Processus de Lévy libre sur des groupes duaux et matrices aléatoires
Introduction au Domaine de Recherche

Michaël Ulrich
Sous la direction d'Uwe Franz [1]

15 octobre 2013

1. Professeur à l'Université de Franche-Comté

Table des matières

Résumé

Ce document vise à introduire le domaine des probabilités libres et à tracer quelques liens avec les matrices aléatoires. Il s'attachera en particulier à définir la notion de processus de Lévy dans le contexte non-commutatif. Il fournira ainsi des éléments permettant de comprendre le contexte de la thèse commencée par l'auteur et qui s'intitule : "Processus de Lévy libre sur des groupes duaux et matrices aléatoires" [1].

1. Je souhaite tout particuliérement utiliser cette occasion pour remercier toutes les personnes qui m'ont accompagnées au cours de ma scolarité à l'ENS et m'ont fait partager leur goût pour les Mathématiques... Des remerciements particuliers vont à ceux qui ont encadré mes mémoires ou thèse : Grégory Miérmont, Lorenzo Zambotti et Uwe Franz.

Chapitre 1

Une théorie des probabilités non commutatives

1.1 Introduction

Nous allons briévement réintroduire le concept de probabilités non-commutatives. L'idée de base est que pour un espace de probabilités "classique" $(\Omega, \mathcal{F}, \mathbb{P})$, l'ensemble des variables aléatoires forment une algèbre qui est bien sûr commutative. On cherche alors à définir une théorie des probabilités sur une algèbre qui n'est plus forcément commutative. On peut ainsi donner une première définition :

Définition 1 *On appelle espace de probabilité non commutatif un couple (A, τ) où A est une algèbre unitaire et τ une forme linéaire unitaire.*

Citons deux exemples de tels espaces :

- L'ensemble des variables aléatoires réelles "classiques" sur Ω, muni de l'espérance, est un espace de probabilités non-commutatif (c'est normal, on l'a défini pour cela !).
- On prend $A = \mathcal{M}_n\left(L^{\infty-}(\Omega)\right)$, l'algèbre des matrices dont les coefficients sont des variables aléatoires ayant tous leurs moments de tous ordres finis et on le munit de la forme

$$\tau(M) = \frac{1}{n}\mathbb{E}\left[Tr(M)\right]$$

.

Remarque 1 *Selon le cas, on peut imposer de la structure supplémentaire sur A. On peut ainsi définir :*

- *un espace de probabilité non commutatif et involutif si on impose qu'il existe une involution $*$ sur A et que $\tau(XX^*)$ est positif (ou nul).*

– *un C^*-espace de probabilité si on impose que A est une C^*-algèbre (et que τ est continue et vérifie la proprieté de positivité précédente)*
– *un W^*-espace de probabilité si on impose que A est une algèbre de von Neumann et τ vérifie les propriétés précédentes.*

On peut en plus montrer que si X est un élément auto-adjoint d'un des espaces définis précédemments, alors il a une "loi au sens classique", c'est-à-dire qu'il existe une mesure de probabilité μ telle que pour tout k entier :

$$\tau\left(X^k\right) = \int x^k d\mu\left(x\right)$$

Remarque 2 *Rappelons rapidement ici, pour éclairer les définitions qui viennent d'être données, ce que l'on entend par des C^*-algèbres et des W^*-algèbres :*
Une C^*-algèbre est une algèbre normée munie d'une involution, notée $*$, et telle que pour tous X et Y de A : $||XY|| \leq ||X||\,||Y||$,$||X^*|| = ||X||$,$||XX^*|| = ||X||^2$
Il se trouve que l'on peut toujours voir une telle algèbre comme une sous-algèbre de $B\left(H\right)$, algèbre des opérateurs bornés sur un certain espace de Hilbert, via ce que l'on appelle la constructionde Gelfand-Naimark-Segal, ou GNS en abrégé.
Soit A une sous-algèbre de $B\left(H\right)$, alors on dit que A est une algèbre de von Neumann si elle est fermée pour les semi-normes :

$$X \mapsto |<\zeta, X\eta>|, \zeta, \eta \in H$$

On peut alors définir une notion analogue à celle de l'indépendance dans le cas classique. On l'appellera ici la liberté.

