Probabilités libres et matrices aléatoires

Motivé par des problèmes de classification d'algèbres d'opérateurs, Voiculescu a inventé des outils de nature probabiliste qui se sont révélés très utiles pour comprendre la structure des matrices aléatoires de grande taille. Ainsi, en utilisant la théorie de Voiculescu, on peut avec une bonne précision et une faible chance de se tromper, prédire la forme du spectre de la somme de deux grandes matrices hermitiennes, en connaissant seulement le spectre de chacune d'elles.

Diagonaliser des matrices hermitiennes est une activité courante aussi bien en mathématiques qu'en physique. Il arrive souvent que la matrice à diagonaliser se présente sous la forme d'une somme de deux matrices hermitiennes A et B dont on connaît les spectres. L'ensemble de tous les spectres possibles pour $A+B$ peut être déterminé explicitement en fonction de ceux de A et B. Par exemple, il est facile de voir que si A et B sont des matrices 2×2 et si, en écrivant les valeurs propres dans l'ordre décroissant, on a $Sp(A)=\{\lambda_1,\lambda_2\}$ et $Sp(B)=\{\mu_1,\mu_2\}$, alors on a

$$Sp(A+B)=\{\nu_1,\nu_2\}$$

où ν_1 et ν_2 vérifient

$$\begin{aligned}&\nu_1+\nu_2=\lambda_1+\lambda_2+\mu_1+\mu_2\\&|(\lambda_1-\lambda_2)-(\mu_1-\mu_2)|\leqslant\nu_1-\nu_2\\&\nu_1-\nu_2\leqslant\lambda_1-\lambda_2+\mu_1-\mu_2.\end{aligned}$$

De plus, tous les couples (ν_1,ν_2) satisfaisant ces conditions peuvent être réalisés en choisissant convenablement les vecteurs propres des matrices A et B. Pour des matrices de taille arbitraire, un ensemble complet d'inégalités caractérisant l'ensemble de tous les spectres possibles a été obtenu récemment par Klyachko, résolvant ainsi un problème qui remonte à Weyl. Toutefois pour des matrices de grande taille, lorsque l'on fixe les spectres des matrices A et B et que l'on choisit leurs vecteurs propres au hasard, on s'aperçoit que parmi tous les spectres possibles pour A et B, seul un tout petit sous-ensemble est réalisé avec une probabilité proche de 1. Cette proposition est illustrée par un exemple concret dans l'encadré 1. Des arguments très généraux, regroupés sous le nom générique de « concentration de la mesure » permettent de prédire un tel phénomène. En effet, c'est un principe bien établi que dans des espaces de grandes dimensions (ici les groupes de matrices unitaires de grande taille), les fonctions « raisonnables » tendent à être concentrées autour de leur moyenne, au sens de la mesure. Par exemple, si l'on considère la mesure de probabilités invariante par rotations sur une sphère de rayon 1, alors pour tout $\epsilon>0$ la probabilité pour que la première coordonnée satisfasse $|x_1|\leqslant\epsilon$ tend vers 1 lorsque la dimension de la sphère tend vers l'infini. On s'attend donc à ce que le comportement moyen du spectre de la somme $A+B$ soit aussi le comportement dominant, c'est-à-dire celui qui apparaîtra avec une grande probabilité. Toutefois, la généralité de ces principes ne nous permet pas d'en déduire cette valeur moyenne, qui dépend de la nature exacte des espaces et des fonctions que l'on considère. C'est ici qu'intervient la théorie des probabilités libres de Voiculescu. Introduite à l'origine pour résoudre des problèmes de classification d'algèbres d'opérateurs, il est apparu que cette théorie fournit le cadre algébrique adéquat pour modéliser le comportement le plus probable d'une famille de matrices dont les vecteurs propres ont été choisis au hasard, et permet de faire de nombreux calculs. Ces relations profondes avec les matrices aléatoires ont fait des probabilités libres un outil extrêmement puissant, qui a permis de résoudre de nombreux problèmes ouverts sur les algèbres d'opérateurs. Je n'aborderai pas ces questions ici, faute de place, mais je vais décrire le formalisme algébrique dans la section suivante, en explicitant la notion de liberté, puis j'expliquerai comment cela s'applique aux matrices aléatoires de grande taille.

