Some additive combinatorics problems in matrix rings

Ferguson, R ; Hoffman, C ; Luca, F ; Ostafe, A ; Shparlinski, I E

DOI: https://doi.org/10.1007/s13163-010-0029-4

Some Additive Combinatorics Problems in Matrix Rings

Ron Ferguson
Department of Mathematics, University of Vlora
Vlora, Albania
ronf@univlora.edu.al

Corneliu Hoffman
School of Mathematics, University of Birmingham
Edgbaston Birmingham B15 2TT, United Kingdom
C.G.Hoffman@bham.ac.uk

Florian Luca
Instituto de Matemáticas, UNAM
C.P. 58089, Morelia, Michoacán, México
fluca@matmor.unam.mx

Alina Ostafe
Institut für Mathematik, Universität Zürich
Winterthurerstrasse 190 CH-8057, Zürich, Switzerland
alina.ostafe@math.uzh.ch

Igor E. Shparlinski
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

January 11, 2010

Abstract

We study the distribution of singular and unimodular matrices in sumsets in matrix rings over finite fields. We apply these results to estimate the largest prime divisor of the determinants in sumsets in matrix rings over the integers.

2000 Mathematics Subject Classification. 11C20, 11D79, 11T23

Keywords. Matrices, finite fields, additive combinatorics

1 Introduction

There is a series of recent works where various problems of additive combinatorics (see [23]) have been considered in the matrix rings (see [2, 3, 4, 5, 12, 13] for several recent results and further references in the area).

Here, we consider several more problems of combinatorial flavor in the set $\mathcal{M}_n(\mathbb{F}_q)$ of all $n \times n$ matrices over a finite field $\mathbb{F}_q$ of q elements.

Furthermore, let $\mathrm{GL}_n(\mathbb{F}_q)$, $\mathrm{SL}_n(\mathbb{F}_q)$ and $\mathcal{Z}_n(\mathbb{F}_q)$ be the group of invertible matrices, the group of matrices of determinant 1 and the set of singular matrices, respectively, where all matrices are from $\mathcal{M}_n(\mathbb{F}_q)$.

We always assume that $n \geq 2$ and in fact some of our results have no analogues in the scalar case $n = 1$.

Given two sets $\mathcal{A}, \mathcal{B} \subseteq \mathcal{M}_n(\mathbb{F}_q)$, we define

$$\begin{aligned} N_{n,q}(\mathcal{A}, \mathcal{B}) &= \#\{A + B \in \mathcal{Z}_n(\mathbb{F}_q) \ : \ A \in \mathcal{A}, \ B \in \mathcal{B}\}, \\ T_{n,q}(\mathcal{A}, \mathcal{B}) &= \#\{A + B \in \mathrm{SL}_n(\mathbb{F}_q) \ : \ A \in \mathcal{A}, \ B \in \mathcal{B}\}. \end{aligned}$$

We show that if $\mathcal{A}$ and $\mathcal{B}$ are sufficiently large, then $N_{n,q}(\mathcal{A}, \mathcal{B})$ and $T_{n,q}(\mathcal{A}, \mathcal{B})$ are close to their expected value $\#\mathcal{A}\#\mathcal{B}/q$. We also adapt the method of D. Hart, A. Iosevich and J. Solymosi [11] to show that pairwise products of matrices from the sumset of $\mathcal{A}, \mathcal{B} \subseteq \mathcal{M}_n(\mathbb{F}_q)$ and the sumset of $\mathcal{C}, \mathcal{D} \subseteq \mathcal{M}_n(\mathbb{F}_q)$ generate the whole group $\mathrm{GL}_n(\mathbb{F}_q)$, provided that

$$\#\mathcal{A}\#\mathcal{B}\#\mathcal{C}\#\mathcal{D} \geq c(n) q^{4n^2-1} \tag{1}$$

holds with a sufficiently large constant $c(n)$ depending only on n. In fact, if $n = 1$, that is for the scalar case, we obtain a result of the same strength of that of D. Hart, A. Iosevich and J. Solymosi [11, Theorem 1.4] (for $d = 2$).

Although the questions we consider are of combinatorial natures, our proofs are based on some tools from analytic number theory and algebraic geometry. In particular, we use estimates of character sums along algebraic varieties due to A. Skorobogatov [22] (see also [8, 9, 15, 17, 18, 21] and references therein). This in turn leads us to study the singularity locus as well as other properties of some algebraic varieties associated with the determinant.

Finally, we apply our results to estimate the number of prime divisors of determinants of matrices from some sumsets of matrices over $\mathbb{Z}$.

Throughout the paper, we always assume that i and j run through the set $\{1, \ldots, n\}$. The implied constants in the symbols 'O', and '$\ll$' may depend on the dimension $n \geq 2$. We recall that the notations $U = O(V)$ and $U \ll V$ are all equivalent to the assertion that the inequality $|U| \leq cV$ holds for some constant $c > 0$.

2 Preliminaries

2.1 Determinantal varieties

Let $\mathbb{K} = \overline{\mathbb{F}}_q$ be the algebraic closure of $\mathbb{F}_q$. We consider $\mathcal{Z}_n$ to be the affine variety in $\mathbb{A}^{n^2}_{\mathbb{K}}$ parameterizing singular matrices of size $n \times n$. Then $\mathcal{Z}_n(\mathbb{F}_q)$ is the set of $\mathbb{F}_q$-rational points of the variety $\mathcal{Z}_n$.

