PROBABILITÉS LIBRES ET MATRICES ALÉATOIRES

Philippe Biane

ALEA

Luminy, 05-06/03/2012

Prologue: vecteurs aléatoires en grandes dimensions

$v_1, \ldots, v_k \in \mathbf{R}^N$.

$a_i = \|v_i\|$ fixées.

$\omega_1 = v_1/\|v_1\|, \ldots, \omega_k = v_k/\|v_k\| \in \mathbf{R}^N$ choisis au hasard indépendamment, uniformément sur la sphère de rayon 1.

Lorsque $N \to \infty$, avec probabilité 1, les v_i deviennent orthogonaux (à ϵ près): pour tout $\epsilon > 0$,

$$P(|\langle \omega_i, \omega_j \rangle - \delta_{ij}| > \epsilon) \to_{N \to \infty} 0$$

On va obtenir des résultats analogues pour des matrices aléatoires au lieu de vecteurs aléatoires.

La géométrie des matrices est plus compliquée que celle des vecteurs.

L'outil algébrique qui permet la description de ces résultats est la théorie des *probabilités libres*.

Exemple:

Π_1 et Π_2, matrices de taille $N \times N$
=Projections orthogonales sur des sous-espace de dimension $N/2$.

On choisit les sous-espaces au hasard "uniformément", i.e.

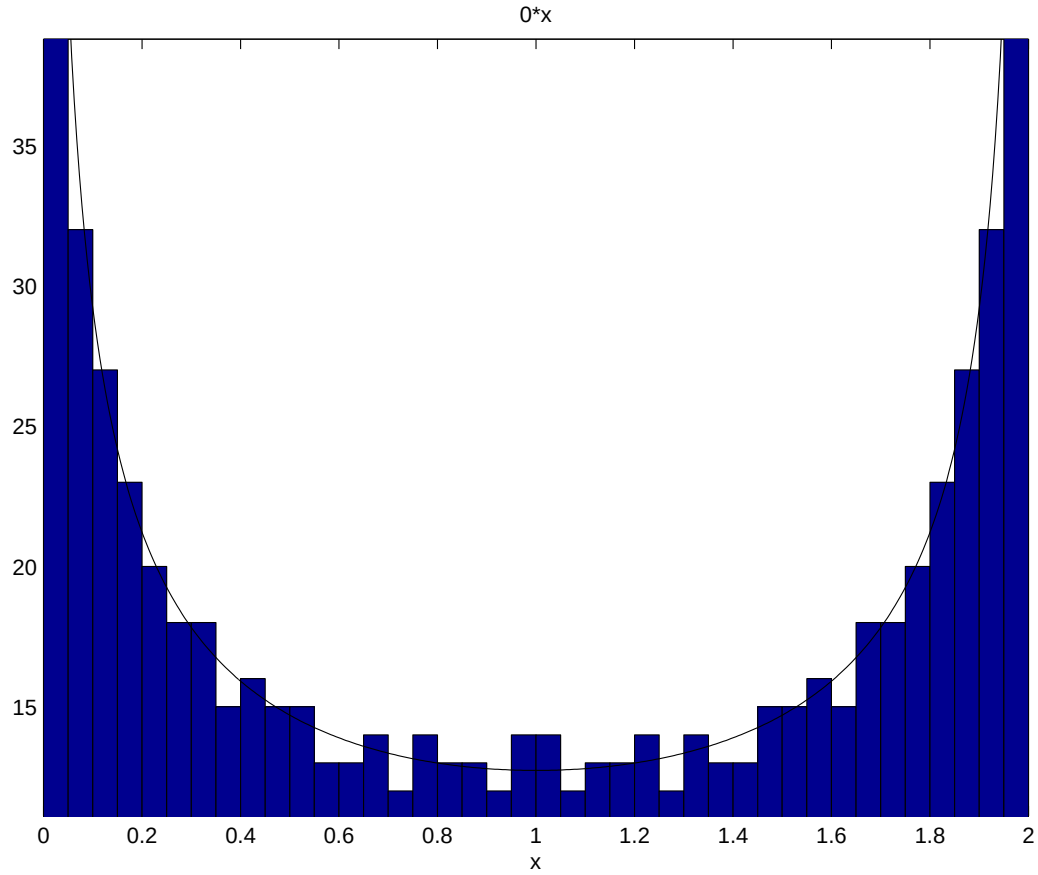
$$\Pi_i = U_i \begin{pmatrix} I_{N/2} & 0 \\ 0 & 0 \end{pmatrix} U_i^*$$

où U_i sont indépendantes choisies avec la mesure de Haar$^{(*)}$ sur $U(N)$.

