Introduction aux probabilités libres

Nicolas Lim
sous la direction de Georges Skandalis

Juin 2002

1 Introduction

1.1 Motivations

Les probabilités libres interviennent dans l'étude des matrices aléatoires de grandes tailles (sous certaines conditions on démontre qu'une famille de matrices aléatoires est asymptotiquement libre). Elles interviennent aussi pour l'étude du groupe fondamental de $L(\mathbb{F}_\infty)$ (on définira cette notation dans la suite).

1.2 Différents types d'algèbres

Définition 1.1 On appelle $*$-algèbre ou algèbre involutive une algèbre A sur $\mathbb{C}$ munie d'une involution notée $x \mapsto x^*$ telle que :

$$\begin{aligned}(x+y)^* &= x^* + y^* \\ (\lambda x)^* &= \bar{\lambda} x^* \\ (xy)^* &= y^* x^*\end{aligned}$$

Définition 1.2 On dit qu'une $*$-algèbre est une C^*-algèbre si elle est munie d'une norme d'algèbre de Banach telle que $||xx^*|| = ||x||^2$.

Définition 1.3 Soit A une C^*-algèbre unitaire, soit φ un morphisme d'espace vectoriel conservant l'involution de A dans $\mathbb{C}$, on dit que φ est un état si $\varphi(1) = 1$ et si pour tout x de A $\varphi(xx^*) \geq 0$.

Définition 1.4 On dit qu'une C^*-algèbre est une W^*-algèbre si elle est isomorphe à une sous-C^*-algèbre d'un $\mathcal{B}(\mathcal{H})$ fermée pour la topologie faible.

Par la suite on travaillera toujours avec des algèbres unitaires. En particulier quand on parlera d'algèbre engendrée il s'agira toujours d'algèbre unitaire engendrée.

Pour plus de détails sur la théorie de ces algèbres, on pourra se référer à [1].

1.3 Espaces de probabilité non commutatifs

Définition 1.5 Un espace de probabilité non commutatif est une algèbre unitaire A sur $\mathbb{C}$ munie d'une forme linéaire $\varphi : A \to \mathbb{C}$ telle que $\varphi(1) = 1$.

Définition 1.6 Un espace de probabilité non commutatif (A, φ) est appelé un C^*-espace de probabilité si A est une C^*-algèbre et φ un état.

Définition 1.7 Un C^*-espace de probabilité non commutatif (A, φ) est appelé un W^*-espace de probabilité si A est une W^*-algèbre et si φ est un état ultra-faiblement continu [1].

1. cf. [1]

1.4 Variables aléatoires dans un espace de probabilité non commutatif

Définition 1.8 Si (A, φ) est un espace de probabilité non commutatif alors on appelle variable aléatoire tout élément f de A. La distribution de f est la forme linéaire μ_f sur $\mathbb{C}[X]$ définie par :

$$\mu_f \ : \ P \mapsto \varphi(P(f))$$

Remarque 1.1 L'analogie avec les probabilités classiques est évidente dans la mesure où la loi d'une variable aléatoire X est définie par la donnée de $\mathbb{E}(F(X))$ pour toute fonction continue F. Cependant on ne peut définir $F(f)$ si F n'est pas un polynôme dans le cas non commutatif, sauf dans des cas particuliers comme celui des C^*-espaces de probabilité. Le terme non commutatif venant du fait que les algèbres considérées ne sont en général pas commutatives.

Remarque 1.2 Dans le cas d'un C^*-espace de probabilité, prenons f dans A tel que $f = f^*$ alors le spectre de f est réel et borné donc compact; notons le K. On va alors montrer qu'il existe une mesure $d\mu_f$ sur K telle que :

$$\varphi(P(f)) = \int_K P(t) d\mu_f(t) \ \ \forall P \in \mathbb{C}[X]$$

On voit donc que $\left((C^0([a,b],\mathbb{C}), ||.||_\infty), \mu\right)$ est un exemple canonique de C^*-espace de probabilité non commutatif.

1.5 Liberté

Définition 1.9 Soit (A, φ) un espace de probabilité non commutatif. Soient $(A_i)_{i\in I}$ des sous-algèbres unitaires de A, elles sont dites libres si $\varphi(a_1 \dots a_n) = 0$ si $a_j \in A_{i_j} \cap \ker(\varphi)$ et $i_1 \neq i_2 \neq \cdots \neq i_n$ (cela signifiera que deux indices consécutifs sont distincts).

Remarque 1.3 Si $(A_i)_{i\in I}$ est libre et engendre A alors φ est entièrement définie par ses restrictions aux A_i. (On peut le voir dans la mesure où $a = b + \varphi(a)1$ où $\varphi(b) = 0$, on notera $\overset{\circ}{a}$ l'élément b)

Remarque 1.4 Soit $(A_i)_{i\in I}$ une famille de sous-algèbres unitaires d'une algèbre. Si on se donne des décompositions en somme directe $A_i = \mathbb{C}1 + \overset{\circ}{A}_i$, la famille des $\overset{\circ}{A}_i$ engendre la même algèbre que la famille des A_i.

On démontre d'autres énoncés techniques sur les probabilités libres (cf. [2]).

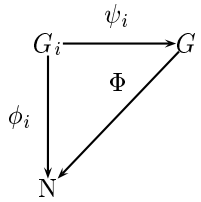
Définition 1.10 Soit (A, φ) un espace de probabilité non commutatif et soit $(a_i)_{i\in I}$ une famille d'éléments de A, on dit qu'elle est libre (resp. $*$-libre) si les algèbres unitaires (resp. les $*$-algèbres) engendrées sont libres.

2 Produits libres

La notion de probabilité libre est intimement liée à la notion de produit libre, qui permet de construire des familles libres de loi donnée. C'est donc l'analogue du produit tensoriel des mesures pour la notion d'indépendance.