Lemma 1. *The variety $\mathcal{Z}_n$ defined over $\mathbb{F}_q$ is absolutely irreducible of dimension $n^2 - 1$.*

Proof. Let $X = (X_{ij})$ be an $n \times n$ matrix of n^2 variables X_{ij} over $\mathbb{K}$. Then $\mathcal{Z}_n$ is the affine variety defined by the equation $\det X = 0$. Since $\det X$ is an irreducible polynomial over $\mathbb{K}$ because it is linear in each variable, the variety is irreducible.

The fact that the dimension of the variety $\mathcal{Z}_n$ is $n^2 - 1$ is just a direct consequence of the principal ideal theorem. □

Next, let $\mathrm{Sing}\,(\mathcal{Z}_n)$ be the singular locus of $\mathcal{Z}_n$.

Lemma 2. *The variety* $\mathrm{Sing}\,(\mathcal{Z}_n)$ *defined over* $\mathbb{F}_q$ *is absolutely irreducible of dimension* $n^2 - 4$.

Proof. Let $X = (X_{ij})$ be an $n \times n$ matrix of indeterminates over $\mathbb{K}$. It follows from [1, Theorem 2.6] that the singular locus of $\mathcal{Z}_n$ is the affine variety defined by all the $(n-1)$-minors of the matrix X. In [1, Proposition 1.1], it is proved that this variety is irreducible over $\mathbb{K}$ by identifying the affine space of $n \times n$ matrices with the affine space of all $\mathbb{K}$-linear maps $f : \mathbb{K}^n \to \mathbb{K}^n$ whose coordinate ring is just the polynomial ring $\mathbb{K}[\{X_{ij}\}]$. Then $\mathrm{Sing}\,(\mathcal{Z}_n)$ is just the variety of all linear maps of rank $r < n - 1$.

The statement on the dimension of $\mathrm{Sing}\,(\mathcal{Z}_n)$ follows immediately from [1, Theorems 2.1 and 2.5]. □

2.2 Character sums over varieties

Given two matrices $U = (u_{ij}), X = (x_{ij}) \in \mathcal{M}_n(\mathbb{F}_q)$, we define their scalar products as

$$U \cdot X = \sum_{i,j=1}^{n} u_{ij} x_{ij}.$$

Let ψ be a fixed nonprincipal additive character of $\mathbb{F}_q$. For $U = (u_{ij}) \in \mathcal{M}_n(\mathbb{F}_q)$ we consider the character sums

$$S(\mathcal{Z}_n(\mathbb{F}_q), U) = \sum_{X \in \mathcal{Z}_n(\mathbb{F}_q)} \psi(U \cdot X),$$

$$S(\mathrm{SL}_n(\mathbb{F}_q), U) = \sum_{X \in \mathrm{SL}_n(\mathbb{F}_q)} \psi(U \cdot X).$$

Lemma 3. *Uniformly over all nonzero matrices* $U \in \mathcal{M}_n(\mathbb{F}_q)$, *we have*

$$S(\mathcal{Z}_n(\mathbb{F}_q), U) = O\left(q^{n^2 - 5/2}\right).$$

Proof. We recall that by Lemma 1 the variety $\mathcal{Z}_n(\mathbb{F}_q)$ is absolutely irreducible. It now follows immediately from a combination of [22, Theorem 3.2] with [22, Lemma 3.6] that

$$S(\mathcal{Z}_n(\mathbb{F}_q), U) = O\left(q^{(n^2 - 1 + s)/2}\right),$$

where s is the dimension of $\mathrm{Sing}\,(\mathcal{Z}_n(\mathbb{F}_q))$ (see, for example, the estimate of the sums $S_1(\mathcal{Y}_p, -u)$ in the proof of [22, Theorem 5.1]). It now remains to apply Lemma 2. $\square$

We also have a similar estimate for the exponential sum $S(\mathrm{SL}_n(\mathbb{F}_q), U)$.

Lemma 4. *Uniformly over all nonzero matrices $U \in \mathcal{M}_n(\mathbb{F}_q)$, we have*

$$S(\mathrm{SL}_n(\mathbb{F}_q), U) = O\left(q^{n^2-2}\right).$$

Proof. Without loss of generality, we may assume that $u_{11} \neq 0$. Let $\widetilde{X}$ be the set of all $n(n-1)$ variable x_{ij}, $1 \le i, j \le n$ with $i \neq 1$. We then have

$$\det X = \sum_{j=1}^{n} x_{1j} F_j(\widetilde{X})$$

for some polynomials $F_1, \ldots, F_n$ (in fact, each F_j depends only on $(n-1)^2$ variables, of course). Then,

$$S(\mathrm{SL}_n(\mathbb{F}_q), U) = \sum_{\widetilde{X} \in \mathbb{F}_q^{n(n-1)}} \sum_{\substack{x_{11}, \ldots, x_{1n} \in \mathbb{F}_q \\ x_{11}F_1(\widetilde{X}) + \cdots + x_{1n}F_n(\widetilde{X}) = 1}} \psi\left(U \cdot X\right), \qquad (2)$$

where the outer sum runs over all the $q^{n(n-1)}$ specialisations of $\widetilde{X}$ over $\mathbb{F}_q$.

