CIMAT Centro de Investigación en Matemáticas, A.C.

APLICACIONES DE PROBABILIDAD LIBRE A LA TEORÍA DE INFORMACIÓN CUÁNTICA

T E S I S

Que para obtener el grado de

Maestro en Ciencias

con Orientación en

Probabilidad y Estadística

Presenta

Saúl Rogelio Mendoza Jacobo

Directores de Tesis:

Dr. Octavio Arizmendi Echegaray

Dr. Carlos Vargas Obieta

Autorización de la versión final

Guanajuato, Gto., diciembre de 2019

A mi esposa

Rosario

Agradecimientos

Quiero empezar estas líneas agradeciendo de manera general a mi familia, compañeros y amigos por su invaluable apoyo.

En particular, agradezco a mi abuelo Saúl Jacobo, a mis hermanos Héctor y Jireh y a mi madre Gabriela, que con su admiración me mantienen motivado a no defraudarlos. Gracias, en especial, a mi esposa Rosario, que me acompaña en las malas y en las peores, y siempre con un "¿qué haremos?", en vez de un "¿qué harás?". A mi hija Arantxa, porque siempre comprendió y mantuvo una sonrisa cuando no podía llevarla al parque porque estaba realizando esta tesis.

Estoy muy agradecido con mis asesores Octavio y Carlos, por su confianza, apoyo y paciencia, y por el gran número de horas que me dedicaron en la realización de este trabajo. Me queda claro que el apoyo que me dieron va más allá de la asesoría típica y por ello, los considero también mis amigos.

Agradezco a los profesores de CIMAT por ser excelentes docentes y personas y haber influido tanto en mis cambios positivos. En particular, estoy agradecido con Joaquín Ortega, Víctor Perez-Abreu, Miguel Nakamura, José Luis Perez y mis asesores, que me inspiran a ser mejor académico y profesionista. Gracias a mis profesores de inglés y amigos Janet Izzo y Sigifredo Aguilar por confiar en mi y brindarme su amistad. También a los amigos que hice en la maestría y que marcaron mi vida: Juan Daniel, Robert, Chelo, Gil y Kenyi.

Finalmente agradezco a mis sinodales Stephen Sontz y Camille Male por el tiempo que dedicaron a la revisión de este trabajo y por sus valiosos comentarios. A Camille, en particular, le agradezco el tiempo en que pudimos compartir y comentar detalles teóricos del capítulo 3. Gracias a CIMAT y CONACyT por los apoyos y las becas que me otorgaron durante mi maestría y así, permitir que me dedicara de tiempo completo a estudiar.

Resumen

El entrelazamiento es un fenómeno físico que surge de la interacción de sistemas cuánticos. Matemáticamente, la información probabilística de cada sistema cuántico individual está representada por una matriz llamada *estado*; a su vez el sistema cuántico conjunto está representado por una matriz que podemos pensar como una matriz a bloques (por ser combinación lineal de producto tensorial de matrices). En este marco, aparecen de manera natural las matrices aleatorias a bloques al considerar estados aleatorios en el sistema compuesto.

La importancia de la detección del entrelazamiento cuántico surge de la teoría de información cuántica como recurso de transmisión de bits y qubits (unidades de información), y los criterios existentes para detectarlo están en términos de mediciones parciales en estados, es decir, funciones aplicadas a los bloques de la matriz estado del sistema compuesto. Más aún, los criterios sólo dependen del espectro de las matrices modificadas a bloques (los estados después de las mediciones parciales).

El análisis del espectro de matrices modificadas a bloques (y por tanto del problema de detección de entrelazamiento en estados aleatorios compuestos), requiere el uso de la teoría de probabilidad libre valuada en operadores para su estudio, ya que la teoría de matrices aleatorias clásica no brinda soluciones para este tipo de matrices.

En el presente trabajo se motiva y expone de manera detallada el problema de detección de entrelazamiento y su importancia en la teoría de información cuántica y se enlistan los trabajos existentes en matrices aleatorias que brindan soluciones parciales al mismo. Se presenta, además, la solución general de este problema usando la teoría de probabilidad libre valuada en operadores.

Palabras Clave: Entrelazamiento, Cuántica, Protocolo de Información, Probabilidad Libre, Matrices Aleatorias.

Contenido

Introducción

La mecánica cuántica surgió a principios del siglo XX como una teoría física que explica el comportamiento de la materia a escalas microscópicas, a velocidades pequeñas respecto a la de la luz; con su formulación vinieron también resultados contraintuitivos para los científicos de la época, entre ellos la dualidad onda-partícula, la superposición cuántica y la naturaleza no determinística de la materia. Uno de estos fenómenos es el llamado *entrelazamiento cuántico*, observado por Schrödinger[1], y el cuál se refiere a la correlación cuántica que preservan las partículas después de haber tenido interacción. En términos prácticos, si dos sistemas de partículas interactuan y después de dicha interacción se realiza una medición en uno de los sistemas, el acto de medir afectará de manera inmediata al otro sistema, independientemente de la distancia entre ellos (lo cual hace imposible que algo viaje entre los dos sistemas de partículas para crear la comunicación, pues de ser así, se violaría el límite asintótico que impone la velocidad de la luz). En 1935, Einstein, Podolsky y Rosen usaron el entrelazamiento para presentar una aparente paradoja que hizo surgir dudas sobre la completitud de la mecánica cuántica [2], plantearon que alguna variable oculta que no estaban considerando provocaba la correlación antes de la separación de los sistemas. Sin embargo, en 1964 Bell demostró que si hubiera una variable oculta antes de la separación, entonces el sistema cumpliría ciertas desigualdades, las cuales no cumplían muchos sistemas cuánticos, dejando claro que el entrelazamiento cuántico es, de hecho, un fenómeno natural (comprobado después experimentalmente).

La teoría de información cuántica tiene como premisa usar las leyes naturales de la mecánica cuántica para transmitir información, y por su naturaleza el entrelazamiento cuántico es protagonista en muchos protocolos de transmisión de información. La idea es mandar bits o qubits (unidades de información) a través de canales cuánticos o clásicos, usando que el sistema conjunto de emisor y receptor está representado por un estado entrelazado y por tanto las mediciones que se realicen en el espacio del emisor afectan al espacio del receptor, el cual interpreta los cambios en su sistema para obtener un mensaje.

Matemáticamente, los estados del sistema conjunto están representados por matrices a bloques (o producto tensorial de matrices) y por tanto, al considerar estados aleatorios, naturalmente se deben de estudiar matrices aleatorias a bloques. Como mencionamos antes, detectar entrelazamiento hace la diferencia entre transmitir información o no, lo que hace relevantes a los criterios existentes de detección de entrelazamiento, tales como el *criterio de reducción*, *criterio Peres-*

[1] Schrödinger usó la palabra alemana "Verschränkung" para este fenómeno, misma que fue cambiada por Einstein por "spukhafte fernwirkung" cuya traducción puede ser "acción fantasmagórica a distancia".

[2] Véase [48], p.p. 10

Horodecki y los *testigos de entrelazamiento*. Estos últimos dependen únicamente del espectro de la *modificación a bloques* del estado del sistema, es decir, el espectro de la matriz resultante de aplicar una función de dominio y rango matricial a cada uno de los bloques de la matriz estado del sistema compuesto.

Por lo discutido en el párrafo anterior, para resolver el problema de detección de entrelazamiento de estados aleatorios compuestos, se debe estudiar la distribución espectral de las matrices aleatorias modificadas a bloques.

La herramienta para atacar dicho problema, estudiada en esta tesis, es la teoría de probabilidad libre valuada en operadores, la cual surgió en los 90's con el objetivo de estudiar el análogo libre al concepto clásico de independencia con respecto a una esperanza condicional.

Uno de los primeros acercamientos a usar matrices aleatorias en el problema de detección de entrelazamiento lo tuvo Aubrun en [4], donde estudia la transpuesta parcial en estados aleatorios representados por una matriz aleatoria a bloques. Posteriormente, Banica y Nechita en [8] y [7] extienden el estudio a otras aplicaciones parciales en ciertas familias de matrices aleatorias utilizando elementos de la teoría de probabilidad libre.

El presente trabajo está organizado de la siguiente manera. En el primer capítulo se exponen los elementos principales de la física cuántica que sirven para presentar los resultados clásicos de la teoría de transmisión de información cuántica, tales como los qubits, canales cuánticos y los protocolos de información: distribución de claves cuánticas, teleportación cuántica y codificación superdensa. En este mismo, se trata el problema de detección de entrelazamiento y los criterios que existen como solución. Es importante mencionar que aunque ésta es una tesis de matemáticas, el Capítulo 1 no trata de describir estos temas con rigor matemático, si no más bien de plantear las ideas básicas que explican el problema de detección de entrelazamiento cuántico y motivan los capítulos posteriores.

En el Capítulo 2 se consideran los *estados cuánticos aleatorios* y los *canales cuánticos aleatorios*. Para este análisis es necesario el uso de la teoría de matrices aleatorias como herramienta para establecer algunos resultados asintóticos. Se estudian también ciertas medidas de probabilidad inducidas en el conjunto de estados no entrelazados. Lo anterior es una exposición de los resultados de Aubrun en [5].

El tercer capítulo es el más relevante de este trabajo. En él se estudia el trabajo de Arizmendi, Nechita y Vargas ([3]), en donde obtienen la distribución asintótica espectral de matrices modificadas a bloques, para dar solución al problema de detección de entrelazamiento. Para la exposición de sus resultados se estudian las herramientas principales de la probabilidad libre y la probabilidad libre valuada en operadores.

Finalmente, en el Capítulo 4 se enlistan las conclusiones del presente trabajo y los aportes del mismo.

Capítulo 1

Teoría de Información Cuántica

El objetivo de este capítulo es presentar los elementos básicos de la teoría de información cuántica que motivan y delimitan el problema de detección de entrelazamiento. Las referencias principales para este capítulo son [48], [1] y [24].

Comenzamos estableciendo el lenguaje de la mecánica cuántica que nos permite exponer de manera detallada la teoría de información cuántica. La exposición se hace desde el punto de vista de física, ya que, a pesar de ser un trabajo de matemáticas, el objetivo de este capítulo es motivar los elementos que surgen en los capítulos posteriores.

Seguido dicha exposición, motivamos el problema de la detección de entrelazamiento usando como ejemplos los protocolos de información, para finalmente estudiar los criterios existentes para tal detección.

1.1 Preliminares de Mecánica Cuántica

En esta sección se da un breve repaso de algunos elementos básicos de la mecánica cuántica. Se definen la notación de Dirac, los observables y estados. Finalmente se discute el producto tensorial de sistemas cuánticos (en donde surge el entrelazamiento).

Para los fines de este trabajo nos basaremos sólo en los sistemas cuánticos de dimensión finita.

1.1.1 Notación de Dirac

La formulación matemática de la mecánica cuántica para describir un sistema físico tiene como espacio subyacente a un espacio de Hilbert complejo separable $\mathcal{H}$ (llamado el *espacio de estados*). En este trabajo consideraremos sólo el caso de dimensión finita. En dicho espacio, Paul Dirac introdujo la notación de *kets* y *bras* para referirse a los vectores del espacio de Hilbert y sus duales, respectivamente.

Por *Ket* nos referimos a cualquier vector del espacio de estados y se representa como $|\psi\rangle$, para alguna etiqueta ψ y un *Bra* es cualquier elemento del dual $\mathcal{H}^*$.

Notación: Sea $|\psi\rangle \in \mathcal{H}$, entonces denotamos por $\langle\psi|$ al elemento dual asociado a $|\psi\rangle$, i.e., el

único funcional que cumple que

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

donde $\langle\cdot,\cdot\rangle$ es el producto interior del espacio de Hilbert, es decir, evaluar el funcional $\langle\psi|$ en el vector $|\phi\rangle$ nos dá el mismo complejo que hacer el producto interior de $|\psi\rangle$ con $|\phi\rangle$.

En adelante, por la observación anterior, se usa $\langle\psi|\phi\rangle$ para denotar el producto interior de $|\psi\rangle$ y $|\phi\rangle$.

Observación 1.1. La notación de los bras y kets es muy conveniente para usos en física, ya que la etiqueta "ψ" no tiene un contexto definido, podría usarse por ejemplo, $|$arriba$\rangle$ y $|$abajo$\rangle$ para denotar los estados del spin de un electrón, como también podría ser $|\uparrow\rangle$ y $|\downarrow\rangle$, o $|0\rangle$ y $|1\rangle$, etc.

Observación 1.2. Una operación que podemos definir para $T \in \mathcal{H}^*$ y $x \in \mathcal{H}$ es $xT : \mathcal{H} \to \mathcal{H}$ dada por

$$(xT)(v) = T(v)x.$$

Es decir, xT le asigna a v el vector x multiplicado por el complejo $T(v)$. En notación de Bras y Kets, eso se ve como

$$|\phi\rangle\langle\psi|,$$

y denota la misma operación. Usaremos esta notación en adelante.

Ejemplo 1.1. Si tomamos el espacio $\mathcal{H} = \mathbb{C}^3$ con el producto estándar, tenemos que $|\phi\rangle \in \mathcal{H}$ es de la forma

$$|\phi\rangle = \begin{pmatrix}\alpha\\ \beta\\ \gamma\end{pmatrix}$$

para algunos $\alpha, \beta, \gamma \in \mathbb{C}$ y $\langle\phi| = [\alpha, \beta, \gamma] \in \mathcal{H}^*$ (bajo el isomorfismo natural). Y por tanto, si $|\psi\rangle = [a, b, c]^T \in \mathcal{H}$, entonces

$$\langle\phi|\psi\rangle = [\alpha, \beta, \gamma]\begin{pmatrix}a\\ b\\ c\end{pmatrix} = \alpha a + \beta b + \gamma c = \begin{pmatrix}\alpha\\ \beta\\ \gamma\end{pmatrix} \cdot \begin{pmatrix}a\\ b\\ c\end{pmatrix}.$$

En este caso $|\phi\rangle\langle\psi|$ es la operación $L_A : \mathbb{C}^3 \to \mathbb{C}^3$, $L_A(x) = Ax$, donde A es la matriz

$$A = \begin{pmatrix}\alpha\\ \beta\\ \gamma\end{pmatrix}(a, b, c) = \begin{pmatrix}\alpha a & \alpha b & \alpha c\\ \beta a & \beta b & \beta c\\ \gamma a & \gamma b & \gamma c\end{pmatrix}.$$

Observación 1.3. Sean $\{|\psi_i\rangle\}_{i\in I}$ y $\{|\phi_i\rangle\}_{i\in I}$ dos bases ortonormales de nuestro espacio $\mathcal{H}$.

1. Se cumple que $\sum_{i\in I} |\psi_i\rangle\langle\psi_i| = Id = \sum_{i\in I} |\phi_i\rangle\langle\phi_i|$ y $\langle a|a\rangle = \sum_{i\in I} |\langle\psi_i|a\rangle|^2$.
2. El operador $A = \sum_{i\in I} |\psi_i\rangle\langle\phi_i|$, es la transformación *basis-flip*, i.e, si $|a\rangle$ está expresado en la

base $\{|\phi_i\rangle\}$ como $|a\rangle = \sum_{i\in I} \alpha_i|\phi_i\rangle$, entonces $A|a\rangle$ nos devuelve un vector $|b\rangle$ que expresado en la base $\{|\psi_i\rangle\}$ es $|b\rangle = \sum_{i\in I} \alpha_i|\psi_i\rangle$.

Definición 1.1. Una *medición proyectiva* en $\mathcal{H}$ es una familia $\{\Pi_i\}_{i\in I}$, $\Pi_i : \mathcal{H} \to \mathcal{H}$ que cumple,

$$\sum_{i\in I} \Pi_i = Id,$$
$$\Pi_i\Pi_j = \delta_{ij}\Pi_i = \delta_{ij}\Pi_i^*.$$

Si J es un operador hermitiano en $\mathcal{H}$, con eigenvalores $\{\lambda_i\}_{i\in I}$ y Π_i la proyección $\Pi_i : \mathcal{H} \to E_{\lambda_i}$, donde E_{λ_i} es el eigenespacio asociado a λ_i, entonces $\{\Pi_i\}$ es una medición proyectiva; esto se sigue de la descomposición,

$$\mathcal{H} = \bigoplus_i E_{\lambda_i}.$$

Se cumple además que $J = \sum_{i\in I} \lambda_i\Pi_i$. Llamaremos a esta medición proyectiva *la resolución de la identidad de* J.

1.1.2 Estados, Mediciones y Observables

La definición de estado puro está basada en el primer postulado de la mecánica cuántica.

Definición 1.2. Sea $\mathcal{H}$ un espacio de estados. Un *estado puro* es cualquier vector de norma uno $|\psi\rangle \in \mathcal{H}$ con la identificación $|\psi\rangle \sim |\phi\rangle$ si $|\phi\rangle = e^{i\theta}|\psi\rangle$, es decir, la clase de equivalencia asociada a dicha relación. En caso de que $|\psi\rangle \sim |\phi\rangle$, se dice que los vectores representan el mismo estado físico.

Observación 1.4. En este trabajo, también llamaremos a las proyecciones de rango uno, de la forma $|\psi\rangle\langle\psi|$ con $|\psi\rangle$ unitario, un estado puro (ver Observación 1.13). Notemos que dichas proyecciones coinciden para todos los representantes de una misma clase de equivalencia según la definición anterior.

En mecánica clásica, los observables son una cantidad o propiedad del estado del sistema, que puede ser medida (observada), mediante una secuencia de operaciones físicas, por ejemplo leer valores en un equipo de medición; dichos observables se representan por funciones $f(x, p)$ que dependen del momento lineal y la posición (el llamado, *espacio de fase clásico*). En cambio en mecánica cuántica, los observables requieren más estructura; la definición de observable cuantico viene del segundo postulado de la mecánica cuántica.

Definición 1.3. Un observable en un espacio de estados $\mathcal{H}$ es cualquier operador hermitiano actuando en $\mathcal{H}$.

El acto de hacer una medición en nuestro espacio de estados está contemplado en el tercer postulado cuántico, que nos dice que los observables sólo pueden tomar valores en su espectro, es

decir, el espectro es su soporte. En el presente trabajo, se consideran sólo observables con espectro finito.

Definición 1.4. Dado un observable A y $|\psi\rangle$ el estado del sistema, se define la esperanza de A por:

$$\langle A\rangle = \langle\psi|A|\psi\rangle.$$

Observación 1.5. Observemos que la bilinealidad del producto interior implica que la esperanza es lineal. Además cumple que

$$\langle I\rangle = \langle\psi|I|\psi\rangle = \langle\psi|\psi\rangle = 1,$$

por ser $|\psi\rangle$ vector unitario.

Presentamos ahora los ejemplos más importantes de espacios de estados para la teoría de información cuántica. Usaremos sus elementos y principales operadores para entender la transmisión de información en los protocolos de la sección 1.3.

Ejemplo 1.2 (Qubit)**.** Un qubit es un elemento de un sistema cuántico de dos niveles, es decir, de un espacio de Hilbert complejo $\mathcal{H}$ de dimensión 2, que sin perdida de generalidad lo tomamos como $\mathbb{C}^2$ con la norma $\|\cdot\|_2$.

Denotamos por $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ y $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$, entonces cualquier $|\psi\rangle \in \mathcal{H}$ es de la forma

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha\begin{pmatrix}1\\0\end{pmatrix} + \beta\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}\alpha\\\beta\end{pmatrix}.$$

Mencionamos antes que dos estados $|\psi\rangle$ y $|\phi\rangle = e^{ai}|\psi\rangle$ representan el mismo sistema físico y los identificamos (vía la relación de equivalencia) como el mismo. Teniendo esto en cuenta es fácil ver que todo estado puede representarse como:

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle,$$

para algunos $0 \leq \theta \leq \pi$ y $0 \leq \varphi < 2\pi$. Es decir, en el caso de qubits, hay una biyección entre estados y puntos en la esfera de radio 1; a esta representación de estados en la esfera, se le llama *la esfera de Bloch*.

Definición 1.5. Consideremos el espacio de un qubit.

1. A la base ortonormal $\{|0\rangle, |1\rangle\}$ se le llama *base computacional*.
2. A la base ortonormal $\{|+\rangle, |-\rangle\}$, donde

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \quad \text{y} \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix},$$

se le llama *base de Hadamard* o base $+/-$.

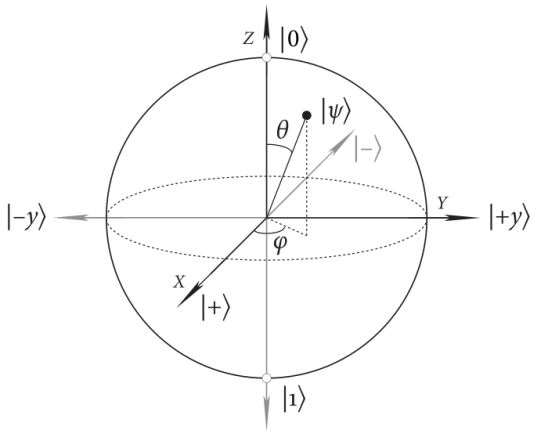


Figura 1.1: Esfera de Bloch

Definimos la transformación *NOT-gate* por $X|0\rangle = |1\rangle$ y $X|1\rangle = |0\rangle$. La representación matricial de X en la base computacional es:

$$\sigma_1 = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

De forma análoga se definen las transformaciones con matrices asociadas

$$\sigma_2 = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \text{y} \quad \sigma_3 = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Definición 1.6. A las matrices σ_i, $i = 1, 2, 3$ se les llama *matrices de Pauli*.

Proposición 1.1. Las matrices de Pauli son hermitianas, unitarias, con eigenvalores ± 1, además conmutan o anticonmutan entre ellas. Se cumple también que $Tr(\sigma_i \sigma_j) = 2\delta_{ij}$ y más aún, $\sigma_i^2 = I$.

Definimos también la operación unitaria de Hadamard, la cual denotaremos por H en los protocolos de información.

Definición 1.7. La transformación H definida como $H|0\rangle = |+\rangle$, $H|1\rangle = |-\rangle$, o bien, como $H = |+\rangle\langle 0| + |-\rangle\langle 1|$ es llamada *transformación de Hadamard*.

Observación 1.6. La matriz representación del operador de Hadamard es

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

y representa una rotación de ángulo π sobre el eje $\frac{\hat{x}+\hat{z}}{\sqrt{2}}$ en la esfera de Bloch.

Ejemplo 1.3 (Qudits)**.** Esta es una generalización del qubit para dimensión d. Como caso particular de los qudits tendremos a los qubits $d = 2$, los qutrits $d = 3$, etc.

Un qudit es un sistema cuántico de d niveles, es decir un espacio de Hilbert complejo de dimensión d, que sin perdida de generalidad podemos tomar como $\mathbb{C}^d$ y $\{|i\rangle\}_{i=0,1,\ldots,d-1}$ la base estándar de $\mathbb{C}^d$. Los estados en este caso son de la forma

$$|\psi\rangle = \sum_{j=0}^{d-1} \alpha_j |j\rangle,$$

con $\sum_{j=0}^{d-1} |\alpha_j|^2 = 1$. Para $x \in \mathbb{N} \cup \{0\}$ definimos el operador de shift cíclico, $X(x)$ como

$$X(x)|j\rangle = |j \oplus x\rangle,$$

suma módulo d. Y también el operador de fase $Z(z)$ como

$$Z(z)|j\rangle = \exp(2\pi i z j/d)|j\rangle$$

A la familia de operadores (d^2 operadores) $\{X(x)Z(z)\}_{x,z\in\{0,1,\ldots,d-1\}}$ se les llama *operadores de Heisenberg-Weyl* y son el análogo a las matrices de Pauli para los Qudits.

Observación 1.7. En mecánica cuántica es de importancia cambiar el estado del sistema $|\psi\rangle$ por $T|\psi\rangle$ pero de tal forma que el resultado siga siendo un estado y que además podamos "devolver" el proceso para regresar a $|\psi\rangle$. Esto funciona para los operadores unitarios ya que

- Los operadores unitarios son invertibles, de hecho $U^* = U^{-1}$ y por tanto nuestra evolución del sistema es reversible si aún no se ha hecho una medición.
- Los operadores unitarios preservan la norma 1; eso nos garantiza que $U|\psi\rangle$ es también un estado cuántico. De hecho los operadores unitarios son los únicos que preservan normas.

Las compuertas X,Y, Z y H y los operadores de Heisenberg-Weyl son ejemplos de operaciones unitarias.

1.1.3 Producto Tensorial y Entrelazamiento

Cuando hacemos el producto tensorial de dos espacios de Hilbert $(\mathcal{H}_1, \langle\cdot|\cdot\rangle_1)$ y $(\mathcal{H}_2, \langle\cdot|\cdot\rangle_2)$, se toma el producto tensorial de espacios vectoriales y se hace la completación del espacio para que toda sucesión de Cauchy converja respecto al producto interior:

$$\langle a \otimes b | c \otimes d\rangle = \langle a|c\rangle_1 \langle b|d\rangle_2.$$

Si T_1 es una transformación lineal en $\mathcal{H}_1$ y T_2 en $\mathcal{H}_2$ entonces se define la transformación $T_1 \otimes T_2$ en el producto tensorial $\mathcal{H}_1 \otimes \mathcal{H}_2$ como

$$T_1 \otimes T_2(v \otimes w) = T_1(v) \otimes T_2(w).$$

Una propiedad importante es que la composición de estas transformaciones cumple que $(T_1 \otimes T_2)(S_1 \otimes S_2) = (T_1 S_1) \otimes (T_2 S_2)$.

Si tomamos los espacios vectoriales $M_n(\mathbb{C})$ y $M_m(\mathbb{C})$, el producto tensorial es $M_n(\mathbb{C}) \otimes M_m(\mathbb{C}) \cong M_{nm}(\mathbb{C})$ (el producto corresponde, de hecho, al producto de Kronecker), por ejemplo en dimensión 4:

$$A \otimes B = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \otimes \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} & a_{12}\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \\ a_{21}\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} & a_{22}\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \end{pmatrix}$$
$$= \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{pmatrix}.$$

Observación 1.8. El espacio dado por el producto tensorial es un nuevo espacio de estados, correspondiente a la interacción de los dos sistemas originales, lo llamaremos *espacio compuesto*.

Establezcamos algo de notación. Si $|\phi\rangle \in \mathcal{H}_A$ y $|\psi\rangle \in \mathcal{H}_B$, entonces $|\phi\psi\rangle$ representa al vector $|\phi\rangle \otimes |\psi\rangle$ en $\mathcal{H}_A \otimes \mathcal{H}_B$. De igual forma, $\langle\phi\psi|$ es el funcional $\langle\phi| \otimes \langle\psi|$.

Así, en el espacio compuesto asociado al producto de dos sistemas de qubits, tenemos la siguiente notación para los elementos base del nuevo espacio $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, que por la identificación $\mathbb{C}^2 \otimes \mathbb{C}^2 \cong \mathbb{C}^4$ podemos expresar como

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix},\ |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},\ |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix},\ |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix};$$

y de hecho un vector general en el espacio compuesto (o producto tensorial) será

$$\alpha|0\rangle \otimes |0\rangle + \beta|0\rangle \otimes |1\rangle + \gamma|1\rangle \otimes |0\rangle + \delta|1\rangle \otimes |1\rangle,$$

o bien,

$$\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle = \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix}.$$

Para finalizar la sección, presentamos la definición de entrelazamiento cuántico para estados puros.

Definición 1.8. Consideremos H_A y H_B dos espacios de estados y su producto tensorial $H = H_A \otimes H_B$.

i) Decimos que $|\eta\rangle \in H$ es *separable* si existen estados $|\psi\rangle_A \in H_A$ y $|\phi\rangle_B \in H_B$ tal que

$$|\eta\rangle = |\psi\rangle_A \otimes |\phi\rangle_B.$$

ii) Diremos que $|\eta\rangle \in H$ es **entrelazado** si no es separable.

Ejemplo 1.4. En el espacio producto de dos sistemas de qubits, consideremos el estado EPR definido como,

$$|\Phi^+\rangle_{AB} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Si suponemos que $|\Phi^+\rangle_{AB}$ es separable, entonces existen $|a\rangle = \alpha|0\rangle + \beta|1\rangle \in H_A$ y $|b\rangle = \gamma|0\rangle + \delta|1\rangle \in H_B$, tal que $|\Phi^+\rangle_{AB} = |a\rangle \otimes |b\rangle$ y por tanto,

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} = |\Phi^+\rangle_{AB} = |a\rangle \otimes |b\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle,$$

o equivalentemente que,

$$\left(\alpha\gamma - \frac{1}{\sqrt{2}}\right)|00\rangle + \left(\beta\delta - \frac{1}{\sqrt{2}}\right)|11\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle = \mathbf{0}.$$

Como los vectores $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ son linealmente independientes, lo anterior implica que,

$$\alpha\gamma = \frac{1}{\sqrt{2}}, \quad \beta\delta = \frac{1}{\sqrt{2}}, \quad \alpha\delta = 0, \quad \text{y} \quad \beta\gamma = 0.$$

De las ecuaciones anteriores se deduce que $\frac{1}{2} = \alpha\beta\gamma\delta = 0$, lo cual es una contradicción. Por lo que el estado EPR es entrelazado.

1.2 Información Cuántica

En esta sección se generaliza la definición de estado y se establecen los elementos suficientes para estudiar los protocolos de información y los criterios de detección de entrelazamiento.

1.2.1 Matrices de Densidad (Estados)

En este espacio compuesto, hay algunas operaciones que podemos aplicar al segundo o primer qubit, "sin afectar" al otro. Hablamos de mediciones parciales.

Definición 1.9. Una *medición parcial* en $\mathcal{H}_A \otimes \mathcal{H}_B$ es una operación de alguno de los siguientes tipos

1. $(I_A \otimes \varphi_1) : \mathcal{H}_A \otimes \mathcal{H}_B \to \mathcal{H}_A \otimes \mathcal{H}_B$,

2. $(\varphi_2 \otimes I_B) : \mathcal{H}_A \otimes \mathcal{H}_B \to \mathcal{H}_A \otimes \mathcal{H}_B$;

donde I_A es la transformación identidad $I_A : \mathcal{H}_A \to \mathcal{H}_A$, I_B es la identidad en $\mathcal{H}_B$, φ_1 una transformación lineal $\varphi : \mathcal{H}_B \to \mathcal{H}_B$ y φ_2 transformación lineal de $\mathcal{H}_A$ a $\mathcal{H}_A$.

Un ejemplo de lo anterior es hacer un *flip* (aplicar X) en el segundo espacio:

$$I_1 \otimes X : \ \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \mapsto \alpha|01\rangle + \beta|00\rangle + \gamma|11\rangle + \delta|10\rangle.$$

Sin embargo, también podemos aplicar la operación X a ambos qubit:

$$X \otimes X : \ \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \mapsto \alpha|11\rangle + \beta|10\rangle + \gamma|01\rangle + \delta|00\rangle.$$

Observación 1.9. También para estos espacios tenemos una representación matricial para las operaciones. Por ejemplo la representación matricial de $X_1 \otimes I_2$ es

$$[X_1 \otimes I_2] = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = [X_1] \otimes [I_2].$$

Lo anterior, de hecho, se cumple en general:

Proposición 1.2. La matriz representación de $X \otimes Y$ es el producto tensorial de las matrices representación de X y Y.

Otra proposición muy útil es la siguiente.

Proposición 1.3. Sea $|\phi_0\rangle, |\phi_1\rangle \in \mathcal{H}_A$ y $|\psi_0\rangle, |\psi_1\rangle \in \mathcal{H}_B$ entonces

$$\langle \phi_1\psi_1|\phi_0\psi_0\rangle = \langle \phi_1|\phi_0\rangle\langle \psi_1|\psi_0\rangle.$$

Definimos ahora otra operación en el producto tensorial que nos será de utilidad en los protocolos de información, la llamada puerta CNOT.

Definición 1.10. La *puerta CNOT* (o Controlled-NOT gate) es la aplicación definida por

$$|00\rangle \to |00\rangle, \ |01\rangle \to |01\rangle, \ |10\rangle \to |11\rangle, \ |11\rangle \to |10\rangle,$$

o bien,

$$\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \overset{\text{CNOT}}{\to} \alpha|00\rangle + \beta|01\rangle + \gamma|11\rangle + \delta|10\rangle.$$

Observación 1.10. Podemos también poner a la puerta CNOT en términos de bras y kets como

$$|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X;$$

y su representación matricial es

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Para entender mejor el entrelazamiento, consideremos que el estado del sistema compuesto es $|0\rangle_A|1\rangle_B$, en este caso podremos decir de manera segura que el estado del sistema $\mathcal{H}_A$ es $|0\rangle_A$ y el de $\mathcal{H}_B$ es $|1\rangle_B$. Sin embargo, como vimos en el ejemplo 1.4, el estado EPR

$$|\Phi^+\rangle_{AB} = \frac{|00\rangle + |11\rangle}{\sqrt{2}},$$

no es separable, por tanto, es un estado que surge de la interacción y no pueden distinguirse los elementos particulares de cada espacio de estados.

Otros estados entrelazados de interés son

$$|\Phi^-\rangle_{AB} = \frac{|00\rangle - |11\rangle}{\sqrt{2}},\ |\Psi^+\rangle_{AB} = \frac{|01\rangle + |10\rangle}{\sqrt{2}},\ |\Psi^-\rangle_{AB} = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

En lo anterior, $|ij\rangle$ representa a $|i\rangle_A|j\rangle_B$, para $i, j \in \{0, 1\}$.

Definición 1.11. A los estados $|\Phi^+\rangle_{AB}, |\Phi^-\rangle_{AB}, |\Psi^+\rangle_{AB}$ y $|\Psi^-\rangle_{AB}$ se les llama *estados de Bell*.

Proposición 1.4. Los estados de Bell forman una base para el sistema compuesto de dos qubits.

En lo siguiente, trabajaremos con exactamente dos sistemas cuánticos H_A y H_B y de algunos elementos correspondientes a su producto tensorial. Usando terminología de libros de información cuántica llamaremos "Alice" a H_A y "Bob" a H_B. Diremos que ellos *comparten un estado* σ_{AB} si σ_{AB} es el estado del sistema compuesto $H_A \otimes H_B$. Este manejo informal de los conceptos se justifica en las aplicaciones, por ejemplo, las mediciones parciales del tipo $I_A \otimes \varphi$ se interpretan como "mediciones que hace sólo Bob", mientras Alice "deja" su sistema intacto.

Si suponemos que Alice y Bob comparten el estado entrelazado $|\Psi^+\rangle_{AB}$ y Bob hace una medición parcial (en su estado) en la que obtiene el valor $|1\rangle$, entonces el nuevo estado del sistema será

$$(I \otimes \langle 1|)|\Psi^+\rangle_{AB}(I \otimes |1\rangle) = |0\rangle \otimes |1\rangle.$$

Si a continuación Alice realiza una medición, por el estado nuevo del sistema, ella obtendrá lo correspondiente al valor $|0\rangle$. Es decir, la medición individual de Bob, en su sistema, afectó al sistema de Alice aún que esté alejado de toda aparente influencia, sólo por compartir un estado entrelazado.

Generalicemos lo anterior, para el caso qudit.

Definición 1.12. Consideremos el espacio compuesto de dos qudits.

i) Definimos el estado máximamente entrelazado como

$$|\Phi\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle_A |i\rangle_B.$$

ii) El vector máximamente entrelazado es

$$|\Gamma\rangle_{AB} = \sum_{i=0}^{d-1} |i\rangle_A |i\rangle_B.$$

iii) A los d^2 operadores

$$|\Phi^{x,z}\rangle_{AB} = (X_A(x) Z_A(z) \otimes I_B)|\Phi\rangle_{AB}, \quad x, z \in \{0, 1, \ldots, d-1\},$$

se les llama estados de Bell.

Observación 1.11. Los estados de Bell forman una base ortonormal para el sistema compuesto.

Teorema 1.1 (Teorema de Schmidt)**.** Supongamos que tenemos un estado puro $|\Psi\rangle_{AB} \in H_A \otimes H_B$, donde H_A, H_B son espacios de Hilbert finito dimensionales, de dimensión d_A y respectivamente d_B. Entonces existen λ_i reales estríctamente positivos, con $\sum_i \lambda_i^2 = 1$ y tal que

$$|\Psi\rangle_{AB} = \sum_{i=0}^{d-1} \lambda_i |i\rangle_A |i\rangle_B,$$

donde $\{|i\rangle_A\}$ es base de H_A y $\{|i\rangle_B\}$ es base de H_B. El valor d es el llamado *rango de Schmidt* y $\{\lambda_i\}_{0 \leq i \leq d-1}$ son los *coeficientes de Schmidt* que cumplen que

$$d \leq \min(d_A, d_B).$$

Demostración. $|\Psi\rangle_{AB}$ está en el producto tensorial, así que lo podemos poner como

$$|\Psi\rangle_{AB} = \sum_{j=0}^{d_A-1} \sum_{k=0}^{d_B-1} \alpha_{j,k} |j\rangle_A |k\rangle_B.$$

Sea $(\alpha_{j,k}) = G = U \Delta V$, donde U unitaria $d_A \times d_A$, V unitaria $d_B \times d_B$ y Δ matriz $d_A \times d_B$ con d números positivos en su diagonal principal (para algún $d \leq d_A, d_B$) y cero en lo demás, esto es posible pues toda matriz tiene su descomposición en valores singulares, como puede verse en [9]; dicho teorema establece que

Resultado: Si M matriz $m \times n$ con entradas complejas [reales],entonces existe una factorización de la forma

$$M = U \Sigma V^*,$$

donde U es matriz de $m \times m$ unitaria [ortogonal], Σ matriz $m \times n$ diagonal con números no negativos en su diagonal y V es matriz de $n \times n$ unitaria [ortogonal].

Se cumple entonces que

$$\alpha_{j,k} = \sum_{i=0}^{d-1} U_{j,i}\lambda_i V_{i,k};$$

sustituyendo en $|\Psi\rangle_{AB}$ tenemos que

$$\begin{aligned}
|\Psi\rangle_{AB} &= \sum_{j=0}^{d_A-1}\sum_{k=0}^{d_B-1}\left(\sum_{i=0}^{d-1} U_{j,i}\lambda_i V_{i,k}\right)|j\rangle_A|k\rangle_B \\
&= \sum_{i=0}^{d-1}\lambda_i \underbrace{\left(\sum_{j=0}^{d_A-1} U_{j,i}|j\rangle_A\right)}_{|i\rangle_A} \otimes \underbrace{\left(\sum_{k=0}^{d_B-1} V_{i,k}|k\rangle_B\right)}_{|i\rangle_B} \\
&= \sum_{i=0}^{d-1}\lambda_i|i\rangle_A|i\rangle_B.
\end{aligned}$$

■

El teorema de Schmidt nos permite caracterizar el entrelazamiento de estados puros como veremos más adelante. Vamos ahora a generalizar la definición de estado.

