Jacobienne de graphes aléatoires

par

Ludovic Stephan
& Erkan Narmanli

Introduction : Le but de cet exposé est d'étudier la limite, lorsque n tend vers l'infini, de la probabilité qu'un p-groupe donné G_p soit le p-sous-groupe de Sylow de la *Jacobienne* (ou du groupe *tas de sable*) d'un graphe à n sommets choisit aléatoirement selon la distribution de Erdős-Rényi. On s'intéressera notamment à la répartition de tels groupes munis d'un accouplement de dualité tel que présenté dans l'article *A Cohen-Lenstra heuristic for Jacobian of random graphs* [**?**]. On parlera aussi rapidement le résultat de Mélanie Matchett Wood dans son article *The distribution of sandpile groups of random graphs* [**?**].

Il s'agit donc d'étudier les Jacobiennes des graphes tirés selon la distribution d'Erdős-Rényi. Soient n un entier non nul et q un réel strictement compris entre 0 et 1 ; un graphe G est tiré selon la distribution d'Erdős-Rényi lorsque toute paire de sommets de G forme une arête avec probabilité q, indépendamment des autres arrêtes dans le graphe ; on notera alors $G \in G(n,q)$ pour dire que G a été tiré selon cette distribution. n, q $G(n,q)$

Si G est un graphe fini connexe, on notera L_G le laplacien de G. Dès lors, si on note $\mathrm{Div}^0(G)$ l'ensemble des diviseurs de G de degré nulle, on a clairement l'inclusion $\mathrm{Princ}(G) \subset \mathrm{Div}^0(G)$. On définit alors la *Jacobienne* de G comme étant le groupe $\mathrm{Jac}(G)$ donné par : L_G $\mathrm{Div}^0(G)$

$$\mathrm{Jac}(G) = \mathrm{Div}^0(G)/_{\mathrm{Princ}(G)}. \qquad \mathrm{Jac}(G)$$

où, $\mathrm{Princ}(G)$ désigne l'ensemble des diviseurs des fonction méromorphes sur G. On notera $\mathcal{M}(G)$ l'ensemble des fonctions méromorphes sur G. $\mathrm{Princ}(G)$ $\mathcal{M}(G)$

Si G n'est pas connexe, on définira la jacobienne de G comme étant la somme directe des jacobiennes de ses composantes connexes.

Exposé de deuxième année rédigé à l'École normale supérieure sous la direction de Omid Amini le 28 février 2018

A Accouplements de dualité

Soient D_1 un diviseur de G de degré nul. Puisque $\mathrm{Jac}(G)$ est un groupe d'ordre fini, alors il existe m_1 un entier positif non nul tel que la classe $\overline{D_1}$ de D_1 dans $\mathrm{Jac}(G)$ vérifie $m_1\overline{D_1} = \overline{0}$; c'est à dire $m_1 D_1 \in \mathrm{Princ}(G)$. Ainsi on prend m_1, m_2 des entiers tels que :

$$m_1 D_1 = \mathrm{div}(f_1)$$
$$m_2 D_2 = \mathrm{div}(f_2),$$

où f_1, f_2 sont deux applications méromorphes sur G. Avec ces notations, on définit ensuite l'application $\langle \cdot \mid \cdot \rangle : \mathrm{Div}^0(G) \times \mathrm{Div}^0(G) \to \mathbb{Q}$ et donnée par :

$\langle \cdot \mid \cdot \rangle$

$$\langle D_1 \mid D_2 \rangle = \frac{1}{m_2} \sum_{v \in V} D_1(v) f_2(v).$$

Remarque. L'application $\langle \cdot \mid \cdot \rangle$ est symétrique et bilinéaire. Le caractère bilinéaire est clair, pour démontrer le caractère symétrique il suffit de remplacer $D_1(v)$ par $\mathrm{ord}_v(f_1)/m_1$ dans la définition plus haut, puis de mettre ensemble les deux contributions des u, v voisins, ce qui nous donne une expression clairement symétrique en f_1, f_2 :

$$\langle D_1 \mid D_2 \rangle = \frac{1}{m_1 \cdot m_2} \sum_{u \sim v} \Big(f_2(v)\,(f_1(u) - f_1(v)) + f_3(u)\,(f_1(v) - f_1(u)) \Big).$$

