Sur le nombre d'éléments singuliers dans l'anneau des matrices sur un corps fini

N. Lygeros

1. Introduction

Définition : F, F_n, $o(F_n)$, $s(F_n)$ désignent respectivement un corps fini de caractéristique q, l'anneau des matrices $n * n$ sur F, le nombre d'éléments de F_n et le nombre d'éléments singuliers de F_n.

Historique : En 1967, K. Koh [2] a démontré que si R est un anneau avec m diviseurs de zéro, où $m>1$, alors le nombre total d'éléments dans R est inférieur ou égal à m^2. Puis grâce au théorème suivant de J. J. Rotman [6]

Théorème : (J. J. Rotman 1968) $s(F_n) = q^{n^2} - \prod_{k=0}^{n-1} (q^n - q^k)$.

K. Koh [3] a pu expliciter le théorème sur l'anneau des matrices carrées d'ordre n sur un corps fini de caractéristique q.

Théorème : (K. Koh 1985) Pour $n > 1$, $o(F_n) < s(F_n)^{1+1/n(n-1)}$ et $\lim_{n \to +\infty} \frac{\ln o(F_n)}{\ln s(F_n)} = 1$.

Le théorème de Koh s'appuie essentiellement sur le lemme de Koh.

Lemme : (K. Koh 1985) Pour $q \geq 2$ et $n \geq 2$: $s(F_n) > q^{n^2-1}$.

Quant à la limite du rapport logarithmique elle provient directement de l'inégalité du théorème puisque nous avons de manière élémentaire $o(F_n) = q^{n^2}$.

Par la suite Th. Vougiouklis [7], en utilisant la technique de N. Jacobson [1], a montré qu'il n'existe que deux types de sous-groupes additifs dans les anneaux associatifs avec des diviseurs de zéro. Cette approche lui a permis via l'introduction des matrices xy-symétriques et le formalisme de D. Kurepa [4] d'améliorer l'inégalité du théorème de Koh.

Théorème : (Th. Vougiouklis 1990) $o(F_n) < s(F_n) s_n^{xy\,4/(n^2-1)} < s(F_n)^{1+1/(n(n+1))}$

où $s_n^{xy} = q^{n^2/4}$ pour n pair et $s_n^{xy} = q^{(n^2-1)/4}$ pour n impair.

Ce résultat amène à se poser la question de l'optimalité de la borne et c'est pour répondre à cette question que nous avons étudié les matrices singulières d'ordre 2 [5].

2. Résultats

Lemme : Pour $n > 1$, $s(F_n) = q^{n^2-1} + q^{n^2-2} + O\left(q^{n^2-3}\right)$.

Démonstration : $s(F_n) = q^{n^2} - \prod_{k=0}^{n-1}\left(q^n - q^k\right) = q^{n^2} - q^{1+\ldots+(n-1)}\prod_{k=1}^{n}\left(q^k - 1\right)$

$$s(F_n) = q^{n^2} - q^{\frac{n(n-1)}{2}}\prod_{k=1}^{n}\left(q^k - 1\right) = q^{n^2} - q^{\frac{n(n-1)}{2}}\left(q^n - 1\right)\left(q^{n-1} - 1\right)\ldots\left(q - 1\right)$$

$$s(F_n) = q^{n^2} - q^{\frac{n(n-1)}{2}}.q^{\frac{n(n+1)}{2}} + q^{\frac{n(n-1)}{2}}.q^{\frac{n(n-1)}{2}} + q^{\frac{n(n-1)}{2}}.q^{\frac{n(n-1)}{2}-1} + O\left(q^{n^2-3}\right)$$

$$s(F_n) = q^{n^2} - q^{n^2} + q^{n^2-1} + q^{n^2-2} + O\left(q^{n^2-3}\right) = q^{n^2-1} + q^{n^2-2} + O\left(q^{n^2-3}\right) \quad \square$$

Ce lemme est optimal dans sa généralité puisque nous avons $s(F_4) = q^{15} + q^{14} - 2q^{11} + q^8 + q^7 - q^6$. Aussi il permet de montrer que le lemme de Koh est lui-même optimal dans sa généralité puisque nous avons $s(F_2) = q^3 + q^2 - q$. De plus il rend évident le résultat sur le rapport logarithmique. Ainsi cette approche par les équivalents est plus puissante que celle qui n'exploite que les inégalités. Enfin en modifiant la borne de n nous pouvons obtenir un théorème plus précis suivant la même méthode et qui est optimal pour cette borne.

Théorème : Pour $n \geq 11$: $s(F_n) = q^{n^2-1} + q^{n^2-2} - q^{n^2-5} - q^{n^2-7} + O\left(q^{n^2-12}\right)$.

La démonstration du théorème utilise le lemme suivant.

Lemme : $s(F_{n+1}) = q^{n^2+n} + q^n\left(q^{n+1} - 1\right)s(F_n)$.

