C. R. Acad. Sci. Paris, Ser. I 357 (2019) 766–770

Contents lists available at ScienceDirect

C. R. Acad. Sci. Paris, Ser. I

www.sciencedirect.com

Number theory/Combinatorics

A sum–product theorem in matrix rings over finite fields

Un théorème somme–produit dans les anneaux de matrices sur les corps finis

Thang Pham

Department of Mathematics, University of Rochester, NY, USA

ARTICLE INFO

Article history:
Received 22 December 2018
Accepted after revision 12 September 2019
Available online 26 September 2019

Presented by the Editorial Board

ABSTRACT

In this note, we study a sum–product estimate over matrix rings $M_n(\mathbb{F}_q)$. More precisely, for $A \subset M_n(\mathbb{F}_q)$, we have

- if $|A \cap GL_n(\mathbb{F}_q)| \le |A|/2$, then

$$\max\{|A+A|, |AA|\} \gg \min\left\{|A|q, \frac{|A|^3}{q^{2n^2-2n}}\right\};$$

- if $|A \cap GL_n(\mathbb{F}_q)| \ge |A|/2$, then

$$\max\{|A+A|, |AA|\} \gg \min\left\{|A|^{\frac{2}{3}}q^{\frac{n^2}{3}}, \frac{|A|^{3/2}}{q^{\frac{n^2}{2}-\frac{1}{4}}}\right\}.$$

We also will provide a lower bound of $|A+B|$ for $A \subset SL_n(\mathbb{F}_q)$ and $B \subset M_n(\mathbb{F}_q)$.

RÉSUMÉ

Dans cette Note, nous étudions le phénomène somme–produit dans les anneaux de matrices $M_n(\mathbf{F}_q)$. Plus précisément, pour $A \subset M_n(\mathbf{F}_q)$, nous montrons :

- si $|A \cap GL_n(\mathbf{F}_q)| \le |A|/2$, alors

$$\max\{|A+A|, |AA|\} \gg \min\left\{|A|q, \frac{|A|^3}{q^{2n^2-2n}}\right\};$$

- si $|A \cap GL_n(\mathbf{F}_q)| \ge |A|/2$, alors

$$\max\{|A+A|, |AA|\} \gg \min\left\{|A|^{\frac{2}{3}}q^{\frac{n^2}{3}}, \frac{|A|^{3/2}}{q^{\frac{n^2}{2}-\frac{1}{4}}}\right\}.$$

E-mail address: vanthangpham@rochester.edu.

https://doi.org/10.1016/j.crma.2019.09.008

Nous donnons également une minoration de $|A+B|$ pour $A \subset SL_n(\mathbf{F}_q)$ et $B \subset M_n(\mathbf{F}_q)$.

1. Introduction

Let A be a set in $\mathbb{Z}$. We define the sum and product sets as follows:

$$A+A=\{a+b\colon a,b\in A\},$$
$$A\cdot A=\{ab\colon a,b\in A\}.$$

A celebrated result of Erdős and Szemerédi [4] states that there is no set $A\subset\mathbb{Z}$ that has both additive and multiplicative structures. More precisely, given any finite set $A\subset\mathbb{Z}$, we have

$$\max\{|A+A|,|A\cdot A|\}\gg|A|^{1+\varepsilon}$$

for some positive constant ε.

In the setting of finite fields, Bourgain, Katz, and Tao [1] showed that, given any set $A\subset\mathbb{F}_p$ with p prime and $p^\delta<|A|<p^{1-\delta}$ for some $\delta>0$, one has

$$\max\{|A+A|,|A\cdot A|\}\ge C_\delta|A|^{1+\varepsilon},$$

for some $\varepsilon=\varepsilon(\delta)>0$. Note that the relation between ε and δ is difficult to determine. Using Fourier analytic methods, Hart, Iosevich, and Solymosi [6] obtained a bound over arbitrary finite fields that gives an explicit dependence of ε on δ. The precise statement of their result is as follows.

Theorem 1.1 *(Hart–Iosevich–Solymosi, [6]). Let $\mathbb{F}_q$ be an arbitrary finite field of order q, and A be a set of $\mathbb{F}_q$. Suppose that $|A+A|=m$ and $|A\cdot A|=n$, then we have*

$$|A|^3\le\frac{cm^2n|A|}{q}+cq^{1/2}mn, \tag{1}$$

for some positive constant c.