Remarque. On remarque par ailleurs que si D_1 (ou D_2) est dans $\mathrm{Princ}(G)$, alors m_1 (ou m_2) vaut 1 et donc $\langle D_1 \mid D_2 \rangle$ est dans $\mathbb{Z}$. On peut donc passer au quotient, ce qui nous permet de définir :

δ_G

$$\delta_G : \mathrm{Jac}(G) \times \mathrm{Jac}(G) \to \mathbb{Q}/\mathbb{Z},$$

comme quotient de $\langle \cdot \mid \cdot \rangle$. On appelle δ_G l'*accouplement canonique* associé à G.

app. parfaite

Définition A.1. Une application $\delta : \Gamma \times \Gamma \to \mathbb{Q}/\mathbb{Z}$ est dite *parfaite* lorsque pour tout x dans Γ on a : pour tout y dans $\Gamma, \delta(x, y) = 0$ si et seulement si $x = 0$.

accouplement

On dit que δ est un *accouplement* lorsque δ est symétrique, bilinéaire, et parfaite.

Proposition A.2. *L'application δ_G est un accouplement.*

Démonstration. Il s'agit de montrer que δ_G est une application parfaite, c'est à dire que pour x dans Γ on a $\delta_G(x, \cdot) = 0$ si et seulement si x est nul.

Pour le sens direct : si pour tout diviseur D_2 on a que $\langle D_1 \mid D_2 \rangle$ est un entier, alors en particulier en prenant les diviseurs $D_2 = (v_k) - (v_1)$ pour $2 \leqslant k \leqslant n$ on a pour tout entier k entre 2 et n que $(f_1(v_k) - f_1(v_1))/m_1$ est un entier, que l'on notera $f(k)$. Cela revient à dire que l'on peut écrire :

$$\frac{f_1}{m_1} = \frac{f_1(v_1)}{m_1} + f \quad , f \in \mathcal{M}(G).$$

Dès lors on peut passer au diviseurs dans l'expression ci-dessus, sachant que $\mathrm{div}(f + c) = \mathrm{div}(f)$ pour toute constante c, cela nous donne que $D_1 = \frac{1}{m_1}\mathrm{div}(f_1) = \mathrm{div}(f)$ est principal, ce qui est bien ce que nous souhaitions montrer.

La réciproque est triviale puisque δ_G est bilinéaire. ◆

Aussi, plutôt que de travailler simplement avec $\mathrm{Jac}(G)$, on préfère travailler avec le couple $(\mathrm{Jac}(G), \delta_G)$ parce que la répartition est pus facile à étudier ainsi. Ceci nous amène donc à poser :

$$A = \{(\Gamma, \delta), \Gamma \text{ abélien fini}, \delta \text{ accouplement}\}. \qquad A$$

Par la suite on dit que deux couples (Γ, δ) et (Γ', δ') sont équivalents lorsque : Γ et Γ' sont isomorphes et qu'il existe un isomorphisme f entre Γ' et Γ qui préserve l'accouplement, à savoir que pour tout x, y dans Γ', on a $\delta(f(x), f(y)) = \delta'(x, y)$. Dans le cas où $\delta = \delta'$, on notera $\mathrm{Aut}(\Gamma, \delta)$ l'ensembles des tels f. $\mathrm{Aut}(\Gamma, \delta)$

On note $\sim$ cette relation d'équivalence. On pose alors $\mathscr{A} = A/_\sim$ l'ensemble quotient induit par $\sim$. On pose également $\mathscr{A}(m)$ l'ensemble des éléments (Γ, δ) de $\mathscr{A}$ tels que Γ soit de cardinal m. $\sim, \mathscr{A}$ $\mathscr{A}(m)$