Définition 2 *Soient A_1 et A_2 des sous-algèbres de A. On dira que A_1 et A_2 sont libres si pour tout $n \in \mathbb{N}$, tout $X_1, \ldots X_n$ tel que :*
– *Pour tout $i \in \{1, \ldots, n\}$, $\tau\left(X_i\right) = 0$*
– *Pour tout i, X_i est pris dans A_{j_i} avec $j_1 \neq j_2 \neq \ldots \neq j_n$*

Alors :

$$\tau\left(X_1 \ldots X_n\right) = 0$$

Remarque 3 *On remarque que si A_1 et A_2 sont libres, alors on connait la valeur de τ sur le produit libre*[1] *des deux algèbres simplement en la connaissant sur chacune d'elles. En effet, pour $X \in A_1, Y \in A_2$:*

$$\tau\left(XY\right) \quad = \quad \tau\left(\left(X - \tau\left(X\right)\right)\left(Y - \tau\left(Y\right)\right)\right) + \tau\left(X\right)\tau\left(Y\right)$$

1. Sans vouloir rentrer dans les détails techniques de la définition du produit libre de deux algèbres unitaires, on peut intuitivement considérer la chose comme l'ensemble des combinaisons linéaires de mots de longueurs quelconque formés à partir des éléments des deux algèbres et en identifiant les unités respectives.

Remarque 4 *On peut se poser la question de savoir combien il existe de définitions possibles du concept d'indépendance. En termes algébriques, on souhaite se donner un règle qui à une fonctionnelle ϕ_1 sur A_1 et une fonctionelle $\phi 2$ sur A_2 associe une fonctionelle, notée $\phi_1 \odot \phi 2$, sur le produit libre. Quitte à imposer quelques conditions supplémentaires, qui paraissent d'ailleurs logiques, tel que le fait que si A_1 est indépendant de A_2, alors A_2 est aussi indépendant de A_1, on peut montrer qu'il n'y a qu'une seule définition possible pour le cas d'algèbres commutatives : c'est l'indépendance utilisée par les probabilistes, également appelée indépendance tensorielle.*
Dans le cas général non-commutatif, il existe deux possibilités : l'indépendance tensorielle et la liberté que nous venons de définir !
Il est assez satisfaisant - et en même temps fascinant ! - de voir qu'il est possible de montrer par des moyens purement algébriques que l'indépendance utilisée par les probabilistes est la "seule bonne" notion possible dans le contexte considéré.

On peut également définir une notion de convergence en distribution : si (X_n) est une suite à valeurs dans l'algèbre et si X est un élément de l'algèbre, on dit que cette suite converge en distribution vers X si pour tout entier p, on a :

$$\phi\left(X_n^p\right) \to \phi\left(X^p\right)$$

A partir de ces, on peut développer toute une théorie des probabilités libres qui possède de grands parallèles avec la théorie classique des probabilités. Cependant, alors que dans le cas classique, la loi gaussienne occupe un rôle prépondérant, ce rôle est rempli ici par la loi dite semicirculaire, c'est-à-dire :

$$d\mu\left(x\right) = \frac{1}{\pi}\sqrt{4-x^2}\mathbf{1}_{[-2,2]}dx$$

En particulier, il est par exemple possible de prouver un théorème central limite libre [2] : toute suite d'éléments X_i libres [3], ayant la même distribution (ie dans ce cas caractérisée par la famille $\left(\tau\left(X^k\right)\right)_{k\in\mathbf{N}}$), d'espérance nulle et de variance unité ($\tau\left(X\right)=0$) vérifie :

$$\frac{X_1+\ldots X_n}{\sqrt{n}} \to C$$

où C est une loi semicirculaire et où la convergence se fait en distribution (c'est-à-dire que l'on a en fait la convergence des τ-moments). On le voit, la ressemblance avec le cas classique est frappante !

2. Ce théorème est, par exemple, prouvé dans [3]
3. On dit que des éléments sont libres si les algèbres engendrées par ces éléments le sont.