If $\widetilde{X} \in \mathbb{F}_q^{n(n-1)}$ is fixed such that the linear forms $x_{11}F_1(\widetilde{X}) + \ldots + x_{1n}F_n(\widetilde{X})$ and $x_{11}u_{11} + \cdots + x_{1n}u_{1n}$ are linearly independent, then for each $z \in \mathbb{F}_q$ the system of two equations

$$x_{11}F_1(\widetilde{X}) + \cdots + x_{1n}F_n(\widetilde{X}) = 1 \qquad \text{and} \qquad x_{11}u_{11} + \cdots + x_{1n}u_{1n} = z$$

has exactly q^{n-2} solutions in $x_{11}, \ldots, x_{1n} \in \mathbb{F}_q$. In this case

$$\sum_{\substack{x_{11}, \ldots, x_{1n} \in \mathbb{F}_q \\ x_{11}F_1(\widetilde{X}) + \cdots + x_{1n}F_n(\widetilde{X}) = 1}} \psi\left(U \cdot X\right) = q^{n-2} \psi\left(\sum_{i=2}^{n} \sum_{j=1}^{n} u_{ij} x_{ij}\right) \sum_{z \in \mathbb{F}_q} \psi\left(z\right) = 0.$$

For $\widetilde{X} \in \mathbb{F}_q^{n(n-1)}$ such that the linear forms $x_{11}F_1(\widetilde{X}) + \cdots + x_{1n}F_n(\widetilde{X})$ and $x_{11}u_{11} + \cdots + x_{1n}u_{1n}$ are linearly dependent, we estimate the inner sum over $x_{11}, \ldots, x_{1n} \in \mathbb{F}_q$ trivially as the number of solutions to

$$x_{11}F_1(\widetilde{X}) + \cdots + x_{1n}F_n(\widetilde{X}) = 1, \qquad x_{11}, \ldots, x_{1n} \in \mathbb{F}_q,$$

which is $O(q^{n-1})$. Furthermore, if $x_{11}F_1(\widetilde{X}) + \cdots + x_{1n}F_n(\widetilde{X})$ and $x_{11}u_{11} + \cdots + x_{1n}u_{1n}$ are linearly dependent, then

$$F_1(\widetilde{X})u_{12} = F_2(\widetilde{X})u_{11}. \tag{3}$$

Since $u_{11} \neq 0$, equation (3) has at most $q^{n(n-1)-1}$ solutions $\widetilde{X}$.

Recalling (2), we conclude the proof. □

We note that Lemma 4 can be alternatively derived from [16].

Our next character sum is a matrix analogue of the classical Kloosterman sums (see [14]). Namely, for $H, U, V \in \mathcal{M}_n(\mathbb{F}_q)$, we consider the character sum

$$K(\mathrm{GL}_n(\mathbb{F}_q), U, V, H) = \sum_{X \in \mathrm{GL}_n(\mathbb{F}_q)} \psi(U \cdot X + V \cdot (HX^{-1})).$$

Lemma 5. *Uniformly over all matrices $U, V \in \mathcal{M}_n(\mathbb{F}_q)$ among which at least one is a nonzero matrix, and $H \in \mathrm{GL}_n(\mathbb{F}_q)$, we have*

$$K(\mathrm{GL}_n(\mathbb{F}_q), U, V, H) \ll q^{n^2 - 1/2}.$$

Proof. For every $\lambda \in \mathbb{F}_q^*$, the matrix λX runs through the whole group $\mathrm{GL}_n(\mathbb{F}_q)$, when so does X. Therefore,

$$\begin{aligned} K(\mathrm{GL}_n(\mathbb{F}_q), U, V, H) &= \frac{1}{q-1} \sum_{\lambda \in \mathbb{F}_q^*} \sum_{X \in \mathrm{GL}_n(\mathbb{F}_q)} \psi(U \cdot (\lambda X) + V \cdot (\lambda H X^{-1})) \\ &= \frac{1}{q-1} \sum_{X \in \mathrm{GL}_n(\mathbb{F}_q)} \sum_{\lambda \in \mathbb{F}_q^*} \psi(\lambda(U \cdot X) + \lambda^{-1}(V \cdot (HX^{-1}))). \end{aligned}$$

If both $U \cdot X$ and $V \cdot (HX^{-1})$ are nonzero elements of $\mathbb{F}_q$, then the sum over λ is a Kloosterman sum of size $O(q^{1/2})$ (see [14, Theorem 11.11]).

If only one of $U \cdot X$ and $V \cdot (HX^{-1})$ is nonzero element of $\mathbb{F}_q$, then the sum over λ is equal to -1.