– Philippe Biane, Département de mathématiques et applications – UMR 8553 CNRS – École normale supérieure, 45 rue d'Ulm, 75230 Paris cedex 05.
philippe.biane@ens.fr

LA LIBERTÉ

On considère une algèbre complexe A, avec une unité 1 et une forme linéaire $\tau : A\to\mathbf{C}$, telle que $\tau(1)=1$. Bien que les exemples intéressants pour la théorie soient hautement non commutatifs, il est utile pour l'intuition de se représenter les éléments de l'algèbre A comme des variables aléatoires et l'application τ comme étant l'espérance. En particulier, si $a\in A$, on appellera moments de a les nombres $\tau(a^n)$; $n\geqslant 1$. On a coutume d'appeler un tel couple (A,τ) un *espace de probabilités non commutatif*. La définition de base de la théorie est la suivan-

Encadré 1

SOMME DE DEUX PROJECTEURS

On tire au hasard, et indépendamment, deux projecteurs orthogonaux Π_1 et Π_2 de rang N dans un espace complexe de dimension $2N$, sous la forme $\Pi_i = U_i D U_i^*$ où D est la matrice diagonale dont les N premiers éléments diagonaux valent 1 et les autres 0, et U_i est une matrice unitaire, choisie selon la mesure de Haar sur le groupe unitaire $U(2N)$. Tirer une matrice unitaire selon la mesure de Haar est très facile : on commence par tirer le premier vecteur colonne uniformément parmi tous les vecteurs de norme 1, puis on choisit le deuxième vecteur colonne uniformément parmi les vecteurs de norme 1 orthogonaux au premier, et ainsi de suite. Un moyen simple de réaliser cela consiste à choisir une matrice $2N \times 2N$ à coefficients indépendants avec des lois gaussiennes complexes standard, puis à appliquer le procédé de Gramm-Schmidt à ses vecteurs colonnes.

La figure représente l'histogramme obtenu à partir du spectre d'une matrice $\Pi_1 + \Pi_2$ choisie comme ci-dessus, avec $N = 400$. Avec deux projections de rang 400 on peut obtenir des histogrammes très différents, par exemple si $\Pi_1 = I - \Pi_2$ alors toutes les valeurs propres valent 1, alors que si $\Pi_1 = \Pi_2$ la moitié vaut 2 et l'autre moitié vaut 0, mais on observe que pour N grand, avec une probabilité presque égale à 1, cet histogramme reste dans le voisinage d'une certaine courbe, que la théorie des probabilités libres permet de calculer explicitement.

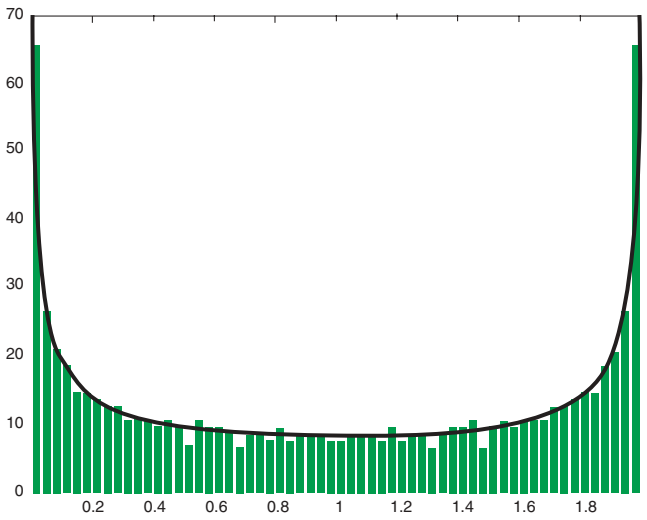

Figure - *Histogramme du spectre de $\Pi_1 + \Pi_2$.*

Dans le cas de notre figure, cette courbe est le graphe de la fonction $y = \dfrac{80}{3\pi\sqrt{x(2-x)}}$.

te, qui est un analogue non commutatif de la notion d'indépendance en théorie des probabilités.