We note that Theorem 1.1 is non-trivial when $|A|\gg q^{1/2}$. In particular, if $q^{1/2}\le|A|\le q^{7/10}$, then we have

$$\max\{|A+A|,|A\cdot A|\}\gg\frac{|A|^{\frac{3}{2}}}{q^{\frac{1}{4}}}.$$

Hence, $\max\{|A+A|,|A\cdot A|\}\gg|A|^{8/7}$ when $|A|\sim q^{7/10}$. We refer the interested reader to [8] for a current result when the size of A is not too big.

Here and throughout, $X\gg Y$ means that $X\ge CY$ for some positive constant C, $X\sim Y$ means that $X\gg Y$ and $Y\gg X$.

For an integer $n\ge2$, let $M_n(\mathbb{F}_q)$ be the set of $n\times n$ matrices with entries in $\mathbb{F}_q$, $SL_n(\mathbb{F}_q)$ be the special linear group in $M_n(\mathbb{F}_q)$, $Z_n(\mathbb{F}_q)$ be the set of matrices in $M_n(\mathbb{F}_q)$ with zero determinant, and $GL_n(\mathbb{F}_q)$ be the set of invertible matrices in $M_n(\mathbb{F}_q)$.

For $A\subset M_n(\mathbb{F}_q)$, we define:

$$A+A:=\{a+b\colon a,b\in A\},\ \ AA:=\{a\cdot b\colon a,b\in A\}.$$

In the setting of matrix rings, the first sum–product estimate bound over $M_2(\mathbb{F}_q)$ was obtained by Karabulut, Koh, Shen, Vinh, and the author in [2]. In particular, they proved the following theorem.

Theorem 1.2 *(Demiroglu Karabulut et al., [2]). For $A\subset M_2(\mathbb{F}_q)$ with $|A|\gg q^3$, we have*

$$\max\{|A+A|,|AA|\}\gg\min\left\{\frac{|A|^2}{q^{7/2}},\ q^2|A|^{1/2}\right\}.$$

The main purpose of this note is to extend this theorem to the setting of $M_n(\mathbb{F}_q)$ for any $n\ge3$. Our first result is as follows.

Theorem 1.3. *For $A \subset M_n(\mathbb{F}_q)$ with $n \geq 3$, we have*

- *if $|A \cap GL_n(\mathbb{F}_q)| \leq |A|/2$, then*

$$\max\{|A+A|, |AA|\} \gg \min\left\{|A|q, \frac{|A|^3}{q^{2n^2-2n}}\right\};$$

- *if $|A \cap GL_n(\mathbb{F}_q)| \geq |A|/2$, then*

$$\max\{|A+A|, |AA|\} \gg \min\left\{|A|^{\frac{2}{3}}q^{\frac{n^2}{3}}, \frac{|A|^{3/2}}{q^{\frac{n^2}{2}-\frac{1}{4}}}\right\}.$$

In [2], Demiroglu Karabulut et al. also proved that, for $A \subset SL_2(\mathbb{F}_q)$ and $B \subset M_2(\mathbb{F}_q)$, one has

$$|A+B| \gg \min\left\{\frac{|A||B|^2}{q^3}, |A|q\right\}.$$

This estimate was one of the two key ingredients to show that the polynomials $x+yz$ and $x(y+z)$ are *moderate expanders* over $SL_2(\mathbb{F}_q)$ and $M_2(\mathbb{F}_q)$. We refer our readers to [2] for more details. In our second main theorem, we will give a lower bound of $|A+B|$ where $A \subset SL_n(\mathbb{F}_q)$ and $B \subset M_n(\mathbb{F}_q)$ with $n \geq 3$.

Theorem 1.4. *For $A \subset SL_n(\mathbb{F}_q)$ and $B \subset M_n(\mathbb{F}_q)$ with $n \geq 3$, we have*

$$|A+B| \gg \min\left\{|A|q, \frac{|A|^2|B|}{q^{2n^2-2n-2}}\right\}.$$

Corollary 1.5. *Let A be a set in $SL_n(\mathbb{F}_q)$ with $n \geq 3$. Suppose that $|A| \geq q^{\frac{2n^2-2n-2}{2-\varepsilon}}$ with $0 < \varepsilon < \frac{2n}{n^2-1}$, then we have*

$$|A+A| \gg \min\left\{|A|^{1+\frac{1}{n^2-1}}, |A|^{1+\varepsilon}\right\}.$$

2. Proofs of Theorems 1.3 and 1.4

In the proofs of Theorems 1.3 and 1.4, we will make use of the following results. The first result is given by Li and Su [7] by using Gauss sums of general linear groups and special linear groups.