Definición 1.13. Sea $\mathcal{H}$ un sistema cuántico y $\{|\psi_i\rangle\}_{i\in I}$ un subconjunto de estados de $\mathcal{H}$, con I finito. Consideremos también X una variable aleatoria clásica discreta que tome valores en I y sea P_X su función de masa. Al conjunto:

$$\varepsilon = \{P_X(i), |\psi_i\rangle\}_{i\in I},$$

lo llamamos *ensamble de estados cuánticos*.

Definición 1.14. Para un operador A actuando en $\mathcal{H}$, se define su traza como

$$Tr(A) = \sum_{i\leq d}\langle i|A|i\rangle,$$

donde $\{|i\rangle\}_{i\leq d}$ es cualquier base ortonormal de $\mathcal{H}$.

Sea ahora J un observable y $\{\Pi_j\}$ familia de proyectores de medición de J, también consideremos el ensamble $\{P_X(x), |\psi_x\rangle\}_{x\in\mathcal{X}}$ con $\mathcal{X}$ finito. Observemos que

$$\begin{aligned}\sum_{x\in\mathcal{X}}\langle\psi_x|\Pi_j|\psi_x\rangle P_X(x) &= \sum_{x\in\mathcal{X}} Tr(\pi_j|\psi_x\rangle\langle\psi_x|)P_X(x)\\ &= Tr\Bigg(\Pi_j \underbrace{\sum_{x\in\mathcal{X}} P_X(x)|\psi_x\rangle\langle\psi_x|}_{\rho}\Bigg)\\ &= Tr(\Pi_j\rho).\end{aligned}$$

Lo anterior motiva la siguiente definición.

Definición 1.15. El *operador de densidad* o *matriz de densidad* ρ correspondiente al ensamble $\varepsilon = \{P_X(x), |\psi_x\rangle\}_{x\in\mathcal{X}}$, con $\mathcal{X}$ finito, está definido como

$$\rho = \sum_{x\in\mathcal{X}} P_X(x)|\psi_x\rangle\langle\psi_x|.$$

Teorema 1.2. Los operadores de densidad cumplen que $Tr(\rho) = 1$ y $\rho \geq 0$.

Demostración.

$$\begin{aligned}Tr(\rho) = Tr\left(\sum_{x\in\mathcal{X}} P_X(x)|\psi_x\rangle\langle\psi_x|\right) &= \sum_{x\in\mathcal{X}} P_X(x)Tr(|\psi_x\rangle\langle\psi_x|)\\ = \sum_{x\in\mathcal{X}} P_X(x)\langle\psi_x|\psi_x\rangle = \sum_{x\in\mathcal{X}} P_X(x) &= 1.\end{aligned}$$

Tomemos $|\varphi\rangle$ cualquiera, entonces

$$\begin{aligned}\langle\varphi|\rho|\varphi\rangle &= \langle\varphi|\left(\sum_{x\in\mathcal{X}} P_X(x)|\psi_x\rangle\langle\psi_x|\right)|\varphi\rangle\\ &= \sum_{x\in\mathcal{X}} P_X(x)\langle\varphi|\psi_x\rangle\langle\psi_x|\varphi\rangle = \sum_{x\in\mathcal{X}} P_X(x)|\langle\varphi|\psi_x\rangle|^2 \geq 0.\end{aligned}$$

■

Observación 1.12. Todo ensamble tiene una única matriz de densidad, pero el recíproco no es cierto. De hecho los ensambles

$$\varepsilon_1 = \{\{1/2, |0\rangle\}, \{1/2, |1\rangle\}\} \quad \text{y} \quad \varepsilon_2 = \{\{1/2, |+\rangle\}, \{1/2, |-\rangle\}\},$$

tienen la misma matríz de densidad.

A pesar de lo anterior, dada una matriz ρ que cumpla las condiciones del teorema 1.2 podemos construir un ensamble *canónico* del cual ρ es su matriz de densidad; sea $m = |spec(\rho)|$ y tomemos

$\{\lambda_x, |\phi_x\rangle\}_{x\in\{0,1,\ldots,m-1\}}$ la descomposición espectral de ρ (existe ya que ρ es hermitiano), entonces

$$\rho = \sum_{x=0}^{m-1} \lambda_x |\phi_x\rangle\langle\phi_x|.$$

Además se cumple que $1 = Tr(\rho) = \sum_{x=0}^{m-1} \lambda_x$ y como ρ es positiva semidefinida, entonces $\lambda_x \geq 0$ para todo x, es decir, si definimos la función $P(x) = \lambda_x,\ x \leq m-1$, ésta define una función de masa de probabilidad y por tanto existe una variable aleatoria discreta con valores en $\{0, 1, \ldots, m-1\}$ con función de masa P.

Definición 1.16. En un espacio de Hilbert $\mathcal{H}$ con producto interior $\langle\cdot,\cdot\rangle$, la transformación lineal $T : \mathcal{H} \to \mathcal{H}$ es positiva, y se denota por $T \geq 0$, si se cumple que

$$\langle Tx, x\rangle \geq 0,$$

para todo $x \in \mathcal{H}$.

En el Teorema 12.32 de [38] se establece que un operador T acotado es positivo si y sólo si es autoadjunto y $\sigma(T) \subseteq [0, \infty)$. Más aún, se prueba en el teorema 12.33 que todo operador positivo tiene una única raíz cuadrada. Por lo tanto, existe V acotado tal que $T = V^*V$.

La siguiente definición es central para este trabajo.

Definición 1.17 (Definición General de Estado)**.** Un **estado** de un sistema cuántico $\mathcal{H}$ es un operador $\rho : \mathcal{H} \to \mathcal{H}$, que cumple $\rho \geq 0$ y $Tr(\rho) = 1$.

Denotamos por $D(\mathcal{H}) = \{\rho : \mathcal{H} \to \mathcal{H} : \rho \geq 0, Tr(\rho) = 1\}$, el conjunto de los estados u operadores de densidad; este conjunto es convexo. En efecto, para $t \in (0, 1)$ y sean ρ_1, ρ_2 estados en $\mathcal{H}$, y sea $\rho_t = t\rho_1 + (1-t)\rho_2$, entonces

$$Tr(\rho_t) = tTr(\rho_1) + (1-t)Tr(\rho_2) = t \cdot 1 + (1-t) \cdot 1 = 1,$$

debido a la linealidad de la traza y también se cumple que, para todo $x \in \mathcal{H}$,

$$\langle \rho_t x, x\rangle = t\langle \rho_1 x, x\rangle + (1-t)\langle \rho_2 x, x\rangle \geq 0$$

ya que $\langle \rho_1 x, x\rangle \geq 0, \langle \rho_2 x, x\rangle \geq 0$ y $t \in (0, 1)$. Concluimos que $\rho_t \in D(\mathcal{H})$.

Definición 1.18. Sea C un conjunto convexo. Un elemento $c \in C$ es llamado *extremal* si la igualdad $c = c_1 t + c_2(1-t)$, con $c_1, c_2 \in C$ y $t \in (0, 1)$ implica que $c_1 = c_2 = c$. Se denota por $\partial_e C$ al conjunto de todos los elementos extremales del convexo C.

Lo anterior nos permite definir estados puros.

Definición 1.19. Un estado $\rho \in D(\mathcal{H})$ es un *estado puro* si es un elemento extremal del convexo $D(\mathcal{H})$.

Observación 1.13. Vamos ahora a probar que los estados de la forma $\rho = |\psi\rangle\langle\psi| \in D(\mathcal{H})$, con $|\psi\rangle \in \mathcal{H}$ vector unitario, son estados puros. Sean $\rho_1, \rho_2 \in D(\mathcal{H})$ y $t \in (0,1)$ tal que $\rho = t\rho_1 + (1-t)\rho_2$. Si $\rho_j = \sum_i p_i^{(j)} |v_i^{(j)}\rangle$, con $\{|v_i^{(j)}\rangle\}_i$ base ortonormal de eigenvectores de ρ_j, $j = 1, 2$, entonces se cumple que $p_i^{(j)} \geq 0$ y $\sum_i p_i^{(j)} = 1$, para $j = 1, 2$. También se cumple lo siguiente

$$\langle\psi|\rho_j|\psi\rangle = \sum_i p_i^{(j)} |\langle\psi|v_i^{(j)}\rangle|^2 \leq \sum_i p_i^{(j)} = 1,$$

lo anterior por la desigualdad de Cauchy-Schwarz: $|\langle\psi|v_i^{(j)}\rangle|^2 \leq \||\psi\rangle\|^2 \||v_i^{(j)}\rangle\|^2 = 1$. Ahora bien,

$$1 = \langle\psi|\rho|\psi\rangle = t\langle\psi|\rho_1|\psi\rangle + (1-t)\langle\psi|\rho_2|\psi\rangle \leq t + (1-t) = 1,$$

por lo tanto, para $j = 1, 2$ y los $p_i^{(j)} \neq 0$ se alcanza la igualdad en la desigualdad de Cauchy-Schwarz: $|\langle\psi|v_i^{(j)}\rangle|^2 = 1$, lo cuál sucede sólo si $|\psi\rangle = z_j |v_i^{(j)}\rangle$ para algún $z_j \in \mathbb{C}$ que cumpla $|z_j| = 1$. Sin embargo, por la positividad de los sumandos y lo anterior, sólo existe un $p_i^{(j)} \neq 0$ y por tanto $\rho = |\psi\rangle\langle\psi| = |v_i^{(j)}\rangle$ para $j = 1, 2$, es decir $\rho_1 = \rho_2 = \rho$. Concluimos que ρ es extremal.

Observemos que los estados puros son casos particulares de la matriz de densidad cuando la variable aleatoria X del ensamble asociado toma con probabilidad 1 un sólo valor $x \in I$, es decir, la variable tiene distribución degenerada en x.

Definición 1.20. Sea $\mathcal{H}$ un espacio cuántico de estados.

i) Si un estado ρ no es puro, decimos que es un *estado mixto*.

ii) El *estado máximamente mixto* π es el operador de densidad asociado al ensamble uniforme de estados ortogonales $\{\frac{1}{d}, |x\rangle\}_{0 \leq x \leq d-1}$, donde $1 \leq d = dim(\mathcal{H}) < \infty$, es decir:

$$\pi = \frac{1}{d} \sum_{x=0}^{d-1} |x\rangle\langle x| = \frac{I}{d}.$$

iii) Se define la *pureza* de ρ como

$$P(\rho) = Tr(\rho^* \rho) = Tr(\rho^2).$$

Proposición 1.5. La pureza cumple que $P(\rho) \leq 1$ y se cumple que el estado ρ es puro si y sólo si $P(\rho) = 1$.

Demostración. Observemos que si $\rho = \sum_n \rho_n |\psi_n\rangle\langle\psi_n|$, las propiedades de ρ (del Teorema 1.2) implican que ρ_n real y además $\rho_n \geq 0$, y $\sum_n \rho_n = 1$. Por lo anterior, $0 \leq \rho_n \leq 1$, lo cuál implica que $\rho_n^2 \leq \rho_n$ y en conclusión,

$$Tr(\rho^2) = \sum_n \rho_n^2 \leq \sum_n \rho_n = 1.$$

Más aún, por la desigualdad anterior, si $Tr(\rho^2) = 1$ entonces $\rho_n^2 = \rho_n$ para todo n, lo cuál no ocurre a menos que $\rho_n = 0$ o $\rho_n = 1$. Pero como la suma $\sum_n \rho_n = 1$, concluimos que el hecho $Tr(\rho^2) = 1$ implica que exactamente uno de los ρ_n es igual a 1 y los demás son cero, es decir, es un estado puro. ■

En secciones pasadas, vimos que había una biyección entre estados puros qubit y la esfera de Bloch. Sin embargo ésto es más general, para cada estado (puro o no) existe un punto en la bola unitaria y viceversa; véase en la página 108 de [48] el desarrollo que prueba la siguiente proposición.

Proposición 1.6. Considere el espacio de un qubit. Hay una biyección entre cada vector $r \in \mathbb{R}^3$ tal que $\|r\| \leq 1$ y las matrices de densidad del qubit, a saber:

$$\rho_r = \frac{1}{2}(I + r_x X + r_y Y + r_z Z).$$

Por tanto el origen corresponde al estado máximamente mixto.

Presentamos ahora la definición general de entrelazamiento para estados (mixtos y puros).

Definición 1.21. Consideremos el producto tensorial de dos espacios de estados H_A y H_B, el estado σ_{AB} es separable si se puede poner como

$$\sigma_{AB} = \sum_i p_i \sigma_i^A \otimes \tau_i^B,$$

para algunos estados puros σ_i^A en H_A y τ_i^B en H_B y números p_i, que cumplen que $\sum_i p_i = 1,\ p_i \geq 0$. Si el estado no es separable, decimos que está **entrelazado**.

En los casos en que los espacios de estados son de dimensión finita, la matriz de densidad del espacio compuesto es en efecto una matriz, decimos entonces que $\sigma_{AB} \in M_{d_A d_B}(\mathbb{C})$ (las matrices complejas de dimensión $d_A d_B \times d_A d_B$).

1.2.2 Medidas Parciales

Observación 1.14. Si H_A y H_B dos espacios de estados, consideremos el espacio compuesto $H_{AB} = H_A \otimes H_B$. Denotamos D_{AB} al conjunto:

$$D_{AB} = \{\rho \in M_{d_A d_B}(\mathbb{C}) : \rho \text{ es un estado de } H_{AB}\}.$$

También denotamos $SEP_{AB} = \{\rho \in D_{AB} : \ \rho \text{ es separable}\}$. Notemos que estos son subconjuntos del espacio de matrices con entradas complejas y tamaño $d_A d_B \times d_A d_B$.

Existen varias maneras de medir uno de los factores de un sistema compuesto sin afectar al otro factor (que es la idea de las mediciones parciales), una de ellas es con la traza parcial.

Definición 1.22. Sea ρ_{AB} un operador actuando en $H_A \otimes H_B$ y $\{|l\rangle_B\}$ base ortonormal de H_B. La traza parcial sobre H_B es

$$\rho_A := Tr_B(\rho_{AB}) := \sum_l (I_A \otimes \langle l|_B)\rho_{AB}(I_A \otimes |l\rangle_B).$$

Se cumple, usando la traza parcial, que

$$P_J(j) = Tr(\Lambda_A^j \rho_A).$$

Proposición 1.7. Se cumple lo siguiente.

i) $Tr(\rho_{AB}) = Tr_A(Tr_B(\rho_{AB})) = Tr_B(Tr_A(\rho_{AB}))$.

ii) El operador de densidad de Alice ρ_A, no cambia si Bob hace una operación unitaria o una medición a su sistema.

iii) La pureza del estado de Alice es

$$Tr(\rho_A) = \frac{1}{(d_A d_B)^2} Tr\left(Tr_B(I_A \otimes |l\rangle_B\langle l|_B)\right).$$

Caso General

Como hemos visto, los estados de los sistemas compuestos están descritos por matrices grandes de dimensión $d_A d_B \times d_A d_B$; conviene, por tanto, pensar a la matriz del sistema como una matriz a bloques ($d_A \times d_A$ bloques de tamaño $d_B \times d_B$ cada uno). Definimos ahora una medida parcial para matrices a bloques.

Definición 1.23. Dada la matriz a bloques σ_{AB}, definimos una *medida parcial* como una operación del tipo

$$(I_{d_A} \otimes \varphi)\sigma_{AB},$$

donde I_{d_A} es la transformación identidad en H_A y $\varphi : M_{d_B}(\mathbb{C}) \to M_{d_B}(\mathbb{C})$. La matriz que resulta después de aplicar la medición parcial a σ_{AB} es la matriz a bloques original con la modificación a bloques $B_{ij} \to \varphi(B_{ij})$.

Algunos ejemplos importantes para el resto del trabajo son los siguientes. Denotemos por M_n al espacio $M_n(\mathbb{C})$.

1. **Traza parcial:** $[I_{d_A} \otimes Tr] : M_{d_A d_B} \to M_{d_A}$, como sigue:

$$\sigma_{AB} = \begin{pmatrix} B_{11} & \cdots & B_{1d_A} \\ \vdots & \ddots & \vdots \\ B_{d_A 1} & \cdots & B_{d_A d_A} \end{pmatrix} \overset{[I_{d_A} \otimes Tr]}{\to} \begin{pmatrix} Tr(B_{11}) & \cdots & Tr(B_{1d_A}) \\ \vdots & \ddots & \vdots \\ Tr(B_{d_A 1}) & \cdots & Tr(B_{d_A d_A}). \end{pmatrix}$$

2. **Transpuesta parcial:** $[I_{d_A} \otimes T] : M_{d_A d_B} \to M_{d_A d_B}$, como sigue:

$$\sigma_{AB} = \begin{pmatrix} B_{11} & \cdots & B_{1d_A} \\ \vdots & \ddots & \vdots \\ B_{d_A 1} & \cdots & B_{d_A d_A} \end{pmatrix} \overset{[I_{d_A} \otimes T]}{\to} \begin{pmatrix} B_{11}^T & \cdots & B_{1d_A}^T \\ \vdots & \ddots & \vdots \\ B_{d_A 1}^T & \cdots & B_{d_A d_A}^T, \end{pmatrix}$$

donde X^T denota la transpuesta de la matriz X. A la transpuesta parcial del estado compuesto σ_{AB} la denotamos por σ_{AB}^{Γ}, pues Γ es la mitad de una T.

3. Definimos la aplicación $R : M_{d_B} \to M_{d_B}$ por $R(X) = Tr(X) \cdot I_{d_B} - X$. Definimos la **aplicación de reducción** como $[I_{d_A} \otimes R] : M_{d_A d_B} \to M_{d_A d_B}$, es decir:

$$\sigma_{AB} = \begin{pmatrix} B_{11} & \cdots & B_{1d_A} \\ \vdots & \ddots & \vdots \\ B_{d_A 1} & \cdots & B_{d_A d_A} \end{pmatrix} \overset{[I_{d_A} \otimes R]}{\to} \begin{pmatrix} R(B_{11}) & \cdots & R(B_{1d_A}) \\ \vdots & \ddots & \vdots \\ R(B_{d_A 1}) & \cdots & R(B_{d_A d_A}), \end{pmatrix}.$$

4. Si fijamos una matriz unitaria $U \in M_{d_B}$, podemos definir la aplicación $\varphi : M_{d_B} \to M_{d_B}$ como $X \mapsto UXU^*$. Definimos la **rotación unitaria parcial** por $[I_{d_A} \otimes \varphi] : M_{d_A d_B} \to M_{d_A d_B}$, es decir

$$\sigma_{AB} = \begin{pmatrix} B_{11} & \cdots & B_{1d_A} \\ \vdots & \ddots & \vdots \\ B_{d_A 1} & \cdots & B_{d_A d_A} \end{pmatrix} \overset{[I_{d_A} \otimes \varphi]}{\to} \begin{pmatrix} \varphi(B_{11}) & \cdots & \varphi(B_{1d_A}) \\ \vdots & \ddots & \vdots \\ \varphi(B_{d_A 1}) & \cdots & \varphi(B_{d_A d_A}). \end{pmatrix}$$

Observación 1.15. Lo anterior son casos particulares de la función parcial $[I_{d_A} \otimes \varphi] : M_{d_A d_B} \to M_{d_A d_C}$:

$$\sigma_{AB} = \begin{pmatrix} B_{11} & \cdots & B_{1d_A} \\ \vdots & \ddots & \vdots \\ B_{d_A 1} & \cdots & B_{d_A d_A} \end{pmatrix} \overset{[I_{d_A} \otimes \varphi]}{\to} \begin{pmatrix} \varphi(B_{11}) & \cdots & \varphi(B_{1d_A}) \\ \vdots & \ddots & \vdots \\ \varphi(B_{d_A 1}) & \cdots & \varphi(B_{d_A d_A}), \end{pmatrix}$$

donde $\varphi : M_{d_B} \to M_{d_C}$. A la nueva matriz $[I_{d_A} \otimes \varphi]\sigma_{AB}$ la llamamos **modificación a bloques de** σ_{AB} y la denotamos por σ_{AB}^{φ}.

Observación 1.16. También pueden tomarse mediciones parciales en H_A dejando fijo H_B, usando funciones del tipo $[\varphi \otimes I_{d_B}]$.

1.2.3 Canales Cuánticos

Necesitamos una aplicación $\mathcal{N}$ que preserve estados en general, como las unitarias lo hacían con los estados puros.

Definición 1.24. Diremos que el operador $M : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ es *positivo* si $M(X_A) \geq 0$ para todo $X_A \geq 0$. El operador $M : \mathcal{L}(H_A) \to \mathcal{L}(H_B)$ es *completamente postivo* si $I_R \otimes M$ es positivo

para cualquier sistema de referencia H_R de dimensión arbitraria.

Las propiedades que queremos preservar son positividad y traza 1, esto motiva la definición de canal cuántico.

Definición 1.25. Un **canal cuántico** $\mathcal{N}_{A,B}$ es una aplicación lineal de A a B, completamente positiva que preserva trazas. Usaremos también la notación $\mathcal{N}_{A\to B}$.

Recordemos que el estado máximamente entrelazado es

$$|\Gamma\rangle_{RA} = \sum_{i=0}^{d_A-1} |i\rangle_R \otimes |i\rangle_A.$$

En términos de lo anterior, tenemos la siguiente definición.

Definición 1.26 (Matriz de Choi)**.** La **matriz de Choi** correspondiente a $\mathcal{N}_{A\to B}$ y las bases antes mencionadas, es:

$$(I_R \otimes \mathcal{N}_{A\to B})|\Gamma\rangle\langle\Gamma|_{RA} = \sum_{i,j=0}^{d_A-1} |i\rangle\langle j|_R \otimes \mathcal{N}_{A\to B}(|i\rangle\langle j|_A).$$

En el caso qudit-qudit, la matriz de Choi asociada a un operador $\varphi_{A\to B}$ es

$$C_\varphi = \sum_{i,j} E_{ij} \otimes \varphi(E_{i,j}),$$

para la base estándar de M_{d_A}. Al isomorfismo $\varphi \mapsto C_\varphi$ para aplicaciones positivas, lo llamamos **biyección de Choi-Jamiolkowsky**.

Una propiedad importante de la matriz de Choi es que caracteriza que un operador sea completamente positivo.

Proposición 1.8. $\mathcal{N}_{A\to B}$ es completamente positivo si y sólo si su matriz de Choi es positiva.

Teorema 1.3 (Choi-Kraus)**.** $\mathcal{N}_{A\to B}$ es un canal cuántico si y sólo si tiene una descomposición de Choi-Kraus:

$$\mathcal{N}_{A\to B}(X_A) = \sum_{l=0}^{d-1} V_l X_A V_l^*,$$

donde $X_A \in \mathcal{L}(H_A)$, $V_l \in \mathcal{L}(H_A, H_B)$ y se cumple

$$\sum_{l=0}^{d-1} V_l^* V_l = I_A,$$

$d \leq d_A, d_B$. A los operadores V_l los llamamos operadores de Kraus.

La demostración del teorema anterior se sigue como caso particular de los teoremas de la subsección 1.2.4.

Observación 1.17. Los canales cuánticos describen evoluciones físicamente factibles del sistema cuántico y por el teorema anterior, cualquier cambio o evolución del sistema (interacción unitaria, pérdida de información, un operador de densidad, medir, etc.) está caracterizada por ciertos operadores de Kraus adecuados que codifiquen ese cambio.

Un ejemplo de canal cuántico es

$$\Lambda(\rho_A) = Tr_B\left(U_{AB\to AB}(\rho_A \otimes |0\rangle\langle 0|_B)U^*_{AB\to AB}\right),$$

donde $U_{AB\to AB}$ es un operador unitario. Lo importante de este ejemplo es que también el recíproco es cierto.

Teorema 1.4 (Stinespring)**.** Λ es canal cuántico si y sólo si

$$\Lambda(\rho_A) = Tr_B\left(U_{AB\to AB}(\rho_A \otimes |0\rangle\langle 0|_B)U^*_{AB\to AB}\right),$$

para alguna $U_{AB\to AB}$ unitaria adecuada.

Observación 1.18. En términos prácticos un canal cuántico es un canal de comunicación que permite transmitir información cuántica, como el estado $\alpha|0\rangle + \beta|1\rangle$ de un qubit. Por otro lado un canal clásico sólo permite transmitir bits; una cadena de n bits es una n-ada de 0 y 1. Actualmente las computadoras transmiten y almacenan información con grandes cadenas de bits.

1.2.4 Teorema de Choi-Kraus

A continuación presentamos una serie de teoremas de los cuales se sigue la prueba del teorema de Choi-Kraus.

Teorema 1.5. Si $\varphi : M_n(\mathbb{C}) \to M_n(\mathbb{C})$ es aplicación autoadjunta (es decir que cumple $\varphi(A)^* = \varphi(A^*)$), entonces existen matrices $V_t \in M_n(\mathbb{C})$ y reales ρ_t, $t = 1, \dots n^2$, tal que para todo $A \in M_n(\mathbb{C})$ se tiene que

$$\varphi(A) = \sum_{t=1}^{n^2} \rho_t V_t A V_t^*$$

y también

$$Tr[V_{t_1} V_{t_2}^*] = \delta_{t_1,t_2}.$$

Si además φ es c_n*-trace preserving*, i.e., $Tr(\varphi(A)) = c_n Tr(A),\ \forall A$, entonces

$$\sum_{t=1}^{n^2} \rho_t V_t^* V_t = c_n I_n.$$

Demostración. Consideremos C_φ la matriz de Choi asociada a φ. Por ser φ autoadjunta, se tiene que

$$C_\varphi^* = \left[\sum_{i,j=1}^{n} E_{ij} \otimes \varphi(E_{ij})\right]^* = \sum_{i,j=1}^{n} E_{ji} \otimes \varphi(E_{ij})^* = \sum_{i,j=1}^{n} E_{ji} \otimes \varphi(E_{ji}) = C_\varphi.$$

Como $C_\varphi \in M_n(\mathbb{C}) \otimes M_n(\mathbb{C}) \cong M_{n^2}(\mathbb{C})$ es matriz autoadjunta entonces podemos considerar su descomposición espectral

$$C_\varphi = \sum_{t=1}^{n^2} \rho_t v_t v_t^*,$$

con las siguientes características:

- $\rho_1, \ldots, \rho_{n^2}$ son los eigenvalores **reales**, no necesariamente distintos de C_φ.
- $\{v_1, v_2, \ldots, v_{n^2}\}$ es una base ortonormal para $\mathbb{C}^n \otimes \mathbb{C}^n$ de eigenvectores de C_φ.

Consideremos la siguiente descomposición en la base estándar de $\mathbb{C}^n \otimes \mathbb{C}^n$, $v_t = \sum\limits_{i,j=1}^{n} h_{ij}^{(t)}\, E_i \otimes E_j$, por la ortonormalidad tenemos

$$\delta_{t_1,t_2} = \langle v_{t_1}, v_{t_2} \rangle = \sum_{i,j=1}^{n} h_{ij}^{(t_1)} \overline{h_{ij}^{(t_2)}}. \tag{1.1}$$

Vamos a hacer una observación importante.

Observación: Si tomamos $y \in \mathbb{C}^n \otimes \mathbb{C}^n$ cualquiera, digamos, $y = \sum\limits_{i,j=1}^{n} \alpha_{i,j} E_i \otimes E_j$, definimos la matriz $V_y = \sum\limits_{i,j=1}^{n} \alpha_{i,j} E_{ji}$ y como $V_y E_l = \sum\limits_{i,j=1}^{n} \alpha_{i,j} \delta_{il} E_j$, si tomamos el estado máximamente mixto $\Gamma = \sum\limits_{l=1}^{n} E_l \otimes E_l$, entonces

$$(I_n \otimes V_y)\Gamma = \sum_{l=1}^{n} E_l \otimes V_y E_l = \sum_{i,j=1}^{n} \alpha_{i,j} \sum_{l=1}^{n} E_l \otimes \delta_{il} E_j = \sum_{i,j=1}^{n} \alpha_{i,j} E_i \otimes E_j = y;$$

es decir, para todo $y \in \mathbb{C}^n \otimes \mathbb{C}^n$, existe $V_y \in M_n(\mathbb{C})$ tal que $(I_n \otimes V_y)\Gamma = y$.

Dada la observación anterior, si tomamos $V_t = \sum\limits_{i,j=1}^{n} h_{ij}^{(t)} E_{ji}$, tenemos que $(I_n \otimes V_t)\Gamma = v_t$ y por lo tanto si

$$\Omega = \Gamma\Gamma^* = \left[\begin{array}{c|c|c} E_{11} & \cdots & E_{1n} \\ \hline \vdots & \ddots & \vdots \\ \hline E_{n1} & \cdots & E_{nn} \end{array}\right],$$

ent.

$$E_{ij} \otimes \varphi(E_{ij}) = (E_i \otimes I_n)C_\varphi(E_j \otimes I_n) = (E_i \otimes I_n)\left(\sum_{t=1}^{n^2} \rho_t v_t v_t^*\right)(E_j \otimes I_n)$$
$$= \sum_{t=1}^{n^2} \rho_t (E_i \otimes I_n) v_t v_t^* (E_j \otimes I_n)$$
$$= \sum_{t=1}^{n^2} \rho_t (E_i \otimes I_n)(I_n \otimes V_t)\Gamma[(I_n \otimes V_t)\Gamma]^*(E_j \otimes I_n)$$
$$= \sum_{t=1}^{n^2} \rho_t (E_i \otimes I_n)(I_n \otimes V_t)\Gamma\Gamma^*(I_n \otimes V_t^*)(E_j \otimes I_n) = \sum_{t=1}^{n^2} \rho_t (E_i \otimes V_t)\Omega(E_j \otimes V_t^*)$$
$$= E_{ij} \otimes \sum_{t=1}^{n^2} \rho_t V_t E_{ij} V_t^*.$$

Como lo anterior se cumple para todo i, j, entonces

$$\varphi(A) = \sum_{t=1}^{n^2} \rho_t V_t A V_t^*.$$

Además se cumple que

$$V_{t_1} V_{t_2}^* = \left(\sum_{i,j=1}^{n} h_{ij}^{(t_1)} E_{ji}\right)\left(\sum_{l,m=1}^{n} h_{lm}^{(t_2)} E_{ml}\right)^* = \left(\sum_{i,j=1}^{n} h_{ij}^{(t_1)} E_{ji}\right)\left(\sum_{l,m=1}^{n} \overline{h_{lm}^{(t_2)}} E_{lm}\right)$$
$$= \sum_{i,j,l,m=1}^{n} h_{ij}^{(t_1)} \overline{h_{lm}^{(t_2)}} E_{ji} E_{lm} = \sum_{i,j,l,m=1}^{n} h_{ij}^{(t_1)} \overline{h_{lm}^{(t_2)}} \delta_{il} E_{jm} = \sum_{i,j,m=1}^{n} h_{ij}^{(t_1)} \overline{h_{im}^{(t_2)}} E_{jm};$$

aplicando la traza a lo anterior, tenemos que

$$Tr(V_{t_1} V_{t_2}^*) = \sum_{i,j,m=1}^{n} h_{ij}^{(t_1)} \overline{h_{im}^{(t_2)}} Tr(E_{jm}) = \sum_{i,j,m=1}^{n} h_{ij}^{(t_1)} \overline{h_{im}^{(t_2)}} \delta_{jm} = \sum_{i,j=1}^{n} h_{ij}^{(t_1)} \overline{h_{ij}^{(t_2)}} = \delta_{t_1,t_2},$$

la última igualdad por la ecuación 1.1.

Por último, si φ es c_n-trace preserving, entonces

$$c_n \delta_{ij} = c_n Tr(E_{ij}) = Tr(\varphi(E_{ij})) = \sum_{t=1}^{n^2} \rho_t Tr(V_t E_{ij} V_t^*),$$

pero como AE_{ij} es la matriz que tiene ceros en todos lados excepto en la columna j, en donde

tiene la columna i de A, se cumple que $Tr(AE_{ij}) = A_{ji}$ y entonces por la tracialidad

$$c_n\delta_{ji} = c_n\delta_{ij} = \sum_{t=1}^{n^2} \rho_t Tr(V_t^* V_t E_{ij}) = \sum_{t=1}^{n^2} \rho_t (V_t^* V_t)_{ji} = \left(\sum_{t=1}^{n^2} \rho_t V_t^* V_t \right)_{ji},$$

por lo que se concluye que $\sum_{t=1}^{n^2} \rho_t V_t^* V_t = c_n I_n$.

■

Teorema 1.6. Una función $\varphi : M_n(\mathbb{C}) \to M_n(\mathbb{C})$ es autoadjunta si y sólo si existen matrices $V_t \in M_n(\mathbb{C})$ y reales ρ_t, $t = 1, \dots n^2$, tal que para todo $A \in M_n(\mathbb{C})$ se tiene que

$$\varphi(A) = \sum_{t=1}^{n^2} \rho_t V_t A V_t^*,$$

y también

$$Tr[V_{t_1} V_{t_2}^*] = \delta_{t_1,t_2}.$$

Demostración. Por el teorema 1.5, basta ver el regreso: si φ es de esa forma entonces

$$\varphi(A)^* = \left(\sum_{t=1}^{n^2} \rho_t V_t A V_t^* \right)^* = \sum_{t=1}^{n^2} (\rho_t V_t A V_t^*)^* = \sum_{t=1}^{n^2} \rho_t V_t A^* V_t^* = \varphi(A^*),$$

por lo que φ es autoadjunta. ■

Teorema 1.7. $\varphi : M_n(\mathbb{C}) \to M_n(\mathbb{C})$ es aplicación autoadjunta y c_n-trace preserving si y sólo si existen matrices $V_t \in M_n(\mathbb{C})$ y reales ρ_t, $t = 1, \dots n^2$, tal que para todo $A \in M_n(\mathbb{C})$ se tiene que

$$\varphi(A) = \sum_{t=1}^{n^2} \rho_t V_t A V_t^* \quad \text{y} \quad Tr[V_{t_1} V_{t_2}^*] = \delta_{t_1,t_2},$$

y también

$$\sum_{t=1}^{n^2} \rho_t V_t^* V_t = c_n I_n.$$

Demostración. De nuevo por el teorema 1.5, basta ver sólo el regreso, sabemos que si se cumple la descomposición, por el teorema 1.6, φ es autoadjunta, veamos que también es c_n-trace preserving, para todo i, j se cumple

$$Tr(\varphi(E_{ij})) = \sum_{t=1}^{n^2} \rho_t Tr(V_t^* V_t E_{ij}) = \sum_{t=1}^{n^2} \rho_t (V_t^* V_t)_{ji} = \left(\sum_{t=1}^{n^2} \rho_t V_t^* V_t \right)_{ji} = (c_n I)_{ji} = c_n \delta_{ij};$$

por lo anterior si $A = \sum_{i,j=1}^{n} \alpha_{ij} E_{ij}$ entonces

$$Tr(\varphi(A)) = \sum_{i,j=1}^{n} \alpha_{ij} Tr(\varphi(E_{ij})) = c_n \sum_{i,j=1}^{n} \alpha_{ij}\delta_{ij} = c_n Tr(A).$$

■

Ejemplo 1.5. Vamos a aplicar lo anterior al caso en que $\varphi(A) = A^T$ en el caso $n = 3$, en este caso

$$C_\varphi = \left[\begin{array}{c|c|c} E_{11}^T & E_{12}^T & E_{13}^T \\ \hline E_{21}^T & E_{22}^T & E_{23}^T \\ \hline E_{31}^T & E_{32}^T & E_{33}^T \end{array}\right] = \left[\begin{array}{c|c|c} E_{11} & E_{21} & E_{31} \\ \hline E_{12} & E_{22} & E_{32} \\ \hline E_{13} & E_{23} & E_{33} \end{array}\right] = \sum_{i,j=1}^{n} E_{ij} \otimes E_{ji}.$$

Queremos encontrar los eigenvectores y de la matriz C_φ, para ello consideramos a y como

$$y = \sum_{i,j=1}^{3} \alpha_{ij} E_i \otimes E_j,$$

entonces

$$\begin{aligned} \sum_{i,j=1}^{3} \lambda\alpha_{ij} E_i \otimes E_j = \lambda y = C_\varphi y &= \sum_{i,j,l,m=1}^{3} \alpha_{lm} E_{ij} E_l \otimes E_{ji} E_m \\ &= \sum_{i,j,l,m=1}^{3} \alpha_{lm}\delta_{jl} E_i \otimes \delta_{im} E_j = \sum_{i,j=1}^{3} \alpha_{ji} E_i \otimes E_j; \end{aligned}$$

necesitamos entonces que $\lambda\alpha_{ij} = \alpha_{ji}$. Al ver a y como matriz, esto sucede para las matrices simétricas y antisimétricas (y ellas forman una base para el espacio, por lo que ya es todo el espectro).

