos

$$W_\rho(\alpha) = \frac{1}{d}\left(\sum_{\lambda\ni\alpha} \mathrm{Tr}\left(\rho Q(\lambda)\right) - 1\right). \tag{3.38}$$

Utilizando las propiedades de la traza podemos expresar la función de Wigner en términos del valor esperado de un operador $A(\alpha)$ en el estado ρ:

$$W_\rho(\alpha) = \frac{1}{d}\,\mathrm{Tr}\left(\rho A(\alpha)\right), \tag{3.39}$$

donde

$$A(\alpha) = \sum_{\lambda\ni\alpha} Q(\lambda) - I. \tag{3.40}$$

Los operadores $A(\alpha)$ son los ánologos a los operadores puntuales $\hat{\Delta}(\alpha)$ en el caso continuo, por lo que también lleverán el mismo nombre.

Por construcción la función de Wigner discreta satisface la propiedad tomográfica y la propiedad de normalización. Probando ciertas propiedades de los operadores puntuales $A(\alpha)$ análogos a las propiedades los operadores $\hat{\Delta}(\alpha)$, podremos demostrar el resto de las propiedades de Stratonovich-Weyl para la función discreta.

Proposición 17. *Los operadores puntuales $A(\alpha)$ donde $\alpha = (a, b) \in \mathbb{F}\oplus\mathbb{F}$ satisfacen las siguientes propiedades:*

1. *$A(\alpha)$ es auto-adjunto.*
2. *Son de traza unitaria.*
3. *Son ortogonales bajo el producto interno de Hilbert-Schmidt.*

Demostración.

1. Recordemos que $Q(\lambda)$ es un operador auto-adjunto ya que representa un estado cuántico. Así que por definición inmediatamente tenemos que

$$A(\alpha)^* = \left(\sum_{\lambda\ni\alpha} Q(\lambda) - I\right) = \sum_{\lambda\ni\alpha} Q(\lambda)^* - I = \sum_{\lambda\ni\alpha} Q(\lambda) - I = A(\alpha). \tag{3.41}$$

2. Similarmente, los operadores $Q(\lambda)$ son de traza unitaria, porque de nuevo, representan un estado cuántico. Asi que de la linealidad de la traza obtenemos

$$\mathrm{Tr}(A(\alpha)) = \mathrm{Tr}\left(\sum_{\lambda\ni\alpha} Q(\lambda) - I\right) = \sum_{\lambda\ni\alpha} \mathrm{Tr}(Q(\lambda)) - d = (d+1) - d = 1. \tag{3.42}$$

3. Para la última propiedad dependeremos del hecho de que los operadores $Q(\lambda)$ proyectan hacia elementos que son mutuamente insesgados. Sean $\alpha, \beta \in \mathbb{F} \oplus \mathbb{F}$, por definición tenemos

$$\begin{aligned}
\mathrm{Tr}\left(A(\alpha)A(\beta)\right) &= \mathrm{Tr}\left[\left(\sum_{\lambda \ni \alpha} Q(\lambda) - I\right)\left(\sum_{\nu \ni \beta} Q(\nu) - I\right)\right] && (3.43)\\
&= \mathrm{Tr}\left[\sum_{\lambda \ni \alpha}\sum_{\nu \ni \beta} Q(\lambda)Q(\nu) - \sum_{\lambda \ni \alpha} Q(\lambda) - \sum_{\nu \ni \beta} Q(\nu) + I\right] && (3.44)\\
&= \sum_{\lambda \ni \alpha}\sum_{\nu \ni \beta} \mathrm{Tr}\left[Q(\lambda)Q(\nu)\right] - 2(d+1) + d. && (3.45)
\end{aligned}$$

Sea $|\lambda\rangle$ el eigenvector asignado a la linea λ por medio de Q. Si $\lambda = \nu$ entonces $\langle\lambda|\lambda\rangle = 1$. Si $\lambda \neq \nu$ pero λ es paralela a ν, entonces $\langle\lambda|\nu\rangle = 0$, pues las bases asignadas a cada estría son ortonormales. Ahora, si λ y ν pertenecen a estrías distintas, entonces los eigenvectores son mutuamente insesgados:

$$|\langle\lambda|\nu\rangle|^2 = \frac{1}{d}, \tag{3.46}$$

por lo tanto

$$\begin{aligned}
\mathrm{Tr}\left(Q(\lambda)Q(\nu)\right) &= \mathrm{Tr}\left(|\lambda\rangle\langle\lambda|\,|\nu\rangle\langle\nu|\right) && (3.47)\\
&= \langle\lambda|\nu\rangle\,\mathrm{Tr}\left(|\lambda\rangle\langle\nu|\right) && (3.48)\\
&= \langle\lambda|\nu\rangle\left(\sum_k \langle k|\,|\lambda\rangle\langle\nu|\,|k\rangle\right) && (3.49)\\
&= \langle\lambda|\nu\rangle\left(\sum_k \langle\nu|\,|k\rangle\langle k|\,|\lambda\rangle\right) && (3.50)\\
&= \langle\lambda|\nu\rangle\langle\nu|\lambda\rangle && (3.51)\\
&= |\langle\lambda|\nu\rangle|^2 && (3.52)\\
&= \frac{1}{d}. && (3.53)
\end{aligned}$$

La doble suma de la ecuación (3.45) tiene $(d+1)^2 = d^2+2d+1 = (d+1)+d(d+1)$ términos. Si $\alpha = \beta$, entonces $d+1$ de esos términos corresponden a las mismas lineas por lo que las trazas tienen valor de 1. El resto de los $d(d+1)$ términos corresponden a las trazas de lineas de distintas estrías por lo tanto toman el valor $1/d$. Así que en el caso en que $\alpha = \beta$ se sigue que

$$\begin{aligned}
\mathrm{Tr}\left(A(\alpha)A(\beta)\right) &= \sum_{\lambda \ni \alpha}\sum_{\nu \ni \beta} \mathrm{Tr}\left[Q(\lambda)Q(\nu)\right] - 2(d+1) + d && (3.54)\\
&= (d+1) + \frac{1}{d}[d(d+1)] - 2(d+1) + d && (3.55)\\
&= d. && (3.56)
\end{aligned}$$

Ahora, si $\alpha \neq \beta$ entonces sabemos que solamente una linea pasa por los dos puntos, por lo que la traza tomará el valor de 1 en un solo término. Las d restantes

lineas que pasan por el punto α serán paralelas a las d restante lineas que pasan por β, por lo que se anula la traza cuando λ y ν son paralelas. Los restantes $d(d+1)$ términos cruzados serán igual a $1/d$ por ser mutuamente insesgados. Asi que para $\alpha \neq \beta$ tenemos

$$\begin{aligned}
\mathrm{Tr}\left(A(\alpha)A(\beta)\right) &= \sum_{\lambda \ni \alpha} \sum_{\nu \ni \beta} \mathrm{Tr}\left[Q(\lambda)Q(\nu)\right] - 2(d+1) + d && (3.57)\\
&= 1 + \frac{1}{d}[d(d+1)] - 2(d+1) + d && (3.58)\\
&= d + 2 - 2d - 2 + d && (3.59)\\
&= 0. && (3.60)
\end{aligned}$$

Por lo tanto los operadores puntuales son ortogonales respecto al producto interno de Hilbert-Schmidt.

□

La propiedad tres de la proposición (17) nos dice que los operadores $A(\alpha)$ forman una base del espacio de operadores lineales del espacio de Hilbert. En particular podemos expresar a cualquier operador de densidad en términos de los operadres puntuales:

$$\rho = \sum_{\alpha \in \mathbb{F} \oplus \mathbb{F}} a_\alpha A(\alpha). \tag{3.61}$$

Utilizando la ortogonalidad de $A(\alpha)$ podemos probar que los coeficientes en la expansión son precisamente los valores de la función de Wigner en el punto α, i.e., $a_\alpha = W(\alpha)$. Sea $\beta \in \mathbb{F} \oplus \mathbb{F}$, entonces

$$\begin{aligned}
\mathrm{Tr}(\rho A(\beta)) &= \mathrm{Tr}\left[\left(\sum_\alpha a_\alpha A(\alpha)\right) A(\beta)\right] && (3.62)\\
&= \sum_\alpha \mathrm{Tr}\left(a_\alpha A(\alpha)A(\beta)\right) && (3.63)\\
&= \sum_\alpha a_\alpha \,\mathrm{Tr}(A(\alpha)A(\beta)) && (3.64)\\
&= d a_\beta, && (3.65)
\end{aligned}$$

pero por definición de la función de Wigner $\mathrm{Tr}(\rho(A\beta)) = dW(\beta)$, por lo tanto $dW(\beta) = da_\beta$, es decir,

$$a_\beta = W(\beta), \quad \text{para todo } \beta \in \mathbb{F} \oplus \mathbb{F}\,. \tag{3.66}$$

Así que dada una función de Wigner W_ρ, podemos recuperar el estado ρ de la siguiente manera:

$$\rho = \sum_\alpha W(\alpha)A(\alpha). \tag{3.67}$$

Con ésto tenemos una representación completa de cualquier estado cuántico en el espacio de fase discreto ya que siempre podemos *invertir* la función de Wigner y recuperar el estado correspondiente mediante la expansión en los operadores puntuales. A partir de las propiedades de los operadores puntuales, podemos finalmente demostrar las propiedades de la función de Wigner que se deseaban al inicio del capítulo.

Proposición 18. *Sea ρ un estado cuántico y W_ρ su función de Wigner discreta. Entonces*

1. *La función de Wigner es real.*
2. *La suma de W_ρ sobre cualquier recta λ es igual al valor esperado de $Q(\lambda)$ en el estado ρ.*
3. *La suma de W_ρ sobre todo el espacio de fase es igual a 1.*
4. *La función de Wigner es covariante bajo traslaciones: sea ρ un operador de densidad y W_ρ su función de Wigner y consideremos el estado ρ' y su función de Wigner $\mathrm{W}_{\rho'}$, donde*
$$\rho' = D(\beta)\rho D(\beta)^*.$$
Entonces $W_{\rho'}(\alpha) = W_\rho(\alpha - \beta)$.

Demostración.

1. El estado cuántico ρ y los operadores puntuales son auto-adjuntos, entonces de las propiedades de la traza tenemos
$$\begin{aligned} dW_\rho(\alpha) &= \mathrm{Tr}(\rho A(\alpha)) && (3.68)\\ &= \mathrm{Tr}\left(\rho^* A(\alpha)^*\right) && (3.69)\\ &= \mathrm{Tr}\left((A(\alpha)\rho)^*\right) && (3.70)\\ &= \overline{\mathrm{Tr}\left(A(\alpha)\rho\right)} && (3.71)\\ &= \overline{dW_\rho(\alpha)}. && (3.72)\end{aligned}$$
Por lo tanto $W_\rho(\alpha) = \overline{W_\rho(\alpha)}$ para todo α, así que W_ρ es real.
2. La función de Wigner satisface ésta propiedad por construcción.
3. Consideremos una estría S de rectas paralelas. Dado que Q asgina una base ortonormal del espacio de Hilbert a la estría, de los postulados de medición de la mecánica cuántica sabemos que
$$\sum_{\lambda\in S} \mathrm{Tr}\left(\rho Q(\lambda)\right) = 1.$$
Se sigue de la propiedad anterior, que al sumar la función de Wigner sobre cada recta obtenemos
$$\sum_\alpha W_\rho(\alpha) = \sum_{\lambda\in S}\left(\sum_{\alpha\in\lambda} W_\rho(\alpha)\right) = \sum_{\lambda\in S}\mathrm{Tr}(\rho Q(\lambda)) = 1. \quad (3.73)$$
4. La prueba de que la función de Wigner es covariante bajo traslaciones es directa y se obtiene a partir de la definición de la red cuántica Q. Sea $\beta \in \mathbb{F}\oplus F$ y ρ un

estado cuántico. Primero, de la definición de los operadores puntuales tenemos:

$$D(\beta)^* A(\alpha) D(\beta) = D(\beta)^* \left(\sum_{\lambda \ni \alpha} Q(\lambda) - I \right) D(\beta) \tag{3.74}$$

$$= \sum_{\lambda \ni \alpha} D(\beta)^* Q(\lambda) D(\beta) - I \tag{3.75}$$

$$= \sum_{\lambda \ni \alpha} D(-\beta) Q(\lambda) D(-\beta)^* - I. \tag{3.76}$$

Pero Q es covariante bajo traslaciones,

$$D(-\beta) Q(\lambda) D(-\beta)^* = Q\left(\mathcal{T}(-\beta)\lambda\right), \tag{3.77}$$

así que todas las lineas que pasan por el punto α son trasladas de manera paralela para cruzar al punto $\alpha - \beta$, así la ecuación (3.76) se puede escribir de manera equivalente como:

$$D(\beta)^* A(\alpha) D(\beta) = \sum_{\lambda \ni \alpha - \beta} Q(\lambda) - I = A(\alpha - \beta). \tag{3.78}$$

El resultado buscado se sigue de lo anterior y de la definición de $W_{\rho'}$:

$$W_{\rho'}(\alpha) = \frac{1}{d} \operatorname{Tr}\left(\rho' A(\alpha)\right) \tag{3.79}$$

$$= \frac{1}{d} \operatorname{Tr}\left(D(\beta) \rho D(\beta)^* A(\alpha)\right) \tag{3.80}$$

$$= \frac{1}{d} \operatorname{Tr}\left(D(\beta) \rho D(\beta)^* A(\alpha) D(\beta) D(\beta)^*\right) \tag{3.81}$$

$$= \frac{1}{d} \operatorname{Tr}\left(\rho D(\beta)^* A(\alpha) D(\beta)\right) \tag{3.82}$$

$$= \frac{1}{d} \operatorname{Tr}\left(\rho A(\alpha - \beta)\right) \tag{3.83}$$

$$= W_\rho(\alpha - \beta). \tag{3.84}$$

□

Hemos construido una función de Wigner discreta siguiendo el método de Wootters y Gibbons, la cual satisface las propiedades análogas al caso continuo y además comparte varios aspectos de su construcción con la formulación continua, en particular el uso de operadores puntuales. Por otro lado, la construcción involucra elecciones durante dos pasos de la construcción: en la definición de los operadores de desplazamiento y sobre todo en la definición de la red cuántica. Wootters y Gibbons analizan transformaciones en el espacio de fase discreto para hacer una clasificación de funciones de Wigner en clases de equivalencia. En éste trabajo no estudiaremos éste aspecto de la función de Wigner discreta a fondo, pero en el siguiente capítulo tendremos que mencionar un poco más debido a los resultados que se obtuvieron en la construcción no estándar. Por el momento pasemos a algunos ejemplos de funciones de Wigner discretas.

3.2. Ejemplos ilustrativos

Daremos dos ejemplos para mostrar el procedimiento de Wootters. Visualizamos el espacio de fase discreto así como los rayos de cada estría, luego formamos la malla cuántica eligiendo un estado para cada rayo. Finalmente construimos los operadores puntuales para formar la función de Wigner en ambos casos.

Ejemplo 5. *Consideremos de nuevo el sistema cuántico que modela un qutrit. Recordemos que* $\mathcal{H} = \mathbb{C}^3$ *y el espacio de fase discreto es* $\mathbb{Z}_3 \oplus \mathbb{Z}_3$*. En éste caso como* 3 *es primo, no es necesario hablar de extensiones de Galois ni de expansiones en alguna base. Los operadores de desplazamiento simplemente son productos y potencias de las matrices de Pauli generalizadas para* $\dim \mathcal{H} = 3$*. Las matrices* X *y* Z *están dadas por*

$$X = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix} \tag{3.85}$$

donde ω *es un tercera raíz primitiva de la unidad, i.e.,* $\omega = e^{2\pi i/3}$*. El espacio de fase está ilustrado en la figura (3.3) la cual también muestra sus* $3{+}1$ *rayos. Hasta ahora solo*

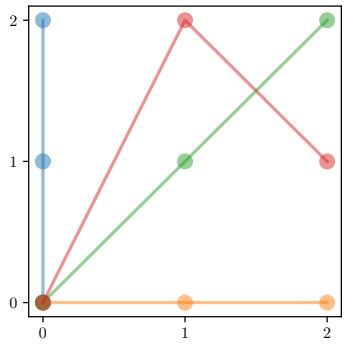


Figura 3.3: Espacio de fase discreto para $\mathbb{C}^3$. Notemos que los rayos no se intersectan en otro punto distinto al origen $(0, 0)$.

hemos dicho que las bases de vectores que se usarán para definir la malla cuántica son los eigenvectores de familias de operadores de desplazamientos. En el siguiente capítulo veremos una manera de constuirlos explícitamente, por ahora solo mostramos la familia de bases mutuamente insesgadas, etiquetadas por las traslaciones correspondientes en

el espacio de fase:

$$\mathcal{T}(0,u) \leftrightarrow \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\} \tag{3.86}$$

$$\mathcal{T}(u,0) \leftrightarrow \left\{ \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \omega \\ \omega^2 \end{pmatrix}, \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \omega^2 \\ \omega \end{pmatrix} \right\} \tag{3.87}$$

$$\mathcal{T}(u,u) \leftrightarrow \left\{ \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \omega^2 \\ \omega^2 \end{pmatrix}, \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ \omega \end{pmatrix}, \frac{1}{\sqrt{r_3}} \begin{pmatrix} 1 \\ \omega \\ 1 \end{pmatrix} \right\} \tag{3.88}$$

$$\mathcal{T}(u,2u) \leftrightarrow \left\{ \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \omega \\ \omega \end{pmatrix}, \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \omega^2 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ \omega^2 \end{pmatrix} \right\}. \tag{3.89}$$

Las traslaciones de cada base son las que dejan invariantes a las rectas de alguna estría. Por ejemplo la base estándar corresponde a las traslaciones verticales y la tercera base corresponde al rayo vertical. Se puede verificar de manera directa que los elementos de cada conjunto son eigenvectores de los operadores de desplazamiento correspondientes, por ejemplo para el operador de traslación $D(1,0)$ y el primer eigenvector de la base correspondiente tenemos:

$$D(1,0)\left[\frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}\right] = \frac{1}{\sqrt{3}} X \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \tag{3.90}$$

$$= \frac{1}{\sqrt{3}} X \left(|0\rangle + |1\rangle + |2\rangle\right) \tag{3.91}$$

$$= \frac{1}{\sqrt{3}} \left(|1\rangle + |2\rangle + |0\rangle\right) \tag{3.92}$$

$$= \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}. \tag{3.93}$$

Para construir la malla cuántica elegimos asignar el primer vector de cada conjunto a cada rayo. Las asignaciones restantes de cada estría quedan determinadas por las traslaciones y operadores de desplazamiento. Por ejemplo, al rayo horizontal $\lambda_0 = \{(u,0) : u \in \mathbb{Z}_3\}$ le asignamos el vector $\frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle)$. Podemos obtener a la recta horizontal $\lambda_1 = \{(u,1) : u \in \mathbb{Z}_3\}$ trasladando al rayo λ_0 por $\mathcal{T}(0,1)$. Por lo tanto el eigenestado $Q(\lambda_1)$ que se le asigna a la recta λ_1 es

$$D(0,1)\left[\frac{1}{\sqrt{3}}\left(|0\rangle + |1\rangle + |2\rangle\right)\right] = \frac{1}{\sqrt{3}} Z \left(|0\rangle + |1\rangle + |2\rangle\right) \tag{3.94}$$

$$= \frac{1}{\sqrt{3}} \left(|0\rangle + \omega\,|1\rangle + \omega^2\,|2\rangle\right) \tag{3.95}$$

$$= \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \omega \\ \omega^2 \end{pmatrix}. \tag{3.96}$$

Notemos que éste nuevo vector es el segundo elemento del conjunto de eigenvectores de los operadores $D(0,u)$. Ésta coincidencia en el orden se debe a la manera en que se programó las bases mutuamente insesgadas, pero en general el orden no es una restricción. De la misma manera podemos hacer el resto de las asignaciones y así definir totalmente a la malla cuántica Q.

Dada Q, podemos utilizar la ecuación (3.40) para construir a los operadores puntuales. Recordemos que su definición es

$$A(x,y) = \sum_{\lambda \ni (x,y)} Q(\lambda) - I,$$

i.e., consiste en la suma de todos las proyecciones a los eigenestados asignados a las rectas λ que pasan por el punto (x,y). La figura (3.4) nos muestra dos planos con distintos puntos seleccionados y las rectas que pasan por esos puntos. A cada una de esas rectas se le asigna un estado cuántico cuyos proyectores se suman para obtener el operador puntual.

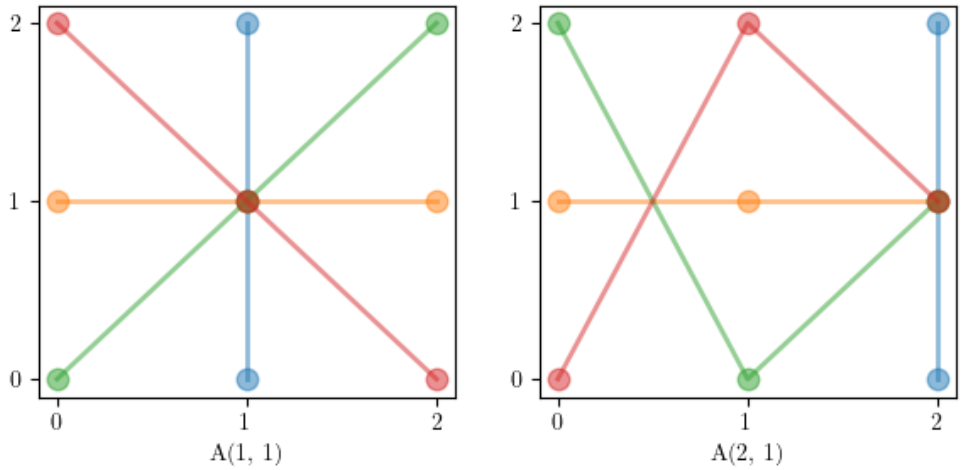


Figura 3.4: Las rectas que pasan por los puntos $(1,1)$ y $(2,1)$ respectivamente.

Para ilustrar el cálculo, vamos a construir el operador puntual correspondiente al origen. Como ya sabemos, las $3+1$ rectas que pasan por el origen son precisamente los rayos. Entonces, como hemos elegido asignar a los rayos del espacio de fase discreto, el operador de proyección del primer elemento de cada conjunto de vectores, un cálculo directo nos brinda

$$A(0,0) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}. \tag{3.97}$$

Notemos que las propiedes 1 y 2 de (17) se satisfacen para éste operador puntual, ya que $A(0,0)$ es auto-adjunta y su traza es igual a 1. En total existen $3^2 = 9$ operadores puntuales para éste espacio de fase. Dado un operador de densidad ρ, su función de Wigner queda determinada como $W(x,y) = \frac{1}{3}\operatorname{Tr}(\rho A(x,y))$. Hemos gráficado la función

de Wigner discreta para tres estados cuánticos:

$$|\psi_1\rangle = |0\rangle \tag{3.98}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{3}}\left(|0\rangle + \omega\,|1\rangle + \omega\,|2\rangle\right) \tag{3.99}$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \tag{3.100}$$

Los dos primeros estados cuánticos corresponden al primero vector de la primera base y al primer vector de la última base. El tercero es un vector arbitrario. La gráfica representa el espacio de fase discreto y el tamaño de la barra en el punto (x, y) indica el valor de $W(x, y)$.

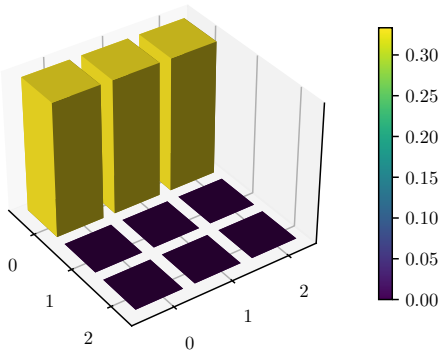


Figura 3.5: Función de Wigner para el estado $|\psi_1\rangle$ en el ejemplo de un qutrit.

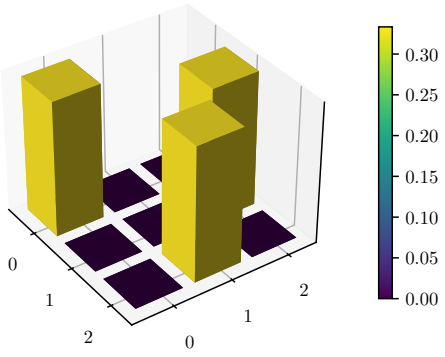


Figura 3.6: Función de Wigner para el estado $|\psi_2\rangle$ en el ejemplo de un qutrit.

