Universidad de Guanajuato

El teorema de De Finetti

T E S I S

Que para obtener el título de

Licenciado en Matemáticas

P R E S E N T A:

Daniel Muñoz George

Directores de Tesis:

Dr. Octavio Arizmendi Echegaray
Dr. Arno Siri Jégousse

GUANAJUATO, GTO SEPTIEMBRE 2016

Agradecimentos

Antes que nada quiero agradecer a mis padres, Humberto y Daniela, quienes me han apoyado en todo momento a lo largo de mi vida, sobre todo cuando decidí emprenderme en este bello proyecto de vida que son las matemáticas, sin ustedes nada de esto hubiera sido posible.

Agradezco a mis hermanos, Humberto y Kevin, quienes han estado conmigo en todo momento, su apoyo y amor me han hecho crecer no sólo como estudiante si no también como persona impulsándome a ser mejor cada día. Gracias mi novia, Carmen, por todo el apoyo brindado a lo largo de mis últimos años de carrera, por animarme en aquellos momentos difíciles que pase a lo largo de mi formación.

Quiero agradecer también a mis asesores de tesis, Dr. Arno Siri Jégousse y Dr. Octavio Arizmendi Echegaray, por el apoyo que me brindaron al momento de redactar esta tesis, así como el tiempo que se tomaron en revisar cada detalle.

Agradezco también a mis sinodales, Dr. Carlos Vargas Obieta, Dr. Antonio Murillo Salas y Dr. Pierre Tarrago, por el tiempo dedicado en la lectura de esta tesis.

Finalmente quiero agradecer a la comunidad CIMAT-DEMAT, por permitirme ser parte de uno de ellos y ayudarme a crecer como estudiante. Gracias por el apoyo recibido tanto económicamente como académicamente. De manera particular agradezco a mis amigos mas cercanos, Carlos, Miguel y Javier, quienes estuvieron conmigo a lo largo de mi carrera.

Índice general

Introducción

En 1924, William Ernest Johnson [2] introdujo el concepto de intercambiabilidad de una sucesión de variables aleatorias. La intercambiabilidad nos dice que la distribución de una sucesión de variables aleatorias es invariante bajo permutaciones finitas. En particular, una sucesión de variables idénticamente distribuidas es intercambiable. Lo que significa que el concepto de intercambiabilidad generaliza el concepto de ser idénticamente distribuidas. En esta tesis se estudia el concepto de intercambiabilidad de variables aleatorias en probabilidad clásica y en probabilidad no conmutativa.

Una duda inmediata es como caracterizar a dichas sucesiones. Durante los años 30, Bruno De Finetti presentó y demostró el teorema que caracteriza las sucesiones intercambiables. Este último nos dice que una sucesión es intercambiable si y sólo si es independiente e idénticamente distribuida dada una medida aleatoria. El teorema de De Finetti juega un rol crucial dentro de la estadística Bayesiana, pues muchas veces pedir que la muestra sea idénticamente distribuida es muy restrictivo, sin embargo varias muestras cumplen la asunción de intercambiabilidad. Numerosas aplicaciones del teorema de De Finetti han sido desarrolladas en estadística Bayesiana.

En la primera parte de esta tesis se hablará de la intercambilidad y del teorema de De Finetti. Presentaremos la demostración de este teorema y se extenderá el mismo para el caso de particiones aleatorias intercambiables ambos basándonos en [1]. Una partición es una colección de conjuntos disjuntos y cuya unión es el espacio total. Este concepto es de gran utilidad en estadística pues muchas veces podemos agrupar la muestra en conjuntos de acuerdo a lo que estemos interesados obtener. Dichos conjuntos forman una partición y si la muestra original es intercambiable entonces la nueva partición resultará intercambiable. La primera parte de este trabajo termina brindando un teorema para particiones aleatorias intercambiables análogo al teorema de De Finetti dearrollado por John Frank Charles Kingman desarrollado en [3].

La segunda parte de este trabajo se enmarca en la teoría de probabilidad libre. Esta teoría fue iniciada, alrededor del año de 1986, por Dan Voiculescu en [10], donde introdujo el concepto de independencia libre y desarrolló las primeras herramientas de probabilidad libre. La probabilidad libre busca desarrollar un espacio de probabilidad en donde las variables aleatorias son operadores en un espacio de Hilbert, y contrario a como sucede en el caso clásico las variables aleatorias no son necesariamente conmutativas. La probabilidad libre mantiene muchas de las ideas de la probabilidad clásica, tales como la independencia y la esperanza, pero presentadas en el caso no conmutativo. En el último siglo se ha trabajado y desarrollado un glosario muy extenso en el área de probabilidad libre. Se han demostrado varios teoremas en esta área los cuales tienen una versión análoga en el caso clásico. Fue el mismo Voiculescu quien presentó la prueba del teorema del Límite Central en su versión no conmutativa.

En la segunda parte de esta tesis daremos pie a la versión libre del teorema de De Finetti, demostrada por Koestler y Speicher [4]. Para esto, primero, se introducirán de manera rápida las herramientas básicas de probabilidad libre y después hablaremos de la intercambiabilidad en el sentido cuántico la cual generaliza el concepto de intercabiabilidad clásica. Finalizaremos presentando y demostrando el teorema de De Finetti en el caso libre, el cual nos dice que la sucesión es independiente en el sentido libre e idénticamente distribuida dada una álgebra si y sólo si la sucesión es intercambiable en el sentido cuántico.

Capítulo 1

Intercambiabilidad y el caso clásico

1.1. Definiciones preliminares

En esta sección se describirán algunas nociones de probabilidad clásica y demás conceptos que se usarán más adelante para dar nuevas definiciones que irán dirigidas al tema a tratar en este trabajo.

Definición 1. Definimos un espacio de medida como un par $(\Omega, \mathcal{F})$, tal que Ω es un conjunto cualquiera, $\mathcal{F}$ es una familia de subconjuntos de Ω llamado σ-álgebra que cumple

1. $\Omega \in \mathcal{F}$
2. Si $A \in \mathcal{F}$ entonces $A^c \in \mathcal{F}$
3. Si $A_1, A_2, .. \in \mathcal{F}$ entonces $\cup_{i\geq 1} A_i \in \mathcal{F}$.

podemos aditar al par $(\Omega, \mathcal{F})$ con una medida μ, la cual es un mapeo $\mu : \mathcal{F} \to [0, \infty]$ tal que

1. $\mu(\emptyset) = 0$
2. para $A_1, A_2, .. \in \mathcal{F}$ disjuntos a pares se cumple $\mu(\cup_{i\geq 1} A_i) = \sum_{i\geq 1} \mu(A_i)$

Diremos además que un espacio de medida tal que $\mu(\Omega) = 1$ es un espacio de probabilidad y denotaremos comúnmente $\mathbb{P} = \mu$, en este caso Ω se conoce como espacio muestral el cual no tiene porqué ser un subconjunto de $\mathbb{R}$. Un ejemplo es el experimento de lanzar una moneda, donde $\Omega = \{Aguila, Sol\}$, $\mathcal{F}$ puede ser 2^Ω el espacio potencia de todas los posibles subconjuntos de Ω y podemos asignar la medida $\mathbb{P}(\{Aguila\}) = \mathbb{P}(\{Sol\}) = \frac{1}{2}$ si la moneda es balanceada. Esto en principio genera un problema cuantitativo, pues queremos una herramienta donde medir con facilidad las probabilidades en un ambiente puramente numérico, esto motiva a la definición de lo que es una variable aleatoria real, que lo que hace es aterrizar el espacio muestral en $\mathbb{R}$ para facilitar la manipulación matemática.

Definición 2. Una variable aleatoria es un mapeo entre dos espacios de medida, $X : (\Omega, \mathcal{F}) \to (E, \mathcal{E})$ tal que $X^{-1}(A) \in \mathcal{F}$ para toda $A \in \mathcal{E}$. Si además $(E, \mathcal{E}) = (\mathbb{R}, \mathcal{B}(\mathbb{R}))$ decimos que X es una variable aleatoria real. Por supuesto tiene sentido considerar un vector de variables aleatorias reales como una $n-$tupla $Y : \Omega \to \mathbb{R}^n$. Dadas una variable aleatoria real X y una medida $\mathbb{P}$ en $(\Omega, \mathcal{F})$ definimos $\mathbb{P}(X \in A) = \mathbb{P}(\{X^{-1}(A)\})$ para toda $A \in \mathcal{B}(\mathbb{R})$, y su función de distribución F como $F(x) = \mathbb{P}(X \leq x)$ para todo $x \in \mathbb{R}$.

Además existen ciertos valores que nos interesarán obtener de una variable aleatoria real X pues nos darán información de valor del experimento, tales como la media y varianza.

Definición 3. Dada una variable aleatoria real X con soporte $S(X)$ definimos:

1. Su media como $\mathbb{E}(X) = \int_{S(X)} x dF(x)$ y la denotamos por μ_X

2. Su varianza como $\mathbb{E}((X - \mathbb{E}(X))^2) = \int_{S(X)} (x - \mathbb{E}(X))^2 dF(x)$ y la denotamos por σ_X^2

Definición 4. Dadas dos variable aleatorias reales X, Y sobre el mismo espacio de probabilidad definimos:

1. su covarianza como $Cov(X, Y) = \mathbb{E}((X - \mathbb{E}(X))(Y - \mathbb{E}(Y)))$

2. su correlación como $\rho(X, Y) = \frac{Cov(X,Y)}{\sigma_X^2 \sigma_Y^2}$

3. Decimos que son independiente si $\mathbb{P}(X \in A, Y \in B) = \mathbb{P}(X \in A)\mathbb{P}(Y \in B)$ para todas $A, B \in \mathcal{B}(\mathbb{R})$.

4. Decimos que $X = Y$ casi seguramente(c.s) si $\mathbb{P}(X = Y) = \mathbb{P}(\{w \in \Omega | X(w) = Y(w)\}) = 1$

Definición 5. Decimos que dos sucesiónes de variables aleatorias reales $(Z_1, Z_2, ...,)$, $(Y_1, Y_2, ...,)$ son iguales en distribución si

$$\mathbb{P}(Z_1 \leq z_1, Z_2 \leq z_2, ..., Z_n \leq z_n) = \mathbb{P}(Y_1 \leq z_1, Y_2 \leq z_2, ..., Y_n \leq z_n),$$

para toda $n \in \mathbb{N}$, para toda $(z_1, z_2, ..., z_n) \in \mathbb{R}^n$, y en ese caso escribimos

$$(Z_1, Z_2, ...,) \stackrel{d}{=} (Y_1, Y_2, ...,).$$

Definición 6. Para $n \in \mathbb{N}$ definimos $\mathbb{N}_n = \{1, 2, ..., n\}$, sea $S(n) = \{f | f : \mathbb{N}_n \to \mathbb{N}_n$ tal que f es biyectiva $\}$ como el conjunto de permutaciones de n elementos. Una transposición es un elemento de $S(n)$ que deja invariante todos los elementos salvo dos que intercambian mutuamente.

Con estos conceptos podemos pasar cómodamente a hablar del teorema de De Finetti, sin embargo en el mismo capítulo se vera una extensión de dicho teorema a particiones aleatorias intercambiables, estamos entonces en el deber de introducir que es una partición.

Definición 7. Para $n \in \mathbb{N}$ denotamos por $P(n)$ el conjunto de particiones de $\mathbb{N}_n$, dado por $\{(A_1, ..., A_k) | A_i \subset \mathbb{N}_n, A_i \cap A_j = \emptyset, \forall i \neq j, \cup_{i=1}^{k} A_i = \mathbb{N}_n,$ con $1 \leq k \leq n\}$. Una partición aleatoria es una variable aleatoria con contradominio en $P(n)$.

No habrá necesidad de introducir que es intercambiabilidad en el sentido de particiones aleatorias pues sobre la marcha del teorema se mencionará. Estamos entonces listos para introducirnos en el teorema de De Finetti y su respectiva versión para el caso de particiones.

1.2. Definiciones y consecuencias inmediatas

Para esta sección comenzaremos introduciendo algunas definiciones y primeros ejemplos del concepto de intercambiabilidad. Esta definición generaliza la noción de ser idénticamente distribuido y es la que se estudiará en este trabajo.

Definición 8. (i) Una sucesión finita $(Z_1, ..., Z_n)$ se dice que es n-intercambiable si se cumple que

$$(Z_1, ..., Z_n) \stackrel{d}{=} (Z_{\sigma(1)}, ..., Z_{\sigma(n)}), \tag{1.2.1}$$

para toda $\sigma \in S(n)$.

(ii) Una sucesión infinita $(Z_1, Z_2, ..)$ es intercambiable si

$$(Z_1, Z_2, ...) \stackrel{d}{=} (Z_{\sigma(1)}, Z_{\sigma(2)}, ...), \tag{1.2.2}$$

para toda $\sigma \in S(n)$ para toda $n \in \mathbb{N}$.

De ahora en adelante se entenderá que si decimos que $(Z_i)_i$ es n-intercambiable entonces $(Z_i)_i = (Z_1, ..., Z_n)$. Haciendo uso de que toda permutación finita $\sigma \in S(n)$ puede escribirse como composición de transposiciones que cambian a 1 con m para $1 \leq m \leq n$, podemos reescribir (1.2.2) en la Definición 8 como sigue: una sucesión infinita $(Z_1, Z_2, ..)$ es intercambiable si

$$(Z_1, Z_2, ..., Z_{n-1}, Z_n, Z_{n+1}, ...) \stackrel{d}{=} (Z_n, Z_2, ..., Z_{n-1}, Z_1, Z_{n+1}, ...), \tag{1.2.3}$$

para toda $n > 1$.

Pasaremos a enunciar algunos ejemplos.

Ejemplo 9. Suponga que una urna contiene n bolas etiquetadas como $x_1, ..., x_n$. Sea Z_i la bola obtenida en el turno i considerando que hay remplazo, es decir podemos tomar más de una vez la misma bola. Entonces la sucesión $(Z_1, Z_2, ...)$ forma una sucesión infinita intercambiable.

Demostración. Se sigue de manera inmediata del hecho de que $(Z_n)_n$ es una sucesión de variables aleatorias i.i.d distribuidas uniformemente en $\{x_1, ..., x_n\}$. Luego para $\sigma \in S(n)$ con $n \in \mathbb{N}$ tenemos,

$$\mathbb{P}(Z_1 \leq z_1, ..., Z_m \leq z_m) = \mathbb{P}(Z_{\sigma(1)} \leq z_1, ..., Z_{\sigma(m)} \leq z_m), \forall m \in \mathbb{N}$$

al ser $(Z_i)_i$ idénticamente distribuidas. □

Este ejemplo deja más claro el hecho que se mencionó al inicio de que el concepto de intercambiabilidad generaliza el concepto de ser idénticamente distribuido.

Ejemplo 10. Haciendo uso del ejemplo anterior pero ahora sea $Z_1, ..., Z_n$ los tiros sin remplazo de la urna, esto genera una sucesión n-intercambiable.

