Anaël Marit ENS Rennes

MATRICES ALÉATOIRES ET PROBABILITÉS LIBRES

- stage supervisé par Camille Male [(i)] -

—

Table des matières

(i). Chargé de recherches CNRS à l'Institut de Mathématiques de Bordeaux

Notations & définitions

Algèbres : Toutes les algèbres manipulées seront considérées unifères sur le corps de base $\mathbb{C}$. Si $\mathcal{A}$ est une telle algèbre, on notera $1_{\mathcal{A}}$ son unité.

Arbre : Un graphe est un arbre si, et seulement si, il est connexe et acyclique. Par connexe, on entend que tout couple de sommets du graphe peut être relié par un chemin formé d'arrêtes ordonnées telles que deux arrêtes successives soient telles que le but de la première soit la source de la seconde. Par acyclique, on veut dire qu'il n'existe aucun tel chemin qui soit une boucle, c'est-à-dire un chemin dont la source et le but sont confondus et dont chaque arrête est parcourue exactement une fois.

Cardinal : Pour un ensemble X donné, on notera $|X|$ ou $\#X$ son cardinal (éventuellement infini).

Espace probabilisé : dans tout ce rapport, on désignera par $(\Omega, \mathfrak{F}, \mathbb{P})$ un espace probabilisé quelconque lorsque la connaissance de l'espace sous-jacent importera peu.

Espaces L^p : pour $p \in [1, +\infty]$, on notera L^p l'ensemble des variables aléatoires complexes sur $(\Omega, \mathfrak{F}, \mathbb{P})$ de puissance p-ième intégrable modulo l'égalité presque partout. On pose de plus :

$$L^{\infty-} := \bigcap_{n \in N^*} L^n \tag{1}$$

l'ensemble des variables aléatoires admettant des moments à tout ordre.

Flèches : On utilisera les conventions suivantes pour donner des indications sur les applications : $f : E \rightarrowtail F$ indique que f est injective ; $f : E \leftrightarrow F$ indique que f est bijective. Si A et B sont deux ensembles finis, on s'autorisera l'écriture :

$$\sum_{f : A \rightarrowtail B} \tag{2}$$

pour indiquer que la somme est prise sur l'ensemble des injections de A dans B.

Graphe squelette : Etant donné un multi-graphe, éventuellement orienté, $G = (V, E)$, c'est-à-dire un graphe dont on autorise les arrêtes à être multiples, on appelle *squelette* de G et on note $\bar{G} = (\bar{V}, \bar{E})$ le graphe non orienté obtenu en oubliant l'orientation et la multiplicité des arrêtes de G.

Intervalles d'entiers Pour $(n, p) \in \mathbb{N}^2$, $n \leqslant p$ on notera simplement $[\![n, p]\!]$ l'intervalle d'entiers $\{n, n+1, \dots p\}$. Si $n = 1$, on écrira de façon plus compacte $[\![p]\!]$.

Multi-indice alterné : Soit I un ensemble d'indices et soit $\boldsymbol{i} = (i_1, \dots i_n) \subset I$ un multi-indice. On dira que $\boldsymbol{i}$ est *alterné* lorsque, pour tout $1 \leqslant k \leqslant n-1$, on a $i_k \neq i_{k+1}$. Par exemple, $(1, 2, 1, 2)$ est alterné, mais $(1, 2, 2, 1)$ ne l'est pas.

Partitions : Etant donné un ensemble X, on notera $\mathcal{P}(X)$ l'ensemble des partitions de X. Si X est un poset (cf définition 2), on notera $NC(X)$ l'ensemble de ses partitions non-croisées (cf définition 4). Dans le cas particulier où $X = [\![n]\!]$, on notera alors $NC(n)$.

Si A et B sont deux ensembles disjoints, et π et σ sont des partitions respectivement de A et de B, on notera $\pi \sqcup \sigma$ la partition de $A \sqcup B$ composée des blocs de σ et π. Dans le cas spécifique où $A = B = [\![n]\!]$ (A et B n'étant alors pas disjoints), on s'autorisera tout de même cette notation en prenant alors des éléments formels $\bar{1}, \dots \bar{n}$ tels que $1 \leqslant \bar{1} \leqslant 2 \dots n \leqslant \bar{n}$, et en voyant σ comme une partition de $\{\bar{1} \dots \bar{n}\}$.

On parlera de partition *paire* lorsque tous les blocs d'une partition sont de taille exactement 2.

Polynômes : Soit $(X_i)_{i\in I}$ une famille d'indéterminées. On notera respectivement $\mathbb{C}[X_i \mid i \in I]$ l'ensemble des polynômes à coefficients dans $\mathbb{C}$ en ces indéterminées, et $\mathbb{C}\langle X_i \mid i \in I\rangle$ celui des polynômes non-commutatifs en ces indéterminées (cf définition 16).

Produits : on travaillera fréquemment dans des algèbres non-commutatives. Lorsqu'on fera le produit de n éléments (x_i) pour lequel on souhaite préciser que l'ordre des facteurs est important, on utilisera la notation :

$$\prod_{i=1}^{\overrightarrow{n}} x_i = x_1 x_2 \dots x_n. \tag{3}$$

Union disjointe : Si A et B sont deux ensembles disjoints, on notera $A \sqcup B$ leur union. L'utilisation du symbole $\sqcup$ dans les union sera utilisé pour signifier que toutes les parties considérées sont disjointes, sans que cela ait été précisé au préalable. Par exemple, on s'autorisera à écrire :

$$\sum_{A\sqcup B=X} \tag{4}$$

pour indiquer que la somme est prise sur l'ensemble des parties disjointes de X dont l'union est X tout entier.

Introduction

Au cours de mon stage, effectué sous la direction de Camille Male, j'ai été amené à étudier les bases de deux théories mathématiques : celle des matrices aléatoires, et celle des probabilités libres. Historiquement, ces deux champs de recherche sont apparus sans connexion l'un avec l'autre. Le premier fut introduit par Eugene Wigner, initialement pour modéliser des problèmes physique, et a su trouver aujourd'hui de nombreuses autres applications, notamment en statistiques. Le second propose une approche des probabilités lorsque les variables aléatoires manipulées ne commutent pas entre elles. Elle fut historiquement développée par Dan Voiculescu afin d'apporter des réponses à des questions d'ordre algébrique, et prolongée par plusieurs mathématiciens tels que les auteurs de [7].

L'enjeu de ce stage a été de découvrir et de s'approprier les outils de base de la théorie des probabilités libres dans le but d'étudier l'une des connexions existant avec celle des matrices aléatoires. Pour ce faire, Camille Male m'a proposé d'apprendre des éléments de formalisme propres à la théorie des trafics - théorie qu'il a lui-même développée avec plusieurs collaborateurs - dans le but d'énoncer et démontrer un théorème dit de liberté asymptotique.

Ce rapport se décomposera en quatre temps. Tout d'abord, nous nous proposons de regrouper des notions de combinatoire dont nous nous servirons abondamment par la suite, et feront office de préliminaires. Ensuite, nous aborderons la théorie des probabilités libres, en détaillerons certains des concepts et outils clefs pour finir sur un analogue du théorème central limite. La troisième partie sera consacrée à une brève familiarisation avec les matrices aléatoires, et plus particulièrement avec l'étude des «grandes matrices aléatoires», c'est-à-dire l'étude des comportements limites de matrices aléatoires lorsque la taille de celles-ci tend vers l'infini. A cette occasion, nous évoquerons le théorème de Wigner, à la base de la théorie des grandes matrices aléatoires. C'est dans cette partie également que nous introduirons le formalisme des trafics. Enfin, la quatrième et dernière partie utilisera tous les outils développés à ce stade pour énoncer et démontrer le théorème de liberté asymptotique, généralisant celui de Wigner.

1 Préliminaires combinatoires

Une bonne partie des résultats que nous aborderons par la suite repose sur certaines notions de combinatoire qu'il nous est nécessaire de développer en amont. Afin de ne pas hypertrophier les différentes sections, et éviter de dévier de nos objectifs chaque fois qu'un tel résultat nous sera nécessaire, nous avons jugé bon de tous les rassembler dans cette première section introductive. Toutefois, nous nous évertuerons à placer des renvois dans le corps du texte, de sorte à aider le lecteur à se référer aux résultats de cette section lorsque cela sera nécessaire.

1.1 Nombres de Catalan

La théorie des probabilités libres, ainsi que celle des matrices aléatoires, font régulièrement apparaître une suite de nombres, appelés nombres de Catalan, qui se trouve être tout à fait centrale dans nombre de résultats.

Définition 1 (Nombres de Catalan). *On appelle* nombres de Catalan *les termes de la suite (C_n) définie par la formule de récurrence :*

$$\begin{cases} C_0 = C_1 = 1 \\ \forall n \in \mathbb{N}^*,\ C_{n+1} = \sum_{k=0}^{n} C_k C_{n-k} \end{cases} \tag{5}$$

La définition des nombres de Catalan ne fait pas consensus, car ces nombres dénombrent plusieurs objets assez fréquents, tels que les arbres enracinés à n sommets ou encore les mots de Dyck de taille $2n$ sur un alphabet à deux lettres. Alice Guionnet étudie dans le premier chapitre de [3] les différentes bijections entre ces ensembles d'objets. Une expression explicite des nombres de Catalan y est démontrée :

Proposition 1 (admise). *On dispose d'une expression explicite des nombres de* Catalan *:*

$$\forall n \in \mathbb{N}^*,\ C_n = \frac{1}{n+1}\binom{2n}{n}. \tag{6}$$

1.2 Partitions non croisées

On se propose maintenant d'étudier certains ensembles de partitions qui seront au cœur de notre étude. Si X est un ensemble, on notera $\mathcal{P}(X)$ l'ensemble de ses partitions.

La notion de partition non-croisée se définit correctement dans le cadre des «poset» :

Définition 2 (Poset). *Un* poset *(de l'anglais «partially ordered set») est un couple $(X, \leqslant)$ tel que X est un ensemble quelconque et $\leqslant$ est une relation d'ordre partielle sur X, c'est-à-dire une relation binaire réflexive, transitive et antisymétrique. Cette relation étant partielle, il n'est pas toujours possible de comparer deux éléments distincts de X.*

Définition 3 (Intervalle). *Soit X un poset et soit $(x, y) \in X^2$ tel que $x \leqslant y$. On pose alors :*

$$[x\ ;\ y] := \{z \in X \mid x \leqslant z \leqslant y\} \tag{7}$$

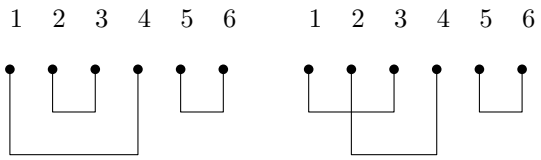
On peut faire la remarque suivante : étant donné un poset fini X, il est toujours possible de donner une énumération de X sous la forme $x_1, \dots x_n$ de telle sorte que pour tout $1 \leqslant i < j \leqslant n$ on ait $x_i < x_j$ ou alors x_i et x_j sont incomparables. Ceci se prouve par récurrence sur le cardinal de X en commençant par considérer un élément minimal de X puis en appliquant l'hypothèse de récurrence au poset obtenu en privant X de cet élément.

Définition 4 (Partition croisée). *Soit X un poset. Soit $\pi \in \mathcal{P}(X)$. On dit que π est* croisée *si, et seulement si :*

$$\exists (B_1, B_2) \in \pi^2,\ B_1 \neq B_2\ :\ \exists (p_1, q_1) \in B_1^2,\ \exists (p_2, q_2) \in B_2^2\ :\ p_1 < p_2 < q_1 < q_2. \tag{8}$$

Une partition non-croisée est simplement une partition qui n'est pas croisée. Nous noterons $NC(X)$ l'ensemble des partitions non-croisées de X. Dans le cas particulier $X = [\![n]\!]$, on notera plus simplement $NC(n)$.

On peut donner une vision très graphique de cette propriété, qui sera beaucoup plus parlante. Prenons pour poset $[\![6]\!]$ et représentons-en une partition en notant côtes à côtes les nombres de 1 à 6, puis en reliant d'un trait tous ceux qui appartiennent à la même classe d'équivalence :



A gauche, la partition $\{\{1,4\},\{2,3\},\{5,6\}\}$ est non croisée. A droite, la partition $\{\{1,3\},\{2,4\},\{5,6\}\}$ est croisée. Aussi, il apparaît que graphiquement, une partition croisée est littéralement «croisée».

Un soucis de cette définition de partition non-croisée est qu'elle s'obtient à partir d'une négation, aussi est-elle souvent peu commode pour travailler autrement que par l'absurde. Il y a une autre définition équivalente, très pratique, que nous donnons ici et utiliserons plus bas, mais sans démonstration :

Théorème 1 (Admis). *Soit $\pi \in \mathcal{P}(n)$. Alors π est non croisée si, et seulement si, π admet ce que nous appellerons un bloc segment , c'est-à-dire un bloc formant un segment d'entiers, et que la partition obtenue en retirant ce bloc de π est toujours non-croisée.*

Les partitions non-croisées sont premier exemple de cas où les nombres de Catalan apparaissent :

Proposition 2.

$$\forall n \in \mathbb{N}^*,\ |NC(n)| = C_n \tag{9}$$

Démonstration. Soit $n \in \mathbb{N}^*$. Pour $1 \leqslant i \leqslant n$, notons $NC^{(i)}(n)$ l'ensemble des partitions non croisées tel que i est l'élément maximal du bloc contenant 1. Pour $\pi \in NC^{(i)}(n)$, la propriété «non-croisée» impose que π se décompose sous la forme $\pi_1 \sqcup \pi_2$, où $\pi_1 \in NC^{(i)}(i)$ et $\pi_2 \in NC(n-i+1)$. Réciproquement, tout partition π admettant une telle décomposition est nécessairement

dans $NC^{(i)}(n)$. Par ailleurs, il est clair que $NC^{(i)}(i)$ a le même cardinal que $NC(i-1)$. D'où :

$$|NC(n)| = \left| \bigsqcup_{i=1}^{n} NC^{(i)}(n) \right| \tag{10}$$

$$= \sum_{i=1}^{n} |NC^{(i)}(n)| \tag{11}$$

$$= \sum_{i=1}^{n} |NC(i-1)||NC(n-i+1)|. \tag{12}$$

C'est exactement la formule (5). □

Faisons quelques observations portant sur la structure de $NC(n)$:

Définition 5. *On définit une relation d'ordre partielle sur $\mathcal{P}(n)$ par :*

$$\forall(\pi,\sigma) \in \mathcal{P}(n)^2,\ \pi \leqslant \sigma \iff (\forall B \in \pi,\ \exists B' \in \sigma\ :\ B \subset B'). \tag{13}$$

En d'autres termes, $\pi \leqslant \sigma$ si, et seulement si, tout bloc de π est contenu dans un bloc de σ. L'ordre $\leqslant$ munit $NC(n)$ d'une structure de poset.

On a même une structure plus riche sur $NC(n)$ qui nous servira par la suite :

Définition 6 (Treillis). *On appelle* treillis *un poset $(X, \leqslant)$ tel que pour tout $(x,y) \in X^2$, les éléments suivants sont bien définis :*
(i) $x \vee y := \min\{z \in X \mid z \geqslant x,\ z \geqslant y\}$ (jointure de x et y)
(ii) $x \wedge y := \max\{z \in X \mid z \leqslant x,\ z \leqslant y\}$ (rencontre [ii] de x et y)

Exemple : $\mathbb{Z}$ muni de la relation de divisibilité est un treillis, en considérant le pgcd et le ppcm de deux éléments.

Proposition 3. *Soit $(X, \leqslant)$ un poset fini admettant un élément maximal 1_X. Si tout couple $(x,y) \in X^2$ admet une rencontre, alors X est un treillis.*

Démonstration. Soit $(x,y) \in X^2$. on considère l'ensemble $M := \{z \in X \mid z \geqslant x,\ z \geqslant y\}$. Cet ensemble est non-vide, car il contient 1_X. On pose alors $z_0 = \bigwedge_{z \in M} z$, qui existe par hypothèse. Or clairement, $x \leqslant z_0$ et $y \leqslant z_0$. Donc z_0 minore M : il s'agit de $x \vee y$. □

Proposition 4. *$NC(n)$ a une structure de treillis pour l'ordre de la définition 5.*

(ii). La traduction des termes anglais «join» et «meet» est peut-être un peu malheureuse.

Démonstration. $NC(n)$ admet un élément maximal, que nous noterons 1_n, correspondant à la partition composée d'un seul bloc. Ainsi, il suffit d'utiliser la propriété précédante et de montrer que tout couple de $NC(n)$ admet une rencontre. Si π et σ sont deux partitions de $NC(n)$, il est aisé de montrer que la partition dont les blocs sont exactement les éléments non-vides de $\{B_\pi \cap B_\sigma, B_\pi \in \pi, B_\sigma \in \sigma\}$ est la rencontre de π et σ. □

L'expression explicite de la jointure de deux partitions non-croisées n'est pas évidente à écrire, ni même à visualiser hors de cas particuliers. Toutefois, on pourra très souvent se contenter d'utiliser le lemme suivant dans nos calculs :

Lemme 1. *Soit $(\pi, \sigma) \in NC(n)^2$ tel que :*

$$\pi \vee \sigma = 1_n, \tag{14}$$

où 1_n est la partition composée d'un unique bloc. Alors :

$$\forall k \in [\![n-1]\!],\ k \sim_\pi k+1 \text{ ou } k \sim_\sigma k+1 \tag{15}$$

Démonstration. Par l'absurde, s'il existe $k \in [\![n]\!]$ tel que k et $k+1$ ne sont appariés ni par σ ni par π, alors clairement, la partition $\{\{1, \dots k\}, \{k+1, \dots n\}\}$ majore π et σ. Donc $\pi \vee \sigma \neq 1_n$. □

La structure de treillis de $NC(n)$ va nous permettre de définir une fonction pratique, dont nous nous servirons pour la démonstration de notre résultat principal, appelé *dual de* Kreweras :

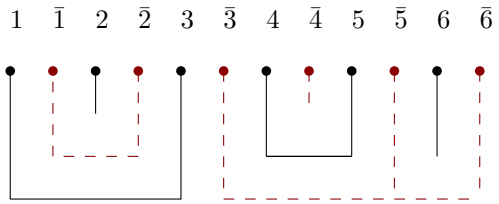
Définition 7 (Dual de Kreweras). *Soit $n \in \mathbb{N}^*$. On considère des éléments formels $\bar{1}, \dots, \bar{n}$ pour lesquels on impose l'ordre :*

$$1 < \bar{1} < 2 < \cdots < n < \bar{n}. \tag{16}$$

Pour $\pi \in NC(n)$, on définit :

$$\mathcal{K}(\pi) := \max\{\sigma \in NC(\bar{n}) \mid \pi \sqcup \sigma \in NC(\{1, \bar{1} \dots n, \bar{n}\})\} \tag{17}$$

Cette définition un peu indigeste se traduit pourtant fort bien graphiquement. Observons plutôt :



En noir, on a représenté la partition $\{\{1, 3\}, \{2\}, \{4, 5\}, \{6\}\}$ et en rouge son dual de Kreweras.

On donne une autre caractérisation équivalente du dual de Kreweras :

Proposition 5. *Soit $n \in \mathbb{N}^*$. Soit $\pi \in NC(n)$. Alors $\mathcal{K}(\pi)$ est l'unique partition de $NC(\{\bar{1}, \dots, \bar{n}\})$ telle que :*

$$(\pi \sqcup \mathcal{K}(\pi)) \vee \{\{1, \bar{1}\}, \{2, \bar{2}\}, \dots \{n, \bar{n}\}\} = \{1, \bar{1}, \dots n, \bar{n}\} \tag{18}$$

1.3 Inversion de Möbius

Considérons X un poset fini. L'objectif de cette section est d'établir les outils d'inversion de Möbius permettant, étant données deux fonctions f et g de X dans $\mathbb{C}$ liées par la relation :

$$\forall x \in X,\ f(x) = \sum_{\substack{y \in X \\ y \leqslant x}} g(y) \tag{19}$$

d'exprimer les valeurs de g à partir de celles de f.

On notera $X^{(2)} := \{(x, y) \in X^2 \mid x \leqslant y\}$.

