Canad. Math. Bull. Vol. **64** (4), 2023, pp. 1280–1295
http://dx.doi.org/10.4153/S000843952300036X

An energy decomposition theorem for matrices and related questions

Ali Mohammadi, Thang Pham, and Yiting Wang

Abstract. Given $A \subseteq GL_2(\mathbb{F}_q)$, we prove that there exist disjoint subsets $B, C \subseteq A$ such that $A = B \sqcup C$ and their additive and multiplicative energies satisfying

$$\max\{\, E_+(B),\, E_\times(C)\,\} \ll \frac{|A|^3}{M(|A|)},$$

where

$$M(|A|) = \min\left\{ \frac{q^{4/3}}{|A|^{1/3}(\log|A|)^{2/3}},\, \frac{|A|^{4/5}}{q^{13/5}(\log|A|)^{27/10}} \right\}.$$

We also study some related questions on moderate expanders over matrix rings, namely, for $A, B, C \subseteq GL_2(\mathbb{F}_q)$, we have

$$|AB + C|,\ |(A+B)C| \gg q^4,$$

whenever $|A||B||C| \gg q^{10+1/2}$. These improve earlier results due to Karabulut, Koh, Pham, Shen, and Vinh ([2019], Expanding phenomena over matrix rings, *ForumMath.*, 31, 951–970).

1 Introduction

Let $\mathbb{F}_q$ denote a finite field of order q and characteristic p, and let $M_2(\mathbb{F}_q)$ be the set of two-by-two matrices with entries in $\mathbb{F}_q$. We write $X \ll Y$ to mean $X \leq CY$ for some absolute constant $C > 0$ and use $X \sim Y$ if $Y \ll X \ll Y$.

Given subsets $A, B \subseteq M_2(\mathbb{F}_q)$, we define the sum set $A + B$ to be the set $\{a + b : (a, b) \in A \times B\}$ and similarly define the product set AB. In this paper, we study various questions closely related to the sum-product problem over $M_2(\mathbb{F}_q)$, which is to determine nontrivial lower bounds on the quantity $\max\{\,|A + A|,\, |AA|\,\}$, under natural conditions on sets $A \subseteq M_2(\mathbb{F}_q)$.

A result in this direction was proved by Karabulut et al. in [4, Theorem 1.12], showing that if $A \subseteq M_2(\mathbb{F}_q)$ satisfies $|A| \gg q^3$ then

$$\max\{\,|A + A|,\, |AA|\,\} \gg \min\left\{ \frac{|A|^2}{q^{7/2}},\, q^2|A|^{1/2} \right\}. \tag{1.1}$$

Received by the editors October 20, 2022; revised May 3, 2023; accepted May 3, 2023.
Published online on Cambridge Core May 15, 2023.
AMS subject classification: **11T06**, 15B33.
Keywords: Matrix rings, expanders, sum-product estimates, energy estimates, finite fields.

A closely related quantity is the additive energy $E_+(A,B)$ defined as the number of quadruples $(a,a',b,b')\in A^2\times B^2$ such that $a+b=a'+b'$. The multiplicative energy $E_\times(A,B)$ is defined in a similar manner. We also use, for example, $E_+(A)=E_+(A,A)$. For $\lambda\in M_2(\mathbb{F}_q)$, we define the representation function $r_{AB}(\lambda)=|\{(a,b)\in A\times B: ab=\lambda\}|$. Note that r_{AB} is supported on the set AB and so we have the identities

$$\sum_{\lambda\in AB} r_{AB}(\lambda)=|A||B| \quad \text{and} \quad \sum_{\lambda\in AB} r_{AB}(\lambda)^2=E_\times(A,B). \tag{1.2}$$

A standard application of the Cauchy–Schwarz inequality gives

$$|A+B|\geq \frac{|A|^2|B|^2}{E_+(A,B)},\ |AB|\geq \frac{|A|^2|B|^2}{E_\times(A,B)}. \tag{1.3}$$

Thus, if either $E_+(A,B)$ or $E_\times(A,B)$ is small, then $\max(|A+B|,|AB|)$ is big. This motivates the study of energy estimates.

Balog and Wooley [2] initiated the investigation into a type of energy variant of the sum-product problem by proving that given a finite set $A\subset\mathbb{R}$, one may write $A=B\sqcup C$ such that $\max\{E_+(B),E_\times(C)\}\ll|A|^{3-\delta}(\log|A|)^{1-\delta}$ for $\delta=2/33$. In the prime field setting, they also provided similar results, namely:

(1) If $|A|\leq p^{\frac{101}{161}}(\log p)^{\frac{71}{161}}$, then

$$\max\{E_+(B),E_\times(C)\}\ll|A|^{3-\delta}(\log|A|)^{1-\delta/2},\quad \delta=4/101.$$

(2) If $|A|>p^{\frac{101}{161}}(\log p)^{\frac{71}{161}}$, then

$$\max\{E_+(B),E_\times(C)\}\ll|A|^3(|A|/p)^{1/15}(\log|A|)^{14/15}.$$

These results have been improved by Rudnev, Shkredov, and Stevens in [10]. In particular, they increased δ from $2/33$ to $1/4$ over the reals, and from $4/101$ to $1/5$ over prime fields. We note that this type of result has many applications in different areas, for instance, bounding exponential sums [5, 8, 12–15] or studying structures in Heisenberg groups [1, 3].

The main goals of this paper are to study energy variants of the sum-product problem, and to obtain new exponents on two moderate expanding functions in the matrix ring $M_2(\mathbb{F}_q)$. While the results in [2, 10] mainly relies on a number of earlier results on the sum-product problem or Rudnev's point–plane incidence bound [9], our proofs rely on graph theoretic methods. It follows from our results in the next section that there exists a different phenomenon between problems over finite fields and over the matrix ring $M_2(\mathbb{F}_q)$.

2 Main results

Our first theorem is on an energy decomposition of a set of matrices in $M_2(\mathbb{F}_q)$.

Theorem 2.1 *Given $A\subseteq GL_2(\mathbb{F}_q)$, there exist disjoint subsets $B,C\subseteq A$ such that $A=B\sqcup C$ and*

$$\max\{E_+(B),E_\times(C)\}\ll\frac{|A|^3}{M(|A|)},$$

where

$$M(|A|) = \min\left\{ \frac{q^{4/3}}{|A|^{1/3}(\log|A|)^{2/3}}, \frac{|A|^{4/5}}{q^{13/5}(\log|A|)^{27/10}} \right\}. \tag{2.1}$$

It follows from this theorem that for any set A of matrices in $M_2(\mathbb{F}_q)$, we always can find a subset with either small additive energy or small multiplicative energy. By the Cauchy–Schwarz inequality, we have the following direct consequence on a sum-product estimate, namely, for $A \subseteq GL_2(\mathbb{F}_q)$, we have

$$\max\{|A+A|, |AA|\} \gg |A| \cdot M(|A|). \tag{2.2}$$

By a direct computation, one can check that this is better than the estimate (1.1) in the range $|A| \ll q^{3+5/8}/(\log|A|)^{1/2}$.