1.2 Cumulants

On peut définir une notion de cumulants (des fonctions qui caractérisent une loi) qui se comporte "bien" par rapport à la liberté. Nous allons les définir comme des fonctions $\kappa_n : A^n \to \mathbb{C}$. Notons également par NC^n l'ensemble des partitions non-croisées de $\{1, \ldots, n\}$.
Ces fonctions sont définies par les relations suivantes : pour tous $a_1, \ldots, a_n$ dans A :

$$\tau(a_1 \ldots a_n) = \sum_{\pi \in NC^n} \kappa_\pi(a_1, \ldots, a_n)$$

où on a noté $\kappa_\pi(a_1, \ldots, a_n) = \prod \kappa_{|V_i|}(V_i)$ où l'on a écrit la partition π sous la forme $\pi = (V_1, \ldots, V_k)$.
On a alors en particulier les deux propriétés suivantes :
D'abord, les κ_n sont linéaires. Ensuite, on montre qu'il existe une fonction μ, dite fonction de Möbius de NC^n telle que :

$$\kappa_n(a_1, \ldots, a_n) \sum_{\pi \in NC^n} \phi_\pi(a_1, \ldots, a_n)\, \mu(\pi)$$

L'intérêt de l'introduction de ces cumulants est qu'ils se comportent bien au regard de la liberté. En effet, on peut montrer que $X_1, \ldots, X_n$ est libre si et seulement si $\kappa_n(X_{i_1}, \ldots, X_{i_n}) = 0$, pour tout n et dès qu'il existe deux indices consécutifs différents.
En particulier, si X et Y sont libres, alors :

$$\kappa_n(X + Y, \ldots, X + Y) = \kappa_n(X, \ldots, X) + \kappa_n(Y, \ldots, Y)$$

car tous les autres termes sont croisés et par la remarque précédente sont nuls.

1.3 Lien avec les matrices

Les matrices ont des liens forts avec la théorie des probabilités libres et on verra en particulier qu'elles donnent lieu à des familles libres lorsqu'on fait tendre la taille vers l'infini.On s'intéresse aux matrices du GUE : il s'agit de matrices aléatoires X hermitiennes de taille n dont les coefficients vérifient :

$$\begin{aligned} X_{k,l} &= \alpha_{k,l} + i\beta_{k,l} \\ X_{l,l} &= \gamma_{l,l} \end{aligned}$$

où les $\beta_{k,l}$ et $\alpha_{k,l}$ sont des gaussiennes réelles centrées et de variance $\frac{1}{2n}$ et les $\gamma_{l,l}$ sont des gaussiennes centrées de variance $\frac{1}{n}$. On se place dans le cadre évoqué précédemment de $A = M_n(L^{\infty-}(\Omega))$ muni de $\tau = \frac{1}{n}\mathbb{E} \circ Tr$. Soit m

un entier naturel et X une matrice du GUE [4]. En notant P_n l'ensemble des appariements de n entiers, on a :

$$\begin{aligned}\tau\left(X^m\right) &= \frac{1}{n}\sum_{i_1,\ldots,i_m}\mathbb{E}\left(x_{i_1,i_2}\ldots x_{i_m,i_1}\right)\\ &= \frac{1}{n}\sum_{i_1,\ldots,i_m}\sum_{\pi\in P_m}\prod_{(r,s)\in\pi}\mathbb{E}\left(x_{i_r,i_{r+1}}x_{i_s,i_{s+1}}\right)\\ &= \frac{1}{n^{1+m/2}}\sum_{\pi}\sum_{i_1,\ldots,i_m}\prod_{(r,s)\in\pi}\delta_{i_r,i_{s+1}}\delta_{i_{r+1},i_s}\end{aligned}$$

Où on utilisé une formule, que l'on appelle formule de Wick, pour passer de la première ligne à la seconde.
On peut identifier un appariement π avec une permutation de la manière suivante : si (r,s) appartient à π, on définit alors $\pi(r)=s$ et $\pi(s)=r$. On pose en outre γ la permutation $(123\ldots n)$.Et donc :

$$\sum_{i_1,\ldots,i_n}\prod_{r=1}^{n}\delta_{i_r,i_{\gamma\pi(r)}}=N^{|\gamma\pi|}$$

