On the structure of distance sets over prime fields

Thang Pham[*] Andrew Suk[†]

January 1, 2019

Abstract

Let $\mathbb{F}_q$ be a finite field of order q and $\mathcal{E}$ be a set in $\mathbb{F}_q^d$. The *distance set* of $\mathcal{E}$, denoted by $\Delta(\mathcal{E})$, is the set of distinct distances determined by the pairs of points in $\mathcal{E}$. Very recently, Iosevich, Koh, and Parshall (2018) proved that if $|\mathcal{E}| \gg q^{d/2}$, then the *quotient set* of $\Delta(\mathcal{E})$ satisfies

$$\left|\frac{\Delta(\mathcal{E})}{\Delta(\mathcal{E})}\right| = \left|\left\{\frac{a}{b} \colon a, b \in \Delta(\mathcal{E}), b \neq 0\right\}\right| \gg q.$$

In this paper, we break the exponent $d/2$ when $\mathcal{E}$ is a Cartesian product of sets over a prime field. More precisely, let p be a prime and $A \subset \mathbb{F}_p$. If $\mathcal{E} = A^d \subset \mathbb{F}_p^d$ and $|\mathcal{E}| \gg p^{\frac{d}{2}-\varepsilon}$ for some $\varepsilon > 0$, then we have

$$\left|\frac{\Delta(\mathcal{E})}{\Delta(\mathcal{E})}\right|, \ |\Delta(\mathcal{E}) \cdot \Delta(\mathcal{E})| \gg p.$$

Such improvements are not possible over arbitrary finite fields. These results give us a better understanding about the structure of distance sets and the Erdős-Falconer distance conjecture over finite fields.

1 Introduction

Let q be an odd prime power, and $\mathbb{F}_q$ be the finite field of order q. For any two points $\mathbf{x} = (x_1, \ldots, x_d)$ and $\mathbf{y} = (y_1, \ldots, y_d)$ in $\mathbb{F}_q^d$, the distance between them is defined by

$$||\mathbf{x} - \mathbf{y}|| = (x_1 - y_1)^2 + \cdots + (x_d - y_d)^2.$$

This function is not a norm, but it is invariant under translations, rotations, and reflections. Given a set $\mathcal{E} \subset \mathbb{F}_q^d$, we define the *distance set*

$$\Delta(\mathcal{E}) := \{||\mathbf{x} - \mathbf{y}|| \colon \mathbf{x}, \mathbf{y} \in \mathcal{E}\}.$$

[*] Department of Mathematics, University of California at San Diego, La Jolla, CA, 92093 USA. Supported by Swiss National Science Foundation grant P2ELP2-175050. Email: v9pham@ucsd.edu

[†] Department of Mathematics, University of California at San Diego, La Jolla, CA, 92093 USA. Supported by an NSF CAREER award and an Alfred Sloan Fellowship. Email: asuk@ucsd.edu

The finite field variant of the Erdős distinct distances problem was first studied by Bourgain, Katz, and Tao in [1], who proved the following theorem.

Theorem 1.1 (**Bourgain-Katz-Tao**, [1])**.** *Suppose $q \equiv 3 \mod 4$ is a prime. Let $\mathcal{E}$ be a set in $\mathbb{F}_q^2$. If $|\mathcal{E}| = q^\alpha$ with $0 < \alpha < 2$, then we have*

$$|\Delta(\mathcal{E})| \gg |\mathcal{E}|^{\frac{1}{2}+\varepsilon},$$

for some positive $\varepsilon = \varepsilon(\alpha) > 0$.

Throughout this paper, we write $X \gg Y$ if there is a positive constant C such that $X \geq CY$, and $X \ll Y$ if $Y \gg X$.