In the next theorem, we show that the lower bound of (2.2) can be improved by a direct energy estimate.

Theorem 2.2 *Let $A, B \subseteq M_2(\mathbb{F}_q)$ and $C \subseteq GL_2(\mathbb{F}_q)$. Then*

$$E_+(A,B) \ll \frac{|A|^2|BC|^2}{q^4} + q^{13/2}\frac{|A||BC|}{|C|}.$$

Corollary 2.3 *For $A \subseteq M_2(\mathbb{F}_q)$, with $|A| \gg q^3$, we have*

$$\max\{\,|A+A|,\ |AA|\,\} \gg \min\left\{ \frac{|A|^2}{q^{13/4}}, q^{4/3}|A|^{2/3} \right\}. \tag{2.3}$$

In addition, if $|AA| \ll |A|$ and $|A| \gg q^{3+1/2}$, then

$$|A+A| \gg q^4. \tag{2.4}$$

If $|AA| \ll |A|$ and $|A| \gg q^{3+2/5}$, then

$$|A+A+A| \gg q^4. \tag{2.5}$$

We point out that the arguments of the proof of Corollary 2.3 could be used iteratively to give stronger results for expansion of k-fold sum sets $A + \cdots + A$ of sets $A \subseteq M_2(F_q)$ with $|AA| \ll |A|$, as k gets larger.

We remark that the estimate (2.3) improves (1.1) in the range $|A| \ll q^{3+5/8}$ and is stronger than (2.2) in the range of $|A| \gg q^{13/4}$. We also note that our assumption to get the estimate (2.4) is reasonable. For instance, let G be a subgroup of $\mathbb{F}_q^*$, and let A be the set of matrices with determinants in G, then we have $|A| \sim q^3 \cdot |G|$ and $|AA| = |A|$.

It has been proved in [4, Theorems 1.8 and 1.9] that for $A, B, C \subseteq M_2(\mathbb{F}_q)$, if $|A||B||C| \geq q^{11}$, then we have

$$|AB+C|,\ |(A+B)C| \gg q^4.$$

In the following theorem, we provide improvements of these results.

https://doi.org/10.4153/S000843952300036X Published online by Cambridge University Press

Theorem 2.4 *Let $A, B, C \subseteq M_2(\mathbb{F}_q)$, we have*

$$|AB + C| \gg \min\left\{ q^4, \frac{|A||B||C|}{q^{13/2}} \right\}.$$

If $C \subseteq GL_2(\mathbb{F}_q)$, the same conclusion holds for $(A + B)C$, i.e.,

$$|(A + B)C| \gg \min\left\{ q^4, \frac{|A||B||C|}{q^{13/2}} \right\}.$$

In particular:

(1) *If $|A||B||C| \gg q^{10+1/2}$, then $|AB + C| \gg q^4$.*
(2) *If $|A||B||C| \gg q^{10+1/2}$ and $C \subseteq GL_2(\mathbb{F}_q)$, then $|(A + B)C| \gg q^4$.*

The condition $C \subseteq GL_2(\mathbb{F}_q)$ is necessary, since, for instance, one can take C being the set of matrices with zero determinant and $A = B = M_2(\mathbb{F}_q)$, then $|(A + B)C| \sim q^3$ and $|A||B||C| \sim q^{11}$.

We expect that the exponent $q^{10+1/2}$, in the final conclusions of the above theorem, could be further improved to q^{10}, which, as we shall demonstrate, is sharp. For $AB + C$, let A and B be the set of lower triangular matrices in $M_2(\mathbb{F}_q)$ and for arbitrary $0 < \delta < 1$, let $X \subseteq \mathbb{F}_q$ be any set with $|X| = q^{1-\delta}$, and let

$$C = \left\{ \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} : c_1, c_3, c_4 \in \mathbb{F}_q, c_2 \in X \right\}.$$

Then $|A||B||C| = q^{10-\delta}$ and $|AB + C| = |C| = q^{4-\delta}$.

For $(A + B)C$, the construction is as follows: For arbitrary k, let $q = p^k$, and let V be the set of elements corresponding to a $(k - 1)$-dimensional vector space over $\mathbb{F}_p$ in $\mathbb{F}_q$. Thus, we have $|V| = p^{k-1} = q^{1-1/k}$. Now, let

$$A = B = \left\{ \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} : x_1, x_2 \in V, x_3, x_4 \in \mathbb{F}_q \right\},$$

and

$$C = \left\{ \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} : c_1, c_3 \in \mathbb{F}_q, c_2, c_4 \in \mathbb{F}_p \right\}.$$

Note that $A + B = A = B$ and so

$$(A + B)C = AC = \left\{ \begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix} : y_1, y_3, y_4 \in \mathbb{F}_q, y_2 \in V \right\},$$

where we have used that $V \cdot \mathbb{F}_p + V \cdot \mathbb{F}_p = V + V = V$.

Thus, $|A||B||C| = (q^2 \cdot q^{2-2/k})^2 \cdot (q^2 \cdot q^{2/k}) = q^{10-2/k}$ while $|(A + B)C| = q^{4-1/k}$.

Also, we remark here that in the setting of finite fields, our approach and that of Karabulut et al. in [4] imply the same result. Namely, for $A, B, C \subseteq \mathbb{F}_q$, we have $|(A + B)C|, |AB + C| \gg q$ whenever $|A||B||C| \gg q^2$. However, this is not true in the matrix ring. Let us briefly sketch the proof. For $\lambda \in AB + C$, write

$$t(\lambda) = |\{ (a, b, c) \in A \times B \times C : ab + c = \lambda \}|.$$

https://doi.org/10.4153/S000843952300036X Published online by Cambridge University Press

By the Cauchy–Schwarz inequality, we have

$$(|A||B||C|)^2 = \left(\sum_{\lambda \in AB+C} t(\lambda)\right)^2 \leq |AB+C| \sum_{\lambda \in AB+C} t(\lambda)^2.$$

Thus, the main task is to bound $\sum_\lambda t(\lambda)^2$, i.e., the number of tuples $(a,b,c,a',b',c') \in (A \times B \times C)^2$ such that $ab + c = a'b' + c'$. In [4], instead of bounding $\sum_\lambda t(\lambda)^2$, they bounded the number of quadruples $(a,b,c,\lambda) \in A \times B \times C \times (AB+C)$ such that $ab + c = \lambda$. These two approaches imply the same lower bounds for $(A+B)C$ and $AB+C$ when $A,B,C \subset \mathbb{F}_q$, but in the matrix rings, bounding $\sum_\lambda t(\lambda)^2$ is more effective. In other words, there exists a different phenomenon between problems over finite fields and over the matrix ring $M_2(\mathbb{F}_q)$.

