PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 146, Number 12, December 2018, Pages 5025–5034
https://doi.org/10.1090/proc/14177
Article electronically published on September 10, 2018

FOUR-VARIABLE EXPANDERS OVER THE PRIME FIELDS

DOOWON KOH, HOSSEIN NASSAJIAN MOJARRAD, THANG PHAM,
AND CLAUDIU VALCULESCU

(Communicated by Alexander Iosevich)

Abstract. Let $\mathbb{F}_p$ be a prime field of order $p > 2$, and let A be a set in $\mathbb{F}_p$ with very small size in terms of p. In this note, we show that the number of distinct cubic distances determined by points in $A \times A$ satisfies

$$|(A-A)^3 + (A-A)^3| \gg |A|^{8/7},$$

which improves a result due to Yazici, Murphy, Rudnev, and Shkredov. In addition, we investigate some new families of expanders in four and five variables. We also give an explicit exponent of a problem of Bukh and Tsimerman, namely, we prove that

$$\max\{|A+A|, |f(A,A)|\} \gg |A|^{6/5},$$

where $f(x,y)$ is a quadratic polynomial in $\mathbb{F}_p[x,y]$ that is not of the form $g(\alpha x + \beta y)$ for some univariate polynomial g.

1. Introduction

Let $p > 2$ be a prime, and let $\mathbb{F}_p$ be the finite field of order p. We denote the set of non-zero elements in $\mathbb{F}_p$ by $\mathbb{F}_p^*$. We say that a k-variable function $f(x_1, \ldots, x_k)$ is an *expander* if there are $\alpha > 1$, $\beta > 0$ such that for any sets $A_1, \ldots, A_k \subset \mathbb{F}_p$ of size $N \ll p^\beta$,

$$|f(A_1 \times \cdots \times A_k)| \gg N^\alpha.$$

We write $X \gg Y$ if $X \geq CY$ for some positive constant C.

As far as we know, there are few known results on two-variable expanders. For example, it has been shown by Yazici, Murphy, Rudnev, and Shkredov [1] that the polynomial $f(x,y) = x + y^2$ is an expander. More precisely, they proved that if $A \subset \mathbb{F}_p$ with $|A| \leq p^{5/8}$, then

$$|A + A^2| \gg |A|^{11/10}.$$

The authors in [1] also indicated that the polynomial $f(x,y) = x(y+1)$ is an expander. In particular, they established that $|A \cdot (A+1)| \gg |A|^{9/8}$.

These exponents have been improved in recent works. For instance, Stevens and de Zeeuw [18] showed that $|A \cdot (A+1)| \gg |A|^{6/5}$, and Pham, Vinh, and de Zeeuw [12] proved that $|A + A^2| \gg |A|^{6/5}$.

Received by the editors July 9, 2017.

2010 *Mathematics Subject Classification.* Primary 11T06, 11T55.

The first listed author was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (NRF-2015R1A1A1A05001374). The second listed author was supported by Swiss National Science Foundation grant P2ELP2175050. The third and fourth listed authors were partially supported by Swiss National Science Foundation grants 200020-162884 and 200021-175977.

Another expander in two variables has been investigated by Bourgain [6]. He proved that if $A, B \subset \mathbb{F}_p$ with $|A| = |B| = N = p^\epsilon$, $\epsilon > 0$, and $f(x, y) = x^2 + xy$, then $|f(A, B)| \gg N^{1+\delta}$ for some $\delta > 0$. An explicit exponent was given by Stevens and de Zeeuw [18], namely, they proved that $|f(A, B)| \gg N^{5/4}$ for $N \leq p^{2/3}$. We refer the reader to [5, 9, 19] and the references therein for two-variable expanders in large sets over arbitrary finite fields.

For three-variable expanders, there are several results which have been proved in recent years. Roche-Newton, Rudnev, and Shkredov [15] proved that

$$|A \cdot (A + A)| \gg |A|^{3/2},\ |A + A \cdot A| \gg |A|^{3/2}, \tag{1}$$

when $|A| \leq p^{2/3}$.

In [12], Pham, Vinh, and de Zeeuw obtained a more general result. More precisely, they showed that for $A, B, C \subset \mathbb{F}_p$ with $|A| = |B| = |C| = N \leq p^{2/3}$, and for any quadratic polynomial in three variables $f(x, y, z) \in \mathbb{F}_p[x, y, z]$ which is not of the form $g(h(x) + k(y) + l(z))$, we have

$$|f(A, B, C)| \gg N^{3/2}. \tag{2}$$

We notice that one can use the inequalities (1) and (2) to obtain some results on expanders in four variables. To see this, observe that the following estimates follow directly from (1) and (2):

$$|(A-A)\cdot(A-A)| \gg |A|^{3/2},\ |A\cdot A+A\cdot A| \gg |A|^{3/2},\ |(A-A)^2+(A-A)^2| \gg |A|^{3/2}.$$

A stronger version of the last inequality can be found in [14]. We refer the reader to [10] for a recent improvement on the size of $(A - A) \cdot (A - A)$.

