
Probabilité pour que deux éléments commutent

Recasage : 101 / 103 / 104 / 106 / 190

Référence : Carnet de Voyage en Analystan (Exercice 105)

► On considère G un groupe fini et non abélien, on s'intéresse ici à la probabilité de tirer deux éléments qui commutent. Le tirage est indépendant et tiré de façon équiprobable. On va utiliser la formule de Burnside dans le développement pour voir que l'on peut calculer explicitement cette probabilité en fonction des classes de conjugaison. On rappelle alors le théorème de Burnside ainsi que sa preuve.

Théorème 1 (Théorème de Burnside)

Soit G un groupe fini opérant sur un ensemble fini X . On note $\text{Fix}(g) = \{x \in X \mid g \cdot x = x\}$. Alors le nombre d'orbites de X sous l'action de G noté $|X/G|$ vaut :

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|$$

Preuve.

L'idée est de calculer le cardinal de l'ensemble $F = \{(g, x) \in G \times X \mid g \cdot x = x\}$, on peut donc partitionner comme ci dessous :

$$F = \bigcup_{g \in G} \{(g, x) \mid x \in \text{Fix}(g)\} = \bigcup_{x \in X} \{(g, x) \mid g \in \text{Stab}(x)\}$$

On peut alors calculer le cardinal de F suivant les deux décompositions précédente alors $|F| = \sum_{g \in G} |\text{Fix}(g)|$.

Reste à calculer pour l'autre décomposition notons d'abord $\text{Orb}(x_1), \text{Orb}(x_2), \dots, \text{Orb}(x_r)$ l'ensemble des orbites de X sous l'action de G . Alors :

$$\begin{aligned} |F| &= \sum_{x \in X} |\text{Stab}(x)| \\ &= \sum_{x \in X} \frac{|G|}{|\text{Orb}(x)|} \quad (\text{Par la formule des classes}) \\ &= \sum_{i=1}^r |G| \underbrace{\left(\sum_{x \in \text{Orb}(x_i)} \frac{1}{|\text{Orb}(x_i)|} \right)}_{=1} \\ &= r|G| \end{aligned}$$

Et donc $r = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|$.

■

On peut maintenant passer aux développements.

Développement 1

Soit G un groupe fini de cardinal n et $Z(G)$ le centre de G , $Z(G) = \{h \in G \mid \forall g \in G \ gh = hg\}$ et note z son cardinal. On note p la probabilité pour que deux éléments g et h de G choisis indépendamment, et de façon équiprobable, commutent. Alors $p \leq \frac{5}{8}$.

Preuve.

► On commence par montrer que $p \leq \frac{z}{2n} + \frac{1}{2}$. On commence par poser

$$K = \{(h, g) \in G^2 \mid gh = hg\}$$

La probabilité p cherché est alors $p = \frac{|K|}{n^2} = \frac{m}{n^2}$ où m est le cardinal de K , on fixe $g \in G$ et on pose alors $Z_g = \{h \in G \mid hg = gh\}$, on peut donc affirmer que $K = \bigcup_{g \in G} Z_g$ et donc : $m = |K| = \sum_{g \in G} |Z_g|$. On va à présent scinder la somme suivant le fait que $g \in Z(G)$ ou pas.

$$|K| = \sum_{g \in Z(G)} |Z_g| + \sum_{g \notin Z(G)} |Z_g|$$

Si $g \in Z(G)$ alors $Z_g = G$ et donc $|K| = nz + \sum_{g \notin Z(G)} |Z_g|$, si $g \notin Z(G)$ alors c'est un sous groupe strict de G et le théorème de Lagrange affirme que $|Z_g| \leq \frac{n}{2}$ ce qui donne donc $m \leq nz + \frac{n-z}{2}$ et donc en divisant par n^2 on obtient donc $p \leq \frac{z}{2n} + \frac{1}{2}$. Pour conclure on va avoir besoin du lemme suivant.

Lemme 1

Si G est un groupe tel que $G/Z(G)$ soit cyclique alors G est abélien.

Preuve.

Supposons que $G/Z(G)$ soit cyclique, cela veut dire qu'il est engendré par la classe d'un élément, disons $\bar{a}$ avec $a \in G$. Soient g, h deux éléments de G et on veut montrer que $gh = hg$. Par hypothèse on peut écrire $g = a^k z$ et $h = a^{k'} z'$ et donc $gh = a^k z a^{k'} z' = a^{k+k'} z z' = hg$ car $z, z' \in Z(G)$ et donc G est abélien. ■

Or G n'étant pas abélien on conclut que $G/Z(G)$ n'est pas cyclique et donc d'ordre au moins 4 (car si c'était 1, 2, 3 il serait cyclique car de cardinal premier). donc $\frac{n}{z} \geq 4 \iff z \leq \frac{n}{4}$. On peut donc en conclure que $p \leq \frac{1}{8} + \frac{1}{2} = \frac{5}{8}$. ■

On va maintenant calculer la probabilité exacte que deux éléments choisis de façon équiprobable dans un groupe fini commutent entre eux en fonction du nombre de classes de conjugaison de ce groupe.

