

2.10 Cardinal du cône nilpotent sur $\mathbb{F}_q$ (101, 123, 156, 190) [5]

Le but de ce développement est de dénombrer le cardinal de l'ensemble des matrices nilpotentes de taille $d \in \mathbb{N}^*$ fixée sur un corps fini de cardinal q , que l'on notera :

$$\mathcal{N}_d(\mathbb{F}_q).$$

Son cardinal sera noté $n_d(q)$. On observe alors un phénomène étrange :

Théorème 2.25 (Cardinal du cône nilpotent). Soient $\mathbb{F}_q$ un corps de cardinal q et $d \in \mathbb{N}^*$. On a :

$$n_d(q) = q^{d(d-1)}.$$

Remarque 2.10.1 (Pourquoi c'est étrange?). *Plusieurs estimations heuristiques de ce résultat peuvent être données. Par exemple, d'après le théorème de réduction de Jordan pour les endomorphismes nilpotents, tout élément de $\mathcal{N}_d(\mathbb{F}_q)$ est conjugué à une matrice de la forme :*

$$\begin{pmatrix} J_{d_1} & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & J_{d_r} \end{pmatrix}$$

avec $\sum_{i=1}^r d_i = d$ et J_k le bloc de Jordan nilpotent de taille k . Or, si on était dans $\mathbb{R}$ par exemple, on pourrait dire que l'orbite de la matrice J_d par conjugaison serait dense dans $\mathcal{N}_d(\mathbb{R})$. Les matrices nilpotentes de taille d seraient donc « presque toutes » dans l'orbite de J_d . Si on extrapole ce résultat dans $\mathbb{F}_q$, on aurait donc :

$$n_d(q) \approx |\mathcal{O}_{J_d}| = \frac{|GL_d(\mathbb{F}_q)|}{|Z(J_d)|}$$

où $Z(J_d)$ désigne le centralisateur de J_d , c'est-à-dire son commutant. Or, étant donné que J_d est une matrice cyclique, son commutant est un espace vectoriel de dimension exactement égale à d . Ainsi, en approchant le cardinal de $GL_d(\mathbb{F}_q)$ par q^{d^2} , on obtient :

$$n_d(q) \approx q^{d^2-d},$$

ce qui est exactement le résultat souhaité !

Une autre interprétation possible peut se faire en terme de variété. $\mathcal{N}_d(\mathbb{F}_q)$ peut se représenter comme étant le lieu des zéros de d applications polynômiales indépendantes sur $\mathcal{M}_d(\mathbb{F}_q)$: les coefficients du polynôme caractéristique ! En effet, une matrice de taille d est nilpotente si et seulement si son polynôme caractéristique est égal à X^d . Ainsi, si on était dans $\mathbb{R}$ par exemple, on pourrait dire que $\mathcal{N}_d(\mathbb{F}_q)$ serait une sous-variété de $\mathcal{M}_d(\mathbb{F}_q)$ de dimension $d^2 - d$ via la caractérisation par « équation ». Ainsi, en approximant le cardinal de $\mathcal{N}_d(\mathbb{F}_q)$ par celui d'un $\mathbb{F}_q$ -espace vectoriel de dimension $d^2 - d$, on obtient :

$$n_d(q) \approx q^{d^2-d} !$$

Démonstration. Soient $e \in \mathbb{F}_q^d$ un vecteur non-nul et $N \in \mathcal{N}_d(\mathbb{F}_q)$. Ce vecteur engendre un sous-espace cyclique pour N , dont une base est :

$$\mathcal{F}_e = (e, Ne, \dots, N^{r-1}e)$$

et telle que $N^r e = 0$. En effet, si $\pi_{N,e}$ désigne le polynôme minimal de N relativement au vecteur e , on a :

$$\pi_{N,e} \mid \pi_N \mid \chi_N = X^d.$$

Ainsi, il existe k entier naturel non-nul tel que :

$$\pi_{N,e} = X^k.$$

Or, $k \geq r$ car la famille $\mathcal{F}_e$ est libre : aucun élément de cette famille n'est nul. Or, par définition du sous-espace cyclique engendré par e , la famille $(e, Ne, \dots, N^{r-1}e, N^r e)$ est liée, donc il existe P de degré r tel que $P(N)e = 0$. Ainsi, $\pi_{N,e}$ divise P , donc $k \leq r$. Donc $N^r e = \pi_{N,e}(N)e = 0$ par définition. Cela permet de justifier la définition suivante :