Finally, if both $U \cdot X = 0$ and $V \cdot (HX^{-1}) = 0$, then the sum over λ is equal to $q-1$. However, because at least one of U or V is a nonzero matrix, this happens for at most q^{n^2-1} matrices $X \in \mathrm{GL}_n(\mathbb{F}_q)$ because $H \in \mathrm{GL}_n(\mathbb{F}_q)$. Now, after some simple calculations, we obtain the desired bound. □

3 Singular matrices in sumsets

We show that if for some fixed $\varepsilon > 0$ we have $\#\mathcal{A}\#\mathcal{B} \ge q^{2n^2-3+\varepsilon}$, then

$$N_{n,q}(\mathcal{A},\mathcal{B}) = \left(\frac{1}{q} + o(1)\right)\#\mathcal{A}\#\mathcal{B}, \tag{4}$$

as $q \to \infty$.

Theorem 6. *We have*

$$\left|N_{n,q}(\mathcal{A},\mathcal{B}) - \frac{\#\mathcal{Z}_n(\mathbb{F}_q)\#\mathcal{A}\#\mathcal{B}}{q^{n^2}}\right| = O\left(q^{n^2-5/2}\sqrt{\#\mathcal{A}\#\mathcal{B}}\right).$$

Proof. Let ψ be a nontrivial additive character of $\mathbb{F}_q$. We have

$$N_{n,q}(\mathcal{A},\mathcal{B}) = \frac{1}{q^{n^2}} \sum_{X \in \mathcal{Z}_n(\mathbb{F}_q)} \sum_{A \in \mathcal{A}} \sum_{B \in \mathcal{B}} \sum_{U \in \mathcal{M}_n(\mathbb{F}_q)} \psi\left(U \cdot (X - A - B)\right),$$

as the inner sum vanishes unless $x_{ij} = a_{ij} + b_{ij}$ for all $i, j = 1, \ldots, n$, in which case it is equal to q^{n^2}. Here we put $A = (a_{ij})$, $B = (b_{ij})$ and $X = (x_{ij})$.

We now change the order of summation by taking the summation over U outside, and then separate the term $\#\mathcal{Z}_n(\mathbb{F}_q)\#\mathcal{A}\#\mathcal{B}/q^{n^2}$ corresponding to the zero matrix $U = O_n$, getting

$$\left|N_{n,q}(\mathcal{A},\mathcal{B}) - \frac{\#\mathcal{Z}_n(\mathbb{F}_q)\#\mathcal{A}\#\mathcal{B}}{q^{n^2}}\right| = \frac{1}{q^{n^2}} \sum_{\substack{U \in \mathcal{M}_n(\mathbb{F}_q) \\ U \ne O_n}} S(\mathcal{Z}_n(\mathbb{F}_q), U) \sum_{A \in \mathcal{A}} \psi\left(-U \cdot A\right) \sum_{B \in \mathcal{B}} \psi\left(-U \cdot B\right).$$

By Lemma 3, we have

$$\begin{aligned}\left|N_{n,q}(\mathcal{A},\mathcal{B})-\frac{\#\mathcal{Z}_n(\mathbb{F}_q)\#\mathcal{A}\#\mathcal{B}}{q^{n^2}}\right| & \\ \ll q^{-5/2}\sum_{\substack{U\in\mathcal{M}_n(\mathbb{F}_q)\\ U\neq O_n}}\left|\sum_{A\in\mathcal{A}}\psi\left(-U\cdot A\right)\right|\left|\sum_{B\in\mathcal{B}}\psi\left(-U\cdot B\right)\right| & \\ \ll q^{-5/2}\sum_{\substack{U\in\mathcal{M}_n(\mathbb{F}_q)\\ U\neq O_n}}\left|\sum_{A\in\mathcal{A}}\psi\left(U\cdot A\right)\right|\left|\sum_{B\in\mathcal{B}}\psi\left(U\cdot B\right)\right|. &\end{aligned}$$

We now add the term with $U=O_n$ back and use the Cauchy inequality. This yields

$$\begin{aligned}\sum_{\substack{U\in\mathcal{M}_n(\mathbb{F}_q)\\ U\neq O_n}}\left|\sum_{A\in\mathcal{A}}\psi\left(U\cdot A\right)\right|\left|\sum_{B\in\mathcal{B}}\psi\left(U\cdot B\right)\right| & \\ \leq\sum_{U\in\mathcal{M}_n(\mathbb{F}_q)}\left|\sum_{A\in\mathcal{A}}\psi\left(U\cdot A\right)\right|\left|\sum_{B\in\mathcal{B}}\psi\left(U\cdot B\right)\right| & \\ \leq\sqrt{\sum_{U\in\mathcal{M}_n(\mathbb{F}_q)}\left|\sum_{A\in\mathcal{A}}\psi\left(U\cdot A\right)\right|^2}\sqrt{\sum_{U\in\mathcal{M}_n(\mathbb{F}_q)}\left|\sum_{B\in\mathcal{B}}\psi\left(U\cdot B\right)\right|^2}. &\end{aligned}$$

We now remark that

$$\begin{aligned}\sum_{U\in\mathcal{M}_n(\mathbb{F}_q)}\left|\sum_{A\in\mathcal{A}}\psi\left(U\cdot A\right)\right|^2 &= q^{n^2}\#\mathcal{A},\\ \sum_{U\in\mathcal{M}_n(\mathbb{F}_q)}\left|\sum_{B\in\mathcal{B}}\psi\left(U\cdot B\right)\right|^2 &= q^{n^2}\#\mathcal{B},\end{aligned}$$

which are just variants of the Parseval identity.