où $|\gamma\pi|$ désigne le nombre de cycles de $\gamma\pi$.Au final, on obtient l'expression : $\tau\left(X^m\right)=\sum_\pi N^{|\gamma\pi|-1-m/2}$.
Or, on peut montrer que $|\gamma\pi|-1-m/2$ est nul si π est un appariement non-croisé, strictement négatif sinon. Par conséquent, lorsque n tend vers l'infini, on a que $\tau\left(X^m\right)$ tend vers le nombre d'appariements non-croisés de $\{1,\ldots,m\}$, où l'on reconnait les moments de la loi-semicirculaire.
Cependant, on peut également refaire ce raisonnement avec une famille $X_1,\ldots,X_k$ de matrices du GUE, indépendantes entre elles. Le raisonnement est le même à ceci près qu'un indice supplémentaire apparait afin de différencier les éléments de matrices différentes. Comme les matrices sont indépendantes, les espérances du type $\mathbb{E}\left(x^{(\alpha)}_{i_r,i_{r+1}}x^{(\beta)}_{i_s,i_{s+1}}\right)$ sont nuls si α et β, qui indiquent de quelle matrice il s'agit, sond différents. On peut traduire cela en terme d'appariements qui respectent la "couleur". En notant $NC_2\left(p_1,\ldots,p_m\right)$ le nombre d'appariements non-croisés de $p_1+\ldots+p_m$ points, dont p_1 de la couleur 1, p_2 de la couleur 2, etc. et qui respectent ces couleurs (ainsi, on refuse d'apparier, par exemple, un point de couleur 1 avec un autre de couleur 3...). Alors :

$$\tau\left(X_1^{p_1}\ldots X_k^{p_k}\right)=\left|NC_2\left(p_1,\ldots,p_k\right)\right|$$

On reconnait là les moments de k éléments semicirculaires libres. On a donc bien le résultat que des matrices gaussiennes indépendantes sont asymptotiquement libres.

4. Pour plus de détails, se référer à [4]

On remarquera en outre que si on prend une famille de matrices $(X_i)_{i\geq 0}$ réalisant un mouvement brownien matriciel (à valeur dans les matrices symétriques), on obtient asymptotiquement, lorsque la dimension tend vers l'infini, un mouvement brownien libre (techniquement, on parle de mouvement brownien additif libre), c'est-à-dire un processus X_t qui satisfait les axiomes suivants :

- X_t est de loi semicirculaire de paramètre t.
- X_{t-s} est de même loi que $X_t - X_s$ pour tous t, s.
- $X_{t_1}, X_{t_2} - X_{t_1}, \ldots, X_{t_n} - X_{t_{n-1}}$ sont libres pour tous $0 \leq t_1 \leq \ldots \leq t_n$ et tout n entier.

On voit que cette définition est assez naturelle lorsqu'on connait celle du mouvement brownien "classique".

Chapitre 2

Le concept de groupe dual

2.1 Motivation

Dans le cas classique, on peut définir la notion de processus de Lévy, dont le "bon" cadre de définition est celui de groupe (voire de semigroupe). (X_t) est un processus de Lévy sur le groupe G si :

- $X_0 = e$ presque sûrement, où e désigne l'élément unité de G.
- $X_{t_1}, X_{t_2}^{-1} X_{t_1}, \ldots, X_{t_n}^{-1} X_{t_{n-1}}$ sont indépendants pour tous $0 \leq t_1 \leq \ldots \leq t_n$ et tout n entier.
- $X_s^{-1} X_t$ a la même loi que X_{t-s} pour tous $0 \leq s \leq t$.
- X_t converge vers e en probabilité lorsque t tend vers 0 (continuité faible).

L'idée est que l'on souhaite profiter du cadre non-commuitatif pour généraliser autant que possible cette définition. On va pour cela définir une catégorie d'objets plus vaste que les groupes.

2.2 Une première généralisation : la notion de groupe quantique

La notion de groupe est une des plus simples notions que l'on puisse rencontrer en algèbre, et est en même temps une structure extrêmement riche. On cherche à généraliser cette notion via une idée analogue à la généralisation du commutatif au non-commutatif précédemment employée.
Soit G un groupe. On considère $E = \mathcal{C}(G)$ l'ensemble des applications de G à valeurs complexes. On peut alors y définir ce que l'on appelle une comultiplication :

$$\begin{aligned} \Delta \quad : \quad & E \to E \otimes E \simeq \mathcal{C}(G \otimes G) \\ & f \mapsto \{(x,y) \mapsto f(xy)\} \end{aligned}$$

On remarque en particulier que cette comultiplication est coassociative, c'est-à-dire :

$$(\Delta \otimes Id) \circ \Delta = (Id \otimes \Delta) \circ \Delta$$

Cela provient directement de l'associativité de la multiplication sur G. On peut alors définir à partir de là la notion de groupe quantique compact.

