Probabilités libres et matrices aléatoires

Ioan Manolescu et Alexandre Thiéry

20 janvier 2007

Résumé

Dans ce mémoire on donne un aperçu de la théorie des probabilités libres illustré d'un exemple : un théorème sur le comportement asymptotique des grandes matrices aléatoires à entrées gaussiennes.

Nous remercions Florent Benaych-Georges pour ses nombreux conseils et son encadrement.

Table des matières

1 Probabilités libres : définitions et exemples

1.1 Variables Aléatoires, Liberté

En probabilités classiques une variable aléatoire est une fonction mesurable $f : \Omega \to \mathbb{C}$ où Ω est un espace de probabilité. On peut alors définir l'espérance de f, $E(f) = \int_\omega f dw$, lorsque f est intégrable.
Pour généraliser ce concept, on dira que f est une variable aléatoire si f est un élément de A, où A est une $\mathbb{C}$-algèbre unitaire munie d'une forme linéaire ϕ appellée fonction d'état vérifiant $\phi(1) = 1$. Cette fonction état jouera le rôle de l'espérance ($E(1) = 1$). Si de plus la propriété supplémentaire $\phi(fg) = \phi(gf)$ est vérifiée pour tout couple $(f, g) \in A$, on dira que ϕ est une trace.

Exemple :

1. $A = (M_n(\mathbb{C}), +, .)$ munie de la trace normalisée $\tau_n(M) = \frac{1}{n}Tr(M)$ comme fonction d'état.
2. $A = L^\infty(\Omega)$ où Ω est un espace de probabilité, munie de l'espérance comme fonction état.

L'indépendance au sens des probabilités sera alors remplacée par la notion de liberté. On fera néanmoins attention au fait que des variables aléatoires indépendantes ne seront pas en générales libres.

Définition 1 (Liberté) *Soit $(A_i)_I$ des sous-algèbres de A, indexées par un ensemble quelconque I, chacune contenant l'identité. Alors ces sous-algèbres sont dites libres si quelques soient les éléments $a_1, a_2, \ldots, a_n \in A$ vérifiant :*
- $a_i \in A_{i(j)}$, $i(j) \in I$
- $i(k) \neq i(k+1)$ *pour tout* $1 \leq k \leq n-1$
- $\phi(a_i) = 0$ *pour tout* $1 \leq i \leq n$

Alors $\phi(a_1 a_2 \ldots a_n) = 0$

Comme en probabilité lorsqu'on dit que deux fonctions X, Y sont indépendantes lorsque les sigma-algèbres $\sigma(X)$ et $\sigma(Y)$ sont indépendantes, on peut définir la liberté de sous-ensembles $(H_i)_I$ lorsque les sous-algèbres unitaires générées par ces $(H_i)_I$ sont libres.

Exemple :
1. Dans $A = (M_n(\mathbb{C}), +, .)$ munie de la trace normalisée $\tau_2(M) = \frac{1}{n}Tr(M)$, les matrices scalaires forment une sous-algèbre libre par rapport à n'importe quelle autre sous-algèbre
2. Dans $A = (M_2(\mathbb{C}), +, .)$ munie de la trace normalisée $\tau_n(M) = \frac{1}{2}Tr(M)$, les sous-algèbres $A_1 = \{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}, a, b \in \mathbb{C}\}$ et $A_2 = \{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, a, b \in \mathbb{C}\}$ sont libres. (On montre néanmoins qu'il n'existe pas de sous $*$-algèbres libres non triviales dans $M_n(\mathbb{C})$)
3. d'autre exemples sont facilement construits une fois la notion de produit libre d'algèbre introduite, chose faite plus bas.

Le fait important lorsqu'on a affaire à des sous-algèbres libre $(A_i)_I$ est que l'on peut connaître ϕ sur l'algèbre engendrée par les A_i en ne connaissant ϕ que sur les $(A_i)_I$. Il est en général faux que la connaissance de $\phi(a)$ et de $\phi(b)$ permette d'en déduire la valeur de $\phi(ab)$.
Traitons d'abord le cas instructif de deux variables qui permet entre autre de voir l'intérêt du fait que chaque sous-algèbre contienne l'identité.

Proposition 2 *Si les éléments $a, b \in A$ sont libres alors $\phi(ab) = \phi(a)\phi(b)$*

Démonstration : Soient A_a et A_b les sous-algèbres générées par a et b respectivement. On peut écrire $a = a_1 + a_2$ où $a_1 = \phi(a)1_A \in A_a$ et $a_2 = a - a_1 \in A_a$, et similairement $b = b_1 + b_2$. Alors :

$$\begin{aligned}
\phi(ab) &= \phi(a_1b_1) + \phi(a_2b_1) + \phi(a_1b_2) + \phi(a_2b_2) \\
&= [\phi(a)\phi(b)\phi(1)] + [\phi(b)\phi(a_2)] + [\phi(a)\phi(b_2)] + [\phi(a_2)\phi(b_2)] \\
&= \phi(a)\phi(b)
\end{aligned}$$

où l'on a utilisé la liberté de a_2 et b_2 pour conclure que $\phi(a_2b_2) = 0$
$\square$

Cependant le cas général n'est pas si simple et l'on n'a pas l'identité $\phi(a_1b_1a_2b_2) = \phi(a_1)\phi(b_1)\phi(a_2)\phi(b_2)$ pour des éléments $a_1, a_2 \in A_a$, $b_1, b_2 \in A_b$ dans des sous-algèbres libres A_a, A_b. Le même raisonnement que ci-dessus montrerait la formule suivante :

$$\phi(a_1b_1a_2b_2) = \phi(a_1a_2)\phi(b_1)\phi(b_2) + \phi(a_1)\phi(a_2)\phi(b_1b_2) - \phi(a_1)\phi(ba_2)\phi(b_1)\phi(b_2)$$

Cependant comme précédemment on remarque que la connaissance de ϕ sur A_a et A_b permet d'en déduire ϕ sur les éléments de la forme $a_1b_1a_2b_2$, conformément à ce que l'on attendait. La proposition suivante rend ce constat plus précis :

Proposition 3 (Coefficients Universels) *Soit $(A_i)_I$ des sous-algèbres libres de A et $a_1, a_2, .., a_n$ des éléments de ces sous-algèbres avec $a_j \in A_{i(j)}$*
Soit Π la partition de $\{1, 2, \ldots, n\}$ associée à la relation d'équivalence $a \sim b$ ssi $i(a) = i(b)$. On définit alors $\phi_\pi = \Pi_{\{i_1<i_2<..<i_r\}\in\pi}\phi(a_{i_1}a_{i_2}..a_{i_r})$. Alors il existe des coefficients universels $c(\pi, \Pi)$ tels que :

$$\phi(a_1a_2..a_n) = \sum_{\pi\prec\Pi} c(\pi, \Pi)\phi_\pi$$

où la somme est faites sur toutes les sous-partitions π plus fines que Π.