Iosevich and Rudnev [8] observed that the conclusion of Theorem 1.1 can not be extended to arbitrary finite fields in general. For instance, when q is a square, i.e. $q = p^2$ for some prime p, we can choose $\mathcal{E} = \mathbb{F}_p \times \mathbb{F}_p$. One can check that in this case, we have $|\Delta(\mathcal{E})| = |\mathcal{E}|^{1/2}$. Furthermore, if -1 is a square number in $\mathbb{F}_q$, i.e. $-1 = i^2$ for some $i \in \mathbb{F}_q$, then we can choose $\mathcal{E} = \{(t, it) \in \mathbb{F}_q^2 : t \in \mathbb{F}_q\}$. This set only gives us the distance zero. In light of these constructions, Iosevich and Rudnev [8] made the following reformulation of the distinct distances problem, in the spirit of the Falconer distance conjecture [6].[1]

Problem 1.2. *Let $\mathcal{E}$ be a set in $\mathbb{F}_q^d$, and $\Delta(\mathcal{E})$ be the set of distinct distances determined by the pairs of points in $\mathcal{E}$. How large does $\mathcal{E}$ need to be to guarantee that $|\Delta(\mathcal{E})| \gg q$?*

This problem is now known as the Erdős-Falconer distance problem over finite fields. Using Fourier methods, Iosevich and Rudnev [8] proved that if $|\mathcal{E}| \gg q^{(d+1)/2}$, then the distance set $\Delta(\mathcal{E})$ covers a positive proportion of all elements in $\mathbb{F}_q$, that is, $|\Delta(\mathcal{E})| \gg q$. Hart et al. [7] showed that we can have all distances whenever $|\mathcal{E}| \geq 4q^{\frac{d+1}{2}}$. They also gave constructions for the sharpness of the exponent $(d+1)/2$ in odd dimensions. However, in even dimensions, it is still possible to break the $(d+1)/2$ exponent. Chapman et al. [4] made the first step in this direction by showing that if $d = 2$, then the exponent $3/2$ can be decreased to $4/3$, which is directly in line with Wolff's result [16] for the Falconer distance problem in $\mathbb{R}^2$. It has been conjectured that in even dimensions, the assumption $|\mathcal{E}| \gg q^{\frac{d}{2}}$ is sufficient for $|\Delta(\mathcal{E})| \gg q$.

In a recent work, Iosevich, Koh, and Parshall [9] proved that the exponent $d/2$ holds for the *quotient set* of the distance set, which is defined by

$$\frac{\Delta(\mathcal{E})}{\Delta(\mathcal{E})} = \left\{\frac{a}{b} \colon a, b \in \Delta(\mathcal{E}), b \neq 0\right\}.$$

The statement of their result is as follows.

Theorem 1.3 (**Iosevich-Koh-Parshall**, [9])**.** *Let $\mathbb{F}_q$ be a finite field of order q, and $\mathcal{E}$ be a set in $\mathbb{F}_q^d$.*

[1] The Falconer distance conjecture states that for any compact set $\mathcal{E} \subset \mathbb{R}^d$ with the Hausdorff dimension greater than $d/2$, the distance set $\Delta(\mathcal{E})$ has positive Lebesgue measure.

1. *If $d \geq 2$ is even and $|\mathcal{E}| \geq 9q^{d/2}$, then we have*
$$\frac{\Delta(\mathcal{E})}{\Delta(\mathcal{E})} = \mathbb{F}_q.$$

2. *If $d \geq 3$ is odd and $|\mathcal{E}| \geq 6q^{d/2}$, then we have*
$$\{0\} \cup \mathbb{F}_q^+ \subset \frac{\Delta(\mathcal{E})}{\Delta(\mathcal{E})},$$
where $\mathbb{F}_q^+ = \{x^2 \colon x \in \mathbb{F}_q, x \neq 0\}$.

Notice that the condition $|\mathcal{E}| \gg q^{d/2}$ in Theorem 1.3 is sharp over arbitrary finite fields, even if we wish to cover only a positive proportion of all elements in $\mathbb{F}_q$. Indeed, suppose that $q = p^2$ for some prime p. By setting $\mathcal{E} = \mathbb{F}_p^d$, we have $|\mathcal{E}| = q^{\frac{d}{2}}$ and $|\Delta(\mathcal{E})/\Delta(\mathcal{E})| = |\mathbb{F}_p| = q^{1/2}$. We refer the interested reader to [9] for more discussions.

