On the determinants and permanents of matrices with restricted entries over prime fields

Doowon Koh∗ Thang Pham† Chun-Yen Shen ‡ Le Anh Vinh §

Abstract

Let $A$ be a set in a prime field $\mathbb{F}_p$. In this paper, we prove that $d \times d$ matrices with entries in $A$ determine almost $|A|^{d+1/4}$ distinct determinants and almost $|A|^{2-1/4}$ distinct permanents when $|A|$ is small enough.

1 Introduction

Throughout the paper, let $q = p^r$ where $p$ is an odd prime and $r$ is a positive integer. Let $\mathbb{F}_q$ be a finite field with $q$ elements. The prime base field $\mathbb{F}_p$ of $\mathbb{F}_q$ may then be naturally identified with $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$.

Let $M = [a_{ij}]$ be an $n \times n$ matrix. Two basic parameters of $M$ are its determinant

$$\text{Det}(M) := \sum_{\sigma \in S_n} \text{sgn}(\sigma) \prod_{i=1}^{n} a_{i \sigma(i)}$$

and its permanent

$$\text{Per}(M) := \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i \sigma(i)},$$

where $S_n$ is the symmetric group on $n$ elements.

For a positive integer $d$, let $M_d(A)$ denote the set of $d \times d$ matrices with components in the set $A$. For a given $t$ in the field, let $D_d(A, t)$ and $P_d(A, t)$ be the number of matrices in $M_d(A)$ having determinant $t$ and permanent $t$, respectively. Let $f_d(A)$ and $g_d(A)$ be the number of distinct determinants and distinct permanents determined by matrices in $M_d(A)$, respectively.

In [1], Ahmadi and Shparlinski studied some classes of matrices over the prime field $\mathbb{F}_p$ of $p$ elements with components in a given interval

$$[-H, H] \subset [-(p-1)/2, (p-1)/2].$$

∗Department of Mathematics, Chungbuk National University. Email: koh131@chungbuk.ac.kr
†Department of Mathematics, UCSD. Email: v9pham@ucsd.edu
‡Department of Mathematics, National Taiwan University. Email: cyshen@math.ntu.edu.tw
§Department of Mathematics, Vietnam National University. Email: vinhla@vnu.edu.vn
They proved some distribution results on the number of $d \times d$ matrices with entries in a given interval having a fixed determinant. More precisely, they obtained that

$$D_d([-H, H], t) = (1 + o(1)) \frac{(2H + 1)^d}{p}$$

if $t \in \mathbb{F}_p^*$ and $H \gg p^{3/4}$, which is asymptotically close to the expected value. In the case $d = 2$, the lower bound can be improved to $H \gg p^{1/2+\epsilon}$ for any constant $\epsilon > 0$. Recall that the notation $U = O(V)$ and $U \ll V$ are equivalent to the assertion that the inequality $|U| \leq cV$ holds for some constant $c > 0$. Note that the implied constants in the symbols $O, o$ and $\ll$ may depend on integer parameter $d$. We also will use the notation $U \gg V$ for the case $U \gg (\log U)^{-cV}$ for some positive constant $c$.

Covert et al. [2] studied this problem in a more general setting, namely, they proved that for any $t \in \mathbb{F}_q^*$ and $A \subset \mathbb{F}_q$, the number of matrices in $M_d(A)$ of determinant $t$ satisfies

$$D_d(A, t) = (1 + o(1)) \frac{|A|^9}{q}.$$

In [14], the fourth listed author extended this result to higher dimensional cases. More precisely, he proved the following:

$$D_d(A, t) = (1 + o(1)) \frac{|A|^{d^2}}{q}$$

for any $t \in \mathbb{F}_q^*$ and $A \subset \mathbb{F}_q$ of cardinality $|A| \gg q^{d^2/3}$.

Another important question is to ask for the number of distinct determinants $f_d(A)$ determined by matrices in $M_d(A)$. The authors of [2] showed that $f_d(A) = q$ whenever $|A| > \sqrt{q}$. Their result can also be extended to higher dimensions.