Démonstration : La démonstration est une généralisation du cas de deux variables traité plus haut. On décompose chaque a_i sous la forme $a_i = a_i^{'} + a_i^{''}$ où $a_i^{'} = \phi(a_i)1_A$ et on utilise la liberté des $(A_i)_I$ pour conclure. $\square$

Remarque 4 *les coefficients $c(\pi, \Pi)$ ne sont pas simples à déterminer explicitement mais cela importe peu pour la suite de l'exposé.*

On utilisera par la suite le lemme suivant, dont on reconnaîtra immédiatement l'analogue en probabilités classiques :

Lemme 5 (Regroupement) *Supposons que $(f_i)_I$ est une famille de variables aléatoires libres et $S = \bigcup_{s\in S} J_s$ une partition de I. Alors les sous-ensembles $\{f_j | j \in J_s\}_{s\in S}$ sont libres.*

Démonstration : Notons et $H_s = \{f_j | j \in J_s\}$ et $A(H)$ la sous-algèbre unitaire engendrée par le sous-ensemble H. On supposera de plus, sans perte de généralité, que $1_A \in H_s$ pour tout $s \in S$.
Soit alors $a_1, a_2, .., a_n$ des variables aléatoires, $a_i \in A(H_{s(i)})$, $s(k) \neq s(k+1)$,

$\phi(a_i) = 0$. Il suffit de montrer que ces conditions entraînent $\phi(a_1 a_2..a_n) = 0$. Or si $a \in A(H_s)$ alors a s'écrit sous la forme $a = \sum_k \prod_m f_{i(k,m)}$ où les sommes/produits sont finis, et $i(k,m) \neq i(k,m+1)$. De plus on peut supposer que $\phi(a_{i(k,m)}) = 0$ pour tout $a_{i(k,m)}$ en utilisant la décomposition habituelle d'un élément en somme de deux éléments dont l'un est lié à 1_A et l'autre d'espérance nulle. La conclusion suit en développant le produit $a_1 a_2..a_n$ et en utilisant la liberté des f_i. $\square$

On introduit maintenant le produit libre d'algèbres. Cela signifie que l'on peut voir des algèbres $(A_i)_I$ comme des sous-algèbres d'une même algèbre A de manière à ce que les $(A_i)_I$ soient libres. C'est en quelques sorte l'analogue du groupe libre engendré par des générateurs a_i n'ayant pas de relations entre eux. Plus précisément :

Théorème 6 (Produit Libre) *Soient $(A_i)_I$ des $\mathbb{C}$-algèbres unitaires munies de fonctions d'états $\phi_i : A_i \to \mathbb{C}$. Alors il existe une $\mathbb{C}$-algèbre unitaire A munie d'une fonction d'état ϕ et des injections $\tau_i : A_i \to A$ vérifiant :*
- $\phi_i = \phi \circ \tau_i$
- *les sous-algèbres $\tau_i(A_i)$ sont libres*

Démonstration : Notons A_i^0 l'ensemble des éléments d'espérance nulle dans (A_i, ϕ_i). Alors on peut prendre pour A, ϕ l'espace de probabilité non-commutatif

$$(\mathbb{C}1 \oplus (\oplus_{n \geq 1}(\oplus_{i_1 \neq i_2 \neq .. \neq i_n \in I} A_{i_1}^0 \otimes ... \otimes A_{i_n}^0)), \phi)$$

Le produit $(a_1 \otimes .. \otimes a_n) \times (b_1 \otimes .. \otimes b_m)$ est défini récursivement par :
- si $i_n \neq i_1$ ce produit vaut $a_1 \otimes .. \otimes a_n \otimes b_1 \otimes .. \otimes b_m$
- sinon il vaut $(a_1 \otimes .. \otimes a_{n-1} \otimes a \otimes b_2 \otimes .. \otimes b_m) + (\lambda a_1 \otimes .. \otimes a_{n-1}) \times (b_2 \otimes .. \otimes b_m)$ en prenant $a_n b_1 = \lambda 1 + a$ et $a \in A_{i_n}^0$

La fonction d'état est alors parfaitement définie en choisissant $\phi(1) = 1$ et $\phi = 0$ sur les $A_{i_1}^0 \otimes .. \otimes A_{i_n}^0$. $\square$

1.2 Propriétés asymptotiques

Définition 7 (Distribution jointe) *Soient $(f_i)_I$ des variables aléatoires de (A, ϕ), $\mathbb{C}\langle X_i | i \in I \rangle$ l'algèbre unitaire libre générée par les $(X_i)_I$ et $h : \mathbb{C}\langle X_i | i \in I\rangle \to A$ l'unique morphisme d'algèbre unitaire vérifiant $h(X_i) = f_i$. Alors la distribution jointe des $(f_i)_I$ est la fonctionnelle $\mu : \mathbb{C}\langle X_i | i \in I\rangle \to \mathbb{C}$ définie par $\mu = \phi \circ h$*

Exemple : Soient A et B deux matrices de $(M_n(\mathbb{C}), \tau_n)$. On considère $\mathbb{C}\langle X, Y\rangle$ l'algèbre unitaire libre à 2 éléments.(on peut penser à $\mathbb{C}\langle X, Y\rangle$ comme l'analogue non commutatif de l'ensemble des polynômes à 2 variables $\mathbb{C}(X, Y)$). Alors la distribution jointe μ de A, B satisfait par exemple $\mu(1 + XYX + Y^2) = \frac{1}{n} Tr(Id + ABA + B^2)$.

Comme en probabilités classiques où l'on parle de convergence en loi (convergence faible), on trouve un analogue en probabilité libre :

Définition 8 (Distribution limite) *Soient* $(f_{i,n})_{i\in I,n\in\mathbb{N}}$ *des variables aléatoires,* $f_{i,n} \in (A_n, \phi_n)$, μ_n *la distribution jointe des* $(f_{i,n})_I$. *Alors cette famille de variables possède une distribution limite* $\mu : \mathbb{C}\langle X_i | i \in I\rangle \to \mathbb{C}$ *lorsque* n *tend vers* $+\infty$ *si pour tout* $a \in \mathbb{C}\langle X_i | i \in I\rangle$, $\lim_{n\to\infty} \mu_n(a) = \mu(a)$

Exemple : la famille $(A_n) \in (M_n(\mathbb{C}), \tau_n)$ où A_n est la matrice de taille n ayant pour coefficients $\frac{1}{n}$ partout admet la distribution limite nulle.

On peut alors définir la liberté asymptotique d'une famille de variables aléatoires.

Définition 9 (Liberté asymptotique) *Soient* $(f_{i,n})_{i\in I,n\in\mathbb{N}}$ *des variables aléatoires,* $f_{i,n} \in (A_n, \phi_n)$, $I = \bigcup_{s\in S} I_s$ *une partition de* I. *Alors la famille de sous-ensembles* $((f_{i,n})_{i\in I_s})_s$ *est dite asymptotiquement libre lorsque* $n \to \infty$ *si les* $(f_{i,n})$ *admettent une distribution limite* μ *et que la famille de sous-ensembles* $((X_i)_{i\in I_s})_s$ *est libre dans* $\mathbb{C}\langle X_i | i \in I\rangle$.

Les sections suivantes donneront des critères pour qu'une famille de variables aléatoires soit asymptotiquement libre.