Définition 8 (Convolution). *Soient $F : X^{(2)} \to \mathbb{C}$ et $g : X \to \mathbb{C}$. On appelle* convolution *de F et de g l'unique fonction de X dans $\mathbb{C}$ définie par :*

$$\forall x \in X,\ (g * F)(x) := \sum_{\substack{y \in X \\ y \leqslant x}} g(y) F(y, x) \tag{20}$$

La convolution dans les posets finis admet une représentation matricielle avec laquelle il est commode de travailler. Notons n le cardinal de X. Grâce à la remarque faite sous la définition 2, on se donne une énumération $X = \{x_1, \dots x_2\}$ de telle sorte que deux éléments x_i et x_j soient tels que $x_i \leqslant x_j$ ou bien incomparables lorsque $i \leqslant j$. Soit $F : X^{(2)} \to \mathbb{C}$ et $g : X \to \mathbb{C}$. On pose alors $M_F = (m_{ij})_{1 \leqslant i,j \leqslant n} \in \mathcal{M}_n(\mathbb{C})$ définie par :

$$m_{ij} = \begin{cases} F(x_i, x_j) \text{ si } x_i \leqslant x_j \\ 0 \text{ sinon.} \end{cases} \tag{21}$$

Pareillement, posons $V_g := (g(x_i))_{1 \leqslant i \leqslant n} \in \mathbb{C}^n$. Alors :

$$V_{g*F} = M_F V_g \tag{22}$$

Lemme 2. *Soit $F : X^{(2)} \to \mathbb{C}$. F admet un inverse au sens de la convolution si, et seulement si, M_F est inversible. Dans ce cas, $(M_F)^{-1} = M_{F^{-1}}$.*

Démonstration. Le sens direct ne pose pas de soucis : si F est inversible, alors :

$$\forall g : X \to \mathbb{C},\ \forall x \in X,\ ((g * F^{-1}) * F(x) = g(x) \tag{23}$$

i.e.

$$\forall v \in \mathbb{C}^n,\ M_{F^{-1}} M_F v = v \tag{24}$$

D'où $M_{F^{-1}} = (M_F)^{-1}$.

Pour le sens indirect, on peut remarquer que $\mathcal{M} := \{M \in \mathcal{M}_n(\mathbb{C}) \mid \exists G : X^{(2)} \to \mathbb{C} \ : \ M = M_G\}$ est un ensemble de matrices triangulaires stable par multiplication, addition et multiplication par un scalaire, qui de plus contient toutes les matrices diagonales. Ainsi, si $T \in \mathcal{M}$ est inversible, on note $T = D - N$ où D est la diagonale extraite de T, nécessairement inversible. N est nilpotente, en conséquence de quoi :

$$\begin{aligned} T^{-1} &= [D(I_n - D^{-1}N)]^{-1} \\ &= (I_n - D^{-1}N)^{-1}D^{-1} \\ &= D^{-1}\sum_{k=0}^{n-1}(D^{-1}N)^k \in \mathcal{M} \end{aligned}$$

Ainsi, en supposant M_F inversible, on a l'existence de $G : X^{(2)}(X) \to \mathbb{C}$ telle que $(M_F)^{-1} = M_G$. Il est alors aisé de montrer que $G = F^{-1}$. □

Une conséquence immédiate de ce résultat est l'existence de la *fonction de* Möbius dans n'importe quel poset fini :

Théorème 2 (Fonction de Möbius). *Soit X un poset fini. On note $\zeta : X^{(2)} \to \mathbb{C}$ la fonction constante égale à 1. Alors, ζ est inversible et on appelle* fonction de Möbius *son inverse, noté μ_X.*

Remarque : Il est possible, dans le cas où $X = NC(n)$, de calculer explicitement les valeurs de la fonction de Möbius à partir de la seule connaissance des quantités $\mu_p(0_p, 1_p)$ pour tout $p \in \mathbb{N}^*$, où μ_p est la fonction de Möbius de $NC(p)$. Encore une fois, les nombres de Catalan interviennent dans ces expressions : on peut montrer que $\mu_p(0_p, 1_p) = (-1)^{p-1}C_{p-1}$. Voir [7] pour le détail de la preuve.

Corollaire 1 (Inversion de Möbius). *Soit X un poset fini. Soient f et g deux fonctions de X dans $\mathbb{C}$. Alors, les assertions suivantes sont équivalentes :*

(i)

$$\forall x \in X,\ f(x) = \sum_{\substack{y \in X \\ y \leqslant x}} g(x) \tag{25}$$

(ii)

$$\forall x \in X,\ g(x) = \sum_{\substack{y \in X \\ y \leqslant x}} f(y)\mu_X(y, x) \tag{26}$$

On dispose par ailleurs d'une généralisation de l'inversion de Möbius, reposant sur la structure de treillis, dont nous nous servirons quelques fois par la suite :

Théorème 3 (Inversion partielle de Möbius). *Soit X un treillis fini. Soient f et g deux fonctions de X dans $\mathbb{C}$ liées par la relation (19). Soit $(x, y) \in X^2$ tel que $x \leqslant y$. Alors :*

$$\sum_{\substack{z \in X \\ x \leqslant z \leqslant y}} f(z)\mu_X(z, y) = \sum_{\substack{z \in X \\ z \vee x = y}} g(z) \tag{27}$$

Démonstration (esquisse). En partant du terme de gauche et en exploitant la formule (19), on obtient :

$$\sum_{\substack{z \in X \\ x \leqslant z \leqslant y}} f(z)\mu(z, y) = \sum_{\substack{z' \in X \\ z' \leqslant y}} \sum_{\substack{z \in X \\ z' \vee x \leqslant z \leqslant y}} \mu(z, y)g(z'). \tag{28}$$

Une discussion sur le calcul effectif de la fonction de Möbius permet ensuite de conclure. Voir [7] pour une démonstration complète. □

On peut remarquer que la fonction de Möbius ne dépend que du poset considéré. En conséquence de quoi, la proposition suivante semble tout à fait naturelle :

Proposition 6. *Soient X et Y deux posets finis, et soit $\Phi : X \leftrightarrow Y$ un isomorphisme de poset (i.e. une bijection préservant l'ordre partiel). Alors :*

$$\forall (x, y) \in X^2,\ \mu_X(x, y) = \mu_Y(\Phi(x), \Phi(y)) \tag{29}$$

Démonstration. Cela se voit très bien en considérant l'écriture matricielle de la convolution. Si $x_1, \dots x_n$ fournit une énumération de X telle que $i \leqslant j \implies x_i \leqslant x_j$ ou x_i et x_j sont incomparables, alors $\Phi(x_1), \dots, \Phi(x_n)$ est une énumération de Y obéissant à la même propriété. Il suffit alors de remarquer que les matrices de μ_X et μ_Y sont identiques (et égales à l'inverse de M_ζ). □

2 Probabilités libres

Force est de constater que la théorie des probabilités repose fortement sur la notion d'espérance et d'indépendance. Or, la manipulation des formules élémentaires relatives à l'indépendance des variables aléatoires s'appuie fortement sur le caractère commutatif des algèbres auxquelles celles-ci appartiennent. En effet, imaginons disposer de deux variables aléatoires X et Y indépendantes à valeurs dans une certaine algèbre non-commutative, telles que $XY \neq YX$ (par exemple X et Y pourraient être des matrices aléatoires), et supposons qu'on désire calculer l'espérance d'un produit $X^i Y^j X^k, (i, j, k) \in \mathbb{N}^3$. Pour retrouver le comportement agréable de l'indépendance avec le calcul d'espérance, tout en s'adaptant au cadre non-commutatif, une idée immédiate serait d'essayer d'obtenir :

$$\mathbb{E}[X^i Y^j X^k] = \mathbb{E}[X^i]\mathbb{E}[Y^j]\mathbb{E}[X^k]. \tag{30}$$

Or une telle propriété ne pourrait pas toujours être vraie, ce que l'on aperçoit en prenant par exemple $j = 0$. Pour cette raison, on va chercher à élaborer une autre théorie des probabilités, appelée théorie des «probabilités libres», bien adaptée au cadre non-commutatif. Cette seconde section vise à présenter les concepts et les résultats essentiels de la théorie des probabilités libres, que l'on appliquera plus tard à des propriétés portant sur les matrices aléatoires.

2.1 Espace de probabilité non-commutatif

Tout comme en probabilités classiques, il nous faut une structure de base, analogue aux espaces probabilisés, sur laquelle construire les probabilités libres. Notre «espace de probabilité non-commutatif» ne reposera pas sur les outils de la théorie de la mesure, mais sur des considérations beaucoup plus algébriques, comme nous allons le voir dans cette section.

Définition 9 (Espace de probabilité non-commutatif). *On appelle* espace de probabilité non commutatif *un couple* $(\mathcal{A}, \varphi)$ *telle que :*
(i) $\mathcal{A}$ *est une* $\mathbb{C}$*-algèbre*[iii].
(ii) $\varphi : \mathcal{A} \to \mathbb{C}$ *est une forme linéaire unitaire, c'est-à-dire que* $\varphi(1_{\mathcal{A}}) = 1$
La fonctionnelle φ *est appelée* espérance non-commutative *et les éléments de* $\mathcal{A}$ *sont appelés* variables aléatoires non-commutatives.
Lorsque :

$$\forall (a, b) \in \mathcal{A}^2,\ \varphi(ab) = \varphi(ba), \tag{31}$$

on dira que φ *est une* trace *et que l'espace de probabilité est* tracial.

Lorsque le contexte est clair, on évitera de préciser «non-commutatif» pour qualifier nos objets. On parlera alors simplement d'espace de probabilité, d'espérance et de variables aléatoires.

On utilisera souvent un vocabulaire analogue à celui employé en probabilités classiques, notamment :

Définition 10 (Elément centré, variance). *Soit* a *un élément d'un espace de probabilité* $(\mathcal{A}, \varphi)$*. On dit que* a *est* centré *si, et seulement si,* $\varphi(a) = 0$*. Par ailleurs on notera souvent :*

$$a^\circ := a - \varphi(a) 1_{\mathcal{A}}$$

l'opération qui consiste à centrer a*.*
On appelle variance de a *la quantité* $\varphi((a^\circ)^2)$*.*

Comme on travaille sur des $\mathbb{C}$-algèbres, il peut être intéressant d'introduire une opération interne qui étende la notion de conjugaison, et à l'égard de laquelle la fonctionnelle φ se comporte bien. Pour nous qui travaillerons sur des matrices aléatoires, cette opération sera tout simplement l'adjonction, mais nous allons étendre cette notion à un cadre plus général.

Définition 11 ($*$-algèbre). *On appelle* $*$-algèbre *un couple* $(\mathcal{A}, *)$ *tel que :*
(i) $\mathcal{A}$ *est une* $\mathbb{C}$*-algèbre (unifère).*
(ii) $* : \mathcal{A} \to \mathcal{A}$ *est une involution antilinéaire telle que :*

$$\forall (a, b) \in \mathcal{A}^2, (ab)^* = b^* a^*. \tag{32}$$

*(Propriété que nous dirons de «*contre-invariance*»)*

Comme escompté, $\mathcal{M}_n(\mathbb{C})$ muni de l'adjonction est une $*$-algèbre. On étendra naturellement un certain nombre de notions propres aux matrices au cadre des $*$-algèbres :

(iii). On rappelle que toutes les algèbres sont considérées sur le corps $\mathbb{C}$, et toutes seront supposées unifères. Pour $\mathcal{A}$ une algèbre, on notera $1_{\mathcal{A}}$ son unité.

Soit $(\mathcal{A}, *)$ une $*$-algèbre et soit $a \in \mathcal{A}$.
— On dit que a est *normal* si, et seulement si, $aa^* = a^*a$.
— On dit que a est *auto-adjoint* si, et seulement si, $a = a^*$.
— On dit que a est *unitaire* si, et seulement si, a est inversible et $a^{-1} = a^*$.

Définition 12 ($*$-espace de probabilité). *Un $*$-espace de probabilité est un espace de probabilité non-commutatif $(\mathcal{A}, \varphi)$ tel que :*
(i) $\mathcal{A}$ est une $*$-algèbre.
(ii) φ est positive, c'est-à-dire :

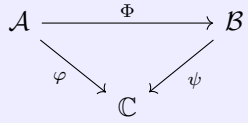
$$\forall a \in \mathcal{A},\ \varphi(a^*a) \in \mathbb{R}_+ \tag{33}$$

Exemples : Donnons ici quelques exemmples d'espaces de probabilités non-commutatifs :
— $L^{\infty}(\Omega, \mathfrak{F}, \mathbb{P})$ muni de l'espérance usuelle est un espace de probabilité non-commutatif tracial (la multiplication d'algèbre étant la multiplication ponctuelle). Muni de la conjugaison complexe, c'est un $*$-espace de probabilité.
— L'exemple peut être étendu aux variables aléatoires classiques admettant tous leurs moments, noté $L^{\infty-}(\Omega, \mathfrak{F}, \mathbb{P}) := \bigcup_{p \in \mathbb{N}^*} L^p(\Omega, \mathfrak{F}, \mathbb{P})$
— L'exemple qui nous intéressera pour notre étude des matrices aléatoires est le suivant :

$$(\mathcal{M}_n(L^{\infty-}(\Omega, \mathfrak{F}, \mathbb{P}), \varphi),\ \varphi : A \mapsto \frac{1}{n}\mathbb{E}[\mathrm{Tr}(A)], \tag{34}$$

c'est-à-dire l'ensembles des matrices dont les coefficients sont des variables aléatoires classiques admettant des moments à tout ordre. L'espérance non-commutative de cet espace est l'espérance de la trace normalisée.

Définition 13 (Morphisme d'espaces de probabilité). *Soient $(\mathcal{A}, \varphi)$ et $(\mathcal{B}, \psi)$ deux espaces de probabilité non-commutatifs. Un* morphisme d'espaces de probabilité *est un morphisme d'algèbres $\Phi : \mathcal{A} \to \mathcal{B}$ tel que $\psi \circ \Phi = \varphi$ i.e. le diagramme suivant commute :*



Faisons dès à-présent une remarque essentielle : les probabilités libres *ne sont pas* une généralisation des probabilités classiques. En effet, nos ensembles de variables aléatoires non-commutatives sont des algèbres, ce qui implique en particulier qu'ils sont stables par évaluation en des polynômes. Or, considérons $(\mathcal{A}, \varphi) := (L^1(\Omega, \mathfrak{F}, \mathbb{P}) \setminus L^2(\Omega, \mathfrak{F}, \mathbb{P}), \mathbb{E})$. Alors clairement, cet ensemble n'est pas stable par passage au carré, et plus généralement par évaluation en des polynômes.

Ceci implique en particulier que les variables aléatoires non-commutatives sont toujours supposées admettre tous leurs moments (notion qu'on introduira formellement plus tard). Encore plus contraignant : on verra dans une section ultérieure que la loi d'une variable aléatoire non-

commutative est toujours caractérisée par ses moments, ce qui n'est pas du tout le cas en probabilités classiques ! [(iv)]

Voyons quelques propriétés élémentaires des espaces de probabilité non-commutatif :

Proposition 7. *Soit $(\mathcal{A}, \varphi)$ un $*$-espace de probabilité. Alors :*

$$\forall a \in \mathcal{A},\ \varphi(a^*) = \overline{\varphi(a)}$$

Démonstration. Montrons qu'il existe un unique couple $(x, y) \in \mathcal{A}^2$ d'éléments auto-adjoints tels que $a = x + iy$. Il suffit pour cela de poser :

$$x := \frac{1}{2}(a + a^*),\ y := \frac{1}{2}(a - a^*). \tag{35}$$

Alors :

$$\varphi(a^*) = \varphi((x + iy)^*) = \varphi(x - iy) = \varphi(x) - i\varphi(y).$$

Or, si $z \in \mathcal{A}$ est auto-adjoint, on peut poser :

$$\alpha := \frac{z + 1_{\mathcal{A}}}{2},\ \beta := \frac{z - 1_{\mathcal{A}}}{2} \tag{36}$$

et on obtiens $z = \alpha^*\alpha - \beta^*\beta$. Par positivité de φ, $\varphi(z) \in \mathbb{R}$ et $\varphi(a^*) = \overline{\varphi(a)}$. □

Proposition 8 (Inégalité de Cauchy-Schwarz). *Soit $(\mathcal{A}, \varphi)$ une $*$-algèbre. Par positivité de φ :*

$$\forall (a, b) \in \mathcal{A}^2,\ |\varphi(ab)| \leqslant \sqrt{\varphi(a^*a)\varphi(b^*b)}$$

Démonstration. La démonstration est rigoureusement identique à celle faite pour les produits hermitiens dans le cadre des espaces préhilbertiens. □

On s'intéressera assez souvent aux algèbres et $*$-algèbres engendrées par des éléments. Nous introduisons donc cette notion dès maintenant :

Définition 14 (Algèbre engendrée par une partie). *Soit $\mathcal{A}$ une algèbre (resp. une $*$-algèbre). Soit $S \subset \mathcal{A}$. On appelle* algèbre engendrée par *S (resp. $*$-algèbre) la plus petite sous-algèbre de $\mathcal{A}$ contenant S (resp. sous-$*$-algèbre). On la notera* $\mathrm{Alg}(S)$ *(resp.* $\mathrm{Alg}^*(S)$*).*

Il sera souvent utile dans nos démonstrations d'avoir une caractérisation en extension de ces objets. Il se trouve justement qu'une caractérisation plutôt simple existe, reposant sur la notion de *polynômes non-commutatifs*, que nous définissons ainsi :

(iv). Nous faisons en réalité plusieurs approximations commodes pour une approche plus facile de la théorie. Il est possible de construire une théorie des probabilités libres parfaitement analogue à la théorie des probabilités classiques, mais cela repose abondamment sur la notion d'algèbre de von Neumann, que nous n'évoquerons pas dans ce rapport.

Définition 15 (Monôme non-commutatif). *Soit I un ensemble d'indices et $(X_i)_{i\in I}$ une famille d'indéterminées. On appelle* monôme non-commutatif en les variables $(X_i)_{i\in I}$ *un mot sur l'alphabet $(X_i)_{i\in I}$, c'est-à-dire une séquence finie de longueur arbitraire $(X_{i_1}, \ldots, X_{i_n})$ à valeurs dans $(X_i)_{i\in I}$, qu'on notera de façon plus compacte $X_{i(1)} \ldots X_{i(n)}$. On y ajoute la règle de simplification suivante :*

$$\forall i \in I,\ \forall (k,l) \in \mathbb{N}^2,\ X_i^k X_i^l = X_I^{k+l}. \tag{37}$$

L'ensemble des monômes non-commutatifs en les $(X_i)_{i\in I}$ muni de la concaténation, de la règle de simplification (37), ainsi que d'un élément neutre formel noté 1 forme un monoïde. Ce monoïde s'étend en une algèbre de polynômes dont les indéterminées sont les monômes non-commutatifs, et où le produit entre monômes s'effectue par concaténation et simplification. On prend pour cela la convention naturelle :

$$\forall z \in \mathbb{C},\ z \cdot 1 = z. \tag{38}$$

Définition 16 (Polynôme non-commutatif). *On appelle* polynôme non-commutatif en les variables $(X_i)_{i\in I}$ *un élément de l'anneau de polynôme dont les indéterminées sont les monômes commutatifs en les (X_i), c'est-à-dire une combinaison formelle :*

$$\sum_{i=1}^{n} \alpha_i M^i, \tag{39}$$

où les M_i sont des monômes non-commutatifs.

On note $\mathbb{C}\langle X_i \mid i \in I\rangle$ l'ensemble des polynômes non-commutatifs en les indéterminées $(X_i)_{i\in I}$, à bien différencier de $\mathbb{C}[X_i \mid i \in I]$ qui est l'anneau des polynômes commutatifs en les $(X_i)_{i\in I}$.

Comme on se servira assez souvent de l'opération $*$ des $*$-espaces de probabilité, on introduit le concept de $*$-polynôme :

Définition 17 ($*$-polynôme). *Soit I un ensemble d'indices et soit $(X_i)_{i\in I}$ une famille d'indéterminées. On appelle* $*$-polynôme en les variables $(X_i)_{i\in I}$ *les éléments de l'ensemble $\mathbb{C}\langle X_i, X_i^* \mid I\rangle$, où les $(X_i^*)_{i\in I}$ sont des indéterminées différentes des $(X_i)_{i\in I}$.*

On définit sans difficulté une notion d'évaluation :

Proposition 9. *Soit I un ensemble d'indices. Soit $(X_i)_{i\in I}$ un ensemble d'indéterminées. Soit $\mathcal{A}$ une $\mathbb{C}$-algèbre. Alors, pour toute famille $a = (a_i)_{i\in I} \in \mathcal{A}^I$:*

(i) il existe un unique morphisme d'algèbres $ev_a : \mathbb{C}\langle X_i \mid i \in I\rangle \to \mathbb{C}$ tel que :

$$\forall i \in I,\ ev_a(X_i) = a_i.$$

(ii) Si de plus $\mathcal{A}$ est une $*$-algèbres, on dispose d'un unique morphisme d'algèbre ev_a : $\mathbb{C}\langle X_i, X_i^* \mid i \in I\rangle \to \mathbb{C}$ tel que :

$$\forall i \in I,\ ev_a(X_i) = a_i,\ ev(X_i^*) = a_i^*.$$

Ainsi, si P est un polynôme non-commutatif (ou un $*$-polynôme) en les indéterminées (X_i), on notera plus simplement $P(a) := ev_a(P)$.