For the permanant, the fourth listed author [17] obtained several results for the distribution of a given permanent and the number of distinct permanents determined by matrices in $M_d(A)$. More precisely, he showed that $g_d(A) = (1 + o(1))q$ if $A \subset \mathbb{F}_q$ with cardinality $|A| \gg q^{d/2+\epsilon}$. Furthermore, if we restrict our study to matrices over the prime field $\mathbb{F}_p$ with components in a given interval $I := [a + 1, a + b] \subset \mathbb{F}_p$, we obtain a stronger result

$$D_d(I, t) = (1 + o(1)) \frac{b^{d^2}}{p}$$

if $b \gg p^{1/2+\epsilon}$ for any constant $\epsilon > 0$. We refer the reader to [17] for more details.

The main purpose of this paper is to study the the number of distinct determinants and permanents determined by matrices in $M_d(A)$ when $A$ is a small subset of $\mathbb{F}_p$. More precisely, we have the following results for the number of distinct determinants.

**Theorem 1.1.** Let $A$ be a set in $\mathbb{F}_p$.

(i) If $|A| \leq p^{2/3}$, then we have

$$f_2(A) \gg |A|^{3/2}.$$
(ii) If $|A| \leq p^{136 \times 2^{d-1} - 137}$ and $d \geq 4$ even, we have

$$f_d(A) \gtrsim |A|^{3 + \frac{1}{180} - 137 \times 2^{d-2}}.$$  

**Theorem 1.2.** Let $A$ be a set in $\mathbb{F}_p$ and $d \geq 3$ odd.

(i) If $|A| \leq p^{1/7}$ and $d = 3$, we have

$$f_3(A) \gg |A|^{7/4}.$$

(ii) If $|A| \leq p^{136 \times 2^{(d-1)/2} - 137}$ and $d \geq 5$ odd, we have

$$f_d(A) \gtrsim |A|^{\frac{5}{2} + \frac{1}{90} - \frac{137}{45 \times 2^{(d+1)/2}}.}$$

From the lower bounds of Theorems 1.1 and 1.2, we make the following conjecture.

**Conjecture 1.3.** For $A \subseteq \mathbb{F}_p$, suppose $d$ is large enough, we have

$$f_d(A) \gtrsim \min \{|A|^4, p\}.$$

For the number of distinct permanents, we have the following results.

**Theorem 1.4.** Let $A$ be a set in $\mathbb{F}_p$ with $|A| \leq p^{2/3}$. We have

$$g_2(A) \gg |A|^{3/2}.$$

**Theorem 1.5.** Let $A$ be a set in $\mathbb{F}_p$ with $|A| \leq p^{1/2}$. For any integer $d \geq 3$, we have

$$g_d(A) \gg |A|^{2 - \frac{1}{d} + \frac{1}{45}}.$$  

If $A$ is a set in an arbitrary finite field $\mathbb{F}_q$ where $q$ is an odd prime power, then it has been shown by Vinh [17] that under the condition $|A| \geq q^{2d-1}$ the matrices in $M_d(A)$ determine a positive proportion of all permanents. The same threshold, i.e. $\frac{2d-1}{2d-1}$, is indicated to be true for the Erdős distinct distances problem in $A^d$ over $\mathbb{F}_q^d$ (see [4]). Recently, Pham, Vinh, and De Zeeuw [10] showed that for $A \subseteq \mathbb{F}_p$, the number of distinct distances determined by points in $A^d$ is almost $|A|^2$ if the size of $A$ is not so large. Thus it seems reasonable to make the following conjecture.

**Conjecture 1.6.** For $A \subseteq \mathbb{F}_p$ and an integer $d \geq 2$, we have

$$g_d(A) \gtrsim \min \{|A|^2, p\}.$$

Recently, another question on determinants of matrices has been studied by Karabulut [7] by employing spectral graph theory techniques. More precisely, she showed that for a set $\mathcal{E}$ of $2 \times 2$ matrices over $\mathbb{F}_p$, if $|\mathcal{E}| \gg p^{5/2}$, then for any $\lambda \in \mathbb{F}_p^*$ there exist two matrices $X, Y \in \mathcal{E}$ such that $\text{Det}(X - Y) = \lambda$. In this paper, we give a result on the case $\mathcal{E} = M_2(A)$ for some small set $A \subseteq \mathbb{F}_p$. For $A \subseteq \mathbb{F}_p$, we define

$$F_2(A) := \{\text{Det}(X - Y) : X, Y \in M_2(A)\}, \quad G_2(A) := \{\text{Per}(X - Y) : X, Y \in M_2(A)\}.$$

**Theorem 1.7.** For $A \subseteq \mathbb{F}_p$ with $|A| \leq p^{9/16}$, we have

$$|F_2(A)|, |G_2(A)| \gtrsim |A|^{\frac{9}{4} + \frac{1}{4}}.$$  

3
2 Proofs of Theorems 1.1 and 1.2

To prove our main theorems, we shall make use of the following lemmas.