Demostración. En efecto como sacamos cada bola con la misma probabilidad $\frac{1}{n}$ para Z_1 , $\frac{1}{n-1}$ para Z_2 de las restantes y así sucesivamente, podemos pensar $Z_1, ..., Z_n$ como un reordenamiento de $x_1, .., x_n$ y dado la uniformidad entonces $(Z_1, .., Z_n)$ es la permutación uniforme de $x_1, .., x_n$, es decir,

$$(Z_1, .., Z_n) = (x_{\sigma^*(1)}, ..., x_{\sigma^*(n)}),$$

donde σ^* es la permutación uniforme aleatoria en $\{1, 2, .., n\}$. Entonces $P(\sigma^* = \sigma) = \frac{1}{n!}$ para todo $\sigma \in S(n)$, así para $\pi \in S(n)$ tenemos,

$$\begin{aligned}\mathbb{P}(Z_1 = z_1, ..., Z_n = z_n) &= \mathbb{P}(x_{\sigma^*(1)} = z_1, ..., x_{\sigma^*(n)} = z_n) \\ &= \mathbb{P}(x_{\sigma^*(\pi(1))} = z_1, ..., x_{\sigma^*(\pi(n))} = z_n) \\ &= \mathbb{P}(Z_{\pi(1)} = z_1, ..., Z_{\pi(n)} = z_n)\end{aligned}$$

donde se uso en la segunda igualdad que σ^* es la permutación uniforme. $\square$

1.3. Estructura de correlación

Ahora veremos que las variables aleatorias de las sucesiones N-intercambiables presentan un coeficiente de correlación es cúal está acotada en algún intervalo A, mas aún veremos que para cualquier $x \in A$ existirá una sucesión N-intercambiable tal que el coeficiente de correlación de sus elementos es x.

Teorema 11. *Sea $(Z_i)_i$ una sucesión de variables aleatorias N-intercambiable, entonces existe un coeficiente de correlación $\rho = \rho(Z_i, Z_j)$ para $i \neq j$, el cual no depende de la elección de i y j, tal que*

$$\rho \geq \frac{-1}{N-1},$$

con igualdad si y solo si $\sum_{i=1}^{N} Z_i = c$ casi seguramente para alguna $c \in \mathbb{R}$.

Demostración. Para la demostración supongamos sin pérdida de la generalidad que $\mathbb{E}(Z_i) = 0$ y $\mathbb{E}_(Z_i^2) = 1$ para toda i, así:

$$0 \leq \mathbb{E}((\sum_{i=1}^{N} Z_i)^2) = \sum_{i=1}^{N} \mathbb{E}(Z_i^2) + \sum_{1\leq i\neq j\leq N} \mathbb{E}(Z_i Z_j) = N + N(N-1)\rho$$

de donde $\rho \geq \frac{-1}{N-1}$ con igualdad si y sólo si $\mathbb{E}((\sum_{i=1}^{N} Z_i)^2) = 0$, lo cúal pasa si y sólo si $\sum_{i=1}^{N} Z_i = 0$ casi seguramente, que en el caso general es cuando $\sum_{i=1}^{N} Z_i = c$ casi seguramente para alguna $c \in \mathbb{R}$. $\square$

Algo que cabe notar es que si hacemos $N \to \infty$ tenemos que $\rho \geq 0$ para una sucesión infinita intercambiable. El converso del teorema también se cumple.

Teorema 12. *Si $\frac{-1}{N-1} \leq \rho < 1$ entonces ρ es el coeficiente de correlación de alguna sucesión N-intercambiable.*

Demostración. Para la prueba construiremos dicha sucesión; sea $(\chi_i)_i$ una sucesión de variables aleatorias i.i.d con $\mathbb{E}(\chi_1) = 0$ y $\mathbb{E}(\chi_1^2) = 1$, definimos

$$Z_i = \chi_i + c\sum_{j=1}^{N} \chi_j,$$

para $1 \leq i \leq N$ y para alguna $c \in \mathbb{R}$, así tenemos que $(Z_i)_i$ es N-intercambiable pues de hecho la sucesión $(Z_i)_i$ es idénticamente distribuida.

Bastará ver que $\rho = \rho(Z_i, Z_j)$. Para esto notemos que $\mathbb{E}(Z_i) = 0$ para toda i, así para $i \neq j$

$$\begin{aligned}
\rho(Z_i, Z_j) &= \frac{\mathbb{E}(Z_i Z_j)}{\sqrt{\mathbb{E}(Z_i^2)\mathbb{E}(Z_j^2)}} \\
&= \frac{\mathbb{E}(\chi_i\chi_j + c\sum_{k=1}^N \chi_i\chi_k + c\sum_{k=1}^N \chi_j\chi_k + c^2(\sum_{k=1}^N \chi_k)^2)}{\mathbb{E}(\chi_i\chi_i + 2c\sum_{k=1}^N \chi_i\chi_k + c^2(\sum_{k=1}^N \chi_k)^2)} \\
&= \frac{\mathbb{E}(\chi_i\chi_j) + c\mathbb{E}(\sum_{k=1}^N \chi_i\chi_k) + c\mathbb{E}(\sum_{k=1}^N \chi_j\chi_k) + c^2\mathbb{E}((\sum_{k=1}^N \chi_k)^2)}{\mathbb{E}(\chi_i\chi_i) + 2c\mathbb{E}(\sum_{k=1}^N \chi_i\chi_k) + c^2\mathbb{E}((\sum_{k=1}^N \chi_k)^2)} \\
&= \frac{2c + c^2\mathbb{E}((\sum_{k=1}^N \chi_k)^2)}{1 + 2c + c^2\mathbb{E}((\sum_{k=1}^N \chi_k)^2)} \\
&= \frac{2c + c^2\mathbb{E}(\sum_{k=1}^N \chi_k^2 + \sum_{1\leq j\neq k\leq N}\sum \chi_j\chi_k)}{1 + 2c + c^2\mathbb{E}(\sum_{k=1}^N \chi_k^2 + \sum_{1\leq j\neq k\leq N}\sum \chi_j\chi_k)} \\
&= \frac{Nc^2 + 2c}{Nc^2 + 2c + 1} = 1 - \frac{1}{Nc^2 + 2c + 1}.
\end{aligned}$$

Por lo tanto tenemos que $\rho(Z_i, Z_j) = \rho(c) = 1 - \frac{1}{Nc^2+2c+1}$. Notemos que $0 \leq \rho(c) \leq 1$. Finalmente veremos que $\frac{-1}{N-1} \leq \rho(c) < 1$ para concluir la prueba. Para verificar esto basta usar el método de máximos y mínimos y verificar que en efecto $c = \frac{-1}{N}$ es un mínimo de la función con $\rho(c) = \frac{-1}{N-1}$. Es decir dado $\frac{-1}{N-1} \leq \rho < 1$ podemos hallar $c \in \mathbb{R}$ tal que $\rho(Z_i, Z_j) = \rho(c) = \rho$

pues la función $\rho(c)$ es claramente continua en $[\frac{-1}{N}, \infty)$ con mínimo $\frac{-1}{N-1}$ y supremo claramente 1. La sucesión $(Z_i)_i$ con correlación $\rho(c)$ cumple lo especificado y con esto concluimos la demostración. $\square$

Podemos extender el teorema anterior al caso infinito de la siguiente manera.

Teorema 13. *Si $0 \leq \rho < 1$, entonces ρ es el coeficiente de correlación de alguna sucesión infinita intercambiable .*

Demostración. Nuevamente la prueba se basa en la construcción de dicha sucesión, tomando $(\chi_i)_{i\geq 0}$ y definiendo $Z_i = c\chi_0 + \chi_i$ con $c \in \mathbb{R}$ tenemos nuevamente que $(Z_i)_i$ es intercambiable y $\rho(Z_i, Z_j) = \rho(c) = \frac{c^2}{c^2+1}$, de la misma manera que antes variando c obtenemos que $0 \leq \rho(c) < 1$ y concluimos como en el Teorema 12. $\square$

1.4. Mezcla de sucesiones independientes e idénticamente distribuidas

Con el concepto de intercambiabilidad ya claro no nos queda más que abrir paso al concepto de lo que es una mezcla de sucesiones independientes e idéntidamente distribuidas, pues nuestro teorema principal, el teorema de De Finetti nos dice precisamente que estos dos conceptos son equivalentes.

Comencemos dando una idea intuitiva de lo que significa una mezcla de sucesiones independientes e idénticamente distribuidas. Sean $\theta_1, ..., \theta_k$ distribuciones de probabilidad reales y $p_1, .., p_k > 0$, con $\sum_{i=1}^{k} p_i = 1$, podemos construir una sucesión de variables aleatorias $(Y_i)_i$ de la siguiente manera:

1. Seleccionamos θ de manera aleatoria en $\{\theta_1, ..., \theta_k\}$ con probabilidades p_k, es decir $\mathbb{P}(\theta = \theta_i) = p_i$

2. Generamos $(Y_i)_i$ una sucesión i.i.d con distribución θ

Lo que esto nos dice es que $(Y_i)_i$ es i.i.d con distribución θ pero θ es aleatorio, a la sucesión $(Y_i)_i$ es a lo que conocemos como mezcla de sucesiones independientes e idénticamente distribuidas y la distribución de θ es lo que más adelante conoceremos como medida aleatoria. Mas generalmente sean P el conjunto de medidas de probabilidad en $\mathbb{R}$, μ una distribución en P y ahora seleccionamos θ con distribución μ, luego generamos $(Y_i)_i$ una sucesión i.i.d con distribución θ. Una manera de formalizar esta descripción es la siguiente.

$$\mathbb{P}(Y \in A) = \int_P \prod_{i \geq 1} \theta(A_i)\mu(d\theta), \tag{1.4.1}$$

con $A = (A_1, A_2, ...) \in \mathcal{B}(\mathbb{R})^\infty$ y Y es la sucesión $(Y_i)_i$. Lo que esto último nos dice es que condicional a que $\theta = \tau$ entonces la sucesión $(Y_i)_i$ es i.i.d con distribución τ.

Ya con la idea podemos introducir la definición formal de medida aleatoria, además podemos dar paso a introducir lo que es una distribución condicional regular la cual estará estrechamente ligada con lo que es una medida aleatoria. Una medida aleatoria α es una simple variable aleatoria P-valuada. Así para cada $\omega \in \Omega$ tenemos que $\alpha(\omega)$ es una medida de probabilidad y asigna probabilidades $\alpha(\omega, A)$ para todo $A \in \mathcal{B}(\mathbb{R})$.

Definición 14. Una medida aleatoria es un mapeo $\alpha : \Omega \times \mathcal{B}(\mathbb{R}) \to \mathbb{R}$ tal que $\alpha(\omega, *)$ es una medida de probabilidad para todo $\omega \in \Omega$ y $\alpha(*, A)$ es una variable aleatoria para todo $A \in \mathcal{B}(\mathbb{R})$.

Definición 15. Dada una variable aleatoria real Y sobre un espacio de probabilidad $(\Omega, \mathcal{A})$ y una σ-álgebra $\mathcal{F} \subset \mathcal{A}$, una distribución condicional regular para Y dada $\mathcal{F}$ es una medida aleatoria $\alpha : \Omega \times \mathcal{B}(\mathbb{R}) \to \mathbb{R}$ tal que

$$\alpha(\cdot, A) \overset{c.s}{=} \mathbb{P}(Y \in A|\mathcal{F})(\cdot), \text{ para toda } A \in \mathcal{B}(\mathbb{R})$$

Es sabido que dicha distribución condicional regular existe y es única casi seguramente.

Como punto de observación notemos que dada α una medida aleatoria, es posible construir una sucesión $(Y_i)_i$ tal que dada $\alpha = \theta$ la sucesión $(Y_i)_i$ es independiente e idénticamente distribuida con distribución θ. La idea intuitiva de la construcción es que si $F(\theta; x)$ es la función de distribución de θ y $F^{-1}(\theta; x) = inf\{t|F(\theta; t) \geq x\}$ la inversa generalizada, si $\chi \sim U(0, 1)$ entonces $F^{-1}(\theta, \chi)$ es una variable aleatoria con distribución θ. Así tomando $(\chi_i)_i$ i.i.d como $U(0, 1)$ tenemos que la sucesión $(F^{-1}(\theta, \chi_i))$ es i.i.d con distribución θ. Ahora para α medida aleatoria tomamos $\hat{Y}_i = F^{-1}(\alpha, \chi_i)$, esto nos dice que dada $\alpha = \theta$ la sucesión $(\hat{Y}_i)_i$ es i.i.d con distribución θ.

Tenemos así que una sucesión $Y = (Y_i)_i$ es una mezcla de sucesiones independientes e idénticamente distribuidas si podemos ver la distribución de Y como en (1.4.1). Entonces surge la pregunta natural de para qué nos van a servir todas las previas definiciones que hemos dado, para responder esta pregunta bastará dar una última definición la cual ligará todas las anteriores con (1.4.1).

Definición 16. Sean $Y = (Y_i)_i$ una sucesión de variables aleatorias definidas sobre un espacio de probabilidad $(\Omega, \mathcal{A})$ y α una medida aleatoria sobre el mismo espacio de probabilidad. Se dice que Y es una mezcla de sucesiones i.i.d dirigidas por α si

$$\alpha \times \alpha \times \alpha ...$$

es una distribución condicional regular (d.c.r) para Y dada $\sigma(\alpha)$.

Por definición de distribución condicional regular esto nos dice que dado $A = (A_1, A_2, ...) \in \mathcal{B}(\mathbb{R})^\infty$ se tiene que

$$\mathbb{P}(Y_i \in A_i | \alpha)(\omega) \stackrel{c.s}{=} \prod_{i \geq 1} \alpha(\omega, A_i)$$

Luego la distribución de Y es de la forma (1.4.1) pues

$$\mathbb{P}(Y \in A) = \int_\Omega \prod_{i \geq 1} (\alpha(\omega, A_i))\mu(d\omega),$$

donde μ es la distribución de α. Es decir tenemos precisamente que Y es una mezcla de sucesiones i.i.d. Entonces basta que $Y = (Y_i)_i$ sea una mezcla de sucesiones i.i.d dirigidas por alguna medida aleatoria para que Y sea una mezcla de sucesiones independientes e idénticamente distribuidas.

Ahora veremos que si una sucesión infinita $(Z_i)_i$ cumple que es i.i.d dada $\mathcal{F}$ una σ-álgebra que cumple ciertas condiciones, entonces $(Z_i)_i$ es una mezcla de sucesiones i.i.d. Para esto introduciremos dos lemas.

Lema 17. *Sean $(Y_i)_i$ una sucesión de variables aleatorias reales sobre $(\Omega, \mathcal{A})$, suponga que $(Y_i)_i$ es condicionalmente i.i.d dada una σ-álgebra $\mathcal{F} \subset \mathcal{A}$. Sea α una distribución condicional regular de Y_1 dada $\mathcal{F}$ entonces $(Y_i)_i$ es una mezcla de sucesiones i.i.d dirigidas por α.*

Demostración. Sabemos que como $(Y_i)_i$ es idénticamente distribuida dada $\mathcal{F}$ entonces α es d.c.r de Y_i dada $\mathcal{F}$ para toda $i \geq 1$. Por otro lado como $(Y_i)_i$ es independiente dada $\mathcal{F}$ tenemos $\mathbb{P}(Y \in A | \mathcal{F}) = \prod_{i \geq 1} \alpha(\cdot, A_i)$.