Let us also remark that it seems difficult apply the methods in [9] to the analogous problem of having the *product set* of the distance set cover a positive proportion of $\mathbb{F}_q$. Using a different approach, Iosevich and Koh [10] proved that for $\mathcal{E} \subset \mathbb{F}_q^d$, if $|\mathcal{E}| \gg q^{\frac{d}{2}+\frac{1}{4}}$, then
$$\Delta(\mathcal{E}) \cdot \Delta(\mathcal{E}) = \{a \cdot b \colon a, b \in \Delta(\mathcal{E})\} = \mathbb{F}_q.$$

The main purpose of this paper is to show that if $\mathcal{E}$ is a Cartesian product of sets over a prime field $\mathbb{F}_p$, we can break the exponent $d/2$ and still guarantee that
$$\left|\frac{\Delta(\mathcal{E})}{\Delta(\mathcal{E})}\right|, \ |\Delta(\mathcal{E}) \cdot \Delta(\mathcal{E})| \gg p.$$

Our first two results are for the case of the quotient set, in even and odd dimensions.

Theorem 1.4. *Let $\mathbb{F}_p$ be a prime field, and $A \subset \mathbb{F}_p$. Then for $\mathcal{E} = A^d \subset \mathbb{F}_p^d$ with $d = 2k$, $k \geq 2 \in \mathbb{N}$, we have*
$$\left|\frac{\Delta(\mathcal{E})}{\Delta(\mathcal{E})}\right| = \left|\left\{\frac{a}{b} \colon a, b \in \Delta(\mathcal{E}), b \neq 0\right\}\right| \geq \frac{p}{3},$$
whenever $|\mathcal{E}| \gg p^{\frac{d}{2}-\varepsilon}$ with $\varepsilon = \frac{d}{2} \cdot \frac{2^k - 2^{k-1} - 1}{2^k - 1}$.

Theorem 1.5. *Let $\mathbb{F}_p$ be a prime field, and $A \subset \mathbb{F}_p$. Then for $\mathcal{E} = A^d \subset \mathbb{F}_p^d$ with $d = 2k+1$, $k \geq 2 \in \mathbb{N}$, we have*
$$\left|\frac{\Delta(\mathcal{E})}{\Delta(\mathcal{E})}\right| = \left|\left\{\frac{a}{b} \colon a, b \in \Delta(\mathcal{E}), b \neq 0\right\}\right| \geq \frac{p}{3},$$
whenever $|\mathcal{E}| \gg p^{\frac{d}{2}-\varepsilon}$ with $\varepsilon = d \cdot \frac{2^{k+2} - 2^{k+1} - 3}{2^{k+3} - 6}$.

Our next two theorems are for the case of the product set, in even and odd dimensions.

Theorem 1.6. *Let $\mathbb{F}_p$ be a prime field, and $A \subset \mathbb{F}_p$. Then for $\mathcal{E} = A^d \subset \mathbb{F}_p^d$ with $d = 2k$, $k \geq 2 \in \mathbb{N}$, we have*

$$|\Delta(\mathcal{E}) \cdot \Delta(\mathcal{E})| = |\{a \cdot b \colon a, b \in \Delta(\mathcal{E})\}| \gg p,$$

whenever $|\mathcal{E}| \gg p^{\frac{d}{2}-\varepsilon}$ with $\varepsilon = \frac{d}{2} \cdot \frac{2^{k+1}-5}{5 \cdot 2^k - 5}$.

Theorem 1.7. *Let $\mathbb{F}_p$ be a prime field, and $A \subset \mathbb{F}_p$. Then for $\mathcal{E} = A^d \subset \mathbb{F}_p^d$ with $d = 2k+1$, $k \geq 2 \in \mathbb{N}$, we have*

$$|\Delta(\mathcal{E}) \cdot \Delta(\mathcal{E})| = |\{a \cdot b \colon a, b \in \Delta(\mathcal{E})\}| \gg p,$$

whenever $|\mathcal{E}| \gg p^{\frac{d}{2}-\varepsilon}$ with $\varepsilon = d \cdot \frac{2^{k+1}-5}{10(2^k-1)}$.

Let us remark that it is not possible to break the exponent $d/2$ for both quotient set and product set of the distance set over arbitrary finite fields. For instance, suppose $q = p^2$, and $\mathcal{E} = A^d \subset \mathbb{F}_q$ with $A = \mathbb{F}_p$. Then we have $|\mathcal{E}| = q^{\frac{d}{2}}$ and $|\Delta(\mathcal{E}) \cdot \Delta(\mathcal{E})| = |\frac{\Delta(\mathcal{E})}{\Delta(\mathcal{E})}| = p = q^{1/2}$.