**Lemma 2.1** ([9], Corollary 4). For $A \in \mathbb{F}_p$, we have

$$|AA \pm AA| \gg \min \{ |A|^{3/2}, p \}.$$ 

**Lemma 2.2** ([12], Corollary 11). Suppose that none of $B, C, D \in \mathbb{F}_p$ is the same as $\{0\}$. Then we have

$$|B(C - D)| \gg \min \{ |B|^{1/2}|C|^{1/2}|D|^{1/2}, p \}.$$ 

**Lemma 2.3** ([8], Theorem 27). For $A \in \mathbb{F}_p$, we have

$$|(A - A)(A - A)| \gg \min \{ |A|^{3/2+1/90}, p \}.$$ 

**Lemma 2.4.** For $A \in \mathbb{F}_p$ with $|A| \leq p^{45/68}$ and $d \geq 4$ even, we have

$$f_d(A) \gg \min \{ f_{d-2}(A)^{1/2}|A|^{3/2+1/90}, p \}.$$ 

**Proof.** We may assume that $|A| \geq 2$. Let $X_d$ be the set of distinct determinants of matrices in $M_d(A)$. Let $M$ be a $d \times d$ matrix in $M_d(A)$ with the following form

$$M = \begin{bmatrix}
    a_{11} & a_{12} & a_{33} & \ldots & a_{3d-1} & a_{3d} \\
    a_{21} & a_{22} & a_{43} & \ldots & a_{4d-1} & a_{4d} \\
    u_1 & u_2 & a_{33} & \ldots & a_{3d-1} & a_{3d} \\
    v_1 & v_2 & a_{43} & \ldots & a_{4d-1} & a_{4d} \\
    a_{51} & a_{52} & a_{53} & \ldots & a_{5d-1} & a_{5d} \\
    \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
    a_{d-11} & a_{d-12} & a_{d-13} & \ldots & a_{d-1d-1} & a_{d-1d} \\
    a_{d1} & a_{d2} & a_{d3} & \ldots & a_{dd-1} & a_{dd}
\end{bmatrix}.$$ 

We have

$$\text{Det}(M) = \begin{vmatrix}
    a_{11} - u_1 & a_{12} - u_2 & 0 & \ldots & 0 & 0 \\
    a_{21} - v_1 & a_{22} - v_2 & 0 & \ldots & 0 & 0 \\
    u_1 & u_2 & a_{33} & \ldots & a_{3d-1} & a_{3d} \\
    v_1 & v_2 & a_{43} & \ldots & a_{4d-1} & a_{4d} \\
    a_{51} & a_{52} & a_{53} & \ldots & a_{5d-1} & a_{5d} \\
    \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
    a_{d-11} & a_{d-12} & a_{d-13} & \ldots & a_{d-1d-1} & a_{d-1d} \\
    a_{d1} & a_{d2} & a_{d3} & \ldots & a_{dd-1} & a_{dd}
\end{vmatrix}.$$ 

$$= \begin{vmatrix}
    a_{11} - u_1 & a_{12} - u_2 \\
    a_{21} - v_1 & a_{22} - v_2
\end{vmatrix} \cdot \begin{vmatrix}
    a_{33} & \ldots & a_{3d-1} & a_{3d} \\
    a_{43} & \ldots & a_{4d-1} & a_{4d} \\
    a_{53} & \ldots & a_{5d-1} & a_{5d} \\
    \vdots & \vdots & \ddots & \vdots \\
    a_{d-13} & \ldots & a_{d-1d-1} & a_{d-1d} \\
    a_{d3} & \ldots & a_{dd-1} & a_{dd}
\end{vmatrix}. $$

4
This implies that
\[ X_{d-2} \cdot ((A - A)(A - A) - (A - A)(A - A)) \subset X_d. \]

Using Lemmas 2.2 and 2.3 we see that
\[ f_d(A) \gtrsim \min \left\{ f_{d-2}(A)^{1/2} \min\{|A|^{3/2 + 1/90}, p\} \right\}. \]  
(2.1)

Thus the lemma follows from the assumption that \(|A| \leq p^{45/68}\) which implies that \(\min\{|A|^{3/2 + 1/90}, p\} = |A|^{3/2 + 1/90} \).