En las tres figuras podemos observar que la suma de la función de Wigner es igual a uno. Las primeras dos figuras muestran una función de Wigner de estados que son elementos del conjunto de mediciones. Sumando sobre la primera recta en la función

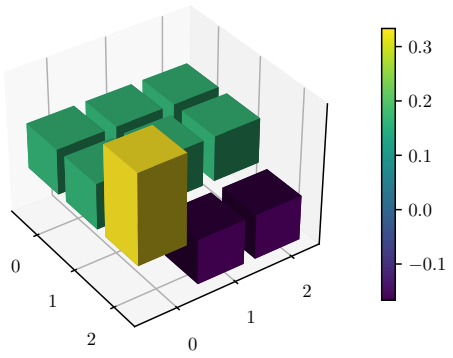


Figura 3.7: Función de Wigner para el estado $|\psi_3\rangle$ en el ejemplo de un qutrit.

de Wigner (figura 3.5) del estado $|\psi_1\rangle$ obtenemos 1. Ésto tiene sentido porque la probabilidad de que el sistema se encuentre en el estado $|0\rangle$ es 1 ya que $|\psi_1\rangle = |0\rangle$. Lo mismo sucede con la figura (3.6) respectivamente. En la figura (3.7) nos encontramos con una combinación lineal de dos elementos del conjunto de MUBs. En éste caso la probabilidad de encontrar el qutrit en el estado $|0\rangle$ es igual $\frac{1}{2}$ y ésto corresponde con la suma de W_{ψ_3} sobre la primera linea vertical, a la cual se le asignó el estado $|0\rangle$. En cambio sumando la función de Wigner sobre la tercera recta vertical obtenemos 0. Ésto es porque la probabilidad de encontrar al sistema en el estado $|2\rangle$ es nula! Notemos que la tercera función de Wigner presenta valores negativos. Por último, de los preliminares sabemos que la probabilidad de observar el sistema en el estado $|\psi\rangle = \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle)$ (eigenestado que corresponde al rayo horizontal) es igual a

$$|\langle\psi|\psi_3\rangle|^2 = \left|\frac{1}{\sqrt{3}}\cdot\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}}\cdot\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}}\cdot 0\right| = \left|\frac{2}{\sqrt{6}}\right|^2 = \frac{2}{3}.$$

Ésta probabilidad coincide con la suma de la función de Wigner sobre el rayo horizontal, algo que se puede observar directamente de la gráfica.

Ejemplo 6. *Ahora consideramos un ejemplo más interesante. Analizaremos el caso de dos qubits. El espacio de Hilbert correspondiente es $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2 \cong \mathbb{C}^4$ y el espacio de fase discreto será una malla de 4×4 puntos etiquetados por los elementos de la extensión de Galois*

$$\mathbb{F} = \mathrm{GF}\left(2^2\right) = \{0, 1, \alpha, \alpha + 1\}.$$

La figura (3.8) muestra el espacio de fase discreto etiquetado por los elementos del campo de Galois. El orden utilizado para las etiquetas coincide con el orden por default de `SageMath`, ésto no tiene consecuencias pues lo que importa es la asignación de estados a las lineas. Siguiendo a Wootters, podemos construir a los generadores del grupo de Pauli, i.e., a las matrices generalizadas de Pauli, a partir de las matrices σ_x y σ_z. Pero antes que ésto, notemos algunas sutilizas a la hora de trabajar con los elementos de la extensión de Galois. Si etiquetamos a la base estándar de $\mathbb{C}^4$ con los elementos de $\mathrm{GF}(2^2)$ en el orden en que aparecen en los ejes de la figura (3.8), tenemos

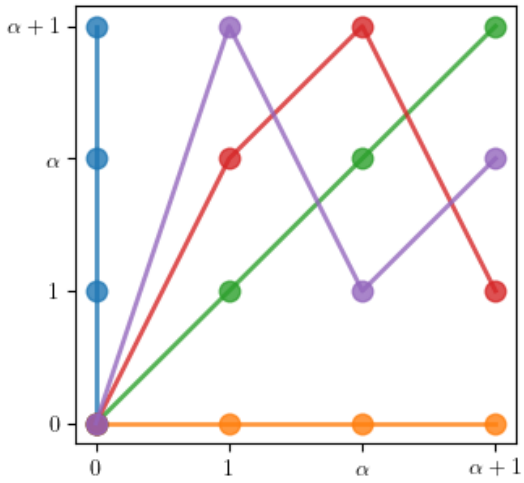


Figura 3.8: Rayos en el espacio de fase discreto sobre el campo GF (2^2).

que

$$|0\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \quad |1\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, \quad |\alpha\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, \quad |\alpha+1\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}.$$

Distintas bases del campo nos brinda distintas maneras de factorizar a la base estándar en productos tensoriales de la base estándar de $\mathbb{C}^2$. *Para que haya un correspondencia adecuada entre la base etiquetada por elementos del campo de Galois y los productos tensoriales, debemos elegir una base adecuada. En éste caso la base* $\{\alpha, 1\}$ *nos brinda una factorización adecuada. En ésta base el elemento* $\alpha+1$ *visto como un elemento del espacio vectorial sobre el campo* $\mathbb{Z}_2$ *tiene componentes* $(1,1)$, *así que*

$$|\alpha+1\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix},$$

lo cual coincide con la etiquetación predeterminada. Ésto es importante para poder asignar estados físicos a las etiquetas del espacio de fase discreto en el caso de sistemas compuestos.

Utilizando las construcciones del capítulo siguiente, podemos verificar que el siguiente conjunto es un conjunto maximal de bases mutuamente insesgadas del espacio

de Hilbert $\mathcal{H} = \mathbb{C}^4$*:*

$$\mathcal{T}(0,1) \leftrightarrow \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\}, \tag{3.101}$$

$$\mathcal{T}(1,0) \leftrightarrow \left\{ \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ -1 \\ -1 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} \right\}, \tag{3.102}$$

$$\mathcal{T}(1,1) \leftrightarrow \left\{ \frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ -i \\ -i \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ i \\ i \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ i \\ -i \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ -i \\ i \end{pmatrix} \right\}, \tag{3.103}$$

$$\mathcal{T}(1,\alpha) \leftrightarrow \left\{ \frac{1}{2}\begin{pmatrix} 1 \\ -i \\ -1 \\ -i \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1 \\ -i \\ 1 \\ i \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1 \\ i \\ 1 \\ -i \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1 \\ i \\ -1 \\ i \end{pmatrix} \right\} \tag{3.104}$$

$$\mathcal{T}(1,\alpha+1) \leftrightarrow \left\{ \frac{1}{2}\begin{pmatrix} 1 \\ -i \\ -i \\ -1 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1 \\ -i \\ i \\ 1 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1 \\ i \\ i \\ -1 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1 \\ i \\ -i \\ 1 \end{pmatrix} \right\}. \tag{3.105}$$

Dadas las bases, utilizamos la misma convención que en el ejemplo anterior, asignamos el primer vector de cada base al rayo con la pendiente correspondiente. Así por ejemplo la primera base corresponde a los eigenvectores de los operadores de traslación $D(0,u)$*. Con las bases asignadas podemos formar los operadores puntuales y enseguida la función de Wigner para cualquier estado cuántico válido. A manera ilustrativa de nuevo calculamos el operador puntual que corresponde al origen:*

$$A(0,0) = \sum_{\lambda \ni (0,0)} Q(\lambda) - I = \begin{pmatrix} 1 & \frac{i}{2} & \frac{i}{2} & \frac{i}{2} \\ -\frac{i}{2} & 0 & \frac{1}{2} & \frac{1}{2} \\ -\frac{i}{2} & \frac{1}{2} & 0 & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 \end{pmatrix}.$$

Vamos graficar la función de Wigner de tres estados cuánticos. Si denotamos la base estándar de $\mathbb{C}^2$*,* $|0\rangle$ *por* $|\uparrow\rangle$ *y* $|1\rangle$ *por* $|\downarrow\rangle$ *entonces podemos etiquetar al eje horizontal del espacio de fase como De una manera análoga, podemos etiquetar a los elementos del eje*

0	1	α	$\alpha+1$
$\|00\rangle$	$\|01\rangle$	$\|10\rangle$	$\|11\rangle$
$\|\uparrow\uparrow\rangle$	$\|\uparrow\downarrow\rangle$	$\|\downarrow\uparrow\rangle$	$\|\downarrow\downarrow\rangle$

Cuadro 3.1: Espacio de fase discreto etiquetado por los estados de dos qubits.

vertical con otra base ortonormal de $\mathbb{C}^4$*, los que corresponden al conjunto de eigenvectores simultáneos de los operadores de desplazamiento horizontales. Denotemos a los*

eigenvectores del segundo conjunto de las MUBs por los estados $|{\rightarrow}{\rightarrow}\rangle, |{\rightarrow}{\leftarrow}\rangle, |{\leftarrow}{\rightarrow}\rangle$ *y* $|{\leftarrow}{\leftarrow}\rangle$*. Con ésto podemos etiquetar al espacio de fase discreto de la siguiente de la manera en que aparece en la figura 3.2.*

$\|{\leftarrow}{\leftarrow}\rangle$	$\circ$	$\circ$	$\circ$	$\circ$
$\|{\leftarrow}{\rightarrow}\rangle$	$\circ$	$\circ$	$\circ$	$\circ$
$\|{\rightarrow}{\leftarrow}\rangle$	$\circ$	$\circ$	$\circ$	$\circ$
$\|{\rightarrow}{\rightarrow}\rangle$	$\circ$	$\circ$	$\circ$	$\circ$
	$\|{\uparrow}{\uparrow}\rangle$	$\|{\uparrow}{\downarrow}\rangle$	$\|{\downarrow}{\uparrow}\rangle$	$\|{\downarrow}{\downarrow}\rangle$

Cuadro 3.2: Etiquetación del espacio de fase discreto para $\mathrm{GF}(2^2)$ por eigenestados.

Con tal etiquetación, graficamos la función de Wigner de los siguientes estados cuánticos:

$$|\psi_1\rangle = |{\uparrow}{\uparrow}\rangle, \quad y \quad |\psi_2\rangle = \frac{1}{\sqrt{2}}\left(|{\uparrow}{\downarrow}\rangle - |{\downarrow}{\uparrow}\rangle\right).$$

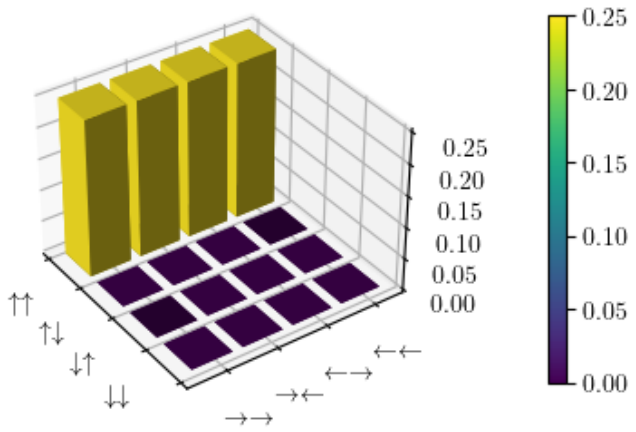


Figura 3.9: Función de Wigner del estado $|{\uparrow}{\uparrow}\rangle$.

Podemos notar que en la figura (3.9), sumando la función de Wigner sobre la primera recta vertical en el espacio de fase obtenemos la probabilidad de que el sistema se encuentre en el estado $|{\uparrow}{\uparrow}\rangle$*. Dado que el estado es precisamente* $|{\uparrow}{\uparrow}\rangle$*, la suma es igual a* 1*. En cambio, en la figura (3.10), el estado está en una superposición equitativa de los estados* $|{\uparrow}{\downarrow}\rangle$ *y* $|{\downarrow}{\uparrow}\rangle$*, por lo tanto la probabilidad de observar* $|{\uparrow}{\downarrow}\rangle$ *ó* $|{\downarrow}{\uparrow}\rangle$ *es igual a* $\frac{1}{2}$*. En cambio, la probabilidad de observar el estado* $|{\uparrow}{\uparrow}\rangle$ *ó el estado* $|{\downarrow}{\downarrow}\rangle$ *es nula, algo se puede observar al sumar la primera y recta vertical (respectivamente). Por otro lado, la probabilidad de observar el eigenestado asignado a la primera recta horizontal*

$$|\psi\rangle = \frac{1}{2}\begin{pmatrix}1\\1\\1\\1\end{pmatrix},$$

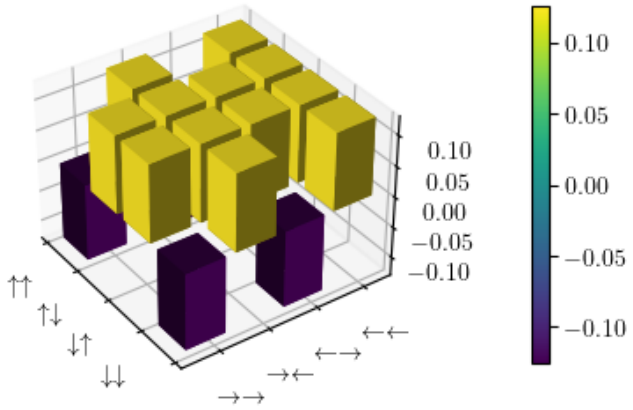


Figura 3.10: Función de Wigner del estado $\frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$.

en el sistema cuántico es

$$|\langle\psi|\psi_2\rangle|^2 = \left|\frac{1}{\sqrt{2}}(\langle\psi|\uparrow\downarrow\rangle - \langle\psi|\downarrow\uparrow\rangle)\right|^2 = \left|\frac{1}{2\sqrt{2}} - \frac{1}{2\sqrt{2}}\right|^2 = 0.$$

Ésto concuerda con la suma de la función de Wigner sobre la primera recta horizontal, en donde los puntos se anula gracias a la negatividad.

Por último, grafiquemos un estado 'maximalmente entrelazado', conocidos como estados GHZ. En la base estándar de $\mathbb{C}^2 \otimes \mathbb{C}^2$, se expresa como

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

De acuerdo a la elección de la base del campo, éstos estados corresponden a los estados de $\mathbb{C}^4$: $|0\rangle$ y $|\alpha+1\rangle$ respectivamente, los cuales la red Q asigna a la primera y última recta vertical del espacio de fase discreto:

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |\alpha+1\rangle).$$

La gráfica de la función $W_{|GHZ\rangle}$ se muestra en la figura (3.11). La interpretación es muy similar al estado anterior $|\psi_2\rangle$.

En éste capítulo hemos descrito el procedimiento y razonamiento de la construcción de la versión de Wootters de la función de Wigner, a la que de aquí en adelante llamaremos la *construcción estándar*. En el siguiente capítulo realizamos una definición alternativa de la función de Wigner. La metodología permanece igual, pero se utilizan conjuntos de bases mutuamente insesgadas que no son unitariamente equivalentes a las que se obtienen mediante el método de Wootters. La construcción de éstas bases difiere en como se *cubre* el espacio de fase discreto con *lineas*. Es más general que la versión de Wootters en el sentido de que se recupera dicha versión cuando las líneas son las rectas en el espacio de fase, pero, podemos obtener otras maneras de cubrirlo que aun preservan las propiedades geométricas. La idea es utilizar éstas estructura geométricas y las MUBs alternativas que producen, para formar una función de Wigner discreta distinta a la de Wootters.

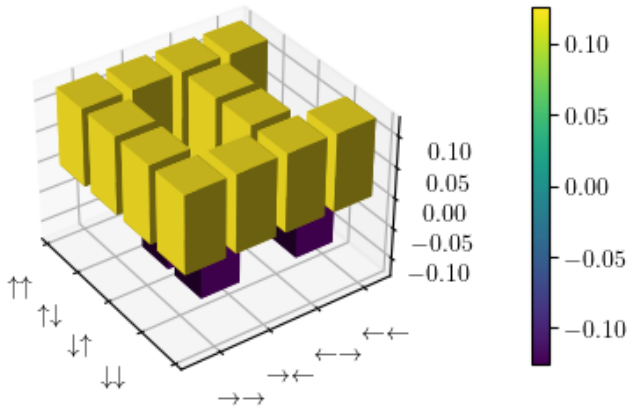


Figura 3.11: Función de Wigner del estado $|GHZ\rangle$.

Capítulo 4

Construcción no-estándar

Para construir la función de Wigner discreta siguiendo la metodología de Wootters y Gibbons, es necesario obtener al menos un eigenvector mutuo para cada una de las $d+1$ estrías (recordemos que solo uno es necesario porque la propiedad de covarianza bajo traslaciones determina el resto). La obtención de los eigenvectores sería analíticamente y computacionalmente latoso conforme la dimensión va creciendo. Por suerte existen múltiples construcciones explícitas de bases mutuamente insesgadas, además Godsil y Roy [36] probaron que las construcciones de MUBs más conocidas, debido a Iványovic, Wootters y Fields [14], Klappenecker [37] y Bandyophyay [35] son todos unitariamente equivalentes en el sentido de que existe una transformación unitaria que nos lleva de una base a otra.

Gibbons y Wootters utilizaron los resultados de Bandyophyay et al para demostrar que los operadores de desplazamiento que corresponden a las traslaciones invariantes de una estría son simultáneamente diagonalizableis. Por otro lado se ha descubierto que las MUBs están directamente relacionadas con otros problemas en diversas áreas de las matemáticas, como en el algebra combinatoria y la matemática discreta. La elección de asignar elementos de bases mutuamente insesgadas a rectas en el espacio de fase es lo que distingue la construcción de Wootters de otros métodos de construcción de funciones de Wigner. Como hemos visto, la idea reside en hacer una partición del espacio de fase discreto en *rectas* paralelas llamadas estrías, pero, la manera en que Wootters hace la partición no es la única manera de hacerlo. Existen otras formas de separar una malla de $d \times d$ en conjuntos de puntos tales que cualesquiera dos puntos distintos residen en uno solo de esos conjuntos. Éstos objetos han sido estudiados en otras áreas de las matemáticas, por ejemplo en la geometría finita donde llevan el nombre de *plano afín* [15].

Definición 20 (Plano afín)**.** *Un plano afín de orden d es un objeto combinatorio que consiste de un conjunto de d^2 puntos, junto con $d(d+1)$ conjuntos de puntos llamados lineas, tales que cualesquiera dos puntos distintos pasa por una única linea. En éste caso las lineas se pueden agrupar en $d+1$ clases de lineas "paralelas" de tamaño d, particionando a todo el conjunto de puntos.*

En su libro de geometría finita [38] Dembowski comenta que todas las técnicas de construcción de planos afines conocidas utilizan espacios vectoriales sobre campos finitos de alguna manera esencial. Es por ésto que éstas construcciones siempre nos llevan a planos de orden de una potencia de un primo. Al igual que en la construcción de MUBs en el espacio $\mathbb{C}^d$, es un gran problema abierto de la geometría finita demostrar

la existencia o no existencia de planos cuyo orden no es una potencia de un primo. A parte de ésta aparente coincidencia, en su artículo [15], Kantor muestra que realmente hay una relación íntima entre planos afines y las bases mutuamente insesgadas. Ésto lo hace recordando algunos resultados más viejos que conectaban planos afínes con otras estructuras algebráicas llamadas *coberturas simplécticas* y con familias de subespacios unidimiensionales mutuamente ortogonales. El método de construcción de MUBs de Kantor es lo suficientemente general para incluir a las construcciones conocidas (en particular la de Wootters) y además permite construir MUBs que *no* son unitariamente equivalente a las construcciones estándares. La idea de éste capítulo es utilizar coberturas simplécticas distintas a los de Wootters para obtener bases de MUBs no unitariamente equivalentes, y por lo tanto una función de Wigner distinta que por construcción sigue preservando la propiedad tomográfica. Unos de los objetivos de éste capítulo es exponer dos ejemplos específicos de sistemas cuánticos para los cuales podemos construir la función de Wigner no estándar: para un sistema de cinco qubits y un sistema de tres qutrits.

Para construir las MUBs de manera explícita, utilizaremos los resultados de Kanat [13], quien nos muestra que de *presemicampos simplécticos* es posible obtener coberturas simplécticas las cuales a su vez nos producen MUBs por medio de los resultados de Kantor, éste procedimiento se organiza como en la figura (4.1). Kanat expone una

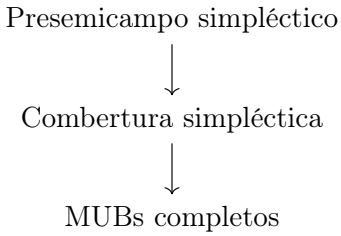


Figura 4.1: Metodología resumida de Kanat.

relación entre un conjunto completo de MUBs y la descomposición ortogonal del álgebra de Lie de las matrices $d \times d$ sobre $\mathbb{C}$ de traza nula, denotado $\mathfrak{L} = \mathfrak{sl}_d(\mathbb{C})$, donde el producto de Lie está dado por el conmutador de matrices. Una descomposición de un álgebra de Lie simple $\mathfrak{L}$ en una suma directa de subalgebras de Cartan

$$\mathfrak{L} = \mathfrak{H}_0 \oplus \mathfrak{H}_1 \oplus \cdots \oplus \mathfrak{H}_n, \tag{4.1}$$

es una descomposición ortogonal si las subálgebras $\mathfrak{H}_i$ son ortogonales entre si respecto a la forma de Killing en $\mathfrak{L}$. Las subálgebras de Cartán de $\mathfrak{sl}_d(\mathbb{C})$ consisten de matrices sin traza las cuales son diagonales y resulta que están en correspondencia con las bases de un conjunto completo de MUBs. Kanat cita al siguiente teorema de Boykin et al [39]:

Teorema 2 (Boykin et al, Teorema 5.2)**.** *Los conjuntos maximales de MUBs en $\mathbb{C}^d$ están en correspondencia con descomposiciones ortogonales del álgebra de Lie $\mathfrak{sl}_d(\mathbb{C})$, donde los subálgebras de Cartán de la descomposición son cerrados bajo la operación de adjunción.*

La prueba consiste en demostrar que las bases de un conjunto completo de MUBs $\mathcal{B} = \{B_0, B_1, \ldots, B_d\}$ están en correspondencia con la subálgebra de Cartan $\mathfrak{H}_i$ la cual

consiste de las matrices sin traza que son diagonales respecto a la base B_i. De aquí podemos ver la relación con el trabajo de Bandyophyay et al. y como consecuencia, con la construcción estándar de Wootters, ya que la idea básicamente se reduce a encontrar una partición de ciertos operadores tales que conmuten entre sí. En dicho artículo Kanat adicionalmente construye MUBs a partir de *funciones planares* y muestra que el grupo de automorfismos de un conjunto completo de MUBs es isomorfo al grupo de automorfismos de la descomposición ortogonal de $\mathfrak{sl}_d(\mathbb{C})$. No es necesario estudiar la descomposición ortogonal de $\mathfrak{sl}_d(\mathbb{C})$ para construir el conjunto completo de MUBs. Basta con construir coberturas simplécticas las cuales nos particionan a los operadores de Pauli generalizados de tal manera que podemos utilizar el teorema de Bandyophyay para garantizar la existencia de las MUBs.

Comenzamos por definir a los operadores de desplazamiento que actúan sobre el espacio de Hilbert $\mathcal{H} = \mathbb{C}^d$ donde $d = p^n$ para un primo p. Consideremos a un campo finito $\mathbb{F}$ de cardinalidad d como un espacio vectorial V unidimensional. La cardinalidad de V es igual a d y etiquetemos a la base estándar de $\mathbb{C}^d$ por los elementos de V, es decir, $\{|e_w\rangle : w \in V\}$. A continuación definimos a los operadores de Pauli generalizados, los cuales serán indexados por los elementos de V.

Definición 21. *Sea $\omega \in \mathbb{C}$ la p-ésima raíz primitiva de la unidad y sean $u, v \in V$. Definimos a los operadores de Pauli generalizados como:*

$$X(u) : |e_w\rangle \mapsto |e_{w+u}\rangle \tag{4.2}$$

$$Z(v) : |e_w\rangle \mapsto \omega^{\mathrm{tr}(vw)} |e_w\rangle . \tag{4.3}$$

Además, un operador de desplazamiento arbitrario se define como:

$$D(u, v) = X(u)Z(v). \tag{4.4}$$

Las matrices $D(u, v)$ forman una base del espacio de matrices complejas de tamaño $d \times d$ de traza nula y son los operadores de despalzamiento que también ya conocemos. Además de ésto, las matrices $D(u, v)$ con u y v distintos del vector cero, generan al algebra de Lie $\mathfrak{sl}_n(\mathbb{C})$. Notemos que ésta definición no está dada por potencias de los operadores X y Z ya que ésto solo tiene sentido cuando los elementos son los enteros módulo p. Pero, en caso de que $V = \mathbb{Z}_p$, la definición anterior se reduce a nuestra definición del capítulo anterior ya que la traza (considerando a $\mathbb{Z}_p$ como una extensión de Galois de grado 1) deja invariante a los elementos del subcampo. Antes de probar algunas propiedades de los operadores de desplazamiento, vamos a ligar ésta nueva definición con la de Wootters del capítulo anterior.