Définition 3 *Un couple (A, Δ) est appelé groupe quantique compact si A est une C^*-algèbre et $\Delta : A \to A \otimes A$ est un $*$-morphisme unitaire coassociatif et tel que :*

$$\Delta(A)(1 \otimes A) \subseteq A \otimes A$$

soit dense.

Cette définition n'est cependant pas entiérement satisfaisante dans notre contexte. En fait, raisonner avec le produit tensoriel constitue une limitation dans notre situation car si $A \otimes A$ est bien canoniquement dotée d'une structure d'algèbre, les éléments issus du "premier" A commutent avec ceux issus du "second". Pour être dans le cas le plus général, nous devrons recourir au produit libre d'algèbre et définir ainsi la notion de groupe dual, telle qu'elle avait été défini par Voiculescu.

2.3 Produit libre et groupe dual

Soient E_1 et E_2 deux algèbres. Nous allons en définir le produit libre, qui correspond intuitivement à l'algèbre engendrée par les mots de longueur quelconque que l'on peut former en prenant arbitrairement des "lettres" dans chaque E_i. Formellement :
On définit $\mathbb{A}_m$ comme l'ensemble des m-uplets $(\epsilon_1, \ldots, \epsilon_m)$ tels que $\epsilon_i \neq \epsilon_{i+1}$, pour tout i. On pose : $\mathbb{A} = \cup_m \mathbb{A}_m$. Alors :

$$\begin{aligned} E_1 \sqcup E_2 &= \bigoplus_{\epsilon \in \mathbb{A}} E_\epsilon \\ E_\epsilon &= E_{\epsilon_1} \otimes \ldots \otimes E_{\epsilon_m} \end{aligned}$$

On nomme $E_1 \sqcup E_2$ le produit libre des deux algèbres. On voit que cela correspond à la notion intuitive donnée précédemment. On constate en outre que si l'on a bien une injection canonique j_1 de E_1 dans $E_1 \sqcup E_2$ (et de même J_2 pour E_2), les images de ces algèbres ne commutent plus, comme ce fut le cas pour le produit tensoriel.
Cette notion de produit libre se traduit aussi au niveau des morphismes par une propriété universelle : soient $f_1 : E_1 \to F$ et $f_2 : E_2 \to F$ deux morphismes d'algèbres, avec F une algèbre quelconque, alors il existe un et un seul morphisme, noté $f_1 \sqcup f_2 : E_1 \sqcup E_2 \to F$ tel que $f_1 \sqcup f_2 \circ j_k = f_k$ pour k valant 1 ou 2.
De même, pour $f_1 : E_1 \to F_1$ et $f_2 : E_2 \to F_2$, avec des notations évidentes,

on définit $f_1 \coprod f_2 : E_1 \sqcup E_2 \to F_1 \sqcup F_2$ en utilisant la propriété universelle précédentes. Informellement, cette application agit sur E_1 comme f_1 et sur E_2 comme f_2, où l'on identifie E_i avec son image dans $E_1 \sqcup E_2$.
Nous pouvons à présent définir la généralisation souhaitée.

Définition 4 *Un semigroupe dual est un couple (A, Δ) se composant d'une $*$-algèbre A et d'un $*$-morphisme $\Delta : A \to A \sqcup A$ tel que :*

$$\begin{aligned} \left(\Delta \coprod Id\right) \circ \Delta &= \left(Id \coprod \Delta\right) \circ \Delta \\ \left(0 \coprod Id\right) \circ \Delta = Id &= \left(Id \coprod 0\right) \circ \Delta \end{aligned}$$

Si de plus, il existe un morphisme $\Sigma : A \to A$, que l'on appelera coïnverse, vérifiant :

$$(\Sigma \sqcup Id) \circ \Delta = 0 = (Id \sqcup \Sigma) \circ \Delta$$

On parle alors de groupe dual.