In this note, we extend the methods from [1, 12, 15] to study different expanders in four variables over $\mathbb{F}_p$.

Yazici et al. [1] proved that if $A \subset \mathbb{F}_p$ with $|A| \leq p^{7/12}$, then the number of distinct cubic distances is at least $|A|^{36/35}$. Our first theorem is an improvement of this result.

Theorem 1.1. *Let $A \subset \mathbb{F}_p$ with $|A| \leq p^{7/12}$. Then we have*

$$|(A - A)^3 + (A - A)^3| \gg |A|^{8/7}.$$

In our next two theorems, we provide two more expanders in four variables.

Theorem 1.2. *Let A be a set in $\mathbb{F}_p$ with $|A| \leq p^{5/8}$, let $f(x) \in \mathbb{F}_p[x]$ be a quadratic polynomial, and let $g(x, y) \in \mathbb{F}_p[x, y]$ be a quadratic polynomial with a non-zero xy-term. Then we have*

$$|f(A) + A + g(A, A)| \gg |A|^{8/5}.$$

Theorem 1.3. *Let $1 \leq N \leq p^{4/7}$ be an integer, let h be a generator of $\mathbb{F}_p^*$, and let $g(x, y) \in \mathbb{F}_p[x, y]$ be a quadratic polynomial with a non-zero xy-term. Then we have*

$$|\{h^x + h^y + g(z, t) \colon 1 \leq x, y, z, t \leq N\}| \gg N^{7/4}.$$

Different families of expanders with superquadratic growth have been studied in recent literature. For instance, Balog, Roche-Newton, and Zhelezov [4] showed that for any $A \subset \mathbb{R}$ we have $|(A - A) \cdot (A - A) \cdot (A - A)| \gg |A|^{2+\frac{1}{8}} / \log^{\frac{17}{16}} |A|$. Murphy, Roche-Newton, and Shkredov [11] proved that for $A \subset \mathbb{R}$ we have $|(A + A + A + A)^2 + \log A| \gg |A|^2 / \log |A|$. In the following theorem, we obtain two more expanders in five variables with quadratic growth.

Theorem 1.4. *Let $\mathbb{F}_p$ be a prime field of order p. Suppose that h is a generator of $\mathbb{F}_p^*$, and $1 \leq N \leq p^{1/2}$ is an integer. Then the following two statements hold:*

(1) $|\{h^x(h^y+h^z+h^t+h^v)\colon 1 \leq x,y,z,t,v \leq N\}| \gg N^2$,

(2) $|\{x(h^y+h^z+h^t+h^v)\colon 1 \leq x,y,z,t,v \leq N\}| \gg N^2$.

For $A \subset \mathbb{F}_p$, the *sumset* of A is the set $A+A=\{a+b : a,b \in A\}$, and the *product set* of A is the set $A \cdot A = \{a \cdot b : a,b \in A\}$. In 2004, Bourgain, Katz, and Tao [3] proved that if $p^\delta < |A| < p^{1-\delta}$ where $0<\delta<1/2$, then

$$\max\{|A+A|, |A\cdot A|\} \geq c|A|^{1+\epsilon} \tag{3}$$

for some positive constants c and ϵ depending only on δ. Hart, Iosevich, and Solymosi [8] obtained bounds that give an explicit dependence of ϵ on δ. In [8], it is shown that if $|A+A|=m$ and $|A\cdot A|=n$, then

$$|A|^3 \leq \frac{cm^2n|A|}{p} + cp^{1/2}mn, \tag{4}$$

where c is some positive constant. Inequality (4) implies a non-trivial sum-product estimate when $p^{1/2} \ll |A| \ll p$. Vinh [21] and Garaev [7] improved the inequality (4) and as a result, obtained a better sum-product estimate.