Los eigenvectores asociados a $\lambda = 1$ son

$$E_1\otimes E_1,\ E_2\otimes E_2, E_3\otimes E_3, \frac{1}{\sqrt{2}}(E_2\otimes E_1+E_1\otimes E_2), \frac{1}{\sqrt{2}}(E_3\otimes E_1+E_1\otimes E_3), \frac{1}{\sqrt{2}}(E_3\otimes E_2+E_2\otimes E_3)$$

y entonces los valores V_t asociados son $V_1 = E_{11},\ V_2 = E_{22},\ V_3 = E_{33}$ y

$$V_4 = \frac{1}{\sqrt{2}}(E_{12} + E_{21}),\ V_5 = \frac{1}{\sqrt{2}}(E_{13} + E_{31}),\ V_6 = \frac{1}{\sqrt{2}}(E_{32} + E_{23}),$$

y los eigenvectores asociados a $\lambda = -1$ son

$$\frac{1}{\sqrt{2}}(E_2 \otimes E_1 - E_1 \otimes E_2), \frac{1}{\sqrt{2}}(E_3 \otimes E_1 - E_1 \otimes E_3), \frac{1}{\sqrt{2}}(E_3 \otimes E_2 - E_2 \otimes E_3)$$

y entonces los valores V_t asociados son

$$V_7 = \frac{1}{\sqrt{2}}(E_{12} - E_{21}),\ V_8 = \frac{1}{\sqrt{2}}(E_{13} - E_{31}),\ V_9 = \frac{1}{\sqrt{2}}(E_{23} - E_{32}).$$

Usando el hecho que $E_{ij}AE_{kl} = A_{jk}E_{il}$ tenemos

$$\begin{aligned}\sum_{t=1}^{9} \rho_t V_t A V_t^* = {} & A_{11}E_{11} + A_{22}E_{22} + A_{33}E_{33} + \frac{1}{2}(A_{21}E_{12} + A_{22}E_{11} + A_{11}E_{22} + A_{12}E_{21}) \\ & + \frac{1}{2}(A_{31}E_{13} + A_{33}E_{11} + A_{11}E_{33} + A_{13}E_{31}) \\ & + \frac{1}{2}(A_{32}E_{23} + A_{33}E_{22} + A_{22}E_{33} + A_{23}E_{32}) \\ & - \frac{1}{2}(A_{22}E_{11} - A_{21}E_{12} - A_{12}E_{21} + A_{11}E_{22}) \\ & - \frac{1}{2}(A_{33}E_{11} - A_{31}E_{13} - A_{13}E_{31} + A_{11}E_{33}) \\ & - \frac{1}{2}(A_{33}E_{22} - A_{32}E_{23} - A_{23}E_{32} + A_{22}E_{33}),\end{aligned}$$

es decir,

$$\begin{aligned}\sum_{t=1}^{9} \rho_t V_t A V_t^* = {} & \begin{pmatrix} A_{11} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 \\ 0 & A_{22} & 0 \\ 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & A_{33} \end{pmatrix} + \frac{1}{2}\begin{pmatrix} A_{22} & A_{21} & 0 \\ A_{12} & A_{11} & 0 \\ 0 & 0 & 0 \end{pmatrix} \\ & + \frac{1}{2}\begin{pmatrix} A_{33} & 0 & A_{31} \\ 0 & 0 & 0 \\ A_{13} & 0 & A_{11} \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 \\ 0 & A_{33} & A_{32} \\ 0 & A_{23} & A_{22} \end{pmatrix} - \frac{1}{2}\begin{pmatrix} A_{22} & -A_{21} & 0 \\ -A_{12} & A_{11} & 0 \\ 0 & 0 & 0 \end{pmatrix} \\ & - \frac{1}{2}\begin{pmatrix} A_{33} & 0 & -A_{31} \\ 0 & 0 & 0 \\ -A_{13} & 0 & A_{11} \end{pmatrix} - \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 \\ 0 & A_{33} & -A_{32} \\ 0 & -A_{23} & A_{22} \end{pmatrix} \\ & = \begin{pmatrix} A_{11} & A_{21} & A_{31} \\ A_{12} & A_{22} & A_{32} \\ A_{13} & A_{23} & A_{33} \end{pmatrix} = A^T\end{aligned}$$

1.3 Importancia del Entrelazamiento

A continuación se exponen tres protocolos de transmisión de información cuántica que usan como parte clave el entrelazamiento cuántico. Cabe mencionar que el objetivo de este capítulo es motivar la importancia del entrelazamiento para lo cuál se utiliza un lenguaje informal; para un manejo formal de los conceptos véase [48].

1.3.1 Distribución de Clave Cuántica

Para entender este protocolo, necesitamos el teorema de no clonación, que en términos prácticos nos dice que es imposible construir una copiadora universal de estados cuánticos, es decir, un dispositivo que puede copiar cualquier estado cuántico que entre a él.

Teorema 1.8. Consideremos el espacio compuesto H_{AB} de dos sistemas de qubits. No existe un operador unitario $U : H_{AB} \to H_{AB}$ que cumpla que $U|\psi\phi\rangle = |\psi\psi\rangle$ para todo $|\psi\rangle, |\phi\rangle$.

Demostración. Supongamos por contradicción que existe un operador unitario U actuando en el espacio compuesto de dos qubits, que actúa como copiadora universal de información cuántica: es decir si tomamos el estado $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ en el primer qubit y ponemos el estado auxiliar (o molde) $|0\rangle$ en el segundo, entonces

$$U|\psi 0\rangle = |\psi\psi\rangle = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle.$$

Ahora bien, como la copiadora es universal, también tenemos que

$$U|00\rangle = |00\rangle \quad \text{y} \quad U|10\rangle = |11\rangle;$$

pero por la linealidad de U,

$$U|\psi 0\rangle = U(\alpha|0\rangle + \beta|1\rangle)|0\rangle = \alpha|00\rangle + \beta|11\rangle.$$

Como consecuencia las dos expresiones para $U|\psi 0\rangle$ deben ser iguales, lo cual no es cierto para todo valor de α y β. ∎

Ahora bien, el objetivo es transmitir información. Pensemos a Alice como la emisora y a Bob como receptor del mensaje. Como bien sabemos, el acto de medir altera nuestro sistema cuántico; ese hecho puede ser usado para detectar si algún intruso, al cual llamaremos *Eva*, ha tenido acceso a la información que estamos transmitiendo.

El protocolo de clave cuántica BB84 (por su año de creación y sus creadores Bennett y Brassard) es un protocolo que permite verificar que un canal cuántico es seguro para empezar a transmitir información. Supondremos que entre Bob y Alice hay un canal cuántico principal y un canal adicional (posiblemente clásico).

Paso 1: Primero, Alice obtiene algunos bits aleatorios, digamos $0-1-1-0-1-0-0-1$ y también de manera aleatoria elige entre las bases computacional (**C**) y de Hadamard (**H**) para cada uno de los bits generados, digamos que obtiene $C-C-H-C-H-H-H-C$ y usa la siguiente tabla

Base	0	1
C	$\|0\rangle$	$\|1\rangle$
H	$\|-\rangle$	$\|+\rangle$

para generar una secuencia de qubits los cuales manda a Bob.

Paso 2: Bob tratará ahora de leer los qubits que Alice mandó, pero no conoce con que base medirlos, así que selecciona también al azar entre las bases de Hadamard y la computacional para medir cada qubit; digamos que obtuvo $C - H - H - H - C - H - C - C$. Recordemos que si Bob mide en la misma base en la que Alice mandó el obtiene el mismo resultado que ella tenía, pero si equivoca la base, obtiene un resultado aleatorio entre las dos posibilidades; por ejemplo, si mide $|+\rangle$ en la base computacional obtiene con probabilidad $1/2$ a $|1\rangle$ y con probabilidad $1/2$ a $|0\rangle$. Bob mide con las bases aleatorias que tomó y obtiene ciertos qubits, que al usar la tabla de regreso, puede pasar a bits. Ahora ambos tienen una secuencia de bits.
Paso 3: A continuación usan el canal adicional para comunicarse las bases que usaron y eliminar los datos correspondientes a las bases en las que no coinciden, es decir, filtran los bits para quedarse con los que ahora saben que ambos tienen.

Los pasos anteriores están resumidos en la siguiente tabla.

Bits aleatorios de Alice	0	1	1	0	1	0	0	1
Bases aleatorias de Alice	**C**	C	**H**	C	H	**H**	H	**C**
Secuencia de qubits para Bob	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$
Bases aleatorias de Bob	**C**	H	**H**	H	C	**H**	C	**C**
Secuencia de qubits de Bob	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	$\|-\rangle$	$\|1\rangle$	$\|1\rangle$
Bits de Bob	0	0	1	0	1	0	1	1
Clave cuántica después del filtro	0		1			0		1

Paso 4: Por último, si el canal cuántico está libre de intrusos que realicen medidas para conocer la información, entonces Alice y Bob tendrán la misma secuencia de bits como clave cuántica, así que usan de nuevo el canal secundario para comunicarse la llave y ver si coincide. Una forma de comunicar la clave cuántica es poner un número mínimo de coincidencias y lanzar bit por bit, si todos los bits lanzados coinciden entonces acuerdan que el canal está limpio de intrusos para proceder con la comunicación.

Observación 1.19. Lo anterior tiene sentido ya que, si Eva hubiera interceptado el mensaje de Alice, tendría que haber usado la misma selección de bases que usó Alice, para dejar los qubits sin cambio, lo cual es muy improbable para secuencias grandes de bits. Con una base en la que no coincida, habrá un bit en el que Alice y Bob difieren y al ver esa diferencia, abortan la comunicación porque el canal no es seguro.

Entonces para que Eva tenga éxito, tendría que elegir todas y cada una de las bases que eligió Alice o bien, clonar los qubits antes de extraer la información y enviar los clones a Bob, lo cual es imposible por el **teorema de la no clonación**; concluimos que por dicho teorema, el protocolo de clave cuántica indica privacidad con alta probabilidad.

Cabe añadir que existen funciones que permiten saber cuantos bits pueden mandarse Alice y Bob para asegurar que el canal ya es seguro con alta probabilidad.

1.3.2 Teleportación Cuántica

La teleportación cuántica es un protocolo que nos permite transmitir información cuántica cuando sólo tenemos un canal clásico y el estado del sistema conjunto es entrelazado.

En concreto, supongamos que Alice quiere enviar el qubit $\alpha|0\rangle + \beta|1\rangle$ a Bob, pero dispone de un canal clásico por el cual puede enviar dos bits M_1, M_2, $M_i \in \{0, 1\}$ a Bob y que el estado del sistema conjunto es el estado de Bell

$$|\Psi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

En principio Alice podría no conocer el estado de qubit $|\psi\rangle := \alpha|0\rangle + \beta|1\rangle$, pero sí lo tiene al alcance para manipularlo. El sistema tiene por estado inicial, entonces, al estado de tres qubits:

$$\begin{aligned}|\Psi_0\rangle = |\psi\rangle|\Psi^+\rangle &= (\alpha|0\rangle + \beta|1\rangle)\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) \\ &= \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)].\end{aligned}$$

Como sabemos, Alice no puede hacer mediciones en el sistema de Bob, sólo en su parte del qubit entrelazado y en el qubit $|\psi\rangle$. Como **primer paso**, Alice aplica la operación $CNOT \otimes I_B$ al estado del sistema, por lo que el nuevo estado conjunto es

$$|\Psi_1\rangle = CNOT \otimes I_B|\Psi_0\rangle = \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)],$$

es decir, Alice afectó el estado del sistema, sólo aplicando una operación a su parte del qubit entrelazado. Como **segundo paso** Alice cambia el estado del sistema afectando ahora al qubit $|\psi\rangle$ con la operación $H \otimes I_A \otimes I_B$ (con H operador de Hadamard), el nuevo estado conjunto es

$$\begin{aligned}|\Psi_2\rangle = H \otimes I_A \otimes I_B|\Psi_1\rangle &= \frac{1}{\sqrt{2}}[\alpha|+\rangle(|00\rangle + |11\rangle) + \beta|-\rangle(|10\rangle + |01\rangle)] \\ &= \frac{1}{2}[|00\rangle_A(\alpha|0\rangle_B + \beta|1\rangle_B) + |01\rangle_A(\alpha|1\rangle_B + \beta|0\rangle_B) \\ &\quad + |10\rangle_A(\alpha|0\rangle_B - \beta|1\rangle_B) + |11\rangle_A(\alpha|1\rangle_B - \beta|0\rangle_B)].\end{aligned}$$

Para finalizar, Alice aplica una operación correspondiente a una de las matrices de Pauli a su qubit, obteniendo un nuevo estado $|\Psi_3(M_1, M_2)\rangle$. Si por ejemplo ella aplica $I \otimes X \otimes I_B$ al sistema y después hace una medición, colapsará el estado de Bob a $\alpha|1\rangle_B + \beta|0\rangle_B$ por lo que si Bob aplica el operador X obtendrá el estado $|\psi\rangle$ en su sistema. Dependiendo que matriz de Pauli aplique Alice es el operador que debe aplicar Bob; y ¿cómo sabe Bob qué operación aplicar?, eso lo sabrá después de que Alice le mande por el canal clásico los dos bits que le darán la respuesta.

Alice manda los bits M_1, M_2 y Bob sabrá qué operación aplicar y así obtener el estado $|\psi\rangle$.

Observación 1.20. Hacemos ahora algunas aclaraciones sobre la teleportación cuántica.

Medida de Alice M_1M_2	Estado de Bob $\|\Psi_3(M_1M_2)\rangle$	Operación a aplicar	Resultado
00	$\alpha\|0\rangle + \beta\|1\rangle$	I	$\mathrm{I}\|\Psi_3(00)\rangle = \alpha\|0\rangle + \beta\|1\rangle$
01	$\alpha\|1\rangle + \beta\|0\rangle$	X	$X\|\Psi_3(01)\rangle = \alpha\|0\rangle + \beta\|1\rangle$
10	$\alpha\|0\rangle - \beta\|1\rangle$	Z	$Z\|\Psi_3(10)\rangle = \alpha\|0\rangle + \beta\|1\rangle$
11	$\alpha\|1\rangle - \beta\|0\rangle$	$ZX = iY$	$ZX\|\Psi_3(11)\rangle = \alpha\|0\rangle + \beta\|1\rangle$

1. No hay transmisión inmediata de información, a pesar de que la medición de Alice afecte inmediatamente el sistema de Bob, para que haya transmisión de información es necesario que Alice transmita información a Bob mediante el canal clásico, el cual está limitado a la velocidad de la luz.

2. A pesar de que el estado $|\psi\rangle$ se copia en el estado de Bob, esto no viola el teorema de no clonación, ya que el estado inicial de Alice se destruye en el protocolo de transmisión, es decir, no hay un momento en que $|\psi\rangle$ exista en A y en B al mismo tiempo.

1.3.3 Codificación Superdensa

La finalidad de la codificación superdensa como protocolo es transmitir información clásica por medio de un canal cuántico (en este sentido es dual a la teleportación cuántica). Supongamos que Alice quiere mandar los bits M_1 y M_2, pero quiere que Bob obtenga esa información después de que ella le manda un qubit $|\psi\rangle$. Esta transmisión de información será posible si Alice y Bob comparten un estado entrelazado como el estado de Bell $|\Psi^+\rangle$.

Primeramente, Alice aplica la operación correspondiente a una matriz de Pauli, dependiendo de los dos bits que quiere mandar, así el estado del sistema cambia de $|\Psi_0\rangle := |\Psi^+\rangle$ a $|\Psi_1(M_1, M_2)\rangle$.

Bits que Alice quiere enviar M_1M_2	Operación a aplicar	Resultado
00	I	$\|\Psi_1(00)\rangle = \mathrm{I}\|\Psi_0\rangle = \frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle) \equiv \|\beta_{00}\rangle$
10	Z	$\|\Psi_1(10)\rangle = Z\|\Psi_0\rangle = \frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle) \equiv \|\beta_{10}\rangle$
01	X	$\|\Psi_1(01)\rangle = X\|\Psi_0\rangle = \frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle) \equiv \|\beta_{01}\rangle$
11	$ZX = iY$	$\|\Psi_1(11)\rangle = ZX\|\Psi_0\rangle = \frac{1}{\sqrt{2}}(\|01\rangle - \|10\rangle) \equiv \|\beta_{11}\rangle$

Eso es todo lo que aplica Alice al sistema, ahora el trabajo para descifrar el mensaje es de Bob. Bob aplica como **primer paso** un operador CNOT al estado $|\Psi_1(M_1, M_2)\rangle$ para obtener

$$|\Psi_2(M_1, M_2)\rangle = CNOT|\Psi_1(M_1, M_2)\rangle.$$

De hecho, obtenemos lo siguiente para las diferentes combinaciones de bits:

$$\begin{cases} |\Psi_2(00)\rangle = \frac{|00\rangle+|10\rangle}{\sqrt{2}}, \\ |\Psi_2(10)\rangle = \frac{|00\rangle-|10\rangle}{\sqrt{2}}, \\ |\Psi_2(01)\rangle = \frac{|11\rangle+|01\rangle}{\sqrt{2}}, \\ |\Psi_2(11)\rangle = \frac{|01\rangle-|11\rangle}{\sqrt{2}}. \end{cases}$$

Bob aplica como **segundo paso** la operación $I_A \otimes H$ (H operador de Hadamard) para obtener:

$$\begin{cases} |\Psi_3(00)\rangle = (I_A \otimes H)|\Psi_2(00)\rangle = |00\rangle, \\ |\Psi_3(10)\rangle = (I_A \otimes H)|\Psi_2(10)\rangle = |10\rangle, \\ |\Psi_3(01)\rangle = (I_A \otimes H)|\Psi_2(01)\rangle = |01\rangle, \\ |\Psi_3(11)\rangle = (I_A \otimes H)|\Psi_2(11)\rangle = |11\rangle. \end{cases}$$

En conclusión, tras aplicar la puerta CNOT y el operador de Hadamard, el estado del sistema es $|M_1 M_2\rangle$, de donde Bob puede saber cuál es el mensaje M_1, M_2 que Alice le manda.

Observación 1.21. Para cada uno de los protocolos antes expuestos, fue de vital importancia que Alice y Bob supieran que compartían un estado entrelazado, si no fuera así, las mediciones de Alice podrían no causar efecto en el estado de Bob (como sucede en el caso separable) y por tanto no habría transmisión de información. En la práctica, se tiene información del estado del sistema conjunto pero a veces no de si es un estado entrelazado o no; interesa, por tanto, poder conocer si el estado es separable o entrelazado para proceder con los protocolos de información o buscar primero entrelazar el sistema con algún mecanismo natural.

Surge entonces la pregunta, ¿porqué mejor no entrelazar el sistema siempre desde el principio?. La respuesta es que si el sistema ya estaba entrelazado y se aplica una operación para entrelazar, podría resultar un sistema separable. Esto sucede por ejemplo con el operador de Hadamard o con el operador CNOT: si el sistema es separable, se aplica uno de estos operadores y nos da uno de los estados de Bell, pero si lo volvemos a aplicar nos queda el estado original separable. Por ello es vital que antes de transmitir información nos aseguremos que el estado del sistema es entrelazado o separable. Sin embargo, computacionalmente es dificil hacerlo a fuerza bruta, ya que detectar entrelazamiento es un problema NP, por lo que tener criterios de detección de entrelazamiento es de vital importancia.

1.4 Criterios de Entrelazamiento

En la sección anterior se explicó la importancia de la detección de entrelazamiento. En la presente, damos algunas condiciones necesarias y algunas suficientes para decir si el estado es entrelazado o no. Empezamos con el caso más sencillo, que es el de los estados puros. El teorema de Schmidt (teorema 1.1) es importante en el sentido que si suponemos que el espacio de Alice es de dimensión 2 y el de Bob es de dimensión un 10^{100}, aún que la dimensión del espacio compuesto es muy grande, si sabemos que el estado del sistema compuesto es puro, podemos entonces encontrar un subespacio de dimensión ≤ 2 del espacio de Bob el cual será suficiente para describir el estado del

sistema, esto ya que $d \leq \min(d_A, d_B)$. Otra aplicación del teorema de Schmidt es que caracteriza el entrelazamiento en estados puros.

Proposición 1.9. Un estado puro es entrelazado si y sólo si tiene más de un coeficiente de Schmidt, i.e., su rango de Schmidt es mayor que 1.

1.4.1 Criterio Peres-Horodecki

Proposición 1.10. Sea $\varphi : M_{d_B} \to M_{d_C}$ positivo y σ_{AB} un estado bipartito separable. Entonces $(I_{d_A} \otimes \varphi)\sigma_{AB} \geq 0$.

Demostración. Como σ_{AB} es separable podemos ponerlo como $\sigma_{AB} = \sum_{i=1}^{r} P_i \rho_i^A \otimes \tau_i^B$, para ρ_i^A estado de H_A y τ_i^B estado de H_B, $P_i \geq 0$, $\sum P_i = 1$. Entonces

$$(I_{d_A} \otimes \varphi)\sigma_{AB} = (I_{d_A} \otimes \varphi) \sum_{i=1}^{r} P_i \rho_i^A \otimes \tau_i^B = \sum_{i=1}^{r} P_i (I_{d_A} \otimes \varphi)(\rho_i^A \otimes \tau_i^B)$$
$$= \sum_{i=1}^{r} P_i \rho_i^A \otimes \varphi(\tau_i^B) \geq 0$$

ya que φ es positivo, $P_i \geq 0, \forall i$ y ρ_i^A es un estado. ∎

En el caso que φ es completamente positivo lo anterior se cumple para cualquier estado, separable o no. Lo interesante es tomar funciones que sean positivas y no completamente positivas (P no CP), pues estas nos dan un criterio de entrelazamiento, tomando la contrapositiva de la proposición anterior:

Proposición 1.11. Sea φ positivo y σ_{AB} cualquier estado. Si la matriz $(I_{d_A} \otimes \varphi)\sigma_{AB}$ tiene un eigenvalor negativo, entonces σ_{AB} es entrelazado.

Corolario 1.1 (Criterio Peres-Horodecki)**.** Si σ_{AB} es separable, entonces $\sigma_{AB}^{\Gamma} = (I \otimes T)\sigma_{AB} \geq 0$.

Demostración. Por la proposición anterior sólo basta ver que $\varphi(A) = A^T$ es una aplicación positiva; pero esto es claro porque A y A^T tienen el mismo polinomio característico y por tanto el mismo espectro, entonces si $A \geq 0$ se sigue que $A^T \geq 0$. ∎

Observación 1.22. La aplicación $\varphi(A) = A^T$ es positiva pero no es completamente positiva, por tanto nos da un criterio de detección de entrelazamiento, a dicho criterio le llamamos **criterio Peres-Horodecki** o **PPT**. Definimos el conjunto $PPT_{AB} = \{\rho \in D_{AB} : \rho^{\Gamma} \geq 0\}$.

En términos de la notación de la Observación 1.14, tenemos que $SEP_{AB} \subseteq PPT_{AB} \subseteq D_{AB}$.

Algo interesante del criterio PPT es que en dimensiones bajas, caracteriza el entrelazamiento; el resultado es el siguiente.

Teorema 1.9. [28, Ch. VI.B.1] Si $d_A d_B \leq 6$ entonces $PPT_{AB} = SEP_{AB}$.

Es decir en los casos qubit-qubit, qubit-qutrit, qutrit-qubit se cumple que σ_{AB} es separable si y sólo si $\sigma_{AB}^{\Gamma} \geq 0$.

Teorema 1.10. Si σ_{AB} es separable, entonces $\sigma_{AB}^{red} := (I \otimes R)\sigma_{AB} \geq 0$ y $(I \otimes S)\sigma_{AB} \geq 0$, donde R es la aplicación de reducción y S la aplicación de rotación unitaria, definidas en la sección 1.2.2.

Demostración. Como antes, sólo basta ver que R y S son positivos. Para S es claro, ya que

$$\langle UAU^*x, x\rangle = \langle AU^*x, U^*x\rangle = \langle Ay, y\rangle, \quad y = U^*x,$$

y por tanto si A es positivo entonces UAU^* también lo es. Para ver que R es positiva tomamos la base de eigenvectores de $X \geq 0$ y vemos que $Tr(X)I - X$ en esa base es la matriz diagonal $diag(\sum_{i\neq 1} \lambda_i)$, la cual es positiva semidefinida. ∎

Si llamamos $RED_{AB} = \{\rho \in D_{AB} : \rho^{red} \geq 0\}$, tenemos el siguiente resultado.

Teorema 1.11. [28, Ch. VI.B.6] $PPT_{AB} \subseteq RED_{AB}$.

1.4.2 Testigos de Entrelazamiento

El objetivo de esta subsección es estudiar las funciones cuyo manejo nos permite distinguir entre estados separables y un estado entrelazado específico. A estas funciones las llamaremos *testigos de entrelazamiento*.

Teorema 1.12. [28, Ch. VI.B.3] Para todo estado entrelazado ρ existe un operador hermitiano A, tal que $Tr(A\rho) < 0$ pero $Tr(A\sigma) \geq 0$ para todo σ separable.

Definición 1.27. Al operador A asociado a ρ que existe por el teorema anterior, lo llamamos **testigo de entrelazamiento** asociado a ρ.

Una observación importante es que el plano $\{\sigma : Tr(A\sigma) = 0\}$ divide al espacio de estados en dos; en una parte están todos los estados separables y en la otra parte hay al menos un estado entrelazado, como lo indica la figura 1.2.

Observación 1.23. La idea es que para cada estado entrelazado, existe un "testigo", un operador que nos asegura que tal estado es entrelazado y que identifica muy bien a los estados separables. Aunque no nos sirva para identificar otros estados entrelazados, "atestigua" por uno.

Otra observación importante que se hace en [28] es que **existe una biyección entre testigos de entrelazamiento y aplicaciones que son positivas pero no completamente positivas (P no CP)**, de hecho tal biyección se da via la biyección de Choi-Jamiolkowsky. Lo anterior permite demostrar el siguiente teorema, que complementa a la caracterización de Schmidt para estados puros.

Teorema 1.13. Un estado mixto $\sigma \in D_{AB}$ es separable si para toda aplicación positiva $\varphi : B(H_B) \to B(H_A)$, el operador $(I_A \otimes \varphi)\sigma$ es positivo.

Como corolario tenemos,

Corolario 1.2. En el caso de dimensión finita. $\sigma \in D_{AB}$ es separable si y sólo si $(I_A \otimes \varphi) \geq 0$ para toda aplicación positiva $\varphi : M_{d_B} \to M_{d_C}$.

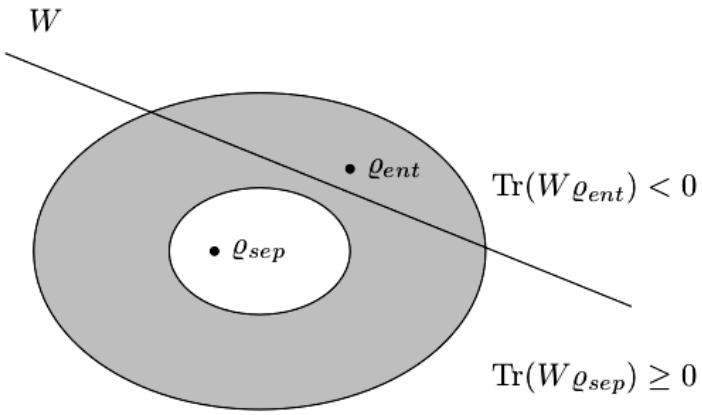


Figura 1.2: Testigo de Entrelazamiento

1.4.3 Otros Métodos

Definición 1.28. Definimos la aplicación de *reordenación* L tal que

$$L(e_i e_j^* \otimes f_a f_b^*) = e_i f_a^* \otimes e_j f_b^*.$$

y extendiendo por linealidad. Denotamos $X^{rln} = L(X)$.

Se define la norma 1 de Schatten por $\|T\|_1 = Tr(\sqrt{T^*T})$. La aplicación de reordenación nos da también un criterio de entrelazamiento.

Teorema 1.14. [28, Ch. VI.B.8] Si $\sigma_{AB} \in D_{AB}$ estado separable, entonces

$$\|\sigma_{AB}^{rln}\|_1 \leq 1.$$

Es decir si $RLN_{AB} = \{\rho \in D_{AB} : \|\rho^{rln}\|_1 \leq 1\}$, entonces $SEP_{AB} \subseteq RLN_{AB}$.
Análogo a la entropía de Shannon, podemos definir también entropía para estados cuánticos.

Definición 1.29. Sea ρ una matriz de densidad. Se definen las siguientes p-entropías.

1. $H_0(\rho) = \log rank(\rho)$.
2. $H_p(\rho) = \frac{1}{1-p} \log Tr(\rho^p)$, para $p \in (0,1) \cup (1,\infty)$.
3. $H(\rho) = H_1(\rho) = -Tr[\rho \log \rho]$.
4. $H_\infty(\rho) = -\log \|\rho\|_\infty$.

Observación 1.24. Existen algunas caracterizaciones de entrelazamiento en términos de la entropía y pueden encontrarse en [28, ch.5].

Capítulo 2

Canales y Estados Cuánticos Aleatorios

2.1 Teoría de Matrices Aleatorias

Definición 2.1. Sea $(\Omega, \mathcal{F}, \mathbb{P})$ un espacio de probabilidad y $\mathcal{Q} \in \mathcal{B}(\mathbb{M}_{m\times n}(\mathbb{C}))$. Una función $X : \Omega \to \mathcal{Q}$ es una *matriz aleatoria* si

$$X^{-1}(A) \in \mathcal{F} \qquad \forall A \in \mathcal{B}(\mathcal{Q}) = \mathcal{Q} \cap \mathcal{B}(\mathbb{M}_{m\times n}(\mathbb{C})),$$

es decir, X es una función $\mathcal{B}(\mathcal{Q}) \setminus \mathcal{F}$-medible.

Observación 2.1. Equivalentemente se cumple que si $X = (X_{ij}) \in \mathcal{Q}$, entonces X es matriz aleatoria con valores en $\mathcal{Q}$ si y sólo si X_{ij} es una variable aleatoria compleja para todo $i = 1, \ldots, m$, $j = 1, \ldots, n$.

Algunos $\mathcal{Q}$ de interés son:

1. $\mathcal{Q} = \mathbb{M}_{m\times n}(\mathbb{C})$, $\mathcal{Q} = \mathbb{M}_{m\times n}(\mathbb{R})$, $\mathcal{Q}$ las matrices hermitianas, $\mathcal{Q} = \mathbb{S}_d(\mathbb{R})$ las matrices simétricas, $\mathcal{Q} = \mathbb{S}_d^+$ el cono de matrices semidefinidas positivas.

2. $\mathcal{Q} = \mathbb{U}(n)$ el grupo unitario, i.e, $\mathbb{U}(n) = \{U \in \mathbb{M}_n(\mathbb{C}) : U^*U = UU^* = I_n\}$ y $\mathcal{Q} = \mathbb{O}(m)$ el grupo ortogonal dado por $\mathbb{O}(m) = \{O \in \mathbb{M}_m(\mathbb{R}) : O^TO = OO^T = I_m\}$.

por la observación anterior, podemos definir matrices aleatorias, sólo definiendo la distribución de sus entradas.

Definición 2.2. Sean $Z_{ij} \sim N(0, 1)$ v.a.i.i.d. para $i = 1, \ldots, m$, $j = 1, \ldots, n$. A la matriz aleatoria $Z = (Z_{ij}) \in M_{m\times n}(\mathbb{R})$ la llamamos matriz *Ginibre normal rectangular* o *ginibre gaussiana*.

Proposición 2.1. Sea Z de $m \times n$ matriz ginibre normal rectangular. Si $O \in \mathbb{O}(m)$ no aleatoria, $OZ \overset{d}{=} Z$ y $\forall P \in \mathbb{O}(n)$, $ZP \overset{d}{=} Z$.

El resultado anterior puede extenderse al caso $Z_{ij} \sim N(0, \sigma^2)$. Para el caso complejo tenemos un resultado similar.

Proposición 2.2. Sea Z_{ij} con $Re(Z_{ij}) \sim Im(Z_{ij}) \sim N(0, \frac{1}{2})$ v.a. independientes para $i = 1, \ldots, m$, $j = 1, \ldots, n$. Sea $Z = (Z_{ij}) \in M_{m\times n}(\mathbb{C})$. Entonces si $U \in \mathbb{U}(m)$ no aleatoria, $UZ \stackrel{d}{=} Z$ y $\forall\, V \in \mathbb{U}(n)$, $ZV \stackrel{d}{=} Z$.

Generalizamos la definición anterior.

Definición 2.3.
1. Si X es matriz aleatoria en $M_n(\mathbb{C})$ con entradas independientes, la llamamos *Matriz de Ginibre* (en caso no cuadrado lo llamamos *Matriz de Ginibre rectangular*).
2. Se dice que $X = (X_{ij}) \in M_n(\mathbb{F})$ es *Matriz de Wigner* si
   i) (Caso real) X es real simétrica y $\{X_{ij} : 1 \leq i \leq j \leq d\}$ son variables aleatorias independientes.
   ii) (Caso complejo) X es hermitiana compleja y $\{X_{ij} : 1 \leq i \leq j \leq d\}$ son variables aleatorias independientes.

Observación 2.2. A veces se pide para una matriz de Wigner que tenga segundo momento finito y que encima de la diagonal tenga un medio de la varianza de la diagonal. También es común pedir segundo momento y simetría de las distribuciones.

Definición 2.4.
1. Una matriz aleatoria $X \in \mathbb{M}_{m\times n}(\mathbb{R})$ es invariante bajo transformaciones ortogonales por la izquierda [derecha] si $\forall\, O \in \mathbb{O}(m)$ [$\forall O \in \mathbb{O}(n)$], $OX \stackrel{d}{=} X$ [$XO \stackrel{d}{=} X$].
2. Una matriz aleatoria $X \in \mathbb{M}_{m\times n}(\mathbb{C})$ es invariante bajo transformaciones unitarias por la izquierda [derecha] si $\forall\, U \in \mathbb{U}(m)$ [$\forall U \in \mathbb{U}(n)$], $UX \stackrel{d}{=} X$ [$XU \stackrel{d}{=} X$].

Lema 2.1. Sea $X \in \mathbb{M}_{m\times n}(\mathbb{R})$ con distribución invariante bajo transformaciones ortogonales por la izquierda (análogamente para unitarias y derecha). Sea $h : \mathbb{M}_{m\times n}(\mathbb{R}) \to \mathbb{M}_{d'\times e'}(\mathbb{R})$ una función $\mathbb{B}(\mathbb{M}_{m\times n}) \setminus \mathbb{B}(\mathbb{M}_{d'\times e'})$-medible. Entonces

$$h(OX) \stackrel{d}{=} h(X).$$

Demostración.
Sea $A \in \mathcal{B}(\mathbb{M}_{d'\times e'})$ y sea $O \in O(m)$.

$$\mathbb{P}(h(OX) \in A) = \mathbb{P}(OX \in h^{-1}(A)) \stackrel{\text{(invarianza)}}{=} \mathbb{P}(X \in h^{-1}(A)) = \mathbb{P}(h(X) \in A).$$

Por lo tanto, $h(OX) \stackrel{d}{=} h(X)$. ∎

Definición 2.5. Sea X matriz aleatoria en $\mathbb{M}_m(\mathbb{R})$. Se dice que X tiene distribución *invariante bajo conjugaciones ortogonales* o bien que X es *ortogonalmente invariante* si $\forall O \in \mathbb{O}(m)$, $OXO^t \stackrel{d}{=} X$.

Si X matriz aleatoria en $X \in \mathbb{M}_m(\mathbb{C})$. Se dice que X tiene distribución *invariante bajo conjugaciones unitarias* o bien que X es *unitariamente invariante* si $\forall U \in \mathbb{U}(m)$, $UXU^* \stackrel{d}{=} X$.

Lema 2.2. Sea $X \in \mathbb{M}_{m\times n}(\mathbb{R})$ ($\mathbb{M}_{m\times n}(\mathbb{C})$) con distribución invariante bajo conjugaciones ortogonales (unitarias) y $h : \mathbb{M}_{m\times n}(\mathbb{R}) \to \mathbb{M}_{d'\times e'}(\mathbb{R})$ una función $\mathbb{B}(\mathbb{M}_{m\times n}) \setminus \mathbb{B}(\mathbb{M}_{d'\times e'})$-medible. Entonces para todo $O \in \mathbb{O}(m)$ ($U \in \mathbb{U}(m)$) tenemos

$$h(OXO^t) \overset{d}{=} h(X). \ (h(UXU^*) \overset{d}{=} h(X)).$$

Observación 2.3. El concepto de invarianza bajo transformaciones ortogonales $OX \overset{d}{=} X$, es una extensión del concepto de variable aleatoria simétrica ($-X \overset{d}{=} X$). No así el de invarianza bajo conjugaciones ortogonales.

Sea Z matriz $m \times m$ Ginibre gaussiana en $\mathbb{M}_d(\mathbb{R})$. Definimos G simétrica como

$$G = \frac{1}{\sqrt{2}}(Z + Z^t). \tag{2.1}$$

Si $Z \in \mathbb{M}_n(\mathbb{C})$, definimos G hermitiana como

$$G = \frac{1}{\sqrt{2}}(Z + Z^*). \tag{2.2}$$

Proposición 2.3. $G \in \mathbb{S}_n$ como en 2.1 es ortogonalmente invariante. Análogamente G hermitiana como en 2.2 es unitariamente invariante.

Demostración.

Caso ortogonal (unitario es análogo). Queremos ver que $\forall O \in \mathbb{O}(d)$ se tiene que $O^tGO \overset{d}{=} G$. En efecto,

$$O^tGO = \frac{1}{\sqrt{2}}(O^tZO + O^tZ^tO) \overset{d}{=} \frac{1}{\sqrt{2}}(ZO + O^tZ^t) = \frac{1}{\sqrt{2}}(Z + Z^t) = G.$$

■

Observación 2.4. Analicemos aspectos distribucionales de ambos casos de G ((2.1) y (2.2)).

i) Consideremos primero el caso complejo para G en el que $Z_{ij} = Re(Z_{ij}) + iIm(Z_{ij})$, con $Re(Z_{ij}), Im(Z_{ij})$ independientes, ambas con distribución $N(0, \frac{1}{2})$. Tenemos entonces que

$$G_{ii} = \frac{1}{\sqrt{2}}[Z_{ii} + \bar{Z}_{ii}] = \frac{1}{\sqrt{2}}[2Re(Z_{ii})] = \sqrt{2}Re(Z_{ii}),$$

y entonces

$$\mathbb{E}(G_{ii}) = 0, \ \ \mathbb{V}(G_{ii}) = \mathbb{V}(\sqrt{2}Re(Z_{ii})) = 2\mathbb{V}(Re(Z_{ii})) = 2 \cdot \frac{1}{2} = 1.$$

Para el caso $i \neq j$, usaremos que las variables G_{ij} son centradas y el hecho de que si Y

variable aleatoria compleja centrada, entonces $\mathbb{V}(Y) = \mathbb{E}(|Y|^2)$. Así pues, como

$$|G_{ij}|^2 = G_{ij}\bar{G}_{ji} = \frac{1}{2}[Z_{ij}\bar{Z}_{ji} + Z_{ij}\bar{Z}_{ij} + \bar{Z}_{ij}\bar{Z}_{ji} + Z_{ij}\bar{Z}_{ji}],$$

entonces, por independencia:

$$\begin{aligned}\mathbb{V}(G_{ij}) &= \mathbb{E}[|G_{ij}|^2] = \frac{1}{2}\mathbb{E}[|Z_{ij}|^2 + |\bar{Z}_{ji}|^2] = \frac{1}{2}\mathbb{E}[2|Z_{ij}|^2] \\ &= \mathbb{E}[[Re(Z_{ij})]^2 + [Im(Z_{ij})]^2] = \mathbb{V}(Re(Z_{ij})) + \mathbb{V}(Im(Z_{ij})) \\ &= \frac{1}{2} + \frac{1}{2} = 1\end{aligned}$$

Concluimos que $G_{ij} \sim N(0,1)$ para todo i, j.

ii) Para el caso en que $G \in \mathbb{S}_n$ tenemos resultados diferentes ya que

$$G_{ij} = \begin{cases} \sqrt{2}Z_{ii}, \ i = j \\ \frac{1}{\sqrt{2}}(Z_{ij} + Z_{ji}), \ i \neq j \end{cases}.$$

y por tanto $\mathbb{V}G_{ii} = 2\mathbb{V}(Z_{ii}) = 2$ y para $i \neq j$, $\mathbb{V}G_{ij} = 1$. Concluimos que $(G_{ij})_{1\leq i\leq j\leq d}$ son variables independientes con distribución:

$$G_{ij} \sim \begin{cases} N(0,2), \ i = j \\ N(0,1), \ i \neq j \end{cases}.$$

Definición 2.6. Un *ensamble* $(X_n)_{n\geq 1}$ es una sucesión de matrices aleatorias tal que para todo $n \geq 1$, X_n es una matriz $n \times n$.