Vu ce qui a été fait à la section précédente, on comprend relativement bien pourquoi on a choisi ces définitions et pourquoi on appelle cela un groupe dual, car on a utilisé cette notion de dualité en comparant avec ce qui se passe pour des groupes "classiques". Fournissons un exemple de tels groupes duaux. Soit V un espace vectoriel. On construit alors $T(V)$ l'algèbre tensorielle de V de la manière suivante :

$$T(V) = \mathbb{C} \oplus V \oplus (V \otimes V) \oplus (V \otimes V \otimes V) \oplus \dots$$

que l'on munit d'une structure d'algèbre via :

$$(v_1 \otimes \dots v_k, w_1 \otimes \dots w_p) \mapsto v_1 \otimes \dots \otimes v_k \otimes w_1 \otimes \dots \otimes w_p$$

On peut alors munir $T(V)$ d'une structure de groupe dual, via :

$$\begin{aligned} \Delta : v \in V &\mapsto v^{(1)} + v^{(2)} \\ \Sigma : v \in V &\mapsto -v \end{aligned}$$

où l'on étend Δ et Σ à tout $T(V)$ via la propriété de morphisme et où les exposants (1) et (2) indiquent si l'élément v appartient à la composante V "gauche" ou "droite" de $T(V) \sqcup T(V)$ [1].

1. En réalité, $T(V)$ est une algèbre unitaire. On peut définir la notion de produit libre d'algèbres unitaires et par suite de groupe dual unitaire. C'est le bon contexte pour l'algèbre tensorielle de V, mais pour ne pas alourdir outre mesure ce texte de présentation, nous avons décidé de ne pas nous attarder sur ces détails techniques.

2.4 Retour sur les processus de Lévy

Nous avons à présent tous les outils pour définir la notion de processus de Lévy sur les groupes duaux [2].

Définition 5 *Soient (B, Δ, Σ) un groupe dual et (A, τ) un espace de probabilité non commutatif, tel que défini plus haut dans ce texte. Soit une famille $(j_s)_{s\geq 0}$ de $*$-morphismes [3] de B dans A. On dit que c'est un processus de Lévy si :*

- $j_t(b) = 0$ *pour tout* b.
- j_t *est libre de l'algèbre engendrée par les* $\{j_u, u \leq t\}$.
- $\lim_{t\to 0} \tau \circ j_t(b) = 0$
- $[(f_s \circ \Sigma) \sqcup f_t] \circ \Delta$ *a la même loi que* j_{t-s} *pour tous* $0 \leq s \leq t$.

On reconnait la similarité que ces notions entretiennent avec la définition "classique" d'un processus de Lévy.

2. Comme pour le cas "classique", où on pouvait définir en toute généralité la notion de processus de Lévy sur des semigroupes, on peut également ici les définir sur des semigroupes duaux. Cependant, toujours dans le souci de présenter l'idée de manière claire sans s'alourdir de détails technique, nous privilégions ici la notion de groupe dual.

3. C'est une définition généralisée de la notion de variable aléatoire non commutative. On remarque en effet que dans le cas classique, une variable aléatoire X est une application (mesurable) de Ω, espace de probabilité, dans un groupe G par exemple. A toute application f de $\mathcal{C}(G)$, on peut alors associer une application de $\mathcal{C}(\Omega)$ par composition avec X. C'est l'idée sous-jacente à cette notion de variable aléatoire "généralisée" non-commutative.

Bibliographie

[1] Anis Ben Ghorbal and Michael Schuermann. Non-commutative notions of stochastic independence. *Math. Proc. Camb. Phil. Soc.*, 133 :531, 2002.

[2] Philippe Biane. Free brownian motion, free stochastic calculus and random matrices. *Fiels Institute Communications*, 12, 1997.

[3] A. Nica and R. Speicher. *Lectures on the Combinatorics of Free Probability.* 2006.

[4] Micha¨ el Ulrich. Une introduction à la théorie des matrices aléatoires. Master's thesis, Université Pierre et Marie Curie (Paris), 2012.

[5] Stefan Voss. *Realisierung von Quanten-Lévy-Prozessen auf Fockräumen.* PhD thesis, Ernst-Moritz-Arndt-Universität Greifswald, 2013.