Lemma 2.1 *(Theorem 3.2, [7]). Let U and V be two sets in $M_n(\mathbb{F}_q)$. Let $Z(U,V)$ be the number of pairs $(u,v) \in U \times V$ such that $u+v \in Z_n(\mathbb{F}_q)$, and $S(U,V)$ be the number of pairs $(u,v) \in U \times V$ such that $u+v \in SL_n(\mathbb{F}_q)$. We have the following estimates*

$$Z(U,V) \leq \frac{|Z_n(\mathbb{F}_q)||U||V|}{q^{n^2}} + q^{n^2-n}\sqrt{|U||V|},$$

and

$$S(U,V) \leq \frac{|SL_n(\mathbb{F}_q)||U||V|}{q^{n^2}} + q^{n^2-n-1}\sqrt{|U||V|}.$$

Theorem 2.2. *For $A \subset Z_n(\mathbb{F}_q)$ and $B \subset M_n(\mathbb{F}_q)$, we have*

$$|A+B| \gg \min\left\{|A|q, \frac{|A|^2|B|}{q^{2n^2-2n}}\right\}.$$

Proof. Set $U = A+B$ and $V = -B$. Let $Z(U,V)$ be the number of pairs $(u,v) \in U \times V$ such that $u+v \in Z_n(\mathbb{F}_q)$. For any pairs $(a,b) \in A \times B$, we have $(a+b)+(-b) \in Z_n(\mathbb{F}_q)$. Therefore, $Z(U,V) \geq |A||B|$.

Since $|GL_n(\mathbb{F}_q)| = q^{\frac{n^2-n}{2}} \prod_{j=1}^{n}(q^j - 1) = q^{n^2} - q^{n^2-1} + O(q^{n^2-2})$ (see [3, Theorem 99]), we have $|Z_n(\mathbb{F}_q)| = q^{n^2-1} + O(q^{n^2-2})$. Thus, it follows from Lemma 2.1 that

$$Z(U,V) \ll \frac{|U||V|}{q} + q^{n^2-n}\sqrt{|U||V|}.$$

Therefore,

$$|A||B| \leq \frac{|A+B||B|}{q} + q^{n^2-n}\sqrt{|A+B||B|}.$$

Solving this inequality with $x = \sqrt{|A+B|}$, we obtain

$$x \gg \min\left\{\frac{|A||B|^{1/2}}{q^{n^2-n}},\ |A|^{1/2}q^{1/2}\right\}.$$

This concludes the proof of the theorem. □

The following result is given by Ferguson, Hoffman, Luca, Ostafe, and Shparlinski [5] by employing a version of the Kloosterman sum over matrix rings.

Lemma 2.3 *(Theorem* 8, *[5]). Let A, B, C, D be sets in $M_n(\mathbb{F}_q)$. For any matrix h in $GL_n(\mathbb{F}_q)$, let $N_h(A,B,C,D)$ be the number of tuples $(a,b,c,d) \in A \times B \times C \times D$ such that $(a+b)(c+d) = h$. We have the following estimate*

$$N_h(A,B,C,D) \leq \frac{|A||B||C||D|}{q^{n^2}} + q^{n^2-\frac{1}{2}}\sqrt{|A||B||C||D|}.$$

We are now ready to prove Theorem 1.3.

Proof of Theorem 1.3. Suppose $|A \cap GL_n(\mathbb{F}_q)| \leq |A|/2$. In this case, we have $|A \cap Z_n(\mathbb{F}_q)| \geq |A|/2$. Without loss of generality, we assume that A is a subset of $Z_n(\mathbb{F}_q)$. It follows from Theorem 2.2 that

$$|A+A| \gg \min\left\{|A|q,\ \frac{|A|^3}{q^{2n^2-2n}}\right\}.$$

Using the fact that $\max\{|A+A|, |AA|\} \geq |A+A|$, the first claim of Theorem 1.3 is proved.

Suppose that $|A \cap GL_n(\mathbb{F}_q)| \geq |A|/2$. Without loss of generality, we assume that $A \subset GL_n(\mathbb{F}_q)$. Thus $AA \subset GL_n(\mathbb{F}_q)$.