Collecting everything, we obtain the result. □

Using the fact that $\#\mathcal{Z}_n(\mathbb{F}_q) = q^{n^2-1} + O\left(q^{n^2-2}\right)$, which follows, from the well-known formula

$$\#\mathrm{GL}_n(\mathbb{F}_q) = q^{(n^2-n)/2}\prod_{j=1}^{n}(q^j-1) = q^{n^2} - q^{n^2-1} + O\left(q^{n^2-2}\right)$$

(see [7, Theorem 99]), we see that Theorem 6 implies (4). Furthermore, following the argument of the proof of Theorem 6, but using Lemma 4 instead of Lemma 3 in the appropriate place, we obtain the following statement.

Theorem 7. *We have*

$$\left|T_{n,q}(\mathcal{A},\mathcal{B}) - \frac{\#\mathrm{SL}_n(\mathbb{F}_q)\#\mathcal{A}\#\mathcal{B}}{q^{n^2}}\right| = O\left(q^{n^2-2}\sqrt{\#\mathcal{A}\#\mathcal{B}}\right).$$

In particular, we derive from Theorem 7 that if for some fixed $\varepsilon > 0$ we have $\#\mathcal{A}\#\mathcal{B} \ge q^{2n^2-2+\varepsilon}$, then

$$T_{n,q}(\mathcal{A},\mathcal{B}) = \left(\frac{1}{q} + o(1)\right)\#\mathcal{A}\#\mathcal{B},$$

as $q \to \infty$.

4 Generating $\mathrm{GL}_n(\mathbb{F}_q)$ by sumset products

Here, we show that if the sets $\mathcal{A},\mathcal{B},\mathcal{C},\mathcal{D} \subseteq \mathcal{M}_n(\mathbb{F}_q)$ are large enough then the sumset products

$$\{(A+B)(C+D) \ : \ A \in \mathcal{A}, B \in \mathcal{B}, C \in \mathcal{C}, D \in \mathcal{D}\}$$

generate the whole group $\mathrm{GL}_n(\mathbb{F}_q)$.

In fact, we give an asymptotic formula for $R(\mathcal{A},\mathcal{B},\mathcal{C},\mathcal{D};H)$, which is the number of solutions to the equation

$$H = (A+B)(C+D), \qquad A \in \mathcal{A}, B \in \mathcal{B}, C \in \mathcal{C}, D \in \mathcal{D}.$$

Theorem 8. *Uniformly over all matrices $H \in \mathrm{GL}_n(\mathbb{F}_q)$, we have*

$$R(\mathcal{A},\mathcal{B},\mathcal{C},\mathcal{D};H) = \frac{1}{q^{n^2}}\#\mathcal{A}\#\mathcal{B}\#\mathcal{C}\#\mathcal{D} + O\left(q^{n^2-1/2}\sqrt{\#\mathcal{A}\#\mathcal{B}\#\mathcal{C}\#\mathcal{D}}\right).$$

Proof. Clearly $R(\mathcal{A},\mathcal{B},\mathcal{C},\mathcal{D};H)$ is equal to the number of solutions to the system of equations

$$A+B=X, \qquad C+D=HX^{-1},$$

where $A\in\mathcal{A}$, $B\in\mathcal{B}$, $C\in\mathcal{C}$, $D\in\mathcal{D}$ and $X\in \mathrm{GL}_n(\mathbb{F}_q)$.

Using the orthogonality property of characters, we now write

$$\begin{aligned}
&R(\mathcal{A},\mathcal{B},\mathcal{C},\mathcal{D};H)\\
&\quad=\sum_{A\in\mathcal{A}}\sum_{B\in\mathcal{B}}\sum_{C\in\mathcal{C}}\sum_{D\in\mathcal{D}}\sum_{X\in\mathrm{GL}_n(\mathbb{F}_q)}\\
&\qquad\frac{1}{q^{2n^2}}\sum_{U,V\in\mathcal{M}_n(\mathbb{F}_q)}\psi(U\cdot(X-A-B)+V\cdot(HX^{-1}-C-D))\\
&\quad=\frac{1}{q^{2n^2}}\sum_{U,V\in\mathcal{M}_n(\mathbb{F}_q)}K(\mathrm{GL}_n(\mathbb{F}_q),U,V,H)\\
&\qquad\sum_{A\in\mathcal{A}}\psi(-U\cdot A)\sum_{B\in\mathcal{B}}\psi(-U\cdot B)\sum_{C\in\mathcal{C}}\psi(-V\cdot C)\sum_{D\in\mathcal{D}}\psi(-V\cdot D).
\end{aligned}$$

Separating the contribution of the zero matrices $U=V=O_n$, we obtain

$$\begin{aligned}
&R(\mathcal{A},\mathcal{B},\mathcal{C},\mathcal{D};H)-\frac{1}{q^{2n^2}}\#\mathcal{A}\#\mathcal{B}\#\mathcal{C}\#\mathcal{D}\#\mathrm{GL}_n(\mathbb{F}_q)\\
&\quad=\frac{1}{q^{2n^2}}\sum_{\substack{U,V\in\mathcal{M}_n(\mathbb{F}_q)\\ U\neq O_n \text{ or } V\neq O_n}}K(\mathrm{GL}_n(\mathbb{F}_q),U,V,H)\\
&\qquad\sum_{A\in\mathcal{A}}\psi(-U\cdot A)\sum_{B\in\mathcal{B}}\psi(-U\cdot B)\sum_{C\in\mathcal{C}}\psi(-V\cdot C)\sum_{D\in\mathcal{D}}\psi(-V\cdot D).
\end{aligned}$$