2 Théorème central limite

On va démontrer dans cette section l'analogue du théorème centrale limite en probabilités classiques. Ce dernier montrait que la loi normale apparaissait naturellement lorsqu'on "moyennait" des variables aléatoires indépendantes de même loi et de carré sommables. Ici, on va montrer que la loi circulaire apparaît dans des circonstances analogues comme "moyenne" de variables aléatoires libres. Plus précisément :

Théorème 10 (Théorème central limite libre) *Soit* (A, ϕ) *un espace de probabilité non-commutatif et* $(a_i)_{i\geq 1}$ *des variables aléatoires libres vérifiant :*
- $\phi(a_i) = 0$
- $\phi(a_i^2) = 1$
- $\sup_{i\geq 1} |\phi(a_i^k)| < \infty$ *pour tout* $k \geq 1$

Alors pour tout $k \geq 1$, $\phi((\frac{a_1+a_2+..+a_n}{\sqrt{n}})^k) \to m_k(w(x)dx)$ *où* $m_k(w(x)dx) = \int_{\mathbb{R}} x^k w(x)dx$ *est le* k*-ième moment de la loi circulaire* $w(x) = \frac{\sqrt{4-x^2}}{2\pi} 1_{[-2;+2]}$

Démonstration :
Introduisons quelque notations :
- Si π est une partition de $[1; n]$ alors on numérote les classes de π par l'ordre d'apparition de leur plus petit éléments. Alors $\pi(k)$ désignera le numéro de la classe de k. Par exemple $\{1; 2, 7\}, \{3; 5\}, \{4; 6\}$ est une partition de $[1, 7]$ et $\pi(1) = \pi(2) = \pi(7) = 1, \pi(4) = \pi(6) = 3$.
- $\Pi_{s,n}$ désigne l'ensemble des partitions de $[1; n]$ en s classes.

Pour démontrer le théorème examinons un peu plus en détails le développement de $\phi((a_1+a_2+..+a_n)^k)$. Choisissons $k \geq 1$ et $n \geq k$. Alors en développant

$(a_1 + a_2 + .. + a_n)^k$ on voit que :

$$\phi((a_1 + a_2 + .. + a_n)^k) = \sum_{s=1}^{k} \sum_{\pi \in \Pi_{s,k}} \sum_{(j_1,..,j_s) \in [1;n]^s distincts} \phi(a_{j_{\pi(1)}} a_{j_{\pi(2)}} .. a_{j_{\pi(k)}})$$

L'idée de la preuve est alors de montrer que seul les partitions en $\frac{k}{2}$ parties ne sont pas négligeables et ensuite de calculer explicitement le terme qui reste, à savoir

$$\sum_{\pi \in \Pi_{\frac{k}{2},k}} \sum_{(j_1,..,j_s) \in [1;n]^s distincts} \phi(a_{j_{\pi(1)}} a_{j_{\pi(2)}} .. a_{j_{\pi(k)}})$$

Par commodité, appelons $S_{1,n}$ la somme sur les partitions en $s < \frac{k}{2}$ parties, $S_{2,n}$ la somme sur les partitions en $\frac{k}{2}$ éléments, $S_{3,n}$ les termes restant.

- $S_{1,n} = o(n^{\frac{k}{2}})$:
  Le fait que les moments des a_i soient uniformément bornés implique qu'il existe une constante C_k telle que $\phi(a_{i_1} a_{i_2} .. a_{i_k}) < C_k$ pour tout $a_{i_1}, a_{i_2}, ..., a_{i_k}$. Posons $N_k = \sum_{s<\frac{k}{2}} \sum_{\pi \in \Pi_{s,k}} 1$. Alors on majore facilement $\frac{|S_{1,n}|}{n^{\frac{k}{2}}}$, en notant K le plus grand entier strictement inférieur à $\frac{k}{2}$ et $A_n^K = n(n-1)(n-2)..(n-K+1)$ le nombre de K-arrangements de $[1, n]$:
  $$\frac{|S_{1,n}|}{n^{\frac{k}{2}}} < N_k C_k \frac{A_n^K}{n^{\frac{k}{2}}} = o(1)$$
- $S_{3,n} = 0$:
  En effet, pour toute partition $\pi \in \Pi_s$ avec $s > \frac{k}{2}$, il existe une classe de π réduit à un élément. Cela entraîne que $\phi(a_{j_{\pi(1)}} a_{j_{\pi(2)}} .. a_{j_{\pi(k)}}) = 0$, conséquence immédiate de la proposition 3.
- Calcul de $S_{2,n}$:
  On suppose $k = 2j$ pair. Alors, comme nous venons de le voir plus haut, seules les partitions n'ayant pas de classe réduit à un élément participent réellement à la somme. Donc dans le cas de $s = \frac{k}{2}$, seules les partitions ayant toutes leurs classes avec exactement 2 éléments sont à prendre en compte. Le lemme suivant permet de calculer la valeur exacte de $S_{2,n}$.

  Lemme 11 *Une partition π par paires de $\{1, 2, ..., k = 2j\}$ est dite non-croisées s'il n'existe pas $a < b < c < d$ vérifiant $a \sim c$ et $b \sim d$. On note P_kl'ensemble de ces partitions non-croisées.*
  Soit π une partition par paires de $\{1, 2, ..., k = 2j\}$ et $a_1, a_2, .., a_j$ des éléments libres comme dans l'énoncé du théorème. Alors si on pose $b = a_{\pi(1)} a_{\pi(2)} ... a_{\pi(k)}$, $\phi(b) = 1$ si π est non-croisée et $\phi(b) = 0$ sinon.
  Démonstration : Montrons ce lemme par récurrence sur $k = 2j$.
  - Le cas $k = 2$ est évident : $\phi(a^2) = 1$
  - $k = 2j$, $j \geq 2$. Plusieurs cas se présentent :
    - Il n'existe pas de i tel que $i \sim i + 1$. Alors par liberté des a_i et le fait qu'il sont tous d'espérance nulle, $\phi(b) = 0$. Ce cas ne peut se produire que si la partition est non croisée. (facile)

– Il existe i tel que $i \sim i+1$, $\pi(i) = \pi(i+1) = c$. Alors si on appelle $b' = a_{\pi(1)}...a_{\pi(i-1)}a_{\pi(i+2)}...a_{\pi(k)}$, la proposition 3 montre immédiatement que $\phi(b) = \phi(a_c^2)\phi(b') = \phi(b')$. L'hypothèse de récurrence permet de conclure car b' est non-croisée ssi b est non-croisée.

Ainsi $\frac{S_{2,n}}{n^{\frac{k}{2}}} = Card(P_k)\frac{n(n-1)(n-2)..(n-\frac{k}{2})}{n^{\frac{k}{2}}}$. De cela on en conclut que

$$\lim_{n\to\infty} \frac{S_{2,n}}{n^{\frac{k}{2}}} = Card(P_k)$$

Le cardinal u_j de $P_{k=2j}$ peut se calculer en remarquant que la suite $\{u_j\}$ vérifie la relation de récurrence des nombres de Catalan : $u_k = u_0u_{k-1} + u_1u_{k-2} + .. + u_{k-1}u_0$. Ainsi $u_j = Card(P_{k=2j}) = \frac{1}{j+1}C_{2j}^j$. Cela finit la preuve du théorème car un calcul montrerait que les moments de la loi circulaire vérifient $m_k(w(x)dx) = Card(P_k)$. $\square$

$\square$

3 Un résultat intermédiaire

Théorème 12 *Soit (A, ϕ) un espace de probabilité non-commutatif, avec ϕ une trace, et prenons $(T_j)_{j\in\mathbb{N}}$ une suite de variables aléatoires non-commutatives dans A. Soit, de plus, Δ une sous-algèbre de A contenant 1 et soit $\beta : \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ une injection.*