Theorem 1.5 ([21]). *For $A \subset \mathbb{F}_p$, suppose that $|A+A|=m$, and $|A\cdot A|=n$, then*

$$|A|^2 \leq \frac{mn|A|}{p} + p^{1/2}\sqrt{mn}.$$

Corollary 1.6 ([21]). *For $A \subset \mathbb{F}_p$, then there is a positive constant c such that the following hold:*

(1) *If $p^{1/2} \ll |A| < p^{2/3}$, then*

$$\max\{|A+A|, |A\cdot A|\} \geq \frac{c|A|^2}{p^{1/2}}.$$

(2) *If $p^{2/3} \leq |A| \ll p$, then*

$$\max\{|A+A|, |A\cdot A|\} \geq c(p|A|)^{1/2}.$$

A more general statement of Corollary 1.6 has been established by Vu [22]. Before presenting his result, we need the following definition.

Definition 1.7. A polynomial $f(x,y) \in \mathbb{F}_p[x,y]$ is *degenerate* if it is of the form $Q(L(x_1,x_2))$ where Q is a one-variable polynomial and L is a linear form in x and y.

Vu [22] proved the following theorem.

Theorem 1.8 ([22]). *Let $f(x,y)$ be a non-degenerate polynomial of degree d in $\mathbb{F}_p[x,y]$. Then for any $A \subset \mathbb{F}_p$, we have*

$$\max\{|A+A|, |f(A,A)|\} \gg \min\left\{\frac{|A|^{3/2}}{dp^{1/4}}, \frac{p^{1/3}|A|^{2/3}}{d^{1/3}}\right\}.$$

We note that, in the case $f(x,y)=xy$, the lower bounds of Theorem 1.8 are weaker than those of Corollary 1.6. Theorem 1.8 is only non-trivial when $|A| \gg p^{1/2}$, and Theorem 1.8 also holds over arbitrary finite fields $\mathbb{F}_q$ with q a prime power. The reader can find a version of Theorem 1.8 over the real numbers in [17].

When $|A| \leq \sqrt{p}$ and $f(x,y)$ is a non-degenerate quadratic polynomial, Bukh and Tsimerman [5] obtained the following improvement.

Theorem 1.9 ([5])**.** *Let $f(x,y) \in \mathbb{F}_p[x,y]$ be a non-degenerate quadratic polynomial. For any $A \subset \mathbb{F}_p$ with $|A| \leq \sqrt{p}$, we have*

$$\max\{|A+A|, |f(A,A)|\} \gg |A|^{1+\epsilon} \tag{5}$$

for some $\epsilon > 0$.

There has been much progress on finding explicit exponents of the inequality (3) for small sets over recent years, and the best lower bound was given by Roche-Newton, Rudnev, and Shkredov [15]. More precisely, they showed that for $A \subset \mathbb{F}_p$ with $|A| \leq p^{5/8}$, the sumset and the product set satisfy

$$\max\{|A+A|, |A \cdot A|\} \gg |A|^{6/5}.$$

In this paper, we give an explicit exponent of the inequality (5) as follows.

Theorem 1.10. *Let $f(x,y) \in \mathbb{F}_p[x,y]$ be a non-degenerate quadratic polynomial. Let A be a set in $\mathbb{F}_p$ with $|A| \leq p^{5/8}$; then we have*

$$\max\{|A+A|, |f(A,A)|\} \gg |A|^{6/5}.$$

The rest of this paper is organized as follows. In Section 2, we mention the main tools in our proofs. We give a proof of Theorem 1.1 in Section 3. Proofs of Theorems 1.2, 1.3, and 1.4 are given in Section 4. In Section 5 we will give a proof of Theorem 1.10, and present a discussion on an improvement of Theorem 1.8 for large sets.

2. Tools

The main tool in our proofs is a point-plane incidence bound due to Rudnev [16], but we use a strengthened version of this theorem, proved by de Zeeuw in [23]. Let us first recall that if $\mathcal{R}$ is a set of points in $\mathbb{F}_p^3$ and $\mathcal{S}$ is a set of planes in $\mathbb{F}_p^3$, then the number of incidences between $\mathcal{R}$ and $\mathcal{S}$, denoted by $I(\mathcal{R},\mathcal{S})$, is the cardinality of the set $\{(r,s) \in \mathcal{R} \times \mathcal{S} : r \in s\}$.

Theorem 2.1 (Rudnev, [16])**.** *Let $\mathcal{R}$ be a set of points in $\mathbb{F}_p^3$ and let $\mathcal{S}$ be a set of planes in $\mathbb{F}_p^3$, with $|\mathcal{R}| \leq |\mathcal{S}|$ and $|\mathcal{R}| \ll p^2$. Suppose that there is no line that contains k points of $\mathcal{R}$ and is contained in k planes of $\mathcal{S}$. Then*

$$\mathcal{I}(\mathcal{R},\mathcal{S}) \ll |\mathcal{R}|^{1/2}|\mathcal{S}| + k|\mathcal{S}|.$$

The following lemma is known as the Plünnecke-Ruzsa inequality. A simple and elegant proof can be found in [13].