2.1 Groupes

Définition 2.1 Soit $(G_i)_{i\in I}$ une famille de groupes, on appelle produit libre de cette famille et on note $*_{i\in I} G_i$ l'unique groupe G (à isomorphisme près) muni de morphismes $\psi_i : G_i \to G$ qui vérifie : quelque soit le groupe N et les morphismes $\phi_i : G_i \to N$, il existe un unique morphisme $\Phi : G \to N$ (noté $*_{i\in I}\phi_i$) tel que le diagramme suivant commute :



En effet si ce groupe existe il est unique (à isomorphisme près) comme élément universel pour la catégorie des groupes. Et on en a une représentation:

$$G = \{g_{i_1} \dots g_{i_n} \mid n \in \mathbb{N} \setminus \{0\}\ , g_{i_j} \in G_{i_j}\} \setminus \{e\} \cup \{\emptyset\}$$

muni de la multiplication par concaténation.

2.2 Algèbres unitaires

On définit de la même manière le produit libre d'algèbres unitaires: $*_{i\in I} A_i$ (qui est aussi un élément fondamental pour la catégorie des algèbres unitaires munies des morphismes unitaires). Il peut être vu comme l'algèbre engendrée par l'ensemble des mots dont l'alphabet est composé des éléments des A_i et munie de la multiplication par concaténation et de la simplification:

$$a_1 \dots a_{j-1}(\lambda a_j^{(0)} + \mu a_j^{(1)})a_{j+1} \dots a_n = \lambda a_1 \dots a_{j-1} a_j^{(0)} a_{j+1} \dots a_n + \mu a_1 \dots a_{j-1} a_j^{(1)} a_{j+1} \dots a_n$$

et le 1 est commun à tous les A_i.

Par ailleurs on voit sans difficulté que si $A_i = \mathbb{C}1 \oplus V_i$ en tant qu'espace vectoriel alors $*_{i\in I} A_i$ est isomorphe en tant qu'espace vectoriel à:

$$C = \mathbb{C}1 \oplus \bigoplus_{n\geq 1} \left(\bigoplus_{i_1 \neq i_2 \neq \dots \neq i_n} V_{i_1} \otimes \dots \otimes V_{i_n} \right)$$

2.3 Espaces de Hilbert

On regarde à présent la catégorie C des espaces de Hilbert munis d'un élément de norme 1 particularisé (noté $(\mathcal{H}, \xi)$) munis des morphismes d'espaces vectoriels $T: \mathcal{H}_1 \to \mathcal{H}_2$ tel que $||T|| \leq 1$ et $T\xi_1 = \xi_2$. On a alors $T^*\xi_2 = \xi_1$ (en effet $\langle \xi_1, T^*\xi_2 \rangle = 1$ et si $||x|| \leq 1$ alors $\langle x, T^*\xi_2 \rangle \leq 1$ donc $||T^*\xi_2|| \leq 1$ et on a bien $T^*\xi_2 = \xi_1$).

Définition 2.2 Soit $(\mathcal{H}_i, \xi_i)_{i\in I}$ une famille d'objets de C, leur produit libre noté $*_{i\in I}\mathcal{H}_i$ est $(\mathcal{H}, \xi)$ donné par:

$$H = \mathbb{C}\xi \oplus \bigoplus_{n\geq 1} \left(\bigoplus_{i_1 \neq i_2 \neq \dots \neq i_n} \overset{\circ}{\mathcal{H}}_{i_1} \otimes \dots \otimes \overset{\circ}{\mathcal{H}}_{i_n} \right)$$

où $\overset{\circ}{\mathcal{H}}_i = \mathcal{H}_i \ominus \mathbb{C}\xi_i$. Ici les sommes sont prises orthogonales et on a complété pour avoir un Hilbert.

Définition 2.3 (Espace de Fock) Soit $\mathcal{H}$ un espace de Hilbert. On appelle espace de Fock:

$$\mathcal{T}(\mathcal{H}) = \mathbb{C}1 \oplus \bigoplus_{n\geq 1} \mathcal{H}^{\otimes n}$$

Là encore les sommes sont orthogonales et on complète. Dans ce cadre 1 est dit vecteur vide.

On remarque que $\left(\mathcal{T}(\bigoplus_{i\in I} \mathcal{H}_i), 1\right) = *_{i\in I}(\mathcal{T}(\mathcal{H}_i), 1)$.

2.4 C^*-algèbres unitaires

Comme pour les algèbres unitaires on peut définir le produit libre dans la catégorie des C^*-algèbres unitaires munies des morphismes d'algèbres unitaires qui commutent avec l'involution comme élément fondamental de cette catégorie (en fait c'est la C^*-algèbre enveloppante du produit libre d'algèbres unitaires).

2.5 Représentations et états

Définition 2.4 (État produit libre) Soit $(A_i)_{i\in I}$ une famille de C^*-algèbres et φ_i des états sur les A_i. On peut alors construire les représentations GNS associées $\pi_i : A_i \to \mathcal{B}(\mathcal{H}, \xi_i)$ telle que $\varphi_i(a) = \langle \pi_i(a)\xi_i, \xi_i \rangle$. On peut alors construire une représentation $\pi = *_{i\in I}\pi_i$ du produit libre $A = *_{i\in I} A_i$ sur $(\mathcal{H}, \xi) = *_{i\in I}(\mathcal{H}_i, \xi_i)$. On définit l'état produit libre par $\varphi(a) = \langle \pi(a)\xi, \xi \rangle$.

Proposition 2.1 Les A_i sont libres dans $(*_{i\in I} A_i, \varphi)$.

On a donc déjà un premier exemple de famille libre. Par ailleurs l'état produit libre ainsi défini est le seul état qui donne une famille libre.

On peut de la même manière donner un sens aux produits libres d'algèbres de von Neumann

3 Analyse harmonique libre

3.1 Convolution libre additive

Définition 3.1 Soit x_1 et x_2 des variables aléatoires libres dans un espace de probabilité non commutatif (A, φ) de distribution μ_{x_1} et μ_{x_2}. On s'intéresse à la distribution $\mu_{x_1+x_2}$. On la notera $\mu_{x_1} \boxplus \mu_{x_2}$.

Remarque 3.1 On peut bien écrire $\mu_{x_1} \boxplus \mu_{x_2}$ car cette distribution ne dépend que de μ_{x_1} et de μ_{x_2}. En effet si l'on se donne un autre espace de probabilité non commutatif (B, ψ) et deux éléments libres a et b dans B qui ont pour distribution μ_{x_1} et de μ_{x_2}, alors la distribution de $a + b$ est la même que celle de $x_1 + x_2$ d'après la remarque 1.3.