B Quelques lois de probabilité

On fixe dans le reste de cet exposé q un réel strictement compris entre 0 et 1. On notera $\tilde{\mu}_n$ la loi des graphes d'Erdős-Rényi sur l'ensemble des graphes à n sommets. On a donc $\tilde{\mu}_n$

$$\tilde{\mu}_n(G) = q^{e(G)}(1-q)^{\binom{n}{2}-e(G)},$$

où $e(G)$ désigne le nombre d'arrêtes de G. On pose alors $J : G(n, q) \to \mathscr{A}$ l'application qui à tout graphe G associe le couple $(\mathrm{Jac}(G), \delta_G)$. On pose enfin $\mu_n = \tilde{\mu}_n \circ J^{-1}$ la mesure image de $\tilde{\mu}_n$ par J. μ_n

Heuristique. *On a l'heuristique suivante :* $\mathbf{P}[(\mathrm{Jac}(G), \delta_G) = (\Gamma, \delta)] \propto \dfrac{1}{\#\Gamma \# \mathrm{Aut}(\Gamma, \delta)}$.

Ceci nous amène alors à définir la mesure η_n sur $\mathscr{A}(1) \sqcup ... \sqcup \mathscr{A}(n)$ selon cette heuristique, on pose pour tout (Γ, δ) dans $\mathscr{A}$ tel que $\#\Gamma \leqslant n$:

$$\eta_n(\Gamma, \delta) \propto \frac{1}{\#\Gamma \# \mathrm{Aut}(\Gamma, \delta)}\,. \qquad \eta_n$$

Cela est possible puisque l'on est sur un ensemble fini. Le but est donc maintenant de comparer η_n et μ_n asymptotiquement, au sens suivant. Soient $(\alpha_n)_{n\in\mathbb{N}}, (\beta_n)_{n\in\mathbb{N}}$ une suite de mesures sur un ensemble mesurable $(E, \mathcal{E})$, on dit que les deux suites sont *faiblement équivalentes* lorsque pour toute fonction $F : E \to \mathbb{R}$ bornée et $\mathcal{E}$-mesurable les deux propriétés suivantes sont vérifiées : éq. faible

a. On a : $\int F \,\mathrm{d}\alpha_n$ converge si et seulement si $\int F \,\mathrm{d}\beta_n$ converge ;

b. Si ces intégrales convergent, alors elles ont la même limite.

On a alors la conjecture suivante :

Conjecture. *Les suites μ_n et η_n sont faiblement équivalentes.*

Pour notre part, nous allons restreindre notre étude au cas où Γ est un p-groupe et donc regarder le p-Sylow de la Jacobienne. D'une part cela nous permet d'étudier des objets plus simples, et d'autre part cela nous fournit toujours beaucoup d'information puisque les p-Sylow déterminent uniquement la Jacobienne. Cela nous amène donc à poser :

$\mathscr{A}_p$

$$\mathscr{A}_p = \bigsqcup_{n\in\mathbb{N}} \mathscr{A}(p^n) = \{(\Gamma,\delta), \exists n \in \mathbb{N}, \#\Gamma = p^n\}.$$

Par la suite, si Γ est un groupe abélien fini, on notera Γ_p son p-Sylow. On défini alors

α_p

l'application $\alpha_p : \mathscr{A} \to \mathscr{A}_p$ qui associe à tout couple (Γ,δ) de $\mathscr{A}$ son image $(\Gamma_p, \delta_{|\Gamma_p})$. Cela nous amène alors à présenter une seconde conjecture :

Conjecture. *La suite de mesures $\mu_n \circ \alpha_p^{-1}$ converge faiblement vers une mesure $\check{\eta}$, où $\check{\eta}(\Gamma_p,\delta)$ est proportionnel à $(\#\Gamma_p \# \operatorname{Aut}(\Gamma_p,\delta))^{-1}$.*

Dans son article *The distribution of sandpile groups of random graphs* [**?**], Mélanie Matchett Wood montre un résultat similaire, en oubliant la notion d'accouplement et qui est une conséquence de la conjecture ci-dessus. Elle montre le théorème suivant pour tout p-groupe Γ :

Théorème B.1. *On a* $\mathbf{P}[(\operatorname{Jac}(G))_p \simeq \Gamma_p] \propto \dfrac{\#\{\textit{accouplements } \Gamma_p \times \Gamma_p \to \Gamma_p\}}{\#\Gamma_p \cdot \#\operatorname{Aut}(\Gamma_p)}$.