Lemma 2.2 (Plünnecke-Ruzsa)**.** *Let A, B be finite subsets of an abelian group such that $|A+B| \leq K|A|$. Then, for an arbitrary $0 < \delta < 1$, there is a non-empty set $X \subset A$ such that $|X| \geq (1-\delta)|A|$ and for any integer k one has*

$$|X + kB| \leq \left(\frac{K}{\delta}\right)^k |X|. \tag{6}$$

To prove Theorems 1.2–1.4, we need the following two lemmas. The first one follows from a result of Pham, Vinh, and de Zeeuw [12].

Lemma 2.3. *Let $g(x,y) \in \mathbb{F}_p[x,y]$ be a quadratic polynomial with a non-zero xy-term. Let $A, X \subset F$ with $|A| \leq |X|$. Then we have*

$$|g(A,A)+X| \gg \min\left\{|A||X|^{1/2}, p\right\}.$$

The second lemma we use is due to Yazici et al. and was proved in [1].

Lemma 2.4. *If $A, X \subset \mathbb{F}_p$ with $|X| \leq |A|$, then*

$$|X \cdot (A-A)| \gg \min\left\{|A||X|^{1/2}, p\right\}.$$

3. Proof of Theorem 1.1

We need the following result in order to prove Theorem 1.1.

Lemma 3.1. *Let $A, X \subset \mathbb{F}_p$ with $|A-A|^2|X| \leq p^2$. Then*

$$|\left\{(b-a)^3+a^3+x\colon a,b\in A, x\in X\right\}| \gg \min\left\{\frac{|X|^{1/2}|A|^4}{|A-A|^3}, \frac{|X||A|^5}{|A-A|^4}\right\}.$$

Proof. First note that

$$(b-a)^3+a^3 = 3b\left((a-b/2)^2+b^2/12\right) = 3b(t^2+b^2/12), \tag{7}$$

where $t=a-b/2$. Define $T=\{a-b/2\colon a,b\in A\}$, and let E be the number of solutions of the following equation:

$$(b-a)^3+a^3+x = (b'-a')^3+a'^3+x',\ \ a,a',b,b'\in A, x,x'\in X.$$

To bound E, we first define a set of points $\mathcal{R}$ and a set of planes $\mathcal{S}$ as follows:

$$\mathcal{R} = \{(t^2, b', -b'^3/4+x)\colon t\in T, b'\in A, x\in X\},$$

$$\mathcal{S} = \{3bX - 3t'^2Y + Z = -b^3/4+x'\colon t'\in T, x'\in X, b\in A\}.$$

It is clear that $|\mathcal{R}| = |\mathcal{S}| \ll |T||A||X|$, and $|T| \leq |A+A-A|$.

Lemma 2.2 implies that for any $0<\delta<1$, there exists a non-empty set $A'\subset A$ with $|A'| \geq (1-\delta)|A|$ satisfying

$$|A+A-A'| \ll \frac{|A-A|^2}{|A|}.$$

Since we can choose δ such that $|A'| = \Theta(|A|)$, [1] we can assume that $|T| \ll \frac{|A-A|^2}{|A|}$. This implies that

$$|\mathcal{R}|, |\mathcal{S}| \ll |A-A|^2|X|.$$

By the assumption, we have $|\mathcal{R}| \ll p^2$. This allows us to apply Theorem 2.1, assuming we can prove an upper bound on the maximum number k for which there is a line that contains k points of $\mathcal{R}$ and is contained in k planes of $\mathcal{S}$. The projection of $\mathcal{R}$ onto the first two coordinates is $\{t^2 : t\in T\}\times A$, so each line contains at most $\max\{|A|, |T|\}$ points of $\mathcal{R}$, unless it is vertical, in which case it could contain $|X|$ points of $\mathcal{R}$. However, the planes in $\mathcal{S}$ contain no vertical lines, so in this case the hypothesis of Theorem 2.1 is satisfied with $k=\max\{|A|,|T|\} \ll |A-A|^2/|A|$.

Therefore, Theorem 2.1 implies that

$$E \ll |X|^{3/2}|A-A|^3 + |X||A-A|^4/|A|.$$

[1] $X=\Theta(Y)$ means that there exist positive constants C_1 and C_2 such that $C_1Y \leq X \leq C_2Y$.