Définition 2.26. Soient $N \in \mathcal{N}_d(\mathbb{F}_q)$ et $r \in \llbracket 1, d \rrbracket$. On note $L_{r,d}$ l'ensemble des familles libres de $\mathbb{F}_q^d$ à r éléments. On dit que N *respecte* une famille $\mathcal{F} = (e_1, \dots, e_r) \in L_{r,d}$ si :

$$\forall i \in \llbracket 1, r-1 \rrbracket, \quad Ne_i = e_{i+1}$$

avec $Ne_r = 0$.

Notons alors :

$$\tilde{\mathcal{N}}_d := \left\{ (N, \mathcal{F}) \in \mathcal{N}_d(\mathbb{F}_q) \times \bigsqcup_{r=1}^d L_{r,d} \mid N \text{ respecte } \mathcal{F} \right\}.$$

Un double décompte de $\tilde{\mathcal{N}}_d$ va nous permettre de trouver une relation de récurrence pour $n_d(q)$!

Décompte 1 : On dénombre d'abord selon la première composante, en notant π_1 la projection sur la première composante :

$$\tilde{\mathcal{N}}_d = \bigsqcup_{N \in \mathcal{N}_d(\mathbb{F}_q)} \pi_1^{-1}(\{N\}).$$

On a alors :

$$|\tilde{\mathcal{N}}_d| = \sum_{N \in \mathcal{N}_d(\mathbb{F}_q)} |\pi_1^{-1}(\{N\})|.$$

Un élément de $\pi_1^{-1}(\{N\})$ sera donc totalement déterminé par la donnée d'un vecteur e non-nul étant donné qu'il sera de la forme $(N, \mathcal{F}_e)$. Plus précisément, l'application :

$$\begin{aligned} \pi_1^{-1}(\{N\}) &\longrightarrow \mathbb{F}_q^d \setminus \{0\} \\ (N, (e_1, \dots, e_r)) &\longmapsto e_1 \end{aligned}$$

est une bijection. Ainsi, on a :

$$\forall N \in \mathcal{N}_d(\mathbb{F}_q), \quad |\pi_1^{-1}(\{N\})| = q^d - 1.$$

D'où :

$$|\tilde{\mathcal{N}}_d| = n_d(q) (q^d - 1).$$

Décompte 2 : On dénombre ensuite selon la deuxième composante. On note alors π_2 la projection sur cette composante, de sorte qu'on ait :

$$|\tilde{\mathcal{N}}_d| = \sum_{r=1}^d \sum_{\mathcal{F} \in L_{r,d}} |\pi_2^{-1}(\{\mathcal{F}\})|.$$

Soit alors $\mathcal{F} \in L_{r,d}$ avec r fixé. Par le théorème de la base incomplète, on peut compléter cette famille en une base $\mathcal{B}$ de $\mathbb{F}_q^d$. Ainsi, $N \in \mathcal{N}_d(\mathbb{F}_q)$ respecte $\mathcal{F}$ si et seulement si, la matrice de son endomorphisme associé (que l'on notera encore N) dans la base $\mathcal{B}$ est :

$$\begin{pmatrix} J_r^T & M \\ \mathbf{0} & N_{d-r} \end{pmatrix}$$

où $M \in \mathcal{M}_{r,d-r}(\mathbb{F}_q)$ est une certaine matrice et $N_{d-r} \in \mathcal{N}_{d-r}(\mathbb{F}_q)$. En effet, par définition, N respecte $\mathcal{F}$ si et seulement si $\text{Vect}(\mathcal{F})$ est stable par N et $N|_{\text{Vect}(\mathcal{F})}$ a pour matrice dans la base $\mathcal{F}$ égal à J_r^T . Enfin, N doit être nilpotent, d'où le fait que la matrice N_{d-r} doive être nilpotente. On obtient donc :

$$|\tilde{\mathcal{N}}_d| = \sum_{r=1}^d \sum_{\mathcal{F} \in L_{r,d}} q^{r(d-r)} n_{d-r} = \sum_{r=1}^d |L_{r,d}| n_{d-r}(q) q^{r(d-r)}.$$