Remarque 3.2 $\boxplus$ est donc commutative.

Exemple 1 Si μ_1 et μ_2 sont deux mesures à support compact sur $\mathbb{R}$ alors on peut les voir comme distributions de variables aléatoires libres autoadjointes et considérer $\mu_1 \boxplus \mu_2$ qui sera encore une mesure à support compact comme distribution d'une variable autoadjointe. (Il suffit de prendre le produit libre des deux espaces de fonctions C^0 munis des mesures sur les compacts supports et dans lesquels l'Id a les bonnes distributions).

Définition 3.2 On note Σ l'ensemble des formes linéaires de $\mathbb{C}[X]$ unitaires (i.e qui envoient 1 sur 1).

On verra par la suite que toute forme linéaire sur $\mathbb{C}[X]$ unitaire peut-être vu comme la distribution d'une variable aléatoire et qu'il existe des polynômes universels P_n tels que:

$$\mu_1 \boxplus \mu_2(X^n) = P_n(\mu_1(X), \dots, \mu_1(X^n), \mu_2(X), \dots, \mu_2(X^n))$$

Il est cependant très difficile de calculer explicitement $\mu_1 \boxplus \mu_2$ et cela n'a bien souvent aucun sens, en particulier dans le cas où l'on a deux mesures. On veut alors un résultat sous forme de mesure et non comme forme linéaire explicite sur $\mathbb{C}[X]$. Pour ce faire on va introduire la $\mathcal{R}$-transformée.

3.2 $\mathcal{R}$-transformée

3.2.1 Opérateurs de création

On va travailler ici dans des $*$-algèbres concrètes: ce sont des algèbres d'opérateurs sur des espaces de Fock ou sur des espaces de Fock algébriques.

Définition 3.3 Soit $\mathcal{H}$ un espace de Hilbert, alors son espace de Fock algébrique est défini comme son espace de Fock sauf que l'on ne complète pas les sommes. On le notera $\mathcal{T}_{al}(\mathcal{H})$. Mais on garde les $\mathcal{H}^{\otimes n}$ (i.e. les produits tensoriels complétés).

Définition 3.4 Soit $\mathcal{H}$ un espace de Hilbert et $x \in \mathcal{H}$ un élément de norme 1. On définit l'opérateur de création à gauche associé à e_1 comme:

$$\begin{aligned} l_x : \mathcal{T}(\mathcal{H}) &\to \mathcal{T}(\mathcal{H}) \\ 1 &\mapsto x \\ k_1 \otimes \cdots \otimes k_n &\mapsto x \otimes k_1 \otimes \cdots \otimes k_n \end{aligned}$$

$l_x \in \mathcal{B}(\mathcal{T}(\mathcal{H}))$ et $||l_x|| = 1$. Si on a une famille de vecteurs $(e_i)_{i\in I}$, on notera l_i l'opérateur de création à gauche associé au vecteur e_i.

On peut calculer l'adjoint de l_x :

$$\begin{aligned} l_x^*(1) &= 0 \\ l_x^*(k) &= \langle k, x\rangle 1 \\ l_x^*(k_1 \otimes \cdots \otimes k_n) &= \langle k_1, x\rangle k_2 \otimes \cdots \otimes k_n \end{aligned}$$

Remarque 3.3 On a $l_e^* l_f = \langle e, f\rangle \,\mathrm{Id}$.

Remarque 3.4 Il nous arrivera de faire agir l_x sur $\mathcal{T}_{al}(\mathcal{H})$, dans ce cas on notera encore l_x^* l'opérateur défini comme précédemment.

Définition 3.5 Soit $\mathcal{H}$ un espace de Hilbert de dimension N et de base orthonormée $(e_1, \ldots, e_n)$. On considère $\mathcal{E}_n$, l'$*$-algèbre des opérateurs agissant sur $\mathcal{T}_{al}(\mathcal{H})$ de la forme :

$$\sum_{\substack{0 \leq p \leq P \\ 0 \leq q}} \sum_{\substack{i_1, \ldots, i_p \\ j_1, \ldots, j_q \\ \in \{1, \ldots, n\}}} c_{i_1, \ldots, i_p ; j_1, \ldots, j_q} l_{i_1} \ldots l_{i_p} l_{j_1}^* \ldots l_{j_q}^*$$

munie de l'application linéaire ω_n qui associe à un tel opérateur le nombre $c_{\emptyset;\emptyset}$

Définition 3.6 On notera Ω l'élément 1 dans $\mathcal{T}(\mathcal{H})$ et on l'appellera vecteur vide.

Remarque 3.5 On a aussi $\omega_n(T) = \langle T(\Omega), \Omega \rangle$.

Proposition 3.1 Les deux variables aléatoires de $\mathcal{E}_2$ suivantes sont libres :

$$\begin{aligned} T_1 &= l_1 + \sum_{k=0}^{\infty} \alpha_{k+1} (l_1^*)^k \\ T_2 &= l_2 + \sum_{k=0}^{\infty} \beta_{k+1} (l_2^*)^k \end{aligned}$$

3.2.2 Une représentation de $(\Sigma, \boxplus)$

Proposition 3.2 Quelque soit $\mu \in \Sigma$, il existe une unique variable aléatoire dans $\mathcal{E}_n$ de la forme $l_1 + \sum_{n=0}^{\infty} \alpha_n (l_1^*)^k$ qui a pour distribution μ.

Définition 3.7 ($\mathcal{R}$-transformée au sens de Voiculescu) Voiculescu appelle alors la série

$$\sum_{n=0}^{\infty} \alpha_n z^n$$

la $\mathcal{R}$-transformée de μ. On la notera plutôt ici $\mathcal{R}^0$-transformée.

Cependant (même si les polynômes L_n sont connus), cette définition n'est pas pratique car il est assez difficile de calculer $\mathcal{R}^0$. On voit cependant immédiatement que la fonction $\mu \mapsto \mathcal{R}^0$ est un morphisme de groupe de $(\Sigma, \boxplus)$ dans $(\mathcal{E}_n, +)$. On privilégiera alors l'approche de Haagerup.