On définit les propriétés :

P1 *Les deux conditions suivantes sont vérifiées :*

1. *pour tout $m \in \mathbb{N}$ et $D_1, \ldots, D_m \in \Delta$ on a*

$$\sup_{j_1,\ldots,j_m\in\mathbb{N}} |\phi(T_{j_1}D_1 \ldots T_{j_m}D_m)| < \infty$$

2. *pour tout $m \in \mathbb{N}$, $\alpha : \{1, \ldots, m\} \to \mathbb{N}$ et $D_j \in \Delta$, $(1 \le j \le m)$. $\phi(T_{\alpha(1)}D_1 \ldots T_{\alpha(m)}D_m)$ est égal à :*
a) 0 si $|\alpha^{-1}(\alpha(1))| = 1$
b) $\phi(D_1)\phi(D_2T_{\alpha(3)}D_3 \ldots T_{\alpha(m)}D_m)$ si $\alpha(1) = \alpha(2)$ et $\forall p \in \mathbb{N}; |\alpha^{-1}(p)| \le 2$
c) 0 si $\alpha(p) \ne \alpha(p+1)$ pour tout $1 \le p \le m-1$, $\alpha(1) \ne \alpha(m)$ et $\forall p \in \mathbb{N}; |\alpha(p)| \le 2$

P2 *On pose*

$$X_{m,n} = \frac{1}{\sqrt{n}} \sum_{j=1}^{n} T_{\beta(m,j)}$$

La famille de sous-ensembles $(\Delta, (\{X_{m,n}\})_{m\in\mathbb{N}})$ est asymptotiquement libre quand $n \to \infty$ et de plus, pour chaque $m \in \mathbb{N}$ la distribution limite de $X_{m,n}$est donné par les moments de la loi semi-circulaire de premier moment 0 et deuxième moment 1 (i.e. la loi sur $\mathbb{R}$ de densité $\frac{1}{2\pi}\sqrt{4-x^2}1_{[-2,2]}$).

P3 *$(\Delta, (\{T_j\})_{j\in\mathbb{N}})$ est une famille libre de sous-ensembles, pour tout $j \in \mathbb{N}$, $\phi(T_j) = 0$, $\phi(T_j^2) = 1$ et $\forall p \in \mathbb{N}$, $\sup_{j\in\mathbb{N}} \phi(T_j)^p < \infty$*

Les implications suivantes sont vraies : **P1** $\Rightarrow$ **P2**, **P3** $\Rightarrow$ **P1** *et* **P3** $\Rightarrow$ **P2**

Avant de commencer la démonstration on va faire quelques petites remarques pour aider le lecteur dans la compréhension des notations un peu lourdes :
$T_{j_1}D_1\ldots T_{j_m}D_m$ est la forme générale, à somme près, d'un élément de l'algèbre engendrée par $(\Delta,(T_j)_{j\in\mathbb{N}})$ car les D_i peuvent être égaux a 1. Par exemple T_1^2 s'écrit $T_1 1 T_1 1$
Dans la condition **P1** 2 on donne la valeur de $\phi(T_{\alpha(1)}D_1\ldots T_{\alpha(m)}D_m)$ dans les cas suivants :

- s'il y a un T_i qui apparaît une seule fois, alors la valeur est 0 (en utilisant la propriété de trace de ϕ on se ramener au cas ou le T_i en question est en première position et ensuite on applique a))
- si chaque T_i apparaît exactement deux fois, soit on est dans la situation c) soit il existe j tel que $\alpha(j)=\alpha(j+1)$ (avec la convention $m+1=1$). Dans ce cas, quitte a utiliser la propriété de trace de ϕ, on peut supposer $j=1$ et on peut utiliser b) pour se ramener a un monôme plus court. En itérant on s'aperçoit qu'on peut calculer la valeur de $\phi(T_{\alpha(1)}D_1\ldots T_{\alpha(m)}D_m)$ que en fonction des $\phi(D_j)$.

Démonstration : On va faire la démonstration en trois étapes :
Première étape **P3** $\Rightarrow$ **P1**
Montrons le **P1** 1 : fixons $m\in\mathbb{N}$ et $D_1,\ldots,D_m\in\Delta$. Soit $J_1,\ldots,J_k$ une partition de $\{1,\ldots,m\}$ et supposons $(j_\alpha=j_\beta)\Leftrightarrow(\alpha$ et β sont dans le meme $J_i)$. On a vu dans la proposition 3 que dans ce cas $\phi(T_{j_1}D_1\ldots T_{j_m}D_m)$ s'exprime comme un polynôme en les moments des T_j (i.e. les $\phi(T_{j_i}^l)$ avec $i\in\mathbb{N}$ et $l\leq m$) et en les $\phi(D_{i_1}\ldots D_{i_p})$ ou $1\leq i_1<\ldots<i_p\leq m$. Mais on a supposé les moments des T_j bornes quand j varie dans $\mathbb{N}$ et les D_i sont fixés, donc $|\phi(T_{j_1}D_1\ldots T_{j_m}D_m)|$ est borne par une constante qui ne dépend que de la partition. Mais comme pour un m fixe il y à qu'un nombre fini de telles partitions on déduit que $\sup_{j_1,\ldots,j_m\in\mathbb{N}}|\phi(T_{j_1}D_1\ldots T_{j_m}D_m)|<\infty$ donc le 1.

Le 2 : a) si $|\alpha^{-1}(\alpha(1))|=1$ alors $T_{\alpha(1)}$ est libre de $\{T_{\alpha(2)},\ldots,T_{\alpha(m)}\}\cup\Delta$ d'où :

$$\phi(T_{\alpha(1)}D_1\ldots T_{\alpha(m)}D_m)=\phi(T_{\alpha(1)})\phi(D_1T_{\alpha(2)}\ldots T_{\alpha(m)}D_m)=0$$

car $\phi(T_{\alpha(1)})=0$
b) On décompose chaque D_j comme $\phi(D_j)1+(D_j-\phi(D_j)1)$ et on utilise la linéarité de ϕ pour voir qu'il suffit de démontrer la propriété en supposant en plus que pour chaque j on a soit $D_j=1$ soit $\phi(D_j)=0$.

Si $D_1=1$ on a, par le même argument de liberté que avant :

$$\phi(T_{\alpha(1)}D_1\ldots T_{\alpha(m)}D_m)=\phi(T_{\alpha(1)}^2D_2\ldots T_{\alpha(m)}D_m)=$$

$$\phi(T_{\alpha(1)}^2)\phi(D_2T_{\alpha(3)}\ldots T_{\alpha(m)}D_m)=\phi(D_2T_{\alpha(3)}\ldots T_{\alpha(m)}D_m)$$

donc la propriété est vérifiée.