Therefore, by Lemma 5, we have

$$\begin{aligned}
&\left|R(\mathcal{A},\mathcal{B},\mathcal{C},\mathcal{D};H)-\frac{1}{q^{2n^2}}\#\mathcal{A}\#\mathcal{B}\#\mathcal{C}\#\mathcal{D}\#\mathrm{GL}_n(\mathbb{F}_q)\right| \\
&\qquad=\frac{1}{q^{n^2-1/2}}\sum_{\substack{U,V\in\mathcal{M}_n(\mathbb{F}_q)\\ U\neq O_n \text{ or } V\neq O_n}}\left|\sum_{A\in\mathcal{A}}\psi\left(-U\cdot A\right)\right|\left|\sum_{B\in\mathcal{B}}\psi\left(-U\cdot B\right)\right| \\
&\qquad\qquad\qquad\left|\sum_{C\in\mathcal{C}}\psi\left(-V\cdot C\right)\right|\left|\sum_{D\in\mathcal{D}}\psi\left(-V\cdot D\right)\right| \\
&\qquad\leq\frac{1}{q^{n^2-1/2}}\sum_{U,V\in\mathcal{M}_n(\mathbb{F}_q)}\left|\sum_{A\in\mathcal{A}}\psi\left(U\cdot A\right)\right|\left|\sum_{B\in\mathcal{B}}\psi\left(U\cdot B\right)\right| \\
&\qquad\qquad\qquad\left|\sum_{C\in\mathcal{C}}\psi\left(V\cdot C\right)\right|\left|\sum_{D\in\mathcal{D}}\psi\left(V\cdot D\right)\right| \\
&\qquad=\frac{1}{q^{n^2-1/2}}\sum_{U\in\mathcal{M}_n(\mathbb{F}_q)}\left|\sum_{A\in\mathcal{A}}\psi\left(U\cdot A\right)\right|\left|\sum_{B\in\mathcal{B}}\psi\left(U\cdot B\right)\right| \\
&\qquad\qquad\qquad\sum_{V\in\mathcal{M}_n(\mathbb{F}_q)}\left|\sum_{C\in\mathcal{C}}\psi\left(V\cdot C\right)\right|\left|\sum_{D\in\mathcal{D}}\psi\left(V\cdot D\right)\right|.
\end{aligned}$$

We apply the Cauchy inequality to each of the sums over U and V and, as in the proof of Theorem 6, estimate them as $q^{n^2}\sqrt{\#\mathcal{A}\#\mathcal{B}}$ and $q^{n^2}\sqrt{\#\mathcal{C}\#\mathcal{D}}$, respectively. We thus obtain

$$\begin{aligned}
&\left|R(\mathcal{A},\mathcal{B},\mathcal{C},\mathcal{D};H)-\frac{1}{q^{2n^2}}\#\mathcal{A}\#\mathcal{B}\#\mathcal{C}\#\mathcal{D}\#\mathrm{GL}_n(\mathbb{F}_q)\right| \\
&\qquad\qquad\ll q^{n^2-1/2}\sqrt{\#\mathcal{A}\#\mathcal{B}\#\mathcal{C}\#\mathcal{D}}.
\end{aligned}$$

Using that $\#\mathrm{GL}_n(\mathbb{F}_q)=q^{n^2}+O\left(q^{n^2-1}\right)$, we obtain

$$\begin{aligned}
&\left|R(\mathcal{A},\mathcal{B},\mathcal{C},\mathcal{D};H)-\frac{1}{q^{n^2}}\#\mathcal{A}\#\mathcal{B}\#\mathcal{C}\#\mathcal{D}\right| \\
&\qquad\ll q^{-n^2-1}\#\mathcal{A}\#\mathcal{B}\#\mathcal{C}\#\mathcal{D}+q^{n^2-1/2}\sqrt{\#\mathcal{A}\#\mathcal{B}\#\mathcal{C}\#\mathcal{D}}.
\end{aligned}$$

Clearly, the first term never dominates and the result now follows. □

We see from Theorem 8 that if for some fixed $\varepsilon > 0$ we have

$$\#\mathcal{A}\#\mathcal{B}\#\mathcal{C}\#\mathcal{D} \ge q^{4n^2-1+\varepsilon},$$

then uniformly over $H \in \mathrm{GL}_n(\mathbb{F}_q)$,

$$R(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}; H) = \left(\frac{1}{q^{n^2}} + o(1)\right) \#\mathcal{A}\#\mathcal{B}\#\mathcal{C}\#\mathcal{D},$$

as $q \to \infty$. We also see that $R(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}; H) > 0$ under the condition (1) with some appropriate constant $c(n)$.