Pour note part, nous allons nous intéresser à montrer un résultat de cette forme, non pas pour le cas de jacobienne (donc de conoyau de laplacien), mais dans le cas plus général des conoyaux de matrices symétriques. On travaillera sur des matrices à coefficients dans les *nombres p-adiques*. Dans la sections suivantes nous allons voir quelques propriétés de tels objets.

C Matrices symétriques p-adiques

C.1 Du laplacien aux matrices symétriques

Remarquons tout d'abord que l'on a pour un graphe G, $\operatorname{Div}(G) = \mathbb{Z} \oplus \operatorname{Div}^0(G)$. En quotientant par $\operatorname{Im}(L_G) \simeq \operatorname{Princ}(G)$, on obtient :

$$\mathbb{Z}^n/_{\operatorname{Im}(L_G)} = \mathbb{Z} \oplus \operatorname{Jac}(G)$$

Ceci nous amène à la définition suivante :

Définition C.1. Soit R un anneau principal intègre, et $A \in \mathcal{M}_n(R)$ une matrice quelconque. On définit alors le conoyau de A comme :

$\operatorname{Cok}(A)$

$$\operatorname{Cok}(A) = R^n/_{\operatorname{Im}(A)}.$$

Remarque. Étant donné que R est principal, A possède une forme normale de Smith de la forme $A \sim \operatorname{Diag}(a_1,\dots,a_n)$. Si A est de rang n, les a_i sont non nuls donc

$$\operatorname{Cok}(A) = \bigoplus_{i=1}^{n} R/_{a_i R}$$

Afin de poursuivre l'analogie avec le laplacien, il nous faut définir un accouplement canonique associé à une matrice symétrique A quelconque. Pour cela, il nous faut supposer que A est inversible dans $K = \mathrm{Frac}(R)$, c'est à dire que $\det(A) \neq 0$.

Définition C.2. Soit A une matrice de $\mathcal{M}_n(R)$ non singulière (i.e. telle que $\det(A) \neq 0$). On peut alors définir un accouplement de $R \times R$ dans K/R défini par :

$$\forall x, y \in R \quad \langle x, y \rangle_A = {}^t x A^{-1} y \qquad \langle \cdot, \cdot \rangle_A$$

Cet accouplement induit un accouplement parfait $\delta_A : \mathrm{Cok}(A) \times \mathrm{Cok}(A) \mapsto K/R$. δ_A

On dispose maintenant pour toute matrice A d'un couple $(\mathrm{Cok}(A), \delta_A)$; il nous reste maintenant à nous placer dans un anneau tel que $\mathrm{Cok}(A)$ soit un p-groupe.

C.2 Entiers p-adiques

Définition C.3. Soientt $(I, \leqslant)$, un ensemble ordonné, $(E_i)_{i \in I}$ une famille d'anneaux, et pour $i \leqslant j$, un morphisme $f_i^j : E_j \to E_i$ tels que :

— $\forall i \in I, f_i^i = \mathrm{Id}_{E_i}$

— $\forall (i, j, k) \in I, i \leqslant j \leqslant k, f_i^j \circ f_j^k = f_i^k$.

On définit alors la limite projective de $(E_i)_{i \in I}$:

$$\varprojlim E_i = \{(a_i)_{i \in I} \in \prod_{i \in I} E_i \quad | \quad \forall i \leqslant j, \quad f_i^j(a_j) = a_i\} \qquad \varprojlim$$

Cette limite est munie des lois induites par chaque E_i : $(a_i) + (b_i) = (a_i +_i b_i)$.