We now state a corollary of the above theorem with $C = AA$ which might be of independent interest.

Corollary 2.5 *Let $A \subset M_2(\mathbb{F}_q)$ with $|A| \gg q^{3+7/16}$, then*

$$\max\{|AA(A+A)|, |AA+A+A|\} \gg q^4.$$

Let $A,B,C,D \subseteq M_2(\mathbb{F}_q)$, our last theorem is devoted for the solvability of the equation

$$x + y = zt, \quad (x,y,z,t) \in A \times B \times C \times D. \tag{2.6}$$

Let $\mathcal{J}(A,B,C,D)$ denote the number of solutions to this equation.

One can check that by using Lemma 4.1 and Theorem 4.2 from [4], one has

$$\left|\mathcal{J}(A,B,C,D) - \frac{|A||B||C||D|}{q^4}\right| \ll q^{7/2}(|A||B||C||D|)^{1/2}. \tag{2.7}$$

Thus, when $|A||B||C||D| \gg q^{15}$, then $\mathcal{J}(A,B,C,D) \sim \frac{|A||B||C||D|}{q^4}$. We refer the interested reader to [11] for a result on this problem over finite fields. In our last theorem, we are interested in bounding $\mathcal{J}(A,B,C,D)$ from above when $|A||B||C||D|$ is smaller.

Theorem 2.6 *Let $A,B,C,D \subseteq M_2(\mathbb{F}_q)$, and let $\mathcal{J}(A,B,C,D)$ denote the number of solutions to equation (2.6). Then, we have*

$$\mathcal{J}(A,B,C,D) \ll \frac{|A||B|^{1/2}|C||D|}{q^2} + q^{13/4}(|A||B||C||D|)^{1/2}.$$

Assume $|A| = |B| = |C| = |D|$, the upper bound of this theorem is stronger than that of (2.7) when $|A| \ll q^{11/3}$.

2.1 Structure

The rest of this paper is structured as follows: In Section 3, we prove a preliminary lemma, which is one of the key ingredients in the proof of our energy decomposition theorem. Section 4 is devoted to proving Theorem 2.1. The proofs of Theorem 2.2 and

Corollary 2.3 will be presented in Section 5. Section 6 contains proofs of Theorem 2.4, Corollary 2.5, and Theorem 2.6.

3 A preliminary lemma

Given sets $A, B, C, D, E, F \subseteq M_2(\mathbb{F}_q)$, let $\mathcal{I}(A, B, C, D, E, F)$ be the number of solutions

$$(a, e, c, b, f, d) \in A \times B \times C \times D \times E \times F: \quad ab + ef = c + d.$$

The main purpose of this section is to prove an estimate for $\mathcal{I}(A, B, C, D, E, F)$, which is one of the key ingredients in the proof of Theorem 2.1.

Proposition 3.1 *We have*

$$\left|\mathcal{I}(A, B, C, D, E, F) - \frac{|A||B||C||D||E||F|}{q^4}\right| \ll q^{13/2}\sqrt{|A||B||C||D||E||F|}.$$

To prove Proposition 3.1, we define the sum-product digraph $G = (V, E)$ with the vertex set $V = M_2(\mathbb{F}_q) \times M_2(\mathbb{F}_q) \times M_2(\mathbb{F}_q)$, and there is a directed edge going from (a, e, c) to (b, f, d) if and only if $ab + ef = c + d$. The setting of this digraph is a generalization of that in [4, Section 4.1]

Let G be a digraph on n vertices. Suppose that G is regular of degree d, i.e., the in-degree and out-degree of each vertex are equal to d. Let m_G be the adjacency matrix of G, where $(m_G)_{ij} = 1$ if and only if there is a directed edge from i to j. Let $\mu_1 = d, \mu_2, \dots, \mu_n$ be the eigenvalues of m_G. Notice that these eigenvalues can be complex numbers, and for all $2 \le i \le n$, we have $|\mu_i| \le d$. Define $\mu(G) := \max_{|\mu_i| \neq d} |\mu_i|$. This value is referred to as the second largest eigenvalue of m_G.

A digraph G is called an (n, d, μ)-digraph if G is a d-regular digraph of n vertices, and the second largest eigenvalue of m_G is at most μ.

We recall the following lemma from [16] on the distribution of edges between two vertex sets on an (n, d, μ)-digraph.

Lemma 3.2 *Let $G = (V, E)$ be an (n, d, μ)-digraph. For any two sets $B, C \subseteq V$, the number of directed edges from B to C, denoted by $e(B, C)$ satisfies*

$$\left|e(B, C) - \frac{d}{n}|B||C|\right| \le \mu\sqrt{|B||C|}.$$

With Lemma 3.2 in hand, to prove Proposition 3.1, it is enough to study properties of the sum-product digraph G.

Definition 3.1 Let $a, b \in M_2(\mathbb{F}_q)$. We say they are equivalent, if whenever the ith row of a is not all-zero, neither is the ith row of b and vice versa, for $1 \le i \le 2$.

Proposition 3.3 *The sum product graph G is a $(q^{12}, q^8, c \cdot q^{13/2})$-digraph, for some positive constant c.*

Proof The number of vertices is $|M_2(\mathbb{F}_q)|^3 = q^{12}$. Moreover, for each vertex (a, e, c), with each choice of (b, f), d is determined uniquely from $d = ab + ef - c$. Thus, there are $|M_2(\mathbb{F}_q)|^2 = q^8$ directed edges going out of each vertex. The number of incoming directed edges can be argued in the same way. To conclude, the digraph G is q^8-regular. Let m_G denote the adjacency matrix of G. It remains to bound the magnitude of the second largest eigenvalue of the adjacency matrix of G, i.e., $\mu(m_G)$.

In the next step, we are going to show that m_G is a normal matrix, i.e., $m_G^T m_G = m_G m_G^T$, where m_G^T is the conjugate transpose of m_G. For a normal matrix m, we know that if λ is an eigenvalue of m, then $|\lambda|^2$ is an eigenvalue of mm^T and $m^T m$. Thus, for a normal matrix m, it is enough to give an upper bound for the second largest eigenvalue of mm^T or $m^T m$.

There is a simple way to check whenever G is normal. For any two vertices u and v, let $\mathcal{N}^+(u, v)$ be the set of vertices w such that $\overrightarrow{uw}, \overrightarrow{vw}$ are directed edges, and $\mathcal{N}^-(u, v)$ be the set of vertices w' such that $\overrightarrow{w'u}, \overrightarrow{w'v}$ are directed edges. It is not hard to check that m_G is normal if and only if $|\mathcal{N}^+(u, v)| = |\mathcal{N}^-(u, v)|$ for any two vertices u and v.