Proposición 19. *Denotemos a los operadores de desplazamiento que actúan sobre un espacio de Hilbert de dimensión prima p, $\mathcal{H}_p$, por $D_p(a, b)$. Sea $D(u, v) = X(u)Z(v)$ para $u, v \in V$, y sea ε una base del campo. Si $\tilde{\varepsilon}$ es una base dual de ε, entonces*

$$D(u, v) = D_p(u_1, \tilde{v}_1) \otimes \cdots \otimes D_p(u_n, \tilde{v}_n), \tag{4.5}$$

donde $u_1, \ldots, u_n$ son los componentes de u en la base ε y $\tilde{v}_1, \ldots, \tilde{v}_n$ son los componentes de v en la base dual, y donde la igualdad es en sentido del isomorfismo entre los productos tensoriales de $\mathcal{H}_p$ y el espacio $\mathcal{H}$.

Recordemos que Wootters llegó a la condición de conmutatividad de los operadores de Pauli a partir de la construcción de la malla cuántica, la cual a su vez estaba sujeta

a la invarianza de los subespacios (lineas) del espacio de fase discreto bajo traslaciones. Ahora deseamos identificar la condición necesaria de la conmutatividad sin restringirnos (por el momento) por las propiedades de la malla cuántica. Primero definimos una forma bilineal alternante sobre el espacio vectorial $W = V \oplus V$ de dimensión $2n$ sobre el subcampo primo de la extensión de Galois.

Definición 22. *Sea $W = V \oplus V$. Definimos la forma bilineal alternante*

$$\langle \cdot, \cdot \rangle : W \to \mathbb{Z}_p$$

para todo $(u, v) \in W$ de la siguiente manera:

$$\langle (u, v), (u', v') \rangle = \operatorname{tr}\left(uv' - vu'\right), \tag{4.6}$$

donde de nuevo $\operatorname{tr} : \mathbb{F} \to \mathbb{Z}_p$ es la traza de la extensión $\mathrm{GF}(p^n)$ al campo primo.

Notemos que la forma bilineal es una forma simpléctica. Continuemos expresando la acción que tienen los operadores de desplazamiento sobre los elementos de la base estándar. Por definición tenemos que:

$$\begin{aligned} X(u)Z(v)\left|e_w\right\rangle &= X(u)\omega^{\operatorname{tr}(vw)}\left|e_w\right\rangle && (4.7)\\ &= \omega^{\operatorname{tr}(vw)}\left|e_{w+u}\right\rangle. && (4.8) \end{aligned}$$

Por lo tanto

$$\begin{aligned} Z(v)X(u)\left|e_w\right\rangle &= Z(v)\left|e_{w+u}\right\rangle && (4.9)\\ &= \omega^{\operatorname{tr}(v(w+u))}\left|e_{w+u}\right\rangle && (4.10)\\ &= \omega^{\operatorname{tr}(vw)+\operatorname{tr}(vu)}\left|e_{w+u}\right\rangle && (4.11)\\ &= \omega^{\operatorname{tr}(vu)}\left(\omega^{\operatorname{tr}(vw)}\left|e_{w+u}\right\rangle\right) && (4.12)\\ &= \omega^{\operatorname{tr}(vu)}X(u)Z(v)\left|e_w\right\rangle. && (4.13) \end{aligned}$$

Así que los productos de X y Z satisfacen la relación de conmutatividad: $Z(v)X(u) = \omega^{\operatorname{tr}(vu)}X(u)Z(v)$ para todo $u, v \in V$. Utilizando ésto, podemos observar que los operadores de desplazamiento satisfacen la propiedad de traslación análoga a la de los operadores de desplazamiento $D_p(a, b)$:

$$\begin{aligned} D(u, v)D(u', v') &= X(u)Z(v)X(u')Z(v') && (4.14)\\ &= X(u)\left(\omega^{\operatorname{tr}(vu')}X(u')Z(v)\right)Z(v') && (4.15)\\ &= \omega^{\operatorname{tr}(vu')}X(u + u')Z(v + v') && (4.16)\\ &= \omega^{\operatorname{tr}(vu')}D(u + u', v + v'). && (4.17) \end{aligned}$$

La propiedad de traslación implica la siguiente relación de conmutatividad:

$$\begin{aligned} D(u', v')D(u, v) &= \omega^{\operatorname{tr}(v'u)}D(u' + u, v' + v) && (4.18)\\ &= \omega^{\operatorname{tr}(uv')}D(u + u', v + v') && (4.19)\\ &= \omega^{\operatorname{tr}(uv')}\omega^{-\operatorname{tr}(vu')}D(u, v)D(u', v') && (4.20)\\ &= \omega^{\operatorname{tr}(uv'-vu')}D(u, v)D(u', v') && (4.21)\\ &= \omega^{\langle (u,v),(u',v')\rangle}D(u, v)D(u', v'). && (4.22) \end{aligned}$$

Usando las propiedades (4.17) y (4.22), podemos calcular el conmutador de dos operadores de desplazamiento e identificar la condición para que el conmutador se anule.

Proposición 20. *Dos operadores de desplazamiento $D(u,v)$ y $D(u',v')$ conmutan si y solo si la forma simpléctica se anula para (u,v) y (u',v'), i.e.,*

$$\langle (u,v),(u',v')\rangle = 0. \tag{4.23}$$

Demostración. Un cálculo directo nos muestra que

$$\begin{aligned}
[D(u,v),D(u',v')] &= D(u,v)D(u',v') - D(u',v')D(u,v) && (4.24)\\
&= D(u,v)D(u',v') - \omega^{\langle (u,v),(u',v')\rangle} D(u,v)D(u',v') && (4.25)\\
&= \left(1-\omega^{\langle (u,v),(u',v')\rangle}\right) D(u,v)D(u',v') && (4.26)\\
&= \omega^{\mathrm{tr}(v\cdot u')}\left(1-\omega^{\langle (u,v),(u',v')\rangle}\right) D(u+u',v+v'). && (4.27)
\end{aligned}$$

□

Notemos que podemos identificar el espacio de fase discreto con el espacio $W = V \oplus V$. La idea de Wootters fue identificar subespacios unidimensionales del espacio de fase tales que los operadores de desplazamiento correspondientes conmutaran. Pero, con la condición (4.23) podemos identificar *más* agrupaciones de los puntos del espacio de fase discreto que también anulan la forma simpléctica. A las agrupaciones maximales Kantor las llama coberturas simplécticas.

Definición 23 (Cobertura simpléctica)**.** *Una cobertura simpléctica Σ de un espacio simpléctico $W = V \oplus V$ es una familia Σ de $d+1$ subespacios de W de dimensión n totalmente isotrópicos, tales que su intersección uno-a-uno es el espacio trivial* 0.

Un n-espacio totalmente isotrópico es un subespacio de dimensión n en donde una forma bilineal se anula. En una cobertura simpléctica, todo vector de $V \oplus V$ está en uno y solo un miembro de Σ, asi que Σ particiona a los vectores no nulos. Kantor nos dice que ésto determina un plano afín de orden d, cuyos puntos son los vectores en $V \oplus V$ y cuyas lineas son traslaciones de los miembros de Σ por los elementos de $V \oplus V$. Entonces siempre podemos obtener un plano afín a partir de una cobertura simpléctica y resulta que la partición en lineas rectas de Wootters del espacio de fase discreto es precisamente un plano afín, producido por una cobertura de Desargues (ésto lo veremos en los ejemplos más adelante).

Con la construcción anterior de los operadores de desplazamiento, y utilizando los resultados de Kantor [40], Kanat concluye que si $\Sigma = \{W_0, W_1, \ldots, W_d\}$ es una cobertura simpléctica, entonces existe una descomposición ortogonal del álgebra de Lie $\mathfrak{sl}_n(\mathbb{C})$ donde las subálgebras $\mathfrak{H}_i$ son generadas por los operadores de desplazamiento agrupados por los puntos del subespacio W_i:

$$\mathfrak{H}_i = \langle D(u,v) : (u,v) \in W_i\rangle. \tag{4.28}$$

De la descomposición ortogonal de $\mathfrak{sl}_d(\mathbb{C})$ se pueden obtener un conjunto de $d+1$ MUBs a partir de la diagonalización de los operadores de desplazamiento que son generadores de las subálgebras de Cartán [39], ésto es basicamente lo que Wootters hizo mediante los resultados de Bandyophyay. Por suerte, Kantor y Kanat nos dan una manera de obtener los MUBs *directamente* de la cobertura simpléctica, sin necesidad de diagonalizar a los operadores de Pauli.

Por otro lado, es natural pensar que distintas coberturas simplécticas nos darán distintos conjuntos de MUBs, pero ésto no es el caso en general. De hecho bajo un significado particular de equivalencia, muchas de las coberturas que parecen ser distintas, en realidad son iguales. La motivación principal de éste trabajo es que para algunas dimensiones es posible obtener coberturas simplécticas no equivalentes. Kantor demuestró que la inequivalencia de coberturas simplécticas conlleva a la inequivalencia de MUBs [15]:

Teorema 3 (Kantor ([15]), Teorema 2.3 (Inequivalencia))**.** *Toda cobertura simpléctica* Σ *de* $V \oplus V$ *determina una conjunto completo de* $d+1$ *MUBs en* $\mathbb{C}^d$*. Además, sea* Σ' *es otra cobertura simpléctica de* $V \oplus V$*, entonces* Σ *y* Σ' *son equivalentes bajo una transformación lineal de* $V \oplus V$ *que preserva la forma bilineal alternante si y solo si las MUBs respecto a* Σ *y* Σ' *son equivalentes bajo una transformación unitaria de* $\mathbb{C}^d$*.*

Como consecuencia del teorema (3), si logramos encontrar una cobertura simpléctica no equivalente, (i.e., encontrar un plano afín no isomorfo al de Wootters), obtendremos bases mutuamente insesgadas que *no* son unitariamente equivalentes. Podremos aplicar el método de construcción de Wootters con éstas bases no equivalentes para obtener operadores puntuales distintos a los de Wootters y por lo tanto una definición alternativa de la función de Wigner discreta, que además, por construcción, preserva la propiedad tomográfica. Para ver ésto, describimos el método que utiliza Kanat para obtener las expresiones explicítas de las MUBs, y como mencionamos anteriormente, dadas algunas sutilezas de los campos de característica par, dividimos la descripción en dos casos.

4.1. Característica impar

De la sección anterior sabemos que un cobertura simpléctica nos produce un plano afín y una descomposición ortogonal de $\mathfrak{sl}_d(\mathbb{C})$, la cual a su vez nos brinda un conjunto completo de MUBs por medio de la diagonalización simultánea de los operadores de desplazamiento conmutativos. Existen múltiples construcciones explícitas de los eigenvectores de los subconjuntos de $D(\alpha)$, iniciando con la construcciones de Ivanovic y Wootters. La mayoría son equivalentes y son un caso particular de los métodos de Kantor y Kanat. Para nuestro trabajo, utilizaremos las construcciones de Kanat y empezamos por demostrar el siguiente teorema que nos permitirá expresar las MUBs a partir de una cobertura simpléctica. Usaremos la forma simpléctica (4.6) y consideramos a V como el espacio unidimensional sobre la extensión de Galois, i.e., $V = \mathbb{F} = \mathrm{GF}(p^n)$ donde en ésta sección, p es un número primo impar. Recordemos que $\{|e_w\rangle : w \in V\}$ es la base estándar de $\mathbb{C}^{p^n}$ etiquetada por los elementos de la extensión de Galois.

Teorema 4. *Sea* Σ *una cobertura simpléctica de* $W = V \oplus V$ *y sea* $h : V \to V$ *un mapeo lineal tal que*

$$\{(u, h(u)) : u \in V\} \in \Sigma. \tag{4.29}$$

Entonces para todo $v \in V$*, el vector dado por*

$$|b_{h,v}\rangle = \sum_{w \in V} \omega^{\mathrm{tr}\left(\frac{1}{2}wh(w)+vw\right)} |e_w\rangle \tag{4.30}$$

es un eigenvector del operador de desplazamiento $D(u, h(u))$ *para todo* $u \in V$*.*

Demostración. Calculando directamente obtenemos:

$$D(u,h(u))\,|b_{h,v}\rangle = \sum_{w\in V} \omega^{\mathrm{tr}\left(\frac{1}{2}wh(w)+vw\right)} X(u)Z(h(u))\,|e_w\rangle \tag{4.31}$$

$$= \sum_{w\in V} \omega^{\mathrm{tr}\left(\frac{1}{2}wh(w)+vw\right)} \omega^{\mathrm{tr}(h(u)w)}\,|e_{w+u}\rangle \tag{4.32}$$

$$= \sum_{w\in V} \omega^{\mathrm{tr}\left(\frac{1}{2}wh(w)+vw+h(u)w\right)}\,|e_{w+u}\rangle \tag{4.33}$$

$$= \sum_{w\in V} \omega^{\mathrm{tr}\left(\frac{1}{2}(w-u)h(w-u)+v(w-u)+h(u)(w-u)\right)}\,|e_w\rangle \tag{4.34}$$

$$= \sum_{w\in V} \omega^{\mathrm{tr}\left(\frac{1}{2}(w-u)h(w)+\frac{1}{2}(w-u)h(u)+vw-vu+h(u)w-h(u)u\right)}\,|e_w\rangle\,. \tag{4.35}$$

La traza en la ecuación (4.35) se puede expresar como

$$\mathrm{tr}\left(\frac{1}{2}wh(w)+vw\right)+\frac{1}{2}\,\mathrm{tr}\left(h(u)w-uh(w)\right)-\mathrm{tr}\left(\frac{1}{2}uh(u)+vu\right), \tag{4.36}$$

pero por hipótesis $(u,h(u))$ pertenece a algún $W_i\in\Sigma$, por lo tanto

$$\mathrm{tr}\left(uh(w)-h(u)w\right)=\langle(u,h(u)),(w,h(w))\rangle=0, \tag{4.37}$$

ya que todo W_i es totalmente isotrópico respecto a la forma bilineal alternante. Así que el exponente de ω en (4.35) está dado por:

$$\mathrm{tr}\left(\frac{1}{2}wh(w)+vw\right)-\mathrm{tr}\left(\frac{1}{2}uh(u)+vu\right). \tag{4.38}$$

Con ésto retomamos el cálculo inicial y verificamos que $|b_{h,v}\rangle$ efectivamente es un eigenvector de $D(u,h(u))$:

$$D(u,h(u))\,|b_{h,v}\rangle = \sum_{w\in V} \omega^{\mathrm{tr}\left(\frac{1}{2}wh(w)+vw\right)-\mathrm{tr}\left(\frac{1}{2}uh(u)+vu\right)}\,|e_w\rangle \tag{4.39}$$

$$= \omega^{-\mathrm{tr}\left(\frac{1}{2}uh(u)+vu\right)} \sum_{w\in V} \omega^{\mathrm{tr}\left(\frac{1}{2}wh(w)+vw\right)}\,|e_w\rangle \tag{4.40}$$

$$= \omega^{-\mathrm{tr}\left(\frac{1}{2}uh(u)+vu\right)}\,|b_{h,v}\rangle\,. \tag{4.41}$$

□

Corolario 1. *Los vectores $|b_{h,v}\rangle$ del teorema 4 son mutuamente insesgados.*

Demostración. Dado que Σ es una cobertura simpléctica, los subespacios $W_h=\{(u,h(u)):u\in\mathbb{F}\}\in\Sigma$, son totalmente isotrópicos. Por lo tanto los conjuntos de operadores

$$\{D(u,h(u)):u\in\mathbb{F}\},$$

son conjuntos maximales de operadores de Pauli conmutativos. Se sigue del teorema 1 (Bandyophyay et al.) que los conjuntos de eigenvectores simultáneos correspondientes a cada subespacio W_h son mutuamente insesgados. □

El teorema anterior nos permite diagonalizar de manera simultánea a los operadores de desplazamiento que conmutan entre si para una cobertura simpléctica dada. La cuestión natural ahora es, ¿cómo obtener coberturas simplécticas o planos afines?, y sobre todo, ¿cómo obtener coberturas que no son equivalentes? Kantor comenta que encontrar coberturas simplécticas no es trivial, pero podemos construir algunas por medio de unas estructuras algebráicas más relajadas que los campos finitos, llamados *presemicampos* y *semicampos*.[1] En la geometría finita el uso de presemicampos y semicampos surge en la descripción de ciertos planos proyectivos, por lo que su uso aparece naturalemente en la construcción de coberturas. Introducimos los conceptos necesarios pero no detallaremos mucho ya que para éste trabajo nos basta con usar algunos de los ejemplos dados por Kantor [15].

Definición 24 (Presemicampo y semicampo)**.** *Un presemicampo es un anillo sin divisores del cero, y con solo la propiedad distributiva (derecha e izquierda). Un semicampo es un presemicampo con una identidad multiplicativa.*

A partir de un campo finito $\mathbb{F}$ podemos obtener un presemicampo finito al introducir una operación nueva $\circ : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$. La operación de suma es la del campo finito, por lo tanto la definición (24) nos dice que el semicampo finito es el conjunto $\mathbb{F}$ tal que

1. $\mathbb{F}$ es un grupo abeliano bajo la suma, con identidad 0.
2. Si $x \circ y = 0$, entonces $x = 0$ ó $y = 0$.
3. Satisface las propiedades distributivas

$$x \circ (y + z) = x \circ y + x \circ z, \quad (x + y) \circ z = x \circ z + y \circ z.$$

Notemos que todo campo finito es un semicampo y un presemicampo. Kantor muestra que todo presemicampo determina un cobertura Σ del espacio $V \oplus V$ por medio de la multiplicación. Ésta cobertura consiste de los subespacios

$$\{(0, v) : v \in \mathbb{F}\}, \quad \{(u, u \circ m) : u \in \mathbb{F}\} \quad \text{para todo } m \in \mathbb{F}. \tag{4.42}$$

Decimos que un presemicampo es *simpléctico* si la cobertura que genera es simpléctica respecto a algúna forma bilineal alternante. La relación entre la cobertura y el plano afín es de la siguiente manera: sea $\mathcal{A}(\Sigma)$ la geometría de puntos y líneas correspondiente a una cobertura Σ, donde los puntos están dados por los vectores de $\mathbb{F} \oplus \mathbb{F}$ y las líneas son las clases laterales $W + v$ donde $W \in \Sigma$ y $v \in \mathbb{F}$. Entonces $\mathcal{A}(\Sigma)$ es un plano afín de orden $d = |\mathbb{F}|$:

- Dos puntos distintos u, v están sobre una única línea, la cual está dada por la clase $W + v$ donde $u - v \in W$.
- Dada una línea λ y un punto v que no pertenece a ella, existe una única línea que pasa por v y que es disjunta a λ. Ésta linea está dada por $W + v$ si λ es una clase lateral de W.[2]

[1] Existen coberturas simplécticas que no provienen de un semicampo simpléctico, pero para nuestra construcción alternativa basta utilizar aquellos que sí provienen de semicampos.

[2] La noción de paralelismo nos permite adjuntar una nueva "línea al infinito" que contiene a todas las clases laterales paralelas, construyendo así a un plano proyectivo de orden d [41].

- Toda línea contiene exáctamente d puntos.

Entonces dado un presemicampo simpléctico obtenemos una cobertura simpléctica y un plano afín. Dada la cobertura podemos generar el conjunto completo de MUBs simplemente utilizando la operación del presemicampo y el siguiente teorema.

Teorema 5 (Kanat ([13]) Teorema 3.3)**.** *Sea $F = \mathrm{GF}(p^n)$. Si $(F, +, \circ)$ es un presemicampo simpléctico finito de característica impar, entonces los conjuntos*

$$B_\infty = \{|e_w\rangle : w \in F\}, \quad B_m = \{|b_{m,v}\rangle : v \in F\} \tag{4.43}$$

donde

$$|b_{m,v}\rangle = \frac{1}{\sqrt{d}} \sum_{w \in F} \omega^{\mathrm{tr}\left(\frac{1}{2} w(w \circ m) + vw\right)} |e_w\rangle \,, \tag{4.44}$$

para todo $m \in F$ forman un conjunto completo de MUBs.

Demostración. Si la cobertura que genera la operación del presemicampo es una cobertura simpléctica, entonces el teorema 4 nos permite construir el conjunto completo de MUBs donde el mapeo $h : V \to V$ está dado por la operación $\circ$ del presemicampo. La linealidad de h se sigue de la distributividad de la operación del presemicampo. □

Para poder utilizar utilizar el teorema 5, debemos formar un presemicampo simpléctico. Dado que todo presemicampo forma una cobertura Σ, solo hemos trasladado la dificultad de encontrar una cobertura simpléctica a la busqueda de presemicampos cuya cobertura es simpléctica, i.e., una cobertura de $d + 1$ subespacios totalmente isotrópicos. Por suerte, en [41] Kantor genera múltiples coberturas simplécticas a partir de presemicampos y en lo que sigue del trabajo hemos elegido algunos de ellos para poder construir MUBs no equivalentes. El ejemplo más sencillo es el que está dado simplemente por la multiplicación del campo finito.

Definición 25 (Cobertura Desarguesiana)**.** *Sea $\mathbb{F} = \mathrm{GF}(p^n)$ un campo finito. En particular $\mathbb{F}$ es un presemicampo con la operación*

$$w \circ m = wm. \tag{4.45}$$

La cobertura simpléctica generada por éste presemicampo se conoce como el cobertura Desarguesiana y consiste simplemente de los subespacios unidimensionales de $V \oplus V$ sobre $\mathbb{F}$.

Las MUBs que Godsil y Roy probaron que son unitariamente equivalentes a las MUBs "estándares", incluyendo a la de Wooters, son casos específico de MUBs generados por una cobertura Desarguesiana. Por lo tanto utilizando la definición 25 y el teorema 5 podemos construir las bases mutuamente insesgadas de Wootters y Gibbons. En éste caso la cobertura simpléctica Σ está dada por los subespacios

$$0 \oplus V \quad \text{y} \quad \{(u, mu) : u \in V\}, \quad m \in V, \tag{4.46}$$

y el plano afín correspondiente está determinado por las rectas:

$$x = 0 \quad y = mx, \quad x \in \mathrm{GF}(p^n), \tag{4.47}$$

las cuales reconocemos como los rayos de Wootters. Se sigue que para todo $v \in V$, el vector

$$|b_{m,v}\rangle = \sum_{w \in V} \omega^{\mathrm{tr}\left(\frac{1}{2}mw^2+vm\right)} |e_w\rangle\,, \tag{4.48}$$

es un eigenvector simultáneo de los operadores de desplazamiento $D(u, mu)$ con $u \in \mathrm{GF}(p^n)$. En éste caso el número $m \in \mathrm{GF}(p^n)$ identifica la pendiente del rayo y por lo tanto identifica a una de las estrías de Wootters.

En vista del teorema de no-equivalencia de Kantor, dado una cobertura simpléctica no equivalente a la Desarguesiana, podremos obtener un conjunto de MUBs no equivalentes a las de Wootters. Para característica impar el siguiente presemicampo genera una cobertura simpléctica no equivalente a la Desarguesiana [41].

Definición 26 (Campo torcido de Albert)**.** *Sea n impar y sea $s \in \mathbb{N}$ un primo relativo de n tal que $1 \leq s \leq \frac{n}{2}$ y consideremos el campo finito $\mathrm{GF}(p^n)$. La operación*

$$w \circ m = mw^{p^{n-s}} + m^{p^s} w^{p^s}, \quad m \in \mathrm{GF}(p^n), \tag{4.49}$$

brinda a $\mathrm{GF}(p^n)$ una estructura de presemicampo, conocido como el campo torcido de Albert.

Kantor muestra que éste presemicampo genera una cobertura simpléctica Σ de $V \oplus V$ que no es equivalente a la Desarguesiana. Utilizando el teorema 5 obtenemos el sguiente conjunto completo de MUBs:

$$|b_{m,v}\rangle = \sum_{w \in V} \omega^{\mathrm{tr}\left(\frac{1}{2}w(w \circ m)+aw\right)} \tag{4.50}$$

$$= \sum_{w \in V} \omega^{\mathrm{tr}\left(\frac{1}{2}\left(mw^{p^{n-s}+1}+m^{p^s}w^{p^s+1}\right)+vw\right)} |e_w\rangle\,, \tag{4.51}$$

donde $m, v \in V$. Por el teorema 3, éstas MUBs no son unitariamente equivalentes a las MUBs generadas por la ecuación (4.48). Notemos que el espacio de Hilbert de dimensión $3^3 = 27$ es el espacio de dimensión más pequeña para el cual podemos construir éste conjunto de MUBs en particular. Ésto se debe a que la cardinalidad mínima de un presemicampo propio, i.e., un presemicampo que no es un campo, es de 16 elementos [38]. Por lo tanto para característica $p = 3$, la extensión de Galois de 27 elementos es el campo finito más pequeño del cual podemos construir presemicampos propios. Más adelante utilizaremos éste ejemplo para construir y comparar dos funciones de Wigner para sistemas de tres qutrits.