Il nous faut donc calculer le cardinal de $L_{r,d}$! Comment faire ? Considérons l'action suivante :

$$\begin{aligned} GL_d(\mathbb{F}_q) \times L_{r,d} &\longrightarrow L_{r,d} \\ (M, (e_1, \dots, e_r)) &\longmapsto (Me_1, \dots, Me_r). \end{aligned}$$

Cette action est transitive : en effet si $\mathcal{F}_1, \mathcal{F}_2 \in L_{r,d}$, alors le théorème de la base incomplète nous dit que l'on peut compléter ces deux familles en bases $\mathcal{B}_1, \mathcal{B}_2$ de $\mathbb{F}_q^d$. En prenant M la matrice de passage de la base $\mathcal{B}_1$ à la base $\mathcal{B}_2$, on a bien que $M \cdot \mathcal{F}_1 = \mathcal{F}_2$. Ainsi :

$$|L_{r,d}| = |\mathcal{O}_{\mathcal{F}}|$$

pour un certain $\mathcal{F} \in L_{r,d}$. Le calcul du cardinal de cette orbite peut s'effectuer grâce à celui du stabilisateur associé via la relation orbite-stabilisateur. Si on complète $\mathcal{F}$ en une base $\mathcal{B}$ de $\mathbb{F}_q^d$, on a qu'une matrice M est dans le stabilisateur de $\mathcal{F}$ si et seulement si la matrice de l'endomorphisme canoniquement associé à M s'écrit, dans la base $\mathcal{B}$:

$$\begin{pmatrix} I_r & A \\ \mathbf{0} & B \end{pmatrix}$$

où $A \in \mathcal{M}_{r,d-r}(\mathbb{F}_q)$ et $B \in GL_{d-r}(\mathbb{F}_q)$. En notant alors $g_k(q)$ le cardinal de $GL_k(\mathbb{F}_q)$, on a donc, grâce à la relation orbite-stabilisateur :

$$|L_{r,d}| = \frac{g_d(q)}{q^{r(d-r)} g_{d-r}(q)}.$$

Ainsi :

$$|\tilde{\mathcal{N}}_d| = \sum_{r=1}^d n_{d-r}(q) \frac{g_d(q)}{g_{d-r}(q)}.$$

Combinons les décomptes : En regroupant les résultats des deux décomptes, on obtient :

$$n_d(q) (q^d - 1) = \sum_{r=1}^d n_{d-r}(q) \frac{g_d(q)}{g_{d-r}(q)}$$

i.e.

$$\frac{n_d(q)}{g_d(q)} (q^d - 1) = \sum_{r=0}^{d-1} \frac{n_r(q)}{g_r(q)}.$$

On en conclut :

$$\frac{n_d(q)}{g_d(q)} (q^d - 1) = \frac{n_{d-1}(q)}{g_{d-1}(q)} + \frac{n_{d-1}(q)}{g_{d-1}(q)} (q^{d-1} - 1),$$

c'est-à-dire :

$$\frac{n_d(q)}{g_d(q)} = \frac{q^{d-1}}{q^d - 1} \frac{n_{d-1}(q)}{g_{d-1}(q)}.$$

On a donc, par produit télescopique :

$$\frac{n_d(q)}{g_d(q)} = \prod_{k=2}^d \left(\frac{q^{k-1}}{q^k - 1} \right) \underbrace{\frac{n_1(q)}{g_1(q)}}_{=\frac{1}{q-1}} = \frac{q^{\frac{d(d-1)}{2}}}{\prod_{k=1}^d (q^k - 1)} = \frac{q^{d(d-1)}}{g_d(q)}.$$

On en conclut :

$$n_d(q) = q^{d(d-1)}$$

ce qui termine la preuve!

□