Définition. *Une famille $(A_i; i \in I)$ de sous-algèbres unitales de A, est dite libre dans (A, τ) si pour tout choix d'éléments $a_1, \ldots, a_n \in \cup_{i \in I} A_i$, vérifiant $\tau(a_1) = \ldots = \tau(a_n) = 0$ et $a_j \in A_{i_j}$ avec $i_1 \neq i_2 \neq \ldots \neq i_n$, on a $\tau(a_1 a_2 \ldots a_n) = 0$.*

Dans cette définition, les indices voisins sont supposés distincts, mais on autorise par exemple $i_1 = i_3$. La notion de liberté incorpore à la fois le concept d'indépendance des probabilités classiques et celui d'indépendance algébrique, même si cela ne saute pas aux yeux en lisant la définition, qui peut paraître compliquée. Un petit calcul va permettre de se familiariser avec la liberté. On considère (A_1, A_2) une famille libre dans (A, τ), et $a_1 \in A_1$, $a_2 \in A_2$. Si on pose $\bar{a}_i = a_i - \tau(a_i)1$, $i = 1, 2$ alors le calcul classique de la covariance montre que

$$\tau(\bar{a}_1 \bar{a}_2) = \tau(a_1 a_2) - \tau(a_1)\tau(a_2)$$

et l'hypothèse de liberté entraîne que $\tau(\bar{a}_1 \bar{a}_2) = 0$. On en déduit que

$$\tau(a_1 a_2) = \tau(a_1)\tau(a_2). \qquad (1)$$

En fait, ce calcul se généralise et l'on montre que si $a = a_1 \ldots a_n$ est un « mot », produit de termes $a_j \in A_{i_j}$ où $(A_i; i \in I)$ est une famille libre dans (A, τ), alors $\tau(a)$ peut s'exprimer comme un polynôme en les quantités de la forme $\tau(a_{j_1} \ldots a_{j_k})$ où tous les termes du produit $a_{j_1}, \ldots, a_{j_k}$, appartiennent à une même sous-algèbre A_i. Par exemple, en reprenant les notations ci-dessus, on peut vérifier que

$$\tau(a_1 a_2 a_1 a_2) = \tau(a_1^2)\tau(a_2)^2 \qquad (2)$$
$$+\tau(a_1)^2\tau(a_2^2) - \tau(a_1)^2\tau(a_2)^2.$$

On en déduit en particulier que si $(A_i; i \in I)$ est une famille libre, alors la restriction de τ à la sous-algèbre engendrée par la famille $(A_i; i \in I)$ est entièrement déterminée par les restrictions de τ à chacune des sous-algèbres A_i. Cette propriété est analogue à celle de l'indépendance des variables aléatoires en probabilités classiques ; on sait bien en effet que si l'on dispose d'une famille de variables aléatoires indépendantes et que l'on connaît la loi de chacune d'elles, alors on peut calculer la loi jointe de cette famille de variables aléatoires. Enfin,

on peut vérifier que la notion de liberté est non vide ; si l'on se donne une famille d'espaces de probabilités non commutatifs $(A_i, \tau_i); i \in I$, alors on peut toujours, au moyen d'une construction de produit libre réduit, trouver un espace de probabilités non commutatif (A, τ) et des morphismes d'algèbres $\iota_i : A_i \to A$, injectifs, préservant l'unité et vérifiant $\tau_i = \tau \circ \iota_i$, tels que les sous-algèbres $(A_i; i \in I)$ forment une famille libre dans (A, τ).