Además tenemos que α es $\mathcal{F}$-medible, luego condicionando en α esto nos da $\mathbb{P}(Y \in A|\alpha) = \prod_{i\geq 1} \alpha(\cdot, A_i)$, es decir $(Y_i)_i$ es una mezcla de sucesiónes independientes e idénticamente distribuidas dirigidas por α. $\square$

Lema 18. *Sea Y una variable aleatoria real y acotada sobre $(\Omega, \mathcal{A})$ y sean $\mathcal{F} \subset \mathcal{G} \subset \mathcal{A}$ σ-álgebras. Si $\mathbb{E}(\mathbb{E}(Y|\mathcal{G})^2) = \mathbb{E}(\mathbb{E}(Y|\mathcal{F})^2)$, en particular si $\mathbb{E}(Y|\mathcal{G}) \overset{d}{=} \mathbb{E}(Y|\mathcal{F})$, entonces $\mathbb{E}(Y|\mathcal{G}) = \mathbb{E}(Y|\mathcal{F})$ casi seguramente.*

Demostración. Para la prueba usaremos las siguientes propiedades

1. $\mathbb{E}(X+Y) = \mathbb{E}(X) + \mathbb{E}(Y)$ para X, Y v.a
2. $\mathbb{E}(X) = \mathbb{E}(\mathbb{E}(X|\mathcal{F}))$ para cualquier v.a X
3. Si X es $\mathcal{F}$-medible entonces $E(XY|\mathcal{F}) = XE(Y|\mathcal{F})$
4. $\mathbb{E}(Y|\mathcal{F}) = \mathbb{E}(\mathbb{E}(Y|\mathcal{G})|\mathcal{F})$

Notemos que

$$\begin{aligned}
&\mathbb{E}((\mathbb{E}(Y|\mathcal{G}) - \mathbb{E}(Y|\mathcal{F}))^2) \\
&= \mathbb{E}(\mathbb{E}(Y|\mathcal{G})^2 - 2\mathbb{E}(Y|\mathcal{G})\mathbb{E}(Y|\mathcal{F}) + \mathbb{E}(Y|\mathcal{F})^2) \\
&= \mathbb{E}(\mathbb{E}(Y|\mathcal{G})^2) - 2\mathbb{E}(\mathbb{E}(Y|\mathcal{F})\mathbb{E}(Y|\mathcal{G})) + \mathbb{E}(\mathbb{E}(Y|\mathcal{F})^2) \text{ por } (1) \\
&= \mathbb{E}(\mathbb{E}(Y|\mathcal{G})^2) - 2\mathbb{E}(\mathbb{E}(\mathbb{E}(Y|\mathcal{F})\mathbb{E}(Y|\mathcal{G})|\mathcal{F})) + \mathbb{E}(\mathbb{E}(Y|\mathcal{F})^2) \text{ por}(2)
\end{aligned}$$

Usando que $\mathbb{E}(Y|\mathcal{F})$ es $\mathcal{F}$-medible tenemos que

$$\begin{aligned}
&\mathbb{E}((\mathbb{E}(Y|\mathcal{G}) - \mathbb{E}(Y|\mathcal{F}))^2) \\
&= \mathbb{E}(\mathbb{E}(Y|\mathcal{G})^2) - 2\mathbb{E}(\mathbb{E}(Y|\mathcal{F})\mathbb{E}(\mathbb{E}(Y|\mathcal{G})|\mathcal{F})) + \mathbb{E}(\mathbb{E}(Y|\mathcal{F})^2) \text{ por}(3) \\
&= \mathbb{E}(\mathbb{E}(Y|\mathcal{G})^2) - 2\mathbb{E}(\mathbb{E}(Y|\mathcal{F})\mathbb{E}(Y|\mathcal{F})) + \mathbb{E}(\mathbb{E}(Y|\mathcal{F})^2) \text{ por}(4) \\
&= \mathbb{E}(\mathbb{E}(Y|\mathcal{G})^2) - 2\mathbb{E}(\mathbb{E}(Y|\mathcal{F})^2) + \mathbb{E}(\mathbb{E}(Y|\mathcal{F})^2) \\
&= \mathbb{E}(\mathbb{E}(Y|\mathcal{G})^2) - \mathbb{E}(\mathbb{E}(Y|\mathcal{F})^2) \\
&= 0
\end{aligned}$$

Es decir $\mathbb{E}((\mathbb{E}(Y|\mathcal{G}) - \mathbb{E}(Y|\mathcal{F}))^2) = 0$ entonces $\mathbb{E}(Y|\mathcal{G}) - \mathbb{E}(Y|\mathcal{F}) = 0$ casi seguramente es decir $\mathbb{E}(Y|\mathcal{G}) = \mathbb{E}(Y|\mathcal{F})$ casi seguramente. $\square$

Por el lema 17 concluimos que si $(Y_i)_i$ es una sucesión de variables aleatorias las cuales son condicionalmente i.i.d dada una σ-álgebra $\mathcal{F}$, entonces dada α una distribución condicional regular de Y_1 dada $\mathcal{F}$ (la cual existe) se tendrá que $(Y_i)_i$ es una mezcla de sucesiones i.i.d dirigidas por α y como ya vimos anteriormente esto nos dice que $Y = (Y_i)_i$ es una mezcla de sucesiones i.i.d pues su densidad es de la forma (1.4.1).

Ya con todos estos conceptos y este último resultado podemos enunciar y probar nuestro teorema principal, el teorema de De Finetti.

Teorema 19. *Una sucesión infinita $(Z_i)_i$ es intercambiable si y solo si es una mezcla de sucesiones i.i.d.*

Demostración. Comencemos notando que una implicación es clara pues si $(Z_i)_i$ es una mezcla de sucesiones i.i.d entonces su densidad es de la forma

$$\mathbb{P}(Z_1 \in A_1, ..., Z_n \in A_n, ...) = \int_P \theta^\infty(A_1, A_2, ..., A_n, ..)\mu(d\theta),$$

donde P es el conjunto de medidas de probabilidad, μ la distribución de alguna medida aleatoria α, θ una medida de probabilidad en P y θ^∞ la distribución de $Z = (Z_i)_i$ dada $\alpha = \theta$, hacemos abuso de notación diciendo θ^∞ precisamente porque sabemos que cada Z_i tiene distribución θ. Luego si $\gamma \in S(n)$, como $(Z_i)_i$ dada $\alpha = \theta$ es i.i.d con distribución θ entonces tenemos que $\theta^\infty(A_1, ..., A_n, ...) = \theta^\infty(A_{\gamma^{-1}(1)}, ..., A_{\gamma^{-1}(n)}, A_{n+1}, ...)$, así

$$\begin{aligned}\int_P \theta^\infty(A_1, A_2, ..., A_n, ..)\mu(d\theta) &= \int_P \theta^\infty(A_{\gamma^{-1}(1)}, A_{\gamma^{-1}(2)}, ..., A_{\gamma^{-1}(n)}, A_{n+1}, ...)\mu(d\theta) \\ &= \mathbb{P}(Z_{\gamma(1)} \in A_1, ..., Z_{\gamma(n)} \in A_n, ...)\end{aligned}$$

y como n fue arbitrario tenemos que se cumple para toda n, que es lo que queríamos probar.

Para la ida haremos lo siguiente; sea $\mathcal{F}_n = \sigma(Z_n, Z_{n+1}, Z_{n+2}, ...)$ la σ-álgebra generada por $Z_n, Z_{n+1}, ...$, llamamos a $\bigcap_n \mathcal{F}_n = \tau$ la σ-álgebra cola. Lo que mostraremos es que si la sucesión $(Z_i)_i$ es intercambiable entonces es i.i.d condicional a τ, que como ya vimos esto basta para que $(Z_i)_i$ sea una mezcla de sucesiones i.i.d. Por intercambiabilidad tenemos que $(Z_1, Z_2, Z_3, ...) \stackrel{d}{=} (Z_1, Z_n, Z_{n+1}, ..)$ para toda $n > 2$, entonces $\mathbb{E}(\Phi(Z_1)|\mathcal{F}_2) \stackrel{d}{=} \mathbb{E}(\Phi(Z_1)|\mathcal{F}_n)$ para toda $\Phi : \mathbb{R} \to \mathbb{R}$ acotada. Aplicando el límite cuando $n \to \infty$ obtenemos por el teorema de convergencia de la esperanza condicional que $\mathbb{E}(\Phi(Z_1)|\mathcal{F}_n) \to \mathbb{E}(\Phi(Z_1)|\tau)$ casi seguramente. Entonces tenemos que $\mathbb{E}(\Phi(Z_1)|\mathcal{F}_2) \stackrel{d}{=} \mathbb{E}(\Phi(Z_1)|\tau)$. Luego por el Lema 18 esto implica que $\mathbb{E}(\Phi(Z_1)|\mathcal{F}_2) = \mathbb{E}(\Phi(Z_1)|\tau)$ casi seguramente, lo que quiere decir que Z_1 y

$\mathcal{F}_2$ son independientes dada τ, pues se dice que X e Y son independientes dada $\mathcal{F}$ si $\mathbb{E}(\Phi(X)|\mathcal{F}, Y) = \mathbb{E}(\Phi(X)|\mathcal{F})$ para toda Φ acotada. En este caso claramente

$$\mathbb{E}(\Phi(Z_1)|\mathcal{F}_2, \tau) = \mathbb{E}(\Phi(Z_1)|\mathcal{F}_2) = \mathbb{E}(\Phi(Z_1)|\tau),$$

que es lo que queríamos (la primera igualdad se sigue de que $\tau \subset \mathcal{F}_2$). Esta independencia nos dice que Z_1 es independiente de $Z_2, Z_3, ...$ dada τ. El mismo argumento se usa para ver que Z_m es independiente de $\mathcal{F}_{m+1}$ dada τ para toda $m \geq 1$ y así tendremos todas la independencias dos a dos de $(Z_i)_i$, es decir tenemos que $(Z_i)_i$ es independiente dada τ.

Por otro lado tenemos que $(Z_1, Z_{n+1}, Z_{n+2}, ..) \stackrel{d}{=} (Z_n, Z_{n+1}, ...)$, entonces

$$\mathbb{E}(\Phi(Z_1)|\mathcal{F}_m) \stackrel{c.s}{=} \mathbb{E}(\Phi(Z_n)|\mathcal{F}_m), \text{ para toda } m, \Phi \text{ acotada},$$

Aplicando límite cuando $m \to \infty$ como antes obtenemos que $\mathbb{E}(\Phi(Z_1)|\tau) = \mathbb{E}(\Phi(Z_n)|\tau)$ casi seguramente. Luego para $A \in \mathcal{B}(\mathbb{R})$ y tomando $\Phi(Z) = 1_{\{Z \in A\}}$ obtenemos que

$$\mathbb{P}(Z_1 \in A|\tau) = \mathbb{P}(Z_n \in A|\tau),$$

Como $A \in \mathcal{B}(\mathbb{R})$ fue arbitrario tenemos que $Z_1 = Z_n$ en distribución dada τ para toda n y así $(Z_i)_i$ es idénticamente distribuida dada τ. Concluimos que $(Z_i)_i$ es i.i.d dada τ que era lo que queríamos probar. $\square$

1.5. Particiones aleatorias intercambiables.

Nuestro objetivo ahora es construir un análogo al teorema de De Finetti pero para el caso de particiones aleatorias, para esto tendremos que introducir la noción de lo que significa intercambiabilidad en este contexto.

Denotamos por $P(N)$ el conjunto de particiones de $\{1, 2, ..., N\}$. Sea R una partición aleatoria de $P(N)$. Para $\sigma \in S(N)$ notemos que dado $B \subset \{1, 2, .., N\}$, σ actúa en B por $\sigma(B) = \{\sigma(i)|i \in B\}$, así dada $A = (A_i)$ una partición de $P(N)$ (podemos ordenar los bloques tomando el menor de sus elementos y usando el orden usual en $\mathbb{R}$) donde A_i representa el bloque i, tenemos que σ actúa en A por

$$\sigma(A) = \sigma(A_1, A_2, ...) = (\sigma(A_1), \sigma(A_2), ...).$$

Definición 20. Decimos que una variable aleatoria R en $P(n)$ es intercambiable si $\sigma(R) = R$ en distribución para toda $\sigma \in S(N)$.

Pasemos a construir una primera partición intercambiable para $N < \infty$, la cual llamaremos "La partición aleatoria intercambiable general". Sea $I_N = \{(n_i)|n_1 \geq n_2 \geq .... \geq 0, \sum n_i = N\}$, definimos la aplicación $L_N : P(N) \to I_N$ donde $L_N((A_i))$ representa la sucesión decreciente de las cardinalidades de (A_i). Sea σ^* la permutación aleatoria uniforme en $S(N)$. Entonces para $A \in P(N)$,$\sigma^*(A)$ es uniforme en $\{B|L_N(B) = L_N(A)\}$ lo cual es fácil de ver. Tenemos así una partición aleatoria $\sigma^*(A)$, la cual es claramente intercambiable por ser σ^* la permutación aleatoria uniforme.

Existe otra alternativa para construir particiones aleatorias intercambiables, la cual describiremos a continuación. Dada una partición aleatoria R definimos:

$$R_{ij} = \{\omega | i, j \in R(\omega)\}$$

donde $i, j \in R(\omega)$ quiere decir que i y j están en el mismo componente de $R(\omega)$. Tenemos la siguiente propiedad:

$$R_{ii} = \Omega, \quad R_{ij} = R_{ji}, \quad R_{ij} \cap R_{jk} \subset R_{ik}, \quad para \quad 1 \leq i, j, k \leq N \quad (1.5.1)$$

Conversamente dada una familia de eventos $\{R_{ij}|1 \leq i, j \leq N\}$ que satisface las condiciones anteriores podemos definir una partición aleatoria R. Para esto definimos la relación de equivalencia bajo ω dada por

$$i \sim_\omega j \qquad ssi \qquad \omega \in R_{ij}$$

La partición aleatoria R queda definida, donde $R(\omega)$ es la partición de las clases de equivalencia. Mas aún, la partición R es intercambiable ssi

$$(R_{ij}|1 \leq i, j \leq N) \stackrel{d}{=} (R_{\sigma(i)\sigma(j)}|1 \leq i, j \leq N),$$

para toda $\sigma \in S(N)$. Consideremos ahora particiones de $\{1, 2, 3, ...\}$. Sea S_∞ el conjunto de todas las particiones. Definimos una partición aleatoria como una aplicación

$$R : \Omega \longrightarrow S_\infty$$

tal que los conjuntos R_{ij} son medibles. Como antes, una partición aleatoria de $\{1, 2, 3, ..\}$ puede ser descrita como una familia de eventos $\{R_{ij}|1 \leq i, j\}$

que satisfacen (1.5.1) para toda N. Antes de verificar la existencia de dicha partición aleatoria S_∞ enunciaremos brevemente el teorema de extensión de Kolmogorov.