On choisit maintenant $I = \mathbb{N}$, $E_n = \mathbb{Z}/p^n\mathbb{Z}$ et f_n^m la projection canonique. On note alors $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ la limite projective de cette suite. $\mathbb{Z}_p$

Remarque. On peut identifier $\mathbb{Z}_p$ à un anneau de sommes formelles :

$$\mathbb{Z}_p \simeq \{\sum_{i=0}^{\infty} b_i \, p^i \mid b_i \in [\![0, p-1]\!]\}$$

Cette identification se fait via les applications $a_i = \overline{b_0 + \cdots + b_{i-1} p^{i-1}}$ et $b_i = \frac{a_{i+1} - a_i}{p^i}$.

On peut définir une topologie sur $\mathbb{Z}_p$ en choisissant comme base d'ouverts l'ensemble des $U_a(n) = n + p^a\mathbb{Z}_p$, où $n \in \mathbb{Z}_p$ et $a \in \mathbb{N}$. Cette topologie est métrisable, associée à la distance $d_p(x, y) = \max\{n \in \mathbb{N} \ ; \ p^n | x - y\}$.

Dans ce qui suit, on notera $\mathrm{Sym}_n(R)$ l'ensemble des matrices symétriques à coefficients dans un anneau R. Soit $A \in \mathrm{Sym}_n(\mathbb{Z}_p)$ inversible ; $\mathbb{Z}_p$ est principal donc d'après ce qui précède il existe $a_1, \ldots a_r$ tels que $\mathrm{Cok}(A) \simeq \bigoplus_{i=1}^r \mathbb{Z}_p/a_i\mathbb{Z}_p$. $\mathrm{Sym}_n(R)$

Or on peut écrire $a_i = p^{d_i} u_i$ avec u_i inversible ; de plus on a $\mathbb{Z}_p/p^{d_i}\mathbb{Z}_p \simeq \mathbb{Z}/p^{d_i}\mathbb{Z}$ d'où :

$$\mathrm{Cok}(A) \simeq \bigoplus_{i=1}^{r} \mathbb{Z}/p^{d_i}\mathbb{Z}$$

Ainsi, $\mathrm{Cok}(A)$ est un p-groupe.

Il nous reste à définir une mesure sur $\mathbb{Z}_p$; on utilise la mesure de Haar h_p définie par $h_p(a + p^n\mathbb{Z}_p) = p^{-n}$ pour tout $a \in \mathbb{Z}_p$. Cette mesure est bien une probabilité (car $\mathbb{Z}_p = 0 + p^0\mathbb{Z}_p$) et est invariante par translation : pour tout E mesurable, $a \in \mathbb{Z}_p$, $h_p(a + E) = h_p(E)$.

On définit alors une mesure $H_{n,p}$ sur $\mathrm{Sym}_n(\mathbb{Z}_p)$ en choisissant chacun des $\frac{n(n+1)}{2}$ coefficients indépendamment.

D Distribution du conoyau d'une matrice aléatoire

Le but est maintenant, étant donnée une matrice A tirée selon $H_{n,p}$, de calculer la distribution de son conoyau. En particulier, on prouve le théorème suivant :

Théorème D.1. *Soient Γ un p-groupe fini de rang r, δ un accouplement sur Γ. Alors pour A une matrice symétrique aléatoire, on a :*

$$H_{n,p}\left[(\mathrm{Cok}(A), \delta_A) \simeq (\Gamma, \delta)\right] = \frac{\prod_{j=n-r+1}^{n}(1-p^{-j})\prod_{i=1}^{\lceil (n-r)/2\rceil}(1-p^{1-2i})}{|\Gamma| \cdot |\operatorname{Aut}(\Gamma, \delta)|}$$

Afin de prouver ce théorème, nous allons avoir besoin de plusieurs lemmes :

Lemme D.2. *Soient $A, M \in \mathrm{Sym}_n(\mathbb{Z}_p)$ inversibles. Alors $\langle \cdot, \cdot \rangle_A = \langle \cdot, \cdot \rangle_M$ si et seulement si les conditions suivantes sont vérifiées :*

a. il existe $R \in \mathcal{M}_n(\mathbb{Z}_p)$ telle que $A = M + MRM$

b. $\mathrm{rg}(\bar{A}) = \mathrm{rg}(\bar{M})$ où $\bar{A}$ est la réduction de A modulo p

La démonstration de ce lemme provient de [**?**], lemme 3.2.