Proof of Theorem 1.1. Let \(M\) be a \(2 \times 2\) matrix in \(M_2(A)\) of the following form
\[ M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}. \]

Then we have \(\det(M) = ad - bc\). This implies that \(f_2(A) = |AA - AA|\). Thus the first part of Theorem 1.1 follows from Lemma 2.1.

In order to prove the second part of Theorem 1.1 we use induction on \(d \geq 4\) even. In the base case when \(d = 4\), the statement follows by combining (2.1) with the first part of Theorem 1.1. Suppose the statement holds for \(d - 2 \geq 4\). We now show that it also holds for \(d\). Indeed, from Lemma 2.4 we see that if \(|A| \leq p^{45/68}\), then
\[ f_d(A) \gtrsim \min \left\{ f_{d-2}(A)^{1/2} |A|^{3/2 + 1/90}, p \right\}. \]

By induction hypothesis, it follows that if \(|A| \leq p^{45\times2(d-2)/2 \times 136 \times 2^{(d-2)/2} - 137}\), then
\[ f_{d-2}(A) \gtrsim |A|^{3 + \frac{1}{45} \frac{137}{45 \times 2^{(d-2)/2}}}. \]

By the above two inequalities, we see that if \(|A| \leq p^{45\times2(d-2)/2 \times 136 \times 2^{(d-2)/2} - 137}\), then
\[ f_d(A) \gtrsim \min \left\{ |A|^{3 + \frac{1}{45} \frac{137}{45 \times 2^{(d-2)/2}}}, p \right\}. \]

By a direct comparison, this clearly implies that if \(|A| \leq p^{45\times2d/2 \times 136 \times 2^{d/2} - 137}\), then
\[ f_d(A) \gtrsim \min \left\{ |A|^{3 + \frac{1}{45} \frac{137}{45 \times 2^{d/2}}}, p \right\} = |A|^{3 + \frac{1}{45} \frac{137}{45 \times 2^{d/2}}}. \]

Hence the proof of the theorem is complete.

In order to prove Theorem 1.2 we need the following result.

Lemma 2.5. Let \(A\) be a set in \(\mathbb{F}_p\) and \(d \geq 3\) odd. We have
\[ f_d(A) \gg \min \left\{ f_{d-1}(A)^{1/2} |A|, p \right\}. \]
Proof. We may assume that $|A| \geq 2$, because the statement of the lemma is obvious for $|A| = 1$. Hence, we are able to invoke Lemma 2.2. Let $X_d$ be the set of distinct determinants of matrices in $M_d(A)$. Let $M$ be a $d \times d$ matrix in $M_d(A)$ of the following form

$$M = \begin{bmatrix}
    a_{11} & a_{12} & a_{13} & \ldots & a_{1d-1} & a_{11} \\
    a_{21} & a_{22} & a_{23} & \ldots & a_{2d-1} & a_{21} \\
    \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\
    a_{d-11} & a_{d-12} & a_{d-13} & \ldots & a_{d-1d-1} & a_{d-11} \\
    x_1 & x_2 & x_3 & \ldots & x_{d-1} & x_d
\end{bmatrix}$$

We expand the last row. Then the basic properties of determinants yield

$$\det(M) = (-1)^{d+1}x_1 \begin{vmatrix}
    a_{12} & a_{13} & \ldots & a_{1d-1} & a_{11} \\
    a_{22} & a_{23} & \ldots & a_{2d-1} & a_{21} \\
    \vdots & \vdots & \ddots & \vdots & \vdots \\
    a_{d-12} & a_{d-13} & \ldots & a_{d-1d-1} & a_{d-11} \\
    a_{d-11} & a_{d-12} & a_{d-13} & \ldots & a_{d-1d-1}
\end{vmatrix} + x_d$$

$$= (x_d - x_1) \begin{vmatrix}
    a_{11} & a_{12} & a_{13} & \ldots & a_{1d-1} \\
    a_{21} & a_{22} & a_{23} & \ldots & a_{2d-1} \\
    \vdots & \vdots & \ddots & \ddots & \vdots \\
    a_{d-11} & a_{d-12} & a_{d-13} & \ldots & a_{d-1d-1} \\
    a_{d-11} & a_{d-12} & a_{d-13} & \ldots & a_{d-1d-1}
\end{vmatrix}.$$

This implies that $(A - A)X_{d-1} \subset X_d$. Hence, the lemma follows immediately from Lemma 2.2.