Definición 2.7. 1) Un ensamble $G = (G^d)_{d\geq 1}$ se dice *Gaussiano Ortogonal* y se abrevia GOE si $\forall d \geq 1$, $G^d = (G^d_{ij})_{i,j=1,\dots,d}$ es tal que $\{G^d_{ij} : 1 \leq i \leq j \leq d\}$ son variables aleatorias independientes, $G^d \in \mathbb{S}_d$ y

$$G^d_{ii} \sim N(0,2)$$
$$G^d_{ij} \sim N(0,1) \qquad \forall i \neq j.$$

Es decir, G^d es como G definida en (2.1).

2) Un ensamble $G = (G^d)_{d\geq 1}$ se dice *Gaussiano Unitario* y se abrevia GUE si $\forall d \geq 1$, $G^d = (G^d_{ij})_{i,j=1,\dots,d}$ es tal que $\{G^d_{ij} : 1 \leq i \leq j \leq d\}$ son variables aleatorias independientes, $G^d \in \mathbb{H}_d$ y $G^d_{ij} \sim N(0,1) \qquad \forall i, j$. Es decir, G^d es como G en (2.2).

Observación 2.5. Las matrices en los ensambles GOE y GUE son matrices de Wigner.

Definimos ahora otro ensamble de matrices, el cuál será de vital importancia en lo siguiente.

Definición 2.8. Sea $Z = \{Z_{ij}\} \in M_{m\times n}(\mathbb{C})$ con Z_{ij} v.a.i.i.d gaussianas para $1 \leq i \leq m$, $1 \leq j \leq n$, $n \leq m$. A la matriz $m \times m$, definida por $W := ZZ^*$ se le conoce como la **matriz de Wishart** de parámetros (m, n) y se denota por $\mathcal{W}_{m,n}$.

Proposición 2.4. La matriz de Wishart W es invariante bajo conjugaciones unitarias y tiene rango completo con probabilidad 1.

Enunciamos a continuación el teorema de Marchenko-Pastur, que corresponde al análogo de la ley de eventos raros en probabilidad libre.

Teorema 2.1. Considere una sucesión de enteros s_d tal que $s_d \sim cd$ cuando $d \to \infty$, para algún $c \in (0, \infty)$. Sean W_d sucesión de matrices aleatorias con distribución Wishart de parámetros (d, s_d). Entonces W_d converge casi seguramente a la distribución de Marchenko-Pastur π_c dada por

$$d\pi_c(x) = \max(1 - c, 0)\delta_0 + \frac{\sqrt{(b - x)(x - a)}}{2\pi x}\mathbf{1}_{(a,b)}(x)dx,$$

donde $a = (1 - \sqrt{c})^2$ y $b = (1 + \sqrt{c})^2$.

Para la prueba se necesita la *fórmula de Wick*:

Teorema 2.2. Sean $X_1, \ldots, X_k$ variables gaussianas, entonces

$$\mathbb{E}[X_1 \cdots X_k] = \sum_{\substack{p=\{\{i_1,j_1\},\ldots,\{i_l,j_l\}\} \\ \text{emparejamientos de } \{1,\ldots,k\}}} \prod_{m=1}^{l} \mathbb{E}[X_{i_m} X_{j_m}].$$

2.2 Estados Cuánticos Aleatorios

Recordemos que por estado nos referíamos a una matriz positiva definida de traza 1. Se define un estado aleatorio de manera natural como sigue.

Definición 2.9. Un *estado aleatorio* es una matriz aleatoria positiva definida y de traza 1.

Podemos obtener estados aleatorios si definimos una distribución de probabilidad μ en el espacio de estados $D_d = \{\rho \in M_d(\mathbb{C}) : \rho \geq 0,\ Tr(\rho) = 1\}$ (cuyos puntos extremos son los estados puros los cuales están identificados con $\{x \in \mathbb{C}^d : \|x\| = 1\}$).

A continuación definimos distribuciones en D_d.

2.2.1 Distribuciones de Probabilidad en Estados Cuánticos

Estados Aleatorios Puros

El primer conjunto de estados en el que definimos una medida de probabilidad es el conjunto de estados puros.

Definición 2.10. Se dice que el estado puro $x \in \mathbb{C}^d$ tiene la *distribución uniforme* si está uniformemente distribuido en la esfera unitaria de $\mathbb{C}^d$. Denotamos esto por $x \sim \chi_d$.

Proposición 2.5. Sea $x \sim \chi_d$. Entonces se cumple lo siguiente:

i) Para cualquier operador unitario $U \in \mathcal{U}_d$ independiente de x, entonces el estado aleatorio puro Ux cumple que $Ux \sim \chi_d$.

ii) Si $X \in \mathbb{C}^d$ es vector gaussiano complejo, $X \sim \mathbb{C}N(0, I_n)$, entonces $\frac{X}{\|X\|} \sim \chi_d$.

iii) Si U matriz aleatoria con distribución de Haar y y la primer columna de U, entonces $y \in \mathbb{C}^d$ cumple $y \sim \chi_d$.

El Ensamble Inducido

Vamos a definir ahora medidas en estados mixtos.

Definición 2.11. Dados dos naturales d, s, considere un estado aleatorio puro $x \in \mathbb{C}^d \otimes \mathbb{C}^s$ (distribución uniforme). La distribución de la matriz aleatoria definida por la traza parcial:

$$\rho := [I_d \otimes Tr_s](xx^*) \in D_d,$$

es llamada la *medida inducida* de parámetros (d, s) y es denotada $\nu_{d,s}$.

Proposición 2.6. Consideremos $\rho \sim \nu_{d,s}$. Se cumple lo siguiente

i) Con probabilidad 1, ρ tiene rango $\min(d, s)$.

ii) Si U es unitario e independiente de ρ, entonces $U\rho U^* \overset{d}{=} \rho$.

iii) Existe una matriz unitaria U y una matriz diagonal $\Delta = diag(\lambda_1, \ldots, \lambda_d)$ tal que U tiene la distribución de Haar, U y Δ son independientes y $\rho = U\Delta U^*$. Se le llama a estos elementos la parte radial y angular de ρ.

iv) Los eigenvalores $(\lambda_1, \ldots, \lambda_d)$ tienen distribución conjunta

$$\frac{\Gamma(ds)}{\prod_{i=0}^{d-1} \Gamma(s-i)\Gamma(d+1-i)} \mathbf{1}_{\lambda_1+\cdots+\lambda_d=1} \prod_{i=1}^{d} \mathbf{1}_{\lambda_i \geq 0} \prod_{1 \leq i < j \leq d} (\lambda_i - \lambda_j)^2 \prod_{i=1}^{d} \lambda_i^{s-d}.$$

Observación 2.6. En el caso $s = d$, la medida $\nu_{d,d}$ es la medida de Lebesgue en el conjunto compacto D_d.

Proposición 2.7. Sea $W \in M_d(\mathbb{C})$ una matriz de Wishart de parámetros (d, s) y sea $\rho := \frac{W}{Tr(W)} \in D_d$. Entonces se cumple lo siguiente:

i) Las variables ρ y $Tr(W)$ son independientes.

ii) La distribución de $Tr(W)$ es χ^2_{ds}, distribución ji-cuadrada con ds grados de libertad.

iii) La matriz aleatoria ρ tiene distribución la medida inducida $\rho \sim \nu_{d,s}$.

iv) La matriz W, condicionada a $Tr(W) = 1$, tiene distribución $\nu_{d,s}$.

Observación 2.7. El evento $Tr(W) = 0$, tiene probabilidad 0, ya que por la proposición 2.4, las matrices de Wishart son de rango completo con probabilidad 1.

Para simular estados aleatorios con distribución $\nu_{d,s}$, podemos considerar matrices $\rho = \frac{GG^*}{Tr(GG^*)}$, con G Ginibre gaussianas.

Nos interesa el comportamiendo asintótico de la medida inducida. Consideremos primero el caso con d fijo y $s \to \infty$.

Proposición 2.8. Para d fijo, consideremos la sucesión de matrices aleatorias $(\rho_s)_s$ con distribución $\rho_s \sim \nu_{d,s}$. Entonces, casi seguramente cuando $s \to \infty$, se tiene $\rho_s \to d^{-1} I_d$.

Consideremos ahora un caso más interesante.

Proposición 2.9. Para c fijo, consideremos la sucesión de matrices aleatorias $(\rho_d)_d$ con distribución ρ_{d,s_d}, con s_d tal que $s_d \sim cd$ cuando $d \to \infty$. Entonces, casi seguramente cuando $d \to \infty$ la distribución espectral asintótica de las matrices $s_d \rho_d$ converge débilmente a la distribución Marchenko-Pastur π_c.

Observación 2.8. Lo anterior se puede interpretar como sigue: si $\psi \in \mathbb{C}^d \otimes \mathbb{C}^{\lfloor cd \rfloor}$ un estado aleatorio puro, entonces los eigenvalores de la traza parcial $\rho = [I \otimes Tr](\psi\psi^*)$ se distribuyen, salvo una escala cd, Marchenko-Pastur π_c.

2.2.2 Umbrales de Entrelazamiento

Recordemos que el conjunto $D_{nk} \supseteq SEP_{nk} = \{\rho \in D_{nk} : \rho \text{ es separable}\}$. En esta parte se presentan algunos resultados sobre el *volumen euclideano* de el conjunto SEP_{nk}.

Proposición 2.10. La máxima bola euclideana centrada en el estado máximamente entrelazado $I/(nk)$ y contenida en D_{nk} es separable y tiene radio $[nk(nk-1)]^{-1/2}$.

Observación 2.9. El radio entre el volumen de $SEP_{n,n}$ y D_{n^2} desaparece cuando $n \to \infty$. En el caso en que el parámetro s de la medida inducida $\nu_{nk,s}$ crece a infinito, con n, k fijos, entonces la medida $\nu_{nk,s}$ se concentra alrededor del estado máximamente mixto I_{nk}, por tanto

$$\lim_{s\to\infty} \mathbb{P}_{\nu_{nk,s}}[\rho \in SEP] = 1.$$

Para establecer los resultados con rigor, presentamos la definición de umbral de entrelazamiento, la cual captura la idea de que $\rho \in D_d$ pertenezca a una familia X_d cuando la probabilidad se mide con la medida inducida $\nu_{d,s}$.

Definición 2.12. Sea $X_d \subseteq D_d$ una familia de matrices de densidad y $\rho \in D_d$, decimos que ocurre un fenómeno de *umbral* con valor c_0 en la escala f si ocurre lo siguiente: sea $s_d \sim cf(d)$ para alguna constante $c > 0$, entonces se cumple lo siguiente:

$$\text{si } c < c_0, \lim_{d\to\infty} \mathbb{P}_{\nu_{d,s_d}}[\rho \in X_d] = 0.$$
$$\text{si } c > c_0, \lim_{d\to\infty} \mathbb{P}_{\nu_{d,s_d}}[\rho \in X_d] = 1.$$

Aplicamos ahora la idea de los umbrales para la detección de entrelazamiento, sustituyendo X_d por los conjuntos que nos dan las medidas parciales en la sección 1.2.2. El problema de detectar si un estado mixto dado es entrelazado o no, es un problema NP. Dada esa dificultad y la importancia de detectar entrelazamiento, establecemos ciertos criterios aleatorios, que nos dan la probabilidad de que un estado cuántico aleatorio sea entrelazado.

Teorema 2.3. Para $k = n$. Existen constantes c y C y una función $f(n)$ que cumplen

$$cn^3 < f(n) < Cn^3 \log^2(n),$$

tal que

$$\text{si } s_n < f(n), \lim_{n\to\infty} \mathbb{P}_{\nu_{n^2,s_n}}[\rho \in SEP_{n,n}] = 0.$$
$$\text{si } s_n > f(n), \lim_{n\to\infty} \mathbb{P}_{\nu_{n^2,s_n}}[\rho \in SEP_{n,n}] = 1.$$

Umbral para PPT

Recordemos de la sección 1.2.2 que $PPT_{n,k} = \{\rho \in D_{n,k} : \rho^\Gamma \geq 0\} \supseteq SEP_{n,k}$.

Proposición 2.11. Considere la sucesión de estados aleatorios $\rho_n \in D_{nk_n}$ del ensamble inducido ν_{nk_n,cnk_n}, donde k_n es una función de n y c constante positiva.

Si $k_n = n$, la distribución espectral de ρ_n^Γ converge a la medida semicircular $\mu_{SC(1,1/c)}$, en particular el umbral del conjunto $PPT_{n,n}$ es $c_0 = 4$.

Si $k_n = k$ fijo, la distribución espectral de ρ_n^Γ converge a la diferencia de distribuciones poisson libres:

$$\pi_{ck(k+1)/2} \boxminus \pi_{ck(k-1)/2},$$

en particular el umbral de $PPT_{n,k}$ con k fijo y $n \to \infty$ es

$$c_0 = 2 + 2\sqrt{1 - 1/k^2}.$$

Umbral para RED

Consideremos ahora el espacio $RED_{n,k}$ definido en la sección 1.2.2.

Proposición 2.12. Los umbrales para los conjuntos $RED_{n,k}$ son:

i) Si ambos $n, k \to \infty$, hay un fenómeno de umbral para el parámetro s de la medida inducida $\nu_{nk,s}$ con valor $c_0 = 1$ en la escala $s \sim cn$.

ii) Si n fijo y $k \to \infty$, el umbral para el parámetro s de $\nu_{nk,s}$ está en la escala $s \sim c$ en el valor $c_0 = n$.

iii) Si k fijo y $n \to \infty$ el umbral para s en $\nu_{nk,s}$ está en la escala $s \sim cnk$ en el valor

$$c_0 = \frac{(1+\sqrt{k+1})^2}{k(k-1)}.$$

Positividad del Soporte

Supongamos que μ es una medida de soporte compacto y sea $X_d \in M_{nd}(\mathbb{C})$ sucesión de matrices aleatorias unitariamente invariantes que convergen a μ cuando $d \to \infty$. Sean $f_d : M_n(\mathbb{C}) \to M_d(\mathbb{C})$ aplicaciones lineales tal que la matriz de Choi de f_d es X_d. Entonces la positividad asintótica de f_d depende sólo de μ, más aún, la k-positividad de f_d depende sólo de μ.

Definición 2.13. La aplicación f es k-positiva si $I_k \otimes f$ es positiva.

Teorema 2.4. La sucesión de aplicaciones lineales $(f_d)_d$ definida como antes tiene las siguientes propiedades:

1. Si $supp(\mu^{\boxplus n/k}) \subset (0, \infty)$, entonces, casi seguramente cuando $d \to \infty$, f_d es k-positivo.
2. Si $supp(\mu^{\boxplus n/k}) \cap (-\infty, 0) \neq \emptyset$, entonces, casi seguramente cuando $d \to \infty$, f_d no es k-positivo.

Observación 2.10. Se sigue de lo anterior que las medidas μ con aplicaciones lineales asociadas que son positivas, pero no completamente positivas, nos dan un criterio de detección de entrelazamiento. Sin embargo, encontrar medidas así no es sencillo.

Terminamos esta sección recordando que en la última parte del capítulo 1 se habló de un criterio diferente, llamado RLN. Este criterio también tiene un umbral.

Proposición 2.13. Los umbrales para los conjuntos $RLN_{n,k}$ son:

1. Si $n = k \to \infty$, el umbral para s en la medida inducida $\nu_{n^2,s}$ está en la escala $s \sim cn^2$ en el valor $c_0 = (8/3\pi)^2$.
2. si k fijo y $n \to \infty$, el umbral para s en la medida inducida $\nu_{nk,s}$ está en la escala $s \sim c$ en el valor $c_0 = k^2$.

2.3 Resultados de Canales Cuánticos Aleatorios

Si consideramos matrices X_n tal que $Tr(X^p) \sim n\phi(x^p)$ con x algún operador de un espacio de Hilbert y normalizamos

$$\tilde{X} = \frac{X}{Tr(X)}.$$

Y si Φ canal cuántico, los momentos de $Z = \Phi(\tilde{X})$ cumplen

$$\mathbb{E}[Tr(Z^p)] = \frac{\mathbb{E}[Tr(\Phi(X)^p)]}{Tr(X)^p}.$$

La siguiente proposición es usada en el contexto de **Problemas de Salida y Aditividad**.

Proposición 2.14. El comportamiento casi seguro de la matriz Z está dado por lo siguiente.

1. Cuando n fijo y $k \to \infty$, Z converge casi seguramente al estado máximamente mixto I_n/n.
2. Si k fijo y $n \to \infty$, la distribución espectral de $\tilde{\mu}knZ$ converge a la medida de probabilidad $\nu = [\mu_{(k)}]^{\boxplus k^2}$.
3. Si $k, n \to \infty$ y $k/n \to c$, la distribución espectral de nZ converge a la medida de Dirac δ_1.

Presentamos el siguiente teorema sobre la salida de canales cuánticos.

Teorema 2.5. Considere un canal aleatorio unitario $M_N \to M_N$ obtenidos con k matrices Haar unitarias i.i.d. Para $N >> k/\epsilon^2$ entonces este canal manda todos los estados a distancia ϵ/k al estado máximamente mixto.

A continuación el problema de aditividad de canales cuánticos aleatorios.

Teorema 2.6. Para todo $p \in [1, \infty]$, existen canales cuánticos Ψ y Φ tal que

$$H_p^{min}(\Psi \otimes \Phi) < H_p^{min}(\Psi) + H_p^{min}(\Phi).$$

2.4 Matrices Aleatorias a Bloques

En la subsección 1.2.2 se estableció que el estado del sistema cuántico conjunto puede verse como una matriz a bloques, donde la matriz "exterior" representa es sistema emisor y los bloques al sistema "receptor". Ahora bien, considerar que los estados son estados aleatorios puede ser más adecuado cuando los sistemas cuánticos son abiertos, es decir, interactuan con su ambiente (como usualmente sucede); ya que la incertidumbre en los elementos del estado se atribuyen a la aleatoriedad. Por lo anterior, en los sistemas cuánticos abiertos, el estado del sistema cuántico conjunto está representado por una **matriz aleatoria a bloques**.

Algunos de los criterios de entrelazamiento para el caso aleatorio, serían los siguientes.

Teorema 2.7 (Criterio Peres-Horodecki)**.** Sea σ_{AB} un estado bipartito aleatorio tal que

$$\sigma_{AB} \overset{d}{=} \sum_{i=1}^{r} P_i \rho_i^A \otimes \tau_i^B,$$

con ρ_i^A estado aleatorio de A y τ_i^B estado aleatorio de B, entonces $\sigma_{AB}^{\Gamma} = (I \otimes T)\sigma_{AB} \geq 0$ casi seguramente.

Por lo anterior, si σ_{AB}^{Γ} tiene eigenvalores negativos con probabilidad positiva, entonces el estado aleatorio es entrelazado.

Teorema 2.8. El estado bipartito aleatorio σ_{AB} es separable si y sólo sí $\sigma_{AB}^{\Gamma} = (I \otimes \varphi)\sigma_{AB} \geq 0$ casi seguramente para todo operador positivo φ.

Observación 2.11. El problema de entrelazamiento lo podemos resolver, al conocer la distribución espectral de la matriz estado del sistema conjunto, para así hacer los cálculos de la probabilidad de que alguno sea negativo. En el presente capítulo repasamos algunas familias de matrices aleatorias cuya distribución espectral (o espectral asintótica) es conocida. Sin embargo, las herramientas desarrolladas no funcionan para matrices a bloques; para ellas hay que usar la teoría de probabilidad valuada en operadores. En el siguiente capítulo usaremos dicha teoría para dar información del espectro de las matrices aleatorias modificadas a bloques y por tanto del entrelazamiento de sistemas cuánticos con estados aleatorios.

Capítulo 3

Probabilidad Libre e Información Cuántica

En las secciones pasadas vimos que la detección de entrelazamiento en los sistemas cuánticos conjuntos es de vital importancia para la transmisión de información cuántica y que en los sistemas cuánticos abiertos es razonable considerar que el estado conjunto es una matriz aleatoria a bloques. En este capítulo usamos la teoría de probabilidad libre valuada en operadores para dar información del espectro de las matrices aleatorias modificadas a bloques y por tanto, para detectar entrelazamiento. Comenzamos repasando algunos de los elementos de la probabilidad libre y la probabilidad libre valuada en operadores. Seguido de esto tenemos la parte principal de esta tesis, donde se usa lo anterior para encontrar la distribución espectral límite de las modificaciones a bloques.

3.1 Probabilidad Libre

Definición 3.1. Decimos que $\mathcal{A}$ es una *álgebra compleja* si es un espacio vectorial sobre $\mathbb{C}$, con un producto $\cdot : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ asociativo, bilineal y con un único neutro multiplicativo.

Si existe en $\mathcal{A}$ una *involución*, i.e., una operación $* : \mathcal{A} \to \mathcal{A}$ que cumple que $(a + \lambda b)^* = a^* + \bar{\lambda} b^*$, $(a^*)^* = a$ y $(ab)^* = b^* a^*$ para todo $a, b \in \mathcal{A}, \lambda \in \mathbb{C}$, entonces $\mathcal{A}$ es llamada *$*$-álgebra compleja*.

Si $\mathcal{A}$ es una $*$-álgebra y además está dotada de una norma $\| \cdot \| : \mathcal{A} \to [0, \infty)$, que la hacen un espacio de Banach y cumple

a) $\|ab\| \leq \|a\|\|b\|$ para todo $a, b \in \mathcal{A}$,

b) $\|a^* a\| = \|a\|^2$ para todo $a \in \mathcal{A}$,

decimos que $\mathcal{A}$ es una C^*-álgebra.

Dados $a_1, a_2, \ldots, a_n \in \mathcal{A}$, el *álgebra generada* por $a_1, a_2, \ldots, a_n$ se define por

$$\langle a_1, \ldots, a_n \rangle := \{p(a_1, \ldots, a_n) : p \in \mathbb{C}\langle x_1, \ldots, x_n \rangle\},$$

donde $\mathbb{C}\langle x_1, \ldots, x_n\rangle$ es el conjunto de polinomios con coeficientes complejos en las variables no conmutativas x_i. En una $*$-álgebra, la $*$-álgebra generada por $a_1, \ldots, a_n$ es $\langle a_1, a_1^*, \ldots, a_n, a_n^*\rangle$ definida como antes pero en el doble de variables.

Definición 3.2. Un *espacio de probabilidad no-conmutativo (EPNC)* es un par $(\mathcal{A}, \varphi)$ donde $\mathcal{A}$ es una álgebra compleja y $\varphi : \mathcal{A} \to \mathbb{C}$ es un funcional lineal que cumple que $\varphi(\mathbf{1}_{\mathcal{A}}) = 1$. A los elementos de $\mathcal{A}$ se les llama *variables aleatorias no-conmutativas*, o sólo variables aleatorias.

Si $\mathcal{A}$ es una $*$-álgebra [C^*-álgebra] y φ cumple también que $\varphi(a^*a) \geq 0$ para toda $a \in \mathcal{A}$, entonces el par $(\mathcal{A}, \varphi)$ es llamado *$*$-espacio de probabilidad no conmutativo ($*$-EPNC)* [C^*-EPNC].

La involución en los $*$-EPNC nos permite definir tipos especiales de variables aleatorias; decimos que $a \in \mathcal{A}$ es *autoadjunta* o *real* si $a = a^*$, *normal* si $aa^* = a^*a$, *unitaria* si $aa^* = a^*a = \mathbf{1}_{\mathcal{A}}$ y *positiva* si existe $x \in \mathcal{A}$ tal que $a = xx^*$. Decimos también que φ es *tracial* si $\varphi(ab) = \varphi(ba)$ para todo $a, b \in \mathcal{A}$ y *fiel* si $\varphi(a^*a) = 0$ sólo si $a = 0$.

En este marco la información probabilística de las variables aleatorias está codificada por el funcional φ cuando actúa en los elementos $(a)^{n_1}(a^*)^{m_1} \cdots (a)^{n_k}(a^*)^{m_k}$, así pues llamamos a la colección $\varphi((a)^{n_1}(a^*)^{m_1} \cdots (a)^{n_k}(a^*)^{m_k})$ *momentos mixtos* de la variable aleatoria a.

Observación 3.1. Para el caso de una variable aleatoria a autoadjunta, la distribución en el sentido analítico (si existe), es una medida μ con soporte compacto en $\mathbb{R}$ y los momentos mixtos son

$$\varphi(a^m) = \int_{-\infty}^{\infty} x^m \mu(dx).$$

En un espacio de probabilidad no conmutativo, no toda variable aleatoria tiene distribución en este sentido; sin embargo, si $(\mathcal{A}, \tau)$ es C^*-EPNC, podemos garantizar que toda variable aleatoria autoadjunta tiene distribución en el sentido analítico, eso es una consecuencia de la representación Gelfand-Naimark-Segal y puede encontrarse en [34].

Ejemplo 3.1. Como ejemplo de espacio de probabilidad no conmutativo consideremos $\mathcal{A} = M_n(\mathbb{C})$ el álgebra de matrices complejas de dimensión $n \times n$ y $\varphi : \mathcal{A} \to \mathbb{C}$ definida por

$$\varphi(A) = tr(A) := \frac{Tr(A)}{n} = \frac{1}{n}\sum_{i=1}^{n} A_{ii}.$$

El espacio $(\mathcal{A}, \varphi)$ es un $*$-EPNC, con la involución $A^* = \bar{A^T}$ y en efecto, las variables aleatorias no conmutan.

En este espacio, si consideramos A matriz normal entonces existe una matriz unitaria U tal que $A = U\Lambda U^*$ y Λ es la matriz diagonal de eigenvalores de A. La $*$-distribución de A entonces es

$$tr(A^k(A^*)^m) = tr[U\Lambda^k(\Lambda^*)^m U^*] = \frac{Tr(\Lambda^k(\Lambda^*)^m)}{n} = \frac{1}{n}\sum_{i=1}^{n} \lambda_i^k(\overline{\lambda_i})^m,$$

que son los momentos de $\mu = \frac{1}{n}\sum_{i=1}^{n} \delta_{\lambda_i}$ (la medida compleja uniforme en los eigenvalores) y por

ello en el caso autoadjunto tenemos

$$tr(A^k) = \frac{1}{n}\sum_{i=1}^{n} \lambda_i^k = \int t^k \, d\mu_A(t),$$

donde de nuevo μ_A es la uniforme en los eigenvalores de A, en este caso medida real.

Definición 3.3. Decimos que la familia de subálgebras $\mathcal{A}_i, i \in I$ de $(\mathcal{A}, \varphi)$, es *libre* si se cumple que

$$\varphi(a_1 a_2 \cdots a_n) = 0,$$

siempre que $\varphi(a_j) = 0$, $a_j \in \mathcal{A}_{i(j)}$ y $i(1) \neq i(2) \neq \cdots \neq i(n)$.

Las variables aleatorias $a_1, ..., a_n \in \mathcal{A}$ son libres, si las subálgebras $\langle a_i \rangle,\ i = 1, 2, ..., n.$ son libres.

Observación 3.2. Como $\langle a \rangle = \{P(a) : P \in \mathbb{C}\langle x \rangle\}$, se sigue que en el caso de variables aleatorias $(a_i)_{i \in I}$ en el EPNC $(\mathcal{A}, \varphi)$, las variables son libres si para cualesquiera polinomios $P_1, \ldots, P_k \in \mathbb{C}\langle x \rangle$ y cualesquiera $a_{i_j},\ j = 1, 2, \ldots, k,\ i_j \in I$ con $i_1 \neq i_2 \neq \cdots \neq i_k$ se cumple que

$$\varphi\left(P_1\left(a_{i_1}\right) P_2\left(a_{i_2}\right) \cdots P_k\left(a_{i_k}\right)\right) = 0,$$

siempre que se cumpla que $\varphi\left(P_j\left(a_{i_j}\right)\right) = 0$ para todo $j = 1, \ldots, k$.

La independencia libre se puede entender como una regla para calcular momentos mixtos. Un resultado sencillo, pero importante es que si a y b son variables aleatorias libres, la $*$-distribución de $a + b$ y de ab sólo dependen de la $*$-distribución de a y la $*$-distribución de b, y por tanto podríamos definir

$$\mu_a \boxplus \mu_b = \mu_{a+b},$$

y en el caso de que a, b variables positivas, también

$$\mu_a \boxtimes \mu_b = \mu_{a^{1/2} b a^{1/2}}.$$

De hecho, si μ y ν son medidas con soporte compacto en $\mathbb{R}$, existe un C^*-espacio de probabilidad no conmutativo $(\mathcal{A}, \varphi)$ y variables aleatorias autoadjuntas $a, b \in \mathcal{A}$ tal que a tiene $*$-distribución μ y b tiene $*$-distribución ν, y además a y b son libres, y por lo tanto podemos extender lo anterior para medidas, así que llamamos a $\mu \boxplus \nu$ la convolución libre aditiva (se define formalmente en la Definición 3.11); si las medidas además tienen soporte positivo entonces las variables que existen en el C^*-EPNC son positivas y libres, por tanto definimos $\mu \boxtimes \nu$ la convolución libre multiplicativa, de las medidas μ y ν.

Definición 3.4. Sea (a_n) una sucesión de variables aleatorias no conmutativas, a_n en $(\mathcal{A}_n, \varphi_n)$. Decimos que la sucesión converge en distribución a la variable $a \in \mathcal{A}$, donde $(\mathcal{A}, \varphi)$ es un $*$-

EPNC, si para cada cada $k \in \mathbb{N}$ y cualesquiera $\epsilon_1, \ldots, \epsilon_k \in \{1, *\}$, se cumple que

$$\lim_{n\to\infty} \varphi_n(a_n^{\epsilon_1} \cdots a_n^{\epsilon_k}) = \varphi(a^{\epsilon_1} \cdots a^{\epsilon_k}).$$

Definición 3.5 (Convergencia en distribución conjunta)**.** Sea $(a_{i,n})_{i\in I}$, $n = 1, 2, \ldots$ una familia de sucesiones de variables aleatorias no conmutativas, cada familia en un $*$-EPNC $(\mathcal{A}_n, \varphi_n)$. Diremos que la sucesión *converge en distribución* a la familia de variables aleatorias no conmutativas $(a_i)_{i\in I}$ en un $*$-EPNC $(\mathcal{A}, \varphi)$, si se cumple que para todo k, para cualesquiera $i_1, \ldots, i_k \in I$ y cualesquiera $\epsilon_1, \ldots, \epsilon_k \in \{1, *\}$, se cumple que

$$\lim_{n\to\infty} \varphi_n(a_{i_1,n}^{\epsilon_1} \cdots a_{i_k,n}^{\epsilon_k}) = \varphi(a_{i_1}^{\epsilon_1} \cdots a_{i_k}^{\epsilon_k}).$$

Si las variables $(a_i)_{i\in I}$ son libres, diremos que las variables $(a_{i,n})_{i\in I}$ son *asintóticamente libres*.

Definición 3.6. Sea μ medida de probabilidad en $(\mathbb{R}, \mathbb{B}(\mathbb{R}))$. Se define la **transformada de Cauchy** G_μ, de μ como

$$G_\mu(z) = \int_{-\infty}^{\infty} \frac{1}{z-t}\, \mu(dt), \quad z \in \mathbb{C} \setminus \mathbb{R}.$$

Definición 3.7. En $(\mathcal{A}, \tau)$ se define la transformada de Cauchy de la variable aleatoria autoadjunta a como la función $G_a : \mathbb{C} \setminus \mathbb{R} \to \mathbb{C}$ definida por $G_a(t) = \tau[(t\mathbf{1}_\mathcal{A} - a)^{-1}]$.

Observación 3.3. La transformada de Cauchy está definida para variables aleatorias, pero cuando la variable a tiene distribución analitica (como es el caso de las variables autoadjuntas en los C^*-EPNC), la transformada de Cauchy de a coincide con la transformada de Cauchy de la medida μ_a.

En caso que μ tenga soporte acotado, y si denotamos $m_k = \int_\mathbb{R} t^k \mu(dt)$, la transformada de Cauchy tiene la siguiente expresión en serie de potencias,

$$G_\mu(z) = z^{-1} + \sum_{k=1}^{\infty} m_k(\mu) z^{-k-1}, \quad |z| > r,$$

con $r = \sup\{|t| : t \in supp(\mu)\}$.

Introducimos aquí una distribución muy importante en probabilidad libre, pues juega un papel análogo al de la normal en probabilidad clásica.

Definición 3.8. Sea $m \in \mathbb{R}$ y $\sigma^2 > 0$ la densidad de la *distribución del semicírculo con media* m *y varianza* σ^2, es

$$w_{m,\sigma}(x) = \frac{1}{2\pi\sigma^2} \sqrt{4\sigma^2 - (x-m)^2} \cdot \mathbf{1}_{[m-2\sigma, m+2\sigma]}(x).$$

Si $m = 0$ y $\sigma = 1$, la densidad queda

$$s_{0,1}(x) = \frac{1}{2\pi}\sqrt{4 - x^2} \cdot \mathbf{1}_{[-2,2]}(x),$$

a esta última la llamamos *semicircular estándar*.

La transformada de Cauchy de la distribución de semicírculo con parámetros m y σ es

$$G_{w_{m,\sigma}}(x) = \frac{2}{r^2}(z - \sqrt{(z-m)^2 - r^2}).$$

Definición 3.9. Sea μ una medida de probabilidad en $\mathbb{R}$. La *transformada de Voiculescu* $\phi_\mu : \Gamma \to \mathbb{C}^-$ esta definida como

$$\phi_\mu(z) = F_\mu^{-1}(z) - z, \quad z \in \Gamma,$$

donde $F_\mu(z) = \dfrac{1}{G_\mu(z)}$ es la *recíproca de la transformada de Cauchy* y $\Gamma := \Gamma_{\alpha,\beta} = \{z = x + iy : y > \beta, |x| < \alpha y\}$.

Una medida de probabilidad en $\mathbb{R}$ está determinada por su transformada de Voiculescu.

Teorema 3.1. Sean μ y ν medidas de probabilidad en $\mathbb{R}$ y ϕ_μ, ϕ_ν sus respectivas transformadas de Voiculescu. Entonces $\phi = \phi_\mu + \phi_\nu$ es la transformada de Voiculescu de una (única) medida de probabilidad en $\mathbb{R}$.

Definición 3.10. Con las mismas restricciones de la transformada de Voiculescu, definimos la *R_μ-transformada (o transformada R de μ)* como

$$R_\mu(z) = \phi_\mu(\frac{1}{z}) = F_\mu^{-1}(z^{-1}) - \frac{1}{z}, \quad z^{-1} \in \Gamma.$$

La transformada de Cauchy y la transformada R están relacionadas por la ecuación

$$G_\mu(R_\mu(z) + \frac{1}{z}) = z.$$

Definamos ahora la convolución libre de medidas.

Definición 3.11. Sean μ y ν medidas de probabilidad en $\mathbb{R}$. La *convolución libre aditiva* de μ y ν es la única medida de probabilidad $\mu \boxplus \nu$ en $\mathbb{R}$ tal que

$$R_{\mu\boxplus\nu}(z) = R_\mu(z) + R_\nu(z), \quad z^{-1} \in \Gamma_{\alpha_1,\beta_1} \cap \Gamma_{\alpha_2,\beta_2}.$$

Para una medida de probabilidad μ en $\mathbb{R}$ con soporte compacto y momentos $m_n(\mu), n \geq 1$,

tenemos la expansión en serie de potencias de la función generadora de momentos clásica de μ,

$$\Psi_\mu(z) = \sum_{n=1}^{\infty} m_n(\mu) z^n. \tag{3.1}$$

Si $m_1(\mu) \neq 0$, la inversa $\chi_\mu(z)$ de $\Psi_\mu(z)$ existe y es única como serie formal en z. En este caso, la transformada S se define como

$$S_\mu(z) = \chi_\mu(z)\frac{1+z}{z}. \tag{3.2}$$

Proposición 3.1. Sean μ_1 y μ_2 dos medidas de probabilidad en $\mathbb{R}^+$ con $\mu_i \neq \delta_0, \quad i = 1, 2$. Entonces $\mu_1 \boxtimes \mu_2 \neq \delta_0$ y

$$S_{\mu_1 \boxtimes \mu_2}(z) = S_{\mu_1}(z) S_{\mu_2}(z).$$

Además $(\mu_1 \boxtimes \mu_2)(\{0\}) = max\{\mu_1(\{0\}), \mu_2(\{0\})\}$.

Observación 3.4. Si $c \neq 0$, se define la dilatación de una medida real μ, como la medida $D_c\mu$ que cumple $D_c\mu(A) = \mu(c^{-1}A)$.

Se cumple para la R-transformada que

$$R_{D_c\mu}(z) = cR_\mu(cz). \tag{3.3}$$

Ejemplo 3.2. Vamos a considerar algunos ejemplos.

1. La ley de semicírculo

$$w_{m,\sigma}(x) = \frac{1}{2\pi\sigma^2}\sqrt{4\sigma^2 - (x-m)^2} \cdot \mathbf{1}_{[m-2\sigma, m+2\sigma]}(x),$$

   tiene transformada R es $R(z) = m + \sigma^2 z$.