4.2. Característica par

Para obtener expresiones explícitas de un conjunto completo de bases mutuamente insesgadas para el espacio de Hilbert $\mathbb{C}^d$ con $d = 2^n$, es necesario hacer modificaciones al procedimiento de la sección anterior. La metodología permanece igual, dado un presemicampo simpléctico obtenemos una cobertura simpléctica y podemos construir las MUBs de manera explícita con la operación del presemicampo, solo que la expresión de los eigenvectores de los operadores de desplazamiento involucra operaciones que no solo suceden en el campo finito si no en un *anillo de Galois*. Una idea intuitiva de porque la construcción impar no funciona en éste caso se debe a la necesidad de utilizar una

raíz primitiva compleja en las expresiones de los vectores. Por lo tanto es necesario utilizar la cuarta raíz primitiva para evitar fases de solo -1 ó 1. Los detalles técnicos son mucho más involucrados, y provienen de la construcción de códigos lineales sobre $\mathbb{Z}_4$ a partir de códigos no lineales llamados códigos de Kerdock [41].

Sea $\mathbb{F} = \mathrm{GF}(2^n)$ el campo de Galois y $\omega \in \mathbb{C}$ una cuarta raíz primitiva de la unidad. Sea $R = \mathrm{GR}(4^n)$ el anillo de Galois de característica cuatro (ver apéndice A.2 para un resumen de extensiones de anillos). Existe un elemento ξ de orden $2^n - 1$ el cual es una raiz de un único polinomio primitivo mónico $h(x)$ de grado n sobre $\mathbb{Z}_4$ que además divide a $x^{2^n-1} - 1$ en $\mathbb{Z}_4[x]$, por lo que es una $2^n - 1$-ésima raíz primitiva de la unidad en el anillo de Galois. El conjunto *Teichmüller* $T \subset R$, está dado por potencias de éste elemento,

$$T = \{0, 1, \xi, \xi^2, \ldots, \xi^{2^n-2}\}, \tag{4.52}$$

y sin el 0 es subgrupo multiplicativo de tamaño 2^n que es isomorfo a $\mathbb{F}$. En ocasiones el generador del anillo coincide con la raíz ξ, pero ésto no es el caso general. Todo elemento $x \in R$ puede ser expresado como la combinación lineal de elementos a, b del Teichmüller en la forma $x = a + 2b$. Utilizando ésta expresión multiplicativa ó 2-ádica de x, la traza del anillo de Galois, $\mathrm{tr} : R \to \mathbb{Z}_4$ se define como

$$\mathrm{tr}(x) = \left(a + a^2 + \cdots + a^{2^{n-1}}\right) + 2\left(b + b^2 + \cdots + b^{2^{n-1}}\right). \tag{4.53}$$

La traza es lineal respecto a la suma para todos los elementos de R. Por otro lado, el cociente $R/2R$ es isomorfo al anillo de Galois $\mathrm{GF}(2^n)$, así que para todo elemento $u \in \mathrm{GF}(2^n)$ existe un único elemento $\hat{u} \in T$, el cual Kanat nombra como el *lift* de u al Teichmüller.

Con lo anterior podemos enunciar el teorema equivalente a 5 para el caso de campos de característica par:

Teorema 6. *Sea $V = \mathrm{GF}(2^n)$ con la operación $\circ$ un presemicampo simpléctico. Entonces la base éstandar $B_\infty = \{|e_w\rangle : w \in V\}$ junto con los conjuntos $B_m = \{|b_{m,v}\rangle : v \in V\}$ cuyos elementos están dados por*

$$|b_{m,v}\rangle = \frac{1}{\sqrt{d}} \sum_{w \in V} \omega^{\mathrm{tr}(\hat{w}(\hat{w}\circ\hat{m})+2\hat{w}\hat{v})} |e_w\rangle, \tag{4.54}$$

forman un conjunto maximal de $2^n + 1$ bases mutuamente insesgadas.

Demostración. La demostración es muy similar a la del teorema 5, solo con algunos detalles causados por el lift al Teichmüller. En particular, Kanat extiende la operación del presemicampo al conjunto $T \times T$ de la siguiente manera. Si $x, y \in F$, entonces la operación del presemicampo se puede expresar como

$$x \circ y = \sum_{i,j} a_{ij} x^{2^i} y^{2^j}.$$

Luego se extiende el producto $\circ$ a $T \times T$ como

$$\hat{x} \circ \hat{y} = \sum_{i,j} \widehat{a_{ij}} \hat{x}^{2^i} \hat{y}^{2^j}.$$

Con ésto se puede demostrar que dado un presemicampo simpléctico, los vectores del teorema 6 son precisamente los eigenvectores de los operadores de desplazamiento $D(u, u \circ m)$ para todo $u \in V$. Se pueden consultar los detalles en [13]. □

De nuevo podemos construir una cobertura Desarguesiana mediante la operación del campo finito. Recordemos que ésto significa que $x \circ y = xy$. El conjunto Σ de espacios uni-dimensionales sobre $\mathrm{GF}(2^n)$ de $W = V \oplus V$ es una cobertura simpléctica de W. De nuevo ésto nos brinda el plano afín

$$x = 0 \quad \text{y} \quad y = mx, \tag{4.55}$$

para todo $m \in F$, los cuales reconocemos como los rayos de las estrías de Wootters. Kantor menciona que para característica par, la dimensión más pequeña para el cual podemos generar MUBs a partir de coberturas simplécticas no equivalentes a la Desarguesiana es para $d = 2^5$. Además menciona que en general son complicadas para describir, pero nos el siguiente ejemplo no equivalente a partir de la siguiente operación binaria.

Definición 27. *Sea $\mathbb{F} = \mathrm{GF}(2^n)$. Supongamos que $n > 3$ e impar. Entonces el campo finito con la operación*

$$x \circ m = m^2 x + m \,\mathrm{tr}(x) + \mathrm{tr}(mx), \tag{4.56}$$

es un presemicampo simpléctico.

Kantor prueba que la cobertura simpléctica de $V \oplus V$ generada por éste presemicampo no es equivalente al Desarguesiana [15]. Utilizando está cobertura podemos construir el plano afín correspondiente, y con el teorema 6 podemos obtener una expresión explícita de las MUBs haciendo las operaciones pertinentes en el anillo de Galois.

4.3. Función de Wigner discreta no estándar

Vamos a recapitular la sección anterior. Dado un campo finito $\mathbb{F}$ siempre podemos formar un presemicampo mediante una nueva operación $\circ$. Todo presemicampo genera una cobertura Σ del espacio $V \oplus V$ donde $V = \mathbb{F}$, que consiste de los subespacios

$$0 \oplus V, \quad \text{y} \quad \{(w, w \circ m) : w \in V\} \quad \text{para todo } m \in \mathbb{F}\,.$$

En ocasiones, la cobertura formada por la operación del semicampo será totalmente istrópico respecto a una forma bilineal alternante. En particular nos interesa los presemicampos que generan coberturas que son simplécticas respecto a la forma definida en (4.6). Los elementos de un subespacio de la cobertura simpléctica por definición anulan a la forma bilineal alternante, ésto a su vez es una condición necesaria para que dos operadores de desplazamiento conmuten, si son los operadores correspondientes a puntos de los subconjuntos de la cobertura. Dado que los operadores de desplazamiento son diagonalizables, dos operadores conmutativos nos brindan una base de eigenvectores del espacio de Hilbert simultánea. Además como la cobertura simpléctica es maximal, obtenemos una partición de los operadores de desplazamiento en subconjuntos de operadores conmutativos, y obtenemos un conjunto maximal de bases mutuamente insesgadas gracias a las construcciones de la sección anterior.

Utilizando nuestra notación, ésto significa que los vectores $|b_{m,v}\rangle$ para todo $v \in \mathbb{F}$ corresponden a las *curvas* $\{(u, u \circ m) : u \in \mathbb{F}\}$ y a sus traslaciones; además son eigenvectores de los operadores $D(u, u \circ m)$ para todo $u \in \mathbb{F}$. Cada base de eigenvectores es invariante bajo el grupo de Pauli [42], ésto significa que al operar un eigenestado por

un operador de desplazamiento, obtendremos algún otro eigenestado correspondiente a la misma base (o al mismo eigenestado si el operador corresponde a las traslaciones que dejan invariante a las curvas de la estría). Por lo tanto, despues de asignar un eigenestado al rayo, el resto de las asignaciones de eigenestados quedan determinados por desplazamientos.

Ésto es precisamente lo que Wootters formó en su construcción de la función de Wigner discreta. Sus rectas corresponden a las lineas del plano afín, cada punto de la linea deja invariante a la linea bajo traslaciones en el espacio de fase discreto, por lo tanto el estado cuántico asignado a la recta debe corresponder a un eigenvector de los operadores de desplazamiento con puntos en en esa linea. Vamos a construir los operadores puntuales de la misma manera, donde las rectas de Wootters son reemplazadas por las curvas de la cobertura simpléctica en cuestión. El caso de la cobertura Desarguesiana coincide con las rectas de Wootters.

Definición 28. *Sea ρ un operador de densidad. La función de Wigner no estándar, denotada como $W_\rho^{\mathcal{K}}$ en referencia a Kantor, se define como*

$$W_\rho^{\mathcal{K}} = \mathrm{Tr}\left(\rho A^{\mathcal{K}}(\alpha)\right), \tag{4.57}$$

donde los operadores puntuales son

$$A^{\mathcal{K}}(\alpha) = \sum_{\alpha \ni \lambda} Q(\lambda) - I, \tag{4.58}$$

para toda curva λ de la cobertura que contienen al punto α.

Elegimos la convención de tomar el primer elemento de las bases generadas de manera algorítmica por los teoremas 5 y 6 respectivamente como el estado correspondiente al rayo. Los estados posteriores de cada estría quedan determinados por los operadores de desplazamiento correspondientes.

Proposición 21. *Los operadores puntuales $A^{\mathcal{K}}(\alpha)$ donde $\alpha = (a, b) \in \mathbb{F} \oplus \mathbb{F}$ satisfacen las siguientes propiedades*

1. *Son auto-adjuntos.*
2. *Son de traza unitaria.*
3. *Son ortogonales bajo el producto interno de Hilbert-Schmidt.*

Demostración. Las pruebas para cada punto son practicamente iguales a las pruebas de la proposición (17). Que los operadores puntuales sean auto-adjuntos y de traza unitaria es consecuencia de que los operadores $Q(\lambda)$ que constituyen al operador puntual son auto-adjuntos y de traza unitaria. La prueba del tercer punto solo dependía de que las bases fuera mutuamente insesgadas, y de la estructura geométrica del espacio de fase discreto. En particular, sabemos que la cobertura simpléctica genera un plano afín, el cual preserva la propiedad de que por cada punto pasan $d + 1$ curvas y que las curvas paralelas no se intersectan, por lo tanto podemos utilizar el mismo argumento de conteo. □

Como consecuencia de la proposición anterior, la construcción no estándar también satisface las propiedades deseadas de una función de Wigner.

Proposición 22. *Sea ρ un estado cuántico y $W_\rho^{\mathcal{K}}$ su función de Wigner discreta no estándar. Entonces*

1. *$W_\rho^{\mathcal{K}}$ es real.*
2. *La suma de $W_\rho^{\mathcal{K}}$ sobre cualquier curva λ del plano afín es igual al valor esperado de $Q(\lambda)$ en el estado ρ.*
3. *La suma de $W_\rho^{\mathcal{K}}$ sobre todo el espacio de fase discreto es igual a 1.*
4. *La función de Wigner no estándar es covariante bajo traslaciones en el espacio de fase discreto.*

Demostración. De nuevo la demostración es prácticamente idéntica a la de la construcción estándar. Los primeros tres puntos surgen directamente de las propiedades de los operadores puntuales. La cuarta propiedad depende del hecho de que Q sea covariante bajo traslaciones, pero ésto también se satisface ya que el grupo de Pauli deja invariante (salvo permutaciones) a cada base ortonormal de las MUBs producidas por cualquier cobertura simpléctica. □

4.4. Ejemplos

El primer ejemplo de ésta sección consiste en calcular las bases mutuamente insesgadas para el sistema cuántico de un par de qubits. Utilizaremos el teorema 6 para la construcción notando que las bases obtenidas son equivalentes a las de Wootters (salvo permutaciones). Despues, daremos dos ejemplos para los cuales calcularemos dos conjuntos completos de MUBs: un conjunto estándar (cobertura Desarguesiana) y un conjunto no estándar. En la siguiente sección utilizaremos ambos conjuntos para comparar las funciones de Wigner.

Ejemplo 7. *Consideremos el sistema cuántico de dos qubits. El espacio de Hilbert es $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2 \cong \mathbb{C}^4$.*

El espacio de fase discreto será una malla de 4×4 pares cuyos componentes son elementos del campo finito $\mathrm{GF}(2^2)$. El anillo de Galois correspondiente será $\mathrm{GR}(4^2)$, para construirlo consideramos el polinomio $f(x) = x^2 + x + 1 \in \mathbb{Z}_4[x]$ para formar el cociente

$$\mathrm{GR}(4^2) \cong \mathbb{Z}_4[x]/\langle x^2 + x + 1\rangle.$$

En éste caso la raíz del polinomio $f(x)$ es una $2^2 - 1$-ésima raíz de la unidad del anillo de Galois. Por definición el conjunto Teichmüller está dado por $T = \{0, 1, \xi, \xi^2\}$, y la traza se cálcula como

$$\mathrm{tr}(x) = (a + a^2) + 2(b + b^2),$$

donde $a + 2b$ es la representación 2-ádica de x. Vamos a utilizar el cobertura Desarguesiana para éste primer ejemplo por lo tanto la operación del presemicampo es simplemente el producto en el campo finito, $x \circ y = xy$. La cobertura simpléctica consiste de los subespacios de $V \oplus V$ dados por $0 \oplus V$, $\{(u, mu) : u \in \mathrm{GF}(2^2)\}$ para todo $m \in \mathrm{GF}(2^2)$. Los rayos del plano afín son las rectas

$$x = 0, \quad y = mx, \quad m \in \mathrm{GF}(2^2),$$

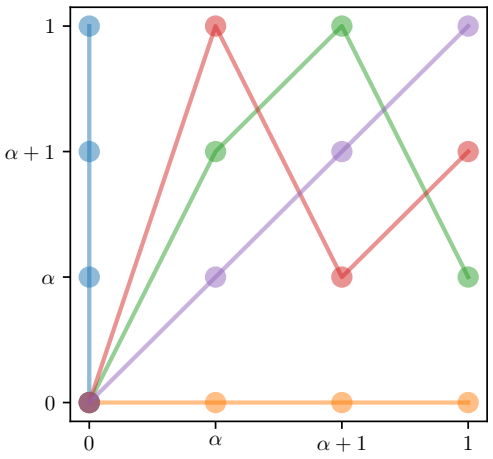


Figura 4.2: Rayos del plano afín correspondiente al espacio de fase discreto de dos qubits. Vemos que coincide con el los rayos de Wootters en el ejemplo (3.8) del capítulo anterior).

y se muestran en la figura (4.2).

Luego, utilizando el teorema 6 para la construcción de eigenvectores en característica par, obtenemos los siguientes vectores:

$$|b_{m,v}\rangle = \frac{1}{\sqrt{d}} \sum_{w \in V} \omega^{\mathrm{tr}\left(\hat{w}^2 \hat{m} + 2\hat{w}\hat{v}\right)} |e_w\rangle \,,$$

para todo $m, v \in V$. Éstas bases son exactamente las que obtiene Wootters al diagonalizar los operadores de desplazamiento que dejan invariantes a cada estría. En el ejemplo (REF) del capítulo anterior se utilizaron para la construcción de la función de Wigner de dos qubits. Las incluímos aquí como referencia (las bases están etiquetadas

por los elementos del Teichmüller):

$$B_\infty = \left\{ \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\0\\1\end{pmatrix} \right\}, \tag{4.59}$$

$$B_0 = \left\{ \frac{1}{2}\begin{pmatrix}1\\1\\1\\1\end{pmatrix}, \frac{1}{2}\begin{pmatrix}1\\1\\-1\\-1\end{pmatrix}, \frac{1}{2}\begin{pmatrix}1\\-1\\-1\\1\end{pmatrix}, \frac{1}{2}\begin{pmatrix}1\\-1\\1\\-1\end{pmatrix} \right\}, \tag{4.60}$$

$$B_1 = \left\{ \frac{1}{2}\begin{pmatrix}1\\-1\\-i\\-i\end{pmatrix}, \frac{1}{2}\begin{pmatrix}1\\-1\\i\\i\end{pmatrix}, \frac{1}{2}\begin{pmatrix}1\\1\\i\\-i\end{pmatrix}, \frac{1}{2}\begin{pmatrix}1\\1\\-i\\i\end{pmatrix}, \right\}, \tag{4.61}$$

$$B_\xi = \left\{ \frac{1}{2}\begin{pmatrix}1\\-i\\-1\\-i\end{pmatrix}, \frac{1}{2}\begin{pmatrix}1\\-i\\1\\i\end{pmatrix}, \frac{1}{2}\begin{pmatrix}1\\i\\1\\-i\end{pmatrix}, \frac{1}{2}\begin{pmatrix}1\\i\\-1\\i\end{pmatrix} \right\}, \tag{4.62}$$

$$B_{\xi^2} = \left\{ \frac{1}{2}\begin{pmatrix}1\\-i\\-i\\-1\end{pmatrix}, \frac{1}{2}\begin{pmatrix}1\\-i\\i\\1\end{pmatrix}, \frac{1}{2}\begin{pmatrix}1\\i\\i\\-1\end{pmatrix}, \frac{1}{2}\begin{pmatrix}1\\i\\-i\\1\end{pmatrix} \right\}. \tag{4.63}$$

Ejemplo 8. *Consideremos un sistema cuántico de cinco qubits. La elección de ésta cantidad de qubits se debe a que la construcción de la cobertura simpléctica 27 es válida solo para una extensión de grado $n > 3$. El espacio de Hilbert correspondiente es $\mathcal{H} = \left(\mathbb{C}^2\right)^{\otimes 5} \cong \mathbb{C}^{32}$.*

El espacio de fase discreto será una malla de 32×32 pares cuyos componentes son elementos del campo finito $\mathrm{GF}(2^5)$. El anillo de Galois será $\mathrm{GR}(4^5)$, un anillo con 4^5 elementos. El polinomio que utilizaremos es el polinomio de Conway[3] dado por $f(x) = x^5 + x^2 + 1$. Así

$$\mathrm{GR}(4^5) \cong \mathbb{Z}_4[x]/\langle x^5 + x^2 + 1\rangle.$$

Utilizando el polinomio de Conway, el generador del anillo α no nos brinda un subgrupo multiplicativo. En su lugar debemos usar la $(2^5 - 1)$-ésima raíz primitiva de la unidad

$$\xi = \alpha^2 + 2\alpha + 1.$$

Con ésto el Teichmüller es el siguiente conjunto de $2^5 - 1$ elementos:

$$T = \{0, 1, \xi, \xi^2, \ldots, \xi^{30}\}.$$

La traza en éste caso se puede calcular como

$$\mathrm{tr}(x) = \left(a + a^2 + \cdots + a^{16}\right) + 2\left(b + b^2 + \cdots + b^{16}\right),$$

[3]La mayoría de los CAS utilizan a los polinomios de Conway para las extensiones de campos y de anillos por default.

donde $a, b \in T$ y $a + 2b$ es la representación 2-ádica de x.

Para este sistema cuántico, sí podemos formar dos MUBs no equivalentes. Primero utilizamos la cobertura Desarguesiana, donde la operación del presemicampo está dada por $x \circ y = xy$. Recordemos qué esta cobertura coincide con las estrías de Wootters, la figura (4.3) nos muestra el espacio discreto etiquetado por los elementos de la extensión de Galois, y nos muestra el plano afín correspondiente a la cobertura Desarguesiana Σ. Utilizamos el teorem 6 para generar las MUBs correspondientes. No las enlistamos

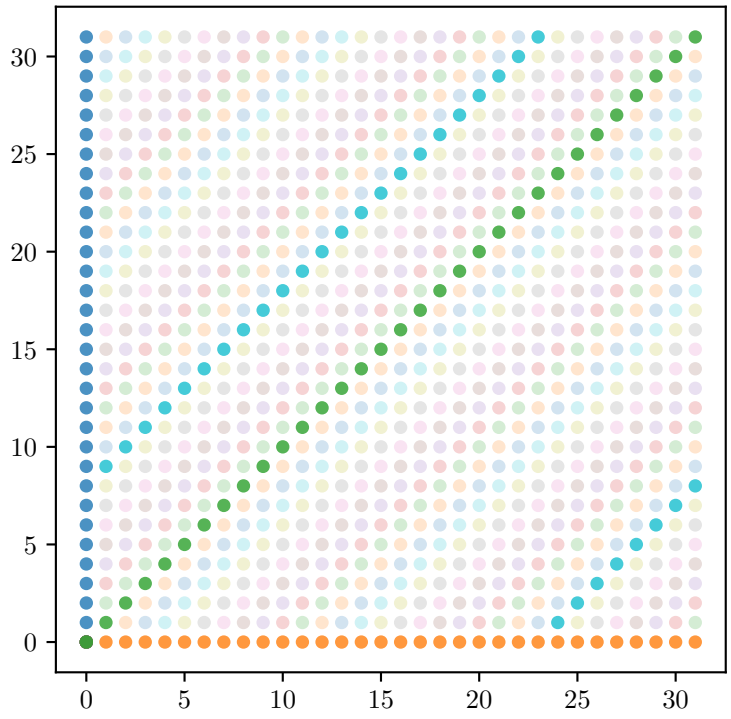


Figura 4.3: $V = \mathrm{GF}(2^5)$, cobertura Desarguesiana. En éste caso los ejes están etiquetados por el orden predeterminado de los elementos del campo de Galois en `SageMath`.

aquí porque cada base de las 33 bases, es un conjunto de 32 vectores de 32 elementos.

Ahora consideramos la cobertura generada en el ejemplo 27. Recordemos que la operación del presemicampo es

$$x \circ m = m^2 x + m \operatorname{tr}(x) + \operatorname{tr}(mx). \tag{4.64}$$

La cobertura simpléctica se puede observar en la figura (4.4). Notemos que el rayo resaltado en la figura (4.3) de la cobertura Desarguesiana correspondiente a un $m \in \mathrm{GF}(2^5)$ distinto a 0 y 1, tiene una forma distinta en la cobertura de Kantor.

Para generar las MUBs a partir del teorema 6 es necesario hacer el lift de la operación del presemicampo al Teichmüller. Utilizando la definición de la traza $\mathrm{tr} : \mathrm{GF}(2^5) \to \mathbb{Z}_2$, podemos expresar la operación del presemicampo en monomios de x y m de la siguiente manera:

$$x \circ m = m^2 x + m\left(x + x^2 + \ldots + x^{16}\right) + \left(mx + (mx)^2 + \ldots + (mx)^{16}\right). \tag{4.65}$$

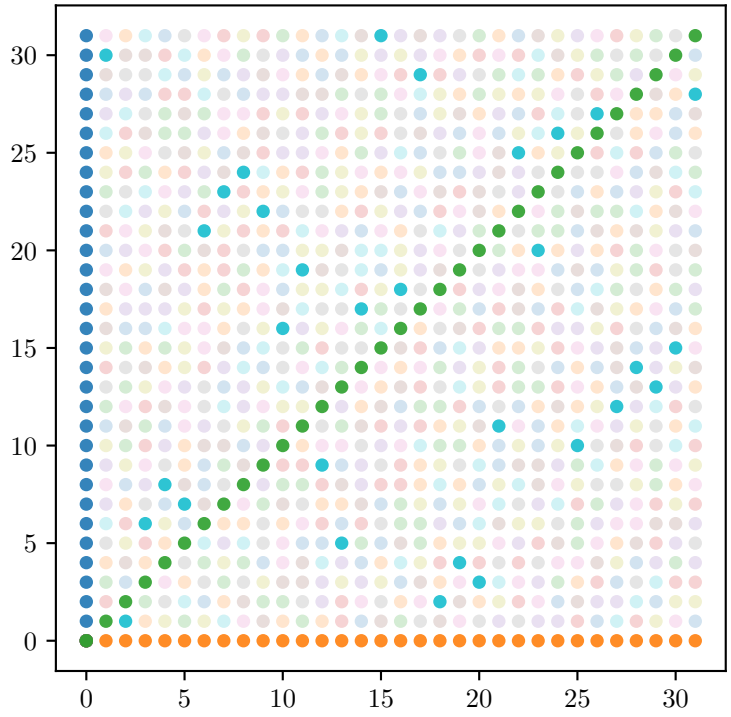


Figura 4.4: $V = \mathrm{GF}(2^5)$, cobertura de Kantor. Notemos que el rayo horizontal, el vertical y el diagonal son los mismos en ambas coberturas. Pero a parte de esos tres, el resto de los rayos tiene una forma distinta al Desarguesiano.