3.3 $\mathcal{R}$-transformée : l'approche de Haagerup

Haagerup a une démarche légèrement différente de celle de Voiculescu : il définit la $\mathcal{R}$-transformée à partir de séries explicites sur la distribution à considérer.

On se place dans une $*$-algèbre $\mathcal{A}$ munie d'une application linéaire φ de $\mathcal{A}$ dans $\mathbb{C}$ telle que $\varphi(1) = 1$ et on se donne une variable aléatoire a dans $\mathcal{A}$ et on considère sa distribution μ_a.

Remarque 3.6 On est amené à travaillé dans l'ensemble des séries symboliques $\mathbb{C}[[z][z^{-1}]]$ qui est un groupe s'il est muni de la composition. Quand on parlera d'inverse ce sera toujours au sens de la composition.

Définition 3.8 Pour a fixé on définit la série symbolique :

$$G(\lambda) = \sum_{n=0}^{\infty} \lambda^{-n-1} \mu_a(X^n)$$

L'inverse de G a alors un sens et est de la forme :

$$G^{-1}(z) = \frac{1}{z} + \sum_{n=0}^{\infty} \alpha_n z^n,$$

et la $\mathcal{R}$-transformée est définie par :

$$\mathcal{R}_{\mu_a}(z) = G^{-1}(z) - \frac{1}{z}$$

Remarque 3.7 Le choix de G n'est pas fortuit : elle apparaît comme une extension de la transformée de Cauchy. En effet si la distribution considérée est une mesure μ à support compact alors :

$$G(\lambda) = \int_{\mathbb{R}} \frac{d\mu(t)}{\lambda - t}$$

et dans le cas général d'une algèbre de Banach, on a :

$$G(\lambda) = \varphi((\lambda - a)^{-1}) \ \ \forall |\lambda| \geq ||a||$$

Remarque 3.8 Pour le théorème qui suit on considère des opérateurs sur $\mathcal{T}(H)$ de la forme $a = l_i + f(l_i)^*$ où f est un polynôme. L'état sur un $\mathcal{B}(\mathcal{T}(\mathcal{H}))$ est $T \mapsto \langle T\Omega|\Omega\rangle$. La distribution de a dans $\mathcal{B}(\mathcal{T}(\mathcal{H}))$ est la même que dans $\mathcal{E}_n$ (pour $n \geq i$). De plus les résultats de liberté sont conservés.

Théorème 3.1 1) Soit f un polynôme et soit

$$a = l_1 + f(l_1^*)$$

$\mathcal{R}_{\mu_a}(z) = f(z)$, $z \in \mathbb{C}$.
2) Si f et g sont deux polynômes et

$$\begin{aligned} a &= l_1 + f(l_1^*) \\ b &= l_2 + f(l_2^*) \end{aligned}$$

alors a et b sont libres
3) et

$$\mathcal{R}_{\mu_a} + \mathcal{R}_{\mu_b} = \mathcal{R}_{\mu_{a+b}}$$

Théorème 3.2 Les assertions du théorème 3.1 restent vraies si on remplace f par n'importe quelle série formelle $\sum_{k=0}^{\infty} \alpha_k z^k$ et g par $\sum_{k=0}^{\infty} \beta_k z^k$ (où α_k et $\beta_k \in \mathbb{C}$).
On obtient aussi l'identité entre $\mathcal{R}^0$-transformée et $\mathcal{R}$-transformée.

Corollaire 3.1 Soit a et b deux variables aléatoires libres dans un espace de probabilité non commutative :

$$\mathcal{R}_{a+b} = \mathcal{R}_a + \mathcal{R}_b$$

Corollaire 3.2 $\mathcal{R}$ est un isomorphisme du groupe $(\Sigma, \boxplus)$ dans le groupe des séries formelles.

3.4 Du bon usage de la $\mathcal{R}$-transformée

Le calcul de la $\mathcal{R}$-transformée apparaît donc comme un moyen simple d'obtenir $\mu_1 \boxplus \mu_2$ sous forme de mesure quand μ_1 et μ_2 sont des mesures (ou bien quand l'on s'attend à trouver une mesure). Le procédé est le suivant :

- Calculer la transformée de Cauchy.
- Inverser les séries qu'on a trouvées.
- Les sommer.
- Les inverser à nouveau.
- Calculer la transformée de Cauchy inverse

3.5 Théorème de la limite centrale libre

Il existe un analogue du théorème de la limite centrale dans le cadre des probabilités libres c'est le résultat énoncé à la fin de ce paragraphe.

Définition 3.9 (Loi du demi-cercle) On appelle loi du demi-cercle centrée en a et de rayon $r > 0$ la distribution définie par :

$$\gamma_{a,r}(P) = \frac{2}{\pi r^2} \int_{a-r}^{a+r} P(t)\sqrt{r^2 - (t-a)^2}dt$$

Ces lois jouent un rôle équivalent à celui des gaussiennes dans le cas des probabilités classiques.

Remarque 3.9 On voit immédiatement que $\gamma_{a,r} \boxplus \gamma_{b,s} = \gamma_{a+b,\sqrt{r^2+s^2}}$

Théorème 3.3 (Représentation de la loi du demi-cercle) La variable aléatoire $a = l_1 + l_1^*$ a pour distribution la mesure $d\mu = (2\pi)^{-1}\phi(t)dt$ où ϕ est la fonction à support dans $[-2, 2]$ définie par $\phi(t) = \sqrt{4 - t^2}$.

Démonstration : Comme a est autoadjoint on sait que sa distribution est une mesure à support compact sur $\mathbb{R}$.

On a $\mathcal{R}(z) = z$ donc $G(\lambda) = \frac{\lambda - \sqrt{4-\lambda^2}}{2}$. L'inversion de la transformée de Cauchy nous dit alors que μ a pour densité :

$$\lim_{y \to 0^+} -\frac{1}{\pi} \Im G(x + iy) = (2\pi)^{-1}\phi(x)$$

Définition 3.10 On dit qu'une suite (μ_n) de distributions converge "en distribution" vers μ si :

$$\forall P \in \mathbb{C}[X], \quad \mu_n(P) \underset{n\to\infty}{\to} \mu(P)$$

Théorème 3.4 (Théorème de la limite centrale) Soit (A, φ) un espace de probabilité non commutatif et soit $(a_j)_{j\in\mathbb{N}^*}$ une suite de variables aléatoires libres dans A telles que :

- (i) $\varphi(a_j) = 0 \ \forall j \geq 1$;
- (ii) $\sup_{j\geq 1} |\varphi(a_j^k)| < \infty \ \forall k \geq 2$;
- (iii) $\lim_{n\to\infty} \frac{1}{n} \sum_{j=1}^n \varphi(a_j^2) = \frac{r^2}{4} > 0$.