By the Cauchy-Schwarz inequality, we have

$$|\{(b-a)^3+a^3+x\colon a,b\in A,\ x\in X\}| \gg \frac{|A|^4|X|^2}{E} \gg \min\left\{\frac{|X|^{1/2}|A|^4}{|A-A|^3}, \frac{|X||A|^5}{|A-A|^4}\right\}.$$

This completes the proof of the lemma. □

Proof of Theorem 1.1. Since the cubic distance function is invariant under translations, we assume that $0\in A$. It follows from the Plünnecke-Ruzsa inequality that there exists a set $X\subset (A-A)^3$ with $|X|=\Theta(|(A-A)|)$ such that

$$|X+(A-A)^3+(A-A)^3| = |X+2(A-A)^3| \ll \frac{|(A-A)^3+(A-A)^3|^2}{|(A-A)^3|^2}|(A-A)^3|.$$

This implies that

$$|(A-A)^3+(A-A)^3|^2 \gg |A-A|\cdot|X+(A-A)^3+(A-A)^3|.$$

On the other hand, if $|A-A|^2|X|>p^2$, then we have $|A-A|\gg p^{2/3}$. This implies that $|A-A|\gg |A|^{8/7}$ since $|A|\le p^{7/12}$, and we are done. Thus, we may assume $|A-A|^2|X|\le p^2$, and it follows from Lemma 3.1 that

$$|X+(A-A)^3+(A-A)^3| \gg \frac{|A|^4}{|A-A|^{5/2}}.$$

Therefore, we obtain

$$|(A-A)^3+(A-A)^3|^2 \gg \frac{|A|^4}{|A-A|^{3/2}},$$

which leads to

$$\max\left\{|(A-A)^3+(A-A)^3|, |A-A|\right\} \gg |A|^{8/7}.$$

This concludes the proof of the theorem. □

4. Proofs of Theorems 1.2, 1.3, and 1.4

We use the following lemmas in the proofs of Theorems 1.2-1.4.

Lemma 4.1. *Let $f(x)\in\mathbb{F}_p[x]$ be a quadratic polynomial. For $A\subset\mathbb{F}_p$ with $|A|\le p^{5/8}$, we have*

$$|f(A)+A| \gg |A|^{6/5}.$$

Proof. Without loss of generality, we can assume that $f(x)=ax^2+bx$ with $a\ne 0$. Consider the following equation:

$$a(x-y)^2+b(x-y)+z=t, \tag{8}$$

with $x\in A+f(A)$, $y\in f(A)$, $z\in A$, and $t\in A+f(A)$. Since f is a quadratic polynomial, we have $|f(A)|=\Theta(|A|)$.

Note that for any $u,v,w\in A$, a solution of (8) is given by $x=u+f(v)\in A+f(A)$, $y=f(v)\in f(B)$, $z=w\in A$, and $t=w+f(u)\in A+f(A)$. Therefore, we have

$$|A|^3 \le \left|\{(x,y,z,t)\in (A+f(A))\times f(A)\times A\times (A+f(A)) : \\ a(x-y)^2+b(x-y)+z=t\}\right|. \tag{9}$$

If we define E to be the cardinality of the following set:

$$\left\{(x,y,z,x',y',z')\in ((A+f(A))\times f(A)\times A)^2\colon f(x-y)+z=f(x'-y')+z'\right\},$$

then (9) together with the Cauchy-Schwarz inequality give

$$\frac{|A|^6}{|A+f(A)|} \ll E. \tag{10}$$

To bound E, we use Theorem 2.1 for the following point set:

$$\mathcal{R} = \{(ax, y', bx + ax^2 + z - a(y')^2 + by') : (x, y', z) \in (A + f(A)) \times f(A) \times A\}$$

and the following set of planes:

$$\mathcal{S} = \{-2yX + 2ax'Y + Z = a(x')^2 + bx' + z' - ay^2 + by : \\ (x', y, z') \in (A + f(A)) \times f(A) \times A\}.$$

Note that if $|A + f(A)| \gg |A|^{6/5}$, then we are already done. Therefore, we can assume that $|A+f(A)| \ll |A|^{6/5}$, from which we obtain $|\mathcal{R}| = |A+f(A)||f(A)||A| \ll |A|^{16/5} \ll p^2$, since $|A| \ll p^{5/8}$. The projection of $\mathcal{R}$ onto the first two coordinates is $(A+f(A))\times f(A)$, so each line contains at most $\max\{|A+f(A)|, |f(A)|\} = |A+f(A)|$ points of $\mathcal{R}$, unless it is vertical, in which case it may contain $|A|$ points of $\mathcal{R}$. However, the planes in $\mathcal{S}$ contain no vertical lines, so in this case the hypothesis of Theorem 2.1 is satisfied with $k = |A + f(A)|$. Thus, Theorem 2.1 implies that

$$E \ll I(\mathcal{R}, \mathcal{S}) \ll |A + f(A)|^{3/2}|A|^3 + |A + f(A)|^2|A|^2. \tag{11}$$