5 Prime divisors of sumset determinants

Given a set $\mathcal{T}$ of integers, we denote by

$$\mathcal{M}_n(\mathcal{T}) = \{T = (t_{ij}) \in \mathcal{M}_n(\mathbb{Z}) \ : \ t_{ij} \in \mathcal{T}, \ 1 \le i, j \le n\}$$

the set of all $n \times n$ matrices with entries from $\mathcal{T}$.

We now use our previous results to obtain a lower bound on the number of distinct prime divisors of the product

$$W(\mathcal{R}, \mathcal{S}) = \prod_{A \in \mathcal{M}_n(\mathcal{R})} \prod_{B \in \mathcal{M}_n(\mathcal{S})} \det(A + B),$$

where the sets $\mathcal{R}, \mathcal{S} \subseteq \{1, \ldots, N\}$ are dense enough and N is a sufficiently large integer.

Given a prime p and a set $\mathcal{S}$ of integers, we denote by $\nu_p(S)$ the number of residue classes modulo p which contain at least one element of $\mathcal{S}$.

We need the following statement which shows that $\nu_p(\mathcal{S})$ is large for sufficiently many primes. It is a simple variant of several other results of this type (see, for example, [6, 10]).

Lemma 9. *Let N and Q be sufficiently large positive integers. Let $\mathcal{T} \subseteq \{1, \ldots, N\}$ be of cardinality $\#\mathcal{T} = T$. If $Q \le T \log N$, then for at least $0.6Q/\log Q$ primes $p \in [Q, 2Q]$ we have*

$$\nu_p(\mathcal{T}) \ge \frac{p}{20 \log N \log p}.$$

Proof. Let $\mu_{u,p}(\mathcal{T})$ be the number of $t \in \mathcal{T}$ with $t \equiv u \pmod{p}$.

By the Cauchy inequality, we have

$$T = \sum_{u=0}^{p-1} \mu_{u,p}(\mathcal{T}) = \sum_{\substack{u=0 \\ \mu_{u,p}(\mathcal{T}) \neq 0}}^{p-1} \mu_{u,p}(\mathcal{T}) \leq \sqrt{\nu_p(S)\sigma_p(\mathcal{T})}, \tag{5}$$

where

$$\sigma_p(\mathcal{T}) = \sum_{u=0}^{p-1} \mu_{u,p}(\mathcal{T})^2.$$

We now consider the product

$$W = \prod_{\substack{t_1,t_2 \in \mathcal{T} \\ t_1 \neq t_2}} (t_1 - t_2)\,.$$

Clearly,

$$1 \leq |W| \leq N^{T(T-1)}. \tag{6}$$

Let $\operatorname{ord}_p z$ denote the exponent of the prime p in the factorization of the integer z. Collecting together pairs s, t in the same residue class u modulo p, we see that

$$\operatorname{ord}_p W \geq \sum_{u=0}^{p-1} \mu_{u,p}(\mathcal{T})\left(\mu_{u,p}(\mathcal{T}) - 1\right) = \sigma_p(\mathcal{T}) - T.$$

Therefore, using the fact that the number of primes $p \in [Q, 2Q]$ is at most $2Q/\log Q$ for large values of Q, which follows from the Prime Number Theorem, we get that

$$|W| = \sum_p p^{\operatorname{ord}_p W} \geq \prod_{p \in [Q,2Q]} Q^{\operatorname{ord}_p W} = Q^{-2QT/\log Q} \prod_{p \in [Q,2Q]} Q^{\sigma_p(\mathcal{T})}, \tag{7}$$

that provided Q is large enough.

Comparing (6) with (7) and recalling that $Q \leq T \log N$, we obtain

$$\sum_{p \in [Q,2Q]} \sigma_p(\mathcal{T}) \leq T^2 \log N + 2QT \leq 3T^2 \log N. \tag{8}$$

Thus,

$$\# \left\{ p \in [Q, 2Q] \ : \ \sigma_p(\mathcal{T}) \geq \frac{10T^2 \log N \log Q}{Q} \right\} \leq \frac{3Q}{10 \log Q}.$$

For the remaining primes $p \in [Q, 2Q]$, the number of which, by the Prime Number Theorem, is at least

$$\left(1 - \frac{3}{10} + o(1)\right) \frac{Q}{\log Q} \geq 0.6 \frac{Q}{\log Q}$$

for large enough Q, we derive from (5) that

$$\nu_p(\mathcal{T}) \geq \frac{Q}{10 \log N \log Q} \geq \frac{p}{20 \log p},$$

which concludes the proof. □

For the purpose of the next result, for a nonzero integer m we write $\omega(m)$ for the number of its distinct prime factors.