Given two vertices (a, e, c) and (a', e', c'), where $(a, e, c) \neq (a', e', c')$, the number of (x, y, z) that lies in the common outgoing neighborhood of both vertices is characterized by

$$\left.\begin{aligned} ax + ey &= c + z \\ a'x + e'y &= c' + z \end{aligned}\right\} \Longrightarrow (a - a')x + (e - e')y = (c - c').$$

For each pair (x, y) satisfying this equation, z is determined uniquely. Thus, the problem is reduced to computing the number of such pairs (x, y).

For convenience, let $\bar{a} = a - a'$, $\bar{c} = c - c'$, and $\bar{e} = e - e'$. Also, let $t = \begin{pmatrix} \bar{a} & \bar{e} \end{pmatrix}_{2\times 4}$. Then, the above relation is equivalent to

$$\begin{pmatrix} \bar{a} & \bar{e} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = t \begin{pmatrix} x \\ y \end{pmatrix}_{4\times 2} = \bar{c}. \tag{3.1}$$

We now have the following cases:

- (*Case 1*: $\operatorname{rank}(t) = 0$) Note that in this case, we need $a = a'$, $c = c'$, and $e = e'$, which is a contradiction to our assumption that $(a, e, c) \neq (a', e', c')$. Thus, we simply exclude this case.
- (*Case 2*: $\operatorname{rank}(t) = 1$) As t is not an all-zero matrix, there is at least one nonzero row. Without loss of generality, assume it is the first row. Then,
$$t = \begin{pmatrix} a_1 & a_2 & e_1 & e_2 \\ \alpha a_1 & \alpha a_2 & \alpha e_1 & \alpha e_2 \end{pmatrix}, \text{ where } (a_1, a_2, e_1, e_2) \neq \mathbf{0} \text{ and } \alpha \in \mathbb{F}_q.$$
  - (*Case 2.1*: $\operatorname{rank}(\bar{c}) = 2$) In this case, there is no solution, as $\operatorname{rank}\left(t\begin{pmatrix} x \\ y \end{pmatrix}\right) \leq \operatorname{rank}(t) = 1$ but $\operatorname{rank}(\bar{c}) = 2$.
  - (*Case 2.2*: $\operatorname{rank}(\bar{c}) = 1$) Let $x = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}$, $y = \begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix}$. We discuss two subcases:
    (a) $\bar{c} = \begin{pmatrix} c_1 & c_2 \\ \alpha c_1 & \alpha c_2 \end{pmatrix}$ with the same factor α, where $(c_1, c_2) \neq (0, 0)$.

In this case, we have the following set of equations:

$$\begin{cases} a_1x_1 + a_2x_3 + e_1y_1 + e_2y_3 = c_1, \\ a_1x_2 + a_2x_4 + e_1y_2 + e_2y_4 = c_2. \end{cases}$$

Since we assume $(a_1, a_2, e_1, e_2) \neq \mathbf{0}$, without loss of generality, let $a_1 \neq 0$. Then,

$$\begin{cases} x_1 = (a_1)^{-1}(c_1 - a_2x_3 - e_1y_1 - e_2y_3), \\ x_2 = (a_1)^{-1}(c_2 - a_2x_4 - e_1y_2 - e_2y_4), \end{cases}$$

which means that for each (x_3, y_1, y_3) there is a unique x_1 and for each (x_4, y_2, y_4) there is a unique x_2. Thus, there are q^6 different (x, y, z) solutions.

(b) In all other sub-cases, there is no solution. If $\bar{c} = \begin{pmatrix} c_1 & c_2 \\ \beta c_1 & \beta c_2 \end{pmatrix}$, where $\beta \neq \alpha$ and $(c_1, c_2) \neq (0, 0)$, then we get the following two equations:

$$\begin{cases} a_1x_1 + a_2x_3 + e_1y_1 + e_2y_3 = c_1, \\ \alpha a_1x_1 + \alpha a_2x_3 + \alpha e_1y_1 + \alpha e_2y_3 = \beta c_1, \end{cases}$$

which obviously do not have any solution.

Otherwise, $\bar{c} = \begin{pmatrix} \beta c_1 & \beta c_2 \\ c_1 & c_2 \end{pmatrix}$, where $(c_1, c_2) \neq (0, 0)$. Note that if $\alpha \neq 0$, then $\beta \neq \alpha^{-1}$, because this case is covered in Case 2.2(a) implicitly. We get the following equations.

$$\begin{cases} a_1x_1 + a_2x_3 + e_1y_1 + e_2y_3 = \beta c_1, \\ \alpha a_1x_1 + \alpha a_2x_3 + \alpha e_1y_1 + \alpha e_2y_3 = c_1, \end{cases}$$

which obviously do not have any solution. Notice that $\alpha = 0$ or $\beta = 0$ corresponds to t and $\bar{c}$ not being equivalent.

– (*Case 2.3*: $\operatorname{rank}(\bar{c}) = 0$) This case is similar to the Case 2.2(a), except $c_1 = c_2 = 0$. We have the following two equations:

$$\begin{cases} a_1x_1 + a_2x_3 + e_1y_1 + e_2y_3 = 0, \\ a_1x_2 + a_2x_4 + e_1y_2 + e_2y_4 = 0. \end{cases}$$

Following the same analysis, we conclude there are q^6 solutions.

- (*Case 3*: $\operatorname{rank}(t) = 2$) In this case, we always have solutions, for any $\bar{c}$.
  – (*Case 3.1*: $\operatorname{rank}(\bar{a}) = 2$ or $\operatorname{rank}(\bar{e}) = 2$) In this case, let us look back on equation (3.1). If $\operatorname{rank}(\bar{a}) = 2$, then we can rewrite (3.1) as $\bar{a}x = \bar{c} - \bar{e}y$. Observe that, for any $y \in M_2(\mathbb{F}_q)$, there is a unique x. Thus, the number of solutions is q^4. The case where $\operatorname{rank}(\bar{e}) = 2$ is similar.
  – (*Case 3.2*: $\operatorname{rank}(\bar{a}) \leq 1$ and $\operatorname{rank}(\bar{e}) \leq 1$) In this case, it is not hard to observe that t must be one of the following four types:

    (i) $\begin{pmatrix} a_1 & a_2 & e_1 & e_2 \\ \alpha a_1 & \alpha a_2 & \beta e_1 & \beta e_2 \end{pmatrix}$, where $(a_1, a_2), (e_1, e_2) \neq (0, 0), \alpha \neq \beta, (\alpha, \beta) \neq (0, 0)$.

https://doi.org/10.4153/S000843952300036X Published online by Cambridge University Press

(ii) $\begin{pmatrix} \alpha a_1 & \alpha a_2 & \beta e_1 & \beta e_2 \\ a_1 & a_2 & e_1 & e_2 \end{pmatrix}$, where $(a_1, a_2), (e_1, e_2) \neq (0, 0)$, $\alpha \neq \beta$, $(\alpha, \beta) \neq (0, 0)$.