Ceci permet l'écriture en extension des sous-algèbres engendrées par des éléments :

Proposition 10. *Soit $\mathcal{A}$ une algèbre. Soit $S = (a_i)_{i\in I} \subset \mathcal{A}$. Alors :*

$$\mathrm{Alg}(S) = \{P(S), P \in \mathbb{C}\langle X_i \mid i \in I\rangle\} = \mathrm{Vect}\{M(S), M \text{ un monôme non-commutatif}\}$$

Si $\mathcal{A}$ est une $*$-algèbre, il suffit de prendre les $*$-polynômes pour engendrer une sous-$*$-algèbre.

Démonstration. Dans un premier temps, on ne considère pas l'opération $*$. En utilisant la caractérisation rapide des sous-algèbres, on voit clairement que l'ensemble calculé est une sous-algèbre de $\mathcal{A}$ contenant S. Par ailleurs, si $\mathcal{B} \subset \mathcal{A}$ est une sous-algèbre de $\mathcal{A}$ contenant S, alors $\mathcal{B}$ est stable par polynômes non-commutatifs. En particulier, $\mathcal{B}$ contient tous les polynômes non-commutatifs en des éléments de S. Donc $\{P(S), P \in \mathbb{C}\langle X_i \mid i \in I\rangle\} \subset \mathcal{B}$. Ceci est à dire qu'il s'agit bien de $\mathrm{Alg}(S)$.

Si on se place maintenant dans le contexte d'une $*$-algèbre, on munit l'ensemble des $*$-polynômes d'une $*$ en imposant que pour tout $i \in I$, $(x_i)^* = X_i^*$, et en généralisant à tout polynôme par linéarité et contre-invariance. On peut alors remarquer que l'ensemble $\{P(S),\ P \in \mathbb{C}\langle X_i, X_i^* \mid i \in I\}$ est une sous-algèbre de $\mathcal{A}$ stable par $*$: c'est une sous-$*$-algèbre. On montre encore une fois que c'est la plus petite sous-$*$-algèbre de $\mathcal{A}$ contenant S, ce qui conclut la preuve. □

2.2 Loi et moments non-commutatifs

Tout comme en probabilités classiques, on souhaite définir une notion de loi pour les variables aléatoires non-commutatives. Nous choisissons ici une approche par les moments : dans celle-ci, la notion de loi repose beaucoup plus fortement sur la notion de moment que son homonyme classique. Par ailleurs il existe deux notions distinctes de loi en probabilités libres.

On peut définir correctement la notion de moment au-travers du prisme des polynômes non-commutatifs et des $*$-polynômes :

Définition 18 (Moments, $*$-moments). *Soit $(\mathcal{A}, \varphi)$ un espace de probabilité non-commutatif et $a \in \mathcal{A}$. On appelle* moments de a *la famille $(\varphi(a^n))_{n\in\mathbb{N}}$. Si $\mathcal{A}$ est une $*$-algèbre, on appellera* $*$-moments *de a la famille $\varphi(M(a))$, où M parcours l'ensemble des $*$-monômes.*

Remarquons que si a n'est pas un élément normal, il est indispensable à l'étude des moments d'utiliser des monômes non-commutatif, même dans le cas où φ est une trace. En effet, en général, $\varphi(aa^*aa^*) \neq \varphi(a^2(a^*)^2$.

On souhaite également faire remarquer qu'en probabilités classiques, les lois sont loin d'être toutes caractérisées par leurs moments, et qu'imposer une telle chose en probabilités libres peut sembler extrêmement contraignant. Toutefois, même en ne s'intéressant qu'à de telles lois en probabilités classiques, on conserve nombre des objets les plus intéressants, tels que la loi normale.

On a déjà évoqué plus haut la place centrale des moments en probabilités non-commutatives. On va voir désormais qu'ils définissent même la notion de loi :

Définition 19 ($*$-distribution analytique). *Soit $(\mathcal{A}, \varphi)$ un $*$-espace de probabilité. Soit $a \in \mathcal{A}$ une variable aléatoire normale. On dit que a admet une* $*$-distribution au sens analytique *s'il existe une mesure de probabilité μ à support compact sur $\mathbb{C}$ telle que :*

$$\forall (n,m) \in \mathbb{N}^2,\ \varphi((a^*)^m a^n) = \int_{\mathbb{C}} z^n \bar{z}^m \,\mathrm{d}\mu(z)$$

Proposition 11. *Si $a \in \mathcal{A}$ est une variable aléatoire normale admettant une distribution analytique μ, alors μ est uniquement déterminée.*

Démonstration. Supposons ν et μ deux distributions analytiques de a. Soit $f \in C_b^0$. Soit $\varepsilon > 0$. D'après le théorème de Stone-Weierstraß, il existe $P \in \mathbb{C}[X]$ tel que $||f - P||_\infty \leqslant \varepsilon$, où la norme infinie est prise sur l'union des supports (compacts réels) de μ et ν. Alors :

$$\begin{aligned}\left|\int_{\mathbb{C}} f(z)\,\mathrm{d}(\mu-\nu)(z)\right| &\leqslant \left|\int_{\mathbb{C}} (f-P)(z)\,\mathrm{d}(\mu-\nu)(z)\right| + \left|\int_{\mathbb{C}} P(z)\,\mathrm{d}(\mu-\nu)(z)\right| \\ &\leqslant 2\varepsilon + 0,\end{aligned}$$

car μ et ν étant deux distributions analytiques de a, les intégrales contre μ et ν coïncident sur les $*$-polynômes. D'où $\mu = \nu$. □

Cette définition, quoi que très proche de la définition usuelle de loi de probabilité, n'est pas très satsfaisante, puisqu'on doit se limiter au cas précis des variables normales. Notre but étant d'étudier des variables aléatoires non-commutatives, ajouter des hypothèses de commutativité semble assez peu indiqué. De plus, l'existence d'une telle loi n'est même pas assurée pour des éléments normaux quelconques ! Il existe une autre définition de loi non-commutative, purement algébrique, qui sera celle que nous étudierons en majorité :

Définition 20 ($*$-distribution algébrique). *Soit $(\mathcal{A}, \varphi)$ un $*$-espace de probabilité. Soit $a \in \mathcal{A}$. On appelle* $*$-distribution algébrique *de a l'unique application linéaire :*

$$\begin{aligned} \mu : \mathbb{C}\langle X_i, X_i^* \mid i \in I\rangle &\to \mathbb{C} \\ P &\mapsto \varphi(P(a)) \end{aligned}$$

Remarque : Cette définition algébrique peut sembler étonnante à première vu, mais elle est peut-être plus naturelle qu'elle n'y paraît. En effet, considérons une variable aléatoire classique X de loi de probabilité $\mathbb{P}_X$. On peut alors voir de façon équivalente la mesure de probabilité $\mathbb{P}_X$ comme une application linéaire :

$$\begin{aligned} \mathbb{P}_X : C_b^0 &\to \mathbb{C} \\ f &\mapsto \int_{\mathbb{C}} f(z)\, \mathrm{d}\mathbb{P}_X(z) \end{aligned}$$

Cette formulation intégrale n'est rien d'autre que l'espérance de $f(X)$. Or, si on impose que la variable X admette tous ses moments, on peut également la considérer comme une variable aléatoire non commutative sur l'espace $(L^{\infty-}, \varphi)$ sur lequel l'espérance non-commutative φ coïncide avec l'espérance usuelle. Notre $*$-distribution algébrique est donc issu d'un procédé analogue, pour lequel on a simplement changé la classe de fonctions tests lors du calcul d'espérance (on a troqué C_b^0 pour $\mathbb{C}\langle X_i, X_i^* \mid i \in I\rangle$).

Sauf mention contraire, on parlera de loi algébrique dès qu'on discutera de la loi de variables aléatoires non-commutatives. Ceci fait sens puisque la loi analytique n'est pas toujours définie.

En probabilités classiques, la notion de loi jointe est importante pour étudier des familles de variables aléatoires. On dispose d'une notion analogue en probabilités libres, pour laquelle on retrouvera encore une fois l'idée centrale que nos $*$-polynômes nous servent de fonctions test.

Définition 21 ($*$-distribution jointe). *Soit $(\mathcal{A}, \varphi)$ un $*$-espace de probabilités. Soit $a = (a_i)_{i\in I} \in \mathcal{A}^I$ une famille de variables aléatoires. On appelle* $*$-distribution jointe des (a_i) *l'application linéaire :*

$$\begin{aligned} \mu_a : \mathbb{C}\langle X_i, X_i^* \mid i \in I\rangle &\to \mathbb{C} \\ P &\mapsto P(a) \end{aligned}$$

Remarque : On définit pareillement une notion de $*$-distribution *analytique* jointe.

Les $*$-distributions jointes sont impliquées dans un fort joli résultat d'isomorphisme que nous présenterons pour clore cette section :

Théorème 4. *Soient $(\mathcal{A}, \varphi)$ et $(\mathcal{B}, \psi)$ deux $*$-espaces de probabilités, et soient $(a_i)_{1\leqslant i\leqslant n}$ et $(b_i)_{1\leqslant i\leqslant n}$ deux familles de variables aléatoires respectivement dans $\mathcal{A}$ et $\mathcal{B}$, de $*$-distribution (algébrique) jointe μ et ν. Supposons :*
(i) $\mathcal{A} = \mathrm{Alg}^*(a_i \mid 1 \leqslant i \leqslant n)$
(ii) $\mathcal{B} = \mathrm{Alg}^*(b_i \mid 1 \leqslant i \leqslant n)$
(iii) $\mu = \nu$
Alors $(\mathcal{A}, \varphi) \cong (\mathcal{B}, \psi)$.

2.3 Libre indépendance

En probabilités classiques, la notion d'indépendance occupe une place centrale. Or celle-ci ne se transporte pas correctement au cas non-commutatif, comme on l'a vu dans l'exemple introductif (30). C'est pourquoi les probabilités libres introduisent une notion de libre indépendance que nous allons voir à-présent.

Définition 22 (Libre indépendance). *Soit $(\mathcal{A}, \varphi)$ un espace de probabilité, et soit $(\mathcal{A}_i)_{i\in I}$ une famille des sous-algèbres de $\mathcal{A}$. On dit que les $(\mathcal{A}_i)$ sont* librement indépendantes *(ou simplement indépendantes lorsque le contexte est clair) si, et seulement si, pour tout famille finie $(a_{i_j})_{1\leqslant j\leqslant n}$ respectant les conditions :*
(i) $\forall j \in [\![n]\!],\ a_{i_j} \in \mathcal{A}_{i_j}$,
(ii) $\forall j \in [\![n-1]\!],\ i_j \neq i_{j+1}$ *(le multi-indice $(i_1, \dots i_n)$ est* alterné*),*
(iii) $\forall j \in [\![n]\!],\ \varphi(a_{i_j}) = 0$,
on ait l'égalité :

$$\varphi\left(\prod_{j=1}^{\overrightarrow{n}} a_{i_j}\right) = 0.$$

Ces formules se résument élégamment par «un produit alterné d'éléments centrés est centré ».

Cette définition peut sembler beaucoup plus lourde que celle d'indépendance usuelle. Toutefois, au cours de la Leçon n°5, [7] montre que celle-ci est loin d'être arbitraire . Nous verrons quant à nous dans la sous-section suivante portant sur le produit libre d'espaces de probabilité une décomposition canonique des espaces qui permettent de mieux cerner le fonctionnement des calculs portant sur des éléments indépendants.

La notion d'algèbre engendrée permet d'étendre la notion de libre indépendance au cas de familles de variables aléatoires :

Définition 23 (Familles librement indépendantes). *Soit $(\mathcal{A}, \varphi)$ un espace de probabilité. Soient $F_1, \dots F_n$ des familles de variables aléatoires de $\mathcal{A}$. On dit que ces familles sont librement indépendantes si, et seulement si, les familles d'algèbres* $\mathrm{Alg}(F_1), \dots \mathrm{Alg}(F_n)$ *sont librement indépendantes.*

Remarques :
— On étend aisément toutes ces défintions au cas de $*$-espaces de probabilité en remplaçant tous les moments par des $*$-moments. On parle alors de $*$-*liberté*.

— Lorsqu'il n'y a pas de risque de confusion avec la liberté au sens des familles de vecteurs, on se permettra de dire simplement «libre» plutôt que «librement indépendant ».

Cette définition d'indépendance libre fournit les résultats attendus d'une notion d'impédence. En probabilités classiques, on sait que la loi jointe de variables indépendantes est donnée par la loi produit. En particulier, la loi jointe est entièrement déterminée par les marginales. Ce résultat reste vrai en probabilités libres :

Théorème 5. *Soit $(\mathcal{A}, \varphi)$ un espace de probabilité non-commutatif. Soit $(a_i)_{1\leqslant i\leqslant n}$ une famille libre de variables aléatoires de $\mathcal{A}$. Alors la loi (algébrique) jointe de (a_i) est entièrement déterminée par la donnée des lois marginales.*

De façon équivalente, si $(\mathcal{B}_i)$ est une famille libre de sous-algèbres de $\mathcal{A}$ telle que $\mathcal{A} = \mathrm{Alg}(\mathcal{B}_i, i \in [\![n]\!])$, alors la donnée de $\varphi|_{\mathcal{B}_i}$ pour tout i détermine φ.

Démonstration. Soit $(\mathcal{B}_i)$ une famille de sous-algèbres libres telles que $\mathcal{A} = \mathrm{Alg}(\mathcal{B}_i,\ i \in I)$ On raisonne par récurrence sur l'ordre des moments calculés. Notons, pour $k \in \mathbb{N}^*$ la propriété :

$$\mathscr{P}(k) :\ \forall \boldsymbol{i} = (i_1, \dots i_n) \subset [\![n]\!] \text{ alterné}, \forall (a_1, \dots a_k) \subset \mathcal{A} \text{ tel que } \forall j \in [\![k]\!]\ a_j \in \mathcal{B}_{i_j}, \varphi\left(\overrightarrow{\prod_{j=1}^{k}} a_j\right)$$

s'exprime comme une fonction explicite de k et des $(\varphi|_{\mathcal{B}_i})$.

Pour $k = 1$, la propriété est tout à fait évidente. Supposons $k \in \mathbb{N}^*$ tel que $\mathscr{P}(l)$ vraie pour tout l plus petit que k, et soit $\boldsymbol{i}$ un multi-indice alterné de longueur $k+1$. Soit $(a_1, \dots a_{k+1}) \subset \mathcal{A}$ tel que $a_j \in \mathcal{B}_{i_j}$ pour tout j. Alors :

$$\varphi\left(\overrightarrow{\prod_{j=1}^{k+1}} a_j\right) = \varphi\left(\overrightarrow{\prod_{j=1}^{k+1}} (a_j^\circ + \varphi(a_j))\right) \tag{40}$$

$$= \varphi\left(\overrightarrow{\prod_{j=1}^{k+1}} a_j^\circ\right) + \sum_{\substack{\pi_1 \sqcup \pi_2 = [\![k+1]\!] \\ \pi_1 \neq \emptyset}} \left[\prod_{j\in\pi_1} \varphi(a_j) \varphi\left(\overrightarrow{\prod_{j\in\pi_2}} a_j^\circ\right)\right] \tag{41}$$

$$= 0 + \sum_{\substack{\pi_1 \sqcup \pi_2 = [\![k+1]\!] \\ \pi_1 \neq \emptyset}} \left[\prod_{j\in\pi_1} \varphi|_{\mathcal{B}_{i_j}}(a_j) \varphi\left(\overrightarrow{\prod_{j\in\pi_2}} a_j^\circ\right)\right] \tag{42}$$

où la somme est prise sur un ensemble de parties de $[\![k+1]\!]$. Le passage de la ligne (41) à la ligne (42) s'effectue en exploitant la libre indépendance et le fait que les (a_j) se trouvent dans les algèbres $(\mathcal{B}_i)$ de façon alternée. Comme π_1 est non vide, $|\pi_2| \leqslant k$. On peut donc appliquer $\mathscr{P}(k)$ au produit indicé par π_2 et on obtient exactement $\mathscr{P}(k+1)$.

□

On souhaite faire remarquer ceci : la libre indépendance est une notion très mal adaptée à l'étude de variables aléatoires commutatives, car elle impose des conditions très fortes dès que les variables commutent. En effet, si deux variables aléatoires a et b commutent et sont librement indépendantes, l'une d'entre elles au moins est de variance nulle. Ainsi, si X et Y sont des variables aléatoires classiques dans $L^{\infty-}$, elles sont librement indépendantes seulement si l'une d'entre elles est presque sûrement constante...

Nous donnons ici un petit lemme qui nous sera très utile par la suite :

Lemme 3. *Soit $(\mathcal{A}, \varphi)$ un espace de probabilité non-commutatif et soit $(\mathcal{A}_i)_{i\in I}$ une famille de sous-algèbres de $\mathcal{A}$. Soient $\boldsymbol{i} = (i_1, \dots i_k)$ et $\boldsymbol{j} = (j_1, \dots, j_l)$ deux multi-indices alternés. Soient $(a_{i_r})_{1\leqslant r\leqslant k}$ et $(b_{j_s})_{1\leqslant s\leqslant l}$ deux familles de variables aléatoires centrées telles que pour tout r et pour tout s, $a_{i_r} \in \mathcal{A}_{i_r},\ b_{j_s} \in \mathcal{A}_{j_s}$. Alors :*

$$\varphi(a_{i_1} \dots a_{i_k} b_{j_s} \dots b_{j_1}) = \begin{cases} \overrightarrow{\prod_{r=1}^{k}} \varphi(a_{i_r} b_{i_r}) \text{ si } \boldsymbol{i} = \boldsymbol{j} \\ 0 \text{ sinon.} \end{cases} \tag{43}$$

2.4 Produit libre et théorèmes d'existence

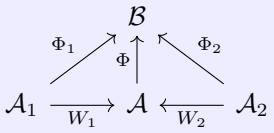
En probabilités classiques, on dispose d'un théorème fondamental qui assure, pour n'importe quelle famille de lois de probabilités $(\mu_i)_{i\in I}$, l'existence d'un espace probabilisé $(\Omega, \mathfrak{F}, \mathbb{P})$ et d'une famille de variables aléatoires $(X_i)_{i\in I}$ sur $(\Omega, \mathfrak{F}, \mathbb{P})$ telles que les (X_i) soient mutuellement indépendantes et que, pour $i \in I$, $X_i \hookrightarrow \mu_i$. Ce résultat repose entièrement sur le produit d'espaces probabilisés et l'existence de la mesure produit. Or en probabilités libres la notion de distribution s'exprime hors du contexte de la théorie de la mesure, et l'indépendance ne s'exprime pas en terme de mesures. Un théorème analogue n'a donc rien d'évident.

Nous allons dans cette section établir une construction dite de «produit libre d'algèbres» et montrer le théorème d'existence, de sorte qu'il nous sera toujours possible de prendre des familles de variables libres suivant des distributions données, pour peu qu'on se place sur le bon espace. Nous le verrons, ce formalisme nous permettra également de jeter un nouvel éclairage sur la définition 22 de libre indépendance, et nous permettra de manipuler plus aisément certains espaces de probabilité.

Toutefois, nous alertons le lecteur que les résultats de cette section ne nous serviront qu'une unique fois par la suite, lors de la démonstration du théorème 9. Nous pensons que son développement est intéressant pour la compréhension théorique des probabilités libres, mais le lecteur pourra se contenter de sauter cette section et d'admettre le théorème d'existence sans plus de conséquences.

Dans cette section, on désignera par K un corps quelconque dans un soucis de généralité.

Définition 24 (Produit libre d'algèbres). *Soient $\mathcal{A}_1, \mathcal{A}_2$ et $\mathcal{A}$ des algèbres sur un corps K. On dit que $\mathcal{A}$ est un* produit libre *des algèbres $\mathcal{A}_1$ et $\mathcal{A}_2$ si, et seulement si, il existe $W_1 : \mathcal{A}_1 \to \mathcal{A}$ et $W_2 : \mathcal{A}_2 \to \mathcal{A}$ des morphismes de K-algèbres tels que, pour toute K-algèbre $\mathcal{B}$ et toute paire de morphismes $(\Phi_1 : \mathcal{A}_1 \to \mathcal{B}, \Phi_2 : \mathcal{A}_2 \to \mathcal{B})$, il exite un unique morphisme $\Phi : \mathcal{A} \to \mathcal{B}$ tel que le diagramme suivant commute :*



c'est-à-dire $\Phi_1 = \Phi \circ W_1$, $\Phi_2 = \Phi \circ W_2$ (propriété universelle du produit libre d'algèbres). On dit alors que Φ est le produit libre *de Φ_1 et Φ_2.*

Remarque : Cette définition s'étend aisément au cas d'une famille quelconque d'algèbres $(\mathcal{A}_i)_{i\in I}$, où l'ensemble I est éventuellement infini et indénombrable.