Si $\phi(D_1)=0$ montrons que $\phi(T_{\alpha(1)}D_1\ldots T_{\alpha(m)}D_m)=0$.
Si il existe j tel que $\alpha(j)=\alpha(j+1)$ et $D_j=1$, en utilisant le fait que ϕ est

une trace et le même argument de liberté que avant, on fait la manipulation suivante :

$$\phi(T_{\alpha(1)}D_1\dots T_{\alpha(m)}D_m) \overset{not}{=} \phi(\Omega_1 T^2_{\alpha(j)}\Omega_2) =$$

$$\phi(T^2_{\alpha(j)}\Omega_2\Omega_1) = \phi(\Omega_2\Omega_1) = \phi(\Omega_1\Omega_2)$$

En iterant ce procédé, et en observant que le terme $T_{\alpha(1)}D_1T_{\alpha(1)}$ ne s'élimine jamais, on arrive à un produit non-vide ou $\alpha(j) = \alpha(j+1) \Rightarrow \phi(D_j) = 0$. Mais on voit que ce produit est un produit de termes consécutif libres et avec chacun des termes de valuation 0, donc sa valuation aussi est nulle.
c) On fait la même décomposition des D_j que pour b) et on se ramène au cas ou les D_j sont soit 1 soit de valuation nulle. Si on regarde les groupes de deux termes consécutifs du produit $T_{\alpha(1)}D_1\dots T_{\alpha(m)}D_m$ on voit qu'il sont forcement d'une de ces formes : $T_{\alpha(j)}D_j$ avec $\phi(D_j) = 0$; $D_jT_{\alpha(j+1)}$ avec $\phi(D_j) = 0$ ou $T_{\alpha(j)}T_{\alpha(j+1)}$ (si $D_j = 1$). Comme on a supposé que $\alpha(j) \neq \alpha(j+1)$ pour tout j on s'aperçoit que tous deux termes consécutifs sont libres et de valuation 0, on en déduit que le produit est aussi de valuation nulle.
Deuxième étape **P3** $\Rightarrow$ **P2**
On suppose que $((T_j)_{j\in\mathbb{N}}, \Delta)$ est une famille libre. Soit $C = \mathbb{C} < (X_j)_{j\in\mathbb{N}}, \Delta >$, l'algèbre libre, non-commutative engendrée par les $(X_j)_{j\in\mathbb{N}}$ et par Δ. On doit montrer que pour tout $k \in \mathbb{N}$, $m_1, \dots, m_k \in \mathbb{N}$ et $D_1, \dots, D_k \in \Delta$, $\phi(X_{m_1,n}D_1\dots X_{m_k,n}D_k)$ converge vers une limite qu'on va noter $\Phi(X_{m_1}D_1\dots X_{m_k}D_k)$, que Φ ainsi défini se prolonge en une fonction d'état sur C et que $((X_j)_{j\in\mathbb{N}}, \Delta)$ est une famille libre dans (C, Φ). Si on suppose que l'expression converge toujours, Φ se prolonge en une fonction d'état sur C par définition de C comme l'algèbre *libre* engendrée par $((X_j)_{j\in\mathbb{N}}, \Delta)$. De plus, comme $((\{T_j\})_{j\in\mathbb{N}}, \Delta)$ est une famille libre, on déduit que $((\{X_{j,n}\})_{j\in\mathbb{N}}, \Delta)$ en est une aussi et donc que $((\{X_j\})_{j\in\mathbb{N}}, \Delta)$ est une famille libre de (C, Φ).

On a donc juste à montrer que pour tout $k \in \mathbb{N}$, $m_1, \dots, m_k \in \mathbb{N}$ et $D_1, \dots, D_k \in \Delta$, $\phi(X_{m_1,n}D_1\dots X_{m_k,n}D_k)$ converge.

Fixons un tel monôme. On sais que pour tout $n \in \mathbb{N}$ la valuation de ce monôme s'exprime comme polynôme (indépendant de n) en les moments d'ordre au plus k des $X_{m_i,n})_{1\leq i\leq k}$. Mais par le théorème central limite, en observant que $\phi(T_j) = 0$ et que $\phi(T_j^2) = 1$ pour tout $j \in \mathbb{N}$, on obtient que les moments de $(X_{m_i,n})$ convergent quand $n \to \infty$ vers les moments de la loi semi-circulaire de premier moment 0 et deuxième moment 1. On a donc obtenu **P2**.
Troisième étape **P1** $\Rightarrow$ **P2**
Supposons que $((T_j)_{j\in\mathbb{N}}, \Delta)$ satisfait $P1$. Notons $\overline{A}$ le produit amalgamé libre de Δ et des sous-algèbres A_j de A engendrées par les $\{T_j\}$. On va noter $\overline{T}_j$ les correspondants des T_j dans $\overline{A}$ et de même pour les $X_{m,n}$. On a déjà vu que les $(\overline{X}_{m,n})_{m,n\in\mathbb{N}}$ vérifient $P2$. Il suffit donc de montrer que, pour tout $k \in \mathbb{N}$, $m_1, \dots, m_k \in \mathbb{N}$ et $D_1, \dots, D_k \in \Delta$, $\phi(X_{m_1,n}D_1\dots X_{m_k,n}D_k)$ converge vers $lim_{n\to\infty}\phi(\overline{X}_{m_1,n}D_1\dots\overline{X}_{m_k,n}D_k)$, ou encore que,

$$\lim_{n\to\infty}\big(\phi(X_{m_1,n}D_1\dots X_{m_k,n}D_k) - \phi(\overline{X}_{m_1,n}D_1\dots\overline{X}_{m_k,n}D_k)\big) = 0$$

Fixons un tel monôme et $m_1, \ldots, m_k \in \mathbb{N}$, et écrivons :

$$\phi(X_{m_1,n}D_1 \ldots X_{m_k,n}D_k) = \phi(\prod_{i=1}^{k} n^{-1/2} \sum_{j=1}^{n} T_{\beta(m_i,j)}D_i) =$$

$$n^{-k/2}\phi(\sum_{1 \leq j_1, \ldots, j_k \leq n} T_{\beta(m_1,j_1)}D_1 \ldots T_{\beta(m_k,j_k)}D_k)$$

Notons cette quantité χ_n. Soient

$$P_n = (\{m_1, \ldots, m_k\} \times \{1, \ldots, n\})^k$$

$$Q_n = \{(p_1, \ldots, p_k) \in P_n \text{ avec } \forall 1 \leq i \leq k, \quad \exists! j \neq i \text{ tel que } p_i = p_j\}$$

et R_n l'ensemble des $(p_1, \ldots, p_k) \in P_n$ tel que chaque p_i apparaît au moins deux fois dans le k-uplet et qu'il y en a au moins un qui apparaît au moins trois fois. Notons enfin, pour $I = (p_1, \ldots, p_k) \in P_n$, $\pi_I = T_{\beta(p_1)}D_1 \ldots T_{\beta(p_k)}D_k$. On voit alors que pour $I \in P_n$ il existe un coefficient $c_I \in \{0, 1\}$, qui ne dépend que de I, tel que $\phi(X_{m_1,n}D_1 \ldots X_{m_k,n}D_k) = n^{-k/2}\phi(\sum_{I \in P_n} c_I \pi_I)$.