Se sigue que el lift al Teichmüller de la operación del presemicampo será:

$$\hat{x} \circ \hat{m} = \hat{m}^2\hat{x} + \hat{m}\left(\hat{x} + \hat{x}^2 + \ldots + \hat{x}^{16}\right) + \left(\hat{m}\hat{x} + (\hat{m}\hat{x})^2 + \ldots + (\hat{m}\hat{x})^{16}\right) \tag{4.66}$$

$$= \hat{m}^2\hat{x} + \hat{m}\,\mathrm{tr}(\hat{x}) + \mathrm{tr}(\hat{m}\hat{x}). \tag{4.67}$$

Notemos que la traza de los elementos del Teichmüller es reduce a la traza usual. Con ésto ya tenemos todo listo para calcular de manera directa al conjunto completo de MUBs utilizando el teorema 6. Dicho teorema nos dice que los eigenvectores de los operadores $D(u, u \circ m)$, con $u \in F$, son:

$$|b_{m,v}\rangle = \frac{1}{\sqrt{d}} \sum_{w \in F} \omega^{\mathrm{tr}(\hat{w}(\hat{w}\circ\hat{m})+2\hat{w}\hat{v})} |e_w\rangle\,. \tag{4.68}$$

De nuevo no desplegamos los 33 conjuntos de 32 vectores de dimensión 32 aquí por razones obvias. Por el teorema 3 de Kantor sabemos que éstas MUBs no son unitariamente equivalentes a las de Wootters.

Ejemplo 9. *Consideremos un sistema cuántico compuesto de tres qutrits. El espacio de Hilbert será* $\mathcal{H} = \mathbb{C}^3 \otimes \mathbb{C}^3 \otimes \mathbb{C}^3 \cong \mathbb{C}^{27}$.

El espacio de fase discreto correspondiente será una malla de 27×27 pares de elementos de la extensión de Galois $V = \mathrm{GF}(3^3)$. Para la extensión consideramos de nuevo un polinomio de Conway, $f(x) = x^3 + 2x + 1$, de tal modo que

$$\mathrm{GF}(3^3) \cong \mathbb{Z}_3[x]/\langle x^3 + 2x + 1\rangle.$$

Primero calcularemos las MUBs correspondientes a la cobertura Desarguesiana. La figura (4.5) muestra los rayos del plano afín correspondiente y recordemos que ésta cobertura está dada simplemente por la operación de presemicampo $x \circ y = xy$. Sea

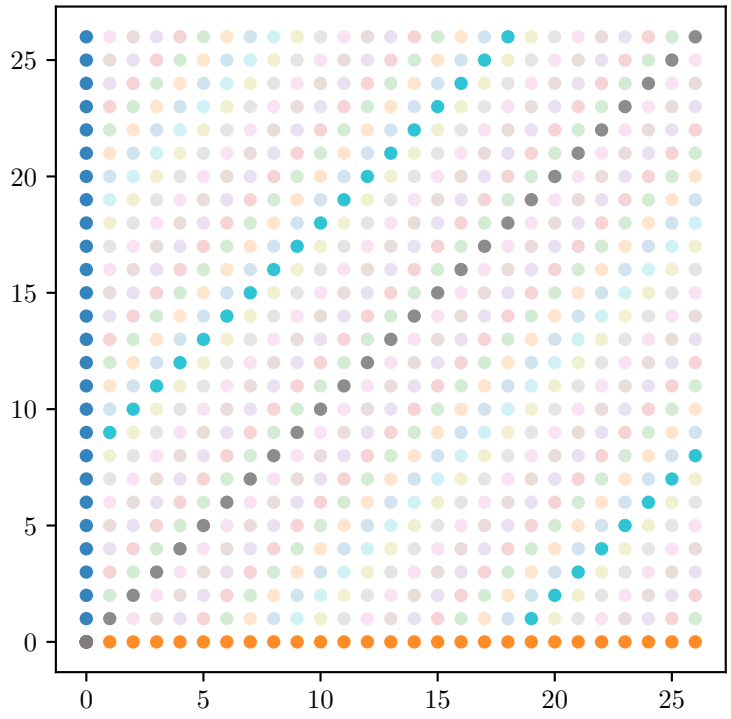


Figura 4.5: $V = \mathrm{GF}(3^3)$, cobertura Desarguesiana.

$\omega \in \mathbb{C}$ una 3-ésima raíz primitiva de la unidad. Dado que $\mathrm{GF}(3^3)$ es característica impar, el teorema 5 nos brinda los siguientes eigenvectores

$$|b_{m,v}\rangle = \sum_{w \in F} \omega^{\mathrm{tr}\left(\frac{1}{2}w(wm)+vw\right)} |e_w\rangle \quad m \in F, \tag{4.69}$$

de los operadores $D(u, u \circ m)$ para todo $u \in F$. El conjunto completo de MUBs es un conjunto de 28 bases mutuamente insesgadas de 27 vectores de dimensión 27. De nuevo, no mostraremos las bases aquí.

La razón para elegir éste ejemplo en particular es para poder construir un conjunto de MUBs que no son unitariamente equivalentes a las de Wootters, utilizando el presemicampo en 26. La cobertura simpléctica del campo torcido de Albert requiere definir

un número $s \in \mathbb{N}$ tal que $1 \leq s \leq \frac{n}{2}$. En éste caso $n = 3$, por lo tanto $s = 1$ es el único valor posible. Con ésto, la operación del presemicampo se define como

$$w \circ m = mw^9 + m^3w^3, \quad m \in \mathrm{GF}(3^3).$$

La cobertura simpléctica está dado por los conjuntos $0 \oplus V$ y $\{(w, w \circ m) : w \in F\}$ para todo $m \in F$, y el plano afín correspondiente queda determinado por los rayos

$$x = 0, \quad y = mx^9 + m^3x^3,$$

y ésto se muestra en la figura (4.6), donde de nuevo se puede observar que el rayo horizontal y vertical son los mismos, pero ahora el rayo correspondiente a $m = 1$, el 'rayo diagonal', es distinto.

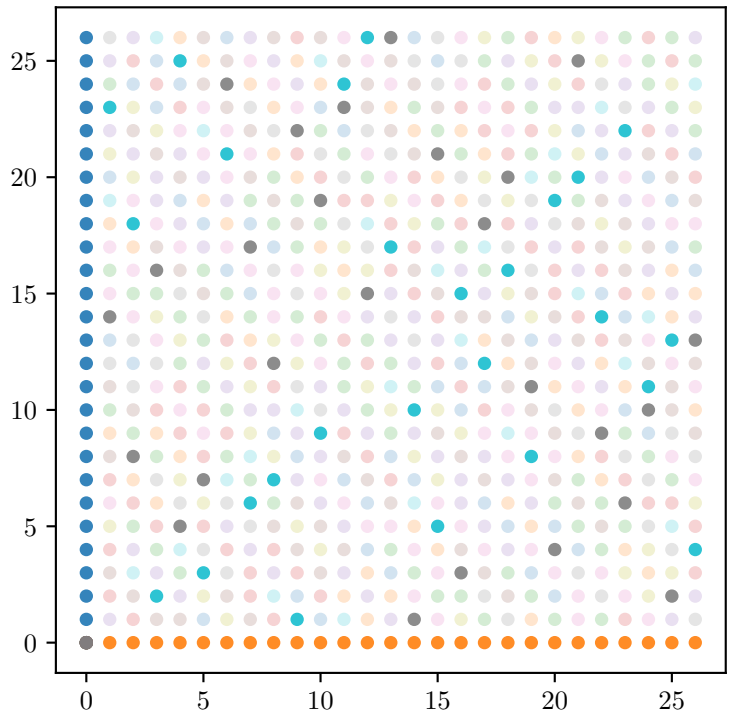


Figura 4.6: $V = \mathrm{GF}(3^3)$, cobertura del presemicampo torcido de Albert.

4.4.1. Ejemplos comparativos

Retomamos los ejemplos (8) y (9) para los cuales hemos construidos dos conjuntos de MUBs no equivalentes. El primer conjunto de MUBs coincide con las construcciones de Wootters en ambos casos. Designemos por $\mathcal{B}_m$ al conjunto de MUBs estándar y por $\mathcal{B}_m^{\mathcal{K}}$ al conjunto de MUBs no estándar, donde $m \in \mathbb{F}$ y $\mathcal{B}_\infty, \mathcal{B}_\infty^{\mathcal{K}}$ denotan la base estándar.

Ejemplo 10. *El primer ejemplo consiste de un sistema cuántico de cinco qubits. Vamos a calcular la función de Wigner estándar y no estándar para tres estados. El primero estado estado cuántico corresponde a un elemento de un conjunto de las MUBs calculadas a partir de la cobertura Desarguesiana,* $|\psi_1\rangle \in \mathcal{B}_m$*. El segundo estado corresponderá a un eigenestado de las MUBs alternativas,* $|\psi_2\rangle \in \mathcal{B}_m^{\mathcal{K}}$*. Finalmente construímos un estado que es combinación lineal de tres elementos de la base estándar:*

$$|\psi_3\rangle = \frac{1}{\sqrt{3}}\left(|\alpha^4 + \alpha^3 + \alpha\rangle + |\alpha + 1\rangle\right).$$

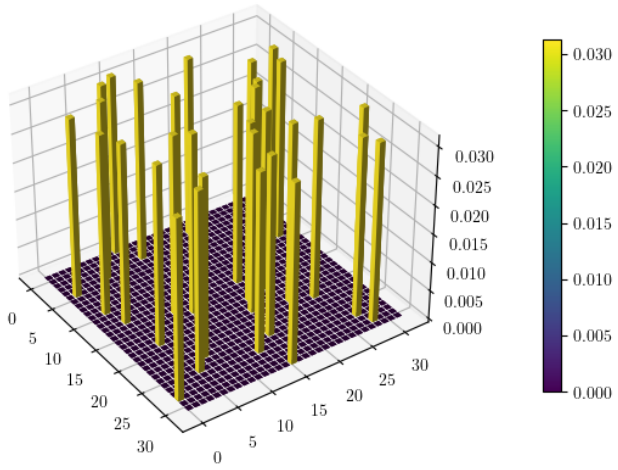


Figura 4.7: Función de Wigner estándar W para el estado $|\psi_1\rangle$, el cual pertenece a las MUBs estándar.

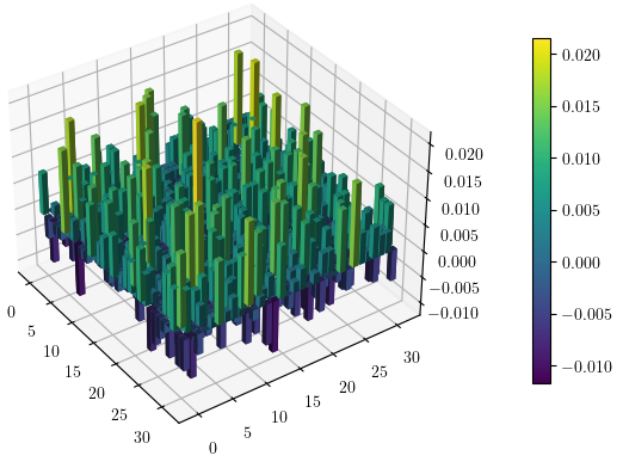


Figura 4.8: Función de Wigner no-estándar $W^{\mathcal{K}}$ para el estado $|\psi_1\rangle$, el cual pertenece a las MUBs estándar.

Observemos en la figura (4.7) que sumando la función de Wigner estándar W sobre la recta correspondiente al estado $|\psi_1\rangle$ obtenemos el valor de 1, indicando que no hay

incertidumbre. Por otro lado, la figura (4.8) nos muestra la función de Wigner no estándar $W^{\mathcal{K}}$ del mismo estado $|\psi_1\rangle$. El aparante desorden en la gráfica es de esperarse, pues nos indica que el estado $|\psi_1\rangle$ *no* es un eigenestado de las MUBs de Kantor, un indicador de la inequivalencia entre las construcciones. Ahora, las bases correspondientes a las rectas horizontales y verticales son las mismas en ambas construcciones, así que la suma de ambas funciones W y $W^{\mathcal{K}}$ sobre éstas rectas nos deben dar la misma probabilidad, algo que se verifica con cálculo directo.

Similarmente, calculamos las funciones W y $W^{\mathcal{K}}$ pero ahora para el estado $|\psi_2\rangle$ el cual pertenece a las MUBs no estándar $\mathcal{B}^{\mathcal{K}}$, y que no pertenece a la estándar $\mathcal{B}$. Como

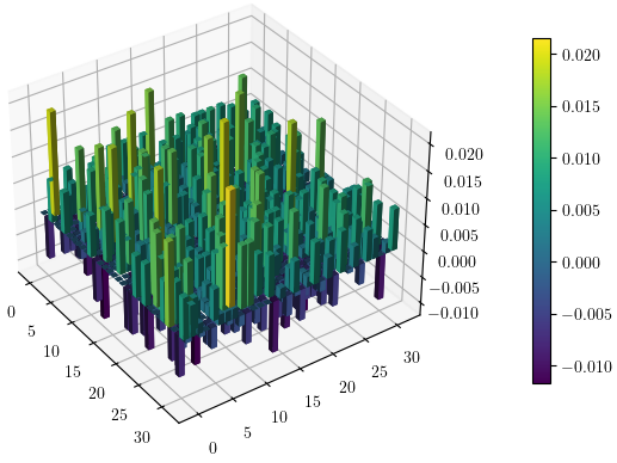


Figura 4.9: Función de Wigner estándar W para el estado $|\psi_2\rangle$, el cual pertenece a las MUBs no estándar.

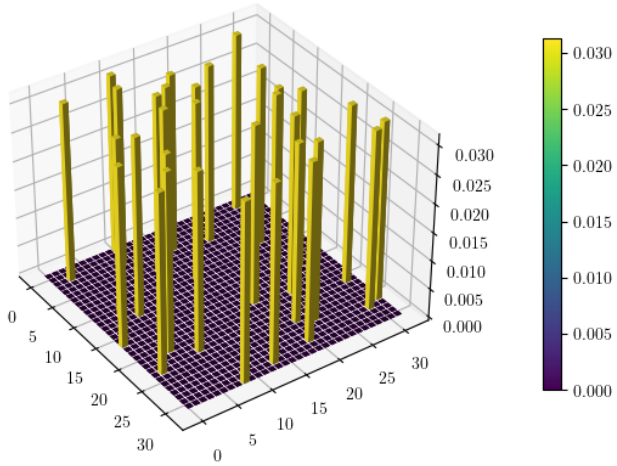


Figura 4.10: Función de Wigner no estándar para $|\psi_2\rangle$.

es de esperarse, la figura (4.9) nos indica que la función de Wigner estándar produce una figura sin mucho. Ésto es de esperarse pues las mediciones se hacen con bases que no son unitariamente equivalentes a las que se usaron para definir la función de Wigner. El mismo estado produce una función de Wigner no estándar con mucho más orden,

en donde se ve claramente que el estado pertenece a una de las MUBs. A pesar de las diferencias, en ambos casos se preserva la propiedad tomográfica y en estados que se comparten en ambas MUBs, las probabilidad obtenidas al sumar las funciones de Wigner son iguales.

Ahora consideremos el estado cuántico $|\psi_3\rangle$. Éste estado cuántico es una superposición equitativa de estados de la base estándar. La base estándar pertenece a ambos conjuntos de MUBs, por lo que no esperaríamos ver mucha diferencia. La figura (4.11) muestra la gráfica de la función de Wigner estándar del estado $|\psi_3\rangle$, notemos las dos barras verticales que sobre salen. Sumando sobre ellas obtenemos la probabilidad de encontrar el sistema en los estados $|\alpha^4 + \alpha^3 + \alpha\rangle$ y $|\alpha + 1\rangle$ respectivamente, en ambos casos la probabilidad es $\frac{1}{2}$. Sumando sobre cualquier otra recta vertical nos da 0 ya que por definición de $|\psi_3\rangle$ no hay probabilidad de que el sistema se encuentre en esos eigenestados. Notamos un pico en la primera linea vertical que sobresale más que los demas. No podemos concluír mucho sobre el significado de ese pico, más de allá del hecho de que la probabilidad de transición de $|\psi_3\rangle$ al estado correspondente a la recta horizontal que cruza por ese punto si coincide con la suma. Como lo esperabamos, la gráfica de la función de Wigner no estándar $W^{\mathcal{K}}$ es muy similar, vuelven aparecer dos rectas verticales positivas correspondientes a los estados de la superposición, como se puede observar en la figura (4.12). Curiosamente, la versión no estándar no muestra el pico centralizado que aparece en la versión estándar, las barras verticales parecen tener alturas distribuidas de una manera más uniforme. El cálculo de probabilidades permanece igual. La figura (4.13) muestra las gráficas en forma de un *mapa de calor* en donde la similutud de ambas funciones se aprecia un poco mejor.

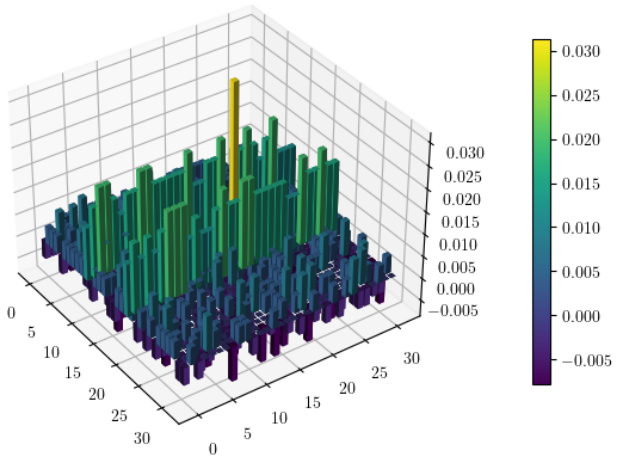


Figura 4.11: Función de Wigner estándar W del estado en superposición.

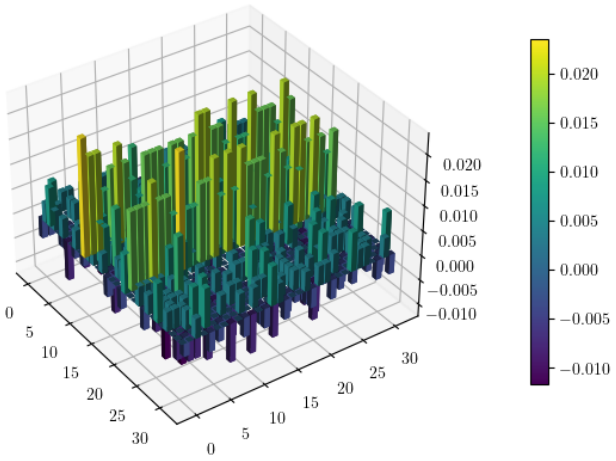
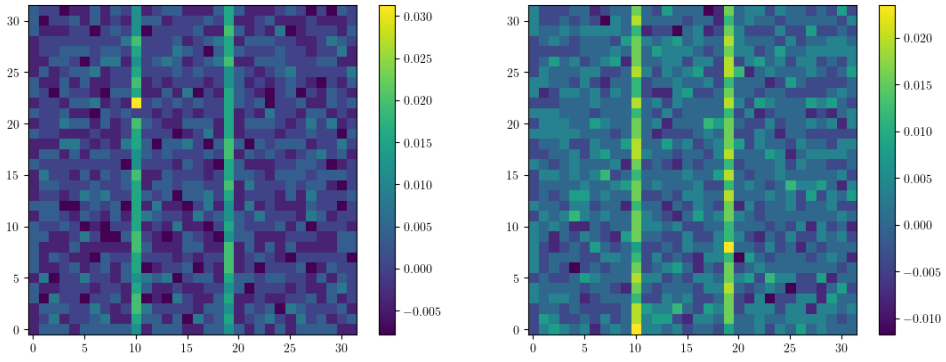


Figura 4.12: Función de Wigner no estándar $W^{\mathcal{K}}$ del estado en superposición.



(a) W (b) $W^{\mathcal{K}}$

Figura 4.13: Comparación de ambas funciones de Wigner para el estado $|\psi_3\rangle$.

Ejemplo 11. *Consideremos el sistema cuántico modelado por tres qutrits. En la sección anterior, construímos dos conjuntos completos de MUBs no unitariamente equivalentes, así que podremos definir dos funciones de Wigner para un estado de interes. Consideramos un eigenestado $|\psi\rangle$ de las MUBs estándar.*

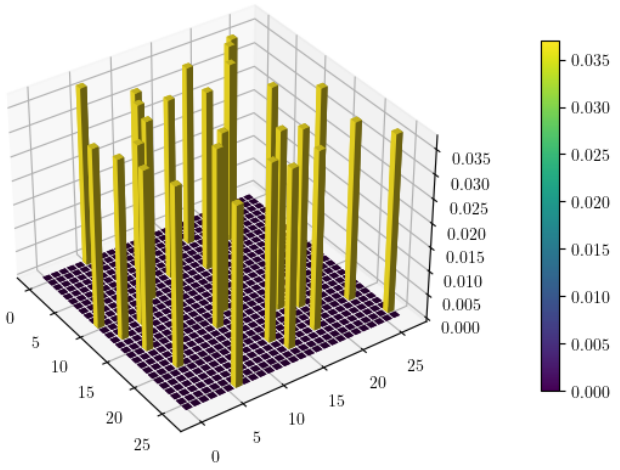


Figura 4.14: Función de Wigner estándar para el estado $|\psi\rangle$.

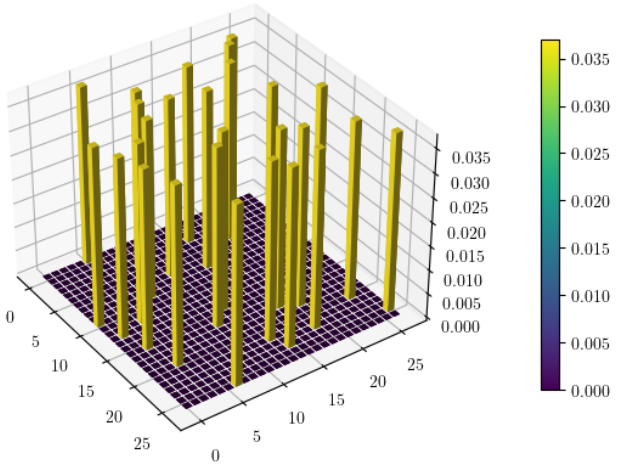


Figura 4.15: Función de Wigner no estándar para el estado $|\psi\rangle$.

Las figuras (4.14) y (4.15) muestran la función de Wigner estándar W y no estándar $W^{\mathcal{K}}$ del elemento $|\psi\rangle$. *Son idénticas!* Esperabamos ver funciones de Wigner muy distintas como sucedió en el caso de los cinco qubits, pero como se puede observar, las funciones de Wigner no difieren en el caso de tres qutrits. Que las MUBs no sean equivalentes bajo ninguna transformación unitaria no necesariamente implica que los operadores puntuales tampoco lo sean. El converso es claro, pero es probable que la suma de las proyecciones de eigenestados de distintas bases *anulen* las diferencias. Fue necesario estudiar ésta situación más a fondo.