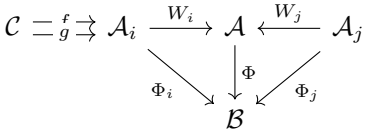
Avant de prouver notre théorème d'existence, étudions un peu le produit libre :

Lemme 4. *Soit $(\mathcal{A}_i)_{i\in I}$ une famille de K-algèbres et soit $\mathcal{A}$ un produit libre de $(\mathcal{A}_i)$. Soient $(W_i)_{i\in I}$ les morphismes associés comme dans la définition 24. Alors les W_i sont injectifs.*

Démonstration. Soit $i \in I$. Soit $\mathcal{C}$ une K-algèbre. On va raisonner uniquement sur la flèche W_i en montrant :

$$\forall f, g : \mathcal{C} \to \mathcal{A}_i,\ W_i \circ f = W_i \circ g \implies f = g.^{(v)} \tag{44}$$

Soient f et g deux telles flèches. Donnons-nous une K-algèbre $\mathcal{B}$ et uen famille de morphismes $W_j : \mathcal{A}_j \to \mathcal{B}$. Alors, par propriété universelle du produit libre, on dispose de $\Phi : \mathcal{A} \to \mathcal{B}$ telle que $\Phi \circ W_j = \Phi_j$ pour tout $j \in I$ (représenté par le diagramme commutatif ci-dessous).



Alors :

$$\begin{aligned} \Phi_i \circ f &= \Phi \circ W_i \circ f && (45)\\ &= \Phi \circ W_i \circ g && (46)\\ &= \Phi_i \circ g && (47) \end{aligned}$$

Comme c'est vrai pour tout morphisme Φ_i, on a bien $f = g$.

□

(v). Dans ce contexte, toutes les applications rencontrées sont des morphismes de K-algèbres, ce qu'on se sera permi de ne pas écrire à chaque flèche introduite.

Remarque : Il peut paraître étonnant de prouver l'injectivité d'un morphisme d'algèbres sans s'intéresser à son noyau. L'intérêt de cette démonstration, peut-être un peu alambiquée, et qu'elle n'utilise en fait à aucun moment la structure d'algèbre : elle se généralise à n'importe quelle autre structure dans laquelle on définirait un produit libre de façon analogue.

Grâce au lemme 4, on peut voir les $(\mathcal{A}_i)$ comme des sous-algèbres de $\mathcal{A}$, et donc se passer d'écrire les (W_i). On obtient une écriture allégée qu'il est plus agréable de manipuler.

Lemme 5. *Soit $(\mathcal{A}_i)_{i\in I}$ une famille de K-algèbres et soit $\mathcal{A}$ un produit libre des $(\mathcal{A}_i)$. Alors les morphismes (W_i) sont uniques et la propriété universelle du produit libre définit $\mathcal{A}$ uniquement à isomorphisme près.*

Démonstration. Supposons qu'on dispose de deux produits libres $\mathcal{A}$ et $\mathcal{A}'$, ainsi que des morphismes (W_i) et (W'_i) :

$$\begin{array}{ccccc} \mathcal{A}_1 & & & & \mathcal{A}_2 \\ {\scriptstyle W_1}\downarrow & \searrow & & \swarrow & \downarrow{\scriptstyle W'_2} \\ & {\scriptstyle W_2}\searrow & & \swarrow{\scriptstyle W'_1} & \\ \mathcal{A} & & & & \mathcal{A}' \end{array}$$

On considère alors, par propriété universelle du produit libre, des morphismes $W : \mathcal{A} \to \mathcal{A}'$ et $W' : \mathcal{A}' \to \mathcal{A}$ obtenus resepectivement à partir des (W_i) et des (W'_i) :

$$\begin{array}{ccccc} \mathcal{A}_1 & & & & \mathcal{A}_2 \\ {\scriptstyle W_1}\downarrow & \searrow & & \swarrow & \downarrow{\scriptstyle W'_2} \\ & {\scriptstyle W_2}\searrow & & \swarrow{\scriptstyle W'_1} & \\ \mathcal{A} & & \leftarrow W' - & & \mathcal{A}' \\ & & - W \rightarrow & & \end{array}$$

Pour $i \in I$, on remarque que :

$$\begin{aligned} W \circ (W' \circ W'_i) &= W \circ W_i && (48) \\ &= W'_i && (49) \end{aligned}$$

Ainsi $W \circ W'$ est l'unique morphisme de $\mathcal{A}'$ dans $\mathcal{A}'$ tel que $W \circ W' \circ W_i = W_i$ pour tout i. Comme l'identité satisfait aussi cette relation, on a bien que W et W' sont inverses l'un de l'autre. Donc $\mathcal{A}$ et $\mathcal{A}'$ sont isomorphes.

On déduit du même coup l'unicité des (W_i) en supposant donnée une autre famille satisfaisant la propriété universelle, et en poursuivant le même raisonnement. □

Ainsi, on dira désormais *le* produit libres de $(\mathcal{A}_i)$ plutôt qu'*un* produit libre, et on utilisera la notation :

$$\mathcal{A} \cong \underset{i\in I}{*} \mathcal{A}_i.$$

On en arrive enfin au résultat qui nous intéresse :

Théorème 6 (Existence du produit libre). *Soit I un ensemble d'indices, et soit $(\mathcal{A}_i)_{i\in I}$ une famille de K-algèbres. Alors il existe une K-algèbre $\mathcal{A}$, unique à isomorphisme près, qui soit produit libre des $(\mathcal{A}_i)$.*

Démonstration. La démonstration de ce résultat consiste à construire explicitement une telle algèbre. C'est cette construction explicite qui, on le verra, nous permettra de jeter un regard nouveau sur la libre indépendance, et de voir que les formules qui l'entourent, qui à première vue peuvent sembler compliquées, sont extrêmement liées à la structure du produit libre.

Quitte à prendre des copies disjointes des $(\mathcal{A}_i)$, on considère que toutes les $(\mathcal{A}_i)$ sont deux-à-deux distinctes.

Commençons par considérer un élément Ω d'un certain ensemble, quel qu'il soit. Cet élément Ω, qu'on appellera «l'état du vide», nous servira d'unité. On définit l'ensemble $K\cdot\Omega := \{\lambda\cdot\Omega, \lambda \in K\}$ de manière purement formelle.

Les éléments de l'algèbre libre peuvent être décrits à la manière de polynômes non-commutatifs en les éléments des $(\mathcal{A}_i)$, de telle sorte qu'il n'y ait pas de règles de simplification pour le produit d'éléments d'algèbres différentes. Ceci peut se formaliser de cette manière :

pour tout $i \in I$, on note $\varphi_i : \mathcal{A}_i \to K$ une forme linéaire unitaire sur $\mathcal{A}_i$. Posons $\mathcal{A}_i^\circ := \ker(\varphi_i)$. Soit $n \in \mathbb{N}^*$, et soit $\boldsymbol{i} = (i_1, \dots, i_n)$ un multi-indice alterné de taille n. On pose alors :

$$\mathcal{W}_{\boldsymbol{i}} := \bigotimes_{j=1}^{n} \mathcal{A}_{i_j}^\circ, \tag{50}$$

où $\mathcal{W}_{\boldsymbol{i}}$ est l'ensemble des mots de taille n tel que la j-ième lettre est prise dans l'alphabet $\mathcal{A}_i^\circ$. De tels ensembles suffisent entièrement à construire l'ensemble de tous les mots sur l'alphabet $\bigsqcup_{i\in I} \mathcal{A}_i$, puisqu'on peut utiliser les règles de calculs internes aux $(\mathcal{A}_i)$ pour réduire tout tel mot à un élément d'un certain $\mathcal{W}_{\boldsymbol{i}}$.

Un moyen d'obtenir l'ensemble de tous les mots alternés sur les $(\mathcal{A}_i)$ est d'utiliser des sommes directes formelles :

$$\bigoplus_{n=1}^{+\infty} \bigoplus_{\substack{\boldsymbol{i} \text{ alterné} \\ \text{de taille } n}} \mathcal{W}_{\boldsymbol{i}} \tag{51}$$

Il reste à rajouter une unité à cette algèbre, et la copie de K qui vient avec. C'est le rôle de l'état du vide : fournir une image unique de toutes les unités des $(\mathcal{A}_i)$. Finalement :

$$\mathcal{A} := K\cdot\Omega \oplus \bigoplus_{n=1}^{+\infty} \bigoplus_{\substack{\boldsymbol{i} \text{ alterné} \\ \text{de taille } n}} \mathcal{W}_{\boldsymbol{i}} \tag{52}$$

sera notre ensemble sous-jacent. Reste à équipper $\mathcal{A}$ des bonnes lois de composition.

L'addition se lit directement sur la structure de $\mathcal{A}$: si deux mots w_1 et w_2 appartiennent à deux ensembles élémentaires $\mathcal{W}_{\boldsymbol{i}}$ et $\mathcal{W}_{\boldsymbol{j}}$ avec $\boldsymbol{i} \neq \boldsymbol{j}$, alors $w_1 + w_2$ est définit par somme formelle comme élément de $\mathcal{W}_{\boldsymbol{i}} \oplus \mathcal{W}_{\boldsymbol{j}}$. Si par contre $\boldsymbol{i} = \boldsymbol{j}$, la somme est donnée par les règles de calcul dans le produit tensoriel.

La multiplication par un scalaire est claire par multilinéarité du produit tensoriel.

La multiplication quant à elle pose plus de problème. Pour la construire, on se servira de la formule donnée par le lemme 3. Soient $\boldsymbol{i} = (i_1, \dots i_n)$ et $\boldsymbol{j} = (j_1, \dots j_m)$. On raisonne par récurrence sur $n + m$. Notons $\mathscr{P}(p)$ la propriété « la multiplication d'algèbre est bien défini pour tout éléments $w_1 \in \mathcal{W}_{\boldsymbol{i}}$ et $w_2 \in \mathcal{W}_{\boldsymbol{j}}$ avec $n + m = p$. Pour $p = 1$, $\mathscr{P}(1)$ est claire avec la convention :

$$\bigotimes_{i\in\emptyset} \mathcal{A}_i = K\cdot\Omega \tag{53}$$

Donnons nous p tel que $\mathscr{P}(p)$ est vraie, et supposons $n+m=p+1$. Alors, si $i_n = j_1$, on pose :

$$(a_{i_1} \otimes \cdots \otimes a_{i_n}) \times (b_{j_1} \otimes \cdots \otimes b_{j_m}) := a_{i_1} \otimes \cdots \otimes (a_{i_n} \cdot b_{j_1}) \otimes \cdots \otimes b_{j_m} \tag{54}$$

le produit entre a_{i_n} et b_{j_1} pouvant être calculé à l'aide des règles de calcul de $\mathcal{A}_{i_n}$. On applique alors $\mathscr{P}(p)$ au terme obtenu.

Si par contre $i_n \neq j_1$, on pose simplement :

$$(a_{i_1} \otimes \cdots \otimes a_{i_n}) \times (b_{j_1} \otimes \cdots \otimes b_{j_m}) := a_{i_1} \otimes \cdots \otimes a_{i_n} \otimes b_{j_1} \otimes \cdots \otimes b_{j_m} \tag{55}$$

et on obtient un nouvel élément formel parfaitement défini.

Prouver que la multiplication ainsi définie est bien une multiplication d'algèbre est laborieux, mais facile. Nous nous en passerons ici.

On dispose clairement des injections W_i :

$$\begin{aligned} W_i : \mathcal{A}_i &\to \mathcal{A} \\ a_i &\mapsto \varphi_i(a_i)\cdot\Omega + (a_i - \varphi_i(a_i)\cdot\Omega) \in K\cdot\Omega \oplus \mathcal{W}_{(i)} \end{aligned}$$

Il faut encore prouver que nous venons bien de construire un produit libre. Soit $\mathcal{B}$ une K-algèbre unitaire, et soit une famille de morphismes d'algèbres $(f_i : \mathcal{A}_i \to \mathcal{B})$. La construction du produit et la décomposition (52) montre qu'un morphisme $f : \mathcal{A} \to \mathcal{B}$ correspondant au produit libre des (f_i) est entièrement déterminé par la donnée de $f(a)$ pour $a \in \bigsqcup_{i\in I} \mathcal{A}_i$. Dans ce cas, si $\boldsymbol{i} = (i_1, \ldots, i_n)$ est un multi-indice alterné, on a nécessairement :

$$\forall (a_i, \ldots, a_n) \in \mathcal{A}_{i_1} \times \ldots, \times \mathcal{A}_{i_n},\ f(a_1 \otimes \cdots \otimes a_n) = \prod_{j=1}^{\overrightarrow{n}} f(a_j) \tag{56}$$

et par linéarité, on détermine la valeur de f sur $\mathcal{W}_{\boldsymbol{i}}$ puis sur $\mathcal{A}$ tout entier. Or la propriété souhaitée pour f est la suivante :

$$\forall i \in I,\ f \circ W_i = f_i, \tag{57}$$

ce qui impose :

$$\forall i \in I,\ \forall a_i \in \mathcal{A}_i,\ f(a_i) = f_i(a_i) \tag{58}$$

Ainsi, il existe bien un unique morphisme d'algèbre satisfaisant la propriété du produit libre. Donc $\mathcal{A}$ est bien le produit libre des $(\mathcal{A}_i)$ □

Remarque : En observant la décompositon (52), on voit que la fonction φ obtenue comme produit libre des (φ_i) s'assimile à la projection sur l'état du vide.

Pour l'instant, nous n'avons de résultats que sur les algèbres elles-mêmes. Pourtant, on verra très simplement que la construction que nous venons de mener, qui repose sur des formes linéaires unitaires - des espérances non-commutatives en somme ! - a un lien très fort avec la libre indépendance. Commençons par introduire la notation suivante :

Lemme 6. *Soit $(\mathcal{A}_i, \varphi_i)$ une famille d'espaces de probabilité non commutatifs. Il existe une unique forme linéaire φ sur $\underset{i\in I}{*} \mathcal{A}_i$ telle que :*

$$\forall i \in I,\ \varphi|_{\mathcal{A}_i} = \varphi_i. \tag{59}$$

On note alors $\varphi = \underset{i\in I}{*} \varphi_i$.

Démonstration. Il suffit d'appliquer la propriété universelle du produits libre aux (φ_i), où l'algèbre but $\mathcal{B}$ est simplement $\mathbb{C}$. □

Théorème 7. *Soit $(\mathcal{A}_i, \varphi_i)_{i\in I}$ une famille d'espaces de probabilité non-commutatifs. Posons $(\mathcal{A}, \varphi) := (\underset{i\in I}{*} \mathcal{A}_i, \underset{i\in I}{*} \varphi_i)$. Alors les $(\mathcal{A}_i)$, vus comme sous-espaces de $\mathcal{A}$, sont librement indépendant par rapport à φ.*

Démonstration. Ecrivont la décomposition de $\mathcal{A}$ comme dans (52) construite par rapport aux φ_i. La propriété de libre indépendance est directement obtenue par définition du produit, et en remarquant que l'espérance φ s'annule sur tous les $(\mathcal{W}_{\boldsymbol{i}})$ de par (56). □

Ce résultat nous permet d'enfin obtenir le théorème d'existence souhaité :

Corollaire 2. *Soit I un ensemble d'indices, et soit $(\mu_i : \mathbb{C}[X] \to \mathbb{C})_{i\in I}$ une famille d'applications linéaires unitaires. Alors il existe un espace probabilisé $(\mathcal{A}, \varphi)$ et une famille de variables aléatoires $(a_i)_{i\in I} \in \mathcal{A}^I$ librement indépendantes telles que pour $i \in I$, a_i ait pour distribution algébrique μ_i.*

Démonstration. Considérons $(\mathcal{A}_i)_{i\in I}$ des copies disjointes de $\mathbb{C}[X]$. On munit alors chaque $\mathcal{A}_i$ de l'espérance non-commutative μ_i pour laquelle la variable aléatoire X a pour distribution algébrique μ_i. Enfin, on forme $\mathcal{A} := \underset{i\in I}{*} \mathcal{A}_i$, $\varphi := \underset{i\in I}{*} \mu_i$ et, en notant $W_i := \mathcal{A}_i \to \mathcal{A}$ l'injection canonique dans le produit libre, les variables aléatoires $(W_i(X))$ sont librement indépendantes en vertu du théorème 7, et ont pour distribution algébrique respective μ_i. □

Les auteurs de [7] montrent que cette construction s'adapte aux cas des $*$-espaces de probabilités en utilisant la même décomposition. Nous nous contenterons d'admettre le théorème d'existence pour des $*$-distributions. La preuve consiste essentiellement à montrer que si les $(\mathcal{A}_i, \varphi_i)$ sont des $*$-espaces de probabilité, alors la fonction $\varphi := \underset{i\in I}{*} \varphi_i$ est positive, et donc que le produit libre des $(\mathcal{A}_i)$ muni de φ est un $*$-espace de probabilité.

Le théorème 4 justifie que dans le cas des $*$-espaces de probabilité, on a en fait équivalence pour deux familles de variables aléatoires $\boldsymbol{a}$ et $\boldsymbol{b}$ entre être libre et $(\mathrm{Alg}^*(\boldsymbol{a}, \boldsymbol{b}), \varphi|_{\mathrm{Alg}^*(\boldsymbol{a},\boldsymbol{b})}) \cong (\mathrm{Alg}^*(\boldsymbol{a}) * \mathrm{Alg}^*(\boldsymbol{b}), \varphi|_{\mathrm{Alg}^*(\boldsymbol{a})} * \varphi|_{\mathrm{Alg}^*(\boldsymbol{b})})$. Aussi propose-t-on un point de vue plus géométrique sur la libre indépendance : on peut remarquer que la fonction $(a, b) \mapsto \langle a, b\rangle := \varphi(a^*b)$ est la forme polaire d'une fonction quadratique sur $\mathcal{A}$. Aussi la décomposition (52) permet d'exprimer la libre indépendance de familles d'algèbres comme l'orthogonalité des espaces $\mathcal{W}_{\boldsymbol{i}}$!

2.5 Cumulants libres

On a pu constater que l'espérance non-commutative se comporte de manière bien moins agréable à l'égard de variables aléatoires libres que l'espérance classique pour des variables aléatoires indépendantes. R. Speicher a introduit une fonctionnelle, appelée *cumulant libre*, dont le comportement est bien meilleur à l'égard des variables aléatoires libres. Cette section vise à introduire les propriétés des cumulants que nous utiliserons par la suite.

La construction et la manipulation des cumulants libres reposent en grande partie sur des

résultats de combinatoire portant sur les partitions non-croisées et l'inversion de Möbius, introduits dans la partie préliminaire 1.

L'objectif ici est, pour une famille de variables aléatoires $(a_i)_{i\in I}$ sur un certain espace de probabilité, de définir des fonctions κ_π, dites «cumulants libres» liées aux moments par la formule :

$$\varphi\left(\overrightarrow{\prod_{j=1}^{n}} x_{i_j}\right) = \sum_{\pi\in NC(n)} \kappa_\pi[a_{i_1},\dots,a_{i_n}] \tag{60}$$

Les auteurs de [7] présentent une motivation à la recherche de telles fonctions en introduisant le théorème central limite libre, que nous verrons quant à nous plus loin. Pour nous, ces cumulants pourront quelque peu paraître posés *ad hoc*, mais nous verrons néanmoins qu'il s'agit d'un outil fort commode à l'étude de la libre indépendance.

Les outils introduits en section 1.3 fournissent une façon de définir de telles fonctions à l'aide d'une inversion de Möbius de la façon suivante : donnons-nous une famille de variables aléatoires $(a_i)_{i\in I}$ sur un certain espace de probabilité $(\mathcal{A},\varphi)$. Soit un multi-indice $(i_1,\dots,i_n)\subset I$ et posons alors :

$$\forall\pi\in NC(n),\ \varphi_\pi[a_{i_1},\dots,a_{i_n}] := \prod_{B\in\pi}\varphi\left(\overrightarrow{\prod_{j\in B}} a_{i_j}\right) \tag{61}$$

Dans ce cas, l'équation (60) se réécrit :

$$\varphi_{1_n}[a_1,\dots,a_n] = \sum_{\substack{\pi\in NC(n)\\ \pi\leqslant 1_n}} \kappa_\pi[a_1,\dots a_n] \tag{62}$$

avec 1_n la partition maximale de $NC(n)$. Ainsi, il fait sens de poser :

Définition 25 (Cumulants libres). *Soit $(\mathcal{A},\varphi)$ un espace de probabilité non-commutatif. On appelle* cumulants libres *la famille de fonctions multilinéaires définie par :*

$$\forall n\in\mathbb{N}^*,\ \forall\pi\in NC(n),\ \kappa_\pi : (a_1,\dots,a_n)\mapsto \sum_{\substack{\sigma\in NC(n)\\ \sigma\leqslant\pi}} \varphi_\sigma[a_1,\dots a_n]\mu_n(\sigma,\pi) \tag{63}$$

avec μ_n la fonction de Möbius *sur $NC(n)$.*

Donnons quelques propriétés élémentaires des cumulants au-travers du prisme des «fonctionnelles multiplicatives».