If $|A+f(A)|^2|A|^2$ is asymptotically larger than $|A+f(A)|^{3/2}|A|^3$, then $|A+f(A)| \gg |A|^2$, so we are done. Otherwise, we can assume that $|A + f(A)|^{3/2}|A|^3$ is larger than $|A + f(A)|^2|A|^2$, so combining (10) and (11) gives

$$\frac{|A|^6}{|A+f(A)|} \ll |A + f(A)|^{3/2}|A|^3,$$

which leads to

$$|f(A) + A| \gg |A|^{6/5}.$$

This completes the proof of the lemma. □

Lemma 4.2. *Let $\mathbb{F}_p$ be a prime field of order p, and suppose that h is a generator of $\mathbb{F}_p^*$, and $1 \leq N \leq p^{2/3}$ is an integer. Then*

$$|\{h^x + h^y : 1 \leq x, y \leq N\}| \gg N^{3/2}.$$

Proof. Define $A := \{h^x : 1 \leq x \leq N/2\}$, and $X := \{h^x : 1 \leq x \leq N\}$. Then one can check that

$$|\,\{h^x + h^y : 1 \leq x, y \leq N\}\,| \gg |A \cdot A + X|.$$

Thus the lemma follows directly from Lemma 2.3. □

Proofs of Theorems 1.2, 1.3, *and* 1.4. Theorem 1.2 follows from Lemmas 2.3 and 4.1. Theorem 1.3 follows directly from Lemmas 2.3 and 4.2. Theorem 1.4 follows from Lemmas 2.4 and 4.2. □

5. Proof of Theorem 1.10

To prove Theorem 1.10, we use the following lemma, which follows directly from Lemmas 2.2 and 2.3 in [12]. We refer the reader to [12] for a detailed proof.

Lemma 5.1. *Let $f(x,y,z)\in\mathbb{F}_p[x,y,z]$ be a quadratic polynomial that depends on each variable and is not of the form $g(h(x)+k(y)+l(z))$. Let $A,B,C\subset\mathbb{F}_p$ with $|A|=|B|\le|C|$ and $|A||B||C|\ll p^2$. Then we have*

$$\begin{aligned}&\left|\left\{(x,y,z,x',y',z')\in(A\times B\times C)^2\colon f(x,y,z)=f(x',y',z')\right\}\right|\\&\qquad\le(|A||B||C|)^{3/2}+|A||B||C|^2.\end{aligned}$$

We are now ready to give a proof of Theorem 1.10.

Proof of Theorem 1.10. Without loss of generality, we assume that $f(x,y)=ax^2+by^2+cxy+dx+ey$ with $a\ne 0$. Let $f'(x,y,z):=f(z-x,y)$. Consider the following equation:

$$f'(x,y,z)=t, \tag{12}$$

with $x\in A, y\in A, z\in A+A, t\in f(A,A)$.

Note that for any $u,v,w\in A$, a solution of (12) is given by $x=u\in A$, $y=v\in A$, $z=u+w\in A+A$, and $t=f(w,v)\in f(A,A)$. Thus, we have

$$|A|^3\ll\left|\{(x,y,z,t)\in A\times A\times(A+A)\times f(A,A): f'(x,y,z)=t\}\right|. \tag{13}$$

Let E be the cardinality of the following set:

$$\left\{(x,y,z,x',y',z')\in(A\times A\times(A+A))^2\colon f'(x,y,z)=f'(x',y',z')\right\}.$$

Then (13) and the Cauchy-Schwarz inequality give

$$\frac{|A|^6}{|f(A,A)|}\ll E. \tag{14}$$

Before applying Lemma 5.1, we need to show that $f'(x,y,z)$ is not of the form $g'(h'(x)+k'(y)+l'(z))$. By the contradiction, suppose

$$f'(x,y,z)=g'(h'(x)+k'(y)+l'(z)).$$

Then g' is a polynomial of degree 2 since $a\ne 0$. Thus, h', k', and l' are linear polynomials. So we can write $f'(x,y,z)$ as

