Soient $n \geqslant 1$ et $X \in \mathcal{M}_n(\mathbf{F}_q)$ une matrice uniformément aléatoire.

Théorème 1. $\mathbb{P}(X \text{ est nilpotente}) = q^{-n}$.

Notons $a_n(q) \coloneqq |\mathfrak{N}({F_q}^n)|$ le nombre de matrices nilpotentes d'ordre n sur $\mathbf{F}_q$.

Lemme 2. Soient k un corps, E un k-ev de dimension finie n et $u \in \mathcal{L}(E)$. Il existe un unique couple (V, W) de sous-espaces vectoriels u-stables tel que :

(i) $E = V \oplus W$,
(ii) $u_V \in \mathfrak{N}(V)$,
(iii) $u_W \in \mathsf{GL}(W)$.

Définition 3. Les sous-espaces V et W sont respectivement appelés *nilespace* et *cœur* de u.

Preuve. **Existence.** Soit $m \in \mathbf{N}$ la valuation de X dans le polynôme minimal π_u de $u \in \mathcal{L}(E)$: il existe $Q \in k[X]$ tel que $\pi_u = X^m Q$ avec $Q(0) \neq 0$. D'après le lemme des noyaux $E = \operatorname{Ker} u^m \oplus \operatorname{Ker} Q(u)$. En particulier, $\dim \operatorname{Ker} Q(u) = n - \dim \operatorname{Ker} u^m = \dim \operatorname{Im} u^m$ grâce à la formule du rang. Or $\pi_u(u) = Q(u) \circ u^m = 0$, donc $\operatorname{Im} u^m \subseteq \operatorname{Ker} Q(u)$. Finalement $\operatorname{Ker} Q(u) = \operatorname{Im} u^m$, d'où

(i) $E = \operatorname{Ker} u^m \oplus \operatorname{Im} u^m$,

et il est clair que $V \coloneqq \operatorname{Ker} u^m$ et $W \coloneqq \operatorname{Im} u^m$ sont des sous-espaces u-stables. Soient $\varphi \coloneqq u_V$ et $\psi \coloneqq u_W$. Alors :

(ii) $\varphi \in \mathfrak{N}(V)$: pour tout $x \in V = \operatorname{Ker} u^m$, $\varphi^m(x) = u^m(x) = 0$ donc $\varphi \in \mathfrak{N}(V)$,
(iii) $\psi \in \mathsf{GL}(W)$: $\operatorname{Ker} \psi = \operatorname{Ker} u \cap \operatorname{Im} u^m \subseteq \operatorname{Ker} u^m \cap \operatorname{Im} u^m = \{0\}$.

Unicité. Soit (V, W) un couple satisfaisant (i), (ii) et (iii). Notons encore $\varphi \coloneqq u_V$ et $\psi \coloneqq u_W$. Soit m l'indice de nilpotence de φ. Tout élément x de E s'écrit de manière unique $x = v + w$ où $(v, w) \in V \times W$. Pour tout $i \in \mathbf{N}$,

$$u^i(x) = \underbrace{\varphi^i(v)}_{\in V} + \underbrace{\psi^i(w)}_{\in W},$$

donc

$$\begin{aligned} x \in \operatorname{Ker} u^i &\iff \varphi^i(v) = 0 \text{ et } \psi^i(w) = 0, \\ &\iff \varphi^i(v) = 0 \text{ et } w = 0, \\ &\iff x \in \operatorname{Ker} \varphi^i \end{aligned}$$

et en particulier $\operatorname{Ker} u^m = \operatorname{Ker} \varphi^m = V$. Aussi, $\operatorname{Im} u^m = \operatorname{Im} \varphi^m \oplus \operatorname{Im} \psi^m = \{0\} \oplus W = W$. ∎

Corollaire 4. Notons $\mathcal{T}(E) \coloneqq \{(V, W, \varphi, \psi) \mid E = V \oplus W,\ \varphi \in \mathfrak{N}(V),\ \psi \in \mathsf{GL}(W)\}$. L'application

$$\begin{aligned} \mathcal{L}(E) &\longrightarrow \mathcal{T}(E) \\ u &\longmapsto (V, W, u_V, u_W) \end{aligned}$$

est une bijection.

Lemme 5. Tout ev V de dimension j sur $\mathbf{F}_q$ admet $b_j(q) \coloneqq (q^j - 1)(q^j - q) \cdots (q^j - q^{j-1})$ bases, et donc aussi $b_j(q)$ automorphismes.