Définition 26 (Fonctionnelles multiplicatives). *Soit $\mathcal{A}$ une algèbre. Soit $(f_n : \mathcal{A}^n \to \mathbb{C})_{n\in\mathbb{N}^*}$ une suite de formes multilinéaires. Cette famille peut être étendue en une famille de fonctions multilinéaires de la façon suivante : pour tout $n \in \mathbb{N}^*$ et pour tout $\pi \in NC(n)$, on pose :*

$$f_\pi : \mathcal{A}^n \to \mathbb{C}$$
$$(a_1, \dots, a_n) \mapsto f_\pi[a_1, \dots, a_n]$$

où $f_\pi[a_1, \dots a_n] = \prod_{B\in\pi} f(B)[a_1, \dots, a_n]$ et $f(B)[a_1, \dots, a_n]$ est la valeur de $f_{|B|}$ évaluée en les $(a_i)_{i\in B}$.

On dit alors qu'une fonctionnelle $\pi \mapsto f_\pi$ est multiplicative si elle découle d'une famille f_n de la façon décrite ci-dessus.

Remarque : L'écriture (61) correspond à la famille multiplicative découlant des fonctionnelles $f_n : (a_1, \dots a_n) \mapsto \varphi(a_1 \dots a_n)$.

On peut faire quelques observations sur les fonctionnelles multiplicatives :
— Si $\pi \mapsto f_\pi$ est multiplicative, alors il est clair qu'elle est entièrement déterminée par la famille (f_n) dont elle découle.
— Par ailleurs, $f_n = f_{1_n}$ avec 1_n la partition de $NC(n)$ composée d'un seul bloc.

Proposition 12 (admise). *$\pi \mapsto \kappa_\pi$ est une fonctionnelle multiplicative.*

En particulier, les cumulants sont entièrement déterminés par la famille $(\kappa_n) = (\kappa_{1_n})$.

Exemples : Donnons l'expression exacte des cumulants pour n petit :
— $\kappa_1[a_1] = \varphi(a_1)\mu_1(1_1, 1_1) = \varphi(a_1)$ [(vi)]
— $\varphi(a_1a_2) = \kappa_2[a_1, a_2] + \kappa_{0_2}[a_1, a_2]$ d'après (63). Donc :

$$\kappa_2[a_1, a_2] = \varphi(a_1a_2) - \kappa[a_1]\kappa[a_2] = \varphi(a_1a_2) - \varphi(a_1)\varphi(a_2) \text{ par multiplicativité.} \quad (64)$$

On se dote d'une formule commode pour calculer avec les cumulants :

(vi). La valeur de $\mu_1(1_1, 1_1)$ s'obtient directement à partir de la matrice de la fonction ζ_1, de taile 1×1...

Proposition 13 (Cumulants de produits). *Soit $n \in \mathbb{N}^*$. Soit $m \leqslant n$. Soient $1 = i_0 < i_1 < i_2 < \cdots < i_m = n$ Soit $a_1, \dots a_n$ des variables aléatoires sur un certain espace de probabilités non-commutatifs. Alors :*

$$\forall \tau \in NC(m),\ \kappa_\tau \left[\overrightarrow{\prod_{j=1}^{i_1}} a_j,\ \overrightarrow{\prod_{j=i_1+1}^{i_2}} a_j, \dots,\ \overrightarrow{\prod_{j=i_{m-1}+1}^{m}} a_j \right] = \sum_{\substack{\pi \in NC(n) \\ \pi \vee \widehat{0_m} = \widehat{\tau}}} \kappa_\pi[a_1, \dots, a_n] \tag{65}$$

où $NC(m) \ni \sigma \mapsto \widehat{\sigma} \in NC(n)$ est définie ainsi :

$$\forall (k,l) \in [\![n]\!]^2, k \sim_{\widehat{\sigma}} l \iff i^{-1}(k) \sim_\sigma i^{-1}(l) \tag{66}$$

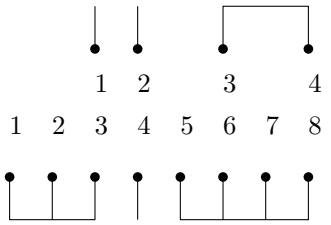
où $i^{-1}(k) := \min\{j \in [\![m]\!] \mid k \leqslant i_j\}$.

Démonstration. L'application $\sigma \mapsto \widehat{\sigma}$ est injective et préserve l'ordre partiel. De plus, $\forall (\sigma, \tau) \in NC(m)^2,\ \widehat{[\sigma;\tau]} = [\widehat{\sigma};\widehat{\tau}]$. Donc par la proposition (6), $\mu_m(\sigma,\tau) = \mu_n(\widehat{\sigma},\widehat{\tau})$.

Soit $\tau \in NC(m)$. Pour simplifier, notons $A_k = \overrightarrow{\prod_{k=i_{j-1}+1}^{i_j}} a_k$. Ainsi :

$$\begin{aligned}
\kappa_\tau[A_1, \dots, A_m] &= \sum_{\substack{\pi \in NC(m) \\ \pi \leqslant \tau}} \varphi_\pi[A_1, \dots, A_m] \mu_m(\pi, \tau) \\
&= \sum_{\substack{\pi \in NC(m) \\ \pi \leqslant \tau}} \varphi_{\widehat{\pi}}[a_1, \dots, a_n] \mu_n(\widehat{\pi}, \widehat{\tau}) \\
&= \sum_{\substack{\sigma \in NC(n) \\ \widehat{0_m} \leqslant \sigma \leqslant \widehat{\tau}}} \varphi_\sigma[a_1, \dots, a_n] \mu_n(\sigma, \widehat{\tau})
\end{aligned}$$

La formule d'inversion partielle de MÖBIUS permet de conclure. □



Ci-dessus : représentation graphique de $\pi \mapsto \widehat{\pi}$, avec $m = 4$, $n = 8$ et $\boldsymbol{i} = (3,4,6,8)$.

Cettte proposition nous sera principalement utile dans le cas où $\tau = 1_m$, où dans ce cas $\widehat{1_m} = 1_n$ et la condition $\widehat{0_m} \leqslant \pi \leqslant 1_n$ devient plus facile à manipuler.

Nous avons évoqué plus haut que les cumulants permettent un calcul efficace avec les variables aléatoires libres. Nous allons donc développer quelques résultats qui nous permettront de travailler avec la libre indépendance. Commençons par un petit lemme :

Lemme 7. *Soit $(\mathcal{A}, \varphi)$ un espace de probabilité, et soient $a_1, \ldots, a_n$ des variables aléatoires avec $n \geqslant 2$. Alors, si l'une de ces variables est proportionnelle à $1_{\mathcal{A}}$, $\kappa_n[a_1, \ldots, a_n] = 0$.*

Démonstration. Par récurrence sur n. Pour $n = 2$, le résultat est clair d'après (64). Soit n tel que le résultat est vrai, et soient $a_1, \ldots a_{n+1}$ des variables aléatoires. Pour simplifier, on note $a_{n+1} = \lambda \cdot 1_{\mathcal{A}}$. Alors :

$$\varphi(a_1 \cdots a_n \lambda \cdot 1_{\mathcal{A}}) = \sum_{\pi \in NC(n+1)} \kappa_\pi[a_1, \ldots, a_n, \lambda \cdot 1_{\mathcal{A}}] \tag{67}$$

$$= \kappa_{n+1}[a_1, \ldots, a_n, \lambda \cdot 1_{\mathcal{A}}] + \sum_{\pi \in NC(n+1) \setminus \{1_{n+1}\}} \kappa_\pi[a_1, \ldots, a_n, \lambda \cdot 1_{\mathcal{A}}], \tag{68}$$

d'où, par l'hypothèse de récurrence, les termes non-nuls dans la somme sont forcément tels que $\{n+1\} \in \pi$. Or, clairement :

$$\{\pi \in NC(n+1) \mid \{n+1\} \in \pi\} = \{\pi \sqcup \{\{n+1\}\}, \pi \in NC(n)\}. \tag{69}$$

Donc :

$$\varphi(a_1 \cdots a_n \lambda \cdot 1_{\mathcal{A}}) = \kappa_{n+1}[a_1, \ldots, a_n, \lambda \cdot 1_{\mathcal{A}}] + \lambda \cdot \sum_{\pi \in NC(n)} \kappa_\pi[a_1, \ldots, a_n] \tag{70}$$

$$= \kappa_{n+1}[a_1, \ldots, a_n, \lambda \cdot 1_{\mathcal{A}}] + \lambda \cdot \varphi(a_1 \ldots a_n), \tag{71}$$

d'où le résultat. □

En particulier, on a que $\kappa_n[a_1, \ldots a_n] = \kappa_n[a_1^\circ, \ldots, a_n^\circ]$ par multilinéarité. Là où le calcul pratique des moments de variables libres nécessite de centrer les variables, ce n'est plus le cas pour le calcul des cumulants. On commence à percevoir pourquoi leur comportement sera meilleur vis-à-vis des variables libres.

Théorème 8 (Annulation des cumulants mêlés). *Soit $(\mathcal{A}, \varphi)$ un espace de probabilité, et soit $(\mathcal{A}_i)_{i \in I}$ une famille de sous-algèbres de $\mathcal{A}$. Les assertions suivantes sont équivalentes :*

(i) Les $(\mathcal{A}_i)$ sont libres.

(ii) Pour tout $n \geqslant 2$ et pour tout $\boldsymbol{i} = (i_1, \ldots i_n) \subset I$. tel que $\boldsymbol{i}$ contient au moins deux indices différents, pour toute famille $a_1, \ldots, a_n$ de variables aléatoires telle que $a_j \in \mathcal{A}_{i_j}$, on a :

$$\kappa_n[a_1, \ldots a_n] = 0 \tag{72}$$

Démonstration.

Supposons (i). Grâce au lemme 7, on peut sans restriction rempalcer les (a_i) par les a_i°. On suppose donc les (a_i) centrés. On raisonne par récurrence sur n.

Pour $n = 2$, $\kappa_2[a_1, a_2] = \varphi(a_1 a_2) - \varphi(a_1)\varphi(a_2)$ d'après (64). Donc, si $i_1 \neq i_2$, l'hypothèse de liberté montre $\kappa_2[a_1, a_2] = 0$.

Soit $n \geqslant 2$ tel que la propriété (ii) est vraie pour tout $2 \leqslant l \leqslant n$. Alors, si le multi-indice $\boldsymbol{i}$ est alterné, on a :

$$\kappa_{n+1}[a_1, \ldots, a_{n+1}] = \sum_{\pi \in NC(n+1)} \varphi_\pi[a_1, \ldots a_{n+1}] \mu_{n+1}(\pi, 1_{n+1}) = 0, \tag{73}$$

car

$$\varphi_\pi[a_1,\dots,a_{n+1}] = \prod_{B\in\pi} \varphi\left(\overrightarrow{\prod_{j\in B}} a_j\right) \tag{74}$$

et que les partitions π admettent un bloc segment, ou réduit à un élément, ou alors contenant uniquement pris dans des algèbres libres alternées.

Si par contre $\boldsymbol{i}$ n'est pas alterné, on multiplie toutes les variables adjacentes appartenant à une même algèbre ensemble. Notons $(A_j)_{1\leqslant j\leqslant m}$ les éléments ainsi obtenus. Ainsi, $2 \leqslant m \leqslant n$. D'après la proposition 13, et par hypothèse de récurrence :

$$0 = \kappa_m[A_1,\dots A_m] = \kappa_{n+1}[a_1,\dots,a_{n+1}] + \sum_{\substack{\pi\in NC(n+1)\setminus\{1_{n+1}\}\\ \pi\vee\widehat{0_m}=1_{n+1}}} \kappa_\pi[a_1,\dots,a_{n+1}] \tag{75}$$

en réutilisant les notations de la proposition 13. D'après le lemme 1, une partition π satisfaisant la condition $\pi\vee\widehat{0_m} = 1_{n+1}$ «couple» forcément les blocs adjacents de $\widehat{0_m}$. Donc par multiplicativité des cumulants, et par hypothèse de récurrence, chacun des termes de la somme est nul, et on a :

$$0 = \kappa_m[A_1,\dots A_m] = \kappa_{n+1}[a_1,\dots,a_{n+1}] \tag{76}$$

Supposons maintenant (ii). Prenons les (a_i) centrées et le multi-indice $\boldsymbol{i}$ alterné. Alors :

$$\varphi(a_1\dots a_n) = \sum_{\pi\in NC(n)} \kappa_\pi[a_1,\dots,a_n] = 0 \tag{77}$$

car les partitions π étant non-croisées, elles contiennent un bloc segment B, et $\kappa(B)[a_1,\dots,a_n] = 0$ par hypothèse (ii) ou parce que les (a_i) sont centrées.

□

Un corollaire immédiat de ce résultat est le suivant :

Corollaire 3 (Additivité des cumulants pour les variables libres). *Soient a et b deux variables aléatoires libres sur un certain espace de probabilité. Alors :*

$$\forall n\in\mathbb{N}^*,\ \kappa_n[a+b,a+b,\dots,a+b] = \kappa_n[a,\dots a] + \kappa_n[b,\dots,b] \tag{78}$$

Enfin, observons une dernière formule qui nous sera très utile pour la dernière partie de la démosntration du théorème qui nous intéressera pour la suite de notre étude :

Théorème 9. *Soient $\boldsymbol{a} = (a_i)_{i\in I}$ et $\boldsymbol{b} = (b_i)_{i\in I}$ deux familles de variables aléatoires sur un espace de probabilité $(\mathcal{A},\varphi)$. Les assertions suivantes sont équivalentes :*

(i) $\boldsymbol{a}$ et $\boldsymbol{b}$ sont libres.

(ii) $\forall n\in\mathbb{N}^*,\ \forall(a_1,\dots,a_n)\in\boldsymbol{a}^n,\ \forall(b_1,\dots,b_n)\in\boldsymbol{b}^n$, on a :

$$\varphi\left(\overrightarrow{\prod_{j=1}^{n}} a_jb_j\right) = \sum_{\pi\in NC(n)} \kappa_\pi[a_1,\dots,a_n]\varphi_{\mathcal{K}(\pi)}[b_1,\dots,b_n], \tag{79}$$

avec $\mathcal{K}$ le dual de Kreweras.

Démonstration.

Supposons (i).

$$\varphi(a_1b_1\dots a_nb_n) = \sum_{\pi\in NC(2n)} \kappa_\pi[a_1,b_1,\dots,a_n,b_n] \tag{80}$$

$$= \sum_{\substack{\pi_1\in NC(\{1,3,\dots 2n-1\}),\pi_2\in NC(\{2,4,\dots,2n\})\\ \pi_1\sqcup\pi_2\in NC(2n)}} \kappa_{\pi_1}[a_1,\dots,a_n]\kappa_{\pi_2}[b_1,\dots,b_n] \tag{81}$$

$$= \sum_{\pi_1\in NC(n)} \left(\kappa_{\pi_1}[a_1,\dots a_n] \sum_{\substack{\pi_2\in NC(\bar n)\\ \pi_1\sqcup\pi_2\in NC(\{b_{\bar 1},\dots,n,\bar n\}}} \kappa_{\pi_2}[b_{\bar 1},\dots,b_{\bar n}] \right) \tag{82}$$

$$= \sum_{\pi_1\in NC(n)} \kappa_{\pi_1}[a_1,\dots a_n]\varphi_{\mathcal{K}(\pi_1)}[b_1,\dots,b_n]. \tag{83}$$

Le pasage à la ligne (81) utilise la multiplicativité des cumulants et l'annulation des cumulants mêlés. Le passage à la ligne (83) exploite quant à lui le fait que si $\pi_2 \in NC(\{\bar 1,\dots,\bar n\})$ satisfait la condition $\pi\sqcup\pi_2 \in NC(\{1,\bar 1,\dots,n,\bar n\})$, alors $\pi_2 \leqslant \mathcal{K}(\pi_1)$ et réciproquement. Il suffit de conclure grâce à la définition des cumulants par inversion de Möbius.

Supposons maintenant (ii). A l'aide du théorème d'existence (corollaire 2), donnons $\boldsymbol{a'} = (a'_i)_{i\in I}$ et $\boldsymbol{b'} = (b'_i)_{i\in I}$ dans un certain espace probabilisé $(\mathcal{B},\psi)$ tels que $\boldsymbol{a'}$ et $\boldsymbol{b'}$ soient égaux en loi jointe respectivement à $\boldsymbol{a}$ et $\boldsymbol{b}$ et soient libres l'une de l'autre. Comme la liberté est une propriété de l'algèbre engendrée, si $x_1\dots x_L$ est un monôme non-commutatif en les éléments de $\boldsymbol{a}$ et $\boldsymbol{b}$, on peut toujours se rammener à une expression de la forme $a_1b_1\dots a_nb_n$ où les facteurs sont pris dans $\mathrm{Alg}(\boldsymbol{a})$ et $\mathrm{Alg}(\boldsymbol{b})$. Or :

$$\psi(a'_1b'_1\dots a'_nb'_n) = \sum_{\pi\in NC(n)} \kappa_\pi[a'_1,\dots,a'_n]\psi_{\mathcal{K}(\pi)}[b'_1,\dots,b'_n] \quad \text{car (i)} \Longrightarrow (2) \tag{84}$$

$$= \sum_{\pi\in NC(n)} \kappa_\pi[a_1,\dots,a_n]\varphi_{\mathcal{K}(\pi)}[b_1,\dots,b_n] \quad \text{par égalité en loi} \tag{85}$$

$$= \varphi(a_1b_1\dots a_nb_n) \quad \text{d'après (ii)} \tag{86}$$

Ainsi, les familles $\boldsymbol{a}\cup\boldsymbol{b}$ et $\boldsymbol{a'}\cup\boldsymbol{b'}$ sont égales en loi jointe. En particulier, $\boldsymbol{a}$ et $\boldsymbol{b}$ sont libres.

□

2.6 Distribution semi-circulaire et théorème central limite

En probabilités classiques, la loi normale occupe un rôle essentiel. Nous allons voir dans cette section qu'en probabilités libres, une autre distribution est au cœur de nombreux phénomènes : la distribution semi-circulaire.

Définition 27 (Distribution semi-circulaire). *Soit $(\mathcal{A}, \varphi)$ un $*$-espace de probabilité. Soit $a \in \mathcal{A}$ une variable aléatoire auto-adjointe. On dit que a suit une* distribution semi-circulaire *de paramètre r et on note $a \hookrightarrow SC(r)$ si, et seulement si, a admet une $*$-distribution au sens analytique de densité contre la mesure de* Lebesgue *:*

$$\begin{aligned} f_r : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto \frac{2}{\pi r^2}\sqrt{r^2 - t^2}\mathbb{1}_{|x|\leqslant r}. \end{aligned}$$

Le paramètre r est appelé rayon *de la semi-circulaire. Lorsque $r = 2$, on parle de* semi-circulaire standard.
Une famille de variables semi-circulaires est appelé système semi-circulaire.

Remarque : On préfèrera souvent utiliser comme paramètre pour la semi-circulaire sa variance σ^2. Celle-ci est donnée par l'équation $\sigma^2 = \dfrac{r^2}{4}$. La semi-circulaire standard est donc centrée et réduite, comme l'est la normale standard.

En probabilités libres, les distributions sont caractérisées par leurs moments, aussi la connaissance des moments de la semi-circulaire se révèle importante.

Proposition 14. *Soit a une variable aléatoire semi-circulaire de variance σ^2 sur un espace de probabilité $(\mathcal{A}, \varphi)$. Alors :*

$$\forall n \in \mathbb{N},\ \varphi(a^n) = \begin{cases} \sigma^n C_{\frac{n}{2}} \text{ si } n \text{ est pair} \\ 0 \text{ sinon} \end{cases} \tag{87}$$

où les nombres C_n désignent les nombres de Catalan.

