CrossMark

The Generalized k-Resultant Modulus Set Problem in Finite Fields

David Covert[1] · Doowon Koh[2] · Youngjin Pi[2]

Abstract

Let $\mathbb{F}_q^d$ be the d-dimensional vector space over the finite field $\mathbb{F}_q$ with q elements. Given k sets $E_j \subset \mathbb{F}_q^d$ for $j = 1, 2, \ldots, k$, the generalized k-resultant modulus set, denoted by $\Delta_k(E_1, E_2, \ldots, E_k)$, is defined by $\Delta_k(E_1, E_2, \ldots, E_k) = \{\|\mathbf{x}^1 + \mathbf{x}^2 + \cdots + \mathbf{x}^k\| \in \mathbb{F}_q : \mathbf{x}^j \in E_j, \ j = 1, 2, \ldots, k\}$, where $\|\mathbf{y}\| = \mathbf{y}_1^2 + \cdots + \mathbf{y}_d^2$ for $\mathbf{y} = (\mathbf{y}_1, \ldots, \mathbf{y}_d) \in \mathbb{F}_q^d$. We prove that if $\prod_{j=1}^{3} |E_j| \geq Cq^{3\left(\frac{d+1}{2} - \frac{1}{6d+2}\right)}$ for $d = 4, 6$ with a sufficiently large constant $C > 0$, then $|\Delta_3(E_1, E_2, E_3)| \geq cq$ for some constant $0 < c \leq 1$, and if $\prod_{j=1}^{4} |E_j| \geq Cq^{4\left(\frac{d+1}{2} - \frac{1}{6d+2}\right)}$ for even $d \geq 8$, then $|\Delta_4(E_1, E_2, E_3, E_4)| \geq cq$. This generalizes the previous result in [3]. We also show that if $\prod_{j=1}^{3} |E_j| \geq Cq^{3\left(\frac{d+1}{2} - \frac{1}{9d-18}\right)}$ for even $d \geq 8$, then $|\Delta_3(E_1, E_2, E_3)| \geq cq$. This result improves the previous work in [3] by removing $\varepsilon > 0$ from the exponent. The new ingredient in our proof is an improved L^3-restriction estimate for spheres.

Keywords Erdős distance problem · k-Resultant modulus set · Restriction theorems · Finite fields

✉ Doowon Koh
koh131@chungbuk.ac.kr

David Covert
covertdj@umsl.edu

Youngjin Pi
pi@chungbuk.ac.kr

[1] Department of Mathematics and Computer Science, University of Missouri-St. Louis, St. Louis, MO 63121, USA

[2] Department of Mathematics, Chungbuk National University, Cheongju, Chungbuk 28644, Korea

Birkhäuser

Mathematics Subject Classification 52C10 · 42B05 · 11T23

1 Introduction

The Erdős distance problem asks us to determine the minimal number of distinct distances between any N points in $\mathbb{R}^d$. This problem was initially posed by Paul Erdős [5] who conjectured that $g_2(N) \gtrsim N/\sqrt{\log N}$, and $g_d(N) \gtrsim N^{2/d}$ for $d \geq 3$, where $g_d(N)$ denotes the minimal number of distinct distances between N distinct points of $\mathbb{R}^d$, and $X \gtrsim Y$ for $X, Y > 0$ means that there is a constant $C > 0$ independent of N such that $CX \geq Y$. This conjecture in two dimension was resolved up to the logarithmic factor by Guth and Katz [7]. However, the problem is still open in higher dimensions.

In [1] Bourgain, Katz, and Tao studied the finite field analog of the Erdős distance problem. Let $\mathbb{F}_q^d$ be the d-dimensional vector space over the finite field $\mathbb{F}_q$ with q elements. Throughout this paper we always assume that the characteristic of $\mathbb{F}_q$ is strictly greater than two. For a set $E \subset \mathbb{F}_q^d$, the distance set, denoted by $\Delta_2(E)$, is defined as

$$\Delta_2(E) = \{\|\mathbf{x} - \mathbf{y}\| \in \mathbb{F}_q : \mathbf{x}, \mathbf{y} \in E\},$$

where $\|\alpha\| = \alpha_1^2 + \cdots + \alpha_d^2$ for $\alpha = (\alpha_1, \ldots, \alpha_d) \in \mathbb{F}_q^d$. With this definition of the distance set, Bourgain, Katz, and Tao [1] proved that if $q \equiv 3 \pmod 4$ is prime and $E \subset \mathbb{F}_q^2$ with $q^\delta \lesssim |E| \lesssim q^{2-\delta}$ for $\delta > 0$, then there exists $\epsilon = \epsilon(\delta)$ such that $|\Delta_2(E)| \geq |E|^{1/2+\epsilon}$. Here we recall that $A \lesssim B$ for $A, B > 0$ means that there exists a constant $C > 0$ independent of q such that $A \leq CB$, and we write $B \gtrsim A$ for $A \lesssim B$. We also use $A \sim B$ if $\lim_{q \to \infty} A/B = 1$. This result was obtained by finding the connection between incidence geometry in $\mathbb{F}_q^2$ and the distance set. Unfortunately, it is not simple to find the relationship between δ and ϵ from their proof. Furthermore, if $E = \mathbb{F}_q^2$, then $|\Delta_2(E)| = \sqrt{|E|}$, which shows that the exponent $1/2$ can not be generically improved. If -1 is a square in $\mathbb{F}_q$, another unpleasant example exists with the finite field Erdős distance problem. For instance, let $E = \{(t, it) \in \mathbb{F}_q^2 : t \in \mathbb{F}_q\}$, where i denotes an element of $\mathbb{F}_q$ such that $i^2 = -1$. Then it is straightforward to see that $|E| = q$ and $|\Delta_2(E)| = |\{0\}| = 1$. In view of aforementioned examples, Iosevich and Rudnev [12] reformulated the Erdős distance problem in general finite field setting as follows.