Teorema 21. *Sean $T \neq \emptyset$ arbitrario, E un espacio métrico compacto y $(E, \mathcal{E})$ un espacio medible. Para cada $G \subset F \subset T$ finitos definimos*

$$P_{F,G} : E^F \longrightarrow E^G,$$

la proyección de E^F a E^G. Para cada $F \subset T$ finito, μ_F es una medida de probabilidad en $(E^F, \mathcal{E}^F)$. Decimos que las distribuciones finito dimensionales $\mathcal{F} = \{\mu_J | J \subset T \text{ finito}\}$ son consistentes si para todos $G \subset F$ en $\mathcal{F}$, $\mu_G \circ P_{F,G} = \mu_F$. Supongamos que se cumplen las propiedades de consistencia, entonces existe una única medida de probabilidad μ_T en $(E^T, \mathcal{E}^T)$ tal que para todo $F \subset T$ finito $\mu_T \circ P_{T,F} = \mu_F$.

Apelando al teorema de extensión de Kolmogorov podemos construir una partición aleatoria sobre $\{1, 2, 3, ...\}$. Notemos que para toda N tenemos una partición aleatoria intercambiable R^N que por construcción satisface las condiciones de consistencia

$$(R^N_{ij} | 1 \leq i, j \leq N) \stackrel{d}{=} (R^{N+1}_{ij} | 1 \leq i, j \leq N)$$

para toda $N \geq 1$. Entonces existe una partición aleatoria intercambiable R de $\{1, 2, ...\}$ tal que

$$(R_{ij} | 1 \leq i, j \leq N) \stackrel{d}{=} (R^N_{ij} | 1 \leq i, j \leq N), \forall N \geq 1.$$

Hasta ahora tenemos claro el concepto de intercambiabilidad en este contexto, pero como nuestro objetivo es un análogo al teorema de De Finetti, habrá todavía que definir lo que es un paintbox, pues más adelante veremos precisamente que “una partición aleatoria intercambiable es una mezcla de paintboxes” el cual seria el análogo al teorema de De Finetti en el contexto de particiones. Pasaremos a construir el paintbox.

Sean μ una distribución en $[0, 1]$ con parte discreta y continua, $(X_i)_i$ i.i.d con ley μ y $R(\omega)$ la partición con componentes $\{i | X_i(\omega) = x\}$ para $0 \leq x \leq 1$. En otras palabras lo que tenemos es que $R_{ij} = \{\omega | X_i(\omega) = X_j(\omega)\}$. Claramente R es intercambiable pues la sucesión $(X_i)_i$ es i.i.d. Mas aún podemos observar que R depende únicamente del tamaño de los átomos de μ.

Sea $P_j = \mu(a_j)$ donde $(a_j)_j$ son los átomos de μ organizados de tal manera que $(P_j)_j$ es decreciente y con $P_j = 0$ si hay menos de j átomos. Esto define un mapeo L de las medidas de probabilidad en $[0,1]$ a $\Lambda = \{(p_1, p_2, ...)|p_1 \geq p_2 \geq p_3 \geq ... \geq 0, \sum p_i \leq 1\}$ dado por

$$L : P[0,1] \longrightarrow \Lambda$$
$$\mu \mapsto P = (P_i)_i$$

Lo que lo anterior nos sugiere es que podemos construir R no sólo a partir de una medida de probabilidad μ en $[0,1]$ si no más bien a partir de un elemento de Λ pues como vimos la familia R_{ij} depende únicamente del tamaño de los átomos de μ, llamamos entonces a la partición aleatoria R bajo esta construcción como el paintbox(P) y denotamos a su distribución por Ψ_P.

El siguiente lema es inmediato del hecho de que $\frac{|\{i \leq N | X_i = a_j\}|}{N} \to P_j$ casi seguramente

Lema 22. *Para $p \in \Lambda$ sea R un paintbox(p), denotamos por R^N a la restricción de R a $\{1, 2, .., N\}$. Entonces $\frac{L_N(R^N)}{N} \to p = (p_1, p_2, ...)$ en Λ casi seguramente*

Llegamos así al teorema principal de la sección, un análogo al teorema de De Finetti para particiones aleatorias intercambiables dado por Kingman[3].

Teorema 23. *Sea R una partición aleatoria intercambiable de $\{1, 2, ...\}$ y sea R^N su restricción a $\{1, 2., , ..N\}$, entonces:*

(I) $\frac{L_N(R^N)}{N} \to (D_1, D_2, ...) = D$ casi seguramente, para algún elemento aleatorio D de Λ.

(II) Ψ_D es una distribución condicional regular de R dada $\sigma(\Psi_D)$

Recordemos lo que era una distribución condicional regular, lo que (ii) nos dice es que condicionando a que $D = p$ la partición aleatoria intercambiable R tiene distribución paintbox(p) es decir Ψ_p. Esto es precisamente la noción que queríamos de que R "es una mezcla de procesos paintbox".

Demostración. Para la demostración de (ii) consideremos (χ_i) i.i.d uniformes en $(0,1)$ independientes de R. Fuera de un conjunto de medida cero podemos asumir que $(\chi_i(\omega)|i \geq 1)$ son distintos. Sean

$$F_i(\omega) = \text{mín}\{j | i, j \in R(\omega)\} \leq i$$

y

$$Z_i = \chi_{F_i}$$

Así para cada ω la partición $R(\omega)$ es precisamente la partición con componentes $\{i | Z_i(\omega) = x\}$ para $0 \leq x \leq 1$ que es precisamente la construcción del paintbox. Bastará ver la distribución de $(Z_i)_i$ para saber cómo se comporta el paintbox. Notemos ahora que $(Z_i)_i$ es intercambiable, pues $Z_i = g((\chi_i), R)$ es función de (χ_i) y de R. Entonces dado n y $\sigma \in S(n)$ tenemos $Z_{\sigma(i)} = g((\chi_{\sigma(i)}), \sigma(R))$ pero $(\chi_{\sigma(i)}) = (\chi_i)$ en distribución pues (χ_i) es i.i.d y $\sigma(R) = R$ en distribución pues R es intercambiable, de donde $(Z_{\sigma(i)})_i = (Z_i)_i$ en distribución, y por ende $(Z_i)_i$ es intercambiable. Por el teorema de De Finetti, tenemos que $(Z_i)_i$ es una mezcla de sucesiones i.i.d es decir existe una medida aleatoria α tal que condicionando a $\alpha = \mu$, $(Z_i)_i$ es i.i.d con distribución μ. Luego como $(Z_i)_i$ es i.i.d con ley μ tenemos que R tiene distribución paintbox con distribución $\Psi_{L(\mu)}$, en otras palabras $\Psi_{L(\alpha)}$ es una distribución condicional regular para R dada $\sigma(\Psi_{L(\alpha)})$ que es lo que establece (ii)

(i) se sigue del Lema 22 condicionando en D. $\square$

Capítulo 2

El teorema de De Finetti en el caso libre.

Hasta ahora hemos establecido el teorema de De Finetti en su versión clásica, y mas aún el teorema de De Finetti para el caso de particiones aleatorias intercambiables. Nuestro propósito ahora será enunciar e introducir el teorema de De Finetti en su caso libre, para esto la idea a seguir es introducirnos un poco en el marco de probabilidad no conmutativa, para después poder abordar el concepto de independencia libre con respecto a una esperanza condicional, el la cual toma el rol de independencia dada una álgebra cola. Por otra parte el concepto de idénticamente distribuido dado una álgebra cola será sustituido por el de idénticamente distribuido con amalgamación sobre un álgebra A_{tail}. Finalmente, el concepto de intercambiabilidad se extiende a intercambiable en el sentido cuántico el cual es un caso más general de intercambiabilidad. Comenzaremos dando una serie de definiciones algebráicas las cuales usaremos para definir lo que es un espacio de probabilidad no conmutativo.

2.1. Elementos de probabilidad libre

Definición 24. Un álgebra es un espacio vectorial A junto con una aplicación bilineal $f : A \times A \to A$ que manda $(a, b) \mapsto ab$ tal que $a(bc) = (ab)c$ para todos $a, b, c \in A$. Podemos además aditar a el álgebra de una norma $\|\cdot\|$ la cual se dice multiplicativa si $\|ab\| \leq \|a\|\|b\|$, en este caso el par $(A, \|\cdot\|)$ es llamada un álgebra normada.

Definición 25. Dada una álgebra normada $(A, \|\cdot\|)$, podemos definir la noción de sucesión de Cauchy en A de la misma manera que se define en $\mathbb{R}$; sea dice que $(x_i)_i \subset A$ es de Cauchy si para todo $\epsilon > 0$ existen $N \in \mathbb{N}$ tal que para todos $m, n > N$ se cumple $\|x_n - x_m\| < \epsilon$, si además toda sucesión de Cauchy converge a un elemento en A decimos que el álgebra es completa, a esto es lo que llamamos un álgebra de Banach.

Estas definiciones algebráicas las usaremos más adelante para definir lo que es un $*$-álgebra pero antes vamos a pasar a definir lo que es un espacio de probabilidad no conmutativo.

Definición 26. Un espacio de probabilidad no conmutativo (EPNC)es un par (A, ψ). Donde A es un álgebra con unidad 1_A y $\psi : A \to \mathbb{C}$ es un funcional lineal tal que $\psi(1_A) = 1$.

Algunos ejemplos de EPNCs son los siguientes:

1. $(A_1, \mathbb{E})$ donde $A_1 = \{x+iy | x, y$ son v. a. con todos sus momentos.$\}$, en este caso $\psi = \mathbb{E}$ es la esperanza usual.

2. (A_2, tr) donde $A_2 = \{M_n(\mathbb{C})\}$ el conjunto de matrices de $n \times n$ con coeficientes en los complejos, en este caso $\psi = \mathrm{tr} = \frac{Tr}{n}$ es la traza normalizada.

3. $(A_3, \mathbb{E}(tr))$ donde $A_3 = \{M | M$ es una matriz con entradas en $A_1\}$, usualmente esto es a lo que llamamos matriz aleatoria, en este caso $\psi = \mathbb{E} \circ tr$.

Al igual que en el caso clásico los cumulantes están definidos en un EPNC, además de la transformada de Cauchy y la R-transformada las cuales están relacionadas con estos.

Sea $k_m^l : A^m \longrightarrow \mathbb{C}$ una función m-lineal, si tenemos una colección de dichas funciones $(k_m^l)_{m=1}^n$ podemos definir su extensión multiplicativa (ver sección 2.2) $k_\pi^l : A^n \longrightarrow \mathbb{C}$ para todo $\pi \in NC(n)$ que además sera también n-lineal. Se definen los cumulantes libres k_π^l como dicha extensión multiplicativa de $(k_m)_{m=1}^n$ que además satisface

$$\psi(a_1 ... a_n) = \sum_{\pi \in NC(n)} k_\pi^l(a_1, ..., a_n).$$

Definimos también la transformada de Cauchy de una variable aleatoria $a \in A$ con distribución analítica μ sobre $\mathbb{R}$ como

$$G_a^l(z) = \int_{\mathbb{R}} \frac{1}{z-t} d\mu(t) \text{ para } z \in \mathbb{C}$$

y su R-transformada como

$$R_a^l(z) = \sum_{n \geq 1} k_n(a, ..., a) z^n \text{ para } z \in \mathbb{C}$$

Podemos además aditar a el álgebra con una involución $*$, a la cual llamaremos un $*$-álgebra de la siguiente manera

Definición 27. Una $*$-álgebra es un par $(A, *)$ donde A es un álgebra y $* : A \to A$ tal que $*(a) = a^*$, y que cumple:

(I) $(a^*)^* = a$

(II) $(a + \lambda b)^* = a^* + \overline{\lambda} b^*$, $\lambda \in \mathbb{C}$

(III) $(ab)^* = b^* a^*$

Las variables aleatorias son elementos en el álgebra y decimos que son auto adjuntos si $a = a^*$

Dado un espacio de probabilidad no conmutativo (A, ψ) es natural pensar en una noción de que las variables aleatorias sean i.i.d, para esto es importante resaltar que la noción de independencia no es única y de hecho existen al menos 3 tipos de independencia

1. Independencia clásica tensorial.
2. Independencia libre.
3. Independencia booleana.

En nuestro trabajo nos centraremos en la independencia libre, pero por completitud enunciaremos lo que quiere decir cada una.

Definición 28. 1. Se dice que $a, b \in A$ son independientes en el sentido clásico si a y b conmutan y además

$$\psi(a^n b^m) = \psi(a^n)\psi(b^m)$$

para todo $n, m \geq 1$

2. Se dice que $a, b \in A$ son independientes en el sentido libre si

$$\psi(p_1(a)q_1(b)...p_n(a)q_n(b)) = 0$$

para todos los polinomios $p_1, q_1, .., p_n, q_n$ tal que $\psi(p_i(a)) = \psi(q_i(b)) = 0$ para todo $i = 1, .., n$.

3. Se dice que $a, b \in A$ son independientes en el sentido booleano si

$$\psi(a^{n_1}b^{m_1}...b^{m_{k-1}}a^{n_k}) = \prod_{i=1}^{k} \psi(a^{n_i})\psi(b^{m_i})$$

para todo $n_i, m_i \geq 1$.

Estas nociones de independencia son muy importantes pues cada una da pie a distintos resultados, un claro ejemplo es el Teorema del Límite Central el cual dice que si $(a_i) \subset A$ son variables aleatorias reales e independientes en el sentido clásico tales que $\psi(a_i) = 0$ y $\psi(a_i^2) = \sigma^2$ entonces $\frac{a_1+...+a_n}{\sigma\sqrt{n}} \to N(0, 1)$. Sin embargo, si consideramos independencia en el sentido libre entonces esto último converge a la ley del semicírculo, análogamente para el caso booleano converge a la distribución Bernoulli con soporte en $\{-1, 1\}$.

Para el caso de que la sucesión sea idénticamente distribuida no existe varias nociones, se dice que $(a_i) \subset A$ es idénticamente distribuido si la expresión $\psi(a_i^n)$ no depende de i, para todo $n \in \mathbb{N}$.

Para terminar la sección introduciremos los conceptos de lo que es un álgebra C^* y un W^*-espacio de probabilidad pues los usaremos más adelante.

Definición 29. Un álgebra de Banach-$*$ es un álgebra de Banach tal que $\|a\| = \|a^*\|$.

Definición 30. Un álgebra C^* es un álgebra de Banach-$*$ tal que $\|a\|^2 = \|aa^*\|$. A esta identidad se le llama "Identidad *".

Haciendo un recordatorio, un producto interior define una norma, si el espacio con dicha norma es completo se le conoce por espacio de Hilbert, dicho esto es claro que todo espacio de Hilbert es en particular un espacio de Banach, pero no viceversa.

Sea H un espacio de Hilbert, denotamos por $B(H)$ al conjunto de operadores acotados de H en H. Recordemos que $T : H \longrightarrow H$ es acotado si $T(B_1(H))$ es acotado, donde $B_1(H) = \{x \in H | \|x\| \leq 1\}$ es la bola cerrada de radio uno.