Theorem 10. *There exists a positive constant $c_0(n)$ depending only on n such that if $\mathcal{A}$, $\mathcal{B}$ are subsets of $\{1, \ldots, N\}$ with*

$$\min\{\#\mathcal{A}, \#\mathcal{B}\} > c_0(n) (\log N)^{2n^2/3 - 1} (\log \log N)^{2n^2/3}$$

and N is sufficiently large, then

$$\omega(W(\mathcal{A}, \mathcal{B})) \gg \min\{\#\mathcal{A}, \#\mathcal{B}\}.$$

Proof. We apply Lemma 9 with

$$T = \min\{\#\mathcal{A}, \#\mathcal{B}\} \qquad \text{and} \qquad Q = \lfloor T \log N \rfloor,$$

getting that for large Q there are are at least

$$(0.2 + o(1)) \frac{Q}{\log Q} \geq 0.1 \frac{Q}{\log Q}$$

primes $p \in [Q, 2Q]$ for which both inequalities

$$\nu_p(\mathcal{A}) \geq \frac{p}{10 \log N \log Q} \qquad \text{and} \qquad \nu_p(\mathcal{B}) \geq \frac{p}{10 \log N \log Q}$$

hold. Since obviously $T \le N$, we have

$$\frac{Q}{\log Q} \gg T$$

such primes. From Theorem 6, we see that

$$p \mid W(\mathcal{A}, \mathcal{B})$$

provided that

$$(10 \log N \log Q)^{2n^2} \le c_1(n) Q^3$$

for an appropriate positive constant $c_1(n)$ depending only n. The above inequality is satisfied if

$$(\log N \log T)^{2n^2/3} \le c_2(n) T \log N$$

for an appropriate constant $c_2(n)$, and this in turn is implied by the condition of the theorem with a sufficiently large $c_0(n)$. □

Acknowledgements

The authors are grateful to Tony Shaska for the invitation to NATO Advanced Study Institute "New Challenges in Digital Communications", Vlora, 2008. The stimulating atmosphere of this meeting, enhanced by Albanian food and wine has led to the idea of this work.

The authors would also like to thank Alexei Skorobogatov for many valuable discussions and clarifications of some results of [22].

During the preparation of this paper, F. L. was supported in part by Grant SEP-CONACyT 79685 and PAPIIT 100508, and I. S. by ARC Grant DP0556431.

References

[1] W. Bruns and U. Vetter, *Determinantal rings*, Graduate Texts in Mathematics, **1327**, Springer-Verlag, 1988.

[2] J. Bourgain and A. Gamburd, 'On the spectral gap for finitely-generated subgroups of SU(2)', *Invent. Math.*, **171** (2008), 83–121.

[3] M.-C. Chang, 'Additive and multiplicative structure in matrix spaces', *Combin. Probab. Comput.*, **16** (2007), 219–238.

[4] M.-C. Chang, 'Product theorems in SL_2 and SL_3', *J. Inst. Math. Jussieu.*, **7** (2008), 1–25.

[5] D. Covert, D. Hart, A. Iosevich, D. Koh and M. Rudnev, 'Generalized incidence theorems, homogeneous forms and sum-product estimates in finite fields', *Eur. J. Comb.* **31** (2010), 306–319.

[6] E. S. Croot and C. Elsholtz, 'On variants of the larger sieve', *Acta Math. Hung.*, **103** (2004), 243–254.

[7] L. E. Dickson, *Linear groups: With an exposition of the Galois field theory*, Dover Publ. Inc., New York, 1958.

[8] É. Fouvry, 'Consequences of a result of N. Katz and G. Laumon concerning trigonometric sums', *Israel J. Math.*, **120** (2000), 81–96.

[9] É. Fouvry and N. Katz, 'A general stratification theorem for exponential sums, and applications', *J. Reine Angew. Math.*, **540** (2001), 115–166.

[10] P. X. Gallagher, 'A larger sieve', *Acta Arith.*, **18** (1971), 77–81.

[11] D. Hart, A. Iosevich and J. Solymosi, 'Sums and products in finite fields via Kloosterman Sums', *Intern. Math. Res. Notices*, **2007** (2007), Article ID rnm007, 1–14.

[12] H. A. Helfgott, 'Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$', *Ann. of Math.*, **167** (2008), 601–623.

[13] H. A. Helfgott, 'Growth in $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$', *J. Eur. Math. Soc.*, to appear.

[14] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[15] N. Katz, 'Estimates for "singular" exponential sums', *International Mathematics Research Notices*, **16** (1999), 875–899.

[16] E. Kowalski, 'Exponential sums over definable subsets of finite fields', *Israel J. Math.*, **160** (2007), 219–251.

[17] G. Laumon, 'Exponential sums and l-adic cohomology: A survey', *Israel J. Math.*, **120** (2000), 225–257.

[18] W. Luo, 'Rational points on complete intersections over $\mathbb{F}_p$', *Internat. Math. Res. Notices*, **999** (1999), 901–907.

[19] C. J. Moreno and O. Moreno, 'Exponential sums and Goppa codes, 1', *Proc. Amer. Math. Soc.*, **111** (1991), 523–531.

[20] A. Rittatore and W. F. Santos, *Actions and invariants of algebraic groups*, Monographs and Textbooks in Pure and Applied Mathematics, vol. 269, Chapman & Hall/CRC, 2005.

[21] I. E. Shparlinski and A. N. Skorobogatov, 'Exponential sums and rational points on complete intersections', *Mathematika*, **37** (1990), 201–208.

[22] A. N. Skorobogatov, 'Exponential sums, the geometry of hyperplane sections, and some Diophantine problems', *Israel J. Math.*, **80** (1992), 359–379.

[23] T. Tao and V. Vu, *Additive combinatorics*, Cambridge Univ. Press, Cambridge, 2006.