Proof of Theorem 1.2. Let $d \geq 3$ odd. Then $d - 1$ is even. Thus combining Theorem 1.1 and Lemma 2.5, we see that

(i) if $|A| \leq p^{2/3}$ we have

$$f_3(A) \gg \min\{f_2(A)^{1/2}|A|, p\} \gg \min\{|A|^{7/4}, p\}.$$

(ii) if $|A| \leq p^{4/7} \frac{125}{116} \frac{1}{d^{11/2}}$ and $d \geq 5$ odd, then we have

$$f_d(A) \gg \min\{f_{d-1}(A)^{1/2}|A|, p\} \gg \min\{|A|^{\frac{5}{2} + \frac{1}{30} - \frac{127}{45 \cdot 2^{(d+1)/2}}}, p\}$$

Since $p^{4/7} < p^{2/3}$, the statement (i) implies that if $|A| \leq p^{4/7}$, then $f_3(A) \gg \min\{|A|^{7/4}, p\} = |A|^{7/4}$, which completes the proof of the first part of Theorem 1.2.
To prove the second part of Theorem 1.2, first observe that
\[
\min \{ |A|^{\frac{5}{2}} + \frac{1}{90} - \frac{137}{45 \times 2^{(d+1)/2}}, \ p \} = |A|^{\frac{5}{2}} + \frac{1}{90} - \frac{137}{45 \times 2^{(d+1)/2}} \quad \text{for} \quad |A| \leq p^{\frac{45 \times 2^{(d+1)/2}}{113 \times 2^{(d+1)/2} - 137}},
\]
and
\[
p^{\frac{45 \times 2^{(d-1)/2}}{113 \times 2^{(d+1)/2} - 137}} \leq p^{\frac{45 \times 3^{(d+1)/2}}{113 \times 2^{(d+1)/2} - 137}} \quad \text{for odd} \quad d \geq 5.
\]
The statement of the second part of Theorem 1.2 follows by these observations and the statement (ii) above.

3 Proofs of Theorems 1.4 and 1.5

Proof of Theorem 1.4. Let \( M \) be a \( 2 \times 2 \) matrix in \( M_2(A) \) of the following form
\[
M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.
\]
Then we have \( \text{Per}(M) = ad + bc \). This implies that
\[
g_2(A) \gg |AA + AA| \gg \min\{|A|^{3/2}, \ p\},
\]
where the second inequality follows from Lemma 2.1. Thus if \( |A| \leq q^{2/3} \), then \( g_2(A) \gg |A|^{3/2} \). This completes the proof of Theorem 1.4.

In order to prove Theorem 1.5, we need the following lemmas.

Lemma 3.1 ([12], Theorem 4). Let \( P_1, P_2 \subset \mathbb{F}_p \) with \( |P_1| \leq |P_2| \), and let \( \mathcal{L} \) denote a finite set of lines in \( \mathbb{F}_p^2 \). Assume that \( |P_1||P_2|^2 \leq |\mathcal{L}|^3 \) and \( |P_1||\mathcal{L}| \ll p^2 \). Then the number of incidences between \( P_1 \times P_2 \) and lines in \( \mathcal{L} \), denoted by \( I(P_1 \times P_2, \mathcal{L}) \), satisfies
\[
I(P_1 \times P_2, \mathcal{L}) \ll |P_1|^{3/4}|P_2|^{1/2}|\mathcal{L}|^{3/4} + |\mathcal{L}|.
\]

Lemma 3.2. For \( A, B, C \subset \mathbb{F}_p \) with \( |B|, |C| \geq |A| \) and \( |A| \leq p^{1/2} \), we have
\[
|A + B||AC| \gg |A|^{8/5}|B|^{2/5}|C|^{2/5}.
\]

Proof. To prove this lemma, we follow the arguments of Stevens and de Zeeuw in [12, Corollary 9]. Suppose that
\[
|A + B| \leq |AC|. \quad (3.1)
\]
Since the case \( |A + B| \geq |AC| \) can be handled in a similar way, we only provide the proof in the case when (3.1) holds.