LIBERTÉ ASYMPTOTIQUE DES MATRICES ALÉATOIRES

Voyons maintenant comment la notion de liberté permet de modéliser le comportement des grandes matrices aléatoires. Commençons par rappeler que, d'après le théorème spectral, une matrice hermitienne M de taille $N \times N$ est déterminée, à une conjugaison par une matrice unitaire près, par son spectre (avec la multiplicité de chaque valeur propre), c'est-à-dire un ensemble de N nombres réels. Des résultats classiques sur les fonctions symétriques montrent que la donnée du spectre de la matrice M est elle-même équivalente à celle de la suite de nombres $\frac{1}{N} Tr(M^n); n \geqslant 1$, (en fait il suffit de connaître seulement les N premiers termes de cette suite). Cette suite de nombres est aussi la suite des moments de la mesure $\frac{1}{N} \sum_j \delta_{\lambda_j}$ où $\lambda_1, \ldots, \lambda_N$ désigne le spectre de M, les valeurs propres étant comptées avec leur multiplicité. Il est commode de désigner par $tr = \frac{1}{N} Tr$ la trace normalisée sur l'espace de matrices de taille $N \times N$, ce que je ferai dans la suite. Si l'on considère plusieurs matrices $M_1, \ldots, M_m$, la donnée du spectre de chacune d'elles ne suffit pas à déterminer leurs positions relatives dans l'espace de toutes les matrices hermitiennes. Néanmoins, une construction classique dans la théorie des algèbres d'opérateurs, la construction de Gelfand-Naimark-Segal (GNS) montre que si l'on connaît les nombres $tr(M_{i_1} \ldots M_{i_k})$ où k parcourt les entiers positifs et les indices $i_1, \ldots, i_k$ prennent des valeurs arbitraires dans $\{1, \ldots, m\}$, alors on peut retrouver les matrices M_i à une conjugaison unitaire globale près $M_i \mapsto U M_i U^*$ (c'est-à-dire que U ne dépend pas de i). Il est facile de voir que la connaissance de ces nombres permet de retrouver le spectre de n'importe quel polynôme en les matrices $M_1, \ldots, M_m$. Supposons maintenant que les spectres des matrices $M_1, M_2, \ldots, M_m$ sont fixés et inclus dans $[-1, 1]$ pour fixer les idées (on peut toujours tout multiplier par une constante pour s'y ramener), mais que leurs vecteurs propres sont choisis au hasard. Autrement dit, les matrices ont la forme $M_i = U_i D_i U_i^*$ où les matrices D_i sont diagonales et les matrices U_i sont des matrices unitaires choisies au hasard, indépendamment, et avec la mesure de Haar sur le groupe unitaire $U(N)$. On se donne alors un espace de probabilités non commutatif (A, τ) et des éléments $a_1, \ldots, a_m \in A$, tels que les sous-algèbres $A_i; i \in I$ (où A_i désigne la sous-algèbre unitaire engendrée par a_i) forment une famille libre. Comme on l'a vu, l'hypothèse de liberté entraîne que la quantité $\tau(a_{i_1} \ldots a_{i_k})$ peut s'exprimer comme un polynôme en les moments $\tau(a_i^n)$. Le résultat fondamental de Voiculescu est que la valeur de $tr(M_{i_1} \ldots M_{i_k})$ est proche de $\tau(a_{i_1} \ldots a_{i_k})$ avec une probabilité qui tend vers 1 lorsque N tend vers l'infini. Plus précisément, pour tout choix d'un réel $\varepsilon > 0$, et d'un multiindice $(i_1, \ldots, i_k)$, il existe une suite C_N, qui tend vers zéro lorsque N tend vers l'infini et telle que, pour tout N, la probabilité pour que

$$|tr(M_{i_1} \ldots M_{i_k}) - \tau(a_{i_1} \ldots a_{i_k})|$$

soit plus grand que ε est majorée par C_N, cette inégalité étant vérifiée pour tout choix des spectres de $M_1, \ldots, M_m$ dans $[-1, 1]$.