2. Como vimos en el capítulo anterior, la ley Marchenko-Pastur de parámetro t es

$$d\pi_t(x) = \max(1-t, 0)\delta_0 + \frac{\sqrt{(b-x)(x-a)}}{2\pi x} \cdot \mathbf{1}_{(a,b)}(x)dx.$$

   con $a = (\sqrt{t}-1)^2$ y $b = (\sqrt{t}+1)^2$. Se cumple que,

$$\pi_t = \lim_{n\to\infty} \left((1-\frac{t}{n})\delta_0 + \frac{t}{n}\delta_1\right)^{\boxplus n},$$

   y su transformada R es $R(z) = \frac{t}{1-z}$.

3. Para una medida μ con soporte acotado y con momentos $(m_p)_{p\geq 1}$ y $\lambda > 0$, se define la distribución poisson libre compuesta de tasa λ y medida de intensidad de saltos μ como

$$\pi_{\lambda,\mu} = \lim_{n\to\infty} \left(\left(1 - \frac{\lambda}{n}\right) \delta_0 + \frac{\lambda}{n}\mu \right)^{\boxplus n}.$$

Esta distribución cumple que su R-transformada es

$$R(z) = \lambda \sum_{p=0}^{\infty} m_{p+1} z^p.$$

La ley semicircular juega un papel muy importante en probabilidad libre por que es la ley límite del teorema de límite central libre.

Teorema 3.2. [34, Teo. 8.10] Sea $(\mathcal{A}, \varphi)$ un $*$-EPNC y sea $(a_n)_{n\geq 1} \in \mathcal{A}$ una sucesión de variables aleatorias autoadjuntas, libres y con la misma distribución, con $\varphi(a_i) = 0$ y $\varphi(a_i^2) = 1$ para todo $i \geq 1$. Sea $S_n = \sum_{i=1}^{n} a_i$, entonces (S_n) converge en distribución a la variable s, donde s es una variable aleatoria con distribución en el sentido analítico semicircular estándar.

Otro teorema de gran importancia es el teorema de libertad asintótica de Voiculescu para matrices aleatorias (las cuales forman un espacio de probabilidad no conmutativo con el funcional $\varphi(\cdot) = tr \circ \mathbb{E}(\cdot)$).

Teorema 3.3. [30, Cap. 4, Teo. 4] Sean $A_N^{(1)}, \ldots, A_N^{(p)}$ matrices $N \times N$ independientes GUE y sean $D_N^{(1)}, \ldots, D_N^{(q)}$ matrices $N \times N$ deterministicas que cumplen:

$$D_N^{(1)}, \ldots, D_N^{(q)} \overset{distr.}{\to} d_1, \ldots, d_q, \quad N \to \infty$$

donde la convergencia es en distribución conjunta. Entonces

$$A_N^{(1)}, \ldots, A_N^{(p)}, D_N^{(1)}, \ldots, D_N^{(q)} \overset{distr.}{\to} s_1, \ldots, s_p, d_1, \ldots, d_q, \quad N \to \infty$$

donde cada s_i es semicircular y $s_1, \ldots, s_p, \{d_1, \ldots, d_q\}$ son libres.

Tenemos también una versión para matrices de Haar.

Teorema 3.4. [30, Cap. 4, Teo. 8] Sean $U_N^{(1)}, \ldots, U_N^{(p)}$ matrices $N \times N$ independientes Haar unitarias y sean $D_N^{(1)}, \ldots, D_N^{(q)}$ matrices $N \times N$ deterministicas que cumplen:

$$D_N^{(1)}, \ldots, D_N^{(q)} \overset{distr.}{\to} d_1, \ldots, d_q, \quad N \to \infty$$

donde la convergencia es en distribución conjunta. Entonces cuando $N \to \infty$ se cumple que

$$U_N^{(1)}, U_N^{(1)*}, \ldots, U_N^{(p)}, U_N^{(p)*}, D_N^{(1)}, \ldots, D_N^{(q)} \overset{distr.}{\to} u_1, u_1^*, \ldots, u_p, u_p^*, d_1, \ldots, d_q,$$

donde cada u_i es Haar unitario y $\{u_1, u_1^*\}, \ldots, \{u_p, u_p^*\}, \{d_1, \ldots, d_q\}$ son libres.

Para los fines de este trabajo, usaremos la siguiente generalización de los teoremas anteriores.

Teorema 3.5. Sean $X_N^{(1)}, \ldots, X_N^{(p)}$ matrices $N \times N$ independientes unitariamente invariantes, tales que

$$\lim_{N\to\infty} \frac{1}{N} Tr(X_N^{(i)}) = x_i \in \mathcal{A}$$

y sean $D_N^{(1)}, \ldots, D_N^{(q)}$ matrices $N \times N$ deterministicas que cumplen:

$$D_N^{(1)}, \ldots, D_N^{(q)} \overset{distr.}{\to} d_1, \ldots, d_q, \quad N \to \infty$$

donde la convergencia es en distribución conjunta y los límites están en $\mathcal{A}$. Entonces cuando $N \to \infty$ se cumple que

$$X_N^{(1)}, X_N^{(1)*}, \ldots, X_N^{(p)}, X_N^{(p)*}, D_N^{(1)}, \ldots, D_N^{(q)} \overset{distr.}{\to} x_1, x_1^*, \ldots, x_p, x_p^*, d_1, \ldots, d_q,$$

y además $\{x_1, x_1^*\}, \ldots, \{x_p, x_p^*\}, \{d_1, \ldots, d_q\}$ son libres.

Terminamos esta sección definiendo los espacios comprimidos, que serán de utilidad más adelante.

Definición 3.12. Sea $(\mathcal{A}, \varphi)$ un EPNC y $p \in \mathcal{A}$ una proyección (es decir que cumple $p^2 = p$) tal que $\varphi(p) \neq 0$, llamamos *espacio comprimido* al EPNC $(p\mathcal{A}p, \varphi^{p\mathcal{A}p})$, donde

$$\begin{aligned} p\mathcal{A}p &= \{pap : a \in \mathcal{A}\}, \\ \varphi^{p\mathcal{A}p}(\cdot) &= \frac{1}{\varphi(p)}\varphi(\cdot), \qquad \text{restringido a } p\mathcal{A}p. \end{aligned}$$

Ejemplo 3.3. Consideremos el EPNC $(M_4(\mathbb{C}), tr_4)$ y la proyección:

$$p = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Entonces para $A = (A_{ij})_{i,j=1,\ldots,4}$ tenemos

$$pAp = \begin{pmatrix} A_{11} & A_{12} & 0 & 0 \\ A_{21} & A_{22} & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

por lo que identificamos a $pM_4(\mathbb{C})p$ con $M_2(\mathbb{C})$ y en este caso el operador $tr_4^{pM_4(\mathbb{C})p}$ coincide con tr_2 en $M_2(\mathbb{C})$.

Observación 3.5. Si $(\mathcal{A}, \varphi)$ es un C^*-EPNC y p es proyección autoadjunta con $\varphi(p) \neq 0$ entonces el espacio comprimido $(p\mathcal{A}p, \varphi^{p\mathcal{A}p})$ también es un C^*-EPNC.

Teorema 3.6. [34, Teo. 14.10] Sea $(\mathcal{A},\varphi)$ un EPNC y $p,a_1,\ldots,a_m \in \mathcal{A}$ tal que p es una proyección con $\lambda := \varphi(p) \neq 0$ y p es libre de $\{a_1,\ldots,a_m\}$. Entonces para todo $n \geq 1$ y $1 \leq i(1),\ldots,i(n) \leq m$,

$$R_n^{p\mathcal{A}p}(pa_{i(1)}p,\ldots,pa_{i(n)}p) = \frac{1}{\lambda}R_n(\lambda a_{i(1)},\ldots,\lambda a_{i(n)}).$$

Definición 3.13. Una *familia de unidades matriciales* en un EPNC $(\mathcal{A},\varphi)$, es un conjunto

$$\{e_{ij}\}_{i,j=1,\ldots,d} \subset \mathcal{A}$$

para algún d, que cumple lo siguiente,

$$e_{ij}e_{kl} = \delta_{jk}e_{il}, \quad i,j,k,l = 1,\ldots,d$$
$$\sum_{i=1}^{d} e_{ii} = \mathbf{1}_{\mathcal{A}}.$$

Ejemplo 3.4. Consideremos $\{E_{ij}\}_{i,j=1,\ldots,d}$ la base estándar del espacio $M_d(\mathbb{C})$, es decir,

$$E_{ij} = (\delta_{ik}\delta_{lj})_{k,l=1,\ldots,d}.$$

La familia $\{E_{ij}\}_{i,j=1,\ldots,d}$ es una familia de unidades matriciales para el espacio $(M_d(\mathbb{C}),tr_d)$.

Se cumple en este espacio que $tr_d(E_{ij}) = \delta_{ij}\frac{1}{d}$.

Definición 3.14. Sea $(\mathcal{A},\varphi)$ un EPNC y consideremos $(M_d(\mathbb{C})\otimes\mathcal{A}, tr\otimes\varphi)$. Decimos que $A = (a_{ij})_{i,j=1,\ldots,d}$ (matriz en $M_d(\mathbb{C})\otimes\mathcal{A}$) es *R-cíclica* si se satisface que

$$R_n(a_{i_1,j_1},\ldots,a_{i_n,j_n}) = 0,$$

excepto quizás para $j_1 = i_2,\ldots,j_{n-1} = i_n, j_n = i_1$.

Teorema 3.7. Sea $(\mathcal{A},\varphi)$ un $*$-EPNC y $\{e_{ij}\}_{i,j=1,\ldots,d} \subset \mathcal{A}$ una familia de unidades matriciales que cumple que $\varphi(e_{ij}) = \delta_{ij}\frac{1}{d}$. Denotemos por $(\mathcal{C},\tau_{11})$ el espacio comprimido por e_{11}. Si $a \in \mathcal{A}$ autoadjunta y libre de $\{e_{ij}\}_{i,j=1,\ldots,d}$. Se cumple que

$$R_n^{\tau_{11}}(c_{i_1,j_1},\ldots,c_{i_n,j_n}) = \begin{cases} d^{-(n-1)}R_n(a,\ldots,a), & \text{si } j_1 = i_2,\ldots,j_{n-1} = i_n, j_n = i_1 \\ 0, & \text{otro caso} \end{cases},$$

donde $c_{ij} = e_{1i}ae_{j1} \in \mathcal{C}$ y $R_n^{\tau_{11}}$ son los operadores cumulantes asociados a la esperanza τ_{11}.

Lo anterior nos permite decir algo de la distribución de los bloques de una matriz, conociendo la distribución de la matriz, en el caso R-cíclico.

Observación 3.6. La libertad de matrices es una condición algebraica muy restrictiva y limita mucho que podamos hablar de distribuciones de algunas matrices de interés. Por ejemplo, si

sabemos que las entradas de dos matrices forman una familia de variables libres, no es cierto que las matrices son libres; o bien, si consideramos matrices a bloques

$$X_N = \begin{pmatrix} A_N & B_N & C_N \\ B_N & A_N & B_N \\ C_N & B_N & A_N \end{pmatrix} \quad \text{y} \quad Y_N = \begin{pmatrix} D_N & D_N & E_N \\ E_N & F_N & D_N \\ F_N & F_N & D_N \end{pmatrix},$$

donde los bloques de X_N son libres de los de Y_N, tampoco podemos usar nuestros teoremas para decir algo de la distribución de $X_N + Y_N$ o $X_N Y_N$. Las anteriores limitantes se superan con la teoría de probabilidad libre valuada en operadores, que veremos en la siguiente sección.

3.2 Probabilidad Libre Valuada en Operadores

En la sección pasada indrodujimos la probabilidad libre. Esta teoría nos permite entender con profundidad la naturaleza asintótica de ciertas familias de matrices aleatorias de relevancia en áreas como teoría de la información, física, gráficas aleatorias, entre otras; en dicha sección se discutieron también, ciertos análogos de la probabilidad clásica. En la presente desarrollamos el análogo libre de la esperanza condicional clásica; estudio que se conoce como probabilidad libre valuada en operadores (abreviado *OVFP* por sus siglas en inglés).

En la teoría de probabilidad, la idea de condicionar es muy útil, ya que permite resolver problemas sujetos a que se tiene cierta información adicional del experimento. Presentamos a continuación la definición clásica de esperanza condicional.

Definición 3.15. Sea $(\Omega, \mathcal{F}, \mathbb{P})$ un espacio de probabilidad y X una variable aleatoria integrable. Si $\mathcal{G} \subset \mathcal{F}$ sub-σ-álgebra, *la esperanza condicional* de X dada $\mathcal{G}$ es cualquier variable aleatoria $Z \in \mathcal{G}$ (i.e. medible respecto a $\mathcal{G}$) e integrable tal que

$$\int_A Z \, d\mathbb{P} = \int_A X \, d\mathbb{P}, \ \ \forall A \in \mathcal{G}.$$

Se denota a Z por $\mathbb{E}[X|\mathcal{G}]$.

Observación 3.7. La esperanza condicional es una variable aleatoria y es única $\mathbb{P}|_{\mathcal{G}}$-casi seguramente; cumple además que $\mathbb{E}[X|\mathcal{G}] \in \mathcal{G}$. La existencia de la variable $\mathbb{E}[X|\mathcal{G}]$, se sigue del teorema de Radon-Nicodym.

Proposición 3.2. Si X, Y son integrables y $\mathcal{G}$ sub-σ-álgebra. La esperanza condicional satisface lo siguiente

a) Es lineal $\mathbb{E}[aX+bY|\mathcal{G}] = a\mathbb{E}[X|\mathcal{G}]+b\mathbb{E}[Y|\mathcal{G}]$ y además $Y \in \mathcal{G}$ implica $\mathbb{E}[YX|\mathcal{G}] = Y\mathbb{E}[X|\mathcal{G}]$.

b) *Propiedad de torre* o *lema de suavizamiento*: $\mathcal{G}_1 \subset \mathcal{G}_2 \Rightarrow \mathbb{E}\left[\mathbb{E}[X|\mathcal{G}_2] \mid \mathcal{G}_1\right] = \mathbb{E}[X|\mathcal{G}_1]$.

c) Propiedad de compatibilidad o ley de *esperanza total*: $\mathbb{E}\left[\mathbb{E}[X|\mathcal{G}]\right] = \mathbb{E}[X]$.

d) Si X es independiente de $\mathcal{G}$ entonces $\mathbb{E}[X|\mathcal{G}] = \mathbb{E}[X]$, en particular $\mathbb{E}[X|\{\emptyset, \Omega\}] = \mathbb{E}[X]$ y $\mathbb{E}[X|\mathcal{F}] = X$.

Definimos a continuación el análogo libre de la esperanza condicional.

Definición 3.16. Sea $(\mathcal{A}, \tau)$ un EPNC y $\mathcal{B} \subset \mathcal{A}$ una sub-álgebra con unidad de $\mathcal{A}$. Una transformación lineal $\mathbb{F} : \mathcal{A} \to \mathcal{B}$ es una **esperanza condicional** si cumple:

i) $\mathbb{F}[b] = b, \ \ \forall b \in \mathcal{B}$.

ii) $\mathbb{F}[b_1 a b_2] = b_1 \mathbb{F}[a] b_2 \ \ \forall b_1, b_2 \in \mathcal{B}, \ a \in \mathcal{A}$.

Decimos también que $\mathbb{F}$ es *compatible con* τ si $\tau[\mathbb{F}(a)] = \tau(a)$. Si $\mathcal{B}_1 \subset \mathcal{B}_2$, decimos que $\mathbb{F}_1$ y $\mathbb{F}_2$ son *compatibles* si $\mathbb{F}_1 [\mathbb{F}_2(a)] = \mathbb{F}_1(a)$.

La definición antes presentada tiene similitudes con la esperanza condicional clásica, que justifican el nombre; primeramente $\mathbb{F}(a)$ es una variable aleatoria (no conmutativa), $\mathbb{F}$ es lineal, y además los elementos de $\mathcal{B}$ salen como constantes de la esperanza condicional. Las propiedades de compatibilidad son prácticamente la ley de esperanza total y la propiedad de torre.

Definición 3.17. $(\mathcal{A}, \tau, \mathcal{B}, \mathbb{F})$ es un *espacio de probabilidad valuado en operadores* (EPVO) si consiste en un EPNC $(\mathcal{A}, \tau)$, una sub-álgebra con unidad $\mathcal{B} \subseteq \mathcal{A}$ y una esperanza condicional $\mathbb{F} : \mathcal{A} \to \mathcal{B}$. Por simplicidad denotaremos a estos espacios sólo por $(\mathcal{A}, \mathbb{F})$.

Ejemplo 3.5. Presentamos ahora algunos ejemplos de EPVO. Sea $(\mathcal{A}, \tau)$ un EPNC.

1. Sea $\mathcal{B} = \mathcal{A}$ y $\mathbb{F} = Id$. Ésta claramente es una esperanza condicional, de hecho por la primer propiedad, es la única esperanza condicional para esa subálgebra. A este EPVO lo llamamos el *EPVO trivial*.

2. El caso $\mathcal{B} = \mathbb{C}\mathbf{1}_{\mathcal{A}}$ y $\mathbb{F}[a] = \tau(a)\mathbf{1}_{\mathcal{A}} \cong \tau(a)$ es también un EPVO, a este espacio lo llamamos *caso escalar*. Es claro que trabajar con este espacio, es equivalente a lo hecho en la sección anterior.

3. Consideremos el espacio de matrices aleatorias $(M_n(\mathbb{C}) \otimes \mathcal{A}, tr \otimes \tau)$. Las siguientes son esperanzas condicionales,

   - $\mathbb{F}_3 : (a_{ij})_{ij} \mapsto (\tau(a_{ij}))_{ij} \in M_n(\mathbb{C})$.
   - $\mathbb{F}_2 : (a_{ij})_{ij} \mapsto (\delta_{ij}\tau(a_{ij}))_{ij} \in D_n(\mathbb{C})$.
   - $\mathbb{F}_1 : (a_{ij})_{ij} \mapsto \left[\sum_{i=1}^{n} \frac{1}{n}\tau(a_{ii})\right] I_n \in \mathbb{C}I_n$.

   Donde $\mathbb{C}I_n \subset D_n(\mathbb{C}) \subset M_n(\mathbb{C})$ son respectivamente, los múltiplos escalares de la identidad, las matrices diagonales escalares y las matrices escalares.

Introducimos ahora el análogo de independencia condicional, usando la esperanza condicional.

Definición 3.18. Defimos que las álgebras $(\mathcal{A}_i)_{i\in I}$ con $\mathcal{B}\subset\mathcal{A}_i$, son **$\mathcal{B}$-libres** (o **libres con amalgamación sobre** $\mathcal{B}$) si $\mathbb{F}(a_1\cdots a_n)=0$ siempre que $n\in\mathbb{N}$, $\mathbb{F}(a_i)=0$ y $a_i\in\mathcal{A}_{j_i}$, $j_1\neq j_2\neq\cdots\neq j_n$.

Observación 3.8. En el caso escalar, las variables o álgebras son $\mathcal{B}$-libres si y sólo si son libres. Cabe decir que toda álgebra unitaria contiene a $\mathbb{C}\mathbf{1}_{\mathcal{A}}$.

La independencia libre la percibimos de manera intuitiva como una fórmula para factorizar momentos mixtos. Por ejemplo si queremos el momento mixto $\tau(aba)$ lo que hacemos primero es centrar e igualar a cero y después usar linealidad para despejar el momento que queremos.

En el caso $\mathcal{B}$-libres podemos hacer lo mismo pues $\mathbb{F}$ es lineal, pero con más cuidado pues en el álgebra los elementos no necesariamente conmutan.

Ejemplo 3.6. Para ejemplificar lo anterior. Si x y $\{y_1,y_2\}$ son $\mathcal{B}$-libres entonces

$$\mathbb{F}[y_1xy_2]=\mathbb{F}[y_1\mathbb{F}(x)y_2].$$

Y si $\{x_1,x_2\}$ y $\{y_1,y_2\}$ son $\mathcal{B}$-libres entonces

$$\mathbb{F}[x_1y_1x_2y_2]=\mathbb{F}[x_1\mathbb{F}(y_1)x_2]\mathbb{F}(y_2)+\mathbb{F}(x_1)\mathbb{F}[y_1\mathbb{F}(x_2)y_2]-\mathbb{F}(x_1)\mathbb{F}(y_1)\mathbb{F}(x_2)\mathbb{F}(y_2).$$

Aunque en el caso escalar la distribución de la variable a era la colección de momentos $\tau(a^n)$, en el caso valuado en operadores no tenemos conmutatividad y las expresiones para la distribución amalgamada, así como para una generalización de cumulantes se vuelve más complicada. Presentamos, no obstante, la definición de ambos:

Definición 3.19. Definimos la *distribución valuada en operadores* de la variable aleatoria a como la colección de todos los momentos $\mathcal{B}$-valuados,

$$\mathbb{F}[ab_1ab_2\cdots ab_{n-1}a]\in\mathcal{B},\quad n\in\mathbb{N},\ b_k\in\mathcal{B}.$$

Definición 3.20. Se define la *transformada de Cauchy* $\mathcal{B}$-valuada de la variable $a\in\mathcal{A}$ como

$$G_a^{\mathcal{B}}(b)=\mathbb{F}[(b-a)^{-1}]=\sum_{n\geq 0}\mathbb{F}[b^{-1}(ab^{-1})^n].$$

Definimos la R-transformada como la función R que se relaciona con la transformada de Cauchy $\mathcal{B}$-valuadas de la siguiente manera,

$$bG(b)=\mathbf{1}_{\mathcal{A}}+R(G(b))\cdot G(b),\qquad \text{o bien}\quad G(b)=(b-R(G(b)))^{-1}. \tag{3.4}$$

Decimos que s es variable semicircular $\mathcal{B}$-valuada si $R_n(sb_1,sb_2,\ldots,sb_{n-1},s)=0$, para todo $n\neq 2$ y todo $b_i\in\mathcal{B}$.

Teorema 3.8. [30, Cap. 9, Teo. 11] Fijemos un EPVO $(\mathcal{A},\mathbb{F})$.

1. Libertad con amalgamación sobre $\mathcal{B}$ de las variables x y y es equivalente a que los cumulantes $\mathcal{B}$-valuados mixtos en x y y, se anulen. Esto implica la aditividad $R_x^{\mathcal{B}}(b) + R_y^{\mathcal{B}}(b) = R_{x+y}^{\mathcal{B}}(b)$, siempre que x y y sean $\mathcal{B}$-libres.

2. Si s es un operador semicircular $\mathcal{B}$-valuado, entonces $R_s^{\mathcal{B}}(b) = \eta(b)$, donde $\eta : \mathcal{B} \to \mathcal{B}$ es la aplicación lineal $\eta(b) = \mathbb{F}[sbs]$.

El siguiente teorema justifica la importancia de la compatibilidad o propiedad de torre.

Teorema 3.9. Supongamos $\mathcal{B}_m \subset \mathcal{B}_{m-1} \subset \cdots \subset \mathcal{B}_1 \subset \mathcal{A}$ y $\mathbb{F}_i : \mathcal{A} \to \mathcal{B}_i$ esperanzas condicionales **compatibles**:

$$\mathcal{A} \xrightarrow{\mathbb{F}_1} \mathcal{B}_1 \xrightarrow{\mathbb{F}_2} \mathcal{B}_2 \xrightarrow{\mathbb{F}_3} \cdots \xrightarrow{\mathbb{F}_m} \mathcal{B}_m.$$

Dado lo anterior, la transformada de Cauchy valuada en operadores satisface:

$$G_a^{\mathcal{B}_{i+1}}(b) = \mathbb{F}_{i+1}\left[G_a^{\mathcal{B}_i}(b)\right].$$

Demostración. Dada la compatibilidad $\mathbb{F}_{i+1} \circ \mathbb{F}_i = \mathbb{F}_{i+1}$ tenemos:

$$\mathbb{F}_{i+1}\left[G_a^{\mathcal{B}_i}(b)\right] = \mathbb{F}_{i+1}\left[\mathbb{F}_i[(b-a)^{-1}]\right] = (\mathbb{F}_{i+1} \circ \mathbb{F}_i)\left[(b-a)^{-1}\right] = \mathbb{F}_{i+1}\left[(b-a)^{-1}\right] = G_a^{\mathcal{B}_{i+1}}(b).$$

■

Corolario 3.1. Si $\mathbb{F} : \mathcal{A} \to \mathcal{B}$ es una esperanza condicional compatible con τ, entonces

$$G_a(b) = \tau[G_a^{\mathcal{B}}(b)].$$

Lo anterior justifica que podamos condicionar a álgebras convenientes y después de trabajar allí apliquemos otras esperanzas condicionales para obtener resultados.

Observación 3.9. Mencionamos en la sección anterior que la transformada de Cauchy escalar tiene una representación integral para elementos autoadjuntos. En el EPVO $(M_n(\mathbb{C}) \otimes \mathcal{A}, Id_m \otimes \tau)$, si tomamos c y x autoadjuntos entonces

$$G_{c\otimes x}(b) = (Id_m \otimes \tau)((b - c \otimes x)^{-1}) = \int_{\mathbb{R}} (b - c \otimes t)^{-1}\, d\mu_x(t).$$

Más aún, en el caso de matrices deterministas, si asumimos $M_n(\mathbb{C}) \subset \mathcal{A}$ y consideramos $x = x^* \in M_m(\mathbb{C}) \otimes M_n(\mathbb{C})$. Entonces

$$G_x^{\mathcal{B}}(b) = (Id_m \otimes \frac{1}{n}Tr)((b \otimes I_n - x)^{-1}),$$

es decir, la transformada de Cauchy es la traza parcial del resolvente.

Definimos ahora, el análogo a la transformada S (definido en [26]).

Definición 3.21. Definimos la transformada $\Psi_a^{\mathcal{B}}$ como $\Psi_a^{\mathcal{B}}(b) = \sum_{n\geq 1} \mathbb{F}[(ab)^n]$, la cual tiene una inversa (en un dominio adecuado) $\Psi_a^{<-1>}(b)$. Se define la S-transformada $\mathcal{B}$-valuada como

$$S_a^{\mathcal{B}}(b) = (\mathbf{1}_{\mathcal{A}} + b)b^{-1}\Psi_a^{<-1>}(b).$$

Teorema 3.10. La S-transformada $\mathcal{B}$-valuada cumple lo siguiente.

1. Si x y y son $\mathcal{B}$-libres, entonces

$$S_{xy}^{\mathcal{B}}(b) = S_y^{\mathcal{B}}(b)S_x^{\mathcal{B}}(S_y^{\mathcal{B}}(b)^{-1}S_y^{\mathcal{B}}(b)).$$

2. Si $\mathcal{B}$ es conmutativa y x y y son $\mathcal{B}$-libres, entonces

$$S_{xy}^{\mathcal{B}}(b) = S_x^{\mathcal{B}}(b)S_y^{\mathcal{B}}(b).$$

3. Si $\mathcal{B}$ es conmutativa, entonces la transformada R y S se relacionan de la siguiente manera.

$$bR^{\mathcal{B}}(b) + S^{\mathcal{B}}(bR^{\mathcal{B}}(b)) = b.$$

En la sección anterior planteamos algunas limitantes de la probabilidad libre escalar; demostramos ahora cómo la probabilidad valuada en operadores puede solucionar dichas limitantes.

Teorema 3.11. Consideremos $(\mathcal{A}, \tau)$ un EPNC y las matrices aleatorias $(M_n(\mathbb{C}) \otimes \mathcal{A}, tr \otimes \tau)$. Si las entradas de dos matrices aleatorias son libres entonces las dos matrices son libres con amalgamación respecto a $\mathbb{F}_3 : M_n(\mathcal{A}) \to M_n(\mathbb{C})$, la esperanza condicional

$$\mathbb{F}_3 : (a_{ij})_{ij} \mapsto (\tau(a_{ij}))_{ij} \in M_n(\mathbb{C}),$$

es decir, son $M_n(\mathbb{C})$-libres.

Ejemplo 3.7. Si $\{a_1, b_1, c_1, d_1\}$ y $\{a_2, b_2, c_2, d_2\}$ son libres respecto a τ, entonces

$$X_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \quad \text{y} \quad X_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix},$$

son libres respecto a $\mathbb{F}_3$, pero no son libres bajo $tr \otimes \tau$.

Para ver lo segundo primeramente observemos que,

$$X_1X_2 = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix},$$

y por tanto,

$$\begin{aligned}(tr\otimes\tau)(X_1X_2) &= \frac{1}{2}[\tau(a_1)\tau(a_2)+\tau(b_1)\tau(c_2)+\tau(c_1)\tau(b_2)+\tau(d_1)\tau(d_2)]\\ &\neq [\tau(a_1)+\tau(d_1)][\tau(a_2)+\tau(d_2)]\\ &= (tr\otimes\tau)(X_1)(tr\otimes\tau)(X_2).\end{aligned}$$

Si tuvieramos libertad tendríamos igualdad en la ecuación anterior. Por otro lado, bajo $\mathbb{F}_3$ no existe ese problema pues:

$$\begin{aligned}\mathbb{F}_3(X_1X_2) &= \begin{pmatrix}\tau(a_1)\tau(a_2)+\tau(b_1)\tau(c_2) & \tau(a_1)\tau(b_2)+\tau(b_1)\tau(d_2)\\ \tau(c_1)\tau(a_2)+\tau(d_1)\tau(c_2) & \tau(c_1)\tau(b_2)+\tau(d_1)\tau(d_2)\end{pmatrix}\\ &= \begin{pmatrix}\tau(a_1) & \tau(b_1)\\ \tau(c_1) & \tau(d_1)\end{pmatrix}\begin{pmatrix}\tau(a_2) & \tau(b_2)\\ \tau(c_2) & \tau(d_2)\end{pmatrix}\\ &= \mathbb{F}_3(X_1)\mathbb{F}(X_2)\end{aligned}$$

ya que se tiene libertad amalgamada a $\mathbb{F}_3$.

Generalizamos lo anterior en el siguiente teorema.

Teorema 3.12. Sea $(\mathcal{A},\mathbb{F})$ un EPVO y considere $(M_n(\mathbb{C})\otimes\mathcal{A},\ id\otimes\mathbb{F})$ espacio $M_n(\mathcal{B})$-valuado. Si $A_1,\ldots,A_k\subset\mathcal{A}$ son $\mathcal{B}$-libres entonces $(M_n(\mathbb{C})\otimes A_1),\ldots,(M_n(\mathbb{C})\otimes A_k)\subset(M_n(\mathbb{C})\otimes\mathcal{A})$ son $(M_n(\mathcal{B}))$-libres.

Demostración. Sean $a^{(1)},\ldots,a^{(m)}\in M_n(\mathbb{C})\otimes\mathcal{A}$ tal que $a^{(i)}\in M_n(\mathbb{C})\otimes A_{j(i)}$ con $j(1)\neq j(2)\neq\cdots\neq j(m)$.

Vamos a denotar $\overline{a}=a-\mathbb{F}(a)$, para alguna a y $\mathbb{E}$ su esperanza correspodiente. Ahora, como

$$\overline{a^{(i)}}=a^{(i)}-(id\otimes\mathbb{F})(a^{(i)})=[(a^{(i)}_{rs})-\mathbb{F}(a^{(i)}_{rs})]_{r,s\leq n}=\left(\overline{a^{(i)}_{rs}}\right)_{r,s\leq n},$$

entonces para todo $i,j\leq n$ se tiene:

$$\left[(id\otimes\mathbb{F})((\overline{a^{(1)}})\cdots(\overline{a^{(m)}}))\right]_{i,j}=\sum_{i_1,\ldots,i_m=1}^{n}\mathbb{F}\left[\left(\overline{a^{(1)}_{i,i_1}}\right)\left(\overline{a^{(1)}_{i_1,i_2}}\right)\cdots\left(\overline{a^{(1)}_{i_{m-1},j}}\right)\right]=0,$$

y se tiene la libertad amalgamada. ∎

Aplicación. Consideremos las matrices de $3N\times 3N$:

$$X_N=\begin{pmatrix}A_N & B_N & C_N\\ B_N & A_N & B_N\\ C_N & B_N & A_N\end{pmatrix}\quad\text{y}\quad Y_N=\begin{pmatrix}D_N & D_N & E_N\\ E_N & F_N & D_N\\ F_N & F_N & D_N\end{pmatrix},$$

donde los bloques de X_N y de Y_N son libres (todos son libres). Veamos que X_N y Y_N son $M_3(\mathbb{C})$-libres.

En efecto, por hipótesis las álgebras $\langle A_N, B_N, C_N\rangle$ y $\langle D_N, E_N, F_N\rangle$ son $\mathbb{C}\mathbf{1}_{\mathcal{A}}$-libres. Ahora bien como X_1 y X_2 son respectivamente elementos de $M_3(\mathbb{C}) \otimes \langle A_N, B_N, C_N\rangle$ y $M_3(\mathbb{C}) \otimes \langle D_N, E_N, F_N\rangle$, por el teorema tenemos que son $M_3(\mathbb{C})$-libres.

La siguiente proposición será de utilidad en las siguientes secciones y puede encontrarse su demostración en [35].

Proposición 3.3. Sean $\mathcal{B} \subseteq A_1, A_2 \subseteq \mathcal{A}$ subálgebras $\mathcal{B}$-libres y sea $\mathcal{D} \subseteq M_N(\mathbb{C})\otimes\mathcal{B}$. Asuma que, individualmente, los momentos (análogamente los cumulantes) $M_N(\mathbb{C}) \otimes \mathcal{B}$-valuados de ambos $x \in M_N(\mathbb{C}) \otimes A_1$ y $y \in M_N(\mathbb{C}) \otimes A_2$, cuando se restringen los argumentos a $\mathcal{D}$, permanecen en $\mathcal{D}$. Entonces x y y son $\mathcal{D}$-libres.

Introducimos ahora otro teorema importante. Para ello, sea $\eta_x(b) = 1 - b(\mathbb{F}((b^{-1} - x)^{-1}))^{-1}$ y $\mathbb{H}^+(\mathcal{B}) := \{b \in \mathcal{B} : \exists\epsilon > 0 \text{ tal que } -i(b - b^*) \geq \epsilon \cdot 1\}$.

Teorema 3.13 (Teorema de subordinación multiplicativo)**.** Sea $x, y \in \mathcal{A}$ tales que $x > 0,\ y = y^*$ y sus esperanzas invertibles y libres sobre $\mathcal{B}$. Existe una aplicación Fréchet holomorfa $\omega_2 : \{b \in \mathcal{B} : Im(bx) > 0\} \to \mathbb{H}^+(\mathcal{B})$, tal que

- $\eta_y(\omega_2(b)) = \eta_{xy}(b),\ Im(bx) > 0$;
- $\omega_2(b)$ y $b^{-1}\omega_2(b)$ son analíticas alrededor de cero;
- para cualquier $b \in \mathcal{B}$ tal que $Im(bx) > 0$, la aplicación $g_b : \mathbb{H}^+(\mathcal{B}) \to \mathbb{H}^+(\mathcal{B})$, $g_b(w) = bh_x(h_y(w)b)$, donde
$$h_x(b) = b^{-1} - \mathbb{F}[(b^{-1} - x)^{-1}]^{-1},$$
está bien definida, es analítica y para cualquier $w \in \mathbb{H}^+(\mathcal{B})$ fijo,
$$\omega_2(b) = \lim_{n\to\infty} g_b^{\circ n}(w),$$
en la topología débil.

  Más aún, si definimos $\omega_1(b) := h_y(\omega_2(b))b$, entonces
$$\eta_{xy}(b) = \omega_2(b)\eta_x(\omega_1(b))\omega_2(b)^{-1},\ Im(bx) > 0.$$

Proposición 3.4. Sea $\mathcal{B}$ álgebra finito dimensional y $x > 0$, $y = y^*$ libres sobre $\mathcal{B}$. Existe una función $g : \{b \in \mathcal{B} : Im(bx) > 0\} \times \mathbb{H}^+(\mathcal{B}) \to \mathbb{H}^+(\mathcal{B})$ tal que

i) $\omega_2(b) = \lim_{n\to\infty} g_b^{\circ n}(w)$ existe, no depende de $w \in \mathbb{H}^+(\mathcal{B})$ y es analítica en $\{b \in \mathcal{B} : Im(bx) > 0\}$;

ii) Se tiene que
$$\eta_y(\omega_2(b)) = \eta_{xy}(b),\ b \in \{b \in \mathcal{B} : Im(bx) > 0\}.$$

Observación 3.10. Desde una perspectiva numérica, es sencillo pasar de h_x a G_x y por tanto, de la proposición anterior concluimos que sólo se necesitan las transformadas de Cauchy $\mathcal{B}$-valuadas individuales para obtener la transformada de Cauchy $\mathcal{B}$-valuada del producto xy y por tanto su distribución.

3.2.1 Espacios Rectangulares

Una *álgebra de von Neumann*, actuando en un espacio de Hilbert $\mathcal{H}$ es una subálgebra de $B(\mathcal{H})$ que contiene a la función identidad y es cerrada con la operación de tomar adjunto y es cerrado como conjunto en la topología débil inducida por las funcionales lineales $a \mapsto \langle a\xi, \eta\rangle, \xi, \eta \in \mathcal{H}$.

Definición 3.22. Un W^**-espacio de probabilidad* es un par $(\mathcal{A}, \tau)$, donde $\mathcal{A}$ es una álgebra de von Neumann en algún espacio de Hilbert complejo y τ es un funcional fiel, unitario, tracial, positivo y lineal.

Proposición 3.5. Sea $(\mathcal{A}, \tau)$ un W^*-EPNC y $P_1, \ldots, P_k \in \mathcal{A}$ proyecciones ortogonales que cumplen $\mathbf{1}_{\mathcal{A}} = P_1 + \cdots + P_k$ y denotemos por $\mathcal{D} = \langle P_1, \ldots, P_k\rangle$ la W^* álgebra generada. Entonces existe una única esperanza condicional $\mathbb{F} : \mathcal{A} \to \mathcal{D}$ compatible con τ y está dada por:

$$\mathbb{F}(a) = \sum_{i=1}^{k} \tau(P_i)^{-1}\tau(P_i a P_i)P_i.$$

Observación 3.11. En el espacio de matrices, la esperanza condicional anterior manda una matriz por bloques A (pensemos que con bloques del mismo tamaño) a la matriz por bloques que tiene en su diagonal los bloques de A y 0 fuera de la diagonal. Esta idea se puede generalizar y construir una esperanza condicional que manda a A a la matriz que tiene en un acomodo especifico bloques de A y en los demás ceros.