Set \( \mathcal{P} := (A+B) \times (AC) \). Let \( \mathcal{L} \) be the set of lines defined by the equations \( y = c(x-b) \) with \( c \in C \) and \( b \in B \). Without loss of generality, we may assume that \( 0 \notin C \). Then we have \( |\mathcal{P}| = |A + B||AC| \) and \( |\mathcal{L}| = |B||C| \). It is clear that the number of incidences
between $\mathcal{P}$ and $\mathcal{L}$ is at least $|A||B||C|$, because each line $y = c(x - b)$ for $(c, b) \in C \times B$ contains the points of the form $(a + b, ac) \in \mathcal{P}$ for all $a \in A$. In order words, we have

$$|A||B||C| \leq I(\mathcal{P}, \mathcal{L}). \quad (3.2)$$

In order to find an upper bound of $I(\mathcal{P}, \mathcal{L})$, we now apply Lemma 3.1 with $P_1 = A + B$, $P_2 = AC$, and $|\mathcal{L}| = |B||C|$, but we first need to check its conditions

$$|A + B||AC|^2 \leq |B|^3|C|^3 \quad \text{and} \quad |A + B||B||C| \ll p^2. \quad (3.3)$$

Assumet that $|A + B||AC|^2 > |B|^3|C|^3$, which is the case when the first condition in (3.3) does not hold. Then we have $|A + B|^2|AC|^2 > |B|^3|C|^3$, which implies that

$$|A + B||AC| > |B|^{3/2}|C|^{3/2} \geq |A|^{11/5}|B|^{2/5}|C|^{2/5} > |A|^{8/5}|B|^{2/5}|C|^{2/5},$$

where the second inequality above follows from the assumption of Lemma 3.2 that $|B|, |C| \geq |A|$. Thus, to complete the proof of Lemma 3.2 we may assume that $|A + B||AC|^2 \leq |B|^3|C|^3$, which is the first condition in (3.3).

Next, we shall show that we may assume the second condition in (3.3) to prove Lemma 3.2. Since $|A + B||AC| \geq |B||C|$, we see that if $|B||C| > |A|^{8/5}|B|^{2/5}|C|^{2/5}$, then the conclusion of Lemma 3.2 holds. We also see that the conclusion of Lemma 3.2 holds if $|A + B| > |A|^{4/5}|B|^{1/5}|C|^{1/5}$, as we have assumed that $|AC| \geq |A + B|$ in (3.1). Hence, to prove Lemma 3.2 we may assume that $|B||C| \leq |A|^{8/5}|B|^{2/5}|C|^{2/5}$ (namely, $|B||C| \leq |A|^{8/3}$ and $|A + B| \leq |A|^{4/5}|B|^{1/5}|C|^{1/5}$). These conditions imply that

$$|A + B||B||C| \ll |A|^{4/5}|B|^{6/5}|C|^{6/5} \ll |A|^{20/5} \ll p^2,$$

where the last inequality follows from the assumption of Lemma 3.2 that $|A| \leq p^{1/2}$. Therefore, to prove Lemma 3.2 we may assume the second condition in (3.3).

In conclusion, by (3.1) and (3.3), we are able to apply Lemma 3.1 so that we obtain that

$$|A||B||C| \leq I(\mathcal{P}, \mathcal{L}) \ll |A + B|^{3/4}|AC|^{1/2}|B|^{3/4}|C|^{3/4} + |B||C|,$$

where we recall that the first inequality is given in (3.2). This leads to the following

$$|A||B|^{1/4}|C|^{1/4} \ll |A + B|^{3/4}|AC|^{1/2}.$$  

By (3.1), the above inequality implies that

$$|A + B||AC| \gg |A|^{8/5}|B|^{2/5}|C|^{2/5},$$

which completes the proof of Lemma 3.2.