En utilisant ce résultat on peut prédire, avec une bonne précision et une probabilité proche de 1, la valeur d'une quantité de la forme $tr(M_{i_1} \ldots M_{i_k})$, en connaissant seulement les spectres de $M_1, \ldots, M_m$. Par exemple, en reprenant la formule (1) on voit que pour « la plupart » des couples de matrices de grande taille M_1, M_2, on a

$$tr(M_1 M_2) \sim tr(M_1) tr(M_2)$$

ou encore, en utilisant (2)

$$tr(M_1 M_2 M_1 M_2) \sim$$
$$tr(M_1^2) tr(M_2)^2 + tr(M_1)^2 tr(M_2^2)$$
$$- tr(M_1)^2 tr(M_2)^2.$$

De même, on peut calculer grâce à ce théorème le comportement asymptotique des moments $tr((M_1 + M_2)^n); n \geqslant 1$ de la somme de deux matrices, en termes des deux suites de moments $tr(M_1^n); n \geqslant 1$ et $tr(M_2^n); n \geqslant 1$. La connaissance d'un nombre fini de moments ne permet pas de retrouver tout le spectre (n'oublions pas que $N \to \infty$), mais elle permet d'avoir une bonne approximation de la mesure empirique de ce spectre. C'est ce qui permet de tracer la courbe de l'encadré 1. Les calculs algébriques se font au niveau des algèbres libres, sans référence aux matrices aléatoires. Il reste à expliquer comment faire ces calculs de façon économique, ce qui est loin d'être évident. C'est ce que je vais faire dans la section suivante, en décrivant la méthode combinatoire de Speicher.

COMBINATOIRE DE LA LIBERTÉ

La notion combinatoire adéquate pour faire des calculs en probabilités libres est celle de partition non croisée. Une partition de l'ensemble $\{1, 2, \ldots, n\}$ est dite croisée s'il existe deux classes distinctes C et D de la partition et quatre éléments $i, j, k, l \in \{1, 2, \ldots, n\}$ tels

que $i < j < k < l$, on a $i, k \in C$ et $j, l \in D$. Elle est dite non croisée dans le cas contraire. L'ensemble des partitions non croisées de $\{1, 2, \ldots, n\}$ est noté $NC(n)$. C'est une structure combinatoire très riche, qui mérite d'être étudiée pour elle-même (voir l'encadré 2 pour plus d'informations sur cette notion).

Encadré 2

LES PARTITIONS NON CROISÉES

On considère une partition de l'ensemble $\{1, \ldots, n\}$. Il est commode de placer les n points sur un cercle et de tracer, pour chaque classe de la partition, le polygone convexe dont les sommets sont les points dans la classe. La partition est non croisée si et seulement si ces polygones ne s'intersectent pas.