Esta idea de proyectar ortogonalmente puede pensarse como una propiedad análoga a que la esperanza condicional clásica de variables aleatorias cuadrado integrables son proyecciones en L^2.

Los espacios rectangulares permiten incluir las matrices rectangulares al estudio algebraico de la probabilidad libre.

Definición 3.23. A los EPVO $(\mathcal{A}, \tau, \mathbb{F}, \mathcal{D})$ del tipo de la proposición anterior se les llama *espacios rectangulares*.

Observación 3.12. Denotemos por $\mathcal{A}^{(i,j)} = \{a \in \mathcal{A} : a = P_i a Pj\}$ y $\mathcal{A}^{(i)} = \mathcal{A}^{(i,i)}$. A los elementos de $\bigcup_{1\le i,j\le k} \mathcal{A}^{(i,j)}$ los llamamos *simples*.

$(\mathcal{A}^{(i)}, \tau^{(i)})$ denota un espacio comprimido, con $\tau^{(i)}(a) = \tau(P_i)^{-1}\tau(a),\ a \in \mathcal{A}^{(i)}$.

Definición 3.24. Consideremos $(\mathcal{A}, \tau)$ un $(P_1, \ldots, P_k)$-espacio rectangular y sean $(\mathcal{A}_n, \tau_n)_{n\ge1}$ sucesión de $(P_1^n, \ldots, P_k^n)$-espacios rectangulares. Consideremos $a_1, \ldots a_m \in \mathcal{A}$ y $a_1^{(n)}, \ldots a_m^{(n)} \in \mathcal{A}_n$ elementos simples. Decimos que $(a_1^{(n)}, \ldots a_m^{(n)})$ *converge en* $\mathcal{D}$*-distribución* a $(a_1, \ldots a_m)$, si se cumple que $(a_1^{(n)}, \ldots a_m^{(n)}, P_1^{(n)}, \ldots, P_k^{(n)})$ converge en $*$-distribución a $(a_1, \ldots, a_m, P_1, \ldots, P_k)$ y escribimos

$$(a_1^{(n)}, \ldots a_m^{(n)}) \xrightarrow{\mathcal{D}} (a_1, \ldots a_m),\ \ n \to \infty.$$

Si $a_1, \ldots a_m$ son $\langle P_1, \ldots, P_k\rangle$-libres, decimos que $a_1^{(n)}, \ldots a_m^{(n)}$ son *asintóticamente* $\mathcal{D}$*-libres*.

Presentamos ahora, la versión general del teorema de asintoticidad libre de Voiculescu.

Teorema 3.14. [42, Prop. 2.5] Sea k fijo y $(\mathcal{A}_N, \tau_N)_{N\geq 1}$ sucesión de $(P_1^N, \ldots, P_k^N)$-espacios rectangulares de matrices aleatorias tal que $\tau_N(P_i^{(N)}) \to c_i \in (0,1], i = 1, \ldots, k$. Sean $(U_i^{(N)})_{i\geq 1}$ una colección de matrices aleatorias independientes simples en $\mathcal{A}_N$, cada $U_i^{(N)} \in \mathcal{A}_N^{j(i)}$ con distribución Haar unitario en el espacio comprimido $(\mathcal{A}_N^{j(i)}, \tau_N^{j(i)})$ para algún $1 \leq j(i) \leq k$.

Consideremos también $D_N = (D_i^{(N)})_{i\geq 1}$ una colección de matrices deterministicas simples tal que $D_i^{(N)} \in \mathcal{A}_N^{r(i),s(i)}$ para algunos $1 \leq r(i), s(i) \leq k$ y asuma que $(D_i^{(N)})_{i\geq 1}$ converge en $\mathcal{D}$-distribución. Entonces $D_N, U_1^{(N)}, U_2^{(N)}, \ldots$ son asintóticamente $\mathcal{D}$-libres.

Como aplicación del teorema anterior, se demuestra el siguiente teorema.

Teorema 3.15. [42, Teo. 2.7] Sea $(\mathcal{A}_N, \mathbb{E} \circ \frac{1}{N}Tr)$ espacio de matrices aleatorias de $N \times N$ con estructura de $(P_1^{(N)}, \ldots, P_k^{(N)})$-espacio rectangular con elementos simples $U_i^{(N)} \in \mathcal{A}_N^{(i)}$ tal que

i) $\lim_{N\to\infty} \frac{1}{N}Tr(P_i^{(N)}) = c_i > 0$,

ii) $U_1^{(N)}, \ldots, U_k^{(N)}$ tienen entradas independientes, cada U_i matriz aleatoria con distribución de Haar en el espacio comprimido $(\mathcal{A}_N^{(i)}, \tau_N^{(i)})$.

Sea $U_N = U_1^{(N)} + \cdots + U_k^{(N)}$ y sean

$$D_1^{(N)} = \{C_1^{(N)}, \ldots, C_p^{(N)}\} \quad D_2^{(N)} = \{D_1^{(N)}, \ldots, D_q^{(N)}\}$$

colecciones de matrices deterministicas, cada una con $\mathcal{D}$-distribución asintótica. Entonces $D_1^{(N)}$ y $U_N D_2^{(N)} U_N^*$ son asintóticamente D-libres.

Observación 3.13. Para fines de este trabajo usaremos una versión diferente del teorema anterior, en donde las U no necesariamente son Haar unitarias, pero sí de la forma

$$U = \begin{pmatrix} X & 0 \\ 0 & 0 \end{pmatrix}$$

donde X unitariamente invariante. La prueba es identica a la que puede verse en [42]. Se tiene que X es asintóticamente libre de las unitarias y por el teorema 3.12 se tiene la libertad amalgamada en las matrices evaluadas en las proyecciones en la diagonal, la cual se puede restringir a las proyecciones en la diagonal.

3.3 Modificaciones a Bloques

Hasta ahora, sabemos que el problema de detección de entrelazamiento cuántico en estados aleatorios queda resuelto con los siguientes criterios:

1. El estado X_d es separable si y sólo si $X_d^\varphi = (I \otimes \varphi)(X_d) \geq 0$ para todo φ positivo, es decir:

$$X_d = \begin{pmatrix} X_{11} & X_{12} & \cdots & X_{1d} \\ X_{21} & X_{22} & \cdots & X_{2d} \\ \vdots & \vdots & \ddots & \vdots \\ X_{d1} & X_{d2} & \cdots & X_{dd} \end{pmatrix} \in SEP \Leftrightarrow X_d^{\varphi} = \begin{pmatrix} \varphi(X_{11}) & \varphi(X_{12}) & \cdots & \varphi(X_{1d}) \\ \varphi(X_{21}) & \varphi(X_{21}) & \cdots & \varphi(X_{2d}) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi(X_{d1}) & \varphi(X_{d2}) & \cdots & \varphi(X_{dd}) \end{pmatrix} \geq 0.$$

Razón por la cual nos interesa encontrar la distribución asintótica, cuando $d \to \infty$ de matrices modificadas a bloques.

2. El criterio Peres-Horodecki: Si X_d es separable, entonces $(I \otimes T)(X_d) \geq 0$, donde T es la transpuesta.

En esta sección damos información del espectro asintótico de estas modificaciones.

3.3.1 Caso Wishart

Comenzamos analizando el caso en que X_d son matrices Wishart para la transpuesta parcial. Los resultados de este apartado son del artículo [8].

Recordemos que una matriz compleja W Wishart de parámetro (dn, dm) está definida por $(dm)^{-1}GG^*$, donde G es una matriz $dn \times dm$ con entradas i.i.d. $\mathbb{C}N(0,1)$.

Consideremos $W \in M_d(\mathbb{C}) \otimes M_n(\mathbb{C})$ matriz compleja Wishart de parámetro (dn, dm) y sea $W^{\Gamma} = (I_d \otimes T)(W)$, la transpuesta parcial. Nos interesa conocer la distribución asintótica de W^{Γ} y propiedades de la misma.

Teorema 3.16. Para todo $p \geq 1$, si $NC(p)$ son las particiones que no se cruzan de tamaño p, se cumple

$$M_p := \lim_{d\to\infty} (\mathbb{E} \circ tr)[(mW^{\Gamma})^p] = \sum_{\pi \in NC(p)} m^{\#\pi} n^{e(\pi)},$$

donde $\#\pi$ es el número de bloques de π y $e(\cdot)$ denota el número de bloques de tamaño par.

Observación 3.14. La demostración usa la fórmula de Wick y combinatoria de particiones que no se cruzan y puede encontrarse en [8].

Observemos que la función generadora de momentos (f.g.m.) de (mW^{Γ}) es $\Psi(x) = \sum_{p=0}^{\infty} M_p x^p$.

Teorema 3.17. La f.g.m. de (mW^{Γ}) satisface la siguiente ecuación funcional

$$(\Psi - 1)(1 - z^2\Psi^2) = mz\Psi(1 + nz\Psi).$$

Demostración. Si denotamos $N(p, b, e)$ el número de particiones en $NC(p)$ que tienen b bloques y e bloques de tamaño par, tenemos por el teorema anterior que

$$\Psi(z) = 1 + \sum_{p=1}^{\infty} \sum_{\pi \in NC(p)} m^{\#\pi} n^{e(\pi)} z^p = 1 + \sum_{p=1}^{\infty} \sum_{b=0}^{\infty} \sum_{e=0}^{\infty} z^p m^b n^e N(p, b, e).$$

Sea V_1 el bloque que contiene al 1, y r tal que $|V_1| = 1 + r$, entonces

$$N(p,b,e) = \sum_{r \text{ par}} \sum_{p=\sum p_i + r+1} \sum_{b=\sum b_i+1} \sum_{e=\sum e_i} \prod_{j=1}^{r+1} N(p_j, b_j, e_j)$$
$$+ \sum_{r \text{ impar}} \sum_{p=\sum p_i + r+1} \sum_{b=\sum b_i+1} \sum_{e=\sum e_i} \prod_{j=1}^{r+1} N(p_j, b_j, e_j),$$

donde $p_1, \ldots, p_{r+1}$ es el número de puntos entre los elementos de V_1, de tal forma que $p_1 + \cdots + p_{r+1} + r + 1 = p$. Sustituyendo este valor de $N(p,b,e)$ en nuestra expresión para Ψ y simplificando obtenemos:

$$\Psi - 1 = m \sum_{r \text{ par}} (z\Psi)^{r+1} + mn \sum_{r \text{ impar}} (z\Psi)^{r+1} = m \frac{z\Psi}{1 - z^2\Psi^2} + mn \frac{z^2\Psi^2}{1 - z^2\Psi^2} = mz\Psi \frac{1 + nz\Psi}{1 - z^2\Psi^2}.$$

■

Demostramos ahora el teorema principal de esta subsección.

Teorema 3.18. mW^{Γ} converge en distribución, cuando $d \to \infty$ a la diferencia libre de distribuciones poisson libre:

$$\mu_{m,n} = \pi_a \boxminus \pi_b,$$

donde $a = \frac{m(n+1)}{2}$ y $b = \frac{m(n-1)}{2}$.

Demostración. Por el teorema anterior ya tenemos la f.g.m de la distribución límite, Ψ. La transformada de Cauchy de tal distribución es $G(\xi) = \xi^{-1}\Psi(\xi^{-1})$ y su R-transformada es $R(z) = G^{\langle -1 \rangle}(z) - z^{-1}$.

Ahora bien, como

$$(\Psi - 1)(1 - z^2\Psi^2) = mz\Psi(1 + nz\Psi),$$

por las relaciones anteriores tenemos que cambiando $z \to \xi^{-1}$ y Ψ por ξG

$$(\xi G - 1)(1 - G^2) = mG(1 + nG),$$

que de nuevo al cambiar $\xi \to G^{\langle -1 \rangle}$ y $G \to z$ nos queda

$$(zG^{\langle -1 \rangle} - 1)(1 - z^2) = mz(1 + nz),$$

para finalmente cambiar $G^{\langle -1 \rangle} \to R + z^{-1}$ obteniendo

$$zR(1 - z^2) = mz(1 + nz),$$

despejando, tenemos que la R transformada de la distribución límite es

$$R(z) = \frac{m(1 + nz)}{1 - z^2} = \frac{m}{2}\left(\frac{n+1}{1-z} - \frac{n-1}{1+z}\right).$$

Por otro lado $R_{\pi_a}(z) = \frac{a}{1-z} = \frac{m}{2}\frac{n+1}{1-z}$ y por el comportamiento de la R-transformada en dilataciones $R_{-\pi_b} = -R_{\pi_b}(-z) = \frac{-b}{1+z} = -\frac{m}{2}\frac{n-1}{1+z}$, finalmente por la libertad nos queda

$$R_{\pi_a \boxminus \pi_b}(z) = R_{\pi_a} + R_{-\pi_b} = \frac{m(1+nz)}{1-z^2} = \frac{m}{2}\left(\frac{n+1}{1-z} - \frac{n-1}{1+z}\right),$$

de la igualdad se tiene el resultado. ∎

Enlistamos ahora algunas propiedades de la distribución límite de inmediata demostración.

Teorema 3.19. [8, Teo. 5.3] La distribución $\mu_{m,n}$ satisface lo siguiente.

1. Tiene media m y varianza mn.
2. Su transformada de Cauchy satisface la ecuación
$$(zG-1)(1-G^2) = mG(1+nG).$$
3. Su R transformada está dada por
$$R(z) = \frac{m(1+nz)}{1-z^2}.$$
4. Si $n = 1$ tenemos las leyes de Marchenko-Pastur, $\mu_{m,1} = \pi_m$.
5. Si $m = \alpha n \to \infty$ obtenemos las semicirculares del resultado de Aubrun.
6. Si $m = t/n \to 0$ obtenemos la distribución Bessel libre $\tilde{\pi}_{2,t}$.
7. Tiene a lo más un átomo en 0 de masa $\max(1-mn, 0)$.

Finalmente enunciamos el teorema que caracteriza los parámetros para los cuales el soporte de $\mu_{m,n}$ es positivo; de gran importancia para nuestros fines de detección de entrelazamiento.

Teorema 3.20. La medida $\mu_{m,n}$ tiene soporte positivo si y sólo si $m \geq 2$ y $n \leq m/4 + 1/m$.

Observación 3.15. Cabe mencionar que en el artículo [7] generalizan los resultados expuestos en esta subsección para φ's que cumplen ciertas condiciones planares, obteniendo el siguiente resultado:

Teorema 3.21. Sea $\tilde{W} = (I_d \otimes \varphi)(W)$, donde W es matriz Wishart compleja de parámetro (dn, dm) y $\varphi : M_n(\mathbb{C}) \to M_n(\mathbb{C})$ aplicación lineal autoadjunta que cumple "ciertas condiciones planares" con matriz asociada Λ. Entonces la distribución espectral asintótica de $\delta m\tilde{W}$ es $\pi_{1,mn\rho} \boxtimes \nu$, donde ρ es la medida uniforme en los eigenvalores de Λ, ν medida uniforme en los eigenvalores de D, $\delta = tr(D)$, con $D = \varphi(1)$ y $\pi_{1,mn\rho}$ es la distribución poisson compuesta con tasa 1 y medida de saltos $mn\rho$.

3.3.2 Solución General

Solucionamos en esta sección el problema general de encontrar la distribución asintótica de la matriz $X_d^\varphi := [I_d \otimes \varphi](X_d) \in M_d(\mathbb{C}) \otimes M_n(\mathbb{C})$, cuando $d \to \infty$, en el caso general $\varphi : M_m(\mathbb{C}) \to M_n(\mathbb{C})$ positivo autoadjunto y $X_d \in M_d(\mathbb{C}) \otimes M_m(\mathbb{C})$ matriz aleatoria autoadjunta y unitariamente invariante.

Recordemos que la matriz de Choi de la aplicación φ es

$$C := C_\varphi = \sum_{i,j=1}^{m} E_{ij} \otimes \varphi(E_{ij}) \in M_m(\mathbb{C}) \otimes M_n(\mathbb{C}),$$

donde (E_{ij}) la base estándar de $M_m(\mathbb{C})$ (la cual, como vimos en el ejemplo 3.4, forma una familia de unidades matriciales).

Observación 3.16. Algunas propiedades de la matriz de Choi que cabe destacar es que, como se mencionó en la prueba del Teorema 1.5, si φ es autoadjunta entonces C_φ también es autoadjunta, y por tanto si denotamos por $c_{ij} \in M_n(\mathbb{C})$ a los bloques de C, se cumple que $c_{kl}^{ij} = \bar{c}_{ji}^{lk}$. Usaremos la notación C_{ijkl} para denotar a C_{kl}^{ij}, el elemento ij del bloque kl.

Proposición 3.6. Sea C la matriz de Choi de φ y $c_{ijkl} = \langle E_{il} \otimes E_{jk}, C \rangle$ (el elemento ij del bloque kl). Entonces se tiene la siguiente descomposición,

$$X_d^\varphi = [I_d \otimes \varphi](X_d) = \sum_{i,l=1}^{n} \sum_{j,k=1}^{m} c_{ijkl} (I_d \otimes E_{ij}) X_d (I_d \otimes E_{kl}) \in M_d(\mathbb{C}) \otimes M_n(\mathbb{C}).$$

La siguiente observación es crucial para este trabajo.

Observación 3.17. Para el caso cuadrado $m = n$, se cumple lo siguiente.

1. La distribución conjunta de $(I_d \otimes E_{ij})_{i,j \le m}$ respecto a τ_{md}, no depende de d:

$$\begin{aligned}
\tau_{dm}((I_d \otimes E_{i_1,j_1}) \cdots (I_d \otimes E_{i_k,j_k})) &= \tau_{dm}(I_d \otimes (\delta_{j_1,i_2} \cdots \delta_{j_{k-1},i_k} E_{i_1,j_k})) \\
&= \frac{1}{dm} Tr(I_d) \cdot Tr(\delta_{j_1,i_2} \cdots \delta_{j_{k-1},i_k} E_{i_1,j_k}) \\
&= \tau_m(\delta_{j_1,i_2} \cdots \delta_{j_{k-1},i_k} E_{i_1,j_k}) \\
&= \frac{1}{m} \delta_{j_1,i_2} \cdots \delta_{j_{k-1},i_k} \delta_{i_1,j_k} \\
&= \tau(e_{i_1,j_1} \cdots e_{i_k,j_k}),
\end{aligned}$$

donde (e_{ij}) son unidades matriciales del EPNC $(\mathcal{A}, \tau)$ que cumple $M_m(\mathbb{C}) \subset \mathcal{A}$ y $\tau|_{M_m(\mathbb{C})} = \tau_m$. Se tiene por tanto que las matrices deterministicas $(I_d \otimes E_{11}, \ldots, I_d \otimes E_{mm})$ convergen en distribución conjunta a $(e_{11}, \ldots, e_{mm})$.

2. Si X_d es matriz autoadjunta $md \times md$ y es GUE, Wishart o aleatoriamente rotada que cumple $\lim_{d\to\infty} \tau_{dm}(X_d^k) = \tau(x^k)$, para algúna variable x en un EPNC $(\mathcal{A}, \tau)$, entonces por la observación anterior y el Teorema 3.5 de libertad asintótica de Voiculescu, tenemos que

$$(X_d, I_d \otimes E_{11}, \ldots, I_d \otimes E_{mm}) \to (x, e_{11}, \ldots, e_{mm}),$$

donde x y $\langle e_{ij} : i, j \leq m\rangle$ son libres.

Las observaciones anteriores, demuestran la siguiente proposición.

Proposición 3.7. Consideremos el caso en que $m = n$. La distribución límite, cuando $d \to \infty$, de $X_d^{\varphi} = \sum_{i,j,k,l}^{m} c_{ijkl}(I_d \otimes E_{ij})X_d(I_d \otimes E_{kl})$, es la misma distribución que la del elemento

$$x^{\varphi} := \sum_{i,j,k,l}^{m} c_{ijkl} e_{ij} x e_{kl},$$

donde $(e_{ij})_{i,j\leq m}$ unidades matriciales libres de x, todas las variables en algún espacio $(\mathcal{A}, \tau)$.

El caso rectangular, $m \neq n$ requiere el uso de los espacios rectangulares que definimos en la sección pasada. Como X_d y X_d^{φ}, no son de la misma dimensión, pensaremos en identificarlos con bloques de matrices más grandes, tal que las matrices nuevas tengan la misma dimensión, como se muestra a continuación. Definimos $\hat{X}_d$ y $\hat{X}_d^{\varphi}$ como sigue,

$$\hat{X}_d = \begin{vmatrix} X_d & 0_{m\times n} \otimes I_d \\ 0_{n\times m} \otimes I_d & 0_{n\times n} \otimes I_d \end{vmatrix},$$
$$\hat{X}_d^{\varphi} = \begin{vmatrix} 0_{m\times m} \otimes I_d & 0_{m\times n} \otimes I_d \\ 0_{n\times m} \otimes I_d & X_d^{\varphi} \end{vmatrix} = \sum_{i,l=1}^{n}\sum_{j,k=1}^{m} c_{ijkl}(E_{m+i,j} \otimes I_d)\hat{X}_d(E_{k,m+l} \otimes I_d).$$

Cada uno de los anteriores es una matriz $d(m+n) \times d(m+n)$. En este caso, también tenemos que $(I_d \otimes E_{11}, \ldots, I_d \otimes E_{(m+n)(m+n)})$ converge en distribución conjunta a $(e_{11}, \ldots, e_{(m+n)(m+n)})$ (unidades matriciales en un EPNC). Definimos ahora las proyecciones

$$P_{d,m} = \sum_{i\leq m} I_d \otimes E_{ii}, \quad P_{d,n} = \sum_{i=m+1}^{m+n} I_d \otimes E_{ii},$$

y

$$p_m = \sum_{i\leq m} e_{ii}, \quad p_n = \sum_{i=m+1}^{m+n} e_{ii},$$

se tiene que $\tau(p_m) = \frac{m}{n+m}$ y $\tau(p_n) = \frac{n}{n+m}$. Se cumplen todas las hipótesis de la Observación 3.13, y por lo tanto

$$(X_d, I_d \otimes E_{11}, \ldots, I_d \otimes E_{(m+n)(m+n)})$$

converge en distribución conjunta a

$$(x, e_{11}, \ldots, e_{(m+n)(m+n)}),$$

donde x y $\langle e_{ij} : i, j \leq m+n \rangle$ son $\langle p_n, p_m \rangle$-libres.

Lo anterior prueba el siguiente teorema.

Proposición 3.8. La distribución límite, cuando $d \to \infty$, de $\hat{X}_d^{\varphi} = \sum_{i,l=1}^{n} \sum_{j,k=1}^{m} c_{ijkl}(E_{m+i,j} \otimes I_d)\hat{X}_d(E_{k,m+l} \otimes I_d)$ es la misma que la de $\hat{x}^{\varphi} \in \mathcal{A}$ de la forma

$$\hat{x}^{\varphi} = \sum_{i,l=1}^{n} \sum_{j,k=1}^{m} c_{ijkl} e_{m+i,j} \hat{x} e_{k,m+l},$$

donde $\hat{x}$ y la familia de unidades matriciales $(e_{ij})_{i,j=1}^{m+n}$ son libres con amalgamación sobre $\langle p_m, p_n \rangle$, donde

$$p_m = \sum_{i \leq m} e_{ii}, \quad p_n = \sum_{i=m+1}^{m+n} e_{ii},$$

y se cumple que $\tau(p_m) = \frac{m}{n+m}$ y $\tau(p_n) = \frac{n}{n+m}$.

Corolario 3.2. En términos de la proposición anterior, si μ es la distribución límite de X_d, entonces la distribución de $\hat{x}$ es $\frac{m}{m+n}\mu + \frac{n}{m+n}\delta_0$, y en particular X_d^{φ} converge en distribución a una variable cuya distribución en el sentido analítico es μ^{φ}, que es la medida que cumple que $\hat{x}^{\varphi}$ tiene distribución $\frac{m}{m+n}\delta_0 + \frac{n}{m+n}\mu^{\varphi}$.

Observación 3.18. En el último ejemplo identificamos las matrices que nos interesaban analizar en espacios más grandes, pero después de que los espacios grandes nos permitieron usar los teoremas conocidos, nos devolvemos a nuestro problema inicial que era calcular la distribución espectral límite de X_d^{φ}.

Puede verse que, en la Proposición 3.8, la variable $\hat{x}$ y la familia de unidades matriciales $(e_{ij})_{i,j=1}^{m+n}$ no son $\mathbb{C}$-libres, ya que si lo fueran entonces

$$\tau(x^2 e_{(m+1)(m+1)}) = \tau(x^2)\tau(e_{(m+1)(m+1)}) = \tau(x^2)\tau(e_{ii}) = \frac{1}{m+n}\tau(x^2),$$

pero $x^2 e_{(m+1)(m+1)} = 0$ y por tanto, implicamos que

$$\tau(x^2) = 0;$$

sin embargo, esto no pasa a menos que $x = 0$. La razón por la que el teorema escalar de Voiculescu (Teorema 3.5) no aplica es por que la nueva matriz $\hat{X}_d$ no es unitariamente invariante a pesar de que sus bloques sí lo sean.

Solución Numérica General

Consideremos el caso cuadrado, $n = m$. Ya tenemos que la distribución límite de X_d^{φ} es la misma que la de

$$x^{\varphi} := \sum_{i,j,k,l}^{m} c_{ijkl} e_{ij} x e_{kl},$$

donde $(e_{ij})_{i,j\leq m}$ unidades matriciales libres de x. Cabe mencionar que los sumandos de la expresión anterior no necesariamente son libres (de hecho en algunos casos los sumandos conmutan), por tanto, para aproximar la distribución de ese elemento utilizaremos el teorema de subordinación multiplicativa el cual, sin embargo, funciona para productos ab, donde $a \geq 0$ y $b = b^*$. Pondrémos a x^{φ} en estos términos. Recordemos que $c_{kl}^{ij} = c_{ijkl}$ es el elemento ij del bloque kl y que por ser C autoadjunta se tiene que $c_{kl}^{ij} = \bar{c}_{ji}^{lk}$. Si hacemos $re^{i\theta} = c_{kl}^{ij}$, entonces para $(i,j) < (l,k)$:

$$re^{i\theta} e_{ij} x e_{kl} + re^{-i\theta} e_{lk} x e_{ji} = r^{1/2}(e^{i\theta/2} e_{ij} + e^{-i\theta/2} e_{lk}) x r^{1/2}(e^{-i\theta/2} e_{ji} + e^{i\theta/2} e_{kl}) - re_{ij} x e_{ji} - re_{lk} x e_{kl},$$

por tanto si hacemos $f_{kl}^{ij} = r^{1/2}(e^{i\theta/2} e_{ij} + e^{-i\theta/2} e_{lk})$, tenemos

$$re^{i\theta} e_{ij} x e_{kl} + re^{-i\theta} e_{lk} x e_{ji} = (f_{kl}^{ij}) x (f_{kl}^{ij})^* - re_{ij} x e_{ji} - re_{lk} x e_{kl},$$

y esto se puede hacer para cada $(i,j) < (l,k)$ (donde los r y θ dependen de $ijkl$). Ahora bien, para el caso $(i,j) = (l,k)$, los coeficientes son reales y entonces $\theta = 0$ o $\theta = \pi$, por tanto el término $(f_{kl}^{ij}) x (f_{kl}^{ij})^* - re_{ij} x e_{ji} - re_{lk} x e_{kl}$ se vuelve:

$$4re_{ij} x e_{ji} - re_{ij} x e_{ji} - re_{ij} x e_{ji} = 2re_{ij} x e_{ji},$$

en el caso $\theta = 0$ y $-2re_{ij} x e_{ji}$ en el caso $\theta = \pi$. Analicemos primeramente el siguiente término,

$$\begin{aligned} T_1 :&= \sum_{(i,j)<(l,k)} -r_{ijkl}[e_{ij} x e_{ji} + e_{lk} x e_{kl}] = \sum_{i,j=1}^{m} \sum_{l=i}^{m} \sum_{k=j}^{m} -r_{ijkl} e_{ij} x e_{ji} + \sum_{i,j=1}^{m} \sum_{l=i}^{m} \sum_{k=j}^{m} -r_{ijkl} e_{lk} x e_{kl} \\ &= \sum_{i,j=1}^{m} e_{ij} x e_{ji} \sum_{l=i}^{m} \sum_{k=j}^{m} -r_{ijkl} + \sum_{l,k=1}^{m} \sum_{i=1}^{l} \sum_{j=1}^{k} -r_{ijkl} e_{lk} x e_{kl}, \end{aligned}$$

si llamamos $h_{ij} = \sum_{l=i}^{m} \sum_{k=j}^{m} r_{ijkl}$ y $q_{lk} = \sum_{i=1}^{l} \sum_{j=1}^{k} r_{ijkl}$, tenemos que

$$T_1 = -\left[\sum_{i,j=1}^{m} h_{ij} e_{ij} x e_{ji} + \sum_{l,k=1}^{m} q_{kl} e_{lk} x e_{kl} \right] = -\sum_{i,j=1}^{m} (h_{ij} + q_{ij}) e_{ij} x e_{ji}.$$

Por otro lado si $(i,j) = (l,k)$, llamamos θ_{ij} y r_{ij} al argumento y módulo de c_{ji}^{ij}, definimos

$$T_2 = \sum_{\substack{i,j\leq m,\\ \theta_{ij}=0}} 2r_{ij}e_{ij}xe_{ji} + \sum_{\substack{i,j\leq m,\\ \theta_{ij}=\pi}} -2r_{ij}e_{ij}xe_{ji}.$$

Por lo anterior, si hacemos

$$f_{ij} = \begin{cases} (2r_{ij} + h_{ij} + q_{ij})^{1/2}e_{ij}, \text{ si } \theta_{ij} = \pi, \\ (2r_{ij} - h_{ij} - q_{ij})^{1/2}e_{ij}, \text{ si } \theta_{ij} = 0, \end{cases} \quad \text{y} \quad \epsilon(i,j) = \begin{cases} 1, \text{ si } \theta_{ij} = \pi, \\ 0, \text{ si } \theta_{ij} = 0, \end{cases}$$

entonces

$$\begin{aligned} T_1 + T_2 &= \sum_{i,j=1}^{m} -(h_{ij} + q_{ij})e_{ij}xe_{ji} + \sum_{\substack{i,j\leq m,\\ \theta_{ij}=0}} 2r_{ij}e_{ij}xe_{ji} + \sum_{\substack{i,j\leq m,\\ \theta_{ij}=\pi}} -2r_{ij}e_{ij}xe_{ji} \\ &= \sum_{\substack{i,j\leq m,\\ \theta_{ij}=0}} (2r_{ij} - h_{ij} - q_{ij})e_{ij}xe_{ji} + \sum_{\substack{i,j\leq m,\\ \theta_{ij}=\pi}} -(2r_{ij} + h_{ij} + q_{ij})e_{ij}xe_{ji} \\ &= \sum_{i,j=1}^{m} f_{ij}(-1)^{\epsilon(i,j)}xf_{ij}^{*} \end{aligned}$$

Finalmente definimos,

$$f_{kl}^{ij} = \begin{cases} r_{ijkl}^{1/2}(e^{i\theta/2}e_{ij} + e^{-i\theta/2}e_{lk}), \text{ si } (i,j) < (l,k), \\ \frac{1}{\sqrt{2}}f_{ij}, \text{ si } (i,j) = (l,k), \end{cases} \quad \text{y } \varepsilon_{kl}^{ij} = \begin{cases} 1, \text{ si } (i,j) < (l,k), \\ (-1)^{\epsilon(i,j)}, \text{ si } (i,j) = (l,k), \end{cases}.$$

Usando todo lo anterior tenemos que

$$x^{\varphi} = \sum_{i,j,k,l}^{m} c_{ijkl}e_{ij}xe_{kl} = \sum_{(i,j)\leq(l,k)}^{m} [c_{kl}^{ij}e_{ij}xe_{kl} + \overline{c_{kl}^{ij}}e_{lk}xe_{ji}] = \sum_{\substack{1\leq i,j,k,l\leq m\\ (i,j)<(l,k)}} (f_{kl}^{ij})x(f_{kl}^{ij})^{*} + T_1 + T_2$$

$$= \sum_{\substack{1\leq i,j,k,l\leq m\\ (i,j)<(l,k)}} (f_{kl}^{ij})x(f_{kl}^{ij})^{*} + \sum_{i,j=1}^{m} f_{ij}(-1)^{\epsilon(i,j)}xf_{ij}^{*} = \sum_{\substack{1\leq i,j,k,l\leq m\\ (i,j)\leq(l,k)}} (f_{kl}^{ij})\varepsilon_{kl}^{ij}x(f_{kl}^{ij})^{*}.$$

Del desarrollo anterior queda probado el siguiente teorema,

Teorema 3.22. Sea $N := \frac{m^2(m^2+1)}{2}$ y f el vector de dimensión N,

$$f = (f_{11}^{11}, f_{12}^{11}, \ldots, f_{mm}^{mm}),$$

sea también $\Sigma = diag(\varepsilon_{11}^{11}, \varepsilon_{12}^{11}, \ldots, \varepsilon_{mm}^{mm})$. Entonces

$$x^{\varphi} = f\tilde{x}f^*,$$

donde $\tilde{x} = \Sigma \otimes x$.

Observación 3.19. Los elementos $f\tilde{x}f^*$ y $f^*f\tilde{x}$ tienen el mismo rango, pero el primer término es de dimensión 1 y el segundo es de dimensión N, por lo que tienen diferente kernel, es decir, el elemento $f\tilde{x}f^*$ es de rango completo, mientras que $f^*f\tilde{x}$ tiene nulidad $N-1$, lo que implica que este último tiene eigenvalor 0 con multiplicidad $N-1$.

Por lo anterior, $f^*f\tilde{x}$ tiene distribución espectral $(1-1/N)\delta_0+1/N\mu$ donde μ es la distribución de $f\tilde{x}f^*$. Concluimos que los elementos $f^*f\tilde{x}$ y $f\tilde{x}f^*$ **tienen la misma distribución salvo una masa en cero** pero, en el C^*-EPNC $(M_N(\mathbb{C}) \otimes \mathcal{A}, tr_N \otimes \tau)$.

De la observación anterior y del hecho que los bloques de $\tilde{x}$ son elementos de la álgebra $\langle x \rangle$ y los bloques de f^*f son elementos de la álgebra $\langle e_{ij} \rangle$, tenemos que los bloques de $\tilde{x}$ y los de f^*f son libres. Como resultado del Teorema 3.12, $\tilde{x}$ y f^*f son libres con amalgamación sobre $\mathcal{B} = M_N(\mathbb{C})$ con la esperanza condicional $\mathbb{F} = I_N \otimes \tau$. Además, lo dicho en la observación 3.9 nos permite calcular las transformadas de Cauchy $\mathcal{B}$-valuadas de $\tilde{x}$ y f^*f y como $\tilde{x}$ es autoadjunto y $f^*f > 0$, podemos aplicar entonces el teorema de subordinación multiplicativa y la Observación 3.10 para calcular la transformada de Cauchy $\mathcal{B}$-valuada de $f^*f\tilde{x}$ obteniendo por tanto una aproximación para la distribución de x^{φ}.

De una manera análoga, cuidando los índices, se puede desarrollar el caso rectangular, $m \neq n$.

Observación 3.20. Hacemos ahora dos observaciones importantes.

1. Los resultados hasta ahora no habrían sido posibles si la matriz de Choi no fuera determinística; plantear un enfoque en que los funcionales fueran aleatorios no nos permitiría usar el teorema de asintoticidad libre de Voiculescu (Teorema 3.5) a menos que tuvieramos casos triviales; pero aún en esos casos, no habríamos podido concluir lo anterior ya que tanto el elemento $\tilde{x}$ como f^*f dependen de los elementos de la matriz de Choi de una manera no trivial.

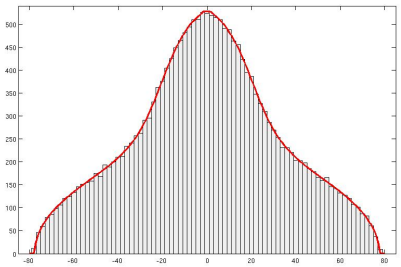
2. En el desarrollo anterior obtuvimos una descomposición para x^{φ} que salvo una masa en cero tiene la misma distribución que el producto $(f^*f)\tilde{x}$; sin embargo, eso no es suficiente para calcular la S-transformada valuada en operadores con el objetivo de dar la distribución analítica de x^{φ}. Para obtener la distribución de dicho elemento, en la sección 3.3.2 se encontrará otra descomposición de dicho elemento pero en términos del espectro de la matriz de Choi; dicha descomposición será de la misma forma que la actual, pero los factores serán libres sobre álgebras conmutativas, lo que nos permitirá calcular la transformada S y obtener una expresión analítica.

Simulaciones

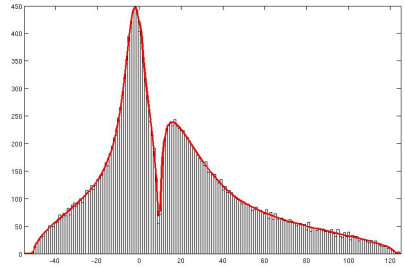
Para ejemplificar el resultado anterior consideremos la aplicación $\varphi : M_2(\mathbb{C}) \to M_2(\mathbb{C})$ definida por

$$\varphi((a_{ij})_{i,j\leq 2}) = \begin{pmatrix} 11a_{11} + 15a_{22} - 25a_{12} - 25a_{21} & 36a_{21} \\ 36a_{12} & 11a_{11} - 4a_{22} \end{pmatrix}.$$

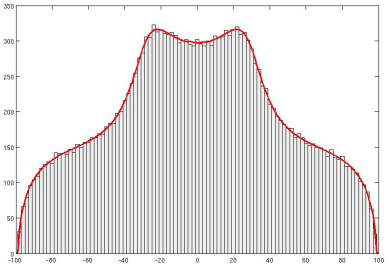
Si consideramos X_d sucesión de matrices unitariamente invariantes con distribución espectral límite Wigner, Marchenko-Pastur o si X_d es una arcoseno rotada aleatoriamente, podemos obtener (usando lo discutido en la sección pasada) aproximaciones para la distribución asintótica de la modificación a bloques. En los siguientes gráficos se muestran histogramas de X_d^{φ} en los tres casos mencionados y en línea sólida la aproximación que nos da la subordinación para esos tres casos; dichos gráficos pueden encontrarse en [3].