2 Proofs of Theorem 1.4 and Theorem 1.5

To prove Theorems 1.4 and 1.5, we make use of the following results. The first result was given by the first author, Vinh and De Zeeuw [13]. The second was given by Balog [2].

Lemma 2.1. *Let $\mathbb{F}_p$ be a prime field, and A be a set in $\mathbb{F}_p$. For $k \geq 2$, we have*

$$\left|\Delta(A^k)\right| \gg \min\left\{|A|^{2-\frac{1}{2^{k-1}}}, p\right\}.$$

Lemma 2.2. *Let $\mathbb{F}_q$ be an arbitrary finite field of order q, and B, C be sets in $\mathbb{F}_q$. Suppose that $B \cap C = \emptyset$ and $|B||C| \gg q$, then we have*

$$\left|\frac{B-C}{B-C}\right| \geq \frac{q}{3}.$$

Lemma 2.3. *Let $\mathbb{F}_p$ be a prime field, and A be a set in $\mathbb{F}_p$. For $k_1, k_2 \geq 2$, we have*

$$\Delta(A^{k_1+k_2}) = \Delta(A^{k_1}) + \Delta(A^{k_2}).$$

Proof. We first show that $\Delta(A^{k_1+k_2}) \subset \Delta(A^{k_1}) + \Delta(A^{k_2})$. Let t be an element in $\Delta(A^{k_1+k_2})$. We now prove that t can be presented as a sum of two elements $t_1 \in \Delta(A^{k_1})$ and $t_2 \in \Delta(A^{k_2})$. Indeed, suppose that

$$t = (x_1 - y_1)^2 + \cdots + (x_{k_1} - y_{k_1})^2 + (x_{k_1+1} - y_{k_1+1})^2 + \cdots + (x_{k_1+k_2} - y_{k_1+k_2})^2,$$

where $x_i, y_i \in A$. Set $t_1 = (x_1 - y_1)^2 + \cdots + (x_{k_1} - y_{k_1})^2$ and $t_2 = (x_{k_1+1} - y_{k_1+1})^2 + \cdots + (x_{k_1+k_2} - y_{k_1+k_2})^2$. It is clear that t_1 is an element in $\Delta(A^{k_1})$, t_2 is an element in $\Delta(A^{k_2})$, and $t = t_1 + t_2$. This implies that $\Delta(A^{k_1+k_2}) \subset \Delta(A^{k_1}) + \Delta(A^{k_2})$.

We now prove the inverse direction $\Delta(A^{k_1}) + \Delta(A^{k_2}) \subset \Delta(A^{k_1+k_2})$.

Let t_1 be an element in $\Delta(A^{k_1})$, t_2 be an element in $\Delta(A^{k_2})$. Suppose that t_1 is the distance between $x=(x_1,\ldots,x_{k_1})\in A^{k_1}$ and $y=(y_1,\ldots,y_{k_1})\in A^{k_1}$, t_2 is the distance between $z=(z_1,\ldots,z_{k_2})\in A^{k_2}$ and $y=(t_1,\ldots,t_{k_2})\in A^{k_2}$. Then we have t_1+t_2 is the distance between $(x_1,\ldots,x_{k_1},z_1\ldots,z_{k_2})\in A^{k_1+k_2}$ and $(y_1,\ldots,y_{k_1},t_1,\ldots,t_{k_2})\in A^{k_1+k_2}$. Hence, $t_1+t_2\in\Delta(A^{k_1+k_2})$. In other words, $\Delta(A^{k_1})+\Delta(A^{k_2)}\subset\Delta(A^{k_1+k_2})$. □

We are ready to prove Theorem 1.4.