Démonstration (esquisse). On se ramène au cas réduit et on calcule l'intégrale :

$$\int_{-2}^{2} \frac{t^n}{2\pi}\sqrt{4 - t^2}\,\mathrm{d}t \tag{88}$$

par changement de variable $t \leftarrow 2\cos(\theta)$ et en utilisant des intégrales de Wallis. □

De façon équivalente aux moments, on peut exprimer les cumulants d'une semi-circulaire :

Proposition 15. *Soit a une variable aléatoire semi-circulaire de variance σ^2. Alors :*

$$\forall n \in \mathbb{N}^*,\ \kappa_n[a, \ldots, a] = \begin{cases} \sigma^2 \text{ si } n = 2 \\ 0 \text{ sinon} \end{cases} \tag{89}$$

Par ailleurs, on a une caractérisation qui pourra peut-être sembler anecdotique ici, mais qui sera la clef de la démonstration de notre théorème principal :

Théorème 10. *Soit $(\mathcal{A}, \varphi)$ un espace de probabilité. Soient $\boldsymbol{a} = (a_i)_{i\in I}$ et $\boldsymbol{b} = (b_i)_{i\in I}$ deux familles de variables aléatoires sur $\mathcal{A}$. Alors, les assertions suivantes sont équivalentes :*

(i) $\boldsymbol{a}$ est un système semi-circulaire libre et $\boldsymbol{a}$ et $\boldsymbol{b}$ sont libres l'une de l'autre.

(ii) Pour tout $n \in \mathbb{N}^*$, $(a_1, \dots a_n) \in \boldsymbol{a}^n$ et $(b_1, \dots, b_n) \in \boldsymbol{b}^n$:

$$\varphi(a_1 b_1 \dots a_n b_n) = \sum_{\pi \in NC_2(2n)} \kappa_\pi[a_1, \dots a_n]\varphi_{\mathcal{K}(\pi)}[b_1, \dots b_n] \tag{90}$$

où $NC_2(2n)$ désigne l'ensemble des partitions non-croisées de $[\![2n]\!]$ dont tous les blocs sont de taille exactement 2.

Démonstration (esquisse). Le sens direct utilise essentiellement le théorème 9, la multiplicativité des cumulants et la proposition 15. La preuve du sens réciproque est identique à celle faite pour le théorème 9. □

On se propose de conclure cette section sur la théorie des probabilités libres par l'analogue libre du théorème central limite. Celui-ci nous permettra d'utiliser les concepts développés jusqu'à maintenant, et montrera le rôle particulier de la semi-circulaire en probabilités libres. Toutefois, il ne nous servira pas pour la suite, mais nous pensons qu'il est important au développement d'une théorie des probabiltiés, comme l'était le théorème d'existence développé en section 2.4.

Il est difficile ici de parler convergence en loi, aussi parlerons-nous plutôt de l'analogue le plus immédiat : la convergence en moments.

Définition 28 (Convergence en moments). *Soit I un ensemble d'indices. Soit $(a_i^{(N)})_{N\in\mathbb{N}}$ une suite de familles de variables aléatoires sur des espaces de probabilité $(A_N, \varphi_N)_{N\in\mathbb{N}}$, et soit $(b_i)_{i\in I}$ une famille de variables aléatoires sur un espace de probabilité (B, ψ). On dit que $(a_i^{(N)})$* converge en moments *vers (b_i) si, et seulement si :*

$$\forall P \in \mathbb{C}\langle X_i \mid i \in I\rangle, \ \lim_{N\to+\infty} \varphi_N(P(a_i^{(N)})) = \psi(P(b_i)) \tag{91}$$

Remarque : La convergence en moments est équivalente à la convergence des cumulants.

On a bien sûr une définition analogue de convergence en $*$-moments dans les $*$-espaces de probabilité.

Théorème 11 (central limite libre). *Soit $(\mathcal{A}, \varphi)$ un $*$-espace de probabilité. Soit $(a_N)_{N\in\mathbb{N}}$ une suite de variables aléatoires libres, auto-adjointes, centrées, de variance σ^2 et identiquement distribuées. Alors :*

$$\frac{1}{\sqrt{N}} \sum_{n=0}^{N} a_n \rightharpoonup SC(\sigma) \tag{92}$$

où la flèche $\rightharpoonup$ désigne la convergence en moments.

Démonstration. Soit $N \in \mathbb{N}^*$. Notons $S_N := \frac{1}{\sqrt{N}} \sum_{n=0}^{N} a_n$. On calcule les cumulants de S_n. Soit $k \in \mathbb{N}^*$. Alors :

$$\kappa_k \text{ (vii)}[S_N, \ldots, S_N] = N^{-\frac{k}{2}} \kappa_k \left[\sum_{n=0}^{N} a_n, \ldots, \sum_{n=0}^{N} a_n \right] \quad \text{par multilinéarité} \tag{93}$$

$$= N^{-\frac{k}{2}} \sum_{n=0}^{N} \kappa_k[a_n, \ldots, a_n] \quad \text{d'après le corollaire 3} \tag{94}$$

$$= \frac{\kappa_k[a_1, \ldots, a_1]}{N^{\frac{k}{2}-1}} \quad \text{car les } (a_n) \text{ sont identiquement distribués.} \tag{95}$$

Ainsi, il est clair que pour $k > 2$, le k-ème cumulant tend vers 0. Pour $k = 1$, $\kappa_1[a_1] = \varphi(a_1) = 0$ par hypothèse. Enfin, pour $k = 2$, $\kappa_2[a_1, a_1] = \varphi(a^2) = \sigma^2$. Donc on a bien la convergence des cumulants vers ceux de la semi-circulaire de variance σ^2. □

3 Matrices aléatoires et théorie des trafics

Dans ce second temps, nous allons nous intéresser à l'étude des grandes matrices aléatoires. Une matrice aléatoire est, comme chacun s'attend, une matrice dont les coefficients sont des variables aléatoires au sens classique du terme. Nous ne nous intéresserons qu'au cas de variables aléatoires complexes. Par «grandes» matrices aléatoires, on veut signifier que l'on va s'intéresser à des comportements asymptotiques lorsque la taille des matrices tend vers l'infini.

Notre étude s'articulera autour de la démonstration d'une généralisation du célèbre théorème de Wigner, que nous présenterons dans une première sous-section. Pour cela, nous ferons appel aux outils de probabilités libres développés dans la première section, ainsi qu'au formalisme de la théorie des trafics dont nous introduirons les outils essentiels plus bas. On ne s'intéressera dans notre étude qu'au cas de matrices carrées, aussi sous-entendrons-nous que toutes les matrices sont carrées sans plus de précisions. Le symbole N désignera toujours un entier non-nul représentant la dimension des matrices.

Pour alléger les notations qui, on le verra, deviendront vite extrêmement lourdes, posons d'ores et déjà quelques notations.

— Lorsqu'on se donnera une matrice aléatoire A_N de taille $N \times N$, on se donnera en fait implicitement une suite $(A_N)_{N \in \mathbb{N}^*}$ de matrices aléatoires telles que pour tout N, A_N est de taille $N \times N$. On confondra alors souvent la famille avec un élément de la famille. Par exemple, en disant que A_N et B_N sont deux matrices aléatoires indépendantes, on sous-entend que pour tout N, A_N est indépendante de B_N.

Toutes les variables aléatoires manipulées seront considérées sur le même espace probabilisé $(\Omega, \mathfrak{F}, \mathbb{P})$.

3.1 Théorème de Wigner

Outre l'énoncé du théorème de Wigner, cette première section va nous permettre d'introduire des notations et des objets essentiels à notre étude. On s'intéressera en effet principalement à certaines familles particulières de matrices aléatoires :

(vii). On note $\kappa_k = \kappa_{1_k}$

Définition 29 (Matrices de Wigner). *Une matrice aléatoires* $A_N = \left(\frac{a(i,j)}{\sqrt{N}}\right)_{1\leqslant i,j\leqslant N}$ *est dite de* Wigner *si, et seulement si :*

(i) $\forall \omega \in \Omega, A_N(\omega)$ *est hermitienne.*

(ii) Les variables $(a(i,j))$ *admettent des moments à tout ordre, sont centrées et ne dépendent pas de* N *en loi*[(viii]).

(iii) Les coefficients diagonaux sont identiquement distribués.

(iv) Les coefficients sur-diagonaux sont identiquement distribués.

(v) Les coefficients diagonaux et sur-diagonaux sont mutuellement indépendants.

Les valeurs propres étant des fonctions continues des entrées des matrices [(ix)], on peut s'intéresser à la mesure (aléatoire) empirique des valeurs propres, définie comme suit : on note $\lambda, \dots \lambda_N$ les valeurs propres comptées avec multiplicité d'une matrice aléatoire A_N. On note alors sa mesure empirique des valeurs propres :

$$L_N := \frac{1}{N}\sum_{n=1}^{N} \delta_{\lambda_n} \tag{96}$$

C'est cet objet qui sera au cœur de notre étude, et cela n'a rien d'étonnant ! Dans le langage des probabilités libres, une matrice aléatoire hermitienne dont tous les coefficients admettent des moments à tous ordres est une variable aléatoire non commutative pour l'espérance non-commutative $\varphi_N : M_N \mapsto \frac{1}{N}\mathbb{E}[\mathrm{Tr}(M_N)]$. Ainsi, si P est un $*$-polynôme :

$$\varphi_N(P(A_N)) = \mathbb{E}\left[\frac{1}{N}\sum_{n=0}^{N} P(\lambda_n)\right] = \frac{1}{N}\sum_{n=1}^{N} P(\mathbb{E}[\lambda_N]) = \int_{\mathbb{R}} P \,\mathrm{d}\mathbb{E}[L_N]. \tag{97}$$

Donc $\mathbb{E}[L_N]$ n'est rien d'autre que la $*$-distribution analytique de A_N !

On en arrive au théorème de Wigner, essentiel à la théorie des matrices aléatoires :

Théorème 12 (Wigner). *Soit* $(W_N)_{N\in\mathbb{N}^*}$ *une famille de matrices de* Wigner *dont les coefficients sont centrés. Pour* $N \in \mathbb{N}^*$*, on note* L_N *la mesure empirique des valeurs propres de* W_N*. Alors :*

$$\forall f \in C_b^0,\ \lim_{N\to+\infty} \int_{\mathbb{R}} f \,\mathrm{d}L_N = \int_{\mathbb{R}} f \,\mathrm{d}\sigma \tag{98}$$

où σ *est la mesure semi-circulaire.*

On peut reformuler cet énoncé dans le langage des probabilités libres : si (W_N) est une suite de matrices de Wigner aux coefficients centrés, alors elle converge en moments, en tant que variable aléatoire non-commutative de $\left(\underset{N\in\mathbb{N}^*}{*} \mathcal{M}_N(L^{\infty-}), \underset{N\in\mathbb{N}^*}{*} \frac{1}{N}\mathbb{E}[\mathrm{Tr}(\cdot)]\right)$ [(x)], vers une semi-circulaire standard. Le théorème de Stone-Weierstraß permet en effet de montrer que la convergence en moments est ici équivalente à la convergence faible de la mesure.

(viii). On rappelle qu'on se donne implicitement une suite de matrices $(A_N)_{N\in\mathbb{N}^*}$. La condition «la loi ne dépend pas de N» n'a donc rien de triviale.

(ix). Ce résultat, loin d'être trivial, a été présenté dans une section complémentaire du chapitre 3 du cours d'Analyse numérique de Benjamin Boutin.

(x). L'utilisation du produit libre ici permet de se placer sur un espace unique contenant des matrices de toute dimension. Cette notion est introduite dans la section 2.4.

Faisons une remarque sur cet énoncé : la mesure empirique de valeurs propres mesure la proportion de valeurs propres d'une matrice contenue dans un borélien donné. Dans le cas des matrices aléatoires, il s'agit d'une mesure elle-même aléatoire. Pourtant, celle-ci tend vers une mesure déterministe lorsque la dimension devient grande.

Le but de notre étude est de démontrer une généralisation de ce théorème, aussi ne le démontrerons-nous pas dans ces pages. Il existe essentiellement deux démonstrations usuelles de ce théorème, l'une combinatoire, l'autre analytique, reposant sur la transformée de Stieltjes. Toutes deux sont présentées dans [4].

Nous nous reposerons quant à nous sur un formalisme plus puissant, issu de la théorie des trafics. La prochaine section vise à en introduire les outils les plus élémentaires qui sont serviront à la démonstration de notre énoncé. La théorie des trafics est introduite plus avant dans [5].

3.2 Distribution de trafics

La théorie des trafics propose de travailler dans une certaine structure, appelée « espace de trafics », sur lequel il est possible d'opérer sur les éléments à l'aide de généralisations des opérations algébriques en faisant agir des graphes sur des matrices. Ces opérations se formalisent à l'aide de la notion *d'opérade symétrique*, que nous ne développerons pas ici, nous contentons d'introduire directement les formules.

Pour simplifier, on notera dans toute la suite φ l'espérance non-commutative usuelle sur l'ensemble des matrices aléatoires.

Une bonne partie des propositions que nous allons introduire seront laissées sans démonstration, lorsqu'elles reposent simplement sur le calcul, dans un objectif de concision.

Définition 30 ($*$-graphe test). *Soit $\mathbb{X} = (X_i)_{i\in I}$ un ensemble d'indéterminées. On appelle* $*$-graphe test en les indéterminées $\mathbb{X}$ *un quadruplet $(V, E, \gamma, \varepsilon)$ tel que :*

(i) (V, E) est un graphe fini, orienté, connexe, tel que $V \neq \emptyset$. On autorise les arrêtes à être multiples.

(ii) $\gamma : E \to \mathbb{X}$ est une fonction d'étiquetage des arrêtes.

(iii) $\varepsilon : E \to \{1, *\}$ est une application.

On note $\mathcal{T}\langle\mathbb{X}, \mathbb{X}^*\rangle$ l'ensemble des $*$-graphes tests.

Remarque : E peut tout à fait être vide dans un graphe test. Dans ce cas, par connexité, ce graphe est nécessairement réduit à un sommet unique.

Définition 31 ($*$-graphe-polynôme). *On appelle* $*$-graphe monôme en les indéterminées $\mathbb{X}$ *une triplet (T, in, out) tel que T est un $*$-graphe test et in et out sont deux sommets, éventuellement confondus, de V.*

On appelle $*$-graphe polynôme en les indéterminées $\mathbb{X}$ *un élément de $\mathbb{C}\langle\mathcal{T}\langle\mathbb{X}, \mathbb{X}^*\rangle\rangle$, c'est-à-dire une combinaison formelle formant un polynôme non commutatif en les indéterminées $\mathcal{T}\langle\mathbb{X}, \mathbb{X}^*\rangle$.*

Remarque : Dans la suite, on supposera toujours les espaces munis d'une involution $*$, sans plus de précision dans la terminologie, afin d'alléger les notations.

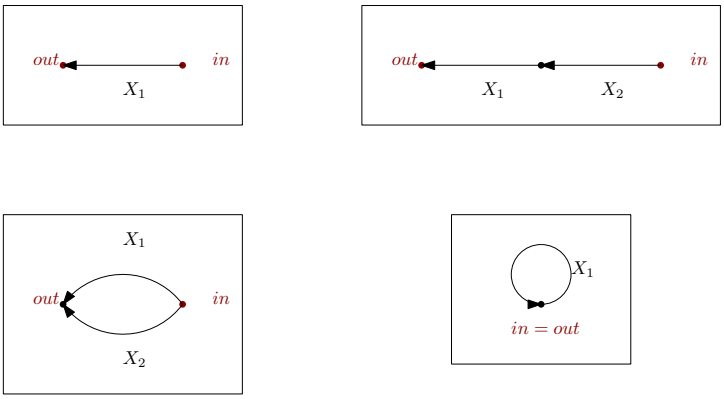
Ainsi qu'on l'a dit, le but de ce formalisme et de transformer ces graphes on opérateurs sur les matrices. On définit donc :

Définition 32 (Graphe opérateur). *Soit $N \in \mathbb{N}^*$. Soi $\mathbb{A}_N = (A_i)_{i\in I}$ une famille de matrices complexes carrées de taille N. Soit g un graphe monôme en les indéterminées $\mathbb{X} = (X_i)_{i\in I}$. On pose alors $g(\mathbb{A}_N) \in \mathcal{M}_N(\mathbb{C})$ définit par :*

$$\forall (i,j) \in [\![N]\!]^2,\ g(\mathbb{A}_N)(i,j) := \sum_{\substack{\Phi: V \to [\![N]\!] \\ \Phi(in)=j, \Phi(out)=i}} \prod_{e=(v,w)\in E} A^{\varepsilon(e)}_{\gamma(e)}(\Phi(w), \Phi(v)) \tag{99}$$

On étend naturellement ces opérations à des graphes polynômes.

Donnons quelques exemples pour se fixer les idées :



— Le graphe en haut à gauche est l'opération identité : $g_1(A) = A$.
— Celui en haut à droite est le produit matriciel et $g_2(A_1, A_2) = A_1 A_2$ (attention à l'ordre des termes).
— Celui en bas à gauche est le produit entrée par entrée, ou produit de Shur, des matrices A_1 et A_2.
— Le dernier renvoie la matrice diagonale extraite de A_1.

Un des intérêts des trafics est qu'ils donnent une généralisation des distributions au sens des probabilités libres. En effet :

Définition 33 (Distribution de trafic). *Si $\mathbb{A}_N$ est une famille de matrices aléatoires de taille N, on appelle distribution de trafic jointe l'application :*

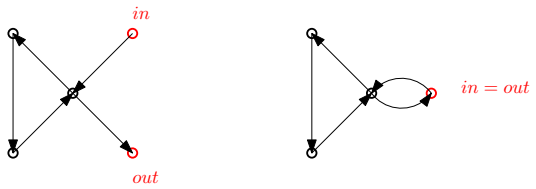
$$\begin{aligned} \mu_{\mathbb{A}_N} : \mathbb{C}\langle \mathcal{T}\langle \mathbb{X}, \mathbb{X}^*\rangle\rangle &\to \mathbb{C} \\ g &\mapsto \frac{1}{N}\mathbb{E}[\mathrm{Tr}(g(\mathbb{A}_N))] \end{aligned}$$

Comme on s'intéresse à des asymptotiques lorsque $[N \to +\infty]$, on se donne une notion de convergence au sens des trafics :

Définition 34 (Convergence en distribution de trafic). *On dit qu'une famille $\mathbb{A}_N$ de matrices aléatoires de taille N* converge en distribution de trafic *si, et seulement si, la distribution de trafic jointe de $\mathbb{A}_N$ converge simplement lorsque $[N \to +\infty]$.*

On peut remarquer que tout polynôme non commutatif évalué en une famille de matrices peut s'écrire comme un certain graphe-polynôme évalué en cette famille. Donc la distribution de trafic généralise bien la $*$-distribution algébrique, et la convergence en distribution de trafic généralise celle en moments.

On peut remarquer en utilisant la formule (99) que, pour un graphe monôme g, le calcul de $\varphi(g(\mathbb{A}_N))$ fournirait le même résultat en identifiant les sommets *in* et *out* de g. De plus, en cas d'une telle identification, la position choisie pour le sommet *in* n'a aucune importance. On note $\Delta(g)$ le graphe test obtenu par ce procédé. On a représenté en-dessous un graphe monôme g, à gauche, et son graphe $\Delta(g)$, à droite.