Podemos definir distintas topologías sobre $B(H)$, en nuestro caso nos enfocaremos en dos en especial, conocidas como la topología operador norma (TON) y la topología operador débil (TOD).

Sea $\|T\| = sup\{\|Tx\| | \|x\| \leq 1\}$, esto define una norma en $B(H)$, llamamos a la topología resultante bajo esta norma la topología operador norma.

La topología operador débil es la topología en $B(H)$ cuyos abiertos son de la forma

$$V_{T_0,v,w,\epsilon} = \{T \in B(H) \text{ tal que } | < Tv, w > - < T_0 v, w > | < \epsilon\}.$$

Dado esto se puede verificar lo siguiente.

Teorema 31. *TON* $\subset$ *TOD*

Además diremos que la aplicación $T \mapsto G : B(H) \longrightarrow B(H)$ es débilmente cerrada si es cerrada con respecto a la topología operador débil.

Definición 32. Un álgebra de Von Neumann es una $*$-subálgebra unitaria débilmente cerrada en $B(H)$.

Mas aún se puede verificar que toda $*$-algebra cerrada con respecto a la topología operador norma es un álgebra C^*, es decir una consecuencia del teorema (31) es que toda álgebra de Von Neumann es en particular un álgebra C^*.

Definición 33. Un W^*-espacio de probabilidad es un par (A, ψ) donde A es un álgebra de Von Neumann y (A, ψ) un EPNC.

Retomando la idea principal de nuestro teorema en el caso clásico, este nos dice que la sucesión (x_i) es i.i.d dada la álgebra cola A_{tail} si y sólo si (x_i) es intercambiable. Es importante notar que estamos diciendo que la sucesión es independiente pero dada el álgebra cola τ. Esto en el caso clásico nos decía que $E(x_i|x_j, \tau) = E(x_i|\tau)$. Para definir el concepto análogo en el caso libre necesitamos que la sucesión (x_i) sea independiente en el sentido libre dada un álgebra, aquí es donde entra el concepto de lo que es una esperanza condicional E.

2.2. Esperanza condicional

Definición 34. Una esperanza condicional E es una función $E : A \to B$ donde A es un álgebra con unidad, $B \subset A$ es una subálgebra de A que además satisface:

1. $E(b) = b \ \forall b \in B$
2. $E(b_1 a b_2) = b_1 E(a) b_2$, $\forall b_1, b_2 \in B, a \in A$.

Definición 35. Un espacio de probabilidad valuado en operadores es un par $(A, E : A \to B)$ donde A es un álgebra unitaria, $B \subset A$ una subálgebra de A y E una esperanza condicional, los elementos en A son llamados variables aleatorias valuados en operadores.

Además si B es un álgebra unitaria usamos la notación:

$$B\langle X\rangle = \{b_0 X b_1 X ... b_{n-1} X b_n | n \in \mathbb{N}, b_1, ..., b_n \in B\}$$

Una pregunta natural es dado un EPNC (A, ψ) y una subálgebra $B \subset A$ de A cuando existe una esperanza condicional $E : A \to B$ que preserve ψ es decir $\psi \circ E = \psi$, para esto tenemos el siguiente teorema.

Teorema 36. *Sea (A, ψ) un W^*-espacio de probabilidad tracial y $B \subset A$ una subálgebra de A entonces existe una esperanza condicional $E : A \longrightarrow B$ la cual es única y que preserva ψ es decir $\psi \circ E = \psi$.*

Demostración. Para la prueba ver [9]. □

Para nuestro trabajo se trabaja sobre un W^*-espacio de probabilidad no necesariamente tracial por lo que veremos sobre la marcha que gracias a la intercambiabilidad de las variables existe dicha esperanza condicional E la cual estará restringida en su dominio a A_∞ el álgebra de Von Neumann generada por las variables aleatorias i.e $E : A_\infty \longrightarrow A_{tail}$ donde $A_{tail} \subset A$ es una subálgebra de A. Esto no será inconveniente en la prueba de nuestro teorema pues de hecho solo necesitaremos dicha esperanza condicional definida sobre A_∞.

Por el momento estamos interesados en definir que significa que la sucesión sea i.i.d dada una esperanza condicional, el cual es el concepto análogo a que la sucesión sea i.i.d dada la álgebra cola en el caso clásico.

Definición 37. Sea $(A, E : A \to B)$ un espacio de probabilidad valuado en operadores y $(x_i) \subset A$, decimos que (x_i) es idénticamente distribuido con respecto a E (o idénticamente distribuido con amalgamación sobre B) si $\forall p \in B\langle X\rangle$ la expresión $E(p(x_i))$ no depende de $i \in \mathbb{N}$.

Cabe mencionar que en el caso de un espacio de probabilidad no conmutativo cuando $B = \mathbb{C}$ y $E = \psi$ es decir tenemos el par (A, ψ) con $\psi : A \to \mathbb{C}$, se tiene que $B\langle X\rangle = C\langle X\rangle$ es decir los polinomios con coeficientes en $\mathbb{C}$,así nuestra definición de idénticamente distribuido con respecto a E no es más que los momentos $\psi(x_i^n)$ no dependen de i como era de esperarse. Ahora veremos que significa que la sucesión sea independiente en el sentido libre dada la esperanza condicional.

Definición 38. Sea $(A, E : A \to B)$ un espacio de probabilidad valuado en operadores e I un conjunto de índices arbitrario. Sea $(a_i) \subset A$ una sucesión de variables aleatorias, se dice que las variables aleatorias son libres con respecto a E o libres con amalgamación sobre B si para toda $n \in \mathbb{N}$, $i(1) \neq i(2) \neq ... \neq i(n)$ y todos los polinomios $B-$valuados $p_1, .., p_n \in B\langle X\rangle$ tal que $E(p_m(x_{i(m)})) = 0$ para $m = 1, .., n$ se cumple que $E(p_1(x_{i(1)})...p_n(x_{i(n)})) = 0$.

Notemos que estas últimas definiciones son justamente que la sucesión sea independiente en el sentido libre e idénticamente distribuida, pero estamos cambiando ψ por E. Con esto tenemos establecido que significa que una sucesión de variables aleatorias en un EPNC sea i.i.d dada una esperanza condicional. Aprovechando que ya estamos encaminados en lo que es una esperanza condicional vamos a definir lo que son los cumulantes valuados en operadores, los cuales usaremos en la prueba de el teorema central de este capítulo.

Definición 39. Sea $(A, E : A \to B)$ un espacio de probabilidad valuado en operadores, para $n \in \mathbb{N}$ definimos

(I) Una aplicación $P : A^n \longrightarrow B$ es llamado $B-$funcional si es n lineal y para todo $b_0, b_1, ..., b_n \in B$ y $a_1, ..., a_n \in A$ se cumple

$$P(b_0a_1b_1, a_2b_2, ..., a_{n-1}b_{n-1}, a_nb_n) = b_0P(a_1, b_1a_2, ..., b_{n-2}a_{n-1}, b_{n-1}a_n)b_n.$$

(II) Si para todo $1 \leq k \leq n$ tenemos $P_k : A^k \longrightarrow B$ un $B-$ funcional, entonces para $\pi \in NC(n)$ se define un B-funcional $P_\pi : A^n \longrightarrow B$ recursivamente de la siguiente manera : Si $\pi = 1_n$ para $a_1, .., a_n \in A$ se define $P_{1_n}(a_1, .., a_n) = P_n(a_1, ..., a_n)$. De otra manera si $V = (i+1, .., i+r)$ es un intervalo maximal de π(un intervalo que no esta contenido dentro de otro), entonces para $a_1, .., a_n \in A$ definimos

$$P_\pi(a_1, .., a_n) = P_{\pi/V}(a_1, ..., a_iP_r(a_{i+1}, ..., a_{i+r}), a_{i+r+1}, ..., a_n).$$

A este definición se le suele llamar la extensión multiplicativa.

Veamos como funciona con el siguiente ejemplo: Sea $n = 6$ y $\pi \in NC(6)$ la partición $\{\{1,4\},\{2,3\},\{5,6\}\}$, Entonces:

$$P_\pi(1,2,3,4,5,6) = P_2(1 * P_2(2,3), 4)P_2(5,6).$$

Dado esto podemos definir los cumulantes valuados en operadores k_l $1 \leq l \leq n$ como un B-funcional tal que:

$$E(a_1 a_2 ... a_n) = \sum_{\pi \in NC(n)} k_\pi(a_1, ..., a_n).$$

Notemos que esta es justamente la definición de los cumulantes libres k_n^l dados por $\psi(a_1 a_2 ... a_n) = \sum_{\pi \in NC(n)} k_\pi^l(a_1, ..., a_n)$. Se puede verificar vía el teorema de inversión de Moebius que existe una formula para los cumulantes en función de los momentos dada por

$$k_\pi^l(a_1, ..., a_n) = \sum_{\sigma \leq \pi} \psi_\sigma(a_1, .., a_n)\mu_n(\sigma, \pi),$$

donde $\mu_n : NC(n)^2 \longrightarrow \mathbb{C}$ es la formula de Moebius para particiones que no se cruzan, $\psi_n(a_1, ..., a_n) = \psi(a_1....a_n)$ y ψ_σ es su extensión multiplicativa. Es decir, tenemos una relación directa entre cumulantes y momentos, como era de esperarse también lo tendremos para los cumulantes valuados en operadores y los momentos $E(a_1...a_n)$ dado por

$$k_\pi(a_1, ..., a_n) = \sum_{\sigma \leq \pi} E_\sigma(a_1, .., a_n)\mu_n(\sigma, \pi),$$

con μ_n y E_σ definidos como antes.

Mucha de la teoría definida en un EPNC se puede trasladar a un espacio de probabilidad valuado en operadores, un ejemplo es la transformada de Cauchy, que llamaremos la transformada de Cauchy valuada en operadores dada por

$$G_a^B(b) = E(\frac{1}{b - a}) = \sum_{n \geq 0} E(b^{-1}(ab^{-1})^n).$$

Por otra parte, la R-transformada valuada en operadores está dada por

$$R_a^B(b) = \sum_{n \geq 1} k_n(a, ba, ba.., ba).$$

Cabe mencionar que si a_1, a_2 son libres con respecto a $E : A \to B$ entonces tenemos que para todo $b \in B$ se cumple $R_{a_1+a_2}(b) = R_{a_1}(b) + R_{a_2}(b)$, tal y como sucede en un EPNC, donde si a_1 y a_2 son libres entonces $R^l_{a_1+a_2}(z) = R^l_{a_1}(b) + R^l_{a_2}(z)$ para todo $z \in \mathbb{C}$, donde R^l_a es la R-transformada de a.

Antes de terminar esta sección vamos a hacer una observación: Sea $(a_i)_{i\in I} \subset A$ una sucesión de variables aleatorias que son independientes con respecto a E, como era de esperarse con los momentos, los cumulantes se anulan si los elementos son independientes, es decir $k_n(a_{i(1)}, ..., a_{i(n)}) = 0$ siempre y cuando exista $1 \leq k, l \leq n$ tal que $i(k) \neq i(l)$. Si transferimos esto a k_π con $\pi \in NC(n)$ tendremos que la independencia de los (a_i) implica que $k_\pi(a_{i(1)}, ..., a_{i(n)})$ es cero si en algún bloque los i-indices son distintos, es decir esto puede no anularse solo en el caso en el que todos los i-indices pertenecientes al mismo bloque son iguales. Introduzcamos la siguiente notación: para $n \in \mathbb{N}$ y $\mathbf{i} = (i(1), ..., i(n))$ denotamos por $ker\mathbf{i} \in P(n)$ a la partición de $\{1, .., n\}$ que esta dada por k, l en el mismo bloque ssi $i(k) = i(l)$. Bajo esta notación tenemos que si $(a_i)_{i\in I}$ son independientes con respecto a E entonces $k_\pi(a_{i(1)}, ..., a_{i(n)})$ puede no anularse solo en el caso en el que $ker\mathbf{i} \geq \pi$.

2.3. Intercambiabilidad en el sentido cuántico.

Ahora buscaremos cambiar el sentido de intercambiable por intercambiable en el sentido cuántico. Dado el espacio de probabilidad (A, ψ) diremos que dos sucesiones (y_n) e (y_n) en A tienen la misma distribución si

$$\psi(x_{i(1)}x_{i(2)}...x_{i(n)}) = \psi(y_{i(1)}y_{i(2)}...y_{i(n)})$$

para todas la $n-$tuplas $i = \{1, 2, 3..., n\} \to N \cup \{0\}$, $n \in \mathbb{N}$. Además será conveniente introducir los siguientes conceptos.

Definición 40. 1. Se dice que una sucesión (x_n) es **intercambiable** si para toda permutación finita π,

$$(x_0, x_1, ...) \stackrel{d}{=} (x_{\pi(1)}, x_{\pi(2)}, ...)$$

2. Se dice que una sucesión (x_n) es **esparcible** si para toda subsucesión $(n(0), n(1), ...)$ de $(0, 1, 2, 3, ...)$,

$$(x_0, x_1, ...) \stackrel{d}{=} (x_{n(0)}, x_{n(1)}, ...)$$

3. Se dice que una sucesión (x_n) es **estacionaria** si para toda $k \in \mathbb{N}$,

$$(x_0, x_1, ...) \stackrel{d}{=} (x_k, x_{k+1}, ...)$$

4. Se dice que una sucesión (x_n) es **idénticamente distribuida** si para toda $k, l \in \mathbb{N} \cup \{0\}$,

$$(x_k, x_k, ...) \stackrel{d}{=} (x_l, x_l, ...)$$

Ya con estas previas definiciones, podemos hablar del término "cuántico", el estudio de grupos cuánticos puede ser dividido en 3 principales áreas:

1. Grupos cuánticos de permutación.

2. Grupos cuánticos libres.

3. Grupos cuánticos discretos.

Pasaremos ahora a enunciar que es un grupo cuántico ortogonal.

Definición 41. Un grupo cuántico ortogonal G esta dado por un álgebra C^* A generada por n^2 operadores auto adjuntos u_{ij} , $i, j = 1, ..., n$ que cumple además:

(I) La inversa de (u_{ij}) es (u_{ji})

(II) $\Delta(u_{ij}) = \sum_k u_{ik} \bigotimes U_{kj}$ define un morfismo $\Delta : A \to A \bigotimes A$

(III) $\Sigma(U_{ij}) = u_{ij}$ define un morfismo $\Sigma : A \to \mathbb{C}$

(IV) $S(u_{ij}) = u_{ji}$ define un morfismo $S : A \to A^{op}$

Debido a la definición y la condición (1) tenemos inmediatamente que $UU^t = I$ de ahí el nombre de grupo cuántico ortogonal.

Para nuestro objetivo haremos uso más preciso de un grupo cuántico de permutación, antes de pasar a la definición formal retomemos la idea de como esto esta ligado con De Finetti y como se motiva a dar estas definiciones las cuales parecen muy alejadas de los previos capítulos, pero que al final veremos que de hecho están estrechamente ligadas.