Proof of Theorem 1.4: Let X be a subset of $\Delta(A^k)$ such that for any $x\in X$ we have $-x\notin X$. Without loss of generality, we assume that $|X|\ge|\Delta(A^k)|/2$. From Lemma 2.3, we have $\Delta(\mathcal{E})=\Delta(A^k)+\Delta(A^k)$. Hence,

$$\left|\frac{\Delta(\mathcal{E})}{\Delta(\mathcal{E})}\right|\ge\left|\frac{X-(-X)}{X-(-X)}\right|.$$

Set $B=X$ and $C=-X$. It follows from our setting that $B\cap C=\emptyset$. Therefore, applying Lemma 2.2, we have

$$\left|\frac{\Delta(\mathcal{E})}{\Delta(\mathcal{E})}\right|\ge\frac{p}{3},$$

whenever $|B||C|\gg p$. Since $|B|=|C|=|X|\gg|\Delta(A^k)|$, the condition $|B||C|\gg p$ is equivalent to $|\Delta(A^k)|^2\gg p$. Lemma 2.1 tells us that

$$\left|\Delta(A^k)\right|\gg\min\left\{|A|^{2-\frac{1}{2^{k-1}}},p\right\}.$$

Hence, by a direct computation, if $|\mathcal{E}|\gg p^{\frac{d}{2}-\varepsilon}$ with $\varepsilon=\frac{d}{2}\cdot\frac{2^k-2^{k-1}-1}{2^k-1}$, then $|A|\gg p^{\frac{2^{k-2}}{2^k-1}}$. So $|\Delta(A^k)|^2\gg p$. This concludes the proof of the theorem. □

Proof of Theorem 1.5: Let B be a subset of $\Delta(A^k)$ such that $|B|\ge|\Delta(A^k)|/2$ and $B\cap -B=\emptyset$. Let C be a subset of $\Delta(A^{k+1})$ such that $B\subset C$, $C\cap -C=\emptyset$, and $|C|\ge|\Delta(A^{k+1})|/2$. We note that the condition $B\subset C$ can be satisfied since $\Delta(A^k)\subset\Delta(A^{k+1})$. As in the proof of Theorem 1.4, we have

$$\left|\frac{\Delta(\mathcal{E})}{\Delta(\mathcal{E})}\right|\ge\left|\frac{B-(-C)}{B-(-C)}\right|.$$

The condition $B\cap -C=\emptyset$ holds since $B\subset C$ and $C\cap -C=\emptyset$. Lemma 2.2 implies that if $|B||C|\gg p$, then we have

$$\left|\frac{\Delta(\mathcal{E})}{\Delta(\mathcal{E})}\right|\ge\frac{p}{3}.$$

Thus, in the rest of the proof, we will clarify the condition $|B||C|\gg p$. It follows from our setting that $|B||C|\gg|\Delta(A^k)|\cdot|\Delta(A^{k+1})|$. Applying Lemma 2.1, we get

$$|\Delta(A^k)|\cdot|\Delta(A^{k+1})|\gg\min\left\{p^2,|A|^{\frac{2^{k+2}-3}{2^k}},p|A|^{2-\frac{1}{2^k}},p|A|^{2-\frac{1}{2^{k-1}}}\right\}.$$

In other words, if $|A| \gg p^{\frac{2^k}{2^{k+2}-3}}$, i.e. $|\mathcal{E}| \gg p^{\frac{d}{2}-\varepsilon}$ with $\varepsilon = d \cdot \frac{2^{k+2}-2^{k+1}-3}{2^{k+3}-6}$, the condition $|B||C| \gg p$ holds. This completes the proof of the theorem. □

3 Proofs of Theorem 1.6 and Theorem 1.7

The ideas in the proofs of Theorems 1.6 and 1.7 are similar to those of Theorems 1.4 and 1.5, except that we will use the following lemma in the place of Lemma 2.2.

Lemma 3.1 (Proof of Theorem F, [12])**.** *Let $\mathbb{F}_p$ be a prime field of order p, and $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ be sets in $\mathbb{F}_p$. Let $N(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$ be the number of 8-tuples $(a, b, c, d, a', b', c', d') \in (\mathcal{A} \times \mathcal{B} \times \mathcal{C} \times \mathcal{D})^2$ such that $(a-b)(c-d) = (a'-b')(c'-d')$. Suppose that $|\mathcal{A}| = |\mathcal{C}|$, $|\mathcal{B}| = |\mathcal{D}|$, and $|\mathcal{A}| \le |\mathcal{B}|$, then we have*

$$N(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}) \ll \frac{|\mathcal{A}|^2|\mathcal{B}|^2|\mathcal{C}|^2|\mathcal{D}|^2}{p} + p^{1/2}(|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}|)^{11/8} + \frac{|\mathcal{A}|^{11/4}|\mathcal{B}|^4}{p^{1/4}} + (|\mathcal{A}||\mathcal{C}||\mathcal{D}|)^2.$$