On calcule le spectre de $\Pi_1 + \Pi_2$.

(*): mesure de Haar sur $U(N)$=unique probabilité invariante par les translations: $U \mapsto UV$

Histogramme du spectre de $\Pi_1 + \Pi_2$ $\quad (N = 800)$



$$y = \frac{1}{\pi\sqrt{x(2-x)}}$$

X=matrice hermitienne, $N \times N$.

$X = UDU^*$, avec

U=unitaire (vecteurs propres de X);

$$D = \begin{pmatrix} \lambda_1 & 0 & 0 & \cdots & 0 \\ 0 & \lambda_2 & 0 & \cdots & 0 \\ 0 & 0 & \lambda_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \cdots & \lambda_N \end{pmatrix}$$

À conjugaison par une matrice unitaire près, X est déterminée par son spectre.
Le spectre lui-même est déterminé par les nombres

$$\frac{1}{N} Tr(X^n) = \frac{1}{N} \sum_{i=1}^{N} \lambda_i^n; \qquad n = 1, 2, \ldots$$

$X_1, \ldots, X_n =$ matrices hermitiennes $N \times N$.

Pas simultanément diagonalisables.

Proposition: À une conjugaison unitaire près

$$X_1, \ldots, X_n \mapsto UX_1U^*, \ldots, UX_nU^*$$

le n-uplet $X_1, \ldots, X_n$ est déterminé par les "moments mixtes"

$$\frac{1}{N} Tr(X_{i_1} \ldots X_{i_k}); \qquad k \geq 1; \quad i_1, \ldots, i_k \in \{1, \ldots, n\}$$

Remarque Les moments mixtes remplacent les produits scalaires entre vecteurs pour déterminer la géométrie d'un ensemble de matrices.

On considère des matrices de la forme $X_i = U_i D_i U_i^*$ où les D_i sont des matrices diagonales et les U_i sont des matrices unitaires aléatoires, prises avec la mesure de Haar sur $U(N)$.

Les nombres $\frac{1}{N} Tr(X^n) = \frac{1}{N} \sum_{i=1}^{N} \lambda_i^n; \qquad n = 1, 2, \ldots$ (et donc les valeurs propres) sont fixés, mais les vecteurs propres sont choisis au hasard.

Théorème

(Voiculescu, 1990) *Lorsque* $N \to \infty$ *les moments mixtes*

$$\frac{1}{N} Tr(X_{i_1} \dots X_{i_k})$$

s'expriment (asymptotiquement) de façon polynomiale en les moments $\frac{1}{N} Tr(D_i^k) = \frac{1}{N} Tr(X_i^k)$

Exemples: $(\frac{1}{N}Tr = tr)$

$$tr(X_1X_2) \sim tr(X_1)tr(X_2)$$

$$tr(X_1^k X_2^l) \sim tr(X_1^k)tr(X_2^l)$$

$$tr(X_1X_2X_1X_2) \sim tr(X_1^2)tr(X_2)^2 + tr(X_1)^2 tr(X_2^2) - tr(X_1)^2 tr(X_2)^2$$

Ici $\sim$ signifie que la différence est petite en probabilités.

Corollaire

Si on connait les spectres de $X_1, \ldots, X_n$ alors on peut calculer, avec une bonne approximation le spectre de n'importe quel polynôme en les X_i

par exemple:

$$tr((X_1 + X_2)^n) = \sum_{i_1 \ldots i_n} tr(X_{i_1} \ldots X_{i_n})$$

se calcule asyptotiquement au moyen des nombres

$$tr(X_1^k), tr(X_2^k), \qquad k = 1, 2, \ldots$$

Le calcul effectif de ces polynômes se fait au moyen de la théorie des probabilités libres.

Espace de probabilités non-commutatif

A=algèbre (de *variables aléatoires non-commutatives*).

$1 \in A, \quad a+b, \quad ab, \quad \lambda a \quad \in A$ si $a, b \in A$

$\tau : A \to \mathbf{C}$=forme linéaire (=espérance). $\tau(1) = 1$

Si $x \in A$, les $\tau(x^n)$ sont les *moments* de x.

Si $x_1, \ldots, x_n \in A$, les $\tau(x_{i_1} \ldots x_{i_k})$ sont les *moments mixtes* des x_i.

LIBERTÉ

Definition (Voiculescu, 1983)

$\{A_i; i \in I\}$=*famille de sous-algèbres (unifères) de* A.