Démonstration. D'après la définition de $\langle \cdot, \cdot \rangle_A$ il est clair que les accouplements sont égaux si et seulement si $A^{-1} - M^{-1} \in \mathcal{M}_n(\mathbb{Z}_p)$. Supposons tout d'abord que ce soit le cas, et posons $N = A^{-1} - M^{-1}$. Alors $A^{-1}M = NM + I_n$ est dans $\mathcal{M}_n(\mathbb{Z}_p)$, et de même pour $M^{-1}A$. Ainsi $MA^{-1} \in \mathrm{GL}_n(\mathbb{Z}_p)$ donc $\bar{M}\bar{A}^{-1} \in \mathrm{GL}_n(\mathbb{F}_p)$; on en déduit que $\mathrm{rg}(\bar{A}) = \mathrm{rg}(\bar{M})$.

Enfin, $A = M + ANM = M + M(M^{-1}AN)M$, ce qui conclut.

Réciproquement, supposons les conditions a. et b. vérifiées. Alors $\mathrm{Ker}(\bar{M}) \subseteq \mathrm{Ker}(\bar{A})$ et l'égalité du rang donne $\mathrm{Ker}(\bar{M}) = \mathrm{Ker}(\bar{A})$. Soit $v \in \mathrm{Ker}(\overline{I_n + AM})$, alors $v \in \mathrm{Ker}(\bar{A})$ donc $v \in \mathrm{Ker}(\bar{M})$. Ainsi $v = 0$, d'où on déduit $\det(\overline{I_n + AM}) \neq 0$ et $M^{-1}A = I_n + AM \in \mathrm{GL}_n(\mathbb{Z}_p)$. Or, $A^{-1} - M^{-1} = -(A^{-1}M)R \in \mathcal{M}_n(\mathbb{Z}_p)$, ce qui conclut la démonstration. ◆

Soit $[\,,\,]$ une application bilinéaire de $\mathbb{Z}_p^n \times \mathbb{Z}_p^n$ dans $\mathbb{Q}_p/\mathbb{Z}_p$. On définit alors :

$\mathrm{Cok}([\,,\,])$
$$\mathrm{Cok}([\,,\,]) = \mathbb{Z}_p^n / \{x \in \mathbb{Z}_p^n, \forall y \in \mathbb{Z}_p^n \ [x, y] = 0\}$$

Remarque. On dispose alors d'un accouplement induit $\widehat{[\,,\,]}$ sur $\mathrm{Cok}([\,,\,])$.

Lemme D.3. *Le nombre d'applications bilinéaires* $[\,,\,]$ *telles que* $(\mathrm{Cok}([\,,\,]), \widehat{[\,,\,]}) \simeq (\Gamma, \delta)$ *est :*

$$\frac{|\Gamma|^n \cdot \prod_{j=r-n+1}^{n} (1 - p^{-j})}{|\operatorname{Aut}(\Gamma, \delta)|}$$

Démonstration. Soit f une surjection de $\mathbb{Z}_p^n$ dans Γ. Posons $[x, y]_f = \delta(f(x), f(y))$; alors $\mathrm{Cok}([\,,\,]) = \mathbb{Z}_p^n/\mathrm{Ker}(f)$ est isomorphe à $\mathrm{Im}(f) = \Gamma$, et par définition cet isomorphisme envoie $[\,,\,]_f$ sur δ. Réciproquement, si on a un isomorphisme f entre $\mathrm{Cok}([\,,\,])$ et Γ, alors $\pi \circ f$ est une surjection de $\mathbb{Z}_p^n$ dans Γ (où π est la projection sur $\mathrm{Cok}([\,,\,])$). On a alors de plus $[\,,\,] = [\,,\,]_{\pi\circ f}$; on a donc une équivalence entre $\mathrm{Sur}(\mathbb{Z}_p^n, \Gamma)$ et les applications considérées. Or, $[\,,\,]_f = [\,,\,]_g$ ssi $\hat{f} \circ \hat{g}^{-1} \in \mathrm{Aut}(\Gamma, \delta)$; ainsi le cardinal cherché est $|\mathrm{Sur}(\mathbb{Z}_p^n, \Gamma)|/|Aut(\Gamma, \delta)|$.