4.4.2. Equivalencia de la función de Wigner respecto a la cobertura de Albert

Una comparación numérica de las funciones de Wigner del ejemplo anterior nos dirigió hacia la igualdad de los operadores puntuales para ambas coberturas simplécticas. Utilizando algunos resultados sobre sumas de caracteres de campos finitos logramos demostrar que, *utilizando la cobertura generada por la familia de campos torcidos de Albert, obtenemos el mismo operador puntual del origen que se obtiene en la construcción estándar.* La propiedad de ser covariante bajo traslaciones nos permite concluir que el resto de los operadores puntuales también son iguales por lo que ambas coberturas producen la misma función de Wigner discreta. El caso de los tres qutrits es el ejemplo básico. Para simplificar la demostración podemos solo considerar el operador puntual en el origen $A(0,0)$. De la definición de $A(a,b)$ tenemos que

$$A(0,0) = \sum_{\lambda \ni (0,0)} Q(\lambda) - I \tag{4.70}$$

$$= \sum_{m \in \mathbb{F} \cup \{\infty\}} |\lambda_{m,0}\rangle \langle \lambda_{m,0}| - I \tag{4.71}$$

$$= |e_0\rangle \langle e_0| + \sum_{m \in \mathbb{F}} |\lambda_{m,0}\rangle \langle \lambda_{m,0}| - I, \tag{4.72}$$

donde $\lambda_{m,0}$ corresponde al rayo con pendiente m. El caso $m = \infty$ corresponde con la estría vertical, y en particular $|\lambda_{\infty,0}\rangle$ es el vector $|e_0\rangle$ de la base estándar. Utilizando la expresión (4.44) tenemos que

$$|\lambda_{m,0}\rangle = \frac{1}{\sqrt{d}} \sum_{w \in \mathbb{F}} \omega^{\mathrm{tr}\left(\frac{1}{2} w (w \circ m)\right)} |e_w\rangle , \tag{4.73}$$

donde $\circ$ es la operación del presemicampo en cuestión. Utilizando la definición de $|\lambda_{m,0}\rangle$, cada proyección se puede expresar como:

$$|\lambda_{m,0}\rangle \langle \lambda_{m,0}| = \frac{1}{d} \left(\sum_{k \in \mathbb{F}} \omega^{\mathrm{tr}\left(\frac{1}{2} k (k \circ m)\right)} |e_k\rangle \right) \left(\sum_{j \in \mathbb{F}} \omega^{-\mathrm{tr}\left(\frac{1}{2} j (j \circ m)\right)} \langle e_j| \right) \tag{4.74}$$

$$= \frac{1}{d} \sum_{k \in \mathbb{F}} \sum_{j \in \mathbb{F}} \omega^{\mathrm{tr}\left(\frac{1}{2} k (k \circ m)\right) - \mathrm{tr}\left(\frac{1}{2} j (j \circ m)\right)} |e_k\rangle \langle e_j| \tag{4.75}$$

$$= \frac{1}{d} \sum_{k,j \in \mathbb{F}} \omega^{\mathrm{tr}\left(\frac{1}{2} (k (k \circ m) - j (j \circ m))\right)} |e_k\rangle \langle e_j| . \tag{4.76}$$

De la ecuación (4.72), vemos que dos operadores puntuales en el origen para dos presemicampos $(\mathbb{F}, +, \circ)$ y $(\mathbb{F}, +, *)$ serán iguales si el término en medio, que consiste de la suma sobre $m \in \mathbb{F}$, es igual. Notemos que $\left(|e_k\rangle \langle e_j|\right)_{kj} = \delta_{kj}$ respecto a la base estándar, por lo tanto se obtiene la igualdad si y solo si las sumas

$$S_1 = \sum_{m \in \mathbb{F}} \omega^{\mathrm{tr}\left\{\frac{1}{2}[k (k \circ m) - j (j \circ m)]\right\}}, \tag{4.77}$$

y

$$S_2 = \sum_{m \in \mathbb{F}} \omega^{\mathrm{tr}\left\{\frac{1}{2}[k (k * m) - j (j * m)]\right\}} \tag{4.78}$$

son iguales para todo $k, j \in \mathbb{F}$. A éste tipo de sumas se les conoce como *sumas de Weil*, generalmente se expresan en términos de los caracteres χ del grupo aditivo:

$$\sum_{c\in\mathbb{F}} \chi(f(x)), \tag{4.79}$$

donde $f \in \mathbb{F}[x]$, (ver la sección de *sumas exponenciales* (A.2.3) del apéndice para un resumen rápido de los caracteres aditivos de un campo finito). Las sumas de Weil generalmente no son fáciles de evaluar [43]. Usualemente solo podemos obtener estimaciones de las cotas superiores e inferiores del valor absoluto de la suma. Para nuestra suerte, en el caso de la cobertura Desarguesiana y la de Albert, sí existen fórmulas de evaluación.

Primero consideremos la suma (4.77), en donde la cobertura simpléctica es la Desarguesiana. Recordemos que la operación del presemicampo que genera a ésta cobertura es simplemente la multiplicación del campo finito, $a \circ b = ab$, para todo $a, b \in \mathbb{F}$. El argumento de la traza se reduce a

$$\frac{1}{2}[k(k\circ m) - j(j\circ m)] = \frac{1}{2}\left(k^2 m - j^2 m\right) = \frac{1}{2}\left(k^2 - j^2\right) m. \tag{4.80}$$

En ésta forma y notando que $\chi(c) = \omega^{\mathrm{tr}(c)}$ es el caracter aditivo canónico, podemos ver a partir del teorema (14) que la suma de Weil nos dará igual a 0 siempre que $k^2 - j^2 \neq 0$. Si ésto no es el caso, entonces el argumento de χ se vuelve nulo, por lo tanto la suma nos dará d ya que $\chi(0) = 1$. Por lo tanto la suma de Weil es

$$S_1 = \begin{cases} d & \text{si } k^2 - j^2 = 0, \\ 0 & \text{en otro caso,} \end{cases} \tag{4.81}$$

para todas las entradas del operador puntual indexadas por $k, j \in \mathbb{F}$. Ahora evaluamos la segunda suma de Weil dada por (4.78) utilizando la versión de presemicampo de Kantor de los campos torcidos de Albert. El ejemplo de la sección anterior corresponde a la dimensión más pequeña para el cual podemos generar una cobertura simpléctica no equivalente a la estándar. La prueba que daremos enseguida funciona para todo p, n y s que satisface las condiciones del campo torcido de Albert. Recordemos que la operación del presemicampo está dada por $x * m = mx^{p^{n-s}} + m^{p^s} x^{p^s}$ para n impar, un s coprimo a n y $1 \leq s \neq n/2$. Para evaluar la suma de Weil utilizaremos el teorema (15), para ésto debemos expresar el argumento de la traza como un múltiplo escalar de un p-polinomio afín. Ignorando el factor $1/2$ por el momento obtenemos

$$\begin{aligned} k(k*m) - j(j*m) &= k\left(mk^{p^{n-s}} + m^{p^s}k^{p^s}\right) - j\left(mj^{p^{n-s}} + m^{p^s}j^{p^s}\right) && (4.82)\\ &= mk^{p^{n-s}+1} + m^{p^s}k^{p^s+1} - mj^{p^{n-s}+1} - m^{p^s}j^{p^s+1} && (4.83)\\ &= \left(k^{p^s+1} - j^{p^s+1}\right)m^{p^s} + \left(k^{p^{n-s}+1} - j^{p^{n-s}+1}\right)m. && (4.84) \end{aligned}$$

Observamos que la ecuación (4.84) es un p-polinomio afín donde

$$a_s = k^{p^s+1} - j^{p^s+1}, \quad a_0 = k^{p^{n-s}+1} - j^{p^{n-s}+1}, \quad \text{y} \quad a = 0. \tag{4.85}$$

El resto de los coeficientes a_{r-i} son nulos. Dado que $\chi_b(c) = \chi(bc) = \omega^{\mathrm{tr}(bc)}$, es fácil ver que la suma S_2 (4.78) tiene la forma requerida para usar el teorema (15) para $b = 1/2$ y $a = 0$. Por lo tanto

$$S_2 = \begin{cases} d & \text{si } 2a_s + 2^{p^s} a_0^{p^s} = 0, \\ 0 & \text{en otro caso.} \end{cases} \tag{4.86}$$

Podemos simplificar la ecuación que aparece en el primer caso utilizando ciertas propiedades de campos finitos de característica impar:

$$\begin{aligned} 2a_s + 2^{p^s} a_0^{p^s} &= 2\left(k^{p^s+1} - j^{p^s+1}\right) + 2^{p^s}\left(k^{p^{n-s}+1} - j^{p^{n-s}+1}\right)^{p^s} && (4.87)\\ &= 2\left(k^{p^s+1} - j^{p^s+1}\right) + 2^{p^s}\left(k^{p^s+1} - j^{p^s+1}\right) && (4.88)\\ &= (2+2)\left(k^{p^s+1} - j^{p^s+1}\right) && (4.89)\\ &= k^{p^s+1} - j^{p^s+1}. && (4.90) \end{aligned}$$

Por lo tanto

$$S_2 = \begin{cases} d & \text{if } k^{p^s+1} - j^{p^s+1} = 0, \\ 0 & \text{en otro caso.} \end{cases} \tag{4.91}$$

Comparando los valores de las sumas S_1 y S_2 observamos que los operadores puntuales en el origen para ambas coberturas simplécticas serán iguales si y solo si las ecuaciones

$$k^2 - j^2 = 0 \quad \text{y} \quad k^{p^s+1} - j^{p^s+1} = 0 \tag{4.92}$$

comparten el *mismo* conjunto de soluciones en $\mathrm{GF}(p^n)$. La estructura particular de éste sistema de ecuaciones permite una verificación relativamente sencilla de que efectivamente sucede ésto para todo p, n y s apropiados.

Ignorando a la solución trivial y utilizando el cambio de variable $r = k/j$, las ecuaciones del sistema (4.92) se pueden expresar como

$$r^2 = 1 \quad \text{y} \quad r^{p^s+1} = 1. \tag{4.93}$$

Éstas dos ecuaciones comparten el mismo conjunto de soluciones si y solo si el sistema original también comparte las suyas. En característica impar la ecuación $r^2 = 1$ tiene dos soluciones, dadas por $r = 1$ y $r = -1$. Notemos que éstas dos soluciones también satisfacen la ecuación $r^{p^s+1} = 1$, por lo tanto realmente solo tenemos que demostrar que $r^{p^s+1} = 1$ *no tiene más de dos* soluciones en $\mathrm{GF}(p^n)$.

Consideremos un generador g del grupo cíclico $\mathbb{F}^*$ de $p^n - 1$ elementos, el cual es el grupo multiplicactivo del campo $\mathbb{F}$. Se conoce en la teoría de los grupos cíclicos que el orden del elemento g^{p^s+1} es

$$\left|g^{p^s+1}\right| = \frac{p^n - 1}{\gcd(p^n - 1, p^s + 1)}, \tag{4.94}$$

donde $\gcd(a, b)$ es el máximo común divisor de los números a y b. Sea $\phi : \mathbb{F}^* \to \mathbb{F}^*$ el mapa definido por $x \mapsto x^{p^s+1}$. El mapa ϕ claramente es un homomorfismo de grupos y dado que g es un generador de $\mathbb{F}^*$, la imágen de g bajo ϕ es un generador de $\mathrm{img}(\phi)$. Ésto a su vez implica que $|\operatorname{img}(\phi)| = \left|g^{p^s+1}\right|$. Entonces del primer teorema de isomorfía y de la ecuación (4.94) obtenemos

$$|\ker(\phi)| = \frac{|\,\mathbb{F}^*\,|}{|\operatorname{img}(\phi)|} = \frac{p^n - 1}{|g^{p^s+1}|} = \gcd(p^n - 1, p^s + 1). \tag{4.95}$$

Se sigue que el demostrar que $r^{p^s+1} = 1$ no tiene más de dos soluciones es equivalente a demostrar que $\gcd(p^n - 1, p^s + 1) \leq 2$. Supongamos que d es un divisor de $p^n - 1$ y de $p^s + 1$. Dado que divide a $p^s + 1$, también divide a $p^{2s} - 1 = (p^s + 1)(p^s - 1)$. Se puede demostrar utilizando el algoritmo Euclideano sobre los exponentes que

$$d \mid p^{2s} - 1, p^n - 1 \implies d \mid p^{\gcd(2s,n)} - 1.$$

Por hipótesis, n es impar y $\gcd(s,n) = 1$, por lo tanto $\gcd(2s,n) = \gcd(s,n) = 1$. Entonces $d \mid p-1$, lo cual significa que $p \equiv 1 \mod d$. Ésto a su vez implica que $p^s \equiv 1$ mód d para todo s, en particular $d \mid p^s - 1$. Dado que $d \mid p^s + 1, p^s - 1$, se sigue que $d \mid 2$. Por lo tanto $\gcd(p^n - 1, p^s + 1) \leq 2$ y así $|\ker(\phi)| \leq 2$. Ésto concluye la demostración.

Con lo anterior, hemos demostrado que las ecuaciones en (4.92) comparten el mismo conjunto de soluciones. Por lo tanto las sumas de Weil S_1 y S_2 son iguales para todo $k, j \in \mathbb{F}$. Ésto a su vez significa que los operadores puntuales en el origen para ambas coberturas simplécticas son iguales. La covarianza bajo traslaciones implica que *todos* los operadores puntuales para ambas coberturas también serán iguales. Como consecuencia, obtenemos la misma función de Wigner discreta para la construcción estándar y no estándar, para cualquier cobertura de la famila de presemicampos de Albert. Ésto sucede a pesar de que las MUBs no son unitariamente equivalentes. Al parecer la inequivalencia unitaria de las MUBs *no* es suficiente para garantizar la desigualdad de las funciones de Wigner estándar y no estándar.

Wootters y Gibbons propusieron una manera de estudiar la equivalencia de funciones de Wigner discretas bajo relaciones de equivalencia dadas por transformaciones unitarias de las mallas cuánticas.

Definición 29. *Decimos que dos mallas cuánticas son equivalentes si solo difieren por una transformación unitaria, es decir, dos mallas cuánticas Q y Q' son iguales si existe una transformación unitaria U tal que*

$$Q'(\lambda) = UQ(\lambda)U^*, \tag{4.96}$$

para toda curva λ del espacio de fase discreto.

Por un lado es fácil ver que si Q y Q' son unitariamente equivalentes, entonces los operadores puntuales $A(\alpha)$ y $A'(\alpha)$ también lo son, ya que

$$\begin{aligned} A'(\alpha) &= \sum_{\lambda \ni \alpha} Q'(\lambda) - I && (4.97)\\ &= \sum_{\lambda \ni \alpha} UQ(\lambda)U^* - I && (4.98)\\ &= U\left(\sum_{\lambda \ni \alpha} Q(\lambda) - I\right)U^* && (4.99)\\ &= UA(\alpha)U^*. && (4.100) \end{aligned}$$

Naturalmente nos preguntamos si la proposición conversa también se cumple. Si los operadores puntuales son unitariamente equivalentes, ¿ésto implica que las mallas también lo son? Dicho de otra manera, si utilizamos MUBs no equivalentes, ¿los operadores puntuales tampoco serán equivalentes? El resultado que obtuvimos en ésta sección es un contra ejemplo de la proposición conversa, ya que la identidad es una transformación unitaria. En otras palabras, incluso cuando no existe una transformación unitaria entre dos mallas cuánticas, los operadores puntuales pueden ser equivalentes. Por lo tanto el método de Wootters para clasificar funciones de Wigner equivalentes parece no ser apropiado cuando uno desea estudiar la inequivalencia de la función de Wigner. Parece ser necesario estudiar que propiedades adicionales debe tener una malla cuántica o el espacio de fase discreto en particular, para poder determinar cuando una función de Wigner es unitariamente distinta a otra.

El hecho de que ésto no sucede (al menos numericamente) en el ejemplo de los cinco qubits puede ser consecuencia de la cobertura particular que usamos para la construcción no estándar, ó, posiblemente es otro detalle interesante consecuencia de los campos de característica par. Un siguiente paso sería estudiar otras coberturas simplécticas para característica impar que también son inequivalentes a la Desarguesiana, para ver si sucede algo similar. Dado que nuestra demostración de la equivalencia depende totalmente de la forma de las operaciones de los presemicampos en cuestión, no podemos concluir mucho sobre las funciones de Wigner discretas obtenidas con otras coberturas simplécticas en general. Creemos que será conveniente utilizar otro método de demostración que no requiera utilizar la forma explícita de la operación del presemicampo, ya que dependemos de fórmulas de evaluación de sumas exponenciales las cuales no siempre se conocen.

4.5. Discusión

Hemos construido dos versiones de funciones de Wigner para sistemas de dimensión finita. El método de construcción se basa en la metodología de Wootters y Gibbons, en donde le asignamos una estructura cuántica al espacio de fase discreto. La estructura cuántica corresponde a un conjunto maximal de bases mutuamente insesgadas, las cuales dotan a la función de Wigner las propiedades análogas al caso continuo, en particular la propiedad tomográfica. Ésta propiedad nos permite recuperar el operador de densidad a partir de su función de Wigner. Dada la libertad en la asignación de la estructura cuántica al espacio de fase discreto, pudimos construir una versión no estándar utilizando MUBs que no son unitariamente equivalentes a las de Wootters. A pesar de ésto, no logramos concluir sobre la inequivalencia entre las funciones de Wigner producidas por ambas construcciones, ya que la no equivalencia de las MUBs no es una condición suficiente para producir funciones de Wigner discretas distintas. Ésto es una consecuencia de nuestra demostración en el ejemplo de la familia de presemicampos de Albert. Éste resultado que obtuvimos nos indica que debemos encontrar otra manera de estudiar la equivalencia de las funciones de Wigner que va más allá de la malla cuántica. En particular es importante identificar si es un resultado que depende de la cobertura particular elegida o sí es una consecuencia de la dimensión del sistema, ya que para el caso de los cinco qubits sí obtuvimos (al menos numéricamente) distintas funciones.

Otro aspecto de éste método de construcción que es victima de la arbitrariedad, es que la gráfica de una función de Wigner depende del orden elegido del campo finito utilizado para armar el espacio de fase. Evidentemente no hay un ordenamiento predilecto, ya que los campos finitos no son ordenados. Durante todo el trabajo hemos optado por utilizar el ordenamiento por potencias del generado de la extensión de Galois, pero se ha observado que distintos ordenamientos producen gráficas con distintas cualidades, unas más ordenadas que otras. Como trabajo futuro sería interesante estudiar los efectos del orden elegido en cuanto alguna medida del orden o aleatoriedad de la gráfica de la función de Wigner, y estudiar si ésto tiene consecuencias en las interpretaciones físicas.

Por otro lado, la metodología de Wootters revela de manera directa la relación que existe entre estructuras geométricas finitas y algunas particularidades de los sistemas cuánticos discretos. Como hemos mencionado anteriormente, aun es un problema abierto el encontrar la cantidad máxima de bases mutuamente insesgados para sistemas de dimensión compuesta que no son potencias de primos. De la misma manera existen problemas abiertos análogos en el álgebra combinatoria [44], en la teoría de códigos [41] y en la teoría de las álgebras de Lie [45, 40, 39], entre otros, que parece indicar una relación más profunda. Es posible que hallazgos y avances en algunas de éstas áreas nos provee la solución al problema de las MUBs o vice-versa. Si los sistemas de dimensión que son potencias de primos son los únicos de los cuales podemos obtener la cantidad máxima de MUBs, ¿qué nos dice ésto en cuestión de la tomografía cuántica y en la cuestión de la medición de estados cuánticos? Por otro lado, existen conjuntos de MUBs, digamos $\mathcal{B}$, que no son maximales y que además son *inextendibles* en el sentido de que no existen otras bases del espacio de Hilbert que son mutuamente insesgadas respecto a los conjuntos de $\mathcal{B}$ [46]. Seguramente existen relaciones entre éstos conjuntos y las estructuras geométricas estudiadas en éste trabajo.

En un aspecto más práctico, el hecho de que podemos obtener MUBs que no son

unitariamente equivalentes a las 'clasicas', nos da la posibilidad de encontrar otros esquemas de factorización que pudieran resultar útiles para ciertos problemas físicos. Ésto es otra dirección interesante que nos gustaría investigar posteriormente. También recordamos que unas de las motivaciones principales de éste trabajo fueron los resultados relativamente recientes de Gross [7] entre otros, que relacionan la positividad de una versión particular de la función de Wigner discreta con estados Gaussianos, entre ellos los estabilizadores, de los cuales se ha probado que son simulables de manera clásica. Una investigación futura podría involucrar la busqueda de estados no estabilizadores con funciones de Wigner no estándar no negativa, algo que contrastaría con los resultados previos.

Apéndice A

Apéndices

A.1. La mecánica clásica y el espacio de fase

El concepto del espacio de fase es una herramienta de la mecánica clásica, la cual describe la evolución temporal de un sistema físico. Dicho de una manera muy sencilla, la mecánica clásica estudia partículas y sus trayectorias, las cuales se rigen de acuerdo a las leyes de Newton. Se considera que la partícula se 'mueve' en un espacio euclideano, es decir, su *posición* está dado por $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$. El *momentum* es una cantidad dada por $p_j = m\dot{x}_j$, donde $\dot{x}$ es la derivada respecto al tiempo de la posición, es decir, la velocidad de la partícula, y m es la *masa* de la partícula. Las cantidades que uno desea medir de nuestro sistema físico se les llama *observables*, y en la mecánica clásica, son las funciones continuas que tienen como argumentos las cantidades x, p y m. Ejemplos de ellos son el momentum, la energía cinética, la energía potencial, etc. La función de energía más usual es la que está dada como la suma de la *energía cinética* y *energía potencial*:

$$H(x,p) = \frac{1}{2m}\sum_{j=1}^{n} p_j^2 + V(x). \tag{A.1}$$

A la energía del sistema se le conoce como el *Hamiltoniano*. Utilizando ésta función de energía, la ley de Newton nos brinda las ecuaciones de movimiento de la partícula en cuestión:

$$\frac{dx_j}{dt} = \frac{\partial H}{\partial p_j}, \quad \frac{dp_j}{dt} = -\frac{\partial H}{\partial x_j}. \tag{A.2}$$

Expresada como un sistema de ecuaciones diferenciales, a la ley de Newton se le conoce como las *ecuaciones de Hamilton*. Con ésto, es natural representar el estado del sistema clásico considerando el par $(x,p) \in \mathbb{R}^{2n}$. Al espacio $\mathbb{R}^{2n}$ se le conoce como el *espacio de fase*. A las soluciones de las ecuaciones de Hamilton se les conoce como *trayectorias*, y son curvas que viven en el espacio de fase.

Definición 30. *El espacio de fase de una partícula que se mueve en $\mathbb{R}^n$ es $\mathbb{R}^{2n}$, considerado como el conjunto de las $(2n)$-tuplas de la forma*

$$(x_1, \ldots, x_n, p_1, \ldots, p_n),$$

donde x_j y p_j son elementos de $\mathbb{R}$.

Cabe mencionar que el tratado moderno de la mecánica clásica está fundamentado en la geometría diferencial de las variedades simplécticas [47], en donde el espacio de fase

se define como el espacio cotangente del espacio de configuraciones $T^*\,\mathbb{R}_x \cong \mathbb{R}_x \times \mathbb{R}_p$, donde el espacio de configuraciones $\mathbb{R}_x$ es el espacio de posición y el $\mathbb{R}_p$ es el espacio del momentum. Para nuestros objetivos basta con desginar el espacio de fase como el espacio $\mathbb{R}^{2n}$.

Dado que la mecánica cuántica es una teoría estadística, es más apropiado comparar la mecánica de una sola partícula cuántica con un *conjunto* de partículas clásicas. La maquinaría utilizada para éste propósito es la mecánica estadística, especialmente la ecuación de Liouville para la distribución de un conjunto de partículas.

A.2. Campos finitos

Si intentamos definir el espacio de fase discreto sobre un anillo como por ejemplo $\mathbb{Z}_4$, tendremos problemas a la hora de trabajar con rectas y otras estructuras geométricas. Por ejemplo, la recta

$$x + 2p = 0,$$

tiene como solución al conjunto de puntos

$$\{(0,0),(2,1),(0,2),(2,3)\}. \tag{A.3}$$

Similarmente, la recta

$$x = 0,$$

tiene como solución al conjunto

$$\{(0,0),(0,1),(0,2),(0,3)\}. \tag{A.4}$$

Notemos que los dos conjuntos tiene una intersección con *más* de un elemento, algo que contradice nuestra noción geoemétrica de una linea en el espacio, ya que ambas lineas son distintas. Ésto es un ejemplo de la falta de estructura geométrica de un espacio de fase discreto cuando solo utilizamos un anillo. Para poder preservar las nociones geométricas del espacio Euclideano es necesario utilizar una estructura algebráica más *rica*, especificamente la de un campo finito.

Lo que sigue es un resumén breve de los conceptos y resultados que fundamentan el uso de los campos finitos para trabajar con la geometría necesaria del espacio de fase discreto. La mayoría está basado en las notas de Zhe-Xian Wan [48] y en el libro de Rudolf Lidl y Harald Niederreiter [43].

Definición 31. *Un anillo $(R,+,\cdot)$ es un conjunto R, con dos operaciones binarias, denotadas por $+$ y $\cdot$, tales que:*

1. *R es un grupo abeliano respecto a la suma $+$.*
2. *La operación $\cdot$ es asociativa.*
3. *Las leyes distributivas se cumplen, es decir, para todo $a,b,c \in R$ tenemos que*

$$a\cdot(b+c) = a\cdot b + a\cdot c, \quad y \quad (b+c)\cdot a = b\cdot a + c\cdot a.$$

Un anillo R se llama *anillo con identidad* si tiene una identidad multiplicativa. Si la operación $\cdot$ es conmutativa entonces el anillo es conmutativo. Decimos que el anillo es un *dominio integral* si es un anillo conmutatitivo con identidad $1 \neq 0$, tal que $ab = 0$

implica que $a = 0$ o $b = 0$. Un anillo es un *anillo de división* si los elementos no cero de R forman un grupo bajo $\cdot$. En particular un anillo de división conmutativo es un *campo*. Visto de otra manera tenemos que:

Definición 32. *Sea $\mathbb{F}$ un conjunto con dos operaciones binarias, una llamada suma $+$ y otra llamada multiplicación $\cdot$. Decimos que $\mathbb{F}$ es un campo si*

1. *$(\mathbb{F}, +)$ es un grupo abeliano.*
2. *$(\mathbb{F}^*, \cdot)$ es un grupo abeliano, donde $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ y 0 es el cero del grupo aditivo.*
3. *Se satisfacen las propiedades distributivas:*

$$a(b + c) = ab + ac, \quad (b + c)a = ba + ca,$$

para todo $a, b, c \in \mathbb{F}$.