Les A_i *sont libres dans* (A, τ) *ssi pour tous* $a_1, \ldots, a_n \in A$ *tels que*

i) $\tau(a_j) = 0$ *pour tout* j,

ii) $a_j \in A_{i_j}$, $i_1 \neq i_2$, $i_2 \neq i_3, \ldots, i_{n-1} \neq i_n$,

on a

$$\tau(a_1 \ldots a_n) = 0$$

La liberté incorpore à la fois la notion d'indépendance probabiliste et celle d'indépendance algébrique (au sens d'absence de relations).

Liberté=indépendance probabiliste + indépendance algébrique

Exemple: $a_1 \in A_1, a_2 \in A_2$, libres dans (A, τ)

$$a_1 = \bar{a}_1 + \tau(a_1)1; \quad a_2 = \bar{a}_2 + \tau(a_2)1; \quad \tau(\bar{a}_1) = \tau(\bar{a}_2) = 0$$

$$\tau(a_1 a_2) = \tau([\bar{a}_1 + \tau(a_1)][\bar{a}_2 + \tau(a_2)])$$

d'après l'hypothèse de liberté

$$\tau(\bar{a}_1 \bar{a}_2) = 0$$

finalement

$$\boxed{\tau(a_1 a_2) = \tau(a_1)\tau(a_2)}$$

De même:

$$\boxed{\tau(a_1 a_2 a_1 a_2) = \tau(a_1^2)\tau(a_2)^2 + \tau(a_1)^2\tau(a_2^2) - \tau(a_1)^2\tau(a_2)^2}$$

En général

$$\tau(a_1 \dots a_n)$$

avec $a_j \in A_{i_j}$ peut se calculer au moyen d'un polynôme en les quantités

$$\tau(a_{i_1} \dots a_{j_r})$$

avec tous les $a_{j_1} \dots a_{j_r}$ dans la même algèbre.

Corollaire

Si les A_i sont libres et si on connait $\tau_{|A_i}$ pour tout i alors on connait $\tau_{|\langle A_i;i\rangle}$.

Liberté et matrices aléatoires

Heuristique: des matrices génériques admettent des relations algébriques en dimension finie, mais si leur dimension tend vers l'infini, le degré de ces relations tend vers l'infini. Si on suppose de plus que ces matrices sont des variables indépendantes on s'attend à avoir des variables libres:

Liberté=indépendance probabiliste + indépendance algébrique

Un modèle de matrices aléatoires

$$X_i = U_i D_i U_i^*$$

D_i sont réelles diagonales (fixées), et les U_i unitaires de Haar indépendantes.

Soient $a_1, \ldots, a_n \in (A, \tau)$ libres, telles que

$$\tau(a_i^r) = tr(X_i^r) = tr(D_i^r) \qquad r = 1, 2, \ldots$$

alors, pour N grand, on a

$$tr(X_{i_1} \ldots X_{i_k}) \sim \tau(a_{i_1} \ldots a_{i_k})$$

avec probabilité proche de 1.

On a vu que $\tau(a_{i_1} \dots a_{i_k})$ peut s'écrire comme un polynôme en les moments $\tau(a_i^k) = tr(X_i^k)$.

On en déduit que, lorsque $N \to \infty$

$$tr(X_{i_1} \dots X_{i_k}) \sim Pol(tr(X_i^k))$$

par exemple:

$$tr(X_1 X_2) \sim tr(X_1) tr(X_2)$$

$$tr(X_1 X_2 X_1 X_2) \sim tr(X_1^2) tr(X_2)^2 + tr(X_1)^2 tr(X_2^2) - tr(X_1)^2 tr(X_2)^2$$

Combinatoire de la liberté

Il existe une méthode combinatoire, dûe à R. Speicher, pour calculer avec les variables libres, qui utilise les partitions non-croisées.
Une partition (d'ensemble) de $\{1, \ldots, n\}$ est *non-croisée* si elle n'a pas de croisement. un croisement est un (i, j, k, l) avec