(iii) $\begin{pmatrix} a_1 & a_2 & 0 & 0 \\ 0 & 0 & e_1 & e_2 \end{pmatrix}$, where $(a_1, a_2), (e_1, e_2) \neq (0, 0)$.

(iv) $\begin{pmatrix} 0 & 0 & e_1 & e_2 \\ a_1 & a_2 & 0 & 0 \end{pmatrix}$, where $(a_1, a_2), (e_1, e_2) \neq (0, 0)$.

Since (i) and (ii) are symmetric and so is (iii) and (iv), we only argue for (i) and (iii). For (iii), reusing notations from Case 2.2(a), we have

$$\begin{cases} a_1x_1 + a_2x_3 = c_1, \\ a_1x_2 + a_2x_4 = c_2, \\ e_1y_1 + e_2y_3 = c_3, \\ e_1y_2 + e_2y_4 = c_4. \end{cases}$$

As $(a_1, a_2) \neq (0, 0)$ and $(e_1, e_2) \neq (0, 0)$, without loss of generality, we assume $a_1 \neq 0$ and $e_1 \neq 0$. Then, it means for each (x_3, x_4, y_3, y_4) there is a unique (x_1, x_2, y_1, y_2). Thus, the system has q^4 solutions.

For (i), we have

$$\begin{cases} a_1x_1 + a_2x_3 + e_1y_1 + e_2y_3 = c_1, & (1) \\ a_1x_2 + a_2x_4 + e_1y_2 + e_2y_4 = c_2, & (2) \\ \alpha a_1x_1 + \alpha a_2x_3 + \beta e_1y_1 + \beta e_2y_3 = c_3, & (3) \\ \alpha a_1x_2 + \alpha a_2x_4 + \beta e_1y_2 + \beta e_2y_4 = c_4. & (4) \end{cases}$$

Again, assume $a_1 \neq 0$ and $e_1 \neq 0$. Now, take (1) $\times\, \alpha -$ (3), we get $(\alpha - \beta)(e_1y_1 + e_2y_3) = \alpha c_1 - c_3$. As $\alpha \neq \beta$, this means $e_1y_1 + e_2y_3 = (\alpha - \beta)^{-1}(\alpha c_1 - c_3)$. Thus, for each y_3, there is a unique y_1. Similarly, compute (1) $\times\, \beta -$ (3), and we get $a_1x_1 + a_2x_3 = (\beta - \alpha)^{-1}(\beta c_1 - c_3)$, which means that for each x_3, we get a unique x_1. We can do the same for (2) and (4) and conclude that there are q^4 solutions.

Observe that all cases are disjoint and they together enumerate all possible relations between vertices (a, e, c) and (a', e', c'). We computed $\mathcal{N}^+((a, e, c), (a', e', c'))$ above and the computation for $\mathcal{N}^-((a, e, c), (a', e', c'))$ is the same. Thus, we know m_G is normal. Note that each entry of $m_G m_G^T$ can be interpreted as counting the number of common outgoing neighbors between two vertices. We can write $m_G m_G^T$ as

$$\begin{aligned} m_G m_G^T &= q^8 I + 0E_{21} + q^6 E_{22a} + 0E_{22b} + q^6 E_{23} + q^4 E_{31} + q^4 E_{32} \\ &= (q^8 - q^4)I + q^4 J - q^4 E_{21} + (q^6 - q^4)E_{22a} \\ &\qquad - q^4 E_{22b} + (q^6 - q^4)E_{23} + (q^4 - q^4)E_{31} + (q^4 - q^4)E_{32} \\ &= (q^8 - q^4)I + q^4 J - q^4 E_{21} + (q^6 - q^4)E_{22a} - q^4 E_{22b} + (q^6 - q^4)E_{23}, \end{aligned}$$

where I is the identity matrix, J is the all one matrix and E_{ij}s are adjacency matrices, specifying which entries are involved. For example, for Case 2.3, all pairs

$(a,e,c),(a',e',c')$ with $c=c'$ and $\operatorname{rank}(t)=1$ are involved. Thus, the E_{23} is an adjacency matrix of size $q^{12}\times q^{12}$ (containing all triples (a,e,c)), with pairs of vertices satisfying this property marked 1 and all others marked 0.

Finally, observe that each subgraph defined by the corresponding adjacency matrix E_{ij} is regular. This is due to the fact that the condition does not depend on specific value of (a,e,c). Starting from any vertex (a,e,c), we can get to all possible $\bar{a},\bar{e},\bar{c}$ by subtracting the correct (a',e',c'). Thus, for each case, we get the same number of (a',e',c') that satisfies the condition.

Let κ_{ij} be the maximum number of 1s in a row in E_{ij}. Obviously, κ_{ij} is an upper bound on the largest eigenvalue of E_{ij}. It is not difficult to see that $\kappa_{21}\ll q^9$, $\kappa_{22a}\ll q^7$, $\kappa_{22b}\ll q^8$ and $\kappa_{23}\ll q^5$. For example, in Case 2.1, we have $\operatorname{rank}(t)=1$ and $\operatorname{rank}(\bar{c})=2$. For a fixed (a,e,c), the former implies that there are $O(q^5)$ possibilities for a' and e' while the latter implies there are $O(q^4)$ possibilities for c'. Altogether, there are $O(q^9)$ possibilities for (a',e',c') in Case 2.1. Because the graph induced by E_{21} is regular, we have $\kappa_{21}\ll q^9$. Other cases can be deduced accordingly.

The rest follows from a routine computation: let v_2 be an eigenvector corresponding to $\mu(G)$. Then, because G is regular and connected (easy to see, there is no isolated vertex), v_2 is orthogonal to the all 1 vector, which means $J\cdot v_2=\mathbf{0}$. We now have

$$\begin{aligned}\mu(m_G)^2v_2=m_Gm_G^T\cdot v_2&=(q^8-q^4)I\cdot v_2+(-q^4E_{21}+(q^6-q^4)E_{22a}-q^4E_{22b}+(q^6-q^4)E_{23})\cdot v_2\\&=((q^8-q^4)-q^4\kappa_{21}+(q^6-q^4)\kappa_{22a}-q^4\kappa_{22b}+(q^6-q^4)\kappa_{23})\cdot v_2\\&\ll q^{13}\cdot v_2\,.\end{aligned}$$

Thus, $\mu(m_G)\ll q^{13/2}$. ∎

Proof of Proposition 3.1 It follows directly from Proposition 3.3 and Lemma 3.2 that

$$\left|\mathcal{I}(A,B,C,D,E,F)-\frac{1}{q^4}|A||B||C||D||E||F|\right|\ll q^{13/2}\sqrt{|A||B||C||D||E||F|}\,.$$

This completes the proof. ∎

4 Proof of Theorem 2.1

To prove Theorem 2.1, we will also need several technical results. A proof of the following inequality may be found in [8, Lemma 2.4].