Consideremos una sucesión de n variables aleatorias $(Z_1, Z_2, ...Z_n)$, estamos interesados en ver cuando $Z = (Z_i)_i$ es n-intercambiable, para esto necesitamos que

$$(Z_1, Z_2, ..., Z_n) \stackrel{d}{=} (Z_{\sigma(1)}, Z_{\sigma(2)}, ..., Z_{\sigma(n)}), \forall \sigma \in S(n)$$

Tomando $\sigma \in S(n)$ podemos asociar a σ una matriz de permutación, $M \in M(\mathbb{R}, n)$ el conjunto de matrices de nxn con coeficientes en $\mathbb{R}$, de la siguiente manera, colocamos un uno en la entrada (i, j) de la matriz si $\sigma(i) = j$. Obteniendo entonces la matriz $M = (\delta_{\sigma(i),j})$, esta matriz tiene algunas propiedades tales como

1. Sus entradas en filas y columnas suman 1.
2. $M_{ik}M_{il} = 0$ $M_{ki}M_{li} = 0$ $\forall i, k, l = 1, ..., n$.

Mas aun, $MZ = \sigma(Z)$, es decir lo que buscamos en realidad es que $Z \stackrel{d}{=} MZ$ para toda matriz de permutación, ¿Qué pasaría entonces si en vez de pedir que M sea una matriz de permutación pedimos únicamente las condiciones (1) y (2)?, es decir las entradas no sean necesariamente unos o ceros si no que las filas y columnas sean una partición de la unidad, nace entonces así el concepto de lo que es un grupo cuántico de permutación.

Definición 42. Un grupo cuántico de permutación $A_s(n)$ esta definido como la álgebra C^* unitaria generada por u_{ij} , $i, j = 1, .., n$ tal que

(I) $u_{ij}^* = u_{ij} = u_{ij}^2$ $\forall i, j = 1, ..., n$

(II) $U = (u_{ij})$ los elementos de su fila y de su columna formen una partición de la unidad , es decir, $u_{ik}u_{il} = 0$ $u_{ki}u_{li} = 0$ $\forall i, k, l = 1, ..., n$ y $\sum_k u_{ik} = 1 = \sum_k u_{ki}$ $\forall i = 1, ..., n$

Ya con esto podemos pasar directamente a nuestro análogo a intercambiable para el caso libre, hablamos de intercambiable en el sentido cuántico.

Definición 43. Consideremos un espacio de probabilidad no conmutativo (A, ψ) y $(x_i) \subset A$, decimos que la distribución conjunta (con respecto a ψ) de esta sucesión es invariante bajo permutaciones cuánticas o que (x_i) es intercambiable en el sentido cuántico si para algún $k \in \mathbb{N}$ la acción natural de $A_s(k)$ en la $k-$tupla $(x_1, ..., x_k)$ dada por

$$x_i \to \overline{x_i} = \sum_{j=1}^{k} u_{ij} \bigotimes x_j \in A_s(k) \bigotimes A$$

no cambia de distribución, i.e la distribución conjunta de $(x_1, ..., x_k)$ con respecto a ψ es la misma que $\overline{x_1}, ..., \overline{x_k}$ con respecto a $id \bigotimes \psi$.

Más explícitamente que para toda $k, n \in \mathbb{N}$ y $1 \leq i(1), ..., i(n) \leq k$ tenemos que

$$\psi(x_{i(1)}...x_{i(n)}) = \sum_{j(1)=1,...,j(n)=1}^{k} u_{i(1)j(1)}...u_{i(n)j(n)}\psi(x_{j(1)}...x_{j(n)}),$$

con igualdad en $A_s(k)$.

Como antes lo vimos, es natural pensar entonces en que si tomamos $n \in \mathbb{N}$ y $\sigma \in S_n$, tomando la matriz de permutación $U = (u_{ij})_{ij=1}^n = (\delta_{\sigma(i)j})_{i,j=1}^n$ (la cual genera un grupo cuántico de permutación $A_s(n)$ pues $u_{ij}^* = u_{ij} = u_{ij}^2$ y las filas y columnas de (u_{ij}) forman claramente una partición de la unidad) tenemos:

$$\psi(x_1, ..., x_n) = \sum_{j(1)=1,...,j(n)=1}^{k} \delta_{\sigma(1)j(1)}...\delta_{\sigma(n)j(n)}\psi(x_{j(1)} \cdots x_{j(n)}) = \psi(x_{\sigma(1)} \cdots x_{\sigma(n)})$$

Luego como n y σ fueron arbitrarios podemos concluir que $(x_1, x_2, ...) \stackrel{d}{=} (x_{\sigma(1)}, x_{\sigma(2)}, ...)$ para toda σ permutación finita i.e (x_i) es intercambiable. Tenemos entonces de lo que precisamente hablábamos, intercambiable en el sentido cuántico implica intercambiable en el sentido clásico.

2.4. El teorema de De Finetti en el caso libre.

Estamos listos para enunciar nuestro teorema principal, antes de eso probaremos la existencia de la esperanza condicional.

Teorema 44. *Sea (A, ψ) un W^*-espacio de probabilidad, $A_{tail} \subset A$ la subálgebra cola de A, $(x_i) \subset A$ una sucesión de variables aleatorias intercambiables (en particular si son intercambiables en el sentido cuántico cumple la condición) y A_∞ el álgebra de Von Neumann generada por $(x_i)_i$ entonces existe la esperanza condicional $E : A_\infty \longrightarrow A_{tail}$ que preserva $\psi_\infty = \psi|_{A_\infty}$ es decir $\psi_\infty \circ E = \psi_\infty$. Donde A_{tail} esta dada por*

$$A_{tail} = \bigcap_{n \in \mathbb{N}} vN(x_k | k \geq n)$$

y $vN(x_k | k \geq n)$ denota el álgebra de Von Neumann generada por $\{x_k | k \geq n\}$.

Demostración. Para nuestra prueba asumiéremos sin perdida de la generalidad que A es generado por (x_i) es decir $A = A_\infty$. La intercambiabilidad de (x_i) implica que existe un endomorfismo $\alpha : A \longrightarrow A$ tal que

$$\psi \circ \alpha = \psi \text{ y } \alpha(x_i) = \alpha(x_{i+1}).$$

Sea $A_I = vN(x_i|i \in I)$ para $I \subset \mathbb{N}$, sean $a, b \in \bigcup_{|I|<\infty} A_I$, entonces existe $N \in \mathbb{N}$ tal que $a \in A_I$, $b \in A_J$ y $I \cap (J + N) = \emptyset$. De la intercambiabilidad tenemos que $\psi(b\alpha^n(a)) = \psi(b\alpha^{n+1}(a))$ para todo $n \geq N$, esto último nos asegura la existencia del $\lim_{n\to\infty} \psi(b\alpha^n(a))$ en la $*$-álgebra $\bigcup_{|I|<\infty} A_I$. Un argumento de aproximación nos asegura la existencia de este mismo límite para todos $a, b \in A$ pues podemos aproximar $A = vN(x_i|i \in \mathbb{N})$ con $\bigcup_{|I|<\infty} A_I$. De esto concluimos que el límite puntual de $(\alpha^n)_{n\in\mathbb{N}}$ existe y podemos así definir un mapeo lineal $Q : A \longrightarrow A$ dado por $a \mapsto \lim_{n\to\infty} \alpha^n(a)$ tal que $Q(A) \subset A_{tail}$.

Además es fácil verificar que $\psi \circ Q = \psi$ por cómo está definido Q y $\|Q(a)\| \leq \|a\|$ para todo $a \in A$ pues $\|Q(a)\| = \|\lim_{n\to\infty} \alpha^n(a)\| = \lim_{n\to\infty} \|\alpha^n(a)\|$ al ser la norma una función continua, finalmente se puede verificar que como $\alpha^n : A \longrightarrow A$ es un endomorfismo entonces decrece en norma, es decir $\|\alpha^n(a)\| \leq \|a\|$ (Ver teorema 2.7.1 en [5]). Así si verificamos que $Q(a) = a$ para todo $a \in A_{tail}$ tendremos que Q es una esperanza condicional de A en A_{tail} (Ver [7]). Sean $a \in A_{tail}$ y $b \in \bigcup_{|I|<\infty} A_I$. Tenemos que $A_{tail} \subset \alpha^N(A)$ y $A_{[N,\infty)} \subset \alpha^N(A)$ para todo $N \in \mathbb{N}$ donde $A_{[N,\infty)} = vN(x_i|i \geq N)$. Entonces existe $N \in \mathbb{N}$ tal que $a \in \alpha^N(A)$ y $b \in A_{[0,N-1]}$. Aproximando $a \in A$ por una secuencia $(a_k)_k \subset \bigcup_{|I|<\infty} \alpha^N(A_I)$ y concluyendo de la definición de Q y la intercambiabilidad tenemos que

$$\psi(bQ(a)) = \lim_k \psi(bQ(a_k)) = \lim_k \lim_n \psi(b\alpha^n(a_k)) = \lim_k \psi(ba_k) = \psi(ba)$$

para todo $b \in A$, por lo tanto tenemos que $Q(a) = a$ para todo $a \in A_{tail}$. Así existe $E : A_\infty \to A_{tail}$ que preserva $\psi = \psi_\infty$ es decir $\psi_\infty \circ E = \psi_\infty$. $\square$

Pasaremos a enunciar el teorema central del capítulo.

Teorema 45. *(A, ψ) un W^*-espacio de probabilidad, $(x_i) \subset A$ una sucesión de variables aleatorias, entonces los siguientes son equivalentes:*

1. *La distribución conjunta de (x_i) con respecto a ψ es invariante bajo permutaciones cuánticas o cuánticamente intercambiable.*

2. *La sucesión (x_i) es libremente independiente e idénticamente distribuida con respecto a la esperanza condicional $E : A_\infty \to A_{tail}$ o con amalgamación sobre A_{tail} donde A_∞ es el álgebra de Von Neumann generada por (x_i) y A_{tail} denota el álgebra cola de Von Neumann dada por*

$$A_{tail} = \bigcap_{n\in\mathbb{N}} vN(x_k|k \geq n)$$

donde $vN(x_k|k \geq n)$ denota el álgebra de Von Neumann generada por $\{x_k|k \geq n\}$.

Demostración. Vamos a probar 2) $\Rightarrow$ 1) para esto notemos lo siguiente; sean $n, k \in \mathbb{N}$ e $1 \leq i(1), ..., i(n) \leq k$, tomemos $n = 5$ para dejar más claro la observación con el siguiente ejemplo; sea $\pi = \{\{1, 5\}, \{2, 3, 4\}\}$, luego

$$\sum_{\substack{\pi \leq ker\mathbf{j} \\ j(1),..,j(5)=1}}^{k} u_{i(1)j(1)...u_{i(5)j(5)}} = \sum_{l=1}^{k}\sum_{m=1}^{k} u_{i(1)l}u_{i(2)m}u_{i(3)m}u_{i(3)m}u_{i(5)l},$$

pues si $\pi \leq ker\mathbf{j}$ entonces $j(1) = j(5)$ y $j(2) = j(3) = j(4)$. Esta suma a su vez es

$$\sum_{l=1}^{k} u_{i(1)l}(\sum_{m=1}^{k} u_{i(2)m}u_{i(3)m}u_{i(4)m})u_{i(5)l}.$$

Dada la ortogonalidad de los u_i tenemos que $u_{i(2)m}u_{i(3)m}u_{i(4)m}$ no es cero solo si $i(2) = i(3) = i(4)$, mas aun como $u_i = u_i^2$ tenemos que $u_{i(2)m}u_{i(3)m}u_{i(4)m} = u_{i(2)m}$ si $i(2) = i(3) = i(4)$ y cero en otro caso. Así, la suma original está dada por

$$\sum_{m=1}^{k} u_{i(2)m}u_{i(3)m}u_{i(4)m} = \sum_{m=1}^{k} u_{i(2)m}$$

si $i(2) = i(3) = i(4)$ y cero en otro caso. Finalmente, por condición de los u_i tenemos que $\sum_{m=1}^{k} u_{i(2)m} = 1$, podemos concluir que $\sum_{m=1}^{k} u_{i(2)m}u_{i(3)m}u_{i(4)m} = 1$ si $i(2) = i(3) = i(4)$ y cero en otro caso. Luego

$$\sum_{l=1}^{k} u_{i(1)l}(\sum_{m=1}^{k} u_{i(2)m}u_{i(3)m}u_{i(4)m})u_{i(5)l} = \sum_{l=1}^{k} u_{i(1)l}u_{i(5)l}$$

cuando $i(2) = i(3) = i(4)$ y cero en otro caso. Aplicando lo mismo a esta nueva suma podemos concluir que

$$\sum_{l=1}^{k} u_{i(1)l}(\sum_{m=1}^{k} u_{i(2)m}u_{i(3)m}u_{i(4)m})u_{i(5)l} = 1$$

si $i(1) = i(5)$ e $i(2) = i(3) = i(4)$, es decir ,cuando $\pi \leq ker\mathbf{i}$ y cero en otro caso. Podemos generalizar esta misma idea a cualquier partición π haciendo uso de los intervalos de π.

Con estas herramientas estamos listos para probar 2) $\Rightarrow$ 1). Sean $n, k \in \mathbb{N}$ e $1 \leq i(1), ..., i(n) \leq k$. Tenemos que

$$\begin{aligned}
&\sum_{j(1),...,j(n)=1}^{k} u_{i(1)j(i)}...u_{i(n)j(n)}\psi(x_{j(1)}...x_{j(n)}) \\
=&\sum_{j(1),...,j(n)=1}^{k} u_{i(1)j(i)}...u_{i(n)j(n)}\psi(E(x_{j(1)}...x_{j(n)})) \\
=&\sum_{j(1),...,j(n)=1}^{k} u_{i(1)j(i)}...u_{i(n)j(n)}\psi(\sum_{\pi\in NC(n)} k_\pi(x_{j(1)}, ..., x_{j(n)})) \\
=&\sum_{\pi\in NC(n)}\sum_{j(1),...,j(n)=1}^{k} u_{i(1)j(i)}...u_{i(n)j(n)}\psi(k_\pi(x_{j(1)}, ..., x_{j(n)})).
\end{aligned}$$

Luego recordando que $k_\pi(x_{j(1)}, ..., x_{j(n)})$ puede no ser cero solo si $\pi \leq ker\mathbf{j}$ (como vimos en 2.2)) y dado que los (x_i) son idénticamente distribuidos tenemos que el término $k_\pi(x_{j(1)}, ..., x_{j(n)}) = k_\pi$ así nuestra suma original es

$$\begin{aligned}
&\sum_{\pi\in NC(n)}\sum_{\substack{\pi\leq ker\mathbf{j} \\ j(1),...,j(n)=1}}^{k} u_{i(1)j(i)}...u_{i(n)j(n)}\psi(k_\pi(x_{j(1)}, ..., x_{j(n)})) \\
=&\sum_{\pi\in NC(n)}\sum_{\substack{\pi\leq ker\mathbf{j} \\ j(1),...,j(n)=1}}^{k} u_{i(1)j(i)}...u_{i(n)j(n)}\psi(k_\pi) \\
=&\sum_{\pi\in NC(n)}\psi(k_\pi)\sum_{\substack{\pi\leq ker\mathbf{j} \\ j(1),...,j(n)=1}}^{k} u_{i(1)j(i)}...u_{i(n)j(n)}.
\end{aligned}$$

Por la segunda observación sabemos que $\sum_{\substack{\pi \leq ker\mathbf{j} \\ j(1),...,j(n)=1}}^{k} u_{i(1)j(i)}...u_{i(n)j(n)} =$ 1 si $ker\mathbf{i} \geq \pi$ y cero en otro caso. Así, nuestra suma es igual a

$$\sum_{\substack{\pi \in NC(n) \\ ker\mathbf{i} \geq \pi}} \psi(k_\pi) = \psi(\sum_{\substack{\pi \in NC(n) \\ ker\mathbf{i} \geq \pi}} k_\pi)$$
$$= \psi(\sum_{\substack{\pi \in NC(n) \\ ker\mathbf{i} \geq \pi}} k_\pi(x_{i(1)}, ..., x_{i(n)}))$$

pues $k_\pi(x_{j(1)}, ..., x_{j(n)}) = k_\pi$ si $\pi \leq ker\mathbf{j}$ por ser idénticamente distribuidos. Finalmente esto es igual a

$$\psi(E(x_{i(1)}, ..., x_{i(n)})) = \psi(x_{i(1)}, ..., x_{i(n)}),$$

que es lo que queríamos probar.