Caso Wigner



Caso Marchenko-Pastur



Caso Arcoseno Rotada Aleatoriamente

Solución Analítica

La solucíon numérica general que obtuvimos en la sección pasada considera aplicaciones φ autoadjuntas y positivas. En el presente apartado damos una expresión analítica para la distribución asintótica de las modificaciones a bloques, es decir, para la distribución de x^{φ}, y para ello consideraremos aplicaciones φ que cumplan ciertas condiciones técnicas.

Observación 3.21. De las expresiones para x^{φ} y $\hat{x}^{\varphi}$, parece importante conocer la distribución de los bloques de la matriz x, $x_{ij} = e_{1i}xe_{j1}$, sin embargo, esto no es sencillo en general. Usando el teorema 3.7 tenemos una expresión para los cumulantes de los bloques en términos de los

cumulantes de la matriz; dicha expresión implica que si $\pi \in NC(k)$,

$$R_\pi^{\tau_{11}}(x_{i_1,j_1},\dots,x_{i_k,j_k}) = m^{-(k-|\pi|)} R_\pi(x,\dots,x),$$

siempre que se satisfaga la condición cíclica $j_{v_1} = i_{v_2},\dots,j_{v_{|V|}} = i_{v_1}$ para cada bloque $V = \{v_1,\dots,v_{|V|}\} \in \pi$ y cero en otro caso.

Por lo anterior la distribución de x^φ será la misma que la de

$$\sum_{i,j\leq m} c_{ij} \otimes x_{ij} \in M_n(\mathbb{C}) \otimes \mathcal{A}_{11}$$

respecto al funcional $\phi = tr_n \otimes \tau_{11}$. Los momentos de x^φ están dados por

$$\begin{aligned}
\varphi((x^\varphi)^k) &= \sum_{i_1,j_1,\dots,i_k,j_k=1}^{n} \phi((c_{i_1,j_1} \otimes x_{i_1,j_1}) \cdots (c_{i_k,j_k} \otimes x_{i_k,j_k})) \\
&= \sum_{i_1,j_1,\dots,i_k,j_k=1}^{n} tr_n(c_{i_1,j_1} \cdots c_{i_k,j_k}) \tau_{11}(x_{i_1,j_1} \cdots x_{i_k,j_k}) \\
&= \sum_{i_1,j_1,\dots,i_k,j_k=1}^{n} tr_n(c_{i_1,j_1} \cdots c_{i_k,j_k}) \sum_{\pi\in NC(n)} R_\pi^{\tau_{11}}(x_{i_1,j_1},\dots,x_{i_k,j_k}).
\end{aligned}$$

Se tiene por tanto que los bloques de la matriz de Choi y los de x interactuan de manera no trivial, pues las expresiones anteriores no tienen expresión cerrada para casos generales. El objetivo de esta parte es encontrar condiciones en la matriz de Choi que permitan calcular la distribución de x^φ de manera explícita.

Para obtener las condiciones adecuadas para la matriz de Choi, que nos permitan obtener la solución analítica, establecemos algunos resultados preliminares.

Lema 3.1. Considere la descomposición espectral de la matriz de Choi,

$$C = \sum_{s=1}^{mn} \lambda_s v_s v_s^* = \sum_{t=1}^{r} \rho_t P_t,$$

donde $\lambda_s \in \mathbb{R}$ son los eigenvalores, $v_s \in \mathbb{C}^n \otimes \mathbb{C}^m$, r es el rango de C y los operadores P_t es el proyector al eigenespacio asociado al eigenvalor no cero ρ_t. Entonces para todo $i,j,k,l = 1,\dots,m$, se cumple

$$c_{ijkl} = \langle E_{i1} \otimes E_{jk}, C\rangle = \sum_{s=1}^{mn} \lambda_s \langle E_i \otimes E_j, v_s\rangle \overline{\langle E_l \otimes E_k, v_s\rangle},$$

con $(E_i)_{i=1}^r$ base estándar de $\mathbb{C}^r$.

Vimos en la solución numérica general de la sección anterior que x^φ tiene una descomposición del tipo $f^*\tilde{x}f$ en función de la parte polar de los elementos de C_φ. La siguiente proposición nos

da una expresión parecida pero en términos de la descomposición espectral de C, con miras a encontrar las condiciones en φ que nos permitan dar resultados analíticos.

Proposición 3.9. La variable modificada a bloques $\hat{x}^{\varphi}$ tiene la siguiente expresión en términos de los eigenvalores y eigenvectores de la matriz de Choi:

$$\hat{x}^{\varphi} = f^*(\hat{x} \otimes C)f,$$

donde $f = \sum_{s=1}^{mn} w_s^* \otimes v_s \in \mathcal{A} \otimes M_{nm}(\mathbb{C})$ y la variable $w_s \in \mathcal{A}$ es

$$w_s = \sum_{i=1}^{n}\sum_{j=1}^{m} \langle E_i \otimes E_j, v_s\rangle e_{m+i,j}.$$

Demostración. Usaremos la expresión que tenemos para c_{ijkl}. Se tiene que

$$\begin{aligned}
\hat{x}^{\varphi} &= \sum_{i,l=1}^{n}\sum_{j,k=1}^{m} c_{ijkl} e_{m+i,j}\hat{x}e_{k,m+l} = \sum_{i,l=1}^{n}\sum_{j,k=1}^{m} c_{ijkl} e_{m+i,j}\hat{x}e_{m+l,k}^* \\
&= \sum_{i,l=1}^{n}\sum_{j,k=1}^{m}\sum_{s=1}^{mn} \lambda_s \langle E_i \otimes E_j, v_s\rangle \overline{\langle E_l \otimes E_k, v_s\rangle} e_{m+i,j}\hat{x}e_{m+l,k}^* \\
&= \sum_{s=1}^{mn} \lambda_s w_s \hat{x} w_s^*,
\end{aligned}$$

por otro lado,

$$f^*(\hat{x} \otimes C)f = \sum_{s=1}^{r}\sum_{l=1}^{r} w_s \hat{x} w_l^* \otimes v_s^* C v_l,$$

y usando la ortogonalidad de los eigenvectores v_s se tiene $f^*(\hat{x} \otimes C)f = \sum_{s=1}^{r} \lambda_s w_s \hat{x} w_s^*$, lo que concluye la prueba. ∎

Observación 3.22. La aplicación $\Phi : \mathbb{C}^n \otimes \mathbb{C}^n \to M_n(\mathbb{C})$ definida como sigue, es un isomorfismo.

$$\Phi(v_s) = \sum_{i,j=1}^{n} \langle E_i \otimes E_j, v_s\rangle E_{ij},$$

más aún, es una isometría de $(\mathbb{C}^n \otimes \mathbb{C}^n, \|\cdot\|_2)$ a $(M_n(\mathbb{C}), \|\cdot\|_{FR})$, con

$$\|A\|_{FR} = Tr(AA^*),$$

la norma de Frobenius. Usando esta aplicación, podemos definir

$$\tilde{w_s} = \Phi(v_s),$$

y podemos demostrar que en el caso cuadrado, tenemos la siguiente factorización

$$X_d^{\varphi} = \sum_{s=1}^{n^2} \lambda_s (I_d \otimes w_s) X_d (I_d \otimes w_s^*). \tag{3.5}$$

Observación 3.23. Establezcamos algo de notación. Para cada ρ_t en el espectro de C, sea $J_t \subseteq \{1, \ldots, nm\}$ el conjunto de índices para los eigenvectores v_j que aparecen en el eigenproyector P_t

$$P_t = \sum_{j \in J_t} v_j v_j^*.$$

Se define también $Q_t := \sum_{j \in J_t} w_j w_j^* \in \mathcal{A}$ y observemos que $C \in \langle P_1, P_2, \ldots, P_r \rangle$, donde r es el rango de la matriz C_{φ}.

Si llamamos $h_{ij}^{(s)} = \langle E_i \otimes E_j, v_s \rangle$ y $H^{(s)} = (h_{ij}^s)_{ij} \in M_{n \times m}$, tenemos las siguientes igualdades

$$w_s = \left[\begin{array}{c|c} 0 & 0 \\ \hline H_s & 0 \end{array}\right] \quad \text{y} \quad w_s^* = \left[\begin{array}{c|c} 0 & H_s^* \\ \hline 0 & 0 \end{array}\right].$$

Además, tenemos que $H_s H_s^* \in M_n$ y la siguiente igualdad para Q_t

$$Q_t = \sum_{s \in J_t} w_s w_s^* = \left[\begin{array}{c|c} 0 & 0 \\ \hline 0 & \sum_{s \in J_t} H_s H_s^* \end{array}\right]$$

Ahora bien, ya tenemos de la proposición anterior que $\hat{x}^{\varphi} = f^*(\hat{x} \otimes C) f$, definimos la variable

$$y = (\hat{x} \otimes C) f f^*.$$

Si obtenemos la distribución de y, podemos obtener la distribución de $\hat{x}^{\varphi}$, via la relación

$$\tau[(\hat{x}^{\varphi})^k] = nm \cdot \mathbb{E}[y^k],$$

esto ya que y y $\hat{x}^{\varphi}$ tienen la misma distribución pero viven en diferentes espacios, por lo que cambia la normalización.

Proposición 3.10. En términos de la notación establecida, se cumple que

$$\Psi_{\hat{x}^{\varphi}}^{\mathbb{C}} = r \Psi_y^{\mathbb{C}},$$

donde r es el rango de la matriz de Choi de φ.

Definimos ahora una condición técnica para las transformaciones φ.

Definición 3.25. Decimos que los eigenespacios de C_φ son *tracialmente bien portados* (TWB) si para todo $i_1, \ldots, i_k \leq r = rank(C_\varphi)$, se tiene que

$$\tau(w_{j_1} w_{j_2}^* Q_{i_1} \cdots Q_{i_k}) = \delta_{j_1 j_2} \tau(w_{j_1} w_{j_1}^* Q_{i_1} \cdots Q_{i_k}) = \delta_{j_1 j_2} \tau(w_{j_1'} w_{j_2'}^* Q_{i_1} \cdots Q_{i_k}),$$

para todo $j_1, j_1', j_2 \leq mn$ tal que $j_1, j_1' \in J_i$ para algún $i \leq r$. Equivalentemente se cumple TWB si

$$\tau_n(w_{j_1} w_{j_2}^* Q_{i_1} \cdots Q_{i_k}) = \delta_{j_1 j_2} \tau_n(w_{j_1} w_{j_1}^* Q_{i_1} \cdots Q_{i_k}) = \delta_{j_1 j_2} \tau_n(w_{j_1'} w_{j_2'}^* Q_{i_1} \cdots Q_{i_k}),$$

donde $\tau_n(a) = \frac{1}{n}\tau(p_n a p_n)$.

Teorema 3.23. Sea $\varphi : M_m(\mathbb{C}) \to M_n(\mathbb{C})$ con matriz de Choi $C = C_\varphi \in M_{nm}(\mathbb{C})$ en $\mathcal{A} \otimes M_{nm}(\mathbb{C})$ que tiene eigenespacios tracialmente bien portados. Entonces las variables $\hat{x} \otimes C$ y ff^* son libres con amalgamación sobre el álgebra (conmutativa) $\mathcal{B} = \langle p_m, p_n \rangle \otimes \langle P_1, \ldots, P_r \rangle$.

Demostración. De la proposición 3.8, tenemos que $\hat{x}$ y $\{e_{ij}\}$ son libres con amalgamación sobre $\langle p_m, p_n \rangle$, donde la esperanza condicional es

$$\psi(a) = \frac{1}{\tau(p_m)} \tau(p_m a p_m) p_m + \frac{1}{\tau(p_n)} \tau(p_n a p_n) p_n,$$

por tanto, como resultado del teorema 3.12, $\langle \hat{x} \rangle \otimes M_{nm}(\mathbb{C})$ y $\langle \{e_{ij}\} \rangle \otimes M_{nm}(\mathbb{C})$ son $\langle p_m, p_n \rangle \otimes M_{nm}(\mathbb{C})$-libres respecto a la esperanza condicional $\mathbb{F} = \psi \otimes I$ (ya que hay una biyección natural entre $\langle p_m, p_n \rangle \otimes M_{nm}(\mathbb{C})$ y $M_{nm}(\mathbb{C}) \otimes \langle p_m, p_n \rangle$) y como $ff^* \in \langle \{e_{ij}\} \rangle \otimes M_{nm}(\mathbb{C})$ y $\hat{x} \otimes C \in \langle \hat{x} \rangle \otimes M_{nm}(\mathbb{C})$ entonces $\hat{x} \otimes C$ y ff^* son $\langle p_m, p_n \rangle \otimes M_{nm}(\mathbb{C})$-libres.

Para ver $\mathcal{B}$-libertad, observemos que $\mathcal{B} = \langle p_m, p_n \rangle \otimes \langle P_1, \ldots, P_r \rangle \subseteq \langle p_m, p_n \rangle \otimes M_{nm}(\mathbb{C})$ y por la proposición 3.3, sólo basta ver que los $\langle p_m, p_n \rangle \otimes M_{nm}(\mathbb{C})$-momentos de $\hat{x} \otimes C$ y los de ff^* cuando se restringen los argumentos a elementos de $\mathcal{B}$, siguen siendo elementos de $\mathcal{B}$.

Verifiquemos primero para $\hat{x} \otimes C$, si $i_1, \ldots, i_{k-1} \in \{m, n\}$ y $j_1, \ldots, j_{k-1} \in \{1, 2, \ldots, r\}$ entonces

$$\begin{aligned}
&\mathbb{F}[(\hat{x} \otimes C)(p_{i_1} \otimes P_{j_1})(\hat{x} \otimes C) \cdots (\hat{x} \otimes C)(p_{i_{k-1}} \otimes P_{j_{k-1}})(\hat{x} \otimes C)] \\
&= \psi \otimes I[(\hat{x} p_{i_1} \hat{x} \cdots \hat{x} p_{i_{k-1}} \hat{x}) \otimes (C P_{j_1} C \cdots C P_{j_{k-1}} C)] \\
&= \psi(\hat{x} p_{i_1} \hat{x} \cdots \hat{x} p_{i_{k-1}} \hat{x}) \otimes (C P_{j_1} C \cdots C P_{j_{k-1}} C),
\end{aligned}$$

y como $\psi(\hat{x} p_{i_1} \hat{x} \cdots \hat{x} p_{i_{k-1}} \hat{x}) \in \langle p_m, p_n \rangle$ (ya que $\psi(a) \in \langle p_n, p_m \rangle$ para todo a) y claramente también $(C P_{j_1} C \cdots C P_{j_{k-1}} C) \in \langle P_1, \ldots, P_r \rangle$, se tiene lo deseado.

Para el caso de ff^* notemos primero que

$$ff^* = \left(\sum_{h=1}^{r} w_h^* \otimes v_h \right) \left(\sum_{h'=1}^{r} w_{h'} \otimes v_{h'}^* \right) = \sum_{h,h'=1}^{r} w_h^* w_{h'} \otimes v_h v_{h'}^*,$$

usando que $v_{h'}^* P_i v_h = \delta_{h,h'} \mathbf{1}_{h \in J_i}$ y $w_{h'} p_i w_h^* = \delta_{i,m} w_{h'} w_h^*$ tenemos que

$$\begin{aligned}
&\mathbb{F}[ff^*(p_{i_1} \otimes P_{j_1})ff^* \cdots ff^*(p_{i_{k-1}} \otimes P_{j_{k-1}})ff^*] \\
&= \sum_{\substack{h_1,\ldots,h_k=1 \\ h'_1,\ldots,h'_k=1}}^{r} \mathbb{F}[w_{h_1}^* w_{h'_1} p_{i_1} \cdots p_{i_{k-1}} w_{h_k}^* w_{h'_k} \otimes v_{h_1} v_{h'_1}^* P_{j_1} v_{h_2} v_{h'_2}^* \cdots P_{j_{k-1}} v_{h_k} v_{h'_k}^*] \\
&= \sum_{\substack{h_1,\ldots,h_k=1 \\ h'_1,\ldots,h'_k=1}}^{r} \psi[w_{h_1}^* w_{h'_1} p_{i_1} \cdots p_{i_{k-1}} w_{h_k}^* w_{h'_k}] \otimes v_{h_1} v_{h'_1}^* P_{j_1} v_{h_2} v_{h'_2}^* \cdots P_{j_{k-1}} v_{h_k} v_{h'_k}^*
\end{aligned}$$

y como

$$\begin{aligned}
\psi[w_{h_1}^* w_{h'_1} p_{i_1} \cdots p_{i_{k-1}} w_{h_k}^* w_{h'_k}] &= \left[\prod_{l \leq k-1} \mathbf{1}_{i_l = m} \right] \psi[w_{h_1}^* w_{h'_1} \cdots w_{h_k}^* w_{h'_k}], \\
v_{h_1} v_{h'_1}^* P_{j_1} v_{h_2} v_{h'_2}^* \cdots P_{j_{k-1}} v_{h_k} v_{h'_k}^* &= \left[\prod_{i \leq k-1} \delta_{h'_i h_{i+1}} \mathbf{1}_{h_{i+1} \in J_{j_i}} \right] v_{h_1} v_{h'_k},
\end{aligned}$$

entonces

$$\begin{aligned}
&\mathbb{F}[ff^*(p_{i_1} \otimes P_{j_1})ff^* \cdots ff^*(p_{i_{k-1}} \otimes P_{j_{k-1}})ff^*] \\
&= \left[\prod_{l \leq k-1} \mathbf{1}_{i_l = m} \right] \sum_{\substack{h_1,\ldots,h_k=1 \\ h'_1,\ldots,h'_k=1}}^{r} \psi[w_{h_1}^* w_{h'_1} p_{i_1} \cdots p_{i_{k-1}} w_{h_k}^* w_{h'_k}] \otimes v_{h_1} v_{h'_1}^* P_{j_1} v_{h_2} v_{h'_2}^* \cdots P_{j_{k-1}} v_{h_k} v_{h'_k}^* \\
&= \left[\prod_{l \leq k-1} \mathbf{1}_{i_l = m} \right] \sum_{h_1,\ldots,h_k,h'_k=1}^{r} \psi[w_{h_1}^* w_{h_2} w_{h_2}^* \cdots w_{h_k} w_{h_k}^* w_{h'_k}] \left[\prod_{i \leq k-1} \mathbf{1}_{h_{i+1} \in J_{j_i}} \right] \otimes v_{h_1} v_{h'_k} \\
&= \left[\prod_{l \leq k-1} \mathbf{1}_{i_l = m} \right] \sum_{h_1,h'_k=1}^{r} \psi \left[w_{h_1}^* \left(\sum_{h_2 \in J_{j_1}} w_{h_2} w_{h_2}^* \right) \cdots \left(\sum_{h_k \in J_{j_{k-1}}} w_{h_k} w_{h_k}^* \right) w_{h'_k} \right] \otimes v_{h_1} v_{h'_k} \\
&= \left[\prod_{l \leq k-1} \mathbf{1}_{i_l = m} \right] \sum_{h_1,h'_k=1}^{r} \psi \left[w_{h_1}^* Q_{j_1} \cdots Q_{j_{k-1}} w_{h'_k} \right] \otimes v_{h_1} v_{h'_k} \\
&= \left[\prod_{l \leq k-1} \mathbf{1}_{i_l = m} \right] \sum_{h_1,h'_k=1}^{r} \psi \left[w_{h'_k} w_{h_1}^* Q_{j_1} \cdots Q_{j_{k-1}} \right] \otimes v_{h_1} v_{h'_k},
\end{aligned}$$

esto último ya que si τ tracial, también lo es ψ (ya que $\tau(p_i a b p_i) = \tau(b p_i a) = \tau(p_i b a)$), finalmente como

$$w_{h'_k} w^*_{h_1} Q_{j_1} \cdots Q_{j_{k-1}} = \left[\begin{array}{c|c} 0 & 0 \\ \hline 0 & H_{h'_k} H^*_{h_1} \end{array}\right] \left[\begin{array}{c|c} 0 & 0 \\ \hline 0 & \left(\sum_{s\in J_{j_1}} H_{s_1} H^*_{s_1}\right) \cdots \left(\sum_{s\in J_{j_1}} H_{s_1} H^*_{s_1}\right) \end{array}\right]$$

entonces $p_m w_{h'_k} w^*_{h_1} Q_{j_1} \cdots Q_{j_{k-1}} p_m = 0$ y

$$p_n w_{h'_k} w^*_{h_1} Q_{j_1} \cdots Q_{j_{k-1}} p_n = H_{h'_k} H^*_{h_1} \left(\sum_{s\in J_{j_1}} H_{s_1} H^*_{s_1}\right) \cdots \left(\sum_{s\in J_{j_1}} H_{s_1} H^*_{s_1}\right),$$

y por tanto se tiene que

$$\begin{aligned} \psi[w_{h'_k} w^*_{h_1} Q_{j_1} \cdots Q_{j_{k-1}}] &= \frac{n+m}{n} \tau(w_{h'_k} w^*_{h_1} Q_{j_1} \cdots Q_{j_{k-1}}) p_n \\ &= (n+m) \tau_n(w_{h'_k} w^*_{h_1} Q_{j_1} \cdots Q_{j_{k-1}}) p_n; \end{aligned}$$

usando finalmente la condición TWB obtenemos

$$\begin{aligned} &\mathbb{F}[ff^*(p_{i_1} \otimes P_{j_1}) ff^* \cdots ff^*(p_{i_{k-1}} \otimes P_{j_{k-1}}) ff^*] \\ &= \left[\prod_{l\le k-1} \mathbf{1}_{i_l=m}\right] \sum_{h_1,h'_k=1}^{r} (n+m) \tau_n(w_{h'_k} w^*_{h_1} Q_{j_1} \cdots Q_{j_{k-1}}) p_n \otimes v_{h_1} v_{h'_k} \\ &= \left[\prod_{l\le k-1} \mathbf{1}_{i_l=m}\right] \sum_{h_1,h'_k=1}^{r} (n+m) \delta_{h_1,h'_k} \tau_n(w_{h_1} w^*_{h_1} Q_{j_1} \cdots Q_{j_{k-1}}) p_n \otimes v_{h_1} v_{h'_k} \\ &= p_n \otimes \sum_{j=1}^{r} \left(\left[\prod_{l\le k-1} \mathbf{1}_{i_l=m}\right] (n+m) \tau_n(w_j w^*_j Q_{j_1} \cdots Q_{j_{k-1}})]\right) v_j v^*_j \\ &= p_n \otimes \sum_{j=1}^{r} c_j^{i_1,\ldots,i_{k-1};j_1,\ldots,j_{k-1}} P_j \in \mathcal{B} \end{aligned}$$

donde $c_j^{i_1,\ldots,i_{k-1};j_1,\ldots,j_{k-1}} = \left(\left[\prod_{l\le k-1} \mathbf{1}_{i_l=m}\right] (m+n) \tau_n(w_j w^*_j Q_{j_1} \cdots Q_{j_{k-1}})]\right)$. De lo anterior se sigue el resultado. ∎

Definición 3.26. Decimos que la matriz de Choi C_φ satisface la *condición unitaria* (UC) si para todo t, existe un real d_t tal que $Q_t^{(n)} := \sum_{s\in J_t} H_s H_s^* = d_t \cdot I_n$ o bien que $Q_t = d_t p_n$. Donde p_n es la proyección definida en la Proposición 3.8.

Observación 3.24. El nombre *condición unitaria*, se justifica ya que si las H_s son unitarias, entonces $H_s H_s^* = I_n$ y por tanto $Q_t^{(n)} = d_t I_n$ con $d_t = |J_t|$, i.e., si son unitarias satisfacen la condición unitaria.

Proposición 3.11. Si la matriz de Choi C satisface la condición unitaria, entonces también sus eigenespacios son tracialmente bien portados. Más aún, $d_t = \frac{1}{n}\, rank(P_t) = \frac{1}{n}\, Tr(P_t)$.

Demostración. Observemos primero que para cualquier $s, t \in \{1, 2, \ldots, r\}$ se tiene que

$$\begin{aligned}\tau_n(w_s w_t^*) &= \sum_{i_1,i_2=1}^{n} \sum_{j_1,j_2=1}^{m} \langle E_{i_1} \otimes E_{j_1}, v_s\rangle \overline{\langle E_{i_2} \otimes E_{j_2}, v_t\rangle} \tau_n(e_{m+i_1,j_1} e_{j_2,m+i_2}) \\ &= \sum_{i_1,i_2=1}^{n} \sum_{j_1,j_2=1}^{m} \langle E_{i_1} \otimes E_{j_1}, v_s\rangle \overline{\langle E_{i_2} \otimes E_{j_2}, v_t\rangle} \delta_{i_1,i_2}\delta_{j_1,j_2} n^{-1} \\ &= n^{-1}\langle v_t, v_s\rangle = n^{-1}\delta_{st};\end{aligned}$$

y por tanto,

$$\tau_n(w_{j_1} w_{j_2}^* Q_{i_1} \cdots Q_{i_k}) = d_{i_1} \cdots d_{i_k} \tau_n(w_{j_1} w_{j_2}^*) = n^{-1} d_{i_1} \cdots d_{i_k} \delta_{j_1,j_2},$$

lo que prueba que se satisface la condición TWB. Finalmente:

$$d_t = \tau_n(Q_t) = \sum_{j \in J_t} \tau_n(w_j w_j^*) = \sum_{j \in J_t} \frac{1}{n} = \frac{1}{n} Rank(P_t) = \frac{1}{n} \sum_{j \in J_t} \|v_t\|^2 = \frac{Tr(P_t)}{n}.$$

■

Observación 3.25. Existen aplicaciones φ que satisfacen la condición TWB pero no la condición unitaria. Por ejemplo $\varphi : M_n(\mathbb{C}) \to M_m(\mathbb{C})$ dado por

$$\varphi(A) = \sum_{i \le n, j \le m} \alpha_{ij} E_{ij} A E_{ji},$$

tiene matriz de Choi diagonal $C_\varphi = diag(\alpha_{11}, \alpha_{21}, \ldots, \alpha_{n1}, \alpha_{12}, \ldots, \alpha_{nm})$ y por tanto, los eigenvectores de C_φ son $(E_j \otimes E_k)_{j,k \le n}$ en $\mathbb{C}^{n^2}$, o bien las matrices e_{jk} (viendo los vectores como matrices); concluimos que $Q_{ij} = e_{ii} \neq d_{ij} I$, para ningún d_{ij}, es decir, no satisface la condición unitaria. Sin embargo:

$$\tau(w_{i_1,j_2} w_{i_2,j_2}^* Q_{i_3,j_3} \cdots Q_{i_k,j_k}) = \tau(e_{i_1,j_1} e_{j_2,i_2}^* e_{i_3,j_3} \cdots e_{i_k,j_k}) = n^{-1}\delta_{j_1,j_2} \prod_{s<k} \delta_{i_s,i_{s+1}},$$

de lo cual se sigue la condición TWB.

Más aún, la distribución μ de $x^\varphi = \sum_{i \le m} c_{ii} \otimes x_{ii}$ es $\mu = \frac{1}{n}(\mu_1 + \cdots + \mu_n)$, donde cada μ_i es la distribución de una combinación lineal $\alpha_{i1} x_{11} + \cdots + \alpha_{im} x_{mm}$, donde (x_{ij}) son variables libres, idénticamente distribuidas con la misma distribución de la compresión libre x_{11} de x.

Observación 3.26. Las matrices de Choi de φ y de su dual φ^* están relacionadas por la ecuación

$$C_{\varphi^*} = F_{n,m} C_\varphi^T F_{n,m}^*,$$

con $F_{n,m}$ operador unitario en $\mathbb{C}^n \otimes \mathbb{C}^m$ definido por $F_{n,m}(x \otimes y) = y \otimes x$.

Con lo anterior, demostramos ahora el resultado analítico principal. A pesar de que para la libertad, la condición TWB era suficiente, para el siguiente teorema, es necesaria la hipótesis más fuerte de la condición unitaria.

Teorema 3.24. Si la matriz de Choi C_φ satisface la condición unitaria, entonces la distribución de x^φ tiene la siguiente R-transformada:

$$R_{x^\varphi}(z) = \sum_{i=1}^{s} d_i \rho_i R_x \left[\frac{\rho_i z}{n} \right],$$

donde ρ_i son los s distintos eigenvalores de C_φ y $nd_i = dim(E_{\rho_i}) = rank(P_{\rho_i})$. En otras palabras, si μ distribución de x y μ^φ de x^φ entonces

$$\mu^\varphi = \boxplus_{i=1}^{s} \left(D_{\frac{\rho_i}{n}} \mu \right)^{\boxplus n d_i}.$$

Demostración. Del Teorema 3.23 las variables $\hat{x} \otimes C$ y ff^*, ambas en $\tilde{\mathcal{A}} \otimes M_{mn}(\mathbb{C})$, son libres con amalgamación sobre la álgebra conmutativa $\mathcal{B} = \langle p_m, p_n \rangle \otimes \langle P_1, \ldots, P_r \rangle$. Sin embargo, nos interesa x variable bloque de $\hat{x}$, así que nos restringiremos al espacio $\mathcal{A} \otimes M_{mn}(\mathbb{C})$, donde $\mathcal{A}$ es isomorfo al espacio comprimido $p_n \tilde{\mathcal{A}} p_n$; se puede demostrar gracias a la Proposición 3.3 que las variables $x \otimes C$ y $f\tilde{f}^* = \sum_{h=1}^{nm} H_h^* H_h \otimes v_h v_h^*$ son libres con amalgamación sobre $\mathcal{B} = \mathbb{C}\mathbf{1}_\mathbf{A} \otimes \langle P_1, \ldots, P_s \rangle$, con la esperanza condicional $\mathbb{F} = \tau \otimes I_{mn}$. Como la matriz de Choi satisface la condición unitaria, entonces $\sum_{l \in J_t} H_l^* H_l = d_t \mathbf{1}_\mathcal{A}$, donde $d_t = \frac{1}{n} rank(P_t)$.

A continuación, calcularemos las S transformadas $\mathcal{B}$ valuadas de $x \otimes C$ y $f\tilde{f}^*$, pero sólo para elementos de la forma $\tilde{B} = \mathbf{1}_\mathcal{A} \otimes B$, con

$$B = \sum_{t=1}^{s} b_t P_t = \begin{pmatrix} b_1 P_1 & & & \\ & b_2 P_2 & & \\ & & \ddots & \\ & & & b_s P_s \end{pmatrix} \in \langle P_1, \ldots, P_s \rangle;$$

lo anterior ya que, como veremos más adelante, esos elementos nos bastarán para encontrar la distribución de x^φ.

Observemos que

$$\begin{aligned}\Psi^{\mathcal{B}}_{x\otimes C}(\tilde{B}) &= \sum_{k\geq 1}\mathbb{F}[((x\otimes C)(\mathbf{1}\otimes B))^k] = \sum_{k\geq 1}\mathbb{F}[x^k\otimes (CB)^k]\\ &= \sum_{k\geq 1}\tau(x^k)\mathbf{1}_{\mathcal{A}}\otimes\left(\sum_{t=1}^{s}\rho_t^k b_t^k P_t\right) = \mathbf{1}_{\mathcal{A}}\otimes\sum_{t=1}^{s}\left(\sum_{k\geq 1}\rho_t^k b_t^k \tau(x^k)P_t\right)\\ &= \mathbf{1}_{\mathcal{A}}\otimes\sum_{t=1}^{s}\Psi^{Sc}_{\rho_t x}(b_t)P_t.\end{aligned}$$

De lo anterior se sigue que $\Psi^{\mathcal{B}<-1>}_{x\otimes C}(\tilde{B}) = \mathbf{1}_{\mathcal{A}}\otimes\sum_{t=1}^{s}\Psi^{Sc<-1>}_{\rho_t x}(b_t)P_t$ y por lo tanto, si tomamos $B^{-1} = \sum_{\substack{t=1\\ b_t\neq 0}}^{s} b_t^{-1}P_t$, entonces

$$\begin{aligned}S^{\mathcal{B}}_{x\otimes C}(\tilde{B}) &= (\mathbf{1}_{\mathcal{A}}\otimes I_{mn}+\mathbf{1}_{\mathcal{A}}\otimes B)(\mathbf{1}_{\mathcal{A}}\otimes B^{-1})\Psi^{\mathcal{B}<-1>}_{x\otimes C}(\tilde{B})\\ &= \mathbf{1}_{\mathcal{A}}\otimes\sum_{t=1}^{s}(I_{nm}+B)B^{-1}\Psi^{Sc<-1>}_{\rho_t x}(b_t)P_t = \mathbf{1}_{\mathcal{A}}\otimes\sum_{\substack{t=1\\ b_t\neq 0}}^{s}\frac{1+b_t}{b_t}\Psi^{Sc<-1>}_{\rho_t x}(b_t)P_t\\ &= \mathbf{1}_{\mathcal{A}}\otimes\sum_{\substack{t=1\\ b_t\neq 0}}^{s}S^{Sc}_{\rho_t x}(b_t)P_t.\end{aligned}$$

Observemos ahora que $Tr(B) = \sum_{t=1}^{s} b_t rank(P_t)$. Usemos la condición unitaria para calcular ahora la S transformada para $f\tilde{f}^*$.

$$\begin{aligned}\Psi^{\mathcal{B}}_{f\tilde{f}^*}(\tilde{B}) &= \sum_{k\geq 1}\mathbb{F}[(f\tilde{f}^*(\mathbf{1}_{\mathcal{A}}\otimes B))^k] = \sum_{k\geq 1}\mathbb{F}[(f\tilde{f}^*(\sum_{t=1}^{s}b_t\mathbf{1}_{\mathcal{A}}\otimes P_t))^k]\\ &= \sum_{k\geq 1}\sum_{t_1,\ldots,t_{k-1}=1}^{s} b_{t_1}\cdots b_{t_{k-1}}\mathbb{F}[f\tilde{f}^*(\mathbf{1}_{\mathcal{A}}\otimes P_{t_1})\cdots f\tilde{f}^*(\mathbf{1}_{\mathcal{A}}\otimes P_{t_{k-1}})f\tilde{f}^*](\mathbf{1}_{\mathcal{A}}\otimes B)\\ &= \sum_{k\geq 1}\sum_{t_1,\ldots,t_{k-1}=1}^{s}\sum_{h_1,\ldots h_k=1}^{mn} b_{t_1}\cdots b_{t_{k-1}}\mathbb{F}[H_{h_1}^*H_{h_1}\otimes v_{h_1}v_{h_1}^*(\mathbf{1}_{\mathcal{A}}\otimes P_{t_1})\cdots\\ &\cdots H_{h_{k-1}}^*H_{h_{k-1}}\otimes v_{h_{k-1}}v_{h_{k-1}}^*(\mathbf{1}_{\mathcal{A}}\otimes P_{t_{k-1}})H_{h_k}^*H_{h_k}\otimes v_{h_k}v_{h_k}^*](\mathbf{1}_{\mathcal{A}}\otimes B),\end{aligned}$$

lo anterior implica que $h_i \notin J_{t_i}$ contribuye con cero a la suma, por la construcción de los P_i en términos de los v_s. Entonces,

$$\begin{aligned}\Psi^{\mathcal{B}}_{f\tilde{f}^*}(\tilde{B}) &= \mathbf{1}_{\mathcal{A}} \otimes \sum_{k\geq 1} \sum_{t_1,\ldots,t_{k-1}=1}^{s} b_{t_1}\cdots b_{t_{k-1}} \left(\sum_{h=1}^{s} d_{t_1}\cdots d_{t_{k-1}} P_h\right) \frac{1}{n} B \\ &= \mathbf{1}_{\mathcal{A}} \otimes \left[\sum_{k\geq 1} \left(\sum_{t=1}^{s} b_t rank(P_t)/n\right)^{k-1}\right] \frac{1}{n} B \\ &= \mathbf{1}_{\mathcal{A}} \otimes \left[\sum_{k\geq 1} (Tr(B)/n)^{k-1}\right] \frac{1}{n} B = \mathbf{1}_{\mathcal{A}} \otimes \frac{n^{-1}B}{1-n^{-1}Tr(B)}.\end{aligned}$$

De lo anterior se sigue que $\Psi^{\mathcal{B}<-1>}_{f\tilde{f}^*}(\tilde{B}) = \mathbf{1}_{\mathcal{A}} \otimes \frac{nB}{1+Tr(B)}$ y $S^{\mathcal{B}}_{f\tilde{f}^*}(\tilde{B}) = \mathbf{1}_{\mathcal{A}} \otimes n\frac{(B+I_{nm})}{1+Tr(B)}$. Usando ahora el Teorema 3.10 y el hecho de que el álgebra $\mathcal{B}$ es conmutativa, podemos calcular la S transformada de $y = (x \otimes C)(ff^*)$:

$$S^{\mathcal{B}}_y(\tilde{B}) = S^{\mathcal{B}}_{x\otimes C}(\tilde{B}) S^{\mathcal{B}}_{ff^*}(\tilde{B}) = \mathbf{1}_{\mathcal{A}} \otimes \sum_{\substack{t=1 \\ b_t\neq 0}}^{s} \frac{n(1+b_t)}{1+Tr(B)} S^{Sc}_{\rho_t x}(b_t) P_t.$$

Sea $a \in \mathbb{R}$; buscamos ahora los B que hagan que $\Psi^{\mathcal{B}<-1>}_y(\tilde{B}) = aI$. Se sigue de la relación anterior que en P_i:

$$\frac{n}{\rho_i} \frac{b_i S^{Sc}_x(b_i)}{1+Tr(B)} = a.$$

Sea ahora z_i tal que $b_i = z_i R^{Sc}_x(z_i)$, usando la relación entre la S transformada y la R transformada de la Proposición 3.10, tenemos que $z_i = \frac{\rho_i}{n} a(1+Tr(B))$. Veamos ahora que por la compatibilidad

$$\Psi^{Sc}_y(a) = \frac{1}{nm} Tr[\Psi^{\mathcal{B}}_y(aI)] = \frac{1}{nm} Tr[\Psi^{\mathcal{B}}_y(\Psi^{\mathcal{B}<-1>}_y(\tilde{B}))] = \frac{1}{mn} Tr(B),$$

además $\Psi^{Sc}_{x^\varphi}(a) = mn\Psi^{Sc}_y(a)$, entonces

$$\begin{aligned}\Psi^{Sc}_{x^\varphi}(a) = Tr(B) &= \sum_{i=1}^{s} n d_i b_i = \sum_{i=1}^{s} n d_i z_i R^{Sc}_x(z_i) = \sum_{i=1}^{s} n d_i b_i \\ &= \sum_{i=1}^{s} d_i \rho_i a(1+Tr(B)) R^{Sc}_x(\frac{\rho_i}{n} a(1+Tr(B))).\end{aligned}$$

Lo anterior fue para todo a, vamos a tomar ahora a de la forma $a = \frac{1}{R^{Sc}_{x^\varphi}(\alpha)+1/\alpha}$ para obtener que $\alpha R^{Sc}_{x^\varphi}(\alpha) = Tr(B)$, $a(1+Tr(B)) = \alpha$ y por tanto

$$R^{Sc}_{x^\varphi}(\alpha) = \sum_{i=1}^{s} d_i \rho_i R^{Sc}_x\left(\frac{\rho_i}{n}\alpha\right),$$

lo cual es la R transformada de la medida

$$\mu^{\varphi} = \boxplus_{i=1}^{s} \left(D_{\frac{\rho_i}{n}} \mu \right)^{\boxplus n d_i}.$$

■

3.4 Ejemplos

3.4.1 Matrices GUE

Proposición 3.12. Sea $X_d \in M_d(\mathbb{C}) \otimes M_m(\mathbb{C})$ familia GUE que converge a $\mu_{SC(a,\sigma^2)}$. Entonces para toda $\varphi : M_m(\mathbb{C}) \to M_n(\mathbb{C})$ que satisface la condición unitaria, se cumple que $X_d^{\varphi} = [I \otimes \varphi](X_D)$ converge en distribución a la medida semicircular de media a^{φ} y varianza $(\sigma^{\varphi})^2$, donde

$$a^{\varphi} = \frac{Tr(C_{\varphi})}{n} a \quad \text{y} \quad \sigma^{\varphi} = \frac{\sigma}{n} \sqrt{Tr(C_{\varphi}^2)}.$$

Demostración. En el ejemplo 3.2 vimos que la transdormada R de $\mu_{SC(a,\sigma^2)}$ es $R(z) = a + \sigma^2 z$, por tanto

$$\sum_{i=1}^{s} d_i \rho_i R(\rho_i z/n) = \sum_{i=1}^{s} d_i \rho_i (a + \sigma^2 \rho_i z/n) = \frac{a}{n} \sum_{i=1}^{s} n d_i \rho_i + \frac{\sigma^2}{n^2} z \sum_{i=1}^{s} n d_i \rho_i^2,$$

y como $\sum_{i=1}^{s} n d_i \rho_i = Tr(C_{\varphi})$ y $\sum_{i=1}^{s} n d_i \rho_i^2 = Tr(C_{\varphi}^2)$, por el teorema 3.24:

$$R_{\mu^{\varphi}}(z) = \frac{Tr(C_{\varphi})}{n} a + \frac{\sigma^2}{n^2} Tr(C_{\varphi}^2) z = R_{\mu_{SC(a^{\varphi},(\sigma^{\varphi})^2)}}.$$

■

3.4.2 Matrices Wishart Compuestas

Proposición 3.13. Sean $X_d \in M_{d \times s_d}(\mathbb{C})$ sucesión de matrices Ginibre gaussianas, tal que $s_d \sim \lambda d$ y sean $D_d \in M_{s_d}(\mathbb{C})$ matrices autoadjuntas e independientes de las X_d que convergen en distribución a $\tilde{\mu} = \mu/\lambda$. Entonces la sucesión $\frac{1}{s_d} X_d D_d X_d^*$ converge en distribución a la distribución poisson compuesta libre $\pi_{1,\mu}$.