Lemma 4.1 *Let $V_1,\dots,V_k$ be subsets of an abelian group. Then*

$$E_+\left(\bigsqcup_{i=1}^k V_i\right)\le\left(\sum_{i=1}^k E_+(V_i)^{1/4}\right)^4.$$

The following lemma is taken from [5] and may also be extracted from [8, 10]. Lemma 4.2 is slightly different to its analogs over commutative rings as highlighted by the duality of the inequalities (4.5) and (4.6).

https://doi.org/10.4153/S000843952300036X Published online by Cambridge University Press

Lemma 4.2 *Let $X \subseteq GL_2(\mathbb{F}_q)$. There exist sets $X_* \subset X$, $D \subset XX$, as well as numbers τ and κ satisfying*

$$\frac{E_\times(X)}{2|X|^2} \le \tau \le |X|, \tag{4.1}$$

$$\frac{E_\times(X)}{\tau^2 \cdot \log|X|} \ll |D| \ll (\log|X|)^6 \frac{|X_*|^4}{E_\times(X)}, \tag{4.2}$$

$$|X_*|^2 \gg \frac{E_\times(X)}{|X|(\log|X|)^{7/2}}, \tag{4.3}$$

$$\kappa \gg \frac{|D|\tau}{|X_*|(\log|X|)^2}, \tag{4.4}$$

such that either

$$r_{DX^{-1}}(x) \ge \kappa \quad \textit{for all} \quad x \in X_*, \tag{4.5}$$

or

$$r_{X^{-1}D}(x) \ge \kappa \quad \textit{for all} \quad x \in X_*. \tag{4.6}$$

We need a dyadic pigeonhole argument, which can be found in [6, Lemma 18].

Lemma 4.3 *For $\Omega \subseteq M_2(\mathbb{F}_q)$, let $w, f : \Omega \to \mathbb{R}^+$ with $f(x) \le M$, $\forall x \in \Omega$. Let $W = \sum_{x \in \Omega} w(x)$. If $\sum_{x\in\Omega} f(x)w(x) \ge K$, then there exists a subset $D \subset \Omega$ and a number τ such that $\tau \le f(x) < 2\tau$ for all $x \in D$ and $K/(2W) \le \tau \le M$. Moreover,*

$$\frac{K}{2 + 2\log_2 M} \le \sum_{x\in D} f(x)w(x) \le 2\tau \sum_{x \in D} w(x) \le \min\{2\tau W,\, 4\tau^2|D|\}.$$

Proof of Lemma 4.2 We use the identities in (1.2) and apply Lemma 4.3, by taking $\Omega = XX$, $f = w = r_{XX}$, $M = |X|$, $K = E_\times(X)$, and $W = |X|^2$, to find a set $D \subset XX$ and a number τ, satisfying (4.1), such that $D = \{\, \lambda \in XX : \tau \le r_{XX}(\lambda) < 2\tau \,\}$ and

$$\tau^2|D| \gg E_\times(X)/\log|X|. \tag{4.7}$$

Define $P_1 = \{\, (x,y) \in X \times X : xy \in D \,\}$ and $A_x = \{\, y : (x,y) \in P_1 \,\}$ for $x \in X$. By the definition of D, we know that $\tau|D| \le |P_1| < 2\tau|D|$. We can use Lemma 4.3 again with $\Omega = X$, $f(x) = |A_x|$, $w = 1$, $M = W = |X|$, and $K = |P_1|$ to find a set $V \subset X$ and a number κ_1 such that $V = \{\, x \in X : \kappa_1 \le |A_x| < 2\kappa_1 \,\}$ and

$$|V|\kappa_1 \gg |P_1|/\log|X| \gg \tau|D|/\log|X|. \tag{4.8}$$

Now, we split the analysis into two cases based on $|V|$:

Case 1 ($|V| \ge \kappa_1(\log|X|)^{-1/2}$): In this case, we simply set $X_* = V$ and $\kappa = \kappa_1$. For each $x \in V$, there are at least κ_1 different y such that $xy \in D$. Therefore, $r_{DX^{-1}}(x) \ge \kappa$ $\forall x \in X_*$.

https://doi.org/10.4153/S000843952300036X Published online by Cambridge University Press

Case 2 ($|V| < \kappa_1(\log|X|)^{-1/2}$): In this case, we find another pair U, κ_2 that satisfies $|U| \gg \kappa_2(\log|X|)^{-1/2}$ and set $X_* = U$ and $\kappa = \kappa_2$. Let $P_2 = \{ (x,y) \in P_1 : x \in V \}$ and $B_y = \{ x : (x,y) \in P_2 \}$. By definition, we have $|P_2| \geq |V|\kappa_1$. We apply Lemma 4.3 again, with $\Omega = X, f(y) = |B_y|, w = 1, K = |P_2|$ and $W = M = |X|$ to get $U \subset X$ and a number κ_2 such that $U = \{ y \in X : \kappa_2 \leq |B_y| < 2\kappa_2 \}$ and

$$|U|\kappa_2 \gg |P_2|/\log|X| \geq \kappa_1|V|/\log|X|. \tag{4.9}$$

Combining this inequality with the assumption of this case ($\kappa_1 \geq |V|(\log|X|)^{1/2}$) and $|V| \geq \kappa_2$, we conclude $|U| \gg \kappa_2(\log|X|)^{-1/2}$. We can then argue similarly as in Case 1 to conclude $r_{X^{-1}D}(x) \geq \kappa \ \forall x \in X_*$.

Now, (4.4) follows from either of (4.8) or (4.9). To prove (4.3), we first note that in either of the cases above we have $|X_*| \gg \kappa(\log|X|)^{-1/2}$. Then using the lower bound on κ, (4.7) and (4.1), we have $|X_*|^2 \gg |D|\tau(\log|X|)^{-5/2} \gg E_\times(X)/(|X|\log|X|)^{7/2}$ as required. Finally, to deduce the required upper bound on $|D|$ in (4.2) note that, as shown above, $|D|\tau \ll |X_*|^2(\log|X|)^{5/2}$, which with (4.7) implies $|D|E_\times(X)(\log|X|)^{-1} \ll (|D|\tau)^2 \ll |X_*|^4(\log|X|)^5$. ∎

Lemma 4.4 *Let $X \subseteq GL_2(\mathbb{F}_q)$. Then there exists $X_* \subseteq X$, with*

$$|X_*| \gg \frac{E_\times(X)^{1/2}}{|X|^{1/2}(\log|X|)^{7/4}},$$

such that

$$E_+(X_*) \ll \frac{|X_*|^4|X|^6(\log|X|)^2}{q^4E_\times(X)^2} + \frac{q^{13/2}|X_*|^3|X|(\log|X|)^5}{E_\times(X)}. \tag{4.10}$$

