Anaël Marit ENS Rennes

PROBABILITÉS SUR $GL_2(\mathbb{F}_q)$

- 101, 103, 104, 106, 190 -

—

L'utilisation des probabilités uniformes permet de rendre compte de la proportion de couples commutant dans $GL(E)^2$, et donc d'avoir une idée quantitative d'à quel point ce groupe «n'est pas abélien». Ce genre de résultat est décrit plus généralement par un théorème dû à Dixon, qui affirme qu'en remplaçant $GL(E)$ par un groupe fini non-abélien quelconque, on peut toujours majorer cette probabilité par $5/8$.

Tout le développement est extrait de [1], exercice 108, section XI-5, où seul le cas $q = 5$ est traité, mais c'est exactement pareil pour n'importe quel corps fini.

Dans toute la suite, on fixe q une puissance non-nulle d'un nombre premier et on note $\mathbb{F}_q$ le corps fini à q éléments. Posons $E := \mathbb{F}_q^2$.

Comme $GL(E)$ est un ensemble fini, on peut naturellement considérer des variables aléatoires suivant une loi uniforme sur $GL(E)$. Nous allons démontrer :

Théorème 1. *Soient X et Y deux variables aléatoires indépendantes de loi $\mathcal{U}(GL(E))$. Alors :*

$$\mathbb{P}(XY = YX) = \frac{1}{q^2 - q} \tag{1}$$

Un lemme de théorie des groupes

Notre démonstration va être dirigée par le lemme général suivant :

Lemme 1. *Remplaçons $GL(E)$ par un groupe fini quelconque. On fait agir G sur lui-même par conjugaison et on note k le nombre d'orbites obtenues. Alors :*

$$\mathbb{P}(XY = YX) = \frac{k}{|G|} \tag{2}$$

Pour tout $g \in G$, on note $\mathrm{Fix}(g) := \{x \in G \mid gxg^{-1} = x\}$ le fixateur de g sous l'action par conjugaison. On peut alors remarquer l'égalité des évènements :

$$(XY = YX) = (XYX^{-1} = Y) = (Y \in \mathrm{Fix}(X)) \tag{3}$$

Contactez-moi en cas de coquille à prénom.nom@ens-rennes.fr !

d'où par probabilités uniformes :

$$\mathbb{P}(XY = YX) = \mathbb{P}(Y \in \mathrm{Fix}(X)) \tag{4}$$
$$= \frac{|Y \in \mathrm{Fix}(X)|}{|G|^2} \tag{5}$$
$$= \frac{\left|\bigsqcup_{x\in X}\{x\} \times \mathrm{Fix}(x)\right|}{|G|^2} \tag{6}$$
$$= \frac{1}{|G|^2}\sum_{x\in G} |\mathrm{Fix}(x)| \tag{7}$$

Il suffit donc d'appliquer la formule de Burnside pour obtenir le résultat souhaité.

Dénombrement des orbites

Grâce au lemme 1, il suffit pour calculer notre probabilité de calculer le nombre d'orbites de $GL(E)$ sous l'action de conjugaison. Pour cela, commençons par faire une observation.

On note :

$$\mathscr{D} = \{u \in GL(E) \mid u \text{ est diagonalisable}\}, \tag{8}$$
$$\mathscr{T} := \{u \in GL(E) \mid u \text{ est trigonalisable mais pas diagonalisable}\}, \tag{9}$$
$$\mathscr{N} := \{u \in GL(E) \mid u \text{ n'est pas trigonalisable}\}. \tag{10}$$

Alors, il est clair qu'on a une partition :

$$GL(E) = \mathscr{D} \sqcup \mathscr{T} \sqcup \mathscr{N} \tag{11}$$

et par ailleurs cette partition est stabilisée par l'action de conjugaison. On va donc compter séparément les orbites contenues dans $\mathscr{D}, \mathscr{T}$ et $\mathscr{N}$ respectivement.

Dans toute la suite, on se donne $u \in GL(E)$.

Etude des orbites de $\mathscr{D}$

On remarque :

$$u \in \mathscr{D} \iff \exists(\lambda,\mu) \in (\mathbb{F}_q^\times)^{2\,(\mathrm{i})},\ \exists \mathscr{B} \text{ une base de } E \ :\ Mat_{\mathscr{B}}(u) = \begin{pmatrix}\lambda & 0\\ 0 & \mu\end{pmatrix} \tag{12}$$

Par ailleurs, un tel (λ, μ) est nécessairement décrit, à permuation près, par le spectre de u. Aussi, l'orbite de u est entièrement caractérisée par la classe de (λ, μ) modulo l'action naturelle de $\mathfrak{S}_2$. En d'autres termes, on a une bijection :

$$(\mathbb{F}_q^\times)^2/\mathfrak{S}_2 \to GL(E)\cdot\mathscr{D}$$
$$(\lambda,\mu) \mapsto GL(E)\cdot\begin{pmatrix}\lambda & 0\\ 0 & \mu\end{pmatrix}$$

(i). On prend les valeurs propres dans $\mathbb{F}_q^\times$ car notre endomorphisme est inversible.

et donc le nombre d'orbites dans $\mathscr{D}$ est égal à :

$$|GL(E)\cdot\mathscr{D}| = \left|{(\mathbb{F}_q^\times)^2}/{\mathfrak{S}_2}\right| \tag{13}$$
$$= |\mathbb{F}_q^\times| + |\mathcal{P}_2(F_q^\times)| \tag{14}$$
$$= q-1+\binom{q-1}{2} \tag{15}$$
$$= \frac{q(q-1)}{2} \tag{16}$$

où $\mathcal{P}_2(\mathbb{F}_q^\times)$ désigne l'ensemble des parties à deux éléments de $\mathbb{F}_q^\times$.