Proof of Theorem 1.6: From Lemma 2.3, we have $\Delta(\mathcal{E}) = \Delta(A^k) + \Delta(A^k)$. Thus

$$|\Delta(\mathcal{E}) \cdot \Delta(\mathcal{E})| = |\left(\Delta(A^k) + \Delta(A^k)\right) \cdot \left(\Delta(A^k) + \Delta(A^k)\right)| = |(\mathcal{A} - \mathcal{B})(\mathcal{C} - \mathcal{D})|,$$

where $\mathcal{A} = \mathcal{C} = \Delta(A^k)$, $\mathcal{B} = \mathcal{D} = -\Delta(A^k)$.

By the Cauchy-Schwarz inequality, we have

$$|(\mathcal{A} - \mathcal{B})(\mathcal{C} - \mathcal{D})| \ge \frac{|\mathcal{A}|^2|\mathcal{B}|^2|\mathcal{C}|^2|\mathcal{D}|^2}{N(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})}, \quad (1)$$

where $N(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$ is defined as in Lemma 3.1.

Lemma 2.1 gives us that

$$|\mathcal{A}| = |\mathcal{B}| = |\mathcal{C}| = |\mathcal{D}| \gg \min\left\{|A|^{2-\frac{1}{2^{k-1}}}, p\right\}.$$

Since $|\mathcal{E}| \gg p^{\frac{d}{2}-\varepsilon}$ with $\varepsilon = \frac{d}{2} \cdot \frac{2^{k+1}-5}{5 \cdot 2^k - 5}$, which is equivalent with $|A| \gg p^{\frac{3 \cdot 2^{k-1}}{5 \cdot (2^k-1)}}$, we obtain $|\mathcal{A}| = |\mathcal{B}| = |\mathcal{C}| = |\mathcal{D}| \gg p^{3/5}$. Under this condition and Lemma 3.1, we achieve

$$N(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}) \ll \frac{|\mathcal{A}|^2|\mathcal{B}|^2|\mathcal{C}|^2|\mathcal{D}|^2}{p}. \quad (2)$$

Putting (1) and (2) together, the theorem follows. □

Proof of Theorem 1.7: Since $\mathcal{E} = A^{2k+1}$, we have $|\Delta(\mathcal{E}) \cdot \Delta(\mathcal{E})| \geq |\Delta(A^{2k}) \cdot \Delta(A^{2k})|$. It follows from the proof of Theorem 1.6 that if $|A| > p^{\frac{3 \cdot 2^{k-1}}{5(2^k-1)}}$, then

$$|\Delta(A^{2k}) \cdot \Delta(A^{2k})| \gg p.$$

Therefore, under the condition $|\mathcal{E}| \gg p^{\frac{d}{2}-\varepsilon}$ with $\varepsilon = (2k+1) \cdot \frac{2^{k+1}-5}{10(2^k-1)} = d \cdot \frac{2^{k+1}-5}{10(2^k-1)}$, we obtain

$$|\Delta(\mathcal{E}) \cdot \Delta(\mathcal{E})| \geq |\Delta(A^{2k}) \cdot \Delta(A^{2k})| \gg p.$$

This completes the proof of the theorem. □

4 Concluding remarks

In the setting of arbitrary finite fields $\mathbb{F}_q$, Do and Vinh [5] proved that for $A \subset \mathbb{F}_q$ with $|A| \gg q^{1/2}$, we have

$$|\Delta(A^k)| \gg \min\left\{q, \frac{|A|^{2k-1}}{q^{k-1}}\right\}.$$

One can follow the proofs of Theorems 1.4 and 1.5 to show that

$$\left|\frac{\Delta(A^d)}{\Delta(A^d)}\right|, \left|\frac{\Delta(A^{d+1})}{\Delta(A^{d+1})}\right| \geq \frac{q}{3},$$

under the condition $|A| \gg q^{1/2}$. This matches Theorem 1.3.