$$f'(x,y,z)=g'(\lambda_1x+\lambda_2y+\lambda_3z+\lambda_4)$$

for some $\lambda_1,\lambda_2,\lambda_3,\lambda_4\in\mathbb{F}_p$. Since g' is a polynomial of degree 2, without loss of generality, we assume that $g'(x)=x^2+\lambda_5x+\lambda_6$ for some $\lambda_5,\lambda_6\in\mathbb{F}_p$. It follows from the definition of f' that

$$\lambda_1^2=\lambda_3^2=a,\ 2\lambda_1\cdot\lambda_3=-2a.$$

This implies that $\lambda_1=-\lambda_3$. Hence, f' can be presented as

$$f'(x,y,z)=g'(\lambda_3(z-x)+\lambda_2y+\lambda_4).$$

From here, we can rearrange the coefficients of g' such that $g'(\lambda_3(z-x)+\lambda_2y+\lambda_4)=g''(\lambda_3(z-x)+\lambda_2y)$ for some $g''\in\mathbb{F}_p[x]$. This leads to

$$f(z-x,y)=g''(\lambda_3(z-x)+\lambda_2y),$$

which contradicts the assumption of the theorem.

In other words, we have that $f'(x,y,z)$ is not of the form $g'(h'(x)+k'(y)+l'(z))$.

If $|A|^2|A+A| \gg p^2$, then we have $|A+A| \gg |A|^{6/5}$ since $|A| \leq p^{5/8}$, and we are done. Thus we can assume that $|A|^2|A+A| \ll p^2$. Lemma 5.1 with $B = A$ and $C = A + A$ implies that

$$E \leq |A|^3|A+A|^{3/2} + |A|^2|A+A|^2.$$

Therefore, the theorem follows from the inequality (14). □

We note that if we use the point-plane incidence bound due to Vinh [21] for large sets in the proofs of Lemmas 2.2 and 2.3 in [12], then we are able to obtain the following version of Lemma 5.1 for large sets.

Lemma 5.2. *Let $\mathbb{F}_q$ be an arbitrary finite field. Let $f(x,y,z) \in \mathbb{F}_q[x,y,z]$ be a quadratic polynomial that depends on each variable and is not of the form*

$$g(h(x) + k(y) + l(z)).$$

Let $A, B, C \subset \mathbb{F}_q$; then we have

$$\left|\left\{(x,y,z,x',y',z') \in (A \times B \times C)^2 \colon f(x,y,z) = f(x',y',z')\right\}\right| \\ \leq \frac{(|A||B||C|)^2}{q} + q|A||B||C|.$$

One can follow identically the proof of Theorem 1.10 with Lemma 5.2 to obtain the following improvement of Vu's result for quadratic polynomials. We leave the detailed proof to the reader.

Theorem 5.3. *Let $\mathbb{F}_q$ be an arbitrary finite field. Let $f(x,y) \in \mathbb{F}_q[x,y]$ be a non-degenerate quadratic polynomial. Let A be a set in $\mathbb{F}_q$; then we have*

$$\max\{|A+A|, |f(A,A)|\} \gg \min\left\{\frac{|A|^2}{q^{1/2}}, q^{1/3}|A|^{2/3}\right\}.$$

Acknowledgment

The authors would like to thank Frank de Zeeuw for useful discussions and comments.

References

[1] E. Aksoy Yazici, B. Murphy, M. Rudnev, and I. Shkredov, *Growth estimates in positive characteristic via collisions*, to appear in International Mathematics Research Notices. Also in arXiv:1512.06613, 2015.

[2] E. Aksoy Yazici, *Sum-Product Type Estimates for Subsets of Finite Valuation Rings*, arXiv:1701.08101, 2016.

[3] J. Bourgain, N. Katz, and T. Tao, *A sum-product estimate in finite fields, and applications*, Geom. Funct. Anal. **14** (2004), no. 1, 27–57, DOI 10.1007/s00039-004-0451-1. MR2053599

[4] Antal Balog, Oliver Roche-Newton, and Dmitry Zhelezov, *Expanders with superquadratic growth*, Electron. J. Combin. **24** (2017), no. 3, Paper 3.14, 17. MR3691531

[5] Boris Bukh and Jacob Tsimerman, *Sum-product estimates for rational functions*, Proc. Lond. Math. Soc. (3) **104** (2012), no. 1, 1–26, DOI 10.1112/plms/pdr018. MR2876962

[6] J. Bourgain, *More on the sum-product phenomenon in prime fields and its applications*, Int. J. Number Theory **1** (2005), no. 1, 1–32, DOI 10.1142/S1793042105000108. MR2172328

[7] M. Z. Garaev, *The sum-product estimate for large subsets of prime fields*, Proc. Amer. Math. Soc. **136** (2008), no. 8, 2735–2739, DOI 10.1090/S0002-9939-08-09386-6. MR2399035