El inverso aditivo de un elemento $a \in \mathbb{F}$ se denota como $-a$ y el inverso multiplicativo se denota a^{-1}.

Definición 33. *Sea $\mathbb{F}$ un campo. Si el número de elementos de $\mathbb{F}$ es infinito, entonces $\mathbb{F}$ es un campo infinito. Si el número de elementos es finito, decimos que $\mathbb{F}$ es un campo finito.*

Todos los campos son en particular un dominio integral, pero el converso no es siempre cierto, al menos que el dominio integral sea finito.

Ejemplo 12. *Sea n un número entero. El conjunto $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ consiste de n clases residuales*

$$[a] = a + n\mathbb{Z} = \{a + nk : k \in \mathbb{Z}\}.$$

Como de costumbre, omitimos la notación de clase de equivalencia $[\cdot]$. En $\mathbb{Z}_n$ tenemos que

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ veces}} = 0.$$

Notemos que $\mathbb{Z}_n$ simplemente consiste de los enteros módulo n. En el caso en n es un número primo p, entonces el anillo de clases residuales de los enteros módulo el ideal principal generado por p, $\mathbb{Z}_p$, es un campo.

Definición 34. *Sea $\mathbb{F}$ un campo y 1 su identidad multiplicativa. Si para cualquier entero positivo m tenemos que $m \cdot 1 \neq 0$, entonces la característica de $\mathbb{F}$ es 0. Si existe un entero positivo m tal que $m \cdot 1 = 0$, entonces el entero p más pequeño que satisface $p \cdot 1 = 0$ se llama la característica de $\mathbb{F}$.*

Los campos $\mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ son de característica 0, mientras que $\mathbb{Z}_p$ es de característica prima p. Es fácil probar que la característica de un campo es 0 o es un número primo. Si $\mathbb{F}$ es un campo de característica p entonces

$$\Pi = \{0, 1, 2 \cdot 1, \ldots, (p - 1) \cdot 1\},$$

es un *subcampo* de $\mathbb{F}$. De hecho, es el subcampo más pequeño de $\mathbb{F}$ y se le conoce como el *campo primo* ya que es isomorfo a $\mathbb{Z}_p$.

Lema 1. *Sea $\mathbb{F}$ un campo finito de característica $p \neq 0$. Sea n un entero no negativo, entonces el mapeo $\sigma_n : \mathbb{F} \to \mathbb{F}$ dado por*

$$\sigma_n : a \mapsto a^{p^n}, \quad a \in \mathbb{F}$$

es un automorfismo de $\mathbb{F}$.

Es natural preguntarnos como podemos construir campos finitos de orden no primo. Para ésto investiguemos brevemente a los campos de clases residuales. Sea $\mathbb{F}$ un campo y m un elemento fijo de $\mathbb{F}$. Entonces para cualesquiera dos elementos $a, b \in \mathbb{F}$, decimos que

$$a \cong b \,(\mod m) \tag{A.5}$$

si y solo si $m|(a-b)$. Ésto es una clase de equivalencia en $\mathbb{F}$ y cada clase de equivalencia se conoce como *clase residual* módulo m.

Definición 35. *Sea $\mathbb{F}$ un campo, $\mathbb{F}[x]$ el anillo de polinomios sobre $\mathbb{F}$ y $f(x)$ un polinomio en $\mathbb{F}[x]$. El anillo*

$$F[x]/\langle f(x)\rangle$$

se conoce como el anillo de clases residuales del anillo polinomial $\mathbb{F}[x]$ módulo el polinomio $f(x)$. Más aún, si $f(x)$ es un polinomio irreducible sobre $\mathbb{F}$, entonces $\mathbb{F}[x]/\langle f(x)\rangle$ es un campo.

Teorema 7. *Sea $\mathbb{F}$ un campo, $\mathbb{E}$ un subcampo de $\mathbb{F}$ y $\alpha \in \mathbb{E}$. Sea $p(x)$ un polinomio irreducible de grado n sobre $\mathbb{F}_p$ y supongamos que $p(\alpha) = 0$. Entonces $\mathbb{F}[\alpha]$ es un subcampo de $\mathbb{E}$,*

$$\mathbb{F}[\alpha] = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots a_{n-1}\alpha^{n-1} : \alpha_i \in \mathbb{F}\}, \tag{A.6}$$

y todo elemento de $\mathbb{F}[\alpha]$ puede ser expresado de manera única como

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}. \tag{A.7}$$

Además $F[\alpha]$ es isomofo a la clase residual $\mathbb{F}[x]/\langle p(x)\rangle$.

Teorema 8. *Sea $\mathbb{F}$ un campo y $p(x)$ un polinomio irreducible de grado n sobre $\mathbb{F}$. Denotemos la clase residual de $x \mod p(x)$ por α. Entonces*

$$F[x]/\langle p(x)\rangle \cong F[\alpha]. \tag{A.8}$$

Además si $\mathbb{F}$ es un campo finito con p elementos, entonces el orden de $F[x]/\langle p(x)\rangle$ es p^n.

El teorema anterior nos dice que para construir a $\mathbb{F}_d$ donde $d = p^n$ requerimos de un polinomio $f(x)$ de grado n que es irreducible en $\mathbb{F}_p$. Si α es una raíz de $f(x)$, el campo que obtenemos al adjuntar α a $\mathbb{F}_p$ es

$$\mathbb{F}_N = \mathbb{F}_r(\alpha) \cong \mathbb{F}_r[x]/\langle f(x)\rangle. \tag{A.9}$$

Ejemplo 13. *Consideremos el campo $\mathbb{Z}_2$ y el polinomio $f(x) = x^2 + x + 1$. Notemos que $f(0) = f(1) = 1$, por lo tanto $f(x)$ no tiene raíces en $\mathbb{Z}_2$, i.e., $f(x)$ es irreducible*

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

Cuadro A.1: Tabla de adición de $\mathbb{F}_4$.

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

Cuadro A.2: Tabla de multiplicación de $\mathbb{F}_4$.

sobre $\mathbb{Z}_2$*. De acuerdo al teorema anterior, la extensión de Galois* $\mathbb{Z}_2/\langle f(x)\rangle$ *tiene* 2^2 *elementos y está dada por*

$$\mathbb{F}_4 := \mathbb{Z}_2[x]/(x^2+x+1) \cong \mathbb{Z}_2[\alpha] = \{0, 1, \alpha, \alpha+1\},$$

donde α *es la clase residual de* $x \mod x^2+x+1$*. La tabla de adición está dada por Similarmente podemos calcular la tabla de multiplicación. Cualquier campo de cuatro elementos es isomorfo a* $\mathbb{F}_4$*.*

Si $\mathbb{F}_d$ es un campo finito de d elementos, el grupo multiplicativo $\mathbb{F}_d^*$ es de orden $d-1$. El orden de cada elemento de éste grupo es un divisor de $d-1$, por lo tanto $a^{d-1} = 1$ para todo $a \in \mathbb{F}_d^*$. Además se puede probar que el grupo multiplicativo de cualquier campo finito es cíclico. A los generadores del grupo cíclico $\mathbb{F}_d^*$ se les conoce como *elementos primitivos.*

A.2.1. Automorfismos de campos finitos

Sea d una potencia de un primo y $\mathbb{F}_d$ un campo finito. Sea n un entero positivo, entonces podemos ver a $\mathbb{F}_d$ como un subcampo del campo $\mathbb{F}_{d^n}$. El mapeo

$$\sigma : \alpha \mapsto \alpha^d \tag{A.10}$$

de $\mathbb{F}_{d^n}$ a si mismo es un automorfismo de $\mathbb{F}_{d^n}$. Resulta que $\sigma(a) = a$ si y solo si $a \in \mathbb{F}_d$, i.e., los elementos del subcampo son invariantes bajo σ. Al automorfismo σ de $\mathbb{F}_d$ se le conoce como el *automorfismo de Frobenius.* Denotemos por σ^2 a la composición $\sigma \circ \sigma$, entonces σ^2 también es un automorfismo de $\mathbb{F}_{d^n}$ sobre $\mathbb{F}_d$. En general, si $\sigma^0 = 1$ donde 1 en éste caso significa el mapeo identidad sobre $\mathbb{F}_{d^n}$, tenemos que

$$\sigma^{i+1} = \sigma \circ \sigma^i, \quad i = 1, 2, \ldots, \tag{A.11}$$

son automorfismos sobre $\mathbb{F}_d$. Notemos que $\sigma^n = 1$. Además de que σ fija a todo elemento de $\mathbb{F}_d$, también tenemos que σ^1 y $\sigma^k \neq 1$ para $1 \leq k < n$, y $\sigma^0 = 1, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ son n automorfismos *distintos* de $\mathbb{F}_{d^n}$ sobre $\mathbb{F}_d$. El conjunto de automorfismos de $\mathbb{F}_{d^n}$

sobre $\mathbb{F}_d$ forman un grupo respecto a la composición, llamado el *grupo de Galois* de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_d$, denotado por $\mathrm{Gal}\left(\mathbb{F}_{d^n} / \mathbb{F}_d\right)$. Se puede demostrar que

$$\mathrm{Gal}\left(\mathbb{F}_{d^n} / \mathbb{F}_d\right) = \langle \sigma \rangle, \tag{A.12}$$

i.e., todo automorfismo puede ser expresado como una potencia del automorfismo de Frobenius. En otras palabras, los automorfismos $\sigma^0 = 1$, $\sigma, \ldots, \sigma^{n-1}$ son *todos* los automorfismos de $\mathbb{F}_{d^n}$ sobre $\mathbb{F}_d$.

Definición 36. *Sea d una potencia de un primo y n un entero positivo. Podemos asumir que $\mathbb{F}_d$ es un subcampo de $\mathbb{F}_{d^n}$. Sea σ el automorfismo de Frobenius de $\mathbb{F}_{d^n}$ sobre $\mathbb{F}_d$. Si $\alpha \in \mathbb{F}_{d^n}$, su traza relativa a $\mathbb{F}_q$ es*

$$\mathrm{tr}_{\mathbb{F}_{d^n} / \mathbb{F}_d}(\alpha) = \sum_{i=0}^{n-1} \sigma^i(\alpha) = \alpha + \alpha^d + \alpha^{d^2} + \cdots + \alpha^{d^{n-1}}. \tag{A.13}$$

Si el campo y subcampo son claros dentro del contexto en que se maneja la traza, simplemente la denotamos por tr. La operación tr mapea a todo elemento del campo finito a un elemento del subcampo $\mathrm{tr} : \mathbb{F}_{d^n} \to \mathbb{F}_d$. La traza satisface la siguientes propiedades.

Teorema 9. *Para $\alpha, \beta \in \mathbb{F}_{d^n}$ y $a \in \mathbb{F}_d$ tenemos*

- $\mathrm{tr}(\alpha) \in \mathbb{F}_d$.
- $\mathrm{tr}(\alpha + \beta) = \mathrm{tr}(\alpha) + \mathrm{tr}(\beta)$;
- $\mathrm{tr}(a\alpha) = a\,\mathrm{tr}(\alpha)$ *y* $\mathrm{tr}(a) = n\,\mathrm{tr}(a)$.
- $\mathrm{tr}\left(\alpha^d\right) = \mathrm{tr}(\alpha)$.
- *La traza es suprayectiva y para $\alpha \in \mathbb{F}_{d^n}$, $\mathrm{tr}(\alpha) = 0$ si y solo si existe un elemento $\beta \in \mathbb{F}_{d^n}$ tal que $\alpha = \beta - \beta^d$.*
- *Para cualquier $a \in \mathbb{F}_d$, el número de elementos $\alpha \in \mathbb{F}_{d^n}$ tales que $\mathrm{tr}(\alpha) = a$ es d^{n-1}.*

A.2.2. Bases de campos

Sean $\mathbb{F}_{d^n}$ y $\mathbb{F}_d$ campos finitos, donde d es una potencia de un primo y n es un entero positivo. Supongamos además que $\mathbb{F}_d$ es un subcampo de $\mathbb{F}_{d^n}$. Podemos ver al campo $\mathbb{F}_{d^n}$ como un espacio vectorial sobre $\mathbb{F}_d$ al definir una multiplicación escalar de la siguiente manera:

$$\begin{aligned} \mathbb{F}_d \times \mathbb{F}_{d^n} &\to \mathbb{F}_{d^n} \\ (a, \alpha) &\mapsto a\alpha. \end{aligned}$$

Supongamos que $\dim \mathbb{F}_{d^n} = m$ y sea $\alpha_1, \alpha_2, \ldots, \alpha_m$ una base del espacio vectorial $\mathbb{F}_{d^n}$ sobre $\mathbb{F}_d$. Todo elemento $\beta \in \mathbb{F}_{d^n}$ puede ser expresado como una combinación lineal de elementos de la base con coeficientes en $\mathbb{F}_d$:

$$\beta = b_1\alpha_1 + \ldots + b_n\alpha_m.$$

Por lo tanto $|\mathbb{F}_{d^n}|$ lo que implica que $m = n$. En general, $\mathbb{F}_{d^n}$ es un espacio vectorial sobre $\mathbb{F}_d$ de dimensión n. A la cardinalidad de la base se le conoce grado de la extensión $\mathbb{F}_{d^n}$ sobre $\mathbb{F}_d$ y es común denotarla como

$$[\mathbb{F}_{d^n} : \mathbb{F}_d] = n.$$

Sumar y restar elementos de la base se puede hacer utilizando la base de manera natural. Para obtener las coordenadas de una suma $\beta + \gamma$, basta con sumar las coordenadas de β y de γ en la base. Podemos hacer algo similar para la multiplicación de los elementos. Podemos obtener más bases por medio de matrices no singulares.

Teorema 10. *Sea $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ una base de $\mathbb{F}_{d^n}$ sobre $\mathbb{F}_d$ y*

$$(a_{ij}), \quad 1 \leq i, j \leq n,$$

una matriz $n \times n$ no singular sobre $\mathbb{F}_d$. Los elementos

$$\beta_j = \sum_{i=1}^{n} a_{ij}\alpha_i, \quad j = 1, 2, \ldots, n$$

forman una base de $\mathbb{F}_{d^n}$ sobre $\mathbb{F}_d$.

Existen distintos criterios para identificar cuando un conjunto de elementos del campo es una base para el espacio vectorial, pero éstos criterios no serán importantes para nosotros. Por ahora, consideremos un elemento $\alpha \in \mathbb{F}_{d^n}$ de grado n sobre $\mathbb{F}_d$. Entonces

$$1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$$

es una base del campo. Ésta base comunmente se conoce como la *base polinomial*. Enseguida introducimos el concepto de una base dual del campo finito.

Definición 37. *Sean $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ y $\{\beta_1, \beta_2, \ldots, \beta_n\}$ dos bases de $\mathbb{F}_{d^n}$ sobre $\mathbb{F}_d$. Si*

$$\mathrm{tr}(\alpha_i\beta_j) = \delta_{ij}, \quad \textit{para todo} \quad i, j = 1, 2, \ldots, n,$$

entonces decimos que las bases son duales una respecto a la otra, en particular $\{\beta_1, \beta_2, \ldots, \beta_n\}$ es una base dual a $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$.

Toda base de un campo tiene una *única* base dual. Para construir la base dual y para el cálculo de la traza de los elementos de la extensión, resulta ventajoso definir la siguiente matriz con elementos en el campo primo.

Proposición 23. *Sean g, G las siguientes matrices simétricas e invertibles $n \times n$ con elementos en $\mathbb{Z}_p$:*

$$g_{ij} = \mathrm{tr}(\omega^{i+j}); \quad G = g^{-1}, \quad i, j = 1, \ldots, n. \tag{A.14}$$

El conjunto de elementos $\{\beta_1, \beta_2, \ldots, \beta_n\}$ definido como

$$\beta_i = \sum_j G_{ij}\omega^j, \tag{A.15}$$

es una base dual a $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$.

Con lo anterior, podemos calcular los componentes de cualquier elemento α de la extensión de campos, en términos de la base o de su dual:

$$\alpha_i = \mathrm{tr}(\alpha\beta_i); \quad \overline{\alpha}_i = \mathrm{tr}(\alpha\alpha^i) \tag{A.16}$$

$$\alpha_i = \sum_j G_{ij}\overline{\alpha}_j; \quad \overline{\alpha}_i = \sum_j g_{ij}\alpha_j. \tag{A.17}$$

Entre las bases que podemos elegir de un campo finito, a parte de la base polinomial, existen bases que resultan ser muy útiles, especificamente para la construcción de Wootters de los operadores de Pauli generalizados. Ésto es el concepto de una base *auto-dual*.

Definición 38. *Una base* $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ *de* $\mathbb{F}_{d^n}$ *sobre* $\mathbb{F}_d$ *es una base auto-dual si*

$$\mathrm{tr}_{\mathbb{F}_{d^n}/\mathbb{F}_d}(\alpha_i\alpha_j) = \delta_{ij}, \quad \textit{para todo} \quad i,j = 1,2,\ldots,n. \tag{A.18}$$

La existencia de una base auto-dual no es garantizada para toda potencia de primos. Pero, para $d = 2^r$ sí existe una base auto-dual de $\mathbb{F}_{d^n}$ sobre $\mathbb{F}_d$. El caso de característica impar es más sutil. Si d es una potencia de un primo impar, entonces existe una base auto-dual de $\mathbb{F}_{d^n}$ sobre $\mathbb{F}_d$ si y solo si n también es impar. Es natural preguntarnos ¿cuántas bases auto-duales existen para un campo finito? La respuesta a ésta pregunta no es trivial pero si definitiva, y resulta que también es distinta para los casos de característica par e impar.

Ejemplo 14. *Sea* $\alpha \in \mathbb{F}_{2^3}$ *una raíz del polinomio irreducible* $x^3 + x^2 + 1$ *en* $\mathbb{F}_2[x]$. *Entonces el conjunto* $\{\alpha, \alpha^2, 1 + \alpha + \alpha^2\}$ *es una base de* $\mathbb{F}_{2^3}$ *sobre* $\mathbb{F}_2$. *Además es fácil verificar que es una base auto-dual.*

A.2.3. Sumas exponenciales

El uso de sumas exponenciales para campos finitos resulta ser útil para varias aplicaciones. Hacemos un resumen breve de algunos resultados ya que mucha de la literatura que utilizamos para la construcción explícita de las MUBs requiere de manera directa o indirecta de éstos resultados. En particular exponemos (sin prueba) dos resultados que utilizamos para demostrar la equivalencia de las sumas que aparecen en el ejemplo de los tres qutrits. Las demostraciones y detalles se pueden encontrar en el libro de Lidl y Niederreiter [49].

Las sumas exponenciales están formadas por un grupo especial de homomorfismos llamados *caracteres*.

Definición 39. *Sea* G *un grupo abeliano finito de orden* $|G|$ *con identidad* 1_G. *Un caracter* χ *de* G *es un homomorfismo de* G *a el grupo multiplicativo* U *de los números complejos de valor absoluto unitario. Notemos que*

$$(\chi(g))^{|G|} = \chi\left(g^{|G|}\right) = \chi\left(1_G\right) = 1$$

para todo $g \in G$, *por lo que los valores* χ *son las* $|G|$*-ésimas raíces de la unidad.*

El conjunto $\hat{G}$ de todos los caracteres de G forma un grupo abeliano bajo la multiplicación de caracteres. Ahora veamos algunas propiedades interesantes de los caracteres.

Teorema 11. *Si χ es un caracter no trivial de un grupo finito abeliano G, entonces*

$$\sum_{g\in G}\chi(g)=0. \tag{A.19}$$

Además, si $g\in G$ tal que $g\neq 1_G$, entonces

$$\sum_{\chi\in\hat{G}}\chi(g)=0. \tag{A.20}$$

Recordemos que en un campo finito $\mathbb{F}_d$, existen dos grupos finitos abelianos de importancia, el grupo aditivo y el grupo multiplicativo. En ambos casos podemos obtener expresiones explicítas de los caracteres del grupo. Consideremos el grupo aditivo de $\mathbb{F}_d$. Sea p la característica de $\mathbb{F}_d$, e identificamos al subcampo primo de $\mathbb{F}_d$ con $\mathbb{Z}_p$. Definamos a la función χ_1 de la siguiente manera:

$$\chi_1(c)=e^{2\pi i\,\mathrm{tr}(c)/p},\quad \text{para todo } c\in\mathbb{F}_d\,. \tag{A.21}$$

Es trivial probar que χ_1 es un caracter del grupo aditivo, y le llamamos un *caracter aditivo* de $\mathbb{F}_d$. Cuando el contexto es claro, denotaremos a χ_1 simplemente por χ. Todos los caracteres aditivos de $\mathbb{F}_d$ pueden ser expresados en términos del caracter χ_1. Para los caracteres aditivos χ_a y χ_b tenemos que

$$\sum_{c\in\mathbb{F}_d}\chi_a(c)\overline{\chi_b(c)}=\begin{cases}0 & \text{para } a\neq b\\ d & \text{para } a=b,\end{cases} \tag{A.22}$$

y en particular

$$\sum_{c\in\mathbb{F}_d}\chi_a(c)=0,\quad \text{para } a\neq 0. \tag{A.23}$$

Similarmente podemos formar los caracteres del grupo multiplicativo $\mathbb{F}_d^*$ del campo finito $\mathbb{F}_d$, los cuales se llaman *caracteres multiplicativos*. Éstos caracteres se pueden expresar de la siguiente manera.

Teorema 12. *Sea g un elemento primitivo fijo de $\mathbb{F}_d$. Para todo $j=0,1,\ldots,d-2$, la función ψ_j dada por*

$$\psi_j(g^k)=e^{2\pi ijk/(d-1)},\quad \textit{para todo } k=0,1,\ldots,d-2, \tag{A.24}$$

define un caracter multiplicativo en $\mathbb{F}_d$ y además todo caracter multiplicativo se obtiene de ésta manera.

Muchos de los resultados de las sumas Gaussianas y de Weil que veremos enseguida dependen de ambos caracteres, pero para nuestro trabajo basta con enfocarnos en el grupo de caracteres aditivos. Sin embargo, definimos el concepto de una suma Gaussiana de forma general, la cual involucra a los caracteres multiplicativos. Sean ψ un caracter multiplicativo y χ un caracter aditivo de $\mathbb{F}_d$. La suma Gaussiana $G(\psi,\chi)$ se define como

$$G(\psi,\chi)=\sum_{c\in\mathbb{F}_d^*}\psi(c)\chi(c). \tag{A.25}$$

Las sumas Gaussianas satisfacen las siguientes propiedades en cuanto a los posibles valores que pueden tomar.

Teorema 13. *Sean ψ y χ caracteres multiplicativos y aditivos de $\mathbb{F}_d$ respectivamente. Entonces la suma Gaussiana satisface*

$$G(\psi,\chi)=\begin{cases} d-1 & \text{para } \psi=\psi_0,\chi=\chi_0,\\ -1 & \text{para } \psi=\psi_0,\chi\neq\chi_0,\\ 0 & \text{para } \psi\neq\psi_0,\chi=\chi_0,\end{cases} \tag{A.26}$$

y además, si $\psi\neq\psi$ y $\chi\neq\chi_0$, entonces

$$|G(\psi,\chi)|=\sqrt{d}. \tag{A.27}$$

El teorema anterior es fundamental en muchas de las pruebas de las construcciones de MUBs que investigamos ya que por definición del producto interno del espacio de Hilbert $\mathcal{H}$, el producto interno de dos elementos se expresa en términos de sumas exponenciales. En nuestro trabajo no hicimos uso explícito de éstos resultados ya que nos apoyamos en los teoremas de Kanat y de Bandyophyay et al.

Otro tipo de sumas exponenciales importante para éste trabajo son las sumas de caracteres con argumentos polinomiales.

Definición 40. *Sea χ un caracter aditivo no trivial de $\mathbb{F}_d$ y sea $f\in\mathbb{F}_d[x]$ un polinomio de grado positivo. La suma de la forma*

$$\sum_{c\in\mathbb{F}_d}\chi\left(f(c)\right), \tag{A.28}$$

se conoce como una suma de Weil.

Como mencionamos en el capítulo anterior, la evaluación de éstas sumas generalmente es dificil. En ciertos casos es posible tratar con éstas sumas de manera directa, por ejemplo para polinomios lineales tenemos el siguiente resultado.

Teorema 14. *Si χ es un caracter aditivo no trivial de $\mathbb{F}_d$ y $\gcd(n,d-1)=1$, entonces*

$$\sum_{c\in\mathbb{F}_d}\chi\left(ac^n+b\right)=0, \tag{A.29}$$

para todo $a,b\in\mathbb{F}_d$ con $a\neq 0$.