In the proof of Theorem 1.7, one might try to set $\mathcal{A} = \Delta(A^k) = \mathcal{C}, \mathcal{B} = \mathcal{D} = -\Delta(A^{k+1})$. This is clear that $|\mathcal{A}| \leq |\mathcal{B}|$. However, in Lemma 3.1, in order to get $N(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}) \ll |\mathcal{A}|^2|\mathcal{B}|^2|\mathcal{C}|^2|\mathcal{D}|^2p^{-1}$, we need the condition $|\mathcal{A}| > p^{3/5}$. This implies that $|\mathcal{A}|, |\mathcal{B}|, |\mathcal{C}|, |\mathcal{D}| > p^{3/5}$. So we get the same condition on the size of A as in the proof of Theorem 1.6. One might also try to apply the bound $|X(Y+Z)| \gg \min\left\{(|X||Y||Z|)^{1/2}, p\right\}$ in [15] with $X = \Delta(\mathcal{E}), Y = Z = \Delta(A^k)$ or $Y = \Delta(A^k), Z = \Delta(A^{k+1})$ to bound $|\Delta(\mathcal{E}) \cdot \Delta(\mathcal{E})|$, but the exponents are worse than those of Theorems 1.6 and 1.7.

It is not known if Problem 1.2, the Erdős-Falconer distance problem over finite fields, changes over prime fields. As we mentioned in the introduction, the exponent $(d+1)/2$ can not be improved for odd dimensions over arbitrary finite fields. The constructions in [7], which demonstrates the sharpness of the exponent $(d+1)/2$, were based on the structures of subfields. However, in light of our results, one may be able to break this exponent over prime fields.

References

[1] J. Bourgain, N. Katz, T. Tao, *A sum-product estimate in finite fields, and applications*, Geom. Funct. Anal. **14** (2004), 27–57.

[2] A. Balog, *Another sum-product estimate in finite fields*, Proceedings of the Steklov Institute of Mathematics, **280**(2) (2013): 23–29.

[3] M. Bennett, D. Hart, A. Iosevich, J. Pakianathan, M. Rudnev, *Group actions and geometric combinatorics in $\mathbb{F}_q^d$*, Forum Mathematicum, Volume **29** (2016), Issue 1, pp. 91–110.

[4] J. Chapman, M.B. Erdogan, D. Hart, A. Iosevich, D. Koh, *Pinned distance sets, k-simplices, Wolffs exponent in finite fields and sum-product estimates*, Math. Z. **271** (2012) 63–93.

[5] H. Do, L. A. Vinh, *On distance sets and product sets in vector spaces over finite rings*, Michigan Math. J., **62** (2013), 779–792.

[6] K. J. *Falconer, On the Hausdorff dimensions of distance sets*, Mathematika, **32** (1985),206–212.

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

[8] A. Iosevich, M. Rudnev, *Erdős distance problem in vector spaces over finite fields*, Trans. Am. Math. Soc. **359** (2007), 6127–6142.

[9] A. Iosevich, D. Koh, H. Parshall, *On the quotient set of the distance set*, to appear in Moscow Journal of Combinatorial Number Theory, 2018.

[10] A. Iosevich, D. Koh, *On the product set of the distance set*, preprint 2017.

[11] D. Koh and H. Sun, *Distance sets of two subsets of vector spaces over finite fields*, Proceedings of the American Mathematical Society, **143**(4) (2015), 1679–1692.

[12] B. Murphy, G. Petridis, *Products of Differences over Arbitrary Finite Fields*, arXiv:1705.06581 (2017).

[13] T. Pham, L. A. Vinh, F. De Zeeuw, *Three-variable expanding polynomials and higher-dimensional distinct distances*, Combinatorica (2017): 1–16.

[14] L. A. Vinh, *The solvability of norm, bilinear and quadratic equations over finite fields via spectra of graphs*, Forum Mathematicum, Vol. **26** (2014), Issue 1, pp. 141–175.

[15] S. Stevens, F. De Zeeuw, *An improved pointline incidence bound over arbitrary fields*, Bulletin of the London Mathematical Society, **49**(5) (2017): 842–858.

[16] T. Wolff, *Decay of circular means of Fourier transforms of measures*, Int. Math. Res. Not. (1999), no. 10, 547–567.