Ahora nuestro trabajo sera probar 1) $\Rightarrow$ 2). Claramente tenemos las contenciones $A_{tail} \subset A_\infty \subset A$, para nuestras pruebas asumiremos sin pérdida de la generalidad que A es generado por (x_i) es decir $A = A_\infty$. Para comenzar la prueba lo primero que veremos es que si (x_i) es intercambiable en el sentido cuántico, entonces también lo es bajo E. Esto es $\forall k, n \in \mathbb{N}$, $(u_{ij})_{i,j=i}^{k}$ un generador de un grupo de permutaciones $A_s(k)$, para todo $1 \leq i(1), ..., i(n) \leq k$ y $b_2, ..., b_n \in A_{tail}$ se cumple que

$$E(x_{i(1)}b_2x_{i(2)}...b_nx_{i(n)}) = \sum_{j(1),..,j(n)=1}^{k} u_{i(1)j(1)}...u_{i(n)j(n)}E(x_{j(1)}b_2x_{j(2)}...b_nx_{j(n)}). \tag{2.4.1}$$

Más generalmente para todo $p_1, .., p_n \in A_{tail} < X >$ se cumple

$$E(p_1(x_{i(1)})...p_n(x_{i(n)})) = \sum_{j(1),..,j(n)=1}^{k} u_{i(1)j(1)}...u_{i(n)j(n)}E(p_1(x_{j(1)})...p_n(x_{j(n)})). \tag{2.4.2}$$

Probaremos (2.4.1) y esencialmente la misma prueba se extiende a (2.4.2).Sean $n, k \in \mathbb{N}$, $1 \leq i(1), .., i(n) \leq k$. Como $\psi_{A|_\infty} = \psi_\infty = \psi_\infty \circ E$ tenemos que si $b_1, .., b_n \in A_{tail}$ entonces

$$\psi(b_1x_{i(1)}...b_nx(i(n)) = \psi_\infty(b_1x_{i(1)}...b_nx(i(n)) = \psi_\infty(E[b_1x_{i(1)}...b_nx(i(n)])$$

Si pudiéramos verificar que

$$\psi(b_1 x_{i(1)} ... b_n x_{i(n)}) = \sum_{j(1),...,j(n)=1}^{k} u_{i(1)j(1)} ... u_{i(n)j(n)} \psi(b_1 x_{j(1)} ... b_n x_{j(n)}) \quad (2.4.3)$$

tendríamos por la primera observación que

$$\begin{aligned} \psi_\infty(b_1 E[x_{i(1)} ... b_n x_{i(n)}]) &= \psi_\infty(E[b_1 x_{i(1)} ... b_n x_{i(n)}]) \\ &= \psi_\infty(b_1 x_{i(1)} ... b_n x_{i(n)}) = \psi(b_1 x_{i(1)} ... b_n x_{i(n)}) \\ &= \sum_{j(1),...,j(n)=1}^{k} u_{i(1)j(1)} ... u_{i(n)j(n)} \psi(b_1 x_{j(1)} ... b_n x_{j(n)}) \\ &= \sum_{j(1),...,j(n)=1}^{k} u_{i(1)j(1)} ... u_{i(n)j(n)} \psi_\infty(b_1 x_{j(1)} ... b_n x_{j(n)}) \\ &= \sum_{j(1),...,j(n)=1}^{k} u_{i(1)j(1)} ... u_{i(n)j(n)} \psi_\infty(E[b_1 x_{j(1)} ... b_n x_{j(n)}]) \\ &= \psi_\infty(b_1 \sum_{j(1),...,j(n)=1}^{k} u_{i(1)j(1)} ... u_{i(n)j(n)} E[x_{j(1)} ... b_n x_{j(n)}]) \end{aligned}$$

y como $b_1 \in A_{tail}$ fue arbitrario esto es que

$$\psi_\infty(b_1 E[x_{i(1)} ... b_n x_{i(n)}]) = \psi_\infty(b_1 \sum_{j(1),...,j(n)=1}^{k} u_{i(1)j(1)} ... u_{i(n)j(n)} E[x_{j(1)} ... b_n x_{j(n)}])$$

para todo $b_1 \in A_{tail}$ y por ende

$$E[x_{i(1)} ... b_n x_{i(n)}] = \sum_{j(1),...,j(n)=1}^{k} u_{i(1)j(1)} ... u_{i(n)j(n)} E[x_{j(1)} ... b_n x_{j(n)}],$$

que es lo que queríamos probar, es decir bastará probar (2.4.3).

Para esto notemos que basta probarlo para cuando $b_1, ..., b_n$ es de la forma $x_{r(1)}, .., x_{r(n)}$ con $r(i) > k$ para $1 \leq i \leq n$ pues para los b_i de la forma x_l con $l \leq k$ ya lo tenemos por intercambiabilidad en el sentido cuántico, así si lo probamos para b_i de la forma x_l con $l > k$ habríamos probado que (2.4.3) se cumple para todo b_i de la forma x_j y como A_{tail} queda determinado por

$(x_i)_{i\in\mathbb{N}}$ podemos aproximar cualquier $b_i \in A_{tail}$ por elementos de la forma x_i. Es decir nuestra meta es probar que

$$\psi(b_1 x_{i(1)}...b_n x_{i(n)}) = \sum_{j(1),...,j(n)=1}^{k} u_{i(1)j(1)}...u_{i(n)j(n)}\psi(b_1 x_{j(1)}...b_n x_{j(n)}) \quad (2.4.4)$$

para todo $b_1,..,b_n$ de la forma $x_{r(1)},...,x_{r(n)}$ con $r(i) \geq k+1$ para $1 \leq i \leq n$. Sean $b_1,...,b_n \in A_{tail}$ de esta forma, definimos $N = max\{l|x_{i(s)} = x_l$ ó $x_{r(s)} = x_l$ p.a $s\}$ el máximo de los indices de x_i en el termino $b_1 x_{i(1)}...b_n x_{i(n)}$ (recordemos que $b_i = x_{r(i)}$ para $1 \leq i \leq n$). Sea $\hat{U} = (\hat{u}_{ij})_{i,j=1}^{N}$ dada por $\hat{u}_{i,j} = \begin{cases} u_{i,j} & 1 \leq i,j \leq k \\ \delta_{i,j} & \text{en otro caso} \end{cases}$ Por cómo está definida $\hat{U}$, éste genera un grupo cuántico $A_s(N)$ y la intercambiabilidad en el sentido cuántico de $(x_i)_{i\in\mathbb{N}}$ nos dice que

$$\begin{aligned} &\psi(b_1 x_{i(1)}...b_n x_{i(n)}) = \psi(x_{r(1)}x_{i(1)}...x_{r(n)}x_{i(n)}) \\ = &\sum_{j(1),..,j(2n)=1}^{2k} \hat{u}_{r(1)j(1)}\hat{u}_{i(1)j(2)}....\hat{u}_{r(n)j(2n-1)}\hat{u}_{i(n)j(2n)}\psi(x_{j(1)}...x_{j(2n)}). \end{aligned}$$

Luego como $r(l) > k$ para $1 \leq l \leq n$, entonces $\hat{u}_{r(l)j(l)} = \delta_{r(l)j(l)}$. Así esto es

$$\begin{aligned} &\sum_{\substack{j(2),...,j(2n)=1 \\ j(1)=r(1),..,j(2n-1)=r(n)}}^{2k} \hat{u}_{i(1)j(2)}....\hat{u}_{i(n)j(2n)}\psi(x_{j(1)}x_{j(2)}...x_{j(n)}x_{j(2n)}) \\ = &\sum_{j(2),j(4)..,j(2n)=1}^{2k} \hat{u}_{i(1)j(2)}....\hat{u}_{i(n)j(2n)}\psi(x_{r(1)}x_{j(2)}...x_{r(n)}x_{j(2n)}) \end{aligned}$$

Además, como $1 \leq i(1),...,i(n) \leq k$ y $\hat{u}_{i(l)j(2l)} = 0$ si $j(2l) \geq k+1$, esto es,

$$\sum_{j(2),j(4)..,j(2n)=1}^{k} \hat{u}_{i(1)j(2)}....\hat{u}_{i(n)j(2n)}\psi(x_{r(1)}x_{j(2)}...x_{r(n)}x_{j(2n)})$$

haciendo $j(l) = j(2l)$ y usando que si $j(2l) \leq k$ entonces $\hat{u}_{i(l)j(2l)} = u_{i(l)j(2l)}$

lo anterior es

$$\begin{aligned}
&\sum_{j(1),j(2)..,j(n)=1}^{k} u_{i(1)j(1)}....u_{i(n)j(n)}\psi(x_{r(1)}x_{j(1)}...x_{r(n)}x_{j(n)}) \\
=&\sum_{j(1),j(2)..,j(n)=1}^{k} u_{i(1)j(1)}....u_{i(n)j(n)}\psi(b_1x_{j(1)}...b_nx_{j(n)}).
\end{aligned}$$

Esto último es precisamente (2.4.4), hemos probado así (2.4.1) y (2.4.2).

Ahora probaremos otra propiedad de E a la que llamaremos la propiedad de factorización, la cual dice lo siguiente; si $(x_i)_{i\in\mathbb{N}}$ es intercambiable, entonces para todo $n \in \mathbb{N}$ e $i(1),..,i(n) \in \mathbb{N}$ se cumple que

$$E(p_1(x_{i(1)})...p_n(x_{i(n)})) = E(p_1(x_{i(1)})...E(p_l(x_{i(l)}))...p_n(x_{i(n)})) \qquad (2.4.5)$$

siempre y cuando $i(l) \neq i(r)$ para todo $r \neq l$.

Pasemos a la prueba de (2.4.5). Sea $L^2(A,\psi)$ el GNS espacio de Hilbert con producto interno definido por $< a,b >= \psi(a^*b)$. La intercambiabilidad de (x_i) nos permite definir una isometria α en $L^2(A,\psi)$ dada por $\alpha(x_{i(1)}...x_{i(n)}) = x_{i(1)+1}...x_{i(n)+1}$. Restringidos a $A \subset L^2(A,\psi)$, esta isometría es una aplicación de A en A que actúa como un endomorfismo, sea $A_\alpha = \{a \in A|\alpha(a) = a\}$ el conjunto de puntos fijos bajo α.

Claramente $A_\alpha \subset A_{tail}$ pues si $x_i \in A_\alpha$ entonces $x_i = \alpha(x_i) = x_{i+1}$, y así consecutivamente se llega a que $x_i = x_n$ para todo n y por ende $x_i \in VN(x_k|k \geq n)$ para todo n, es decir $x_i \in A_{tail}$, para un elemento cualquiera de A_α se usa que este elemento puede ser aproximado por elementos de la forma x_i pues $A_\alpha \subset A$ y estamos suponiendo que A es generado por $(x_i)_{i\in\mathbb{N}}$. Veremos que además $A_\alpha \subset A_{tail}$, sea $b \in A_{tail}$ y consideremos para $m \in \mathbb{N}$ y $r(1),..,r(m) \in \mathbb{N}$ el momento $\psi(x_{r(1)}...x_{r(m)}b)$, aproximando b con polinomios no conmutativos en $\{x_k|k > max(r(1),...,r(m))\}$ y usando la intercambiabilidad de (x_i) tenemos que

$$\psi(x_{r(1)}...x_{r(m)}b) = \psi(x_{r(1)}...x_{r(m)} \lim_{n\to\infty} p_n(x_{k_1}, x_{k_2}, .., x_{k_n}))$$

donde p_n es un polinomio en x_{k_i} con $k_i > max(r(1),..,r(m)))$, por otro lado $\alpha(b) \in A$ y como A esta generado por (x_i) tenemos que $\alpha(b) = p_l(x_{s_1},..,x_{s_l})$ es alguna combinación de elementos de (x_i). Finalmente, por intercambiabilidad de (x_i) y por como tomamos x_{k_i} tenemos que

$$\begin{aligned}\psi(x_{r(1)}...x_{r(m)}\lim_{n\to\infty} p_n(x_{k_1},x_{k_2},..,x_{k_n})) &= \psi(x_{r(1)}...x_{r(m)}\lim_{n\to\infty} p_l(x_{s_1},..,x_{s_l}))\\ &= \psi(x_{r(1)}...x_{r(m)}\lim_{n\to\infty}\alpha(b))\\ &= \psi(x_{r(1)}...x_{r(m)}\alpha(b))\end{aligned}$$

Es decir $\psi(x_{r(1)}...x_{r(m)}b) = \psi(x_{r(1)}...x_{r(m)}\alpha(b))$, como $r(1),...,r(m)$ y m fueron arbitrarios esto último nos prueba que $\psi(ab) = \psi(a\alpha(b))$ para todo $a \in A$ y así $b = \alpha(b)$, es decir $b \in A_\alpha$, por lo tanto $A_\alpha = A_{tail}$. Sea $E_\alpha : A \to A_\alpha$ una esperanza condicional, dado que $A_{tail} = A_\alpha$ tenemos que $E_\alpha : A \to A_{tail}$ y por unicidad tenemos $E = E_\alpha$. Ahora, por el teorema ergódico de Von Neumann tenemos que $\lim_{m\to\infty}\frac{1}{m}\sum_{i=1}^{m}\alpha^i(a) = E_\alpha(a) = E(a)$. Por otro lado recordemos que tenemos intercambiabilidad con respecto a E, de donde se sigue que $E(p_1(x_{i(1)})...p_l(x_{i(l)})...p_n(x_{i(n)})) = E(p_1(x_{i(1)})...p_l(x_i)...p_n(x_{i(n)}))$ para todo $i > max(i(1),...,i(n)) = N$. Así,

$$\begin{aligned}&E(p_1(x_{i(1)})...p_l(x_{i(l)})...p_n(x_{i(n)})) = \frac{1}{m}mE(p_1(x_{i(1)})...p_l(x_{N+1})...p_n(x_{i(n)}))\\ &= \frac{1}{m}E(p_1(x_{i(1)})...p_l(x_{N+1})...p_n(x_{i(n)})) + ... + E(p_1(x_{i(1)})...p_l(x_{N+m})...p_n(x_{i(n)}))\\ &= \frac{1}{m}\sum_{j=N+1}^{N+m} E(p_1(x_{i(1)})...p_l(x_j)...p_n(x_{i(n)}))\\ &= E[p_1(x_{i(1)})...(\frac{1}{m}\sum_{j=N+1}^{N+m} p_l(x_j))...p_n(x_{i(n)})],\end{aligned}$$

pero sabemos que

$$\begin{aligned}\frac{1}{m}\sum_{j=N+1}^{N+m} p_l(x_j) &= \frac{1}{m}[p_l(x_{N+1}) + .. + p_l(x_{N+m})]\\ &= \frac{1}{m}[p_l(\alpha(x_N)) + .. + p_l(\alpha^m(x_N))]\\ &= \frac{1}{m}\sum_{i=1}^{m}\alpha^i(p_l(x_N)),\end{aligned}$$

y esto último converge a $E[p_l(x_N)] = E[p_l(x_{i(l)})]$.