Definición 3.27. A la familia $\frac{1}{s_d} X_d D_d X_d^*$ como en la proposición anterior la llamamos *sucesión de matrices Wishart compuestas* o *familia Wishart compuesta*.

Proposición 3.14. Sea $X_d \in M_d(\mathbb{C}) \otimes M_m(\mathbb{C})$ familia Wishart compuesta, i.e., que converge a $\pi_{\lambda,\mu}$, con $supp(\mu) \subseteq \mathbb{R}^+$. Entonces para toda $\varphi : M_m(\mathbb{C}) \to M_n(\mathbb{C})$ que satisface la condición

unitaria, se cumple que $X_d^{\varphi} = [I \otimes \varphi](X_D)$ converge en distribución a la poisson libre compuesta $\pi_{\lambda,\mu^{\varphi}}$, donde

$$\mu^{\varphi} = \sum_{i=1}^{s} n d_i D_{\rho_i/n}[\mu].$$

En particular si $\mu = c\delta_1$ (correspondiente a la poisson libre), entonces

$$\mu^{\varphi} = c \sum_{i=1}^{s} n d_i \delta_{\rho_i/n}.$$

Demostración. Observemos primero que

$$m_{p+1}(D_a\nu) = \int x^{p+1} D_a\nu(dx) = \int x^{p+1}\nu(a^{-1}dx) = a^{p+1} m_{p+1}(\nu),$$

y por lo visto en el ejemplo 3.2, $R_{\pi_{\lambda,\mu}}(z) = \lambda \sum_{p=0}^{\infty} m_{p+1}(\mu) z^p$, de donde obtenemos,

$$\begin{aligned} R_{x^{\varphi}}(z) &= \sum_{i=1}^{s} d_i \rho_i R_{\pi_{\lambda,\mu}}(\rho_i z/n) = \sum_{i=1}^{s} d_i \rho_i \lambda \sum_{p=0}^{\infty} m_{p+1}(\mu)(\rho_i z/n)^p \\ &= \lambda \sum_{i=1}^{s} d_i \rho_i \frac{n}{\rho_i} \sum_{p=0}^{\infty} \left(\frac{\rho_i}{n}\right)^{p+1} m_{p+1}(\mu) z^p = \lambda \sum_{i=1}^{s} n d_i \sum_{p=0}^{\infty} m_{p+1}(D_{\rho_i/n}[\mu]) z^p \\ &= \lambda \sum_{p=0}^{\infty} m_{p+1} \left(\sum_{i=1}^{s} n d_i D_{\rho_i/n}[\mu] \right) z^p = R_{\lambda,\pi_{\mu^{\varphi}}}(z). \end{aligned}$$

■

Observación 3.27. La proposición anterior generaliza el teorema 3.21, en el que se pedía que φ cumpliera ciertas condiciones planares.

Aplicamos ahora el resultado del teorema 3.24 a algunas de las medidas parciales definidas en la sección 1.2.2.

3.4.3 Rotaciones Unitarias

Si consideramos $U \in \mathcal{U}_n$ una rotación unitaria y $\varphi : M_n(\mathbb{C}) \to M_n(\mathbb{C})$ dada por $\varphi(X) = UXU^*$, en ese caso

$$X^{\varphi} = [I \otimes \varphi](X) = (I \otimes U)X(I \otimes U)^*.$$

Entonces si $u \in \mathbb{C}^n \otimes \mathbb{C}^n$ es la vectorización de U:

$$u = \sum_{i,j=1}^{n} \langle e_i, Ue_j \rangle e_i \otimes e_j = \sum_{i,j=1}^{n} U_{ij} e_i \otimes e_j,$$

la matriz de Choi C_φ es uu^* y por tanto tiene rango 1, pero como $\|u\| = \sqrt{n}$, la matriz de Choi tiene como único eigenvalor no cero a n. Dado lo anterior es sencillo probar para este tipo de aplicaciones que C_φ satisface la condición unitaria si y sólo si U es unitario, como es el caso en este ejemplo.

Proposición 3.15. Sea X_d que convergen en distribución a μ y φ como antes. Entonces X_d^φ converge a $\mu^\varphi = \mu$.

Demostración. Esto se sigue de que $s = 1$, $nd_i = 1$ y $\rho_i = n$ y por tanto por el teorema 3.24:

$$\mu^\varphi = \boxplus_{i=1}^{s} (D_{\rho_i/n}\mu)^{\boxplus nd_i} = D_1\mu = \mu.$$

■

3.4.4 La Traza y su Dual

Consideremos $A \in M_m(\mathbb{C})$ matriz autoadjunta y las aplicaciones $\psi_A : M_m(\mathbb{C}) \to M_1(\mathbb{C})$, dada por $\psi_A(X) = Tr(A^T X)$ y $J : M_1(\mathbb{C}) \to M_n(\mathbb{C})$, $J(z) = xI_n$, si $m = n$, ψ_I y J son duales.

Para J, tenemos que $C_J = xI_n \otimes I \in M_n(\mathbb{C}) \times M_1(\mathbb{C})$ y $X_d^J = zX_d \otimes I_n$, usando el teorema 3.24 y que esta sencilla matriz de Choi satisface la condición unitaria, tenemos que la distribución espectral límite de la modificación a bloques es $D_x[\mu]$. Para ψ_A tenemos la siguiente proposición.

Proposición 3.16. Sea $X_d \in M_d(\mathbb{C}) \otimes M_m(\mathbb{C})$ sucesión unitariamente invariante que converge en distribución a μ. Entonces la sucesión $X_d^{\psi_A}$ converge en distribución a μ^{ψ_A} dada por

$$\mu^{\psi_A} = D_{\lambda_1}[\mu] \boxplus \cdots \boxplus D_{\lambda_m}[\mu],$$

donde λ_i son los eigenvalores de A. En particular si $A = I_m$ entonces $X_d^{\psi_I}$ corresponde a la **traza parcial** y $\mu^{\psi_I} = \mu^{\boxplus m}$.

Demostración. Se sigue inmediatamente de que $C_{\psi_A} = I \otimes A$ y el teorema 3.24. ■

3.4.5 Transpuesta Parcial

Si $T : M_n(\mathbb{C}) \to M_n(\mathbb{C})$ la aplicación $T(A) = A^T$ entonces su matriz de Choi es el operador unitario $F \in M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$ definido por $F(x \otimes y) = y \otimes x$. Tal operador tiene eigenvalores 1 y -1 con respectivas multiplicidades $nd_1 = n(n+1)/2$ y $nd_2 = n(n-1)/2$; de hecho $F = P_+ - P_-$, donde P_+ proyección a las matrices simétricas y P_- a las matrices antisimétricas. La condición unitaria es consecuencia de las relaciones:

$$P_+ = \frac{I + F}{2}, \quad \text{y} \quad P_- = \frac{I - F}{2}.$$

Proposición 3.17. Si $X_d \in M_d(\mathbb{C}) \otimes M_n(\mathbb{C})$ unitariamente invariantes que convergen en distribución a μ. Entonces X_d^Γ converge en distribución a μ^Γ dada por

$$\mu^\Gamma = D_{1/n}\left[\mu^{\boxplus n(n+1)/2} \boxminus \mu^{\boxplus n(n-1)/2}\right].$$

Demostración. Observemos primero que

$$R_{(D_a\nu)^{\boxplus k}}(z) = kR_{D_a\nu}(z) = kaR_\nu(az) = aR_{\nu^{\boxplus k}}(az) = R_{D_a(\nu^{\boxplus k})}(z),$$

de donde $(D_a\nu)^{\boxplus k} = D_a(\nu^{\boxplus k})$. De esto, lo mencionado antes y el teorema 3.24 tenemos que

$$\begin{aligned}\mu^\Gamma &= (D_{1/n}\mu)^{\boxplus n(n+1)/2} \boxplus (D_{-1/n}\mu)^{\boxplus n(n-1)/2} \\ &= D_{1/n}[\mu^{\boxplus n(n+1)/2} \boxplus (D_{-1}\mu)^{\boxplus n(n-1)/2}] \\ &= D_{1/n}[\mu^{\boxplus n(n+1)/2} \boxminus \mu^{\boxplus n(n-1)/2}].\end{aligned}$$

■

En el caso μ Poisson libre de parámetro λ, se recupera el resultado del teorema 3.18.

Corolario 3.3. Sea $W_d \in M_d(\mathbb{C}) \otimes M_n(\mathbb{C})$ sucesión de matrices Wishart que convergen en distribución a la poisson libre π_λ. Entonces W_d^Γ converge en distribución a π_λ^Γ dada por

$$\pi_\lambda^\Gamma = D_{1/n}\left[\pi_{\lambda n(n+1)/2} \boxminus \pi_{\lambda n(n-1)/2}\right].$$

Corolario 3.4. Sea $P_d \in M_d(\mathbb{C}) \otimes M_n(\mathbb{C})$ sucesión de proyecciones aleatorias que convergen en distribución a la distribución bernoulli $b_t = (1-t)\delta_0 + t\delta_1$, para algún $t \in (0,1)$. Entonces P_d^Γ converge en distribución a π_λ^Γ dada por

$$\pi_\lambda^\Gamma = D_{1/n}\left[b_t^{\boxplus n(n+1)/2} \boxminus b_t^{\boxplus n(n-1)/2}\right].$$

3.4.6 Aplicación de Reducción

Consideremos ahora la aplicación de reducción definida en la sección 1.2.2.

Proposición 3.18. Si $X_d \in M_d(\mathbb{C}) \otimes M_n(\mathbb{C})$ unitariamente invariantes que convergen en distribución a μ. Entonces X_d^{red} converge en distribución a μ^{red} dada por

$$\mu^{red} = D_{1/n}\left[\mu^{\boxplus n^2-1} \boxminus D_{n-1}\mu\right].$$

Demostración. Como la matriz de Choi de la aplicación de reducción es $C = I - F$, sus eigenvalores son 1 con multiplicidad $n^2 - 1$ y $1 - n$ con multiplicidad 1. Del hecho de que el eigenvector

asociado a $1-n$ es el estado de Bell, se cumple la condición unitaria y por el teorema 3.24 tenemos:

$$\begin{aligned}\mu^{red} &= (D_{1/n}\mu)^{\boxplus n^2-1} \boxplus (D_{(1-n)/n}\mu) \\ &= D_{1/n}[\mu^{\boxplus n^2-1} \boxplus D_{1-n}\mu] \\ &= D_{1/n}[\mu^{\boxplus n^2-1} \boxminus D_{n-1}\mu].\end{aligned}$$

■

Corolario 3.5. Sea $W_d \in M_d(\mathbb{C}) \otimes M_n(\mathbb{C})$ sucesión de matrices Wishart que convergen en distribución a la poisson libre π_λ. Entonces W_d^{red} converge en distribución a $D_{1/n}\pi_{\mu_{n,\lambda}}$ donde

$$\mu_{n,\lambda} = \lambda(n^2-1)\delta_1 + \lambda\delta_{1-n}.$$

3.4.7 Generalización de Transpuesta Parcial y Aplicación de Reducción

Definimos ahora $\varphi : M_n(\mathbb{C}) \to M_n(\mathbb{C})$ como una generalización de la aplicación reducción y la transpuesta parcial, esto es

$$\varphi(A) = \alpha A + \beta Tr(A) I_n + \gamma A^T,$$

con matriz de Choi $C_\varphi = \alpha\Omega_n + \beta I_{n^2} + \gamma F$, donde Ω_n estado de Bell. Los eigenvalores de esta matriz son $\lambda_1 = n\alpha + \beta + \gamma$ con eigenproyector $P_1 = n^{-1}\Omega_n$, $\lambda_2 = \beta + \gamma$ con $P_2 = \frac{I+F}{2} - n^{-1}\Omega_n$ y $\lambda_3 = \beta - \gamma$ con $P_3 = \frac{I-F}{2}$; y como cada proyector es múltiplo de la identidad, se satisface la condición unitaria.

Proposición 3.19. Si $X_d \in M_d(\mathbb{C}) \otimes M_n(\mathbb{C})$ unitariamente invariantes que convergen en distribución a μ y φ como antes. Entonces X_d^φ converge en distribución a μ^φ dada por

$$\mu^\varphi = D_{\alpha+(\beta+\gamma)/n}[\mu] \boxplus D_{(\beta+\gamma)/n}[\mu^{\boxplus n(n+1)/2-1}] \boxplus D_{(\beta-\gamma)/n}[\mu^{\boxplus n(n-1)/2}].$$

3.5 Libertad en Mezclas de Conjugaciones Ortogonales

Definición 3.28. Consideremos constantes $\alpha_i \in \mathbb{R}$ y U_i matrices unitarias en $M_n(\mathbb{C})$ que cumplen

$$Tr(U_i U_j^*) = n\delta_{ij}.$$

Al operador $\varphi : M_n(\mathbb{C}) \to M_n(\mathbb{C})$ de la forma

$$\varphi(A) = \sum_{i=1}^{n^2} \alpha_i U_i A U_i^*,$$

lo llamamos *mezcla de conjugaciones ortogonales*.

Estos canales tienen motivación en los canales Weyl-covariantes de interés en física. Estos operadores tienen una sencilla expresión para la matriz de Choi:

$$C_\varphi = \sum_{i=1}^{n^2} n\alpha_i u_i u_i^*,$$

donde los u_i son vectores ortonormales en $\mathbb{C}^n \otimes \mathbb{C}^n$ dados por

$$u_i = \frac{1}{\sqrt{n}} \sum_{s,t=1}^{n} U_i(s,t) E_s \otimes E_t.$$

Es decir, los eigenvalores de C_φ son $\{n\alpha_i\}$, son simples y $P_t = u_t u_t^*$, por lo que claramente se cumple la condición unitaria. Usamos, pues, el teorema 3.24, para probar el siguiente resultado.

Proposición 3.20. Sea $X_d \in M_d(\mathbb{C}) \otimes M_n(\mathbb{C})$ que converge en distribución a la medida de probabilidad μ. Entonces, para φ mezcla ortogonal de unitarios, X_d^φ converge en distribución a la medida μ^φ dada por

$$\mu^\varphi = \boxplus_{i=1}^{n^2} D_{\alpha_i}[\mu].$$

En el caso particular de que X_d es sucesión Wishart que converge a π_λ la poisson libre de parámetro λ. Entonces W_d^φ converge en distribución a la distribución poisson compuesta libre $\pi_{1,\mu}$, donde

$$\mu = \lambda \sum_{i=1}^{n^2} \delta_{\alpha_i}.$$

3.5.1 Asintoticidad Libre

Analicemos los resultados anteriores desde otro punto de vista. Consideremos que X_d es, como al inicio de este capítulo y consideremos φ la mezcla de conjugaciones ortogonales. Tenemos la siguiente igualdad para la matriz modificada a bloques,

$$X_d^\varphi = \sum_{i=1}^{n^2} \alpha_i (I_d \otimes U_i) X_d (I_d \otimes U_i^*).$$

Ahora bien, definamos $W(s_1, s_2) = (I_d \otimes U_{s_1}^*)(I \otimes U_{s_2})$ y $Y_s = (I_d \otimes U_s) X_d (I_d \otimes U_s^*)$, entonces se cumple lo siguiente.

i) $Tr[W(s_1, s_2)] = 0$ para $s_1 \neq s_2$, ya que

$$Tr[W(s_1, s_2)] = Tr[I_d \otimes U_{s_1}^* U_{s_2}] = Tr[I_d] Tr[U_{s_1}^* U_{s_2}] = Tr[I_d] \cdot 0 = 0,$$

por la ortogonalidad de las matrices unitarias.

ii) Para todo polinomio $P \in \mathbb{C}\langle x\rangle$, se cumple que $P(Y_s) = (I_d \otimes U_s)P(X_d)(I_d \otimes U_s^*)$. En efecto esto se cumple ya que

$$\begin{aligned} Y_s^k &= (I_d \otimes U_s)X_d(I_d \otimes U_s^*)(I_d \otimes U_s)X_d(I_d \otimes U_s^*)\cdots(I_d \otimes U_s)X_d(I_d \otimes U_s^*) \\ &= (I_d \otimes U_s)X_d(I_d \otimes I_n)X_d\cdots(I_d \otimes I_n)X_d(I_d \otimes U_s) \\ &= (I_d \otimes U_s)X_dI_{dn}X_d\cdots I_{dn}X_d(I_d \otimes U_s) = (I_d \otimes U_s)X_d^k(I_d \otimes U_s), \end{aligned}$$

y por linealidad.

Observemos también que por lo anterior,

$$\begin{aligned} Tr[P(Y_s)] &= Tr[(I_d \otimes U_s)P(X_d)(I_d \otimes U_s^*)] = Tr[(I_d \otimes U_s^*)(I_d \otimes U_s)P(X_d)] \\ &= Tr[I_{dn}P(X_d)] = Tr[P(X_d)]. \end{aligned}$$

Podemos ahora demostrar el siguiente teorema.

Teorema 3.25. Las matrices $\{\alpha_i(I_d \otimes U_i)X_d(I_d \otimes U_i^*)\}_{1\leq i\leq n^2}$ son asintóticamente libres.

Demostración. Sabemos que la matriz X_d es unitariamente invariante y que las matrices $(I_d \otimes U_i)$ son determinísticas y unitarias; podemos entonces aplicar el teorema de asintoticidad libre de Voiculescu (Teorema 3.5) para garantizar que las matrices X_d y $(I_d \otimes U_i)$ son asintóticamente libres. Veamos ahora que también los (Y_s) lo son.

Ahora bien, sea $k \in \mathbb{N}$ y $P_1, P_2, \ldots, P_k \in \mathbb{C}\langle x\rangle$ que cumplan que $Tr[P_j(Y_{s_j})] = 0$ para $j = 1, \ldots, k$ y $s_1 \neq s_2 \neq \cdots \neq s_k$ entonces

$$\begin{aligned} &\frac{1}{nd}Tr[P_1(Y_{s_1})P_2(Y_{s_2})\cdots P_k(Y_{s_k})] \\ &= \frac{1}{nd}Tr[(I_d \otimes U_{s_1})P(X_d)(I_d \otimes U_{s_1}^*)\cdots(I_d \otimes U_{s_k})P(X_d)(I_d \otimes U_{s_k}^*)] \\ &= \frac{1}{nd}Tr[W(s_k, s_1)P(X_d)W(s_1, s_2)\cdots W(s_{k-1}, s_k)P(X_d)]. \end{aligned}$$

La hipótesis de polinomios centrados $Tr[P(Y_s)] = 0$ implica, por las observaciones previas al teorema que $Tr[P(X_d)] = 0$. La condición $s_1 \neq s_2 \neq \cdots \neq s_k$ y las observaciones anteriores implican que $Tr[s_i, s_{i+1}] = 0$ y en la situación de $W(s_k, s_1)$ tenemos dos casos, si $s_k \neq s_1$ entonces es igual al caso anterior, y si $s_k = s_1$ entonces $W(s_k, s_1) = I_{dn}$ en cuyo caso no lo contamos. En cualquiera de los casos estamos ante un producto alternado de elementos centrados y asintóticamente libres (las W también son asintóticamente libres de la X_d por un argumento similar), entonces

$$\frac{1}{nd}Tr[P_1(Y_{s_1})P_2(Y_{s_2})\cdots P_k(Y_{s_k})] \to 0,$$

es decir, las matrices $\{Y_i\}$ son asintóticamente libres; lo anterior implica que las matrices $\{\alpha_i Y_i\}$ son también asintóticamente libres pues $\alpha_i Y_i$ pertenece al álgebra generada por Y_i. ■

La prueba anterior puede implicarse del siguiente resultado más general.

Proposición 3.21. Si $\{u_i\}_{i\in I}$ variables aleatorias unitarias en el espacio tracial $(\mathcal{A},\tau)$, que cumplen $\tau(u_i u_j)=\delta_{ij}$ y sean $\{a_i\}$ libres de las $\{u_i\}$. Entonces las variables $v_i = u_i a_i u_i^*$, $i\in I$ son libres.

Demostración. Observemos primero que $(u_i a_i u_i^*)^n = u_i a_i^n u_i^*$, ya que los u_i son unitarios, pero esto implica que si P es un polinomio, entonces

$$P(u_i a_i u_i^*) = u_i P(a_i) u_i^*.$$

Sea k entero y $P_1, P_2, \ldots, P_k$ polinomios tal que $\tau(P(v_i))=0$ para todo i, observemos que eso y la tracialidad implican que

$$0 = \tau(u_i P(a_i) u_i^*) = \tau(u_i^* u_i P(a_i)) = \tau(P(a_i)),$$

además también $\tau(u_j^* u_i) = \tau(u_i u_j^*) = \delta_{ij}$. Si $i_1 \neq i_2 \neq \cdots \neq i_k$ entonces por la libertad de $\{u_i\}$ y $\{a_i\}$ y que $\tau(u_j^* u_i)=0$ para $i\neq j$ y $\tau(P(a_i))=0$ tenemos que

$$\begin{aligned}
0 &= \tau[(u_{i_k}^* u_{i_1} - \tau(u_{i_k}^* u_{i_1}))P_1(a_{i_1})(u_{i_1}^* u_{i_2})\cdots(u_{i_{k-2}}^* u_{i_k})P_k(a_{i_k})] \\
&= \tau[(u_{i_k}^* u_{i_1})P_1(a_{i_1})(u_{i_1}^* u_{i_2})\cdots(u_{i_{k-2}}^* u_{i_k})P_k(a_{i_k})] \\
&- \tau(u_{i_k}^* u_{i_1})\tau[P_1(a_{i_1})(u_{i_1}^* u_{i_2})\cdots(u_{i_{k-2}}^* u_{i_k})P_k(a_{i_k})],
\end{aligned}$$

pero como $\tau[P_1(a_{i_1})(u_{i_1}^* u_{i_2})\cdots(u_{i_{k-2}}^* u_{i_k})P_k(a_{i_k})] = 0$ por la libertad y que sus elementos son centrados, entonces también se tiene que

$$\tau[(u_{i_k}^* u_{i_1})P_1(a_{i_1})(u_{i_1}^* u_{i_2})\cdots(u_{i_{k-2}}^* u_{i_k})P_k(a_{i_k})] = 0. \tag{3.6}$$

Finalmente tenemos que si $i_1 \neq i_2 \neq \cdots \neq i_k$,

$$\begin{aligned}
\tau[P_1(v_{i_1})P_2(v_{i_1})\cdots P_k(v_{i_k})] &= \tau[u_{i_1}P_1(a_{i_1})u_{i_1}^* u_{i_2}P_2(a_{i_2})u_{i_2}^*\cdots u_{i_k}P_k(a_{i_k})u_{i_k}^*] \\
&= \tau[(u_{i_k}^* u_{i_1})P_1(a_{i_1})(u_{i_1}^* u_{i_2})\cdots(u_{i_{k-2}}^* u_{i_k})P_k(a_{i_k})] = 0,
\end{aligned}$$

la igualdad a 0 por la igualdad 3.6, de donde se tiene libertad. ■

Demostración alternativa de la Proposición 3.20. Observemos primero que, por lo antes dicho, se tiene lo siguiente

$$\frac{1}{nd}Tr[(\alpha_i Y_i)^k] = \frac{\alpha_i^k}{nd}Tr[X_d^k] \to \alpha_i^k \int t^k \, d\mu(t) = \int u^k D_{\alpha_i}(du),$$

es decir, las variables $\{\alpha_i Y_i\}$ son asintóticamente libres e individualmente cada una de ellas tiene distribución límite $D_{\alpha_i}\mu$. Concluimos por el teorema 3.25 que la distribución límite de X_d^{φ} es

$$\boxplus_{i=1}^{n^2} D_{\alpha_i}[\mu].$$

■

Observación 3.28. A pesar de que, como vimos en la ecuación 3.5, siempre tenemos una descomposición para X_d^{φ} parecida a la dada en esta sección, los resultados probados no aplican. Lo anterior ya que en general no se tiene que los $\tilde{w}_s$ sean unitarios y por tanto, no podemos factorizar los polinomios $P[(I_d \otimes \tilde{w}_s)X_d(I_d \otimes \tilde{w}_s^*)]$ en términos de los polinomios $P(X_d)$ (esa es la única restricción).

Podríamos preguntarnos si la condición unitaria nos permite saltar ese paso para concluir libertad asintótica aún que los $\tilde{w}_s$ no sean unitarios, pero la respuesta es negativa, de hecho en el caso de la transpuesta parcial algunos de los sumandos conmutan, es decir, no son libres (lo que nos dice que no podríamos tener tal factorización).

Planteamos ahora algunos comentarios finales como conclusión del resultado principal de este capítulo.

Observación 3.29.

1. Dado el resultado del teorema 3.24 se sigue que si μ medida con soporte en $[0, \infty)$ y la matriz de Choi es positiva semidefinida, entonces μ^{φ} también tiene soporte positivo. Por lo tanto, para todo funcional cuya matriz de Choi sea positiva semidefinida y para d grande, la matriz modificada a bloques es positiva definida con probabilidad alta.

2. Conocer o aproximar la distribución asintótica μ^{φ} nos ayuda a conocer si la matriz modificada a bloques tiene eigenvalores negativos para d grande con probabilidad alta. Encontrar eigenvalores negativos en la distribución asintótica nos dice que el estado es entrelazado en el límite con probabilidad alta.

Capítulo 4

Conclusiones

Se enlistan en el presente capítulo las conclusiones de este trabajo, así como algunos comentarios sobre los aportes originales del autor y algo de trabajo futuro.

4.1 Conclusiones Generales

La probabilidad libre valuada en operadores nos permite obtener la distribución espectral asintótica de matrices aleatorias modificadas a bloques, para una amplia gama de aplicaciones autoadjuntas φ. Tener dicha distribución nos ayuda a conocer, para d grande y con probabilidad alta, si la matriz aleatoria que representa el estado conjunto de dos sistemas cuánticos (en el caso en el que consideramos aleatoriedad en ellos) tiene o no eigenvalores negativos. Lo anterior, como vimos, nos permite detectar entrelazamiento con probabilidad alta y así, garantizar la transmisión de información en los protocolos de información cuántica.

4.2 Aporte de este Trabajo

El presente trabajo es un texto autocontenido que detalla el problema del entrelazamiento y los criterios existentes en teoría de matrices aleatorias y probabilidad libre para detectarlo y tiene como ventaja que incluye los fundamentos cuánticos y de transmisión de información, así como la exposición detallada de los elementos clásicos de matrices aleatorias, probabilidad libre y probabilidad libre valuada en operadores.

Presenta, por tanto, este trabajo, un punto de partida para investigación futura en la línea de probabilidad libre en la teoría de información cuántica con notación unificada y organización congruente en pos de los objetivos. Es también esta tesis una revisión crítica de los artículos principales en esta línea.

Cabe mencionar que se han añadido detalles a muchas de las demostraciones encontradas en la literatura y que fueron presentadas en este trabajo. Además, las demostraciones de las secciones 1.2.4 y 3.5 son originales. En particular, la demostración de la proposición 3.21 es original de este trabajo y fue citada en [17].

4.3 Trabajo Futuro

Dado el resultado del Teorema 3.24, sospechamos que debe existir una descomposición del tipo

$$X_d^{\varphi} = \sum_{i=1}^{s} \sum_{j=1}^{nd_i} f_{j,i}(X_d),$$

tal que los sumandos sean libres y tal que la distribución espectral asintótica de $f_{j,i}(X_d)$ sea $D_{\rho_i/n\mu}$ para todo j. Sin embargo, este problema sigue abierto.

El problema de caracterizar cuándo una medida perteneciente a una familia paramétrica de distribuciones, tiene o no soporte positivo en términos de los parámetros que la definen, ayudaría para detectar entrelazamiento; algunos ejemplos de esto se expuesieron en los umbrales de entrelazamiento del segundo capítulo, pero para medidas que involucran convoluciones la respuesta no es trivial. Por ejemplo, es de interés conocer bajo qué condiciones se cumple que:

$$\pi \boxtimes \Big(\frac{1}{k} \sum_j \delta_{\lambda_j}\Big) \geq 0.$$

Bibliografía

[1] AARONSON, S. Quantum computing since democritus. Cambrigde University Press, 2013, pp. 109–131.

[2] ANDERSON, G., GUIONNET, A., AND ZEITUNI, O. An introduction to random matrices. Cambrigde University Press, 2010.

[3] ARIZMENDI, O., NECHITA, I., AND VARGAS, C. On the asymptotic distribution of block-modified random matrices. *J. Math. Phys. 57, 015216* (2016).

[4] AUBRUN, G. Partial transposition of random states and non-centered semicircular distributions. *Random Matrices: Theory Appl. 1(02) 1250001* (2012).

[5] AUBRUN, G., SZAREK, S., AND YE, D. Entanglement thresholds for random induced states. *Commun. Pure Appl. Math. 67(1)* (2014), 129–171.

[6] BAI, Z., AND SILVERSTEIN, J. W. *Spectral analysis of large dimensional random matrices*, vol. 20. Springer, 2010.

[7] BANICA, T., AND NECHITA, I. Block-modified wishart matrices and free poisson laws. *Houston Journal of Mathematics 41* (01 2012).

[8] BANICA, T., AND NECHITA, I. Asymptotic eigenvalue distributions of block-transposed wishart matrices. *J. Theor. Probab. 26(3)* (2013), 855–869.

[9] BATHIA, R. *Matrix Analysis*, vol. 169. Springer Science & Business Media, 2013.

[10] BELINSCHI, S., COLLINS, B., AND NECHITA, I. Almost one bit violation for the additivity of the minimum output entropy. *Commun. Math. Phys. 341* (2016), 885–909.

[11] BELINSCHI, S., MAI, T., AND SPEICHER, R. Analytic subordination theory of operator-valued free additive convolution and the solution of a general random matrix problem. *J. Reine Angew Math.* (2013).

[12] BELL, J. On the einstein podolsky rosen paradox. *Physics 1* (1964), 195–200.

[13] BENAYCH-GEORGES, F. Rectangular random matrices, related convolution. *Probab. Theory Relat. Fields 144* (2009), 471–515.

[14] BENAYCH-GEORGES, F. Rectangular random matrices, related free entropy and free fisher's information. *J. Oper. Theory 62(2)* (2009), 371–419.

[15] BENGTSSON, I., AND ŻYCZKOWSKI, K. Geometry of quantum states: An introduction to quantum entanglement. *Cambridge University Press* (2006).

[16] CHOI, M. Completely positive linear maps on complex matrices. *Linear Algebra Appl. 10(3)* (1975), 285–290.

[17] CIPOLLONI, G., AND ERDOS, L. Thermalization for wigner matrices. *arXiv:2102.09975v2* (2021).

[18] COLLINS, B., HAYDEN, P., AND NECHITA, I. Random and free positive maps with applications to entanglement detection. *International Mathematics Research Notices Vol. 2017, No. 3* (2017), 869–894.

[19] COLLINS, B., AND NECHITA, I. Random quantum channels i: Graphical calculus and the bell state phenomenon. *Commun. Math. Phys. 297(2)* (2010), 345–370.

[20] COLLINS, B., AND NECHITA, I. Gaussianization and eigenvalue statistics for random quantum channels (iii). *Ann. Appl. Probab. 21* (2011), 1136–1179.

[21] COLLINS, B., AND NECHITA, I. Random quantum channels ii: Entanglement of random subspaces, rényi entropy estimates and additivity problems. *Adv. Math. 226(2)* (2011), 1181–1201.

[22] COLLINS, B., AND NECHITA, I. Random matrix techniques in quantum information theory.

[23] COUILLET, R., AND DEBBAH, M. Random matrix methods for wireless communications. *Cambridge University Press, Cambridge* (2011).

[24] DE LLANO, M. Mecánica cuántica. In *Temas de Física*. Las Prensas de Ciencias, Ed. 3, 2015.

[25] DIAZ, M., AND PÉREZ-ABREU, V. On the capacity of block multiantenna channels. *IEEE Transactions on Information Theory* (2017).

[26] DYKEMA, K. On the s-transform over a banach algebra. *J. Funct. Anal. 231(1)* (2006), 90–110.

[27] GRIFFITHS, D. Introduction to quantum mechanics. Prentice Hall Inc., 1995.

[28] HORODECKI, R., HORODECKI, P., HORODECKI, M., AND HORODECKI, K. Quantum entanglement. *Rev. Mod. Phys. 81(2), 865* (2009).

[29] LLUIS-PUEBLA, E. Álgebra lineal, Álgebra multilineal y k-teoría algebraica. Publicaciones Electrónicas de la SMM, Vol. 9, 2008.

[30] MINGO, J., AND SPEICHER, R. Free probability and random matrices. *The Fields Institute for Research in Mathematical Sciences* (2017).

[31] MURPHY, G. c^*-algebras and operator theory. Academic Press, Inc., 1990.

[32] NECHITA, I. Applications of random matrices in quantum information theory. *Notes for ICMAT in Madrid* (2019).

[33] NECHITA, I., PUCHAŁA, Z., PAWELA, L., AND ŻYCZKOWSKI, K. Almost all quantum channels are equidistant. *J. Math. Phys. 59, 052201* (2018).

[34] NICA, A., AND R.SPEICHER. Lectures on the combinatorics of free probability. *London Mathematical Society Lecture Notes 335, Cambridge University Press* (2006).

[35] NICA, A., SHLYAKHTENKO, D., AND SPEICHER, R. Operator-valued distributions. i. characterizations of freeness. *Int. Math. Res. Not. 29* (2002), 1509–1538.

[36] NIELSEN, M., AND CHUANG, I. Quantum computation and quantum information. In *10th anniversary ed*. Cambrigde University Press, 2010.

[37] PERES, A. Separability criterion for density matrices. *Phys. Rev. Lett. 77(8), 1413* (1996).

[38] RUDIN, W. Functional analysis.

[39] S.BELINSCHI, SPEICHER, R., TREILHARD, J., AND VARGAS, C. Operator-valued free multiplicative convolution: analytic subordination theory and applications to random matrix theory. *International Mathematical Research Notices* (2014), 5933–5958.

[40] SHANNON, C. E. A mathematical theory of communication, part i, part ii. *Bell Syst. Tech. J. 27* (1948), 623–656.

[41] SPEICHER, R. Combinatorial theory of the free product with amalgamation and operator-valued free probability theory. *Memoir of the AMS 627* (1998).

[42] SPEICHER, R., AND VARGAS, C. Free deterministic equivalents, renctangular random matrix models and operator-valued free probability. *Random Matrices: Theory and Applications 01, 1150008* (2012).

[43] TAO, T. Topics in Random Matrix Theory. In *Deutsche Mathematiker-Vereinigung*. Springer-Verlag Berlin Heidelberg, 2013.

[44] TELATAR, E. Capacity of multi-antenna gaussian channels. *Transactions on Emerging Telecommunications Technologies 10*, 6 (1999), 585–595.

[45] VARGAS, C. A general solution to (free) deterministic equivalents. *Contemporary Mathematics 709* (2018).

[46] VEDRAL, V. Introduction to quantum information science. Oxford University Press, 2006.

[47] VOICULESCU, D. Limit laws for random matrices and free products. *Invent. Math. 104* (1991), 201–220.

[48] WILDE, M. Quantum information theory. In *2nd ed*. Cambrigde University Press, 2017.