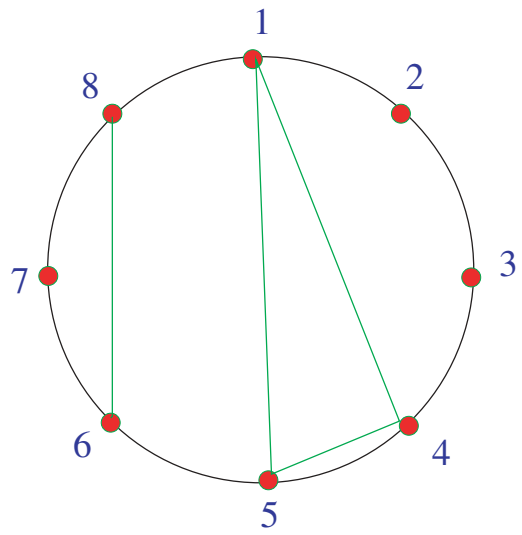

Figure 1 - *Une partition non croisée.*

La figure ci-dessus montre la partition non croisée $\{1, 4, 5\} \cup \{2\} \cup \{3\} \cup \{6, 8\} \cup \{7\}$. Le nombre de partitions non croisées de $\{1, \ldots, n\}$ est le nombre de Catalan $\frac{(2n-2)!}{n!(n-1)!}$. La relation « est moins fine que » est une relation d'ordre qui fait de l'ensemble des partitions non croisées un treillis (tout sous-ensemble admet un plus petit majorant et un plus grand minorant). Les partitions non croisées interviennent dans l'étude du groupe symétrique ; en effet on peut associer à chaque partition non croisée la permutation dont les cycles sont obtenus en parcourant chaque polygone dans le sens des aiguilles d'une montre. On obtient ainsi un sous-ensemble du groupe des permutations de $\{1, \ldots, n\}$ qui admet une caractérisation géométrique simple. On munit le groupe symétrique de la structure de graphe de Cayley induite par l'ensemble de générateurs formé de toutes les transpositions. Autrement dit, deux permutations σ_1 et σ_2 sont les sommets d'une arête de ce graphe si et seulement si $\sigma_1\sigma_2^{-1}$ est une transposition. Les permutations obtenues à partir d'une partition non croisée sont alors celles qui se situent sur une géodésique, c'est-à-dire un chemin de longueur minimale reliant l'identité à la permutation circulaire $c = (12\ldots n)$ dans le graphe de Cayley. On peut exprimer cette condition à l'aide de la fonction de longueur sur le groupe symétrique : $|\sigma|$ est le plus petit nombre k tel que σ peut s'écrire comme le produit de k transpositions. Une permutation σ provient d'une partition non croisée si et seulement si on a $|\sigma| + |\sigma^{-1}| = |c|$. Ce plongement de $NC(n)$ dans le groupe symétrique S_n permet de montrer que le treillis des partitions non croisées est autodual ; en effet l'application $\sigma \mapsto \sigma^{-1}c$ de S_n dans lui-même préserve $NC(n)$ et induit un antiautomorphisme de la structure d'ordre. Cette propriété de $NC(n)$ n'est pas partagée par le treillis de toutes les partitions, ce qui fait que par certains côtés la théorie des probabilités libres possède plus de symétries que la théorie classique.

La figure 2 montre le treillis des partitions non croisées de $\{1, 2, 3, 4\}$ (chacune étant identifiée avec sa permutation image).

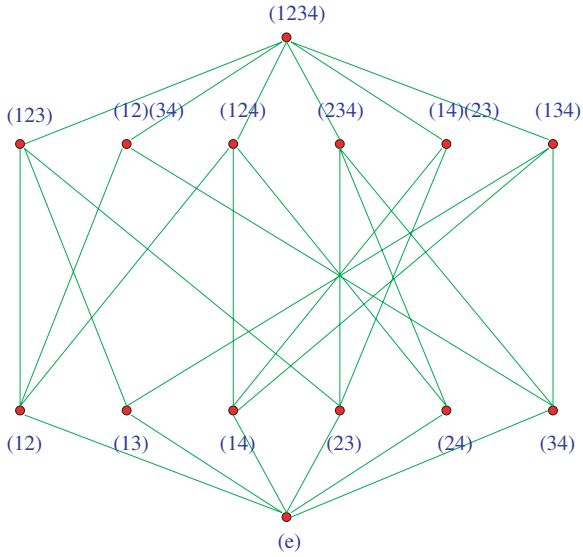

Figure 2 - *NC(4).*

L'élément minimal est l'identité, l'élément maximal est la permutation circulaire (1234). *La relation d'ordre est indiquée par les arêtes du graphe, qui sont aussi les arêtes du graphe de Cayley de S_4, restreint aux éléments se trouvant sur une géodésique reliant la permutation identique au cycle* (1234).