Alors si $s_n = \frac{1}{\sqrt{n}}(a_1 + \cdots + a_n)$ alors la suite $(s_n)_n$ converge en loi vers la loi du demi-cercle $\gamma_{0,r}$.

3.6 Convolution libre multiplicative

Le même genre de raisonnement peut être fait pour l'étude de la distribution du produit ab de deux éléments. On obtient alors l'existence de ce que l'on appelle la $\mathcal{S}$-transformée qui est multiplicative. On note la loi de ab : $\mu_a \boxtimes \mu_b$.

4 Lois infiniment divisibles

De même qu'en théorie classique des probabilités il existe des mesures infiniment divisibles, il existe des mesures infiniment divisibles pour la loi $\boxplus$ et la loi $\boxtimes$. On sait les caractériser dans certains cas par une propriété analogue à celle de la formule de Lévy-Khinchine pour la transformée de Laplace.

Théorème 4.1

- Une mesure $\mu \in \mathbf{M}_\mathbb{R}$ est $\boxplus$-infiniment divisible si et seulement si sa $\mathcal{R}$-transformée admet un prolongement analytique au voisinage de $(\mathbb{C} \setminus \mathbb{R}) \cup \{0\}$ tel que $\Im\mathcal{R}(z) \geq 0$ si $\Im z > 0$.
- Soit $\mathcal{R}$ une fonction analytique au voisinage de $(\mathbb{C} \setminus \mathbb{R}) \cup \{0\}$ telle que $\mathcal{R}(\bar{z}) = \overline{\mathcal{R}(z)}$ et $\Im\mathcal{R}(z) \geq 0$ si $\Im z > 0$. Alors $\mathcal{R}$ est la $\mathcal{R}$-transformée d'une mesure $\boxplus$-infiniment divisible $\mu \in \mathbf{M}_\mathbb{R}$.
- Soit $\mu \in \mathbf{M}_\mathbb{R}$ qui est $\boxplus$-infiniment divisible et soit $\mathcal{R}_\mu$ sa $\mathcal{R}$-transformée. Alors :

$$\mathcal{R}_\mu(z) = \alpha + \int_\mathbb{R} \frac{z}{1 - tz} d\nu(t) \ \forall z \in (\mathbb{C} \setminus \mathbb{R}) \cup \{0\}$$

où α et la mesure positive ν se trouvent comme suit : Soit $\{\mu_t | t \geq 0\} \subset \mathbf{M}_\mathbb{R}$ tel que $\mathcal{R}_{\mu_t}(z) = t\mathcal{R}_\mu(z)$. Alors :

$$\alpha = \lim_{\epsilon\to 0} \frac{1}{\epsilon} \int_\mathbb{R} t d\mu_\epsilon(t)$$

et ν est la limite faible-$*$ de la suite : $\frac{1}{\epsilon} t^2 d\mu_\epsilon$.

Ce théorème ce montre essentiellement en étudiant les propriétés d'analycité de la $\mathcal{R}$-transformée. Par ailleurs on a le même genre de théorème pour la convolution $\boxtimes$ sur le cercle unité de $\mathbb{C}$ ou sur $\mathbb{R}_+$.

5 Matrices aléatoires et liberté asymptotique

Définition 5.1 Soit (Ω, Σ, μ) un espace de probabilité, on note $\mathbb{L} = \bigcap_{1 \leq p < \infty} \mathbb{L}^p(\Omega)$. L'ensemble des matrices aléatoires de taille $n \times n$ sera alors

$$(\mathcal{M}_n, \phi_n) = (\mathbb{L} \otimes M_n(\mathbb{C}), \mathbb{E} \otimes \tau_n)$$

où τ_n est la trace normalisée : $\frac{1}{n}\mathrm{Tr}$.

Définition 5.2 (Liberté asymptotique)
Soit $(T_i^{(n)})_{i \in I}$ une suite de familles de variables aléatoires chacune dans (A_n, ϕ_n). On dit que la suite des distributions jointes $(\mu_{(T_i^{(n)})_{i \in I}})_{n \in \mathbb{N}}$ converge vers μ si :

$$\mu_{(T_i^{(n)})_{i \in I}}(P) \underset{n \to \infty}{\to} \mu(P) \ \ \forall P \in \mathbb{C}\langle X_i | i \in I \rangle$$

Définition 5.3 Soit $I = \bigcup_{j \in J} I_j$ une partition de I. Une suite de familles $(T_i^{(n)} | i \in I_j)_{j \in J}$ d'ensembles de variables aléatoires est dite asymptotiquement libre quand n tend vers l'infini si elle possède une distribution limite μ et si $(X_i | i \in I_j)_{j \in J}$ est libre dans $(\mathbb{C}\langle X_i | i \in I \rangle, \mu)$.