\boxend

**Lemma 3.3.** Let $A$ be a set in $\mathbb{F}_p$ with $|A| \leq p^{1/2}$. Then, for any integer $d \geq 2$, we have

$$|A^d||dA| \gg |A|^{\frac{8}{5} - \frac{2}{5}d^{-1}},$$

where $A^d = A \cdots A$ ($d$ times), and $dA = A + \cdots + A$ ($d$ times).
Proof. We prove this lemma by induction on \(d\). The base case \(d = 2\) follows immediately from Lemma 3.2 with \(B = C = A\). Suppose that the statement holds for \(d - 1 \geq 2\). We now show that it also holds for \(d\). Indeed, from Lemma 3.2 we see that

\[
|A^d||dA| \gg |A|^{8/5}(|A^{d-1}|(d - 1)A)^{2/5}.
\]

By induction hypothesis, we obtain

\[
|A^{d-1}|(d - 1)A \gg |A|^{8/5} (|A|^{d-1})^{2/5} \gg |A|^\frac{8}{5} (\frac{d}{2})^{d-2}.
\]

This implies that

\[
|A^d||dA| \gg |A|^{8/5} (|A^{d-1}|(d - 1)A)^{2/5} \gg |A|^\frac{8}{5} (\frac{d}{2})^{d-1},
\]

which concludes the proof of the lemma. \(\square\)

We are now ready to give a proof of Theorem 1.5.

Proof of Theorem 1.5. Let \(M\) be a \(d \times d\) matrix in \(M_d(A)\) of the following form

\[
\begin{bmatrix}
  x_1 & x_1 & x_1 & \ldots & x_1 & x_1 \\
  x_2 & x_2 & x_2 & \ldots & x_2 & x_2 \\
  x_3 & x_3 & x_3 & \ldots & x_3 & x_3 \\
  \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
  x_{d-1} & x_{d-1} & x_{d-1} & \ldots & x_{d-1} & x_{d-1} \\
  x_d & x_d & x_d & \ldots & x_d & x_d \\
\end{bmatrix}.
\]

We have \(\text{Per}(M) = (d - 1)! (x_1 \cdots x_{d-1}) (x_d + \cdots + x_{dd})\). This implies that

\[
g_d(A) \geq |A^{d-1} \cdot ((d - 1)A + A)|.
\]

From Lemma 2.2 we have

\[
g_d(A) \geq |A^{d-1} \cdot ((d - 1)A + A)| \gg \min \left\{ |A|^{1/2} \left( |A^{d-1}|((d - 1)A) \right)^{1/2}, p \right\}.
\]

From Lemma 3.3 for \(d - 1\), the above inequality implies that

\[
g_d(A) \gg \min \left\{ |A|^\frac{1}{2} \left( |A|^{\frac{8}{5}} (\frac{d}{2})^{d-2} \right)^{1/2}, p \right\} = \min \left\{ |A|^{2 - \frac{1}{5}} (\frac{d}{2})^{d-2}, p \right\} = |A|^{2 - \frac{1}{5}} (\frac{d}{2})^{d-2},
\]

where the last equality follows by the assumption of Theorem 1.5 that \(|A| \leq p^{1/2}\). Thus the proof of Theorem 1.5 is complete. \(\square\)
4 Proof of Theorem 1.7

To prove Theorem 1.7, we make use of the following lemmas.

Lemma 4.1 ([10], Corollary 3.1). For $X, B \subset \mathbb{F}_p$ with $|X| \geq |B|$. We have

$$|X \pm B \cdot B| \gg \min \{|X|^{1/2}|B|, p\}.$$

Lemma 4.2 ([8], Theorem 2). For $A \subset \mathbb{F}_p$ with $|A| \leq p^{9/16}$, we have

$$|A - A|^{18}|AA|^9 \gtrsim |A|^{32}.$$

We are now ready to prove Theorem 1.7.