Para el siguiente caso particular necesitamos el concepto de un p-polinomio afín. Un polinomio de la forma

$$L(x)=\sum_{i=0}^{n}\alpha_i x^{p^i}, \tag{A.30}$$

con coeficientes en la extensión de campos $\mathbb{F}_{p^n}$ de $\mathbb{F}_p$ se conoce como un p-polinomio sobre $\mathbb{F}_{p^n}$. Un polinomio de la forma $A(x)=L(x)-\alpha$, donde $L(x)$ es un p-polinomio sobre $\mathbb{F}_{p^n}$ y $\alpha\in\mathbb{F}_{p^n}$ se conoce como un p-polinomio afín sobre $\mathbb{F}_{p^n}$.

Teorema 15 (Teorema 5.32 de [49])**.** *Sea $\mathbb{F}_d$ un campo finito de característica p y sea*

$$f(x)=a_r x^{p^r}+a_{r-1}x^{p^{r-1}}+\cdots+a_1x^p+a_0x+a \tag{A.31}$$

un p-polinomio afín sobre $\mathbb{F}_d$. *Además sea* χ_b *con* $b \in \mathbb{F}_d^*$ *un caracter aditivo no trivial de* $\mathbb{F}_d$ *donde*

$$\chi_b(c) = \chi(bc). \tag{A.32}$$

Para simplificar la notación, definamos

$$g(x) = xa_r + x^p a_{r-1}^p + \cdots + x^{p^{r-1}} a_1^{p^{r-1}} + x^{p^r} a_0^{p^r}.$$

Entonces

$$\sum_{c \in \mathbb{F}_d} \chi_b\left(f(c)\right) = \begin{cases} \chi_b(a)d & \text{si } g(b) = 0, \\ 0 & \text{en otro caso.} \end{cases} \tag{A.33}$$

A.2.4. Sistemas compuestos y factorización tensorial

Sabemos que una extensión de Galois $\mathrm{GF}(p^n)$ se puede ver como un espacio vectorial sobre el campo primo $\mathbb{Z}_p$ respecto a la adición del campo. Pero también tiene más estructra, como la multiplicación y las transformaciones de Frobenius. Por ésto, Vourdas [CITE] nota que representar un sistema cuántico con una extensión de Galois de grado n no es lo mismo que representarlo con una suma directa del campo primo.

Sea $|\alpha\rangle$ un base ortonormal de un espacio de Hilbert $\mathcal{H}$ de dimensión p^n, indexada por los elementos de una extensión de Galois. Además sea $\mathcal{H}_p$ un espacio de dimensión p y $|k\rangle$ un base ortonormal de $\mathcal{H}_p$ indexado por los elementos del campo primo $\mathbb{Z}_p$. Utilizando la base natural de la extensión de campo, podemos expresar a cualquier elemento $\alpha \in \mathrm{GF}(p^n)$ como $\alpha = \sum_i \alpha_i \omega^i$, ésto nos da un mapeo biyectivo:

$$\alpha \mapsto (\alpha_0, \ldots, \alpha_{n-1}), \tag{A.34}$$

lo cual induce una correspondencia entre los elementos de la base de $\mathcal{H}$ y $\mathcal{H}_p$:

$$|\alpha\rangle = |\alpha_0 + \alpha_1\omega + \ldots + \alpha_{n-1}\omega^{n-1}\rangle \mapsto |\alpha_0\rangle \otimes |\alpha_1\rangle \otimes \cdots \otimes |\alpha_{n-1}\rangle, \tag{A.35}$$

la cual a su vez nos da una correspondencia entre los espacios de Hilbert $\mathcal{H}$ y $\mathcal{H}_p \otimes \cdots \otimes \mathcal{H}_p$. Notemos que la correspondencia depende de la elección de base del campo, por lo que la construcción de otros objetos por medio del producto tensorial también serán afectados. Por ejemplo los operadores de desplazamiento que actuán sobre el espacio de Hilbert de dimensión p^n pueden ser expresados en términos de productos tensoriales de operadores de desplazamiento en los subsistemas. El mapeo(A.34) nos permite hacer ésto como:

$$D(\alpha, \beta) = D(\alpha_0, \beta_0) \otimes \cdots \otimes D(\alpha_{n-1}, \beta_{n-1}), \tag{A.36}$$

donde α_i son los componentes de α en la base elegida, y β_i son los componentes respecto a la base dual, y los operadores $D(\alpha_i, \beta_i)$ son los operadores de desplazamiento actuando sobre los subsistemas $\mathcal{H}_p$.

A.3. Anillos de Galois

En la construcción de las MUBs para campos finitos de característica par fue necesario 'salirnos' del campo y hacer operaciones en el *anillo de Galois*. Aquí enunciamos varios de las definiciones y resultados que se utilizan para tal construcción. La teoría de anillos de Galois fue desarrollada por W. Krull en 1924.

Definición 41. *Un anillo de Galois se define como un anillo finito con identidad* 1 *tal que el conjunto de sus divisores de 0, más el 0, forma un ideal principal* $\langle p \cdot 1 \rangle$ *para algún primo* p.

Ejemplo 15. *Consideremos el anillo* $\mathbb{Z}_{p^s}$ *donde* p *es un número primo y* s *es un entero primo. Identificamos a* $n \cdot 1$ *con* n *para todo* $n \in \mathbb{Z}_{p^n}$. *El conjunto de divisores de 0 más el 0 forma el ideal principal* $\langle p \rangle$. *Por lo tanto* $\mathbb{Z}_{p^s}$ *es un anillo de Galois de* p^s *elementos. Cuando* $s = 1$, $\mathbb{Z}_{p^s} = \mathbb{F}_p$ *es el campo de* p *elementos y* $\langle p \rangle = \langle 0 \rangle$.

Ejemplo 16. *Sea* $h(x)$ *un polinomio irreducible básico mónico de grado* m *en* $\mathbb{Z}_{p^s}[x]$. *Ahora consideremos el anillo de clases residuales*

$$\mathbb{Z}_{p^s}[x]/\langle h(x) \rangle.$$

La clase residual

$$a_0 + a_1 x + \cdots + a_{m-1} x^{m-1} + \langle h(x) \rangle,$$

donde $a_0, a_1, \ldots, a_{m-1} \in \mathbb{Z}_{p^s}$ *son distintos elementos de* $\mathbb{Z}_{p^s}[x]/\langle h(x) \rangle$. *El orden de éste anillo es* p^{sm}. *El elemento* $1 + \langle h(x) \rangle$ *es la identidad multiplicativa de* $\mathbb{Z}_{p^s}[x]/\langle h(x) \rangle$ *y* $\langle h(x) \rangle$ *es el cero, por lo tanto dicho anillo es un anillo conmutativo con uno. Todos los elementos del ideal principal* $\langle p + \langle h(x) \rangle \rangle$ *son divisores del cero o son cero. Ésto demuestra que* $\mathbb{Z}_{p^s}[x]/\langle h(x) \rangle$ *es un anillo de Galois.*

Ahora consideremos $\xi = x + \langle h(x) \rangle$. *Entonces* $h(\xi) = 0$ *y*

$$a_0 + \cdots + a_{m-1} x^{m-1} + \langle h(x) \rangle = a_0 + a_1 \xi + \cdots + a_{m-1} \xi^{m-1}.$$

Por lo tanto

$$\mathbb{Z}_{p^s}[x]/\langle h(x) \rangle = \mathbb{Z}_{p^s}[\xi],$$

y todos los elementos del anillo de Galois pueden ser representados por las potencias de ξ. *Ésta representación se conoce como la representación aditiva de los elementos del anillo de Galois* $\mathbb{Z}_{p^s}[\xi]$.

Definición 42. *Para un anillo conmutativo con identidad* 1, *el orden de* 1 *en el grupo aditivo del anillo se llama la característica del anillo.*

Conmunmente denotamos al anillo de Galois $\mathbb{Z}_{p^s}[x]/\langle h(x) \rangle$ donde $h(x)$ es un polinomio básico irreducible sobre $\mathbb{Z}_{p^s}$ de grado m, por

$$\mathrm{GR}(p^s, p^{sm}),$$

donde p^s es la característica y p^{sm} su cardinalidad. Los elementos de un anillo de Galois pueden ser representados en términos de combinaciones polinomiales de un subgrupo particular de la extensión de anillos.

Teorema 16. *En el anillo de Galois* $\mathrm{GR}(p^s, p^{sm})$ *existe un elemento no cero* ξ *de orden* $p^m - 1$, *el cual es raíz de un polinomio básico primitivo* $h(x)$ *de grado* m *sobre* $\mathbb{Z}_{p^s}$ *que divide a* $x^{p^m - 1} - 1$ *en* $Z_{p^s}[x]$ *tal que*

$$\mathrm{GR}(p^s, p^{sm}) = \mathbb{Z}_{p^s}[\xi] = \{a_0 + a_1 \xi + \ldots + a_{m-1} \xi^{m-1} : a_i \in \mathbb{Z}_{p^s}\}. \tag{A.37}$$

Sea

$$\mathcal{T} = \{0, 1, \xi, \xi^2, \ldots, \xi^{p^m - 2}\}, \tag{A.38}$$

entonces cualquier elemento $c \in \mathrm{GR}(p^s, p^{sm})$ *puede ser escrito de manera única como*

$$c = a_0 + a_1 p + \cdots a_{s-1} p^{s-1},$$

donde $a_0, a_1, \ldots, a_{s-1} \in \mathcal{T}$.

La representación de un elemento de $\mathrm{GR}(p^s, p^{sm})$ en términos de los elementos de $\mathcal{T}$ se conoce como la *representación p-ádica* del elemento. En particular utilizamos la representación 2-ádica para hacer los cálculos requeridos en la construcción de las MUBs en característica dos. Los detalles de dicha construcción se pueden consultar en el trabajo de Calderbank, Cameron, Kantor y Seidel sobre códigos de Kerdock sobre $\mathbb{Z}_4$ [42].

Bibliografía

[1] Daniel Gottesman. «The Heisenberg Representation of Quantum Computers». En: *Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics* (jul. de 1998).

[2] Scott Aaronson y Daniel Gottesman. «Improved Simulation of Stabilizer Circuits». En: *Physical Review A* 70.5 (30 de nov. de 2004), pág. 052328. ISSN: 1050-2947, 1094-1622. DOI: 10.1103/PhysRevA.70.052328. URL: https://link.aps.org/doi/10.1103/PhysRevA.70.052328 (visitado 31-01-2023).

[3] Daniel Gottesman. «Fault-Tolerant Quantum Computation with Higher-Dimensional Systems». En: *Quantum Computing and Quantum Communications*. Ed. por Colin P. Williams. Red. de Gerhard Goos, Juris Hartmanis y Jan van Leeuwen. Vol. 1509. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, págs. 302-313. ISBN: 978-3-540-65514-5 978-3-540-49208-5. DOI: 10.1007/3-540-49208-9_27. URL: http://link.springer.com/10.1007/3-540-49208-9_27 (visitado 31-01-2023).

[4] Mark Howard y col. «Contextuality Supplies the Magic for Quantum Computation». En: *Nature 510* (oct. de 2014).

[5] A. Mari y J. Eisert. «Positive Wigner Functions Render Classical Simulation of Quantum Computation Efficient». En: *Physical Review Letters* 109.23 (4 de dic. de 2012), pág. 230503. ISSN: 0031-9007, 1079-7114. DOI: 10.1103/PhysRevLett.109.230503. URL: https://link.aps.org/doi/10.1103/PhysRevLett.109.230503 (visitado 31-01-2023).

[6] K Wootters. «A Wigner-Function Formulation of Finite-State Quantum Mechanics». En: *Annals of Physics* 176.1 (mayo de 1987), págs. 1-21.

[7] D. Gross. «Hudson's Theorem for Finite-Dimensional Quantum Systems». En: *Journal of Mathematical Physics* 47.12 (dic. de 2006), pág. 122107. ISSN: 0022-2488, 1089-7658. DOI: 10.1063/1.2393152. arXiv: quant-ph/0602001. URL: http://arxiv.org/abs/quant-ph/0602001 (visitado 22-05-2023).

[8] Ernesto F. Galvão. «Discrete Wigner Functions and Quantum Computational Speedup». En: *Physical Review A* 71.4 (1 de abr. de 2005), pág. 042302. ISSN: 1050-2947, 1094-1622. DOI: 10.1103/PhysRevA.71.042302. URL: https://link.aps.org/doi/10.1103/PhysRevA.71.042302 (visitado 31-01-2023).

[9] Cecilia Cormick y Juan Pablo Paz. «Interference in Discrete Wigner Functions». En: *Physical Review A* 74.6 (22 de dic. de 2006), pág. 062315. ISSN: 1050-2947, 1094-1622. DOI: 10.1103/PhysRevA.74.062315. URL: https://link.aps.org/doi/10.1103/PhysRevA.74.062315 (visitado 31-01-2023).

[10] Demosthenes Ellinas y Anthony J. Bracken. «Phase-Space-Region Operators and the Wigner Function: Geometric Constructions and Tomography». En: *Physical Review A* 78.5 (7 de nov. de 2008), pág. 052106. ISSN: 1050-2947, 1094-1622. DOI: 10.1103/PhysRevA.78.052106. URL: https://link.aps.org/doi/10.1103/PhysRevA.78.052106 (visitado 22-05-2023).

[11] Brian C. Hall. *Quantum Theory for Mathematicians*. Vol. 267. Graduate Texts in Mathematics. New York, NY: Springer New York, 2013. ISBN: 978-1-4614-7115-8 978-1-4614-7116-5. DOI: 10.1007/978-1-4614-7116-5. URL: https://link.springer.com/10.1007/978-1-4614-7116-5 (visitado 10-02-2023).

[12] Antoine Royer. «Measurement of Quantum States and the Wigner Function». En: *Foundations of Physics* 19.1 (ene. de 1989), págs. 3-32. ISSN: 0015-9018, 1572-9516. DOI: 10.1007/BF00737764. URL: http://link.springer.com/10.1007/BF00737764 (visitado 22-05-2023).

[13] Kanat Abdukhalikov. «Symplectic Spreads, Planar Functions and Mutually Unbiased Bases». En: *Journal of Algebraic Combinatorics* 41.4 (jun. de 2015), págs. 1055-1077. ISSN: 0925-9899, 1572-9192. DOI: 10.1007/s10801-014-0565-y. arXiv: 1306.3478 [cs, math]. URL: http://arxiv.org/abs/1306.3478 (visitado 22-05-2023).

[14] William K. Wootters y Briand D. Fields. «Optimal State-Determination by Mutually Unbiased Measurements». En: *Annals of Physics* 191 (1989).

[15] W. K. Kantor. «MUBs Inequivalence and Affine Planes». En: *Journal of Mathematical Physics* 53.3 (mar. de 2012), pág. 032204. ISSN: 0022-2488, 1089-7658. DOI: 10.1063/1.3690050. arXiv: 1104.3370 [quant-ph]. URL: http://arxiv.org/abs/1104.3370 (visitado 22-05-2023).

[16] Gerald B. Folland. *Harmonic Analysis in Phase Space*. Princeton University Press, 1989.

[17] E. Wigner. «On the Quantum Correction For Thermodynamic Equilibrium». En: *Physical Review* 40.5 (1 de jun. de 1932), págs. 749-759. ISSN: 0031-899X. DOI: 10.1103/PhysRev.40.749. URL: https://link.aps.org/doi/10.1103/PhysRev.40.749 (visitado 10-02-2023).

[18] Maurice A. de Gosson. *Quantum Harmonic Analysis*. Advances in Analysis and Geometry 4. Boston: De Gruyter, 2021. ISBN: 978-3-11-072261-1.

[19] Thomas L. Curtright y Cosmas K. Zachos. «Quantum Mechanics in Phase Space». En: *Asia Pacific Physics Newsletter* 01.01 (mayo de 2012), págs. 37-46. ISSN: 2251-158X, 2251-1598. DOI: 10.1142/S2251158X12000069. arXiv: 1104.5269 [physics, physics:quant-ph]. URL: http://arxiv.org/abs/1104.5269 (visitado 10-02-2023).

[20] Cosmas Zachos, David Fairlie y Thomas Curtright, eds. *Quantum Mechanics in Phase Space: An Overview with Selected Papers*. World Scientific Series in 20th Century Physics v. 34. New Jersey ; London: World Scientific, 2005. 551 págs. ISBN: 978-981-238-384-6.

[21] J. E. Moyal. «Quantum Mechanics as a Statistical Theory». En: *Mathematical Proceedings of the Cambridge Philosophical Society* 45.1 (ene. de 1949), págs. 99-124. ISSN: 0305-0041, 1469-8064. DOI: 10.1017/S0305004100000487. URL: https://www.cambridge.org/core/product/identifier/S0305004100000487/type/journal_article (visitado 10-02-2023).

[22] H J Groenewold. «On the Principles of Elementary Quantum Mechanics». En: ().

[23] Maurice A. De Gosson. *Symplectic Methods in Harmonic Analysis and in Mathematical Physics*. Basel: Springer Basel, 2011. ISBN: 978-3-7643-9991-7 978-3-7643-9992-4. DOI: 10.1007/978-3-7643-9992-4. URL: https://link.springer.com/10.1007/978-3-7643-9992-4 (visitado 22-05-2023).

[24] Maurice A. De Gosson. «The Weyl Correspondence». En: *Born-Jordan Quantization*. Vol. 182. Cham: Springer International Publishing, 2016, págs. 73-94. ISBN: 978-3-319-27900-8 978-3-319-27902-2. DOI: 10.1007/978-3-319-27902-2_6. URL: http://link.springer.com/10.1007/978-3-319-27902-2_6 (visitado 22-05-2023).

[25] Maurice de Gosson. *The Wigner Transform*. Advanced Textbooks in Mathematics. New Jersey: World Scientific, 2017. 229 págs. ISBN: 978-1-78634-308-6 978-1-78634-309-3.

[26] Benjamin Cahen. «Stratonovich-Weyl Correspondence via Berezin Quantization». En: ().

[27] A. Ibort y col. «An Introduction to the Tomographic Picture of Quantum Mechanics». En: *Physica Scripta* 79.6 (jun. de 2009), pág. 065013. ISSN: 0031-8949, 1402-4896. DOI: 10.1088/0031-8949/79/06/065013. arXiv: 0904.4439 [quant-ph]. URL: http://arxiv.org/abs/0904.4439 (visitado 16-06-2023).

[28] Maurice de Gosson. *A Few Almost Trivial Notes on the Symplectic Radon Transform and the Tomographic Picture of Quantum Mechanics*. 31 de mar. de 2022. arXiv: 2203.17210 [math-ph, physics:quant-ph]. URL: http://arxiv.org/abs/2203.17210 (visitado 16-06-2023). preprint.

[29] David Gross. «Finite Phase Space Methods in Quantum Information». Universität Potsdam, 2005.

[30] A B Klimov y C Muñoz. «Discrete Wigner Function Dynamics». En: *Journal of Optics B: Quantum and Semiclassical Optics* 7.12 (1 de dic. de 2005), S588-S600. ISSN: 1464-4266, 1741-3575. DOI: 10.1088/1464-4266/7/12/022. URL: https://iopscience.iop.org/article/10.1088/1464-4266/7/12/022 (visitado 22-05-2023).

[31] Juan Pablo Paz. «Qubits in Phase Space». En: ().

[32] A Vourdas. «Galois Quantum Systems». En: *Journal of Physics A: Mathematical and General* 38.39 (30 de sep. de 2005), págs. 8453-8471. ISSN: 0305-4470, 1361-6447. DOI: 10.1088/0305-4470/38/39/011. URL: https://iopscience.iop.org/article/10.1088/0305-4470/38/39/011 (visitado 22-05-2023).

[33] Kathleen S. Gibbons, Matthew J. Hoffman y William K. Wootters. «Discrete Phase Space Based on Finite Fields». En: *Physical Review A* 70.6 (3 de dic. de 2004), pág. 062101. ISSN: 1050-2947, 1094-1622. DOI: 10.1103/PhysRevA.70.062101. URL: https://link.aps.org/doi/10.1103/PhysRevA.70.062101 (visitado 31-01-2023).

[34] Gunnar Björk, Andrei B. Klimov y Luis L. Sánchez-Soto. «Chapter 7 The Discrete Wigner Function». En: *Progress in Optics*. Vol. 51. Elsevier, 2008, págs. 469-516. ISBN: 978-0-444-53211-4. DOI: 10.1016/S0079-6638(07)51007-3. URL: https://linkinghub.elsevier.com/retrieve/pii/S0079663807510073 (visitado 22-05-2023).

[35] Somshubhro Bandyopadhyay y col. *A New Proof for the Existence of Mutually Unbiased Bases*. 7 de sep. de 2001. arXiv: quant-ph/0103162. URL: http://arxiv.org/abs/quant-ph/0103162 (visitado 22-05-2023). preprint.

[36] Chris Godsil y Aidan Roy. «Equiangular Lines, Mutually Unbiased Bases, and Spin Models». En: *European Journal of Combinatorics* 30.1 (ene. de 2009), págs. 246-262. ISSN: 01956698. DOI: 10.1016/j.ejc.2008.01.002. arXiv: quant-ph/0511004. URL: http://arxiv.org/abs/quant-ph/0511004 (visitado 22-05-2023).

[37] Andreas Klappenecker y Martin Roetteler. «Mutually Unbiased Bases, Spherical Designs, and Frames». En: Optics & Photonics 2005. Ed. por Manos Papadakis, Andrew F. Laine y Michael A. Unser. San Diego, California, USA, 18 de ago. de 2005, 59140P. DOI: 10.1117/12.615759. URL: http://proceedings.spiedigitallibrary.org/proceeding.aspx?doi=10.1117/12.615759 (visitado 22-05-2023).

[38] Peter Dembowski. *Finite Geometries*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1968. ISBN: 978-3-540-61786-0 978-3-642-62012-6. DOI: 10.1007/978-3-642-62012-6. URL: http://link.springer.com/10.1007/978-3-642-62012-6 (visitado 29-06-2023).

[39] P. Oscar Boykin y col. *Mutually Unbiased Bases and Orthogonal Decompositions of Lie Algebras*. 10 de jun. de 2005. arXiv: quant-ph/0506089. URL: http://arxiv.org/abs/quant-ph/0506089 (visitado 22-05-2023). preprint.

[40] William M. Kantor. «Note on Lie Algebras, Finite Groups and Finite Geometries». En: *Groups, Difference Sets, and the Monster*. Ed. por K.T. Arasu y col. DE GRUYTER, 31 de dic. de 1996, págs. 73-82. ISBN: 978-3-11-014791-9. DOI: 10.1515/9783110893106.73. URL: https://www.degruyter.com/document/doi/10.1515/9783110893106.73/html (visitado 22-05-2023).

[41] William M. Kantor. «Spreads, Translation Planes and Kerdock Sets. I». En: *SIAM Journal on Algebraic Discrete Methods* 3.2 (jun. de 1982), págs. 151-165. ISSN: 0196-5212, 2168-345X. DOI: 10.1137/0603015. URL: https://epubs.siam.org/doi/10.1137/0603015 (visitado 22-05-2023).

[42] A R Calderbank y col. «Z_4-Kerdock Codes, Orthogonal Spreads, and Extremal Euclidean Line-Sets». En: *London Mathematical Society* (1997). DOI: 10.1112/S0024611597000403.

[43] Rudolf Lidl y Harald Niederreiter. *Introduction to Finite Fields and Their Applications*. 2.ª ed. Cambridge University Press, 21 de jul. de 1994. ISBN: 978-0-521-46094-1 978-1-139-17276-9. DOI: 10.1017/CBO9781139172769. URL: https://www.cambridge.org/core/product/identifier/9781139172769/type/book (visitado 22-05-2023).

[44] William M. Kantor. «Commutative Semifields and Symplectic Spreads». En: *Journal of Algebra* 270.1 (dic. de 2003), págs. 96-114. ISSN: 00218693. DOI: 10.1016/S0021-8693(03)00411-3. URL: https://linkinghub.elsevier.com/retrieve/pii/S0021869303004113 (visitado 22-05-2023).

[45] D N Ivanov. «Orthogonal Decompositions of Lie Algebras of Type A_{p^n-1} and Isotropic Fiberings». En: *Russian Mathematical Surveys* 42.4 (31 de ago. de 1987), págs. 141-142. ISSN: 0036-0279, 1468-4829.

[46] Andrés García y Pablo Carlos López. «Unextendible Sets of Mutually Unbiased Basis Obtained from Complete Subgraphs». En: *Mathematics* 9.12 (15 de jun. de 2021), pág. 1388. ISSN: 2227-7390. DOI: 10.3390/math9121388. URL: https://www.mdpi.com/2227-7390/9/12/1388 (visitado 29-06-2023).

[47] Andrew McInerney. *First Steps in Differential Geometry: Riemannian, Contact, Symplectic*. Undergraduate Texts in Mathematics. New York: Springer, 2013. 410 págs. ISBN: 978-1-4614-7731-0.

[48] Z.X. Wan. *Lectures on Finite Fields and Galois Rings*.

[49] Rudolf Lidl y Harald Niederreiter. *Finite Fields*. 2nd ed. Encyclopedia of Mathematics and Its Applications v. 20. Cambridge ; New York: Cambridge University Press, 1997. 755 págs. ISBN: 978-0-521-39231-0.