Le principal théorème qu'a montré Voiculescu sur les matrices aléatoires de ce type est le suivant :

Théorème 5.1 (Matrices symétriques à coefficients complexes gaussiens)

- Soit
$$Y(s,n) = \sum_{1 \leq i,j \leq n} a(i,j;n,s) e(i,j;n) \in \mathcal{M}_n$$
pour $s \in \mathbb{N}$ et telles que $a(i,j;n,s) = \overline{a(i,j;n,s)}$ et :
$$\{\Re a(i,j;n,s) \mid 1 \leq i \leq j \leq n, s \in \mathbb{N}\} \cup \{\Im a(i,j;n,s) \mid 1 \leq i \leq j \leq n, s \in \mathbb{N}\}$$
est une famille de variables aléatoires indépendantes. Et plus précisément : si $i \neq j$ $\Re a(i,j;n,s)$ et $\Im a(i,j;n,s)$ suivent la loi $\mathcal{N}(0, \frac{1}{2n})$ et les $a(i,i;n,s)$ suivent la loi $\mathcal{N}(0, \frac{1}{n})$.
- Soit $(D(t,n))_{t \in \mathbb{N}} \subseteq \Delta_n$ où $\Delta_n \subseteq 1 \otimes M_n(\mathbb{C})$ est l'algèbre des matrices diagonales de tailles $n \times n$ dont les coefficients sont des constantes. Supposons que $(D(t,n))_{t \in \mathbb{N}}$ aie une distribution limite et que $\sup_n ||D(t,n)|| < \infty$ pour tous les t. Alors la famille :
$$(\{D(t,n) | t \in \mathbb{N}\}, \{Y(1,n)\}, \{Y(2,n)\}, \ldots$$
est asymptotiquement libre et la distribution limite de chaque $Y(i,n)$ est une loi du demi-cercle $\gamma_{0,1}$.

Les matrices aléatoires jouent un grand rôle dans la théorie des probabilités libres et plus particulièrement dans leurs applications à la théorie des sous-facteurs du groupe libre à une infinité de générateurs.

Définition 5.4 Si G est un groupe au plus dénombrable, $l^2(G)$ est un espace de Hilbert de base orthonormale $\{\delta_g \mid g \in G\}$. On peut alors considérer $\tau(G)$ l'ensemble des translations à gauche agissant sur $l^2(G) : \tau_g(\delta_h) = \delta_{gh}$. Alors $\tau(G) \subset \mathcal{B}(l^2(G))$. On appellera $L(G) = (\tau(G))''$ l'algèbre de von Neumann engendrée par $\tau(G)$.

Définition 5.5 On appelle $\mathbb{F}_\infty$ le groupe libre à une infinité (dénombrable) de générateurs l'ensemble des éléments α de $\mathbb{R}^+ \setminus \{0\}$ tels qu'il existe $e \in \mathbb{F}_\infty \otimes \mathcal{B}(l^2(\mathbb{F}_\infty))$ de trace α tel que :

$$e(\mathbb{F}_\infty \otimes \mathcal{B}(l^2(\mathbb{F}_\infty)))e \simeq \mathbb{F}_\infty$$

On peut notamment démontrer le théorème suivant dû à Radulescu :

Théorème 5.2 Le groupe fondamental de $\mathbb{F}(\mathbb{N})$ est $\mathbb{R}_+^*$.

Toute cette théorie s'appuie essentiellement sur la proposition suivante :

Proposition 5.1 Soit (A, ϕ) et (B, ψ) deux C^*-algèbres (resp. W^*-algèbres) dont les représentations GNS sont fidèles et telles qu'on possède $(f_i)_{i \in I}$ une famille génératrice de A et $(g_i)_{i \in I}$ une famille génératrice de B qui ont la même $*$-distribution. Alors il existe un isomorphisme de C^*-algèbres (resp. W^*-algèbres) γ de A dans B tel que $\phi = \psi \circ \gamma$ et $\forall i \in I \ \gamma(f_i) = g_i$.

Cette proposition dit qu'il suffit d'étudier un exemple de variable aléatoire qui a la distribution μ pour en déduire un ensemble de propriétés (pas uniquement liées à la distribution comme l'inversibilité, la positivité...) de toute variable aléatoire qui a pour distribution μ et qui est dans une C^*-algèbre.

6 Une autre démonstration pour la $\mathcal{R}$-transformée et la $\mathcal{S}$-transformée

6.1 Préliminaires

Lemme 6.1 Soit M une série formelle non commutative à m variables et P un polynôme non commutatif à m variables. Alors l'opérateur

$$a = M(l_1^*, \ldots, l_m^*) + P(l_1, \ldots, l_m)$$

est bien défini de $\mathcal{T}_{al}(\mathcal{H})$ dans lui-même. Il en est de même de

$$b = P(l_1, \ldots, l_m)M(l_1^*, \ldots, l_m^*)$$

Démonstration : Dans les deux expressions précédentes, les séries infinies mises en jeu sont bien définies comme on les fait agir sur des tenseurs de longueur finie donc les termes de la séries sont nulles au bout d'un certain rang. On peut donc dire que c'est les limites des séries tronquées pour la topologie faible associée à la topologie discrète sur $\mathcal{T}_{al}(\mathcal{H})$.

Définition 6.1 On note ici $\mathcal{M}$ l'ensemble des séries de Laurent formelles, i.e. des :

$$\sum_{k=-n}^{\infty} \alpha_k z^k$$

C'est un corps pour le + et le $\times$ usuels.

Définition 6.2 Pour tout élément $m \in \mathcal{M}$, on notera $\nu(m)$ sa valuation. En particulier $\nu(0) = \infty$.

Le recours à la notation sous forme de série n'implique en rien qu'on définit z comme élément de $\mathbb{C}$: c'est la convention usuelle.

On sera amené à travailler dans les $\mathcal{M}$-espaces vectoriels V_m définis par :

$$V_m = \left\{ \sum_{n=0}^{\infty} \sum_{\substack{i_1, \ldots, i_n \\ \in \{1, \ldots, m\}}} m_{i_1, \ldots, i_n}(z) e_{i_1} \otimes \cdots \otimes e_{i_n} \mid \lim_{n \to \infty} \nu(m_{i_1, \ldots, i_n}) = \infty \right\}$$

muni de la topologie métrique associée à la distance suivante :

$$d(x, y) = \exp(-\nu(x - y))$$

où $\nu(x)$ est la plus petite valuation des coefficients de x.

On a une autre représentation de V_m :

$$V_m = \{ \sum_{k=-N}^{\infty} z^k x_k \mid N \in \mathbb{N},\ x_k \in \mathcal{T}_{al}(\mathcal{H}) \}$$

et alors si $x = \sum_{k=-N}^{\infty} z^k x_k$, $\nu(x)$ est le plus petit k tel que x_k soit non nul (et c'est ∞ si $x = 0$).

Lemme 6.2 V_m est complet quelque soit $m \in \mathbb{N}$.