Calculons donc $|\mathrm{Sur}(\mathbb{Z}_p^n, \Gamma)|$; par le lemme de Nakayama, une fonction de $\mathbb{Z}_p^n$ dans Γ est surjective ssi elle est surjective modulo p. Une surjection est donc donnée par :

— une surjection de $\mathbb{F}_p^n$ dans $\Gamma/p\Gamma \simeq \mathbb{F}_p^r$

— un relèvement des images d'une base de $\mathbb{F}_p^n$ de $\mathbb{F}_p^r$ dans Γ

Par dualité, le premier cardinal est égal à celui des injections de $\mathbb{F}_p^r$ dans $\mathbb{F}_p^n$, qui vaut $\prod_{i=0}^{r-1} (p^n - p^i)$. Pour relever un élément de $\mathbb{F}_p$ dans $\mathbb{F}_{p^d}$, on a $p^{d-1} = p^d/p$ possibilités ; ainsi on a $|\Gamma|/p^r$ possibilités de relèvement pour un élément. On a donc

$$|\mathrm{Sur}(\mathbb{Z}_p^n, \Gamma)| = \frac{|\Gamma| \cdot \prod_{i=0}^{r-1}(p^n - p^i)}{p^{nr}},$$

et le lemme s'en déduit. ◆

On rappelle enfin le lemme de classification des formes quadratiques sur $\mathbb{Q}_p$, tiré de [**?**] :

Lemme D.4. *Soit p un nombre premier, M la matrice d'une forme symétrique sur $\mathbb{Q}_p$. Alors il existe une matrice $H \in \mathrm{GL}_n(\mathbb{Z}_p)$ telle que :*

— *si p est impair, ${}^tHMH$ est diagonale*

— *si $p = 2$, ${}^tHMH$ est diagonale par blocs, avec des blocs de taille au plus 2×2*

Afin de simplifier la démonstration du théorème, on supposera par la suite que p est impair.

Démonstration du théorème. Soit A une matrice aléatoire tirée selon la mesure de Haar ; on peut supposer A non singulière. On remarque alors que $\mathrm{Cok}(\langle \cdot\,, \cdot \rangle_A) = \mathrm{Cok}(A)$, donc nous allons nous intéresser aux applications bilinéaires étudiées plus haut. On a calculé jusqu'ici le nombre d'applications bilinéaires dont le quotient est isomorphe à (Γ, δ) ; il nous reste donc à déterminer la probabilité que $\langle \cdot\,, \cdot \rangle_A$ soit isomorphe à $[\,,\,]$ fixé, tel que $\mathrm{Cok}([\,,\,])$ est isomorphe à (Γ, δ). Remarquons que la mesure de Haar sur $\mathbb{Z}_p$ étant invariante par translation, $H_{n,p}$ est invariante par changement de base.

Soit N une matrice de $\mathcal{M}_n(\mathbb{Q}_p)$ telle que $N_{i,j}$ soit un relèvement de $[e_i, e_j]$ dans $\mathbb{Q}_p$. La classification des formes quadratiques sur $\mathbb{Q}_p$ nous donne l'existence de $H \in \mathrm{GL}_n(\mathbb{Z}_p)$

telle que ${}^tHNH$ soit diagonale. Par invariance de la mesure de Haar, on peut donc directement supposer que N est diagonale, et poser $M = N^{-1}$.