$$i < j < k < l$$

et

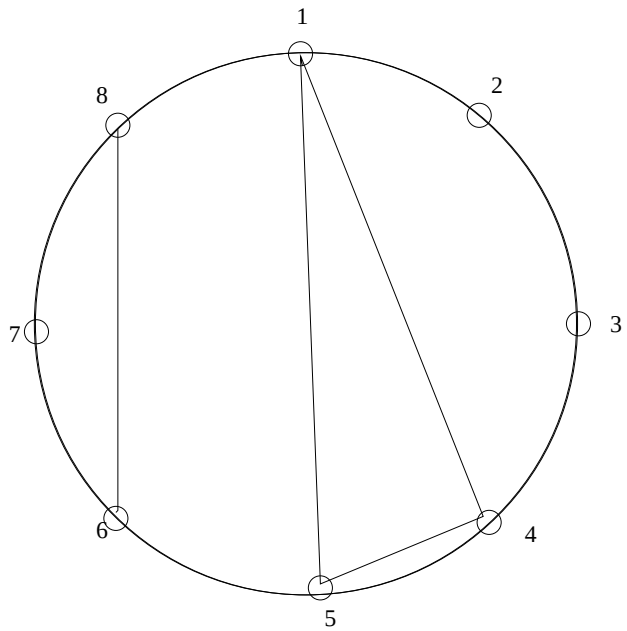
$$i \sim k, \qquad k \sim l$$

et i, j pas dans la même part

Exemple

$$\{1,4,5\} \cup \{2\} \cup \{3\} \cup \{6,8\} \cup \{7\}$$

n'a pas de croisement



Cumulants non-croisés

Sur (A, τ) on définit des fonctionnelles multilinéaires R_n par:

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

$$R_\pi(a_1, \dots, a_n) = \prod_{\text{part de} \pi} R_{|p|}(a_{i_1}, \dots, a_{i_{|p|}})$$

où $p = \{i_1, \dots, i_{|p|}\}$ est une part de π.

Exemples:

$$\tau(a_1) = R_1(a_1) \qquad \{1\}$$

$$\begin{array}{rcc} \tau(a_1 a_2) = & R_2(a_1, a_2) & \{1,2\} \\ & +R_1(a_1)R_1(a_2) & \{1\} \cup \{2\} \end{array}$$

d'où

$$\begin{aligned} R_1(a) &= \tau(a) \\ R_2(a_1, a_2) &= \tau(a_1 a_2) - \tau(a_1)\tau(a_2) \end{aligned}$$

$$\begin{array}{rcl}
\tau(a_1a_2a_3) = & R_3(a_1,a_2,a_3) & \{1,2,3\} \\
& +R_1(a_1)R_2(a_2,a_3) & \{1\}\cup\{2,3\} \\
& +R_2(a_1,a_3)R_1(a_2) & \{1,3\}\cup\{2\} \\
& +R_2(a_1,a_2)R_1(a_3) & \{1,2\}\cup\{3\} \\
& +R_1(a_1)R_1(a_2)R_1(a_3) & \{1\}\cup\{2\}\cup\{2\}
\end{array}$$

$$\begin{array}{rcl}
R_3(a_1,a_2,a_3) & = & \tau(a_1a_2a_3)-\tau(a_1a_2)\tau(a_3)-\tau(a_1a_3)\tau(a_2) \\
& & -\tau(a_1)\tau(a_2a_3)+2\tau(a_1)\tau(a_2)\tau(a_3)
\end{array}$$

Plus généralement, on a une formule d'inversion:

$$R_n(a_1, \ldots, a_n) = \sum_{\pi \in NC(n)} \mu(\pi) \tau_\pi(a_1, \ldots, a_n)$$

où μ est une fonction de Möbius sur $NC(n)$.

Liberté et cumulants libres

Théorème (Speicher). Les $(A_i; i \in I)$ sont libres dans (A, τ), si et seulement si, pour tous $a_1 \in A_{i_1}, \ldots, a_n \in A_{i_n}$, on a

$$R_n(a_1, \ldots, a_n) = 0$$

s'il existe j, k tels que $i_j \neq i_k$.

Remarque: On peut définir des cumulants pour des variables qui commutent, en utilisant le treillis de toutes les partitions. Le résultat ci-dessus est valable en remplaçant la liberté par l'indépendance (Rota).

Conséquence de la caractérisation de Speicher de la liberté:
si $a_k \in A_{i_k}$ (algèbres libres);
Π=partition de $\{1, \ldots, n\}$ induite par $k \sim l$ si $i_k = i_l$.
dans l'expression:

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

beaucoup de termes sont nuls:
On en déduit:

$$\tau(a_1 \ldots a_n) = \sum_{\pi \in NC(n) : \pi \leq \Pi} R_\pi(a_1, \ldots, a_n)$$

Exemple:

$$\tau(a_1 a_2 a_1 a_2); \quad a_1 \in A_1; \quad a_2 \in A_2$$

$$n = 4 \qquad \Pi = \{1,3\} \cup \{2,4\}$$

$$\begin{array}{rcl} \tau(a_1 a_2 a_1 a_2) = & R_2(a_1, a_1) R_1(a_2)^2 & \{1,3\} \cup \{2\} \cup \{4\} \\ & + R_1(a_1)^2 R_2(a_2, a_2) & \{1\} \cup \{3\} \cup \{2,4\} \\ & + R_1(a_1)^2 R_1(a_2)^2 & \{1\} \cup \{2\} \cup \{3\} \cup \{4\} \end{array}$$