Proof We apply Lemma 4.2 to the set X and henceforth assume its full statement, keeping the same notation. Without loss of generality, assume $r_{X^{-1}D}(x) \geq \kappa \ \forall x \in X_*$. Thus,

$$\begin{aligned} E_+(X_*) &= |\{(x_1,x_2,x_3,x_4) \in X_*^4 : x_1 + x_2 = x_3 + x_4\}| \\ &\leq \kappa^{-2}|\{(d_1,d_2,x_1,x_2,y_1,y_2) \in D^2 \times X_*^2 \times X^2 : x_1 + y_1^{-1}d_1 = x_2 + y_2^{-1}d_2\}| \\ &= \kappa^{-2}\mathcal{I}(X^{-1}, D, -X_*, -X^{-1}, D, X_*). \end{aligned}$$

Then applying Proposition 3.1 and (4.4), we obtain

$$\begin{aligned} E_+(X_*) &\ll \kappa^{-2} \cdot \left(\frac{(|D||X||X_*|)^2}{q^4} + q^{13/2}|D||X||X_*| \right) \\ &\ll \frac{|X_*|^4|X|^2(\log|X|)^2}{q^4\tau^2} + \frac{q^{13/2}|X_*|^3|X|(\log|X|)^4}{|D|\tau^2}. \end{aligned}$$

Finally, applying (4.1) and (4.2), we obtain the required bound in (4.10) for $E_+(X_*)$. ∎

We are now ready to prove Theorem 2.1.

https://doi.org/10.4153/S000843952300036X Published online by Cambridge University Press

Proof of Theorem 2.1 We begin by describing an algorithm, which constructs two sequences of sets $A = S_1 \supseteq S_2 \supseteq \cdots \supseteq S_{k+1}$ and $\varnothing = T_0 \subseteq T_1 \subseteq \cdots \subseteq T_k$ such that $S_i \sqcup T_{i-1} = A$, for $i = 1, \ldots, k+1$.

Let $1 \le M \le |A|$ be a parameter. At any step $i \ge 1$, if $E_\times(S_i) \le |A|^3/M$ the algorithm halts. Otherwise if

$$E_\times(S_i) > \frac{|A|^3}{M}, \tag{4.11}$$

through a use of Lemma 4.4, with $X = S_i$, we identify a set $V_i := X_* \subseteq S_i$, with

$$|V_i| \gg \frac{E_\times(S_i)^{1/2}}{|S_i|^{1/2}(\log|A|)^{7/4}} > \frac{|A|}{M^{1/2}(\log|A|)^{7/4}} \tag{4.12}$$

and

$$E_+(V_i) \ll \frac{|V_i|^4|S_i|^6(\log|S_i|)^2}{q^4E_\times(S_i)^2} + \frac{q^{13/2}|V_i|^3|S_i|(\log|S_i|)^5}{E_\times(S_i)}. \tag{4.13}$$

We then set $S_{i+1} = S_i \setminus V_i$, $T_{i+1} = T_i \sqcup V_i$ and repeat this process for the step $i+1$. From (4.12), we deduce $|V_i| \gg |A|^{1/2}(\log|A|)^{-7/4}$ and so the cardinality of each S_i monotonically decreases. This in turn implies that this process indeed terminates after a finite number of iterations k. We set $B = S_{k+1}$ and $C = T_k$, noting that $A = B \sqcup C$ and that

$$E_\times(B) \le \frac{|A|^3}{M}. \tag{4.14}$$

We apply the inequalities (4.11), (4.12) and $|S_i| \le |A|$, to (4.13), to get

$$\begin{aligned} E_+(V_i) &\ll M^2|V_i|^4q^{-4}(\log|A|)^2 + M|A|^{-2}|V_i|^3q^{13/2}(\log|A|)^5 \\ &\ll \left(M^2q^{-4}(\log|A|)^2 + M^{3/2}|A|^{-3}q^{13/2}(\log|A|)^{27/4}\right)\cdot|V_i|^4. \end{aligned}$$

Then, observing that

$$C = T_k = \bigsqcup_{i=1}^{k} V_i \subseteq A,$$

we use Lemma 4.1 to obtain

$$\begin{aligned} E_+(C) &\ll (M^2q^{-4}(\log|A|)^2 + M^{3/2}|A|^{-3}q^{13/2}(\log|A|)^{27/4})\left(\sum_{i=1}^{k}|V_i|\right)^4 \\ &\le M^2|A|^4q^{-4}(\log|A|)^2 + M^{3/2}|A|q^{13/2}(\log|A|)^{27/4}. \end{aligned}$$

Note that Lemma 4.1 is applicable because $M_2(\mathbb{F}_q)$ is an abelian group under addition. Comparing this with (4.14), we see the choice $M = M(|A|)$, given by (2.1) is optimal. ■

5 Proofs of Theorem 2.2 and Corollary 2.3

Proof of Theorem 2.2 We proceed similarly to the proof of [7, Theorem 6]. Note that

$$\begin{aligned} E_+(A,B) &= |C|^{-2}|\{ (a,a',b,b',c,c') \in A^2 \times B^2 \times C^2 : a + bcc^{-1} = a' + b'c'(c')^{-1} \}| \\ &\leq |C|^{-2}|\{ (a,a',s,s',c,c') \in A^2 \times (BC)^2 \times (C^{-1})^2 : a + sc = a' + s'c' \}|. \end{aligned}$$

The required result then follows by applying Proposition 3.1. ■

Proof of Corollary 2.3 Since $|A| \gg q^3$, we may assume $A \subseteq GL_2(\mathbb{F}_q)$. We use Theorem 2.2, with $A = B = C$ and apply the lower bound on $E_+(A)$ given by (1.3) to obtain (2.3). To prove (2.4), we follow the same process and apply the assumption $|AA| \ll |A|$, to obtain

$$|A + A| \gg \min\{ q^4, |A|^3/q^{13/2} \}, \tag{5.1}$$

which gives the required result.

To prove (2.5), we use Theorem 2.2, to get

$$\frac{|A+A|^2|A|^2}{|A+A+A|} \leq E_+(A+A,A) \ll \frac{|A+A|^2|A|^2}{q^4} + q^{13/2}|A+A|.$$

Recalling (5.1), this rearranges to

$$|A+A+A| \gg \min\left\{ q^4, \frac{|A+A||A|^2}{q^{13/2}} \right\} \gg \min\left\{ q^4, \frac{|A|^2}{q^{5/2}}, \frac{|A|^5}{q^{13}} \right\}.$$

The required result then easily follows. ■

6 Proofs of Theorem 2.4, Corollary 2.5, and Theorem 2.6

Proof of Theorem 2.4 For $\lambda \in AB + C$, write

$$t(\lambda) = |\{ (a,b,c) \in A \times B \times C : ab + c = \lambda \}|.$$

By the Cauchy–Schwarz inequality, we have

$$(|A||B||C|)^2 = \left(\sum_{\lambda \in AB+C} t(\lambda) \right)^2 \leq |AB+C| \sum_{\lambda \in AB+C} t(\lambda)^2.$$