Démonstration : Soit (y_n) une suite de Cauchy dans V_m. On utilise la représentation de V_m que l'on vient de donner pour dire que le coefficient de z^k est constant au bout d'un certain rang et on note cette constante x_k (en effet donnons nous un rang n tel que $\nu(x_n - x_{n+p}) \geq k_0 + 1$ pour tout $p \in \mathbb{N}$ alors le coefficient de z^k reste constant à partir du rang n pour tout $k \leq k_0$). De même la valuation est elle aussi constante à partir d'un certain rang et vaut N. Notons :

$$y = \sum_{k=-N}^{\infty} z^k x_k \in V_m$$

alors la suite (y_n) converge vers y.

Lemme 6.3 Soit T linéaire de $\mathcal{T}_{al}(\mathcal{H})$ dans lui-même, on peut la prolonger en une application linéaire continue de V_m dans lui-même (qu'on appellera toujours T).

Démonstration : Il suffit de poser :

$$T(\sum_{-N}^{\infty} z^k x_k) = \sum_{-N}^{\infty} z^k T(x_k)$$

et comme cette application augmente la valuation, elle est 1-lipschitzienne.

Lemme 6.4 Soit T $\mathcal{M}$-linéaire et continu sur V_m, alors il existe une unique famille d'opérateurs (T_k) qui stabilisent $\mathcal{T}_{al}(\mathcal{H})$ tels que :

$$T = \sum_{k=-M}^{\infty} z^k T_k$$

(la somme étant prise au sens de la convergence faible).

Lemme 6.5 Réciproquement, tout opérateur de la forme précédente est bien défini (i.e. la somme converge bien pour la topologie forte).

Démonstration du lemme 6.4 : il suffit de considérer les applications T_k définie comme prolongements à V_m des applications $\Pi_k T_{|\mathcal{T}_{\mathrm{al}}(\mathcal{H})}$ (ou Π_k est la fonction définie de V_m dans $\mathcal{T}_{\mathrm{al}}(\mathcal{H})$ par $\sum_{k=-N}^{\infty} z^k x_k \mapsto x_k$).

On remarque qu'alors T_k est nulle pour k assez petit. En effet : supposons que l'on aie des $k \in \mathbb{Z}$ aussi petit que l'on veut tels que $T_k \neq 0$ et choisissons $(x_k)_{k\in\mathbb{Z}^-} \in (\mathcal{T}_{al}(\mathcal{H}))^{\mathbb{N}}$ tel que la suite $(T_k(x_k))_{k\in\mathbb{Z}^-}$ ne soit pas pas presque nulle et telle que $(\sum_{n=0}^{l} T_{-n}(x_{-n}))_{l\in\mathbb{N}}$ ne soit jamais nulle à partir d'un certain rang (ce qui est bien possible puisque les $T_k(x_k)$ ne sont pas tous nuls et que l'on peut multiplier chaque x_k par un scalaire non nul). Alors si l'on pose pour $p \in \mathbb{N}$:

$$y_p = \sum_{n=0}^{p} z^n x_{-n} \in V_m$$

On obtient que (y_p) est une suite de Cauchy (donc convergente) mais que :

$$T(y_p) = \sum_{n=0}^{p} z^n T(x_{-n})$$

n'est pas de Cauchy puisque si $p \neq q$ et $T_p(x_p) \neq 0$ et $T_q(x_q) \neq 0$ alors $\nu(T(y_p) - T(y_q)) \leq 0$ (pourvu que p et q soient assez grands). Or on a supposé que T était continue donc ce n'est pas possible. On a donc bien démontré le lemme 6.4 :

$$T = \sum_{k=-M}^{\infty} z^k T_k$$

et l'unicité est donnée par l'application de T aux éléments de la forme $e_{i_1} \otimes \cdots \otimes e_{i_n}$.

Démonstration du lemme 6.5 : Prenons :

$$x = \sum_{n=-N}^{\infty} z^n x_n$$

et appliquons lui :

$$U_l(x) = \sum_{k=-M}^{l} z^k T_k(x) = y_l$$

alors (y_l) est de Cauchy puisque pour $p > 0$ et $l \geq 0$:

$$y_{l+p} - y_l = \sum_{k=l+1}^{l+p} z^k T_k(x)$$

et donc :

$$\nu(y_{l+p} - y_l) \geq \nu(x) + (l+1) \underset{l\to\infty}{\to} \infty$$

Donc T est bien définie comme limite des U_l dans la topologie faible. Et par ailleurs il est continu (et même $\exp(-M)$-lipschitzien). Le fait que la topologie métrique soit plus fine que la topologie forte est alors évident.

On peut alors munir $\mathcal{L}(V_m)$ de la distance :

$$d(T,S) = \exp(-\nu(T-U))$$

où $\nu(T)$ est la valuation de T (i.e. le plus petit k tel que T_k soit non nuls si $T \neq 0$ et ∞ sinon). On se place dorénavant dans cette topologie qui est plus fine que la topologie faible.

Proposition 6.1 $\mathcal{L}(V_m)$ munie de cette topologie métrique est complet.

Démonstration : Soit U_n une suite de Cauchy de $\mathcal{L}(V_m)$ alors on peut écrire :

$$U_n = \sum_{k=-M_n}^{\infty} z^k T_k^{(n)}$$

et pour k fixé, la suite $T_k^{(n)}$ est constante et vaut un certain T_k à partir d'un certain rang : il suffit de prendre un rang n tel que $\nu(U_{n+p} - U_n) \geq k+1$. On remarque que M_n est lui aussi constant à partir d'un certain rang et vaut M. Et alors on pose :

$$U = \sum_{k=-M}^{\infty} z^k T_k$$

U est bien limite des U_n.

Proposition 6.2 Soit $(S_k)_{k \geq -M}$ une suite d'opérateurs de valuation minorée agissant sur V_m alors l'opérateur :

$$T = \sum_{k=-M}^{\infty} z^k S_k$$

est bien défini (i.e. il y a bien convergence pour la topologie métrique).

Démonstration : posons $L = \min\{\nu(S_k) \mid k \geq -M\}$ et :

$$U_l = \sum_{k=-M}^{l} z^k S_k$$

alors $\nu(U_{l+p} - U_l) \geq l + L$ donc la suite des U_l est de Cauchy et donc converge vers T qui est alors bien défini.