En utilisant **P1** 2 b) on déduit que $\phi(\pi_I) = 0$ si $I \in P_n \setminus (Q_n \cup R_n)$.
Les propriétés 2 b) et 2 c) nous disent que, pour $I \in Q_n$, $\phi(\pi_I)$ est un produit de $\phi(D_j)$ et que sa forme ne dépend que de I. Mais comme on a démontré avant que les $(\overline{T}_j)_{j \in \mathbb{N}}$ vérifient aussi **P1**, on peut calculer $\phi(\overline{\pi}_I)$ de la même façon et on obtient le même résultat. On a donc $\phi(\pi_I) = \phi(\overline{\pi}_I)$ si $I \in Q_n$.
On est donc arrive a :

$$\phi(X_{m_1,n}D_1 \ldots X_{m_k,n}D_k) - \phi(\overline{X}_{m_1,n}D_1 \ldots \overline{X}_{m_k,n}D_k) =$$

$$n^{-k/2} \sum_{I \in R_n} c_I(\phi(\pi_I) - \phi(\overline{\pi}_I)).$$

On va montrer que $\sum_{I \in R_n} c_I \phi(\pi_I)$ tend vers 0 ; comme **P1** 1 nous dit qu'il existe $C > 0$ telle que $\phi(\pi_I) \leq C$ pour tout $I \in P_n$, il suffit de montrer que $|R_n| = o(n^{k/2})$. On rappelle que $P_n = (\{m_1, \ldots, m_k\} \times \{1, \ldots, n\})^k$, notons $E_n = \{m_1, \ldots, m_k\} \times \{1, \ldots, n\}$. On remarque que $(E_n)_{n \in \mathbb{N}}$ et $(R_n)_{n \in \mathbb{N}}$ sont des suites croissantes d'ensembles. Pour $I \in R_n$ on note H_I l'ensemble des $p \in E_n$ qui intervient dans p. Alors, pour $I \in R_n$, $|H_I| < k/2$, d'ou :

$$R_n = \bigsqcup_{\substack{H \subset E_n \\ |H| < k/2}} \{I \in R_n \text{ avec } H_I = H\}$$

On voit facilement que pour $H \subset E_n, |H| < k/2$ la valeur $|\{I \in R_n \text{ avec } H_I = H\}|$ ne dépend que de $|H|$, notons la $A_{|H|}$. On a donc :

$$|R_n| \leq \sum_{1 \leq i < k/2} \binom{nk}{i} A_i = \sum_{1 \leq i < k/2} O(n^{\frac{k-1}{2}}) = o(n^{n/2})$$

Car $\binom{nk}{i} \leq n^i \frac{r^i}{s!}$ et ici $i \leq \frac{k-1}{2}$ et car tous les autres coefficients ainsi que la somme sont indépendants de n.

On a donc montre que $n^{-k/2} \sum_{I \in R_n} c_I \phi(\pi_I) \longrightarrow 0$, on fait la même chose pour les $\overline{\pi}$ et on en déduit que $\lim_{n\to\infty} n^{-k/2} \sum_{I \in R_n} c_I(\phi(\pi_I) - \phi(\overline{\pi}_I)) = 0$ ce qu'il fallait montrer. $\square$

4 Applications aux matrices aléatoires

Dans la suite on va utiliser ce théorème pour la démonstration d'un résultat plus concret concernant les grandes matrices hermitiennes, mais avant cela on va encore introduire quelques notations.

On se place sur un espace de probabilité Ω muni d'une mesure de probabilité sans atomes, $d\omega$. Notons $L = \bigcap_{1 \leq p < \infty} L^p(\Omega, d\omega, \mathbb{C})$ et $M_n = \mathcal{M}_n(L)$, les matrices $n \times n$ a coefficients dans L, c'est une *-algèbre. On va noter aussi $\mathcal{M}_n$ la sous-algèbre de M_n des matrices constantes et $\Delta_n \subset \mathcal{M}_n \subset M_n$ la sous-algèbre des matrices diagonales constantes. On défini sur M_n la trace normalisée par $\phi_n(A) = \frac{1}{n} E[tr(A)]$. On peut facilement vérifier que ϕ_n est une fonction d'état sur M_n. Notons enfin $(e(i,j;n))_{1 \leq i,j \leq n}$ la base canonique de $\mathcal{M}_n$.

Théorème 13 *Considérons, pour chaque $s, n \in \mathbb{N}$, une matrice*

$$Y(s,n) = (a(j,i;s,n))_{1 \leq i,j \leq n} \in M_n.$$

On impose les conditions suivantes : $\forall s, n \in \mathbb{N}, \quad Y(s,n) = \overline{{}^tY(s,n)}$ et les variables $\{Re(a(i,j;s,n)) | 1 \leq i \leq j \leq n\} \cup \{Im(a(i,j;s,n)) | 1 \leq i < j \leq n\}$ sont indépendantes et de lois gaussiennes avec :
- *$E(a(i,j;s,n)) = 0$, pour $1 \leq i, j \leq n$*
- *$E((Re(a(i,j;s,n)))^2) = E((Im(a(i,j;s,n)))^2) = \frac{1}{2n}$, si $1 \leq i < j \leq n$*
- *$E((Re(a(i,i;s,n)))^2) = \frac{1}{n}$, pour $1 \leq i \leq n$.*

Soient encore, pour chaque $n \in \mathbb{N}$, $(D(k,n))_{k \in \mathbb{N}}$, des éléments de Δ_n avec $\forall k \in \mathbb{N}, \quad \sup_{n \in \mathbb{N}} \|D(k,n)\|_\infty < \infty$ et tels que la famille $(D(k,n))_{k \in \mathbb{N}}$ ait une distribution limite quand $n \to \infty$.

Alors la famille de sous-ensembles $(\{Y(s,n)\}_{s \in \mathbb{N}}, \{D(k,n) | k \in \mathbb{N}\})$ est asymptotiquement libre quand $n \to \infty$. De plus, les distributions limites des $Y(s,n)$ sont donnés par moments de la loi semi-circulaire.

Démonstration : Notons $(d(i;k,n))_{1 \leq i \leq n}$ les éléments diagonaux de $D(k,n)$ et supposons que $D(0,n) = I_n$ et qu'il existe $\theta : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ telle que, pour tout i, j, n, $D(i,n)D(j,n) = D(\theta(i,j),n)$; on peut le faire sans perte de généralité. La démonstration va avoir plusieurs étapes :

Première étape

Fixons $s_1, \ldots, s_m \in \mathbb{N}$ et $t_1 \ldots, t_m \in \mathbb{N}$; on va montrer que

$$\sup_{n \in \mathbb{N}} |\phi_n(Y(s_1,n)D(t_1,n) \ldots Y(s_m,n)D(t_m,n))| < \infty.$$

Posons :

$$\chi_n = |\phi_n(Y(s_1,n)D(t_1,n) \ldots Y(s_m,n)D(t_m,n))| =$$

$$\left|\phi_n(\prod_{k=1}^{m}(\sum_{1\le i,j\le n} a(i,j;s_k,n)e(i,j;n)\sum_{1\le i\le n} d(i;t_k,n)e(i,i;n)))\right| =$$

$$\left|\phi_n(\prod_{k=1}^{m}\sum_{1\le i,j\le n} a(i,j;s_k,n)d(j;t_k,n)e(i,j;n))\right| =$$

$$\Big|\sum_{\substack{1\le i_1,\ldots,i_m\le n\\ 1\le j_1,\ldots,j_m\le n}} \phi_n(\prod_{k=1}^{m} a(i_k,j_k;s_k,n)d(j_k,t_k,n)e(i_k,j_k;n))\Big|$$