Quitte à changer le relèvement, on peut supposer que les coefficients de N ont une valuation p-adique négative, donc M a ses coefficients dans $\mathbb{Z}_p$, qu'on note $p^{d_1}u_1, \dots, p^{d_n}u_n$ avec u_i inversible. Dès lors,

$$\Gamma = \bigoplus_{i=1}^{n} \mathbb{Z}_p/p^{d_i}\mathbb{Z}_p$$

d'où on déduit que sans perte de généralité $d_1 = \cdots = d_{n-r} = 0$, les autres valuations étant non nulles.

On a alors $[\,,\,] = \langle\,\cdot\,,\,\cdot\,\rangle_M$; ainsi on cherche la probabilité que $\langle\,\cdot\,,\,\cdot\,\rangle_A = \langle\,\cdot\,,\,\cdot\,\rangle_M$; donc que A et M vérifient les conditions du lemme D.2.
La deuxième condition donne pour $i < j$, $p^{d_i+d_j} | a_{i,j}$ et $p^{2d_i} | a_{i,i} - p^{d_i}u_i$. Cela revient dans tous les cas à fixer les $(d_i + d_j)$ premiers chiffres de $a_{i,j}$; la probabilité que A vérifie ces conditions est donc :

$$\prod_{1 \leqslant i \leqslant j \leqslant n} p^{-(d_i+d_j)} = \prod_{i=1}^{n} p^{-(n+1)d_i} = \frac{1}{|\Gamma|^{n+1}}$$

On remarque que selon ces conditions, $\bar{A}$ est nulle en dehors du mineur en haut à gauche de taille $n - r$, qui est indépendant des coefficients déterminés précédemment. Or $\mathrm{rg}(\bar{M}) = n - r$ donc ce mineur doit être inversible ; il est distribué uniformément dans $\mathrm{Sym}_{n-r}(\mathbb{F}_p)$ donc la probabilité qu'il soit inversible est

$$\frac{|\,\mathrm{GL}_{n-r}(\mathbb{F}_p) \cap \mathrm{Sym}_{n-r}(\mathbb{F}_p)|}{|\,\mathrm{Sym}_{n-r}(\mathbb{F}_p)|} = \prod_{i=1}^{\lceil (n-r)/2 \rceil} (1 - p^{1-2i})$$

La dernière égalité provient de [**?**], théorème 2.

Ainsi, étant donné que la probabilité ne dépend pas de M, on a finalement en multipliant :

$$H_{n,p}\left[(\mathrm{Cok}(A), \delta_A) \simeq (\Gamma, \delta)\right] = \frac{\prod_{j=n-r+1}^{n} (1 - p^{-j}) \prod_{i=1}^{\lceil (n-r)/2 \rceil} (1 - p^{1-2i})}{|\Gamma| \cdot |\,\mathrm{Aut}(\Gamma, \delta)|}$$

◆

Conclusion

On a donc finalement prouvé un résultat concernant les matrices symétriques dans $\mathbb{Z}_p$, ce qui est éloigné de notre but initial. Cependant, ce résultat a tout de même des conséquences intéressantes.

Tout d'abord, la constante de normalisation (le numérateur du théorème) tend vers $c_p = \prod_i (1 - p^{-i})$ quand n tend vers $+\infty$, ce qui nous donne par le théorème de convergence dominée l'existence d'une mesure $\check{\eta}$ sur $\mathcal{A}_p$ telle que :

$$\check{\eta}[(\Gamma, \delta)] \propto \frac{1}{|\Gamma| \cdot |\operatorname{Aut}(\Gamma, \delta)|}$$

C'est un bon début dans la recherche de la distribution des p-Sylows de la jacobienne ; et en effet, ce qui reste à démontrer (et ce que M. Wood démontre dans [**?**], sans considérer l'accouplement canonique) est que la distribution du laplacien d'un graphe aléatoire dans $\mathbb{Z}_p$ est similaire à la mesure de Haar sur les matrices symétriques.

Cet article est donc le point central pour démontrer la convergence faible de $\mu_n \circ \alpha_p^{-1}$ vers $\check{\eta}_p$, démontrée uniquement pour l'instant pour les fonctions ne dépendant pas de l'accouplement δ.