Further noting that

$$\sum_{\lambda \in AB+C} t(\lambda)^2 = \mathcal{J}(A,B,-C,-A,B,C).$$

We apply Proposition 3.1 to obtain

$$|AB+C| \gg \min\left\{ q^4, \frac{|A||B||C|}{q^{13/2}} \right\}.$$

This immediately implies the required result.

https://doi.org/10.4153/S000843952300036X Published online by Cambridge University Press

For the set $(A+B)C$, as above we have

$$|(A+B)C| \geq \frac{|A|^2|B|^2|C|^2}{|\{\,(a,b,c,a',b',c') \in (A\times B\times C)^2 : (a+b)c = (a'+b')c'\,\}|}.$$

To estimate the denominator, we follow the argument in the proof of Proposition 3.1. In particular, we first define a graph G with the vertex set $V = M_2(\mathbb{F}_q)\times M_2(\mathbb{F}_q)\times M_2(\mathbb{F}_q)$, and there is a direct edge going from (a,e,c) to (b,f,d) if $ba+ef = c+d$. The only difference here compared to that graph in Section 3 is that we switch between ba and ab. By using a similar argument as in Section 3, we have this graph is a $(q^{12}, q^8, cq^{13/2})$-digraph, where c is a positive constant.

To bound the denominator, we observe that the equation

$$(a+b)c = (a'+b')c'$$

gives us a direct edge from $(c,-b',-ac)$ to $(b,c',a'c')$. So, let $U := \{(c,-b',-ac) : a \in A, c\in C, b'\in B\}$ and $W = \{(b,c',a'c') : b\in B, c'\in C, a'\in A\}$. Since $C \subseteq GL_2(\mathbb{F}_q)$, we have $|U| = |W| = |A||B||C|$. So applying Lemma 3.2, the number of edges from U to W is at most

$$\frac{|A|^2|B|^2|C|^2}{q^4} + q^{13/2}|A||B||C|.$$

In other words,

$$|\{\,(a,b,c,a',b',c') \in (A\times B\times C)^2 : (a+b)c = (a'+b')c'\,\}| \ll \frac{|A|^2|B|^2|C|^2}{q^4} + q^{13/2}|A||B||C|,$$

and we get the desired estimate. ∎

Proof of Corollary 2.5 It follows from Theorem 2.4 that

$$|AA+A+A| \gg q^4 \quad \text{if} \quad |A|^2|A+A| \gg q^{10+1/2} \tag{6.1}$$

and

$$|AA(A+A)| \gg q^4 \quad \text{if} \quad |A|^2|AA| \gg q^{10+1/2}. \tag{6.2}$$

Note that by Corollary 2.3, if $|A| \gg q^{3+7/16}$, we have

$$|A|^2 \cdot \max\{\,|A+A|, |AA|\,\} \gg q^{4/3}|A|^{8/3} \gg q^{10+1/2}.$$

Hence, one of the conditions in (6.1) or (6.2) is satisfied, which in turn gives the required estimate. ∎

Proof of Theorem 2.6 By the Cauchy–Schwarz inequality and Proposition 3.1, we have

$$\begin{aligned}\mathcal{J}(A,B,C,D) &= |\{\,(a,b,c,d)\in A\times B\times C\times D : a+b = cd\,\}|\\ &\leq |B|^{1/2}|\{\,(a,a',c,c',d,d') \in A^2\times C^2\times D^2 : cd - a = c'd' - a'\,\}|^{1/2}\\ &\ll \frac{|A||B|^{1/2}|C||D|}{q^2} + q^{13/4}(|A||B||C||D|)^{1/2}.\end{aligned}$$ ∎

https://doi.org/10.4153/S000843952300036X Published online by Cambridge University Press

References

[1] D. N. V. Anh, L. Q. Ham, D. Koh, T. Pham, and L. A. Vinh, *On a theorem of Hegyvári and Hennecart*. Pacific J. Math. **305**(2020), no. 2, 407–421.
[2] A. Balog and T. D. Wooley, *A low-energy decomposition theorem*. Q. J. Math. **68**(2017), 207–226.
[3] N. Hegyvári and F. Hennecart, *Expansion for cubes in the Heisenberg group*. Forum Math. **30**(2018), 227–236.
[4] Y. D. Karabulut, D. Koh, T. Pham, C.-Y. Shen, and L. A. Vinh, *Expanding phenomena over matrix rings*. Forum Math. **31**(2019), 951–970.
[5] A. Mohammadi and S. Stevens, *Low-energy decomposition results over finite fields*. Preprint, 2021. arXiv:2102.01655
[6] B. Murphy and G. Petridis, *Products of differences over arbitrary finite fields*. Discrete Anal. **18**(2018), 1–42.
[7] O. Roche-Newton, M. Rudnev, and I. D. Shkredov, *New sum-product type estimates over finite fields*. Adv. Math. **293**(2016), 589–605.
[8] O. Roche-Newton, I. E. Shparlinski, and A. Winterhof, *Analogues of the Balog–Wooley decomposition for subsets of finite fields and character sums with convolutions*. Ann. Comb. **23**(2019), 183–205.
[9] M. Rudnev, *On the number of incidences between points and planes in three dimensions*. Combinatorica **38**(2018), 219–254.
[10] M. Rudnev, I. D. Shkredov, and S. Stevens, *On the energy variant of the sum-product conjecture*. Rev. Mat. Iberoam. **36**(2020), no. 1, 207–232.
[11] A. Sárközy, *On sums and products of residues modulo p*. Acta Arith. **118**(2005), 403–409.
[12] I. D. Shkredov, *An application of the sum-product phenomenon to sets avoiding several linear equations*. Sbornik: Mathematics, **209**(4), 580.
[13] I. D. Shkredov, *A short remark on the multiplicative energy of the spectrum*. Math. Notes **105**(2019), 449–457.
[14] I. D. Shkredov, *A remark on sets with small Wiener norm*. In: A. Raigorodskii and M. T. Rassias (eds.), Trigonometric sums and their applications, Springer, Cham, 2020, pp. 261–272.
[15] C. Swaenepoel and A. Winterhof, *Additive double character sums over some structured sets and applications*. Acta Arith. **199**(2021), 135–143.
[16] V. Vu, *Sum-product estimates via directed expanders*. Math. Res. Lett. **15**(2008), 375–388.

School of Mathematics and Statistics, University of Sydney, Camperdown, NSW 2006, Australia
e-mail: ali.mohammadi.np@gmail.com

University of Science, Vietnam National University, Hanoi 100000, Vietnam
e-mail: phamanhthang.vnu@gmail.com

Institute of Science and Technology Austria, Klosterneuburg 3400, Austria
e-mail: yiting.wang@ist.ac.at

https://doi.org/10.4153/S000843952300036X Published online by Cambridge University Press