Mais on voit que le produit est non-nul que si $j_k = i_{k+1}, \quad k \in \{1,\ldots,m-1\}$ et si on veut en plus que la valeur non-nulle du produit soit sur une case de la diagonale (pour être prise un compte par ϕ_n) il faut aussi avoir $j_m = i_1$. Des maintenant on va utiliser la convention $m+1=1$ pour les indices. On a donc :

$$\chi_n = \Big|\sum_{1\le i_1,\ldots,i_m\le n} \phi_n(\prod_{k=1}^{m} a(i_k,i_{k+1};s_k,n)d(i_{k+1},t_k,n)e(i_k,i_{k+1};n))\Big|$$

$$\le \frac{1}{n}\sum_{1\le i_1,\ldots,i_m\le n}\Big|\prod_{k=1}^{m} d(i_k,t_k,n)E[\prod_{k=1}^{m} a(i_k,i_{k+1};s_k,n)]\Big|$$

Mais la condition de bornitude sur les $D(t,n)$ nous garanti l'existence d'une constante c, ne dépendent que des $t_1,\ldots,t_m$, telle que $c \le |\prod_{k=1}^{n} D(j_k,t,n)|$, $\forall n\in\mathbb{N}$. On a donc :

$$\chi_n \le \frac{c}{n}\sum_{1\le i_1,\ldots,i_m\le n}\Big|E[\prod_{k=1}^{m} a(i_k,i_{k+1};s_k,n)]\Big|.$$

Pour le calcul de cette quantité on introduit le lemme suivant, qu'on peut démontrer soit en intégrant par parties, soit en appliquant une rotation au vecteur gaussien (X,Y).

Lemme 14 *Soit X,Y deux variables aléatoires réelles, indépendantes et de même loi gaussienne et centrée. Alors, pour $\alpha,\beta\in\mathbb{N}, \quad \alpha\ne\beta$ on a :*

$$E[(X-iY)^{\alpha}(X+iY)^{\beta}] = 0.$$

En appliquant le lemme on obtient que, pour $i\ne j$ et $\alpha,\beta\in\mathbb{N}, \quad \alpha\ne\beta$, $E[a(i,j;s,n)^{\alpha}a(i,j;s,n)^{\beta}] = 0$. De plus on rappelle que les $(a(i,j;s;n))_{1\le i\le j\le n, s\in\mathbb{N}}$ sont indépendantes et que les moments d'ordre impaire de $a(i,i;s,n)$ sont nulles. De ces remarques on déduit que pour que $E[\prod_{k=1}^{m} a(i_k,i_{k+1};s_k,n)]$ soit non-nul il faut pouvoir grouper les termes du produit par paires de la forme $(a(i,j;s,n),a(j,i;s,n))$ (en particulier m doit être paire). Une telle expression est alors de la forme

$$E[|a(i_1,j_1;s_1,n)|^2\ldots|a(i_{m/2},j_{m/2};s_{m/2},n)|^2] \le c''n^{-m/2},$$

ou c'' est une constante qui ne dépend que de m (on peut prendre pour c'' le m-ième moment de $N(0,1)$).

On a donc vu que tout terme non nul de la somme est forcement plus petit que $c''n^{-m/2}$. On a aussi vu que si, pour $I = (i_1, \dots, i_m)$, $E[\prod_{k=1}^m a(i_k, i_{k+1}; s_k, n)]$ est non-nul, il existe une bijection involutive sans point fixe $\gamma : \{1, \dots, m\} \to \{1, \dots, m\}$ avec, pour tout k, $i_k = i_{\gamma(k)+1}, \quad i_{k+1} = i_{\gamma(k)}$ et $s_k = s_{\gamma(k)}$. Notons Ξ_n l'ensemble des m-uplets pour lesquels on peut trouver une telle bijection et, pour un γ_0 fixé, notons $\Xi_n(\gamma_0) \subset \Xi_n$ l'ensemble des m-uplets pour lesquels γ_0 convient. Notons aussi c' le nombre d'involutions sans point fixe de $\{1, \dots, m\}$, qui ne dépend que de m.

Fixons un γ et considérons la relation d'équivalence sur $\{1, \dots, m\}$ générée par $k \sim \gamma(k) + 1$ et $k + 1 \sim \gamma(k)$. Considérons le graphe formé des sommets $\{1, \dots, m\}$ et des m arrêtes $(k, k+1)_{1 \leq k \leq m}$; quotientons le par la relation d'équivalence $\sim$. On obtient ainsi un graphe qui a pour sommets les classes d'équivalence de $\sim$ et qui est connexe car le graphe initial l'était aussi. Mais quand on a quotienté on a confondu, pour chaque k les arrêtes $(k, k+1)$ et $(\gamma(k), \gamma(k)+1)$, qui sont distinctes car γ n'a pas de point fixe. Le graphe quotient a donc au plus $m/2$ arrêtes et, comme il est connexe, au plus $m/2+1$ sommets. Mais, si $(i_1, \dots, i_m) \in \Xi_n(\gamma)$, alors $i_k = i_l$ si $k \sim l$, d'ou, comme on vient de montrer que γ a au plus $m/2+1$ classes d'équivalence, $|\Xi_n(\gamma)| \leq n^{m/2+1}$. Donc $|\Xi_n| \leq c'n^{m/2+1}$ et :

$$\chi_n \leq \frac{cc''}{n} |\Xi_n| n^{-m/2} \leq cc'c'' \qquad \forall n \in \mathbb{N}$$

On vient de montrer le résultat désiré. En plus on remarque que la majoration ne dépend que de m et de $t_1, \dots, t_m$, pas de $s_1, \dots, s_m$, ce qui va être utile dans la suite.

Deuxième étape I

On va supposer ici que pour tout choix de $s_1, \dots, s_m \in \mathbb{N}$ et de $t_1 \dots, t_m \in \mathbb{N}$, $\phi_n(Y(s_1, n)D(t_1, n) \dots Y(s_m, n)D(t_m, n))$ converge quand $n \to \infty$. Comme on a supposer que les $D(t, n)$ sont "stables" par multiplication, on peut définir une fonction d'état μ sur $C = \mathbb{C} < \{X_s | s \in \mathbb{N}\} \cup \{D_t | t \in \mathbb{N}\} >$ par

$$\mu(X_{s_1} D_{t_1} \dots X_{s_m} D_{t_m}) = \lim_{n \to \infty} \phi_n(Y(s_1, n)D(t_1, n) \dots Y(s_m, n)D(t_m, n)).$$

Dans la suite on va calculer μ.

Montrons que les $(X_s)_{s \in \mathbb{N}}$ et la sous-algèbre Δ engendrée par 1 et $\{D_t | t \in \mathbb{N}\}$, respectent la condition **P1** du théorème précèdent.