We now consider the following equation

$$(x+y)(z+t) = w, \tag{2}$$

where $x \in A+A$, $y \in -A$, $z \in A+A$, $t \in -A$, $w \in AA$. Let N be the number of solutions to this equation. It is not hard to check that

$$N = \sum_{w \in AA} N_w(A+A, -A, A+A, -A).$$

Applying Lemma 2.3 for each $w \in AA$, we obtain

$$N \leq |AA|\left(\frac{|A+A|^2|A|^2}{q^{n^2}} + q^{n^2-\frac{1}{2}}|A+A||A|\right).$$

On the other hand, one can check that the tuples $(a+b, -b, c+d, -d, ac)$, with $a, b, c, d \in A$, are solutions to Eq. (2). Therefore,

$$|A|^4 \leq N \leq \frac{|A+A|^2|AA||A|^2}{q^{n^2}} + q^{n^2-\frac{1}{2}}|AA||A+A||A|.$$

Solving this inequality gives us

$$\max\{|A+A|, |AA|\} \gg \min\left\{|A|^{\frac{2}{3}}q^{\frac{n^2}{3}},\ \frac{|A|^{3/2}}{q^{\frac{n^2}{2}-\frac{1}{4}}}\right\}.$$

This completes the proof of the second claim of Theorem 1.3. □

Proof of Theorem 1.4. Set $U = A+B$ and $V = -B$. Let $S(U,V)$ be the number of pairs $(u,v) \in U \times V$ such that $u+v \in SL_n(\mathbb{F}_q)$. For any pairs $(a,b) \in A \times B$, we have $(a+b)+(-b) \in SL_n(\mathbb{F}_q)$. Therefore, $S(U,V) \geq |A||B|$.

Since $|GL_n(\mathbb{F}_q)| = q^{\frac{n^2-n}{2}}\prod_{j=1}^{n}(q^j-1) = q^{n^2} - q^{n^2-1} + O(q^{n^2-2})$ (see [3, Theorem 99]), we have $|SL_n(\mathbb{F}_q)| = (q-1)^{-1}|GL_n(\mathbb{F}_q)| \sim q^{n^2-1} + O(q^{n^2-2})$. Thus, it follows from Lemma 2.1 that

$$S(U,V) \ll \frac{|U||V|}{q} + q^{n^2-n-1}\sqrt{|U||V|}.$$

Therefore,

$$|A||B| \le \frac{|A+B||B|}{q} + q^{n^2-n-1}\sqrt{|A+B||B|}.$$

Solving this inequality with $x = \sqrt{|A+B|}$, we obtain

$$x \gg \min\left\{\frac{|A||B|^{1/2}}{q^{n^2-n-1}},\ |A|^{1/2}q^{1/2}\right\},$$

and the theorem follows. □

Acknowledgement

The author would like to thank Igor Shparlinski for drawing his attention to the paper [7] while the paper was preparing. The author would like to thank the referee for valuable suggestions. The author was supported by Swiss National Science Foundation grant P400P2-183916.

References

[1] J. Bourgain, N. Katz, T. Tao, A sum–product estimate in finite fields, and applications, Geom. Funct. Anal. 14 (2004) 27–57.
[2] Y. Demiroglu Karabulut, D. Koh, T. Pham, C-Y. Shen, L.A. Vinh, Expanding phenomena over matrix rings, Forum Math. 31 (4) (2019), https://doi.org/10.1515/forum-2019-0032.
[3] L.E. Dickson, Linear Groups: With an Exposition of the Galois Field Theory, Dover Publ. Inc., New York, 1958.
[4] P. Erdős, E. Szemerédi, On sums and products of integers, in: Studies in Pure Mathematics. To the Memory of Paul Turan, Birkhäuser Verlag, Basel, Switzerland, 1983, pp. 213–218.
[5] R. Ferguson, C. Hoffman, F. Luca, A. Ostafe, I. Shparlinski, Some additive combinatorics problems in matrix rings, Rev. Mat. Complut. 23 (2) (2010) 501–513.
[6] D. Hart, A. Iosevich, J. Solymosi, Sum-product estimates in finite fields via Kloosterman sums, Int. Math. Res. Not. 2007 (5) (2007) rnm007.
[7] Y. Li, H. Su, Gauss sums over some matrix groups, J. Number Theory 132 (12) (2012) 2967–2976.
[8] M. Rudnev, G. Shakan, I. Shkredov, Stronger sum–product inequalities for small sets, arXiv:1808.08465, 2018.