Etude des orbites de $\mathscr{T}$

Supposons maintenant $u \in \mathscr{T}$. Comme par hypothèse u est trigonalisable, son spectre est non-vide, mais celui-ci est nécessairement réduit à un élément. En effet, dans le cas contraire, son polynôme caractéristique serait scindé à racines simples et donc u serait diagonalisable. Notons donc $\lambda \in \mathbb{F}_q^\times$ l'unique valeur propre de u. Par trigonalisation, il existe une base $\mathscr{B}$ de E telle que :

$$Mat_{\mathscr{B}} = \begin{pmatrix}\lambda & 1\\ 0 & \lambda\end{pmatrix} \text{ (ii)} \tag{17}$$

Posons donc l'application :

$$\begin{aligned}\mathbb{F}_q^\times &\to GL(E)\cdot\mathscr{T}\\ \lambda &\mapsto GL(E)\cdot\begin{pmatrix}\lambda & 1\\ 0 & \lambda\end{pmatrix}\end{aligned}$$

Cette application est surjective d'après le raisonnement précédemment mené. Par ailleurs, elle est nécessairement injective, puisque chaque antécédant d'une orbite est dans le spectre de tout endomorphisme de l'orbite, lequel est réduit à un élément. Donc :

$$|GL(E)\cdot\mathscr{T}| = |\mathbb{F}_q^\times| \tag{18}$$
$$= q-1 \tag{19}$$

Etude des orbites de $\mathscr{N}$

On suppose enfin que $u \in \mathscr{N}$. Puisque u n'est pas trigonalisable, son polynôme caractéristique n'est pas scindé, et donc, celui-ci étant de degré 2, il n'a pas de racines dans $\mathbb{F}_q$. Montrons que dans ce cas, le polynôme caractéristique caractérise entièrement les orbites. Il est clair d'une part que c'est un invariant sous l'action par conjugaison. Réciproquement, on note $\chi_u = X^2+aX+b$. Soit $e_1 \in E\setminus\{0\}$ et $e_2 := u(e_1)$. Comme u n'a pas de valeur propre, $\mathscr{B} := (e_1, e_2)$ est libre. De plus, par le théorème de Cayley-Hamilton :

$$u(e_2) = u^2(e_1) = -au(e_1) - be_1 = -be_1 - ae_2 \tag{20}$$

donc :

$$Mat_{\mathscr{B}}(u) = \begin{pmatrix}0 & -b\\ 1 & -a\end{pmatrix} \tag{21}$$

(ii). Il suffit de prendre une base trigonalisante et de renormaliser le premier vecteur pour imposer le 1 en haut à droite.

Cette forme matricielle ne dépend que du polynôme caractéristique de u : elle détermine complètement l'orbite de u ! Ainsi :

$$|GL(E)\cdot\mathscr{N}| = |\{P\in\mathbb{F}_q[X] \mid \deg(P)=2, \text{ P est unitaire et sans racine dans } \mathbb{F}_q\}| \tag{22}$$

$$= |\{X^2+aX+b,\ (a,b)\in\mathbb{F}_q^2\}\setminus\{(X-\lambda)(X-\mu),\ (\lambda,\mu)\in {(\mathbb{F}_q)^2}/{\mathfrak{S}_2}\}| \tag{23}$$

$$= q^2 - \frac{q(q+1)}{2} \tag{24}$$

$$= \frac{q^2-q}{2} \tag{25}$$

Calcul de la probabilité

Ainsi, en combinant tous nos résultats, le nombre d'orbites de $GL(E)$ sous son action par conjugaison est donné par :

$$|GL(E)\cdot\mathscr{D}| + |GL(E)\cdot\mathscr{T}| + |GL(E)\cdot\mathscr{N}| = \frac{q(q-1)}{2} + q - 1 + \frac{q(q+1)}{2} = q^2-1 \tag{26}$$

Enfin, une application directe du lemme 1 donne le résultat :

$$\mathbb{P}(XY=YX) = \frac{q^2-1}{|GL_2(\mathbb{F}_q)|} = \frac{q^2-1}{(q^2-q)(q^2-1)} = \frac{1}{q^2-q} \tag{27}$$

Remarque : Pour mettre en lien avec le résultat du théorème de Dixon, notons que la fonction $x\mapsto x^2-x$ est croissante pour $x\geqslant 1/2$. Ainsi, la probabilité que deux éléments commutent dans $GL_2(\mathbb{F}_q)$ est maximale pour $q=2$ et vaut dans ce cas $1/2$, donc le groupe linéaire d'ordre 2 sur un corps fini n'atteint jamais l'optimum (notons que la valeur $5/8$ peut être atteinte, c'est le cas par exemple dans D_4 ou Q_8). Par ailleurs, $\mathbb{P}(XY=YX)$ tend vers 0 lorsque q tend vers $+\infty$.

Une question naturelle à se poser et de savoir si la preuve se généralise à $GL_n(\mathbb{F}_q)$. La réponse est non, car la description des matrices non-trigonalisables devient plus compliquée lorsque la dimension de E augmente. En particulier, le polynôme caractéristique ne caractérise plus l'orbite par conjugaison dès que $n\geqslant 3$ et n'est pas forcément sans racine. On pourrait éventuellement envisager la question du dénombrement en utilisant le théorème de réduction de Fröbénius qui permettrait d'exhiber des invariants totaux, mais le problème deviendrait alors beaucoup plus compliqué et je n'ai pas creusé cette piste, je ne garantis donc pas qu'elle puisse aboutir.

Références

[1] Philippe Caldero. *Carnet de voyage en Analystan*. Calvage & Mounet, 2023. ISBN : 978-2-49-323011-9.