Speicher s'est inspiré de l'approche algébrique de l'indépendance en théorie des probabilités due à Rota, qui utilise le treillis des partitions d'un ensemble fini pour définir les cumulants d'une famille de variables aléatoires. C'est ainsi qu'il a défini des « cumulants non croisés » de la façon suivante. Étant donné un espace de probabilités non commutatif (A, τ), les cumulants non croisés sont une famille $R^{(n)}; n \geqslant 1$ de formes multilinéaires sur A, définies de manière implicite ($R^{(n)}$ étant une forme n-linéaire) par les équations

$$\tau(a_1 \dots a_n) = \sum_{\pi \in NC(n)} R_\pi(a_1, \dots, a_n).$$

Dans cette formule, pour chaque partition non croisée $\pi = \cup_i A_i$, avec $p_i = \text{cardinal}(A_i)$, on a

$$R_\pi(a_1, \dots, a_n) = \prod_i R^{(p_i)}(a_{j_1}, \dots, a_{j_{p_i}})$$

où $A_i = \{a_{j_1}, \dots, a_{j_{p_i}}\}$. Par exemple, pour $n = 3$ il y a cinq termes, qui correspondent respectivement aux partitions $\{1, 2, 3\}$, $\{1\} \cup \{2, 3\}$, $\{1, 3\} \cup \{2\}$, $\{1, 2\} \cup \{3\}$ et $\{1\} \cup \{2\} \cup \{2\}$.

$$\begin{aligned}\tau(a_1a_2a_3) = {} & R_3(a_1, a_2, a_3) + R_1(a_1)R_2(a_2, a_3) \\ & + R_2(a_1, a_3)R_1(a_2) + R_2(a_1, a_2)R_1(a_3) \\ & + R_1(a_1)R_1(a_2)R_1(a_3)\end{aligned}$$

En général, $\tau(a_1 \dots a_n)$ est égal à la somme de $R^{(n)}(a_1, \dots, a_n)$ et de termes qui font intervenir les $R^{(k)}$ avec $k < n$, ce qui fait que les $R^{(n)}$ sont bien définis par récurrence sur n. Par exemple on a

$$\begin{aligned}R^{(1)}(a) &= \tau(a) \\ R^{(2)}(a_1, a_2) &= \tau(a_1a_2) - \tau(a_1)\tau(a_2) \\ R^{(3)}(a_1, a_2, a_3) &= \tau(a_1a_2a_3) - \tau(a_1)\tau(a_2a_3) \\ &\quad - \tau(a_2)\tau(a_1a_3) - \tau(a_3)\tau(a_1a_2) \\ &\quad + 2\tau(a_1)\tau(a_2)\tau(a_3).\end{aligned}$$

L'intérêt des cumulants non croisés provient du résultat suivant. Soit $(A_i; i \in I)$ une famille libre dans un espace de probabilités non commutatif (A, τ), alors pour tout choix d'éléments $a_1, \dots, a_n \in \cup_{i \in I} A_i$ avec $a_j \in A_{i_j}$, on a

$$R^{(n)}(a_1, \dots, a_n) = 0$$

dès qu'il existe deux i_k et i_l distincts.

Pour illustrer la puissance de ce résultat, considérons le cas de deux éléments a_1 et a_2 appartenant à des sous-algèbres libres A_1 et A_2, et calculons

$$R^{(n)}(a_1 + a_2, a_1 + a_2, \dots, a_1 + a_2).$$

Si l'on développe par multilinéarité, alors le résultat ci-dessus entraîne que les termes contenant à la fois a_1 et a_2 sont nuls, par conséquent on a

$$\begin{aligned}R^{(n)}(a_1 + a_2, \dots, a_1 + a_2) &= R^{(n)}(a_1, \dots, a_1) \\ &+ R^{(n)}(a_2, \dots, a_2).\end{aligned}$$