Ceci nous motive à introduire les quantités suivantes :

Définition 35 (Trace combinatoire et trace injective (normalisées)). *Soit $\mathbb{A}_N$ une famille de matrices aléatoires de taille N. On pose alors la* trace combinatoire *de $\mathbb{A}_N$:*

$$\tau_{\mathbb{A}_N} : \mathcal{T}\langle \mathbb{X}, \mathbb{X}^* \rangle \to \mathbb{C}$$
$$T \mapsto \frac{1}{N}\mathbb{E}\left[\sum_{\Phi : V \to [\![N]\!]} \prod_{e=(w,v)\in E} A^{\varepsilon(e)}_{\gamma(e)}(\Phi(w), \Phi(v)) \right]$$

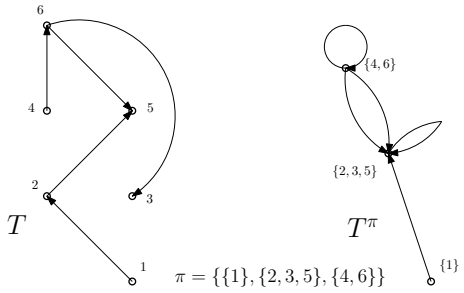
On pose également la trace injective *de $\mathbb{A}_N$:*

$$\tau^{\circ}_{\mathbb{A}_N} : \mathcal{T}\langle \mathbb{X}, \mathbb{X}^* \rangle \to \mathbb{C}$$
$$T \mapsto \frac{1}{N}\mathbb{E}\left[\sum_{\Phi : V \rightarrowtail [\![N]\!]} \prod_{e=(v,w)\in E} A^{\varepsilon(e)}_{\gamma(e)}(\Phi(w), \Phi(v)) \right]$$

où la somme est prise sur l'ensemble des applications injectives de V dans $[\![N]\!]$.
On définit également des version non-normalisée, notées Tr *et* Tr°*, dans l'expression desquelles on ne divise par N et on ne prend pas l'espérance.*

On peut relier la trace combinatoire à la trace injective à l'aide de la notion de *graphe quotient* :

Définition 36 (Graphe quotient). *Soit $T \in \mathcal{T}\langle \mathbb{X}, \mathbb{X}^* \rangle$. Soit $\pi \in \mathcal{P}(V)$. On appelle* graphe quotient de T par π *le graphe T^π obtenu en assimilant tous les sommets de T appartenant à un même bloc de π, et en conservant toutes les arrêtes de T. Le graphe obtenu peut donc être un multi-graphe, c'est-à-dire avoir des arrêtes multiples.*



On a alors :

Proposition 16. *Soit $\mathbb{A}_N$ une famille de matrices aléatoires. Alors :*

$$\forall T \in \mathcal{T}\langle \mathbb{X}, \mathbb{X}^* \rangle,\ \tau_{\mathbb{A}_N}[T] = \sum_{\pi \in \mathcal{P}(V)} \tau^\circ_{\mathbb{A}_N}[T^\pi] \tag{100}$$

On peut faire une remarque qui nous sera fort utile : l'expression de la trace combinatoire se passe des sommets *in* et *out* qu'on voit apparaître dans les graphes polynômes. Aussi, on peut choisir de définir la trace combinatoire non-normalisée de façon purement formelle :

$$\forall T \in \mathcal{T}\langle \mathbb{X}, \mathbb{X}^* \rangle,\ \mathrm{Tr}_{\mathbb{A}_N}[T] := \frac{1}{N}\mathbb{E}\left[\sum_{\Phi : V \to [\![N]\!]} \prod_{e=(v,w)\in E} A^{\varepsilon(e)}_{\gamma(e)}(\Phi(w), \Phi(v)) \right]. \tag{101}$$

Or cette expression formelle ne nécessite en rien que le graphe T soit connexe. Aussi, un calcul immédiat permet d'obtenir l'expression suivante :

Proposition 17. *Soit $\mathbb{A}_N$ une famille de matrices aléatoires. Soient $T_1, \ldots, T_c$ des graphes tests. On note $T := \bigsqcup_{i=1}^{c} T_i$ le graphe dont les composantes connexes sont exactement les (T_i). On suppose que l'ensemble des entrées des matrices forme une famille de variables aléatoires mutuellement indépendantes. Alors :*

$$\mathrm{Tr}_{\mathbb{A}_N}[T] = \prod_{i=1}^{c} \mathrm{Tr}_{\mathbb{A}_N}[T_i] \tag{102}$$

Remarques :

— On voit alors que lorsqu'on a la convergence en distribution de trafic, les termes $\tau_{\mathbb{A}_N}[T_i] := \frac{1}{N}\operatorname{Tr}_{\mathbb{A}_N}[T_i]$ convergent. Ainsi, le terme $\frac{1}{N^c}\operatorname{Tr}_{\mathbb{A}_N}[T]$ converge, avec c le nombre de composantes connexes de T. On notera ce dernier terme $\tau_{\mathbb{A}_N}[T]$ la trace combinatoire normalisée.
— On utilisera cette propriété dans le cas particulier où les matrices sont déterministes, rendant l'hypothèse de mutuelle indépendance triviale.

On aimerait avoir une factorisation simillaire pour la trace injective. Malheureusement, ceci est faux en général. Toutefois, ce résultat est asymptotiquement vrai :

Théorème 13. *Soit $\mathbb{A}_N$ une famille de matrices aléatoires, et soit $T = \bigsqcup_{i=1}^{c} T_I$ un graphe dont les composantes connexes sont des graphes tests. On fait les hypothèses suivantes :*
(i) L'ensembles des entrées des matrices forme une famille de variables aléatoires mutuellement indépendantes.
(ii) $\mathbb{A}_N$ converge en distribution de trafic.
Alors on a l'asymptotique suivante :

$$\tau^{\circ}_{\mathbb{A}_N}[T] = \prod_{i=1}^{c} \tau^{\circ}_{\mathbb{A}_N}[T_i] + \mathcal{O}\left(\frac{1}{N}\right) \tag{103}$$

Démonstration (esquisse). Une inversion de Möbius dans le poset $\mathcal{P}(V)$ permet d'exprimer la trace injective en fonction de la trace et de la fonction de Möbius. On peut alors utiliser la proposition précédante grâce à l'hypothèse (i). Enfin, une discussion sur la fonction de Möbius permet de factoriser les termes correspondant aux partitions π conservant les composantes connexes, faisant de faire apparaître la trace injective, et d'isoler les autres termes, correspondant aux partitions rassemblant des composantes connexes disjointes. On montre alors que ces termes ont un ordre inférieur au produit des traces injectives et tendent vers 0 en $\mathcal{O}\left(\frac{1}{N}\right)$.

Une démonstration complète, dans un cadre un peu plus général, est fournie dans [5]. □

4 Théorème de liberté asymptotique

Dans cette dernière partie, nous allons introduire l'énoncé du théorème généralisant le théorème de Wigner, et le démontrer. Celui-ci nous permettra de mettre en relation la théorie des matrices aléatoires et celle des probabilités libres, qui historiquement se sont développées sans lien apparent.

Théorème 14. *Soit $\mathbb{W}_N$ une famille de matrices de* Wigner *de taille N, et soit $\mathbb{Y}_N$ une famille de matrices déterministes de taille N* [xi]*. On suppose que $\mathbb{Y}_N$ converge en distribution de trafic et que les entrées des matrices de $\mathbb{W}_N$ forment une famille de variables aléatoires mutuellement indépendantes. Alors la famille $\mathbb{W}_N \cup \mathbb{Y}_N$ converge en moments. De plus $\mathbb{W}_N$ converge en moments vers un système semi-circulaire libre, et cette famille limite est libre de la famille limite des $\mathbb{Y}_N$.*

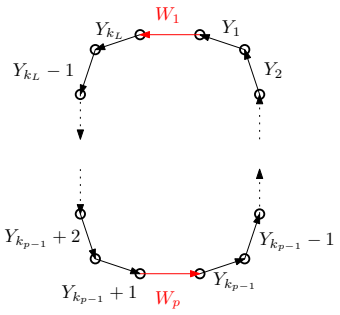
Ce théorème a d'abord été démontré par Eugene WIGNER dans les années 50, dans le cas particulier de matrices de BERNOULLI symétriques, dans [9]. Dans [8], Dan VOICULESCU a ensuite utilisé le Théorème central limite libre pour en produire une preuve dans le cas des matrices gaussiennes, de HAAR et déterministes. Ken DYKEMA a quant à lui démontré ce théorème pour les matrices de WIGNER, sans y inclure les matrices déterministes, dans [2]. Le cas le plus général a finalement été démontré par Greg W. ANDERSON, Alice GUIONNET et Ofer ZEITOUNI dans [1]. Une autre preuve est présentée par James A. MINGO et Roland SPEICHER dans [6].

Commençons par remarquer que le théorème de WIGNER se déduit bien de celui-ci : il suffit pour cela de prendre $\mathbb{W}_N$ réduite à une unique matrice, et $\mathbb{Y}_N$ réduite à l'identité.

Il est temps de démontrer le théorème.

4.1 Reformulation du problème

On va chercher dans un premier temps à montrer l'existence d'une distribution limite, qu'on caractérisera ensuite. Comme on souhaite montrer une convergence en moments : il suffit de montrer que pour tout mot $A_1^{\varepsilon(1)} A_2^{\varepsilon(2)} \dots A_L^{\varepsilon(L)}$ en les matrices $\mathbb{W}_N \cup \mathbb{Y}_N$, $\varphi(A_1^{\varepsilon(1)} \dots A_L^{\varepsilon(L)})$ admet une limite quand $[N \to +\infty]$ [(xii)]. Or, comme on le sait, la convergence en moments des variables aléatoires non-commutatives est une propriété des algèbres qu'elles engendrent. Aussi peut-on sans restriction supposer que $\mathbb{Y}_N$ contient l'identité. En séparant les matrices de $\mathbb{W}_N$ consécutives par l'identité dans un tel mot, on peut toujours se ramener à un mot de la forme $W_1 Y_1 \dots Y_{k_1} W_2 \dots W_L Y_{k_{L-1}+1} \dots Y_{K_L}$ [(xiii)]. Un tel mot s'exprime dans le langage des trafics. Posons $T = (V, E, \gamma, \varepsilon)$ le graphe test suivant :



Alors :

$$\varphi(W_1 Z_1 \dots W_L Z_L) = \tau[T], \tag{104}$$

où pour plus de simplicité, on a rassemblé les éléments de $\mathbb{Y}_N$ en des produits notés (Z_i), et où $\tau[T]$ est la trace combinatoire de T en les matrice $\mathbb{W}_N \cup \mathbb{Y}_N$. Ainsi donc, pour montrer la convergence en moments, il suffit de s'intéresser aux traces injectives. On fixe donc π une partition de V et on s'intéresse au terme $\tau^\circ[T^\pi]$.

(xi). On rappelle qu'on se donne implicitement des suites de familles pour tout $N \in \mathbb{N}^*$.

(xii). Pour une raison de simplicité, on omettra par la suite la possibilité pour ε de prendre la valeur $*$. La démonstration du théorème en incluant l'$*$ est rigoureusement la même, mais simplement plus lourde.

(xiii). On peut supposer que le premier terme est une matrice de WIGNER car l'espérance non-commutative φ est une trace : on peut donc sans perte de généralité appliquer une permutation circulaire à l'ordre des facteurs.

4.2 Expression de la trace injective

Pour $W_{\gamma(e)} \in \mathbb{W}_N$, on note $W_{\gamma(e)} = \left(\frac{W_{\gamma(e)}(i,j)}{\sqrt{N}}\right)_{1\leqslant i,j\leqslant N}$ comme dans la définition 29. Par ailleurs, on note V^π et E^π les ensembles de sommets et d'arrêtes de T^π. On note également par la lettre A les matrices de la famille $\mathbb{W}_N \cup \mathbb{Y}_N$ lorsqu'on ne souhaite pas préciser s'il s'agit de matrices de Wigner ou déterministes. On a :

$$\tau^\circ[T^\pi] = \frac{1}{N}\mathbb{E}\left[\sum_{\Phi:V^\pi\rightarrowtail[\![N]\!]}\prod_{e=(v,w)\in E^\pi} A_{\gamma(e)}(\Phi(w),\Phi(v))\right]. \tag{105}$$

Clairement, on peut écrire $E^\pi = E_W \sqcup E_Y$ où E_W contient toutes les arrêtes étiquetées par des matrices de Wigner, et E_Y celles étiquetées par des matrices déterministes. Alors :

$$\tau^\circ[T^\pi] = \frac{1}{N}\sum_{\Phi:V^\pi\rightarrowtail[\![N]\!]}\mathbb{E}\left[\prod_{e=(v,w)\in E_W}\frac{W_{\gamma(e)}(\Phi(w),\Phi(v))}{\sqrt{N}}\right]\left(\prod_{e=(v,w)\in E_Y} Y_{\gamma(e)}(\Phi(w),\Phi(v))\right) \tag{106}$$

On désignera désormais par T^π_W et T^π_Y les sous-graphe obtenus en ne conservant dans T^π que les arrêtes de E_W et E_Y respectivement, et en supprimant les sommets isolés. Pour $\Phi : V^\pi \rightarrowtail [\![N]\!]$, on note :

$$\delta^\circ_\Phi[T^\pi_W] := \mathbb{E}\left[\prod_{e=(v,w)\in E_W} W_{\gamma(e)}(\Phi(w),\Phi(v))\right] \tag{107}$$

Lemme 8. *$\delta^\circ_\Phi[T^\pi]$ ne dépend pas du choix de Φ. On note alors $\delta^\circ[T^\pi_W]$ sa valeur unique.*

Démonstration (esquisse). Comme les matrices de $\mathbb{W}_N$ sont de Wigner et indépendantes, deux entrées sont égales, conjuguées, ou bien indépendantes l'une de l'autre l'autre. Or étant données deux arrêtes $e = (v,w)$ et $e' = (v',w')$ dans E_W :

$$\neg[W_{\gamma(e)}(\Phi(w),\Phi(v)) \perp\!\!\!\perp W_{\gamma(e')}(\Phi(w'),\Phi(v'))] \iff \gamma(e) = \gamma(e') \text{ et } [(e = e') \text{ ou } (e = -e')] \tag{108}$$

avec $-e' = (w',v')$, par injectivité de Φ. On voit donc que cette condition ne dépend que de T^π. En séparant les cas où les deux entrées considérées sont égales ou conjuguées, on montre l'indépendance en Φ de $\delta^\circ_\Phi[T^\pi_W]$. □

Reprenons notre calcul :

$$\tau^\circ[T^\pi] = N^{-1-\frac{|E_W|}{2}}\delta^\circ[T^\pi_W]\sum_{\Phi:V^\pi\rightarrowtail[\![N]\!]}\prod_{e=(v,w)\in E_Y} Y_{\gamma(e)}(\Phi(w),\Phi(v)) \tag{109}$$

$$= N^{c_Y-1-\frac{|E_W|}{2}}\delta^\circ[T^\pi_W]\tau[T^\pi_Y] \tag{110}$$

Dans ce contexte, c_Y désigne le nombre de composantes connexes du graphe T^π_Y. On fait appraître la trace combinatoire grâce à la proposition 17 et la remarque qui a été faite en-dessous.

On peut désormais faire plusieures remarques sur cette formule :

— $\tau[T^\pi_Y]$ converge quand $[N \to +\infty]$ d'après l'hypothèse que $\mathbb{Y}_N$ admet une distribution de trafic limite.

— $\delta^\circ[T_W^\pi]$ est, par indépendance, un produit des moments des variables aléatoires $(W_{\gamma(e)}(i,j))$, dont la somme de tous les ordres est égale à $|E_W| \leqslant \dfrac{|E|}{2}$. Comme la loi de ces variables est supposées ne pas dépendre de N, on a donc que ce terme est borné.

On pose alors $\eta(\pi) := c_Y - 1 - \dfrac{|E_W|}{2}$. La discussion portant sur la convergence de $\tau^\circ[T^\pi]$ va désormais s'articuler autour de la valeur de $\eta(\pi)$, au vu des remarques que l'on vient de faire.

4.3 Majoration de $\eta(\pi)$ par introduction du «graphe maître»

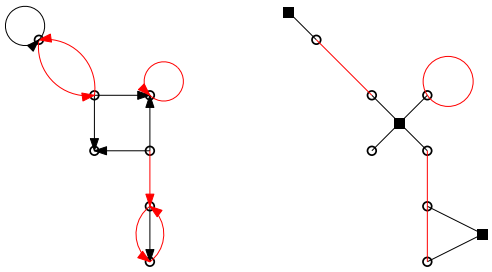
Notre objectif dans cette partie est d'établir le résultat suivant :

Lemme 9. *Soit $\pi \in \mathcal{P}(V)$. Alors $\delta^\circ[T_W^\pi] = 0$ ou $\eta(\pi) \leqslant 0$.*

Pour ce faire, nous allons utiliser un raisonnement combinatoire en introduisant un graphe auxilliaire :

Définition 37 (Graphe maître). *Dans cette situation, on appelle* graphe maître *le graphe non-orienté $\mathscr{T}(\pi) = (\mathscr{V}^\pi, \mathscr{E}^\pi)$, avec $\mathscr{V}^\pi$ composé des sommets de V^π ainsi que des composantes connexes de T_Y^π. Deux sommets de $\mathscr{V}^\pi$ sont reliés par une arrête de $\mathscr{E}^\pi$ si, et seulement si, ces deux sommets appartiennent à V^π et sont reliés par une arrête de E_W dans T^π, ou bien l'un est une composante connexe et l'autre est un sommet appartenant à cette composante connexe.*

Ci-dessous, un exemple d'un graphe et de son graphe maître. On a représenté en rouge les arrêtes étiquetées par des matrices de Wigner. Les sommets correspondant à des composantes connexes sont symbolisés par des carrés, les autres par des cercles.



Faisons un peu de dénombrement sur $\mathscr{T}(\pi)$:
— $|\mathscr{V}^\pi| = |V^\pi| + c_Y$
— $|\mathscr{E}^\pi| = |V^\pi| + |\bar{E}_W|$ avec $\bar{E}_W$ l'ensemble des arrêtes du squelette de T_W^π, c'est-à-dire le graphe obtenu en oubliant l'orientation et la multiplicité des arrêtes. En effet, chaque sommet appartient à une unique composante connexe de T_Y^π, donc on a une arrête pour chacun d'entre eux, plus toutes les arrêtes du squelette de T_W^π.

Ainsi :

$$\eta(\pi) = |\mathscr{V}^\pi| - |V^\pi| - \frac{|E_W|}{2} - 1 \tag{111}$$

$$= (|\mathscr{V}^\pi| - |\mathscr{E}^\pi| - 1) + \left(|\bar{E}_W| - \frac{|E_W|}{2}\right) \tag{112}$$

Pour analyser ce terme, nous allons utiliser le petit lemme suivant :

Lemme 10 (Inégalité de connexité). *Soit $G = (V, E)$ un graphe connexe. Alors :*

$$|V| - |E| - 1 \leqslant 0 \tag{113}$$

avec égalité si, et seulement si, G est un arbre.

Démonstration. On montre pour ce faire la propiété suivante par récurrence sur $|V|$: si G est un arbre, alors $|V|-|E|-1 = 0$. Pour $|V| = 1$, l'égalité est claire. Si maintenant on suppose que pour un certain $n \in \mathbb{N}^*$, l'égalité est vraie pour tout arbre ayant au plus n sommets, on considère G un arbre ayant $n+1$ sommets. Comme tout arbre peut être construit par récurrence , par l'ajout d'un sommet à un arbre plus petit qu'on connecte à un unique sommet déjà existant, on peut retirer exactement un sommet et une arrête à G et obtenir un arbre de n sommets. L'hyothèse de récurrence s'applique et on obtient le résultat souhaité.

Si maintenant G est seulement supposé connexe, on peut lui retirer des arrêtes sans le déconnecter jusqu'à obtenir un arbre. Donc G a au moins autant d'arrêtes qu'un arbre ayant le même nombre de sommets, d'où l'inégalité. Finalement, si G satisfait l'égalité, il est par contraposé impossible de lui retirer des arrêtes sans le déconnecter. Donc c'est un arbre. □

Ainsi, le premier terme mis entre parenthèse dans (112) est négatif ou nul, car le graphe maître est évidemment connexe. On contrôle le second terme de cette façon :

Lemme 11. *Pour $\pi \in \mathcal{P}(V)$, on a $\delta^\circ[T_W^\pi] = 0$, ou alors les arrêtes de T_W^π ont multiplicité au moins 2 (en ne tenant pas compte de l'orientation).*

Démonstration. $\delta^\circ[T_W^\pi]$ est un produit de moments des entrées des matrices de Wigner. Comme toutes ces entrées sont centrées et indépendantes, $\delta^\circ[T_W^\pi] = 0$ dès lors qu'une variable aléatoire apparaît une seule fois dans l'expression de $\delta^\circ[T_W^\pi]$. Or l'injectivité de Φ et le caractère hermitien des matrices de Wigner montrent que ce cas ne se produit que s'il existe une arrête de multiplicité 1 dans T_W^π, sans prendre en compte l'orientation. □

Bien entendu, seuls les termes pour lesquels $\delta^\circ[T_W^\pi] \neq 0$ nous intéressent. On suppose donc désormais que π satisfait cette condition. Dans ce cas, comme toutes les arrêtes de T_W^π sont au moins doubles, on a $|\bar{E}_W| \leqslant \frac{|E_W|}{2}$. Ceci achève la preuve du lemme 9. On a même un résultat un peu plus fort que cela, grâce à la caractérisation des arbres donnée par l'inégalité de connexité, en tenant compte du fait qu'asymptotiquement, seuls les termes pour lesquels $\eta(\pi) = 0$ contribuent au premier ordre :

Lemme 12. *Soit $\pi \in \mathcal{P}(V)$. Alors le terme $\tau^\circ[T^\pi]$ contribue à la trace combinatoire (i.e. $\delta^\circ[T_W^\pi] \neq 0$ et $\eta(\pi) = 0$) seulement si toutes les arrêtes de T_W^π sont exactement doubles et le graphe maître est un arbre.*

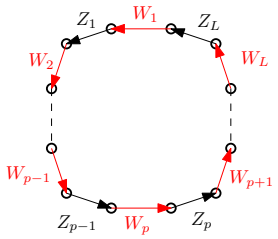
4.4 Etude d'une partition des arrêtes

Supposons que $\pi \in \mathcal{P}(V)$ contribue i.e. $\eta(\pi) = 0$ et $\delta^\circ[T_W^\pi] \neq 0$. Le lemme 12 permet de poser $\sigma(\pi) \in \mathcal{P}(E_W)$ une partition paire des arrêtes étiquetées par des matrices de Wigner définie de la façon suivante : deux arrêtes sont identifiées par $\sigma(\pi)$ si, et seulement si, leurs images dans T^π ont même source et même but, ou leur source et but sont intervertis.