Démonstration : Par récurrence sur $s(F_n) = q^{n^2} - q^{\frac{n(n-1)}{2}}\prod_{k=1}^{n}\left(q^k - 1\right)$

n = 2 : $s(F_2) = q^3 + q^2 - q$

n + 1 : $s(F_{n+1}) = q^{(n+1)^2} - q^{\frac{n(n+1)}{2}}\prod_{k=1}^{n+1}\left(q^k - 1\right)$

$$s(F_{n+1}) = q^{(n+1)^2} - q^n \cdot q^{\frac{n(n-1)}{2}}\left(q^{n+1} - 1\right)\prod_{k=1}^{n}\left(q^k - 1\right)$$

$$s(F_{n+1}) = q^{(n+1)^2} + q^n\left(q^{n+1} - 1\right)\left[s(F_n) - q^{n^2}\right]$$

$$s(F_{n+1}) = q^{(n+1)^2} - q^{n^2+n}\left(q^{n+1} - 1\right) + q^n\left(q^{n+1} - 1\right)s(F_n)$$

$$s(F_{n+1}) = q^{(n+1)^2} - q^{n^2+2n+1} + q^{n^2+n} + q^n\left(q^{n+1} - 1\right)s(F_n)$$

$$s(F_{n+1}) = q^{n^2+n} + q^n\left(q^{n+1} - 1\right)s(F_n) \quad \square$$

Enfin les valeurs de $s(F_n)$ pour $1<n<12$ permettent de comprendre la perturbation engendrée par le coefficient associé à q^{11} dans $s(F_4)$ et sa disparition dans les ordres plus élevés.

Valeurs :

$$s(F_2) = q^3 + q^2 - q$$

$$s(F_3) = q^8 + q^7 - q^5 - q^4 + q^3$$

$$s(F_4) = q^{15} + q^{14} - 2q^{11} + q^8 + q^7 - q^6$$

$$s(F_5) = q^{24} + q^{23} - q^{20} - q^{19} - q^{18} + q^{17} + q^{16} + q^{15} - q^{12} - q^{11} + q^{10}$$

$$s(F_6) = q^{35} + q^{34} - q^{31} - 2\,q^{29} + q^{27} + q^{26} + q^{25} + q^{24} - 2\,q^{22} - q^{20} + q^{17} + q^{16} - q^{15}$$

$$s(F_7) =$$

$$q^{48} + q^{47} - q^{44} - q^{42} - q^{41} + q^{39} + q^{38} + 2\,q^{37} - 2\,q^{33} - q^{32} - q^{31} + q^{29} + q^{28} + q^{26} - q^{23} - q^{22} + q^{21}$$

$$s(F_8) =$$

$$q^{63} + q^{62} - q^{59} - q^{57} - q^{55} + q^{53} + 2\,q^{52} + q^{51} + q^{49} - q^{48} - q^{47} - 2\,q^{46} - q^{45} - q^{44} + q^{43} + q^{41} + 2\,q^{40} + q^{39} - q^{37} - q^{35} - q^{33} + q^{30} + q^{29} - q^{28}$$

$$s(F_9) =$$

$$q^{80} + q^{79} - q^{76} - q^{74} - q^{71} + 2\,q^{69} + q^{68} + q^{67} + q^{66} - q^{64} - q^{63} - q^{62} - 2\,q^{61} - q^{60} - q^{59} + q^{58} + q^{57} + 2\,q^{56} + q^{55} + q^{54} + q^{53} - q^{51} - q^{50} - q^{49} - 2\,q^{48} + q^{46} + q^{43} + q^{41} - q^{38} - q^{37} + q^{36}$$

$$s(F_{10}) =$$

$$q^{99} + q^{98} - q^{95} - q^{93} - q^{89} + q^{88} + q^{87} + q^{86} + 2\,q^{85} - q^{82} - q^{81} - q^{80} - q^{79} - 3\,q^{78} + q^{75} + q^{74} + 2\,q^{73} + 2\,q^{72} + q^{71} + q^{70} - 3\,q^{67} - q^{66} - q^{65} - q^{64} - q^{63} + 2\,q^{60} + q^{59} + q^{58} + q^{57} - q^{56} - q^{52} - q^{50} + q^{47} + q^{46} - q^{45}$$

$$s(F_{11}) =$$

$$q^{120} + q^{119} - q^{116} - q^{114} + q^{107} + 2\,q^{106} + q^{105} - q^{102} - q^{101} - q^{100} - 2\,q^{99} - q^{98} - q^{97} - q^{95} + 2\,q^{94} + 2\,q^{93} + 2\,q^{92} + 2\,q^{91} + q^{90} + q^{89} - q^{87} - q^{86} - 2\,q^{85} - 2\,q^{84} - 2\,q^{83} - 2\,q^{82} + q^{81} + q^{79} + q^{78} + 2\,q^{77} + q^{76} + q^{75} + q^{74} - q^{71} - 2\,q^{70} - q^{69} + q^{62} + q^{60} - q^{57} - q^{56} + q^{55}$$

Références

[1] N. Jacobson: Lectures in Abstract Algebra.
Vol. I. Van Nostrand, N.Y. 1966.

[2] K. Koh: On properties of rings with a finite number of zero divisors.
Math. Ann. 171:79-80 (1967)

[3] K. Koh: On the Matrix Ring over a Finite Field.
Linear Algebra and its Applications 66:195-197 (1985)

[4] D. Kurepa: On Triangular Matrices.
Glasnik MFA, 20/No 1-2, 3-32 (1965)

[5] N. Lygeros: Remarques sur les matrices singulières d'ordre deux.
Perfection vol. 6 1 1/2005

[6] J. J. Rotman: The Theory of Groups.
Allyn and Bacon, Boston, 1968.

[7] Th. Vougiouklis: A Classification of Rings with Zero Divisors.
Mathematica Balkanica. Now Series Vol. 3, 1989, Fasc. 3-4, 241-243.

[8] Th. Vougiouklis: On Rings with Zero Divisors. Strong V-groups.
Commentationes Mathematicae Universitatis Carolinae 31, 3 (1990) 431-433.