Comme les moments $\tau((a_1 + a_2)^n)$ peuvent se retrouver à partir des cumulants $R^{(n)}(a_1 + a_2, \dots, a_1 + a_2)$, on en déduit une expression explicite des moments de $a_1 + a_2$. On peut mettre ce calcul sous une forme plus explicite en introduisant la fonction génératrice des moments

$$G_a(z) = \frac{1}{z} + \sum_{k=1}^{\infty} \frac{\tau(a^k)}{z^{k+1}}.$$

On peut inverser cette série, au sens de la composition des séries formelles. Son inverse se met sous la forme

$$K_a(z) = \frac{1}{z} + \sum_{k=1}^{\infty} R_k(a) z^{k-1}$$

où le coefficient $R_k(a)$ s'exprime polynomialement en terme des moments $\tau(a^j)$ avec $j \leqslant k$, et on a

$$R_n(a) = R^{(n)}(a, \dots, a).$$

Pour calculer les moments de $a_1 + a_2$ on doit donc :

i) calculer les fonctions génératrices G_{a_1} et G_{a_2},

ii) inverser ces fonctions pour trouver K_{a_1} et K_{a_2},

iii) calculer $K_{a_1+a_2}(z) = K_{a_1}(z) + K_{a_2}(z) - \frac{1}{z}$,

iv) calculer $G_{a_1+a_2}$ en inversant $K_{a_1+a_2}$,

v) extraire les coefficients du développement de $G_{a_1+a_2}$.

Reprenons l'exemple de l'encadré 1. Pour une projection orthogonale de rang N dans un espace de dimension $2N$ on a $tr(\Pi^k) = \frac{1}{2}$ pour $k \geqslant 1$ d'où

$$G_{a_i}(z) = \frac{2z - 1}{2z(z - 1)}.$$

On en déduit

$$K_{a_i}(z) = \frac{z + 1 + \sqrt{z^2 + 1}}{2z}.$$

La série génératrice des moments de la somme de deux variables libres a_1 et a_2 ayant les moments de Π_1 et Π_2 est donc la fonction inverse de

$$K_{a_2}(z) + K_{a_2}(z) - \frac{1}{z} = 1 + \frac{\sqrt{z^2 + 1}}{z}$$

soit

$$G_{a_1+a_2}(z) = \frac{1}{\sqrt{z(z-2)}}.$$

On en déduit que les moments $\tau((a_1+a_2)^k)$ sont les moments de la mesure de probabilités sur $[0, 2]$ de densité $\frac{1}{\pi\sqrt{x(2-x)}}$, ce qui a permis de tracer la courbe dans la figure 1.

Bien d'autres calculs sont possibles : on peut calculer par exemple de façon compacte les moments d'un produit $\tau((a_1a_2)^n)$ en terme des moments de a_1 et a_2. Cela permet de prédire, pour des matrices unitaires aléatoires U_1 et U_2, de grandes tailles, le spectre de leur produit en fonction du spectre de chacune d'elles. On peut encore traiter par ces méthodes le cas du spectre de $A^{1/2}BA^{1/2}$ où A et B sont hermitiennes positives, ou encore celui du commutateur $[X, Y] = XY - YX$ de deux matrices hermitiennes.

POUR EN SAVOIR PLUS

Biane (P.), Free probability for probabilists, *math.PR/9809193*, 16 p., 1998.

Biane (P.), Entropie libre et algèbres d'opérateurs, *Séminaire Bourbaki*, exposé 889, juin 2001.

Fulton (W.), Eigenvalues of sums of hermitian matrices (after A. Klyachko), *Séminaire Bourbaki*, exposé 845, juin 1998.

Hiai (F.), Petz (D.), The semicircle law, free random variables and entropy, *Mathematical Surveys and Monographs 77*, American Mathematical Society, Providence, RI, 2000.

Ledoux (M.), The concentration of measure phenomenon, *Mathematical Surveys and Monographs, 89,* American Mathematical Society, Providence, RI, 2001.

Voiculescu (D.V.), Lectures on free probability theory *(Saint-Flour, 1998)*, Lecture Notes in Math, 1738, Springer, Berlin, 2000, 279-349.