La propriété 1 est une conséquence de ce qu'on vient de montrer car la majoration dans la première étape ne dépend pas de $(s_1, \dots, s_m)$. 2 a) découle directement de l'indépendance des $Y(s, n)$. Pour 2 b) on commence par un calcul. Soit $n, s, t \in \mathbb{N}$ alors

$$E[Y(s,n)D(t,n)Y(s,n)] =$$
$$\sum_{1 \leq i,j \leq n} \Big(\sum_{1 \leq k \leq n} E[a(i,k;s,n)d(k;t,n)a(k,j;s,n)] \Big) e(i,j;n) =$$
$$\sum_{1 \leq i,j \leq n} \Big(\sum_{1 \leq k \leq n} d(k;t,n)E[a(i,k;s,n)a(k,j;s,n)] \Big) e(i,j;n)$$

Mais on a vu que $E[a(i,k;s,n)a(k,j;s,n)] = 0$ si $i \neq j$ et $\frac{1}{n}$ si $i = j$. On déduit que

$$E[Y(s,n)D(t,n)Y(s,n)] = \sum_{1 \leq i \leq n} \Big(\sum_{1 \leq k \leq n} \frac{d(k;t,n)}{n} \Big) e(i,i;n) = \frac{trD(t,n)}{n} I_n$$

Supposons qu'on se trouve maintenant sous les conditions du 2 b), en particulier on suppose que $\alpha(1) = \alpha(2) \neq \alpha(j), \quad \forall j \geq 3$. Alors, en utilisant l'indépendance on a :

$$\phi_n(Y(s_1,n)D(t_1,n)\ldots Y(s_m,n)D(t_m,n)) =$$

$$\frac{1}{n} tr(E[Y(s_1,n)D(t_1,n)\ldots Y(s_m,n)D(t_m,n)]) =$$

$$\frac{1}{n} tr(E[Y(s_1,n)D(t_1,n)Y(s_1,n)]E[D(t_2,n)Y(s_3,n)\ldots Y(s_m,n)D(t_m,n)]) =$$

$$\frac{1}{n} tr\Big(\frac{trD(t,n)}{n} E[D(t_2,n)Y(s_3,n)\ldots Y(s_m,n)D(t_m,n)]\Big) =$$

$$\phi_n(D(t_1,n))\phi_n(D(t_2,n)Y(s_3,n)\ldots Y(s_m,n)D(t_m,n))$$

Ce qui nous donne le 2 b). Montrons le 2 c). En utilisant encore que les $D(t,n)$ sont stables par multiplication on doit juste montrer que

$$\lim_{n \to \infty} \phi_n(Y(s_1,n)D(t_1,n)\ldots Y(s_m,n)D(t_m,n)) = 0$$

pour tout n-uplets $(t_1,\ldots,t_n)$ et $(s_1,\ldots,s_n)$ qui vérifient :$\forall 1 \leq k \leq n$, $s_k \neq s_{k+1}$ et $\exists ! l \in \{1,\ldots,n\} \setminus \{k\}$ tel que $s_k = s_l$. Fixons une paire de tels n-uplets et notons γ la involution de $\{1,\ldots,n\}$ qui a k associe le seul $l \neq k$ tel que $s_k = s_l$. Par le calcul de l'étape précédente on a :

$$|\phi_n(Y(s_1,n)D(t_1,n)\ldots Y(s_m,n)D(t_m,n))| \leq cn^{-m/2-1}|\Xi_n(\gamma)|$$

On rappelle que l'ensemble $\Xi_n(\gamma)$ a au plus $n^{d(\gamma)}$ éléments, ou $d(\gamma)$ est le nombre d'orbites de γ. Mais, d'après l'hypothèse faite sur $(s_1,\ldots,s_n)$, chaque orbite de γ a au moins deux éléments, d'ou $d(\gamma) \leq m/2$ et

$$|\phi_n(Y(s_1,n)D(t_1,n)\ldots Y(s_m,n)D(t_m,n))| \leq cn^{-1} \longrightarrow 0$$

On a donc montré aussi 2 c).

Deuxième étape II

On continue a supposer la convergence de ϕ_n sur les monômes. On considère $\beta : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ une injection. On sais que la loi de la somme de n gaussiennes indépendantes de variance σ est une gaussienne de variance $n\sigma$. On en déduit que, pour $k \in \mathbb{N}$, $Y(s,n)$ est de même loi que $k^{-1/2}\sum_{j=1}^{k} Y(\beta(s,j),n)$ et donc que les variables aléatoires non-commutatives $((Y(s,n))_{s\in\mathbb{N}} \cup (D(t,n))_{t\in\mathbb{N}})$ on la même distribution jointe que $((k^{-1/2}\sum_{j=1}^{k} Y(\beta(s,j),n))_{s\in\mathbb{N}} \cup (D(t,n))_{t\in\mathbb{N}})$. Il s'en suit que les $((X_s)_{s\in\mathbb{N}} \cup (D_t)_{t\in\mathbb{N}})$ et $((k^{-1/2}\sum_{j=1}^{k} X_{\beta(s,j)})_{s\in\mathbb{N}} \cup (D_t)_{t\in\mathbb{N}})$ on aussi la même distribution jointe. Mais en appliquant le théorème précèdent on obtient que $\{(\{k^{-1/2}\sum_{j=1}^{k} X_{\beta(s,j)}\})_{s\in\mathbb{N}}\cup\{D_t|t\in\mathbb{N}\}\}$ est une famille asymptotiquement libre quand $k\to\infty$ et que les distributions limite des $k^{-1/2}\sum_{j=1}^{k} X_{\beta(s,j)}$ sont donnes par des lois semi-circulaires de premier moment 0 et deuxième moment 1. On déduit que la famille de sous-ensembles $(\{(X_s)_{s\in\mathbb{N}}\}\cup\{D_t|t\in\mathbb{N}\})$ est libre et que les moments des X_s sont donnes par les moments de la loi semi-circulaire. On vient donc de calculer μ.

Troisième étape

Soit $(u_n)_{n\in\mathbb{N}}$ une suite strictement croissante de nombres naturels. On a vu dans la première étape que pour tous $s_1,\ldots,s_m\in\mathbb{N}$ et $t_1\ldots,t_m\in\mathbb{N}$, $(\phi_{u_n}(Y(s_1,u_n)D(t_1,u_n)\ldots Y(s_m,u_n)D(t_m,u_n)))_{n\in\mathbb{N}}$ est une suite bornée de $\mathbb{C}$. Comme il y a un nombre dénombrable de choix des (s_i) et des (t_i), quitte a faire une extraction diagonale, on peut trouver une sous-suite $(v_n)_{n\in\mathbb{N}}$ de $(u_n)_{n\in\mathbb{N}}$ telle que, pour tout choix des (s_i) et des (t_i), $\phi_{v_n}(Y(s_1,v_n)D(t_1,v_n)\ldots Y(s_m,v_n)D(t_m,v_n))$ converge quand $n\to\infty$. Mais dans ce cas, par la deuxième partie, les limites des $\phi_{v_n}(Y(s_1,v_n)D(t_1,v_n)\ldots Y(s_m,v_n)D(t_m,v_n))$ ne dépendent pas de la suite $(v_n)_{n\in\mathbb{N}}$. Ca implique que $(\phi_n(Y(s_1,n)D(t_1,n)\ldots Y(s_m,n)D(t_m,n)))_{n\in\mathbb{N}}$ converge toujours, ce qui nous donne la conclusion du théorème en appliquant encore un fois la deuxième partie. $\square$

Références

[1] D. Voiculescu : *Limit Laws for Random Matrices and Free Product*, Invent. Math. 104 (1991), 201-220

[2] P. Biane : *Free Probability for Probabilists*, Quantum probability communications, Vol. XI (Grenoble, 1998), 55-71, QP-PQ, XI, World Sci. Publishing, River Edge, NJ, 2003.

[3] F. Benaych-Georges : *Memoire DEA*, disponible sur la page web de l'auteur, 23-30

[4] W. Rudin : *Real and Complex Analysis*, McGraw-Hill International Editions, (1987)