L'objectif de cette partie est de donner une caractérisation des partitions π telles que $\sigma(\pi) = \sigma_0$ pour une certaine σ_0 donnée. En effet, la partition σ_0 suffit à déterminer entièrement le terme $\delta^\circ[T_W^\pi]$, aussi la connaissance de ces partitions nous permettra d'avancer sur la compréhension du terme $\tau[T]$.

Lemme 13. *Pour tout $\pi \in \mathcal{P}(V)$ telle que π contribue, $\sigma(\pi)$ est non-croisée.*

Démonstration. Pour la démonstration de cet énoncé, on considérera une forme réduite de T dans laquelle on assimilera les arrêtes de T consécutives étiquetées par des matrices déterministes à des arrêtes étiquetées par des produits, de sorte à avoir une alternance de matrices de Wigner et déterministes (voir figure ci-dessous).



Commençons par remarquer que cet énoncé a bien un sens en donnant une structure de poset à E_W. T, sous sa forme réduite, contenant $2L$ sommets, on peut toujours étiqueter ceux-ci par $1, \dots, 2L$, où 1 est choisi arbitraire. On notera alors $\bar{k}$ l'arrête $(k, k+1)$ si $k \leqslant 2L-1$, ou l'arrête $(2L, 1)$ si $k = 2L$. On décide que les arrêtes de E_W seront étiquetées par les éléments pairs, et on munit $E_W = \{\bar{2}, \dots \bar{2L}\}$ de l'ordre $\bar{2} < \cdots < \bar{2L}$.

Raisonnons par l'absurde et supposons $\sigma(\pi)$ croisée. Il existe donc $\bar{p_1} < \bar{q_1} < \bar{p_2} < \bar{q_2} \in E_W$ tels que $\bar{p_1} \sim_{\sigma(\pi)} \bar{p_2}$, $\bar{q_1} \sim_{\sigma(\pi)} \bar{q_2}$.

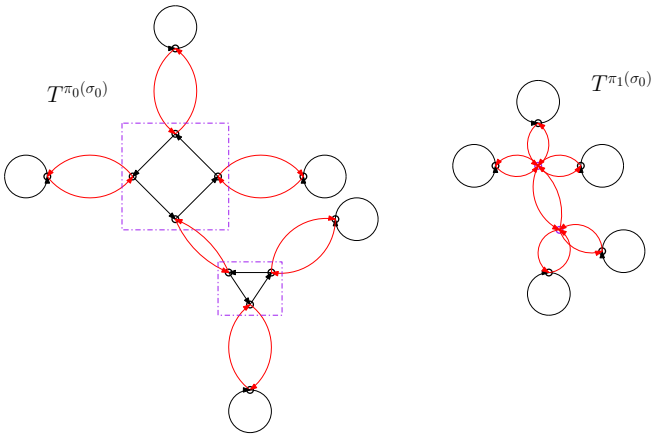
T étant un cycle simple, il existe un chemin reliant p_1 à p_2 suivant l'orientation du cycle et ne parcourant chaque qu'arrête qu'au plus une fois. Ce chemin induit clairement un chemin dans T^π et dans $\mathscr{T}(\pi)$, et quitte à lui ajouter une étape parcourant l'arrête $\bar{p_2}$, comme $\bar{p_1}$ et $\bar{p_2}$ sont identifiées dans $\mathscr{T}(\pi)$, le chemin induit dans $\mathscr{T}(\pi)$ a une source et un but confondus. Or, le choix de parcours du cycle et le fait que $\sigma(\pi)$ est paire montrent que $\bar{q_2}$ n'est pas parcourue dans T, et donc que l'arrête correspondant à $\bar{q_1}$ n'est parcourue qu'une unique fois dans $\mathscr{T}(\pi)$. Ceci suffit à montrer que le chemin induit dans $\mathscr{T}(\pi)$ contient une boucle, et donc que le graphe maître n'est pas un arbre. Ceci est absurde d'après le lemme 12. □

Lemme 14. *Soit $\sigma_0 \in NC_2(E_W)$ une partition paire non-croisée. Alors, il existe $\pi_0(\sigma_0) \in \mathcal{P}(V)$, $\pi_1(\sigma_1) \in \mathcal{P}(V)$ telle que :*

$$\{\pi \in \mathcal{P}(V) \mid \sigma(\pi) = \sigma_0\} = [\pi_0(\sigma_0) \ ; \ \pi_1(\sigma_1)]. \tag{114}$$

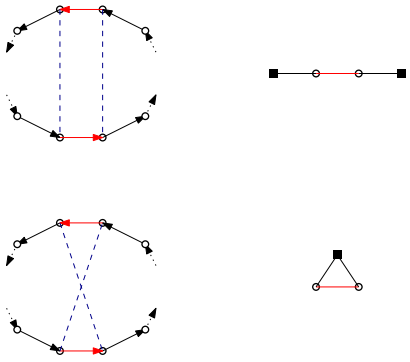
De plus, toutes les composantes connexes de $T_Y^{\pi_0(\sigma_0)}$ sont des cycles simples, et $T_Y^{\pi_1(\sigma_0)}$ est le graphe obtenu en identifiant tous les sommets de $T^{\pi_0(\sigma_0)}$ appartenant à une même composante de $T_Y^{\pi_0(\sigma_0)}$.

Donnons ici un exemple plus visuel (certaines arrêtes noires n'ont pas été représentées sur le graphe de droite pour plus de clareté) :



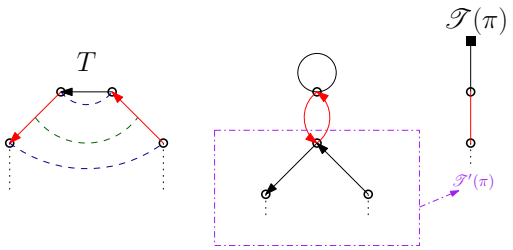
Démonstration (esquisse). On va procéder par récurrence sur l'entier n tel que $L = 2n$ (on se limite aux indices L pairs puisque σ_0 est une partition paire). On pose la proriété de récurrence suivante : $\mathscr{P}(n)$: «Si T est un cycle test ayant la forme souhaitée pour notre étude contenant exactement $2n$ arrêtes étiquetées par des matrices de Wigner, alors pour toute $\sigma_0 \in NC_2(E_W)$, le lemme 14 s'applique».

Pour $n = 1$, on peut simplement étudier tous les cas possibles : les deux seules arrêtes de E_W sont nécessairement appariées par σ_0, donc la discussion ne se fait qu'autour des sommets appariés par une partition π telle que $\sigma(\pi) = \sigma_0$. Si ces deux arrêtes sont notées (p_1, p_2) et (q_1, q_2), on a alors $p_1 \sim_\pi q_1$, $p_2 \sim_\pi q_2$ ou $p_1 \sim_\pi q_2$, $p_2 \sim_\pi q_1$. Or si π contribue, un seul de ces cas est possible, sans quoi le graphe maître n'est pas un arbre :



Avec en bleu les sommets identifiés par π (ces sommets peuvent être identifier à d'autres sommets non représentés ici). Il est alors clair, dans le cas du haut, correspondant au cas où π contribue, que π admet la décomposition souhaitée, sans quoi le graphe maître n'est pas un arbre. On pose dans ce cas π_0 la partition obtenue en ne faisant aucune identification supplémentaire des sommets. On pose également π_1 la partition obtenue en identifiant tous les sommets correpondant à une même composante connexe dans T^{π_0}. Il est alors aisé de montrer que $\mathscr{P}(1)$ est vraie avec $\pi_0(\sigma_0) = \pi_0$ et $\pi_1(\sigma_0) = \pi_1$.

Soit $n \in \mathbb{N}^*$ tel que $\mathscr{P}(n)$ est vraie. On suppose que $L = 2(n+1)$ et soit $\sigma_0 \in NC_2(E_W)$. On utilise alors la structure de σ_0 donnée par le théorème 1 : σ_0 admet un bloc segment. Une discussion simillaire à celle qui vient d'être menée pour le cas $n = 1$ montre qu'alors π ne peut qu'apparier les sommets de la façon suivante [(xiv)] :



Dans le cadre violet, on obtient un cycle ayant la même structure que les cycles étudiés, mais contenant $2n$ arrêtes étiquetées par des matrices de Wigner. De plus, comme $\mathscr{T}(\pi)$ est supposé être un arbre, on a nécessairement que le sous-graphe $\mathscr{T}'(\pi)$ est lui-même un arbre. Il convient alors d'observer que les partitions σ_0 et π induisent des partitions sur le cycle contenu dans le cadre violet, que $\mathscr{T}'(\pi)$ est le graphe maître de ce cycle pour la partition des sommets ainsi induite, et donc que ces deux partitions satisfont toutes les hypothèses de la propriété de récurrence. En appliquant $\mathscr{P}(n)$, pour les partitions ainsi induites, on retrouve facilement les partitions $\pi_0(\sigma_0)$ et $\pi_1(\sigma_0)$ permettant de déduire $\mathscr{P}(n+1)$. □

(xiv). Sur le graphique, en vert : les arrêtes appariées par σ_0, avec ici une vue sur un bloc segment. En bleu : les sommets appariés par π (plus de sommets peuvent être appariés à ceux représentés). Le graphe intermédiaire représente un début de construction du graphe T^{π} où l'on a identifié les sommets représentés sur le graphe de gauche, et seulement ceux là.

4.5 Calcul de la trace combinatoire

Nous avons désormais tous les outils pour conclure. Remarquons que la donnée d'une partition $\sigma_0 \in NC_2(E_W)$ détermine entièrement la valeur de $\delta^\circ[T_W^\pi]$, puisqu'une telle partition permet d'expliciter les différentes variables aléatoires, coefficients des matrices de Wigner, dont $\delta^\circ[T_W^\pi]$ est produit des moments d'ordre 2. Nous noterons donc $\delta^\circ(\sigma_0) := \delta[T_W^\pi]$, où π est telle que $\sigma(\pi) = \sigma_0$. Aussi une sommation par paquets permet d'écrire l'égalité suivante :

$$\tau[T] = \sum_{\pi \in \mathcal{P}(V)} \tau^\circ[T^\pi] \tag{115}$$

$$= \sum_{\sigma_0 \in NC_2(E_W)} \sum_{\substack{\pi \in \mathcal{P}(V) \\ \sigma(\pi) = \sigma_0}} \delta^\circ(\sigma_0) \tau^\circ[T_Y^\pi] + o(1) \tag{116}$$

Or, le terme $\tau^\circ[T_Y^\pi]$ est la trace injective d'un graphe non-connexe pris en des matrices déterministes. Aussi, le théorème 13 s'applique et on a :

$$\tau^\circ[T_\pi^Y] = \left(\prod_{C \in CC_Y(\pi)} \tau^\circ[C] \right) \left(1 + \mathcal{O}\left(\frac{1}{N} \right) \right) \tag{117}$$

où $CC_Y(\pi)$ désigne l'ensemble des composantes connexes de T_Y^π. En appliquant le lemme 14 à (116), on obtient :

$$\tau[T] = \sum_{\sigma_0 \in NC_2(E_W)} \delta^\circ(\sigma_0) \sum_{\substack{\pi \in \mathcal{P}(V) \\ \pi_0(\sigma_0) \leqslant \pi \leqslant \pi_1(\sigma_0)}} \left(\prod_{C \in CC_Y(\pi)} \tau^\circ[C] \right) \left(1 + \mathcal{O}\left(\frac{1}{N} \right) \right) + o(1) \tag{118}$$

Soit $\pi \in [\pi_0(\sigma_0) \ ; \ \pi_1(\sigma_0)]$. Alors nécessairement, π admet une décomposition :

$$\pi = \bigsqcup_{C_0 \in CC_Y(\pi_0(\sigma_0))} \pi_{C_0}, \tag{119}$$

où π_{C_0} est une partition des sommets V dont la classe d'équivalence par $\pi_0(\sigma_0)$ est un sommet de C_0 (ceci découle simplement de la majoration par $\pi_1(\sigma_0)$ et du lemme 14). Soit $C_0 \in CC_Y(\pi_0(\sigma_0))$. D'après le lemme 14, C_0 est un cycle simple. Soit $\pi \in [\pi_0(\sigma_0) \ ; \ \pi_1(\sigma_0)]$ qu'on décompose comme dans (119). Alors, à C_0 correspond une composante connexe C de $CC_Y(\pi)$, obtenue à partir des classes d'équivalences par π des sommets de T appartenants à aux classes d'équivalence par π_0 formant les sommets de C_0. On peut par ailleurs associer à π une unique partition $\bar{\pi}$ des élements de $\pi_0(\sigma_0)$ telle que pour B_1 et B_2 deux blocs de $\pi_0(\sigma_0)$:

$$B_1 \sim_{\bar{\pi}} B_2 \iff \exists B \in \pi \ : \ B_1 \sqcup B_2 \subset B \tag{120}$$

de par le fait que $\pi_0(\sigma_0) \leqslant \pi$. Dans ce cas, $\bar{\pi}$ induit une partition des sommets de C_0, et on a que $C = C_0^{\bar{\pi}}$. Réciproquement, on montre facilement qu'à toute partition $\bar{\pi}$ des sommets de $T^{\pi_0(\sigma_0)}$ correspond une unique partition $\pi \in [\pi_0(\sigma_0) \ ; \ \pi_1(\sigma_0)]$. Autrement dit :

$$\sum_{\substack{\pi\in\mathcal{P}(V)\\ \pi_0(\sigma_0)\leqslant\pi\leqslant\pi_1(\sigma_0)}}\left(\prod_{C\in CC_Y(\pi)}\tau^\circ[C]\right)=\left(\prod_{C_0\in CC_Y(\pi_0(\sigma_0))}\sum_{\bar\pi\in\mathcal{P}(V_{C_0})}\tau^\circ[C_0^{\bar\pi}]\right)\tag{121}$$

$$=\prod_{C_0\in CC_Y(\pi_0(\sigma_0))}\tau[C_0]\tag{122}$$

d'après la proposition 16. Ainsi qu'on l'a dit, les composantes connexes C_0 sont des cycles simples. Autrement dit, pour toute telle C_0, $\tau[C_0]$ est en fait un moment (non-commutatif) joint de la famille $\mathbb{Y}_N$.

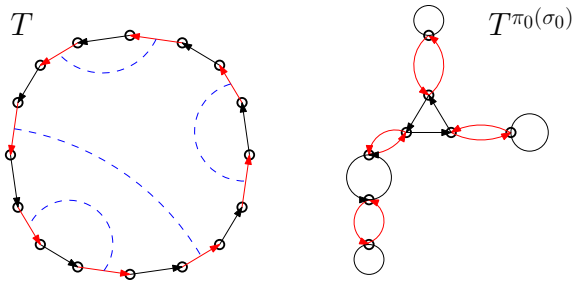
Pour conclure, nous allons rassembler les matrices de $\mathbb{Y}_N$ apparaissant consécutivement dans le calcul de $\tau[T]$, de sorte à écrire $\tau[T]=\varphi(W_1Z_1\dots W_LZ_L)$ (comme dans (104)). Alors, on assimile la partition σ_0 à une partition de $[\![L]\!]$ en identifiant les indices des matrices de $\mathbb{W}_N$ aux arrêtes qu'ils étiquettent. On peut observer qu'il existe une partition σ_0' de $[\![L]\!]$ telle que :

$$\prod_{C_0\in CC_Y(\pi_0(\sigma_0))}\tau[C_0]=\varphi_{\sigma_0'}[\mathbb{Y}_N]\ ^{(\text{xv})}.\tag{123}$$

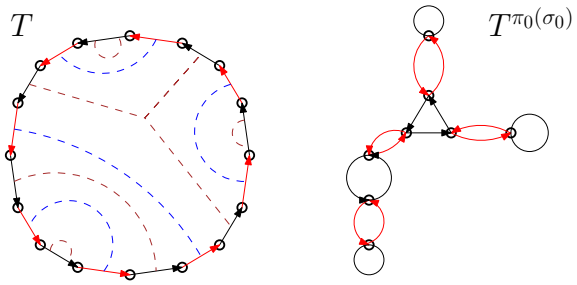
Cette partition correspond exactement à la partition de E_Y identifiant deux arrêtes si, et seulement si, elles appartiennent à la même composante connexe de $T_Y^{\pi_0(\sigma_0)}$.

Lemme 15. *La partition σ_0' est le dual de* Kreweras *de σ_0.*

Démonstration (esquisse). On va se contenter d'une approche graphique de ce dernier lemme. Une partition σ_0 de E_W peut être représentée de la façon suivante :



où on a relié en bleu les arrêtes appariées par σ_0 dans le cycle. On voit alors apparaître la partition σ_0' de la façon suivante :



(xv). Cette notation est celle introduite lors de la discussion portant sur les fonctionnelles multiplicatives en section 2.5

où les arrêtes appariées par σ_0' sont reliées en brun. Le dessin met clairement en valeur que σ_0' est non-croisée et que c'est la partition maximale telle que $\sigma_0 \sqcup \sigma_0' \in NC(\llbracket 2L \rrbracket)$, c'est-à-dire que $\sigma_0' = \mathcal{K}(\sigma_0)$. □

Grâce à ce dernier lemme, et à (122) et (123), on obtient finalement l'asymptotique suivante :

$$\tau[T] = \sum_{\sigma_0 \in NC_2(E_W)} \delta^\circ(\sigma_0) \varphi_{\mathcal{K}(\sigma_0)}[\mathbb{Y}_N] + o(1) \tag{124}$$

Puisqu'à renormalisation près, on peut toujours supposer que les entrées des matrices de Wigner sont réduites, on peut sans perte de généralité supposer que $\delta^\circ(\sigma_0) = 1$ pour toute partition σ_0 paire et non-croisée. Ceci montre l'existence d'une distribution non-commutative limite ! De plus, en passant à la limite $[N \to +\infty]$:

$$\lim_{N \to +\infty} \varphi(W_1 Z_1 \dots W_L Z_L) = \sum_{\sigma_0 \in NC_2(\llbracket L \rrbracket)} \varphi_{\mathcal{K}(\sigma_0)}[\mathbb{Y}_N]. \tag{125}$$

Or cette écriture vaut pour tout L et tous $(W_1, \dots W_L) \in \mathbb{W}_N$, $(Z_1, \dots Z_L) \in \mathrm{Alg}(\mathbb{Y}_N)$. On reconnait la forme décrite par le théorème 10 ! Ainsi, ce même théorème permet d'affirmer que la distribution limite des $\mathbb{W}_N$ est celle d'un système semi-circulaire libre et que les famille $\mathbb{W}_N$ et $\mathbb{Y}_N$ sont asymptotiquement libres. On a prouvé le théorème de liberté asymptotique !

★ ★

★

Références

[1] Greg W. Anderson, Alice Guionnet et Ofer Zeitouni. *An Introduction to Random Matrices*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2009.

[2] K. Dykema. « On Certain Free Product Factors via an Extended Matrix Model ». In : *Journal of Functional Analysis* 112.1 (1993), p. 31-60. issn : 0022-1236. doi : https://doi.org/10.1006/jfan.1993.1025. url : https://www.sciencedirect.com/science/article/pii/S0022123683710256.

[3] Alice Guionnet. *Large Random Matrices: Lectures on Macroscopic Asymptotics*. Springer, 2008. url : https://perso.ens-lyon.fr/aguionne/cours.

[4] *Introduction aux grandes matrices aléatoires*. url : https://www.math.univ-toulouse.fr/~capitain/M2RpolyWEB.pdf.

[5] Camille Male. *Traffic Distributions and Independence: Permutation Invariant Random Matrices and the Three Notions of Independence*. Memoirs of the American Mathematical Society 1300. American Mathematical Society, 2020. isbn : 978-1-4704-4298-9. url : https://www.ams.org/books/memo/1300/.

[6] James A. Mingo et Roland Speicher. « Asymptotic Freeness for Gaussian, Wigner, and Unitary Random Matrices ». In : *Free Probability and Random Matrices*. New York, NY : Springer New York, 2017, p. 93-120. isbn : 978-1-4939-6942-5. doi : 10.1007/978-1-4939-6942-5_4. url : https://doi.org/10.1007/978-1-4939-6942-5_4.

[7] Alexandru Nica et Roland Speicher. *Lectures on the Combinatorics of Free Probability*. London Mathematical Society Lecture Note 335. Cambridge university press, 2006. isbn : 978-0-521-85852-6.

[8] Dan Voiculescu. « Limit laws for Random matrices and free products ». In : *Inventiones mathematicae* 104 (1991).

[9] Eugene P. Wigner. « On the Distribution of the Roots of Certain Symmetric Matrices ». In : *Annals of Mathematics* 67.2 (1958), p. 325-327. issn : 0003486X, 19398980. url : http://www.jstor.org/stable/1970008 (visité le 13/08/2024).