Définition 6.3 On sera amené à travailler dans les espaces de probabilité non commutatif $\mathcal{L}_m$ des opérateurs sur les V_m munis des formes linéaires $\varphi_m(T) = \pi_m(T\Omega)$ où Ω est le vecteur vide (i.e. 1) et :

$$\pi_m \ : \ \sum_{n=0}^{\infty} \sum_{\substack{i_1,\ldots,i_n \\ \in \{1,\ldots,m\}}} m_{i_1,\ldots,i_n}(z) e_{i_1} \otimes \cdots \otimes e_{i_n} \mapsto m_\emptyset$$

Lemme 6.6 Dans $\mathcal{L}_2$, si on se donne $M_1, \ldots, M_n$ des séries formelles non commutatives en deux variables alors :

$$\varphi_2\left(M_1(l_1^*, l_2^*)(l_1+l_2)\ldots M_n(l_1^*, l_2^*)(l_1+l_2)\right) = \varphi_2(M_1(l_1^*, l_1^*)l_1 \ldots M_n(l_1^*, l_1^*)l_1)$$

Démonstration : on le montre par récurrence sur n.
Premier cas : $n = 0$ est évident (0 des deux côtés). Passage de n à $n+1$: Écrivons : $M_1(X,Y) = B_1(X,Y)X + C_1(X,Y)Y + a_1$ alors :

$$\begin{aligned} M(l_1^*, l_2^*)(l_1+l_2) &= a_1(l_1+l_2) + B_1(l_1^*, l_2^*) + C_1(l_1^*, l_2^*) \\ M(l_1^*, l_1^*)l_1 &= a_1 l_1 + B_1(l_1^*, l_1^*) + C_1(l_1^*, l_1^*) \end{aligned}$$

Or comme comme $(l_1+l_2)M_2(l_1^*, l_2^*)(l_1+l_2)\ldots M_n(l_1^*, l_2^*)(l_1+l_2)\Omega$ appartient à $x_1 \otimes \mathcal{T}_{\text{al}}(\mathcal{H}) + x_2 \otimes \mathcal{T}_{\text{al}}(\mathcal{H})$ et $l_1 M_2(l_1^*, l_1^*)l_1 \ldots M_n(l_1^*, l_1^*)l_1\Omega$ appartient à $x_1 \otimes \mathcal{T}_{\text{al}}(\mathcal{H})$, on aboutit en utilisant l'hypothèse de récurrence.

Proposition 6.3 Les distributions de $l_1 + l_2 + f(l_1^*) + g(l_2^*)$ et de $l_1 + f(l_1^*) + g(l_1^*)$ (où f et g sont des séries formelles) sont identiques.

C'est une conséquence immédiate du lemme précédent.

6.2 Démonstration algébrique de l'additivité de la $\mathcal{R}$-transformée

On se place dans le $\mathcal{M}$-espace vectoriel :

$$V_1 = \left\{ \sum_{n=0}^{\infty} m_n(z) e_1^{\otimes n} \mid \lim_{n\to\infty} \nu(m_n) = \infty \right\}$$

On notera :

$$\begin{aligned} \omega_z &= \sum_{n=0}^{\infty} z^n e_1^{\otimes n} \\ \Omega &= e_1^{\otimes 0} = 1 \end{aligned}$$

Et on notera :

$$\pi_1 : \sum_{n=0}^{\infty} m_n(z) e_1^{\otimes n} \mapsto m_0 \in \mathcal{M}$$

On travaillera désormais dans l'espace de probabilité non commutatif des opérateurs sur V_1 muni de la forme linéaire :

$$\varphi \ : \ T \mapsto \pi_1(T\Omega)$$

On notera l_1 la translation vers la droite l_1^* la translation vers la gauche (i.e. on reprend la définition donnée précédemment).

On s'intéresse aux opérateurs de la forme :

$$a = l_1 + f(l_1^*)$$

où f est une série formelle (i.e. il n'y a que des monômes analytiques). Et on note μ_a sa distribution. Il agît bien sur V_1 d'après le lemme 6.3

Proposition 6.4 Soit $T = \frac{1}{z} + zf(z) - a$, alors T est inversible.

En effet, il suffit de montrer que l'opérateur :

$$U = \sum_{p=0}^{\infty} z^p (a - f(z))^p$$

est bien défini. Mais c'est bien le cas grâce à la proposition 6.2.

Proposition 6.5 La $\mathcal{R}$-transformée de a est f.

Si on reprend formellement la démonstration de Haagerup on trouve que :

$$a\omega_z = \left(\frac{1}{z} + f(z)\right)\omega_z - \frac{1}{z}\Omega$$

et donc finalement en inversant et en appliquant φ, on trouve :

$$\varphi\left(\left(\left(\frac{1}{z} + f(z)\right) - a\right)^{-1}\right) = z$$

Il ne reste plus qu'à voir que :

$$\varphi((z-a)^{-1}) = G(z)$$

mais cela est impossible de façon directe (i.e. en utilisant la définition de G que donne Voiculescu) puisque l'on devrait trouver un élément qui est dans $\mathbb{C}[[z][z^{-1}]] \setminus \mathcal{M}$ (si μ_a n'est pas presque nulle) alors qu'a priori on ne veut travailler que dans $\mathcal{M}$. Pour cela on va montrer que la série formelle $G\left(\frac{1}{z}\right)$ convient, i.e. :

$$\varphi\left(\left(\frac{1}{z} - a\right)^{-1}\right) = G\left(\frac{1}{z}\right)$$

Mais cela est évident :

$$\left(\frac{1}{z} - a\right)^{-1} = z(1 - az)^{-1} = z\sum_{n=0}^{\infty} z^n a^n$$

est bien défini d'après la proposition 6.2 et :

$$\pi_1\left(z\sum_{n=0}^{\infty} z^n a^n \Omega\right) = \sum_{n=0}^{\infty} z^{n+1}\mu_a(X^n) = G\left(\frac{1}{z}\right)$$

On a donc bien le résultat énoncé dans la proposition précédente.

Références

[1] Pedersen, C^*-algebras and their automorphism group.

[2] Voiculescu, D.V, Free random variables, CRM monographs series, 1992.