Démonstration. Il y a $|V \setminus \{0\}| = q^j - 1$ choix pour le premier vecteur de base. Puisque tout vecteur de base ne doit pas être dans le sous-espace engendré par les précédents, il reste $q^j - q$ choix pour le deuxième vecteur, $q^j - q^2$ choix pour le troisième, et ainsi de suite, jusqu'à $q^j - q^{j-1}$ choix pour le dernier vecteur. Enfin, si l'on fixe une base $(v_1, \ldots, v_j)$ de V, se donner un automorphisme de V revient à choisir la base-image de $(v_1, \ldots, v_j)$. Le nombre de bases de V est donc $|\mathsf{GL}(V)| = b_j(q)$. ∎

Démonstration du théorème 1. Soit pour tout $0 \leqslant j \leqslant n$,

$$\mathcal{T}_j({\mathbf{F}_q}^n) \coloneqq \{(V, W, \varphi, \psi) \in \mathcal{T}({\mathbf{F}_q}^n) \mid \dim V = j\},$$

de sorte que

$$\mathcal{T}({\mathbf{F}_q}^n) = \bigsqcup_{j=0}^{n} \mathcal{T}_j({\mathbf{F}_q}^n). \qquad (\star)$$

Calculons $|\mathcal{T}_j(\mathbf{F}_q{}^n)|$. Se donner $(V, W, \varphi, \psi) \in \mathcal{T}_j(\mathbf{F}_q{}^n)$, c'est choisir (V, W) en somme directe tel que $j = \dim V = n - \dim W$, un élément de $\mathfrak{N}(V)$ et un élément de $\mathsf{GL}(W)$. Or l'application

$$\begin{aligned} \{ \text{ bases de } \mathbf{F}_q{}^n \} &\longrightarrow \{(V, W) \mid \mathbf{F}_q{}^n = V \oplus W,\ \dim V = j\} \\ (e_1, \dots, e_n) &\longmapsto (\mathrm{Vect}(b_1, \dots, b_j), \mathrm{Vect}(b_{j+1}, \dots, b_n)) \end{aligned}$$

est surjective, et chaque image admet $b_j(q)b_{n-j}(q)$ antécédents. D'où, d'après le lemme des bergers,

$$\begin{aligned} |\mathcal{T}_j(\mathbf{F}_q{}^n)| &= \frac{b_n(q)}{b_j(q)b_{n-j}(q)} \times a_j(q) \times b_{n-j}(q), \\ &= \frac{b_n(q)}{b_j(q)} a_j(q). \end{aligned}$$

Finalement

$$\begin{aligned} q^{n^2} &= |\mathcal{L}(\mathbf{F}_q{}^n)| \\ &= |\mathcal{T}(\mathbf{F}_q{}^n)| && \text{(d'après le corollaire 4)} \\ &= \sum_{j=0}^{n} |\mathcal{T}_j(\mathbf{F}_q{}^n)| && \text{(d'après } (\star)\text{)} \\ &= \sum_{j=0}^{n} \frac{b_n(q)}{b_j(q)} a_j(q), \end{aligned}$$

et si $n \geqslant 1$,

$$\begin{aligned} \mathbb{P}(X \text{ est nilpotente}) &= a_n(q) q^{-n^2} \\ &= 1 - q^{-n^2} \frac{b_n(q)}{b_{n-1}(q)} \sum_{j=0}^{n-1} \frac{b_{n-1}(q)}{b_j(q)} a_j(q) \\ &= 1 - q^{-n^2} \frac{b_n(q)}{b_{n-1}(q)} q^{(n-1)^2} \\ &= 1 - q^{-n^2} q^{n-1} (q^n - 1) q^{(n-1)^2} \\ &= q^{-n}. \end{aligned}$$

■

Références. [Tos]

106 Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $\mathsf{GL}(E)$. Applications.

123 Corps finis. Applications.

151 Dimension d'un espace vectoriel. Rang. Exemples et applications.

153 Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.

157 Endomorphismes trigonalisables. Endomorphismes nilpotents.

190 Méthodes combinatoires, problèmes de dénombrement.

264 Variables aléatoires discrètes. Exemples et applications.

[Tos] Nicolas Tosel : Quelques dénombrements dans $\mathcal{M}_n(\mathbf{F}_q)$. *In Revue de la Filière Mathématiques*, numéro 117–1.