Más adelante veremos que las (x_i) son idénticamente distribuidas con respecto a E, por lo que tomado el límite obtenemos

$$E(p_1(x_{i(1)})...p_l(x_{i(l)})...p_n(x_{i(n)})) = E(p_1(x_{i(1)})...E[p_l(x_{i(l)})]...p_n(x_{i(n)}))$$

que es precisamente (2.4.5).

Estamos listos para probar 1) $\Rightarrow$ 2). Para verificar que (x_i) son idénticamente distribuidas con respecto a E bastará usar un caso particular de simple intercambiabilidad de (2.4.2) para obtener que $E[p_1(x_{i(1)})] = E[p_1(x_{j(1)})]$ para todo $i(1), j(1)$. Faltara ver que (x_i) son libres con respecto a E o independientes con amalgamacion sobre A_{tail}. Sean $n \in \mathbb{N}$, $i(1) \neq i(2) \neq ... \neq i(n)$ y $p_1, ..., p_n \in A_{tail} < X >$ tales que $E[p_j(x_{i(j)})] = 0$ para todo $j = 1, .., n$, nuestro objetivo es ver que $E[p_1(x_{i(1)})...p_n(x_{i(n)})] = 0$. Vamos a probar esto usando inducción hacia atrás sobre el numero de bloques de $Ker\mathbf{i}$, para esto denotaremos a $|ker\mathbf{i}|$ a su numero de bloques. Si $|ker\mathbf{i}| = n$ tenemos que $i(l) \neq i(m)$ para toda $l \neq m$, así por (2.4.5) tenemos que

$$E[p_1(x_{i(1)})...p_n(x_{i(n)})] = \prod_{j=1}^{n} E[p_j(x_{i(j)}) = 0$$

tenemos nuestro caso base probado. Supongamos que para algún r tal que $|ker\mathbf{i}| \geq r+1$ hemos probado que $E[p_1(x_{i(1)})...p_n(x_{i(n)})] = 0$, queremos probar lo mismo para cuando $|ker\mathbf{i}| = r$. Por (2.4.2) tenemos que para algún $k \in \mathbb{N}$, $1 \leq j(1), .., j(n) \leq k$ y algún grupo cuántico de permutaciones $u = (u_{ij})$ se tiene

$$E(p_1(x_{i(1)})...p_n(x_{i(n)})) = \sum_{j(1),..,j(n)=1}^{k} u_{i(1)j(1)}...u_{i(n)j(n)} E(p_1(x_{j(1)})...p_n(x_{j(n)})).$$

Sumando sobre todas las particiones esto es,

$$\sum_{\pi \in P(n)} \sum_{\substack{j(1),..,j(n)=1 \\ ker\mathbf{j}=\pi}}^{k} u_{i(1)j(1)}...u_{i(n)j(n)} E(p_1(x_{j(1)})...p_n(x_{j(n)})).$$

Notemos que $u_{i(l)j(l)}u_{i(l+1)j(l+1)} = 0$ si $j(l) = j(l+1)$ pues $i(l) \neq i(l+1)$. Así esta suma es igual a

$$\sum_{\pi \in P(n)} \sum_{\substack{j(1),..,j(n)=1 \\ ker\mathbf{j}=\pi \\ j(1)\neq j(2)\neq ...\neq j(n)}}^{k} u_{i(1)j(1)}...u_{i(n)j(n)}E(p_1(x_{j(1)})...p_n(x_{j(n)})),$$

pero si $|\pi| \geq r+1$ como $j(1) \neq j(2) \neq ... \neq j(n)$ por hipótesis de inducción sabemos $E[p_1(x_{j(1)})...p_n(x_{j(n)})] = 0$, por lo que esta suma es igual a

$$\sum_{\substack{\pi \in P(n) \\ |\pi|\leq r}} \sum_{\substack{j(1),..,j(n)=1 \\ ker\mathbf{j}=\pi \\ j(1)\neq j(2)\neq ...\neq j(n)}}^{k} u_{i(1)j(1)}...u_{i(n)j(n)}E(p_1(x_{j(1)})...p_n(x_{j(n)})).$$

Por otro lado, del hecho de que $E(p_1(x_{i(1)})...p_n(x_{i(n)}))$ es invariante bajo permutaciones cuánticas tenemos que

$$E(p_1(x_{i(1)})...p_n(x_{i(n)})) = E(p_1(x_{s(1)})...p_n(x_{s(n)}))$$

para todo $1 \leq s(1),...,s(n) \leq k$ con $ker\mathbf{i} = ker\mathbf{s}$. Tomando el caso particular $k = 2r$ por lo anterior podemos fijar diferentes valores para los $i-$índices de los r bloques de $ker\mathbf{i}$, digamos $1, 3, 5, ..., 2r-1$. Consideremos ahora el caso particular donde $U = (u_{ij})_{ij=1}^{k}$ está dada por:

$$u_{i,j} = \begin{cases} q_i & i = j \text{ y ambos son impares} \\ q_{i-1} & i = j \text{ y ambos son pares} \\ 1 - q_i & i + 1 = j \text{ e i es impar} \\ 1 - q_j & i = j + 1 \text{ e i es par} \\ 0 & \text{en otro caso} \end{cases}$$

donde $q_1, .., q_r$ son proyecciones arbitrarias. Notemos que como $i(1), .., i(n)$ tiene la misma paridad, entonces si $j(j) = j(s)$ necesariamente $i(l) = i(s)$, esto nos dice que $ker\mathbf{j} \leq ker\mathbf{i}$, mas aún como $|ker\mathbf{i}| = r$ entonces por lo anterior $|ker\mathbf{j}| \geq r$, por otro lado en nuestra suma tenemos que $ker\mathbf{j} = \pi$ y que sumamos sobre π con $|\pi| \leq r$, esto nos dice que $|ker\mathbf{j}| \leq r$, es decir necesariamente $|ker\mathbf{j}| = r$ y como $ker\mathbf{j} \leq ker\mathbf{i}$ y $|ker\mathbf{i}| = r$ necesariamente

$ker\mathbf{j} = ker\mathbf{i}$, de donde se sigue que nuestra suma no se anula sólo cuando $\pi = ker\mathbf{i}$, por lo que tenemos

$$\begin{aligned} & E(p_1(x_{i(1)})...p_n(x_{i(n)})) \\ &= \sum_{\substack{\pi\in P(n)\\ |\pi|\leq r}} \sum_{\substack{j(1),..,j(n)=1\\ ker\mathbf{j}=\pi \\ j(1)\neq j(2)\neq ...\neq j(n)}}^{k} u_{i(1)j(1)}...u_{i(n)j(n)} E(p_1(x_{j(1)})...p_n(x_{j(n)})) \\ &= \sum_{\substack{j(1),..,j(n)=1\\ ker\mathbf{j}=ker\mathbf{i}}}^{2r} u_{i(1)j(1)}...u_{i(n)j(n)} E(p_1(x_{j(1)})...p_n(x_{j(n)})). \end{aligned}$$

Mas aún como los (x_i) son idénticamente distribuidos con respecto a E y $ker\mathbf{j} = ker\mathbf{i}$ tenemos $E(p_1(x_{j(1)})...p_n(x_{j(n)})) = E(p_1(x_{i(1)})...p_n(x_{i(n)}))$, luego esto es,

$$\sum_{\substack{j(1),..,j(n)=1\\ ker\mathbf{j}=ker\mathbf{i}}}^{2r} u_{i(1)j(1)}...u_{i(n)j(n)} E(p_1(x_{i(1)})...p_n(x_{i(n)})).$$

Es decir, hemos probado que

$$E(p_1(x_{i(1)})...p_n(x_{i(n)})) = E(p_1(x_{i(1)})...p_n(x_{i(n)}))(\sum_{\substack{j(1),..,j(n)=1\\ ker\mathbf{j}=ker\mathbf{i}}}^{2r} u_{i(1)j(1)}...u_{i(n)j(n)}).$$

Si pudiéramos verificar que $\sum_{\substack{j(1),..,j(n)=1\\ ker\mathbf{j}=ker\mathbf{i}}}^{2r} u_{i(1)j(1)}...u_{i(n)j(n)} \neq 1$ tendríamos que necesariamente $E(p_1(x_{i(1)})...p_n(x_{i(n)})) = 0$ y habríamos terminado, nuestro objetivo sera probar esto precisamente. Para esto notemos que si $ker\mathbf{i} \in NC(n)$ entonces la condición de $i(1) \neq i(2) \neq ... \neq i(n)$ asegura que existe un singleton (un bloque con un solo elemento) digamos $i(l)$, luego por (2.4.5) tendríamos que $E(p_1(x_{i(1)})...p_n(x_{i(n)})) = E(p_1(x_{i(1)})...E[p_l(x_{i(l)})]...p_n(x_{i(n)})) = 0$ pues $E[p_l(x_{i(l)})] = 0$, bastara entonces considerar $ker\mathbf{i} \in P(n)/NC(n)$. Pasemos a probar que $\sum_{\substack{j(1),..,j(n)=1\\ ker\mathbf{j}=ker\mathbf{i}}}^{2r} u_{i(1)j(1)}...u_{i(n)j(n)} \neq 1$. Como estamos considerando $ker\mathbf{i} \in P(n)/NC(n)$ sean $i(l)$ e $i(m)$ elementos en distintos bloques del $ker\mathbf{i}$ tal que sus bloques se cruzan, sin perdida de la generalidad supongamos $i(l) = 1$ e $i(m) = 3$, consideremos $q_1 = u_{11} = p$ y $q_2 = u_3 3 = q$ dos proyecciones que no conmutan y $u_l l = 1$ para todo $l \neq 1, 3$. Sean B_1 y B_2 los bloques donde pertenecen 1 y 3 respectivamente y denotamos por $|B_1|$ y $|B_2|$ a su cantidad de elementos. Tenemos que

$$\sum_{\substack{j(1),..,j(n)=1 \\ ker\mathbf{j}=ker\mathbf{i}}}^{2r} u_{i(1)j(1)}...u_{i(n)j(n)} = \sum_{j(l),j(m)=1}^{2r} \sigma\big(u_{i(l)j(l)}...u_{i(l)j(l)}u_{i(m)j(m)}...u_{i(m)j(m)}\big)$$

para alguna $\sigma \in S_{|B_1|+|B_2|}$. Donde si $\sigma \in S_n$ se define $\sigma(a_1, ..., a_n) = \prod_{i=1}^{n} \sigma(a_i)$, además es importante notar que el factor $u_{i(l)j(l)}$ aparece $|B_1|$ veces mientras que $u_{i(m)j(m)}$ aparece $|B_2|$ veces. Luego esta última suma es

$$\begin{aligned}
&= \sum_{j(l)\in\{1,2\}} \sum_{j(m)\in\{3,4\}} \sigma\big(u_{i(l)j(l)}...u_{i(l)j(l)}u_{i(m)j(m)}...u_{i(m)j(m)}\big) \\
&\quad \sum_{p_1\in\{p,1-p\}} \sum_{p_2\in\{q,1-q\}} \sigma(p_1...p_1p_2...p_2) \\
&= \sigma(p...pq...q) + \sigma(p...p(1-q)...(1-q)) + \sigma((1-p)...(1-p)q...q) \\
&+ \sigma((1-p)...(1-p)(1-q)...(1-q)).
\end{aligned}$$

Usando ahora que $p = p^2$,$q = q^2$,$(1-p) = (1-p)^2$ y $(1-q) = (1-q)^2$, esta última igualdad es igual a

$$(pq)^s + (p(1-q))^s + ((1-p)q)^s + ((1-p)(1-q))^s$$

si $|B_1|$ y $|B_2|$ tienen la misma paridad y

$$(pq)^s p + (p(1-q))^s p + ((1-p)q)^s(1-p) + ((1-p)(1-q))^s(1-p) \quad (2.4.6)$$

si $|B_1|$ y $|B_2|$ tienen distinta paridad, para algún $s \geq 1$. Finalmente esto es claramente distinto de 1 y por ende hemos concluido. □

Observación: En la demostración anterior es importante que p y q no conmuten pues en otro caso la Ecuación (2.4.6) es idénticamente 1.

Bibliografía

[1] Aldous D. Exchangeability and related topics. Lecture Notes in Math. 1117, *Springer, Berlin*, (1985).

[2] Johnson W.E. Logic Part III the Logical Foundations of Science, *Cambridge University Press*, First Edition edition (1924).

[3] Kingman J.F. The Representation Theorem of Partition Structures, *Journal of the London Mathematical Society*, (1978), 374-380.

[4] Köstler C; Speicher R. A noncommutative De Finetti theorem: invariance under quantum permutations is equivalent to freeness with amalgamation, *Comm. Math. Phys.* 291, (2009), no. 2, 473–490.

[5] Murphy G.J. C^*-algebras and operator theory, *Academic Press, Inc., Boston, MA*, (1990), x+286 pp.

[6] Nica A; Speicher R. Lectures on the combinatorics of free probability. London Mathematical Society Lecture Note Series 335, *Cambridge University Press, Cambridge*, (2006).

[7] Takesaki M. Theory of operator algebras II. Encyclopaedia of Mathematical Sciences 125, Operator Algebras and Non-commutative Geometry 6, *Springer-Verlag, Berlin*, (2003), xxii+518 pp.

[8] Voiculescu D.V; Dykema K. J.; Nica A. Free random variables. A noncommutative probability approach to free products with applications to random matrices, operator algebras and harmonic analysis on free groups. CRM Monograph Series 1, *American Mathematical Society, Providence, RI*, 1992, vi+70 pp.

[9] Voiculescu D.V. Free probability theory (Waterloo, ON, 1995), *Fields Inst. Commun., 12, Amer. Math. Soc., Providence, RI*, (1997), 189-212.

[10] Voiculescu D.V. Symmetries of some reduced free product C^*-algebras, *Operator algebras and their connections with topology and ergodic theory*, (1983), 556–588.