Proof of Theorem 1.7. It is clear that

$$F_2(A) = (A - A)(A - A) - (A - A)(A - A).$$

Suppose $|A - A| \geq |A|^{1+\epsilon}$ where $\epsilon = 1/90$. It follows from Lemmas 4.1 and 2.3 with $X = (A - A)(A - A)$ and $B = (A - A)$ that for $|A| \leq p^{9/16}$,

$$|F_2(A)| \gtrsim |A|^\frac{1}{2} + \frac{1}{180} + \epsilon,$$

and we are done. Thus we can assume that $|A - A| \leq |A|^{1+\epsilon}$. Let $a$ be an arbitrary element in $A$. Then we have

$$|A - A| = |(A - a) - (A - a)| \leq |A|^{1+\epsilon}.$$

Lemma 4.2 gives us that for $|A| \leq p^{9/16}$,

$$|(A - a)(A - a)| \gtrsim |A|^\frac{14}{9} - 2\epsilon.$$

Thus, if we apply Lemma 4.1 with $X = (A - a)(A - a)$ and $B = (A - A)$, then we are able to obtain the following

$$|(A - a)(A - a) - (A - A)(A - A)| \gtrsim |A|^{1 + \frac{5}{6} - \epsilon} \gtrsim |A|^{\frac{1}{2} + \frac{1}{180}},$$

where we used the condition that $|A| \leq p^{9/16}$.

The same argument also works for the case of $G_2(A)$. Thus we leave the remaining details to the reader. This concludes the proof of the theorem.

Acknowledgments

D. Koh was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(NRF-2015R1A1A1A05001374). T. Pham was supported by Swiss National Science Foundation grant P2ELP2175050. C-Y Shen was supported in part by MOST, through grant 104-2628-M-002-015 -MY4. The authors would like to thank Frank De Zeeuw for useful discussions.
References

[1] O. Ahmadi and I. E. Shparlinski, *Distribution of matrices with restricted entries over finite fields*, Indag. Math., 18 (2007), 327–337.

[2] D. Covert, D. Hart, A. Iosevich, D. Koh and M. Rudnev, *Generalized incidence theorems, homogeneous forms and sum-product estimates in finite fields*, European Journal of Combinatorics, 31(1) (2010), 306–319.

[3] A. Iosevich, O. Roche-Newton, M. Rudnev, *On discrete values of bilinear forms*, arXiv:1512.02670 (2015).

[4] D. D. Hieu, L. A. Vinh, *On distance sets and product sets in vector spaces over finite rings*, Michigan Math. J 62 (2013).

[5] D. Hart and A. Iosevich, *Sums and products in finite fields: an integral geometric viewpoint*, Contemp. Math., 464 (2008).

[6] D. Hart, A. Iosevich, D. Koh and M. Rudnev, *Averages over hyperplanes, sum-product theory in finite fields, and the Erdős-Falconer distance conjecture*, Trans. Amer. Math. Soc., 363 (2011) 3255–3275.

[7] Y. D. Karabulut, *Cayley Digraphs of Matrix Rings over Finite Fields*, arXiv:1710.08872, (2017).

[8] B. Murphy, G. Petridis, O. Roche-Newton, M. Rudnev, I. D. Shkredov, *New results on sum-product type growth over fields*, arXiv 1702.01003.

[9] O. Roche-Newton, M. Rudnev, I. D. Shkredov, *New sum-product type estimates over finite fields*, Advances in Mathematics 293 (2016): 589–605.

[10] T. Pham, L. A. Vinh, F. de Zeeuw, *Three-variable expanding polynomials and higher-dimensional distinct distances*, accepted in Combinatorica, 2017.

[11] I. E. Shparlinski, *On the solvability of bilinear equations in finite fields*, Glasg. Math. J., 50 (2008), 523–529.

[12] S. Stevens, F. de Zeeuw, *An improved point-line incidence bound over arbitrary fields*, Bulletin of the London Mathematical Society, 49 (5) (2017): 842–858.

[13] I. E. Shparlinski, *Arithmetic and geometric progressions in productsets over finite fields*, Bull. Aust. Math. Soc., 78 (2008), 357–364.

[14] L. A. Vinh, *Distribution of determinant of matrices with restricted entries over finite fields*, Journal of Combinatorics and Number Theory, 1(3), 203–212 (2010), (also published as a book chapter in Frontiers of Combinatorics and Number Theory, Vol 1).
[15] L. A. Vinh, *Singular matrices with restricted entries in vector spaces over finite fields*, Discrete Mathematics, **312**(2), 413–418.

[16] L. A. Vinh, *Spectra of product graphs and permanents of matrices over finite rings*, Pacific Journal of Mathematics, **267**(2) 2014, 479–487.

[17] L. A. Vinh, *On the permanents of matrices with restricted entries over finite fields*, SIAM Journal on Discrete Mathematics, **26**(3) (2012), 997–1007.