Développement 2

Soit G un groupe fini de cardinal n non abélien, alors la probabilité pour deux éléments tirés de façon équiprobable et indépendant commutent vaut $p = \frac{k}{n}$ où k est le nombre de classes de conjugaisons du groupe G .

Preuve.

L'idée de la preuve est d'utiliser la formule de Burnside pour une action bien choisie, ici l'action de conjugaison. Pour le bon choix on considère donc l'action naturelle :

$$\Phi: \begin{cases} G \times G \longrightarrow G \\ (g, h) \longmapsto ghg^{-1} \end{cases}$$

Les orbites pour cette action sont exactement les classes de conjugaisons ainsi la formule de Burnside nous donne alors :

$$k = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)| = \frac{1}{n} \sum_{g \in G} |\text{Fix}(g)|$$

Mais alors $\text{Fix}(g) = \{h \in G \mid ghg^{-1} = h\} = \{h \in G \mid gh = hg\} = Z_g$ donc :

$$k = \frac{1}{n} \sum_{g \in G} |Z_g| = \frac{1}{n} pn^2 = np$$

Ce qui donne bien $p = \frac{k}{n}$

■

Remarque.

On peut s'intéresser ici au cas d'égalité, "quelle groupe non abélien est le plus abélien possible?" pour répondre à cette question il suffit de reprendre les conditions imposées dans la première partie du développement, en effet il faut que $Z(G)$ soit d'indice 4 et que Z_g soit d'indice 2. Le groupe diédral D_4 vérifie ces conditions on peut donc voir ce groupe comme le plus abélien possible!

Application 1

La probabilité pour que deux matrices de $GL_2(\mathbb{F}_q)$ commutent est $\frac{1}{q^2 - q}$

Preuve.

► D'après ce qui précède, $|GL_2(\mathbb{F}_q)| = (q^2 - 1)(q^2 - q)$. Il nous faut donc calculer le nombre de classes de conjugaisons pour cela il suffit de compter les classes de similitudes de matrices de $GL_2(\mathbb{F}_q)$. Car deux matrices sont dans la même classe de conjugaison si et seulement si elles sont semblables.

On distingue alors 3 cas :

- Les matrices diagonalisables, On matrice diagonalisable est semblable à une matrice de la forme $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ avec λ_1 et λ_2 non nuls puisque la matrice est inversible. On peut donc dénombrer $|\mathbb{F}_q^*| = q - 1$ donc il y a $q - 1$ possibilités si $\lambda_1 = \lambda_2$ et $\binom{q-1}{2} = \frac{(q-1)!}{2!(q-3)!} = \frac{(q-1)(q-2)}{2}$. Et donc il y a $q - 1 + \frac{(q-1)(q-2)}{2} = \frac{q(q-1)}{2}$ classes de conjugaisons de matrices diagonalisables .
- Soit A une matrice trigonalisable mais non diagonalisable, son polynôme caractéristique est donc scindé (mais pas scindé simple sinon A serait diagonalisable). On a donc nécessairement $\chi_A(X) = (X - \lambda)^2$ avec $\lambda \in \mathbb{F}_q^*$. Par hypothèse A est donc semblable à la matrice $\begin{pmatrix} \lambda & \varepsilon \\ 0 & \lambda \end{pmatrix}$ mais cette matrice est semblable à $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ donc il y a autant de classe de conjugaisons de matrice trigonalisables non diagonalisable que de $\lambda \in \mathbb{F}_q^*$ à savoir $q - 1$ classes de conjugaisons de matrices trigonalisables et non diagonalisables .
- Supposons maintenant que A non diagonalisable et non trigonalisable ainsi le polynôme caractéristique de A est irréductible de degré 2 sur $\mathbb{F}_q[X]$ il y a $\frac{q(q-1)}{2}$ polynômes irréductibles de degré 2 sur $\mathbb{F}_q[X]$. Montrons que chacun de ses polynômes détermine une seule classe de conjugaison. Alors par hypothèse $\chi_A(X) = X^2 + aX + b$ sans racines (irréductibles car de degré 2). Soit $u \in \mathbb{F}_5^*$ non nul alors la famille (u, Au) est une base puisque A n'admet pas de valeurs propre. Ainsi par changement de base il existe P inversible tel que :

$$PAP^{-1} = \begin{pmatrix} 1 & -b \\ 0 & -a \end{pmatrix}$$

Cette matrice ne dépend que du polynôme P ainsi il y donc bien $\frac{q(q-1)}{2}$ classes de conjugaison de matrices non diagonalisables et non trigonalisables.

Finalement il y a en tout $\frac{q(q-1)}{2} + q - 1 + \frac{q(q-1)}{2} = q^2 - 1$ Et donc la probabilité p cherché est $p = \frac{q^2-1}{(q^2-1)(q^2-q)} = \frac{1}{q^2-q}$