[8] Derrick Hart, Alex Iosevich, and Jozsef Solymosi, *Sum-product estimates in finite fields via Kloosterman sums*, Int. Math. Res. Not. IMRN **5** (2007), Art. ID rnm007, 14, DOI 10.1093/imrn/rnm007. MR2341599

[9] Derrick Hart, Liangpan Li, and Chun-Yen Shen, *Fourier analysis and expanding phenomena in finite fields*, Proc. Amer. Math. Soc. **141** (2013), no. 2, 461–473, DOI 10.1090/S0002-9939-2012-11338-3. MR2996950

[10] Oliver Roche-Newton, Misha Rudnev, and Ilya D. Shkredov, *New sum-product type estimates over finite fields*, Adv. Math. **293** (2016), 589–605, DOI 10.1016/j.aim.2016.02.019. MR3474329

[11] Brendan Murphy, Oliver Roche-Newton, and Ilya D. Shkredov, *Variations on the sum-product problem II*, SIAM J. Discrete Math. **31** (2017), no. 3, 1878–1894, DOI 10.1137/17M112316X. MR3691216

[12] T. Pham, L. A. Vinh, F. de Zeeuw, *Three-variable expanding polynomials and higher-dimensional distinct distances*, arXiv:1612.09032, 2016.

[13] Giorgis Petridis, *New proofs of Plünnecke-type estimates for product sets in groups*, Combinatorica **32** (2012), no. 6, 721–733, DOI 10.1007/s00493-012-2818-5. MR3063158

[14] Giorgis Petridis, *Pinned algebraic distances determined by Cartesian products in $\mathbb{F}_p^2$*, Proc. Amer. Math. Soc. **145** (2017), no. 11, 4639–4645, DOI 10.1090/proc/13649. MR3691983

[15] Oliver Roche-Newton, Misha Rudnev, and Ilya D. Shkredov, *New sum-product type estimates over finite fields*, Adv. Math. **293** (2016), 589–605, DOI 10.1016/j.aim.2016.02.019. MR3474329

[16] Misha Rudnev, *On the Number of Incidences Between Points and Planes in Three Dimensions*, Combinatorica **38** (2018), no. 1, 219–254, DOI 10.1007/s00493-016-3329-6. MR3776354

[17] Chun-Yen Shen, *Algebraic methods in sum-product phenomena*, Israel J. Math. **188** (2012), 123–130, DOI 10.1007/s11856-011-0096-3. MR2897726

[18] Sophie Stevens and Frank de Zeeuw, *An improved point-line incidence bound over arbitrary fields*, Bull. Lond. Math. Soc. **49** (2017), no. 5, 842–858, DOI 10.1112/blms.12077. MR3742451

[19] Terence Tao, *The sum-product phenomenon in arbitrary rings*, Contrib. Discrete Math. **4** (2009), no. 2, 59–82. MR2592424

[20] Le Anh Vinh, *On four-variable expanders in finite fields*, SIAM J. Discrete Math. **27** (2013), no. 4, 2038–2048, DOI 10.1137/120892015. MR3138096

[21] Le Anh Vinh, *The Szemerédi-Trotter type theorem and the sum-product estimate in finite fields*, European J. Combin. **32** (2011), no. 8, 1177–1181, DOI 10.1016/j.ejc.2011.06.008. MR2838005

[22] Van H. Vu, *Sum-product estimates via directed expanders*, Math. Res. Lett. **15** (2008), no. 2, 375–388, DOI 10.4310/MRL.2008.v15.n2.a14. MR2385648

[23] F. de Zeeuw, *A short proof of Rudnev's point-plane incidence bound*, arXiv:1612.02719, 2016.

[24] D. Zhelezov, *On additive shifts of multiplicative almost-subgroups in finite fields*, to appear in Proceedings of the American Mathematical Society, 2017.

Department of Mathematics, Chungbuk National University, Cheongju City, Chungbuk-Do, South Korea
Email address: koh131@chungbuk.ac.kr

Institute of Mathematics, École Polytechnique Fédérale de Lausanne, Lausanne CH 1015 Lausanne, Switzerland
Email address: hossein.mojarrad@epfl.ch

Institute of Mathematics, École Polytechnique Fédérale de Lausanne, Lausanne CH 1015 Lausanne, Switzerland
Email address: phamanhthang.vnu@gmail.com

Institute of Mathematics, École Polytechnique Fédérale de Lausanne, Lausanne CH 1015 Lausanne, Switzerland
Email address: adrian.valculescu@epfl.ch