Question 1.1 *Let $E \subset \mathbb{F}_q^d$. What is the smallest exponent $\beta > 0$ such that if $|E| \geq Cq^\beta$ for a sufficiently large constant $C > 0$ then $|\Delta(E)| \geq cq$ for some $0 < c \leq 1$?*

The problem in this question is called the Erdős-Falconer distance problem in the finite field setting. In [12], it was shown that $\beta \leq (d+1)/2$ for all dimensions $d \geq 2$. The authors in [9] proved that $\beta = (d+1)/2$ for general odd dimensions $d \geq 3$. On the other hand, they conjectured that if the dimension $d \geq 2$ is even, then β can be improved to $d/2$. In dimension two, the authors in [2] applied the sharp finite field restriction estimate for the circle on the plane so that they show $\beta \leq 4/3$ which

improves the exponent $(d + 1)/2$, a sharp exponent in general odd dimensions d. Considering the perpendicular bisector of two points in a set of $\mathbb{F}_q^2$, the authors in [8] proved that the exponent $4/3$ holds for the pinned distance problem case. However, in higher even dimensions $d \geq 4$, the exponent $(d + 1)/2$ has not been improved. To demonstrate some possibility that the exponent $(d + 1)/2$ could be improved for even dimensions $d \geq 4$, the authors in [3] introduced a k-resultant modulus set which generalizes the distance set in the sense that any k points can be selected from a set $E \subset \mathbb{F}_q^d$ to determine an object similar to a distance. More precisely, for a set $E \subset \mathbb{F}_q^d$ we define a k-resultant modulus set $\Delta_k(E)$ as

$$\Delta_k(E) = \left\{ \| \pm \mathbf{x}^1 \pm \mathbf{x}^2 + \cdots \pm \mathbf{x}^k \| \in \mathbb{F}_q : \mathbf{x}^j \in E \right\},$$

where $\|\mathbf{y}\| = \mathbf{y}_1^2 + \cdots + \mathbf{y}_d^2 \in \mathbb{F}_q$ for $\mathbf{y} = (\mathbf{y}_1, \ldots, \mathbf{y}_d) \in \mathbb{F}_q^d$. Since the sign "$\pm$" does not affect on our results in this paper, we shall simply takes "$+$" signs. That is, we will use the definition

$$\Delta_k(E) = \left\{ \|\mathbf{x}^1 + \mathbf{x}^2 + \cdots + \mathbf{x}^k\| \in \mathbb{F}_q : \mathbf{x}^j \in E \right\}$$

for consistency. With this definition of the k-resultant modulus set, the following question was proposed in [3].

Question 1.2 *Let $E \subset \mathbb{F}_q^d$ and $k \geq 2$ be an integer. What is the smallest exponent $\gamma > 0$ such that if $|E| \geq Cq^\gamma$ for a sufficiently large constant $C > 0$, then $|\Delta_k(E)| \geq cq$ for some $0 < c \leq 1$.*

This problem is called the k-resultant modulus problem. When $k = 2$, this question is simply the finite field Erdős-Falconer distance problem, and in this sense the k-resultant modulus problem is a direct generalization of the distance problem. It is obvious that the smallest exponent $\beta > 0$ in Question 1.1 is greater than or equal to the smallest exponent $\gamma > 0$ in Question 1.2. However, authors in [3] conjectured that γ must be equal to β. This conjecture means that the solution γ of Question 1.2 is independent of the integer $k \geq 2$. Namely, it is conjectured that the solution of the Erdős-Falconer distance problem is the same as that of the k-resultant modulus problem. In fact, authors in [4] provided a simple example which shows that $\gamma = \beta = (d + 1)/2$ for any integer $k \geq 2$ in odd dimensions $d \geq 3$ provided that -1 is a square number in $\mathbb{F}_q$ and the conclusion of Question 1.2 is replaced by $|\Delta_k(E)| = q$. On the other hand, authors in [3] conjectured that the smallest exponent γ in Question 1.2 is $d/2$ for even dimensions $d \geq 2$ and all integers $k \geq 2$. As a partial credence to this conjecture, they showed that if $k \geq 3$ and the dimension d is even, then one can improve the exponent $(d+1)/2$ which is sharp in odd dimensional case. More precisely, the following results were proved.

Theorem 1.3 ([3]) *Let $E \subset \mathbb{F}_q^d$. Suppose that C is a sufficiently large constant. Then the following statements hold:*
(1) If $d = 4$ or 6, and $|E| \geq Cq^{\frac{d+1}{2} - \frac{1}{6d+2}}$, then $|\Delta_3(E)| \geq cq$ for some $0 < c \leq 1$.

(2) *If $d \geq 8$ is even and $|E| \geq Cq^{\frac{d+1}{2} - \frac{1}{6d+2}}$, then $|\Delta_4(E)| \geq cq$ for some $0 < c \leq 1$.*

(3) *If $d \geq 8$ is even, then for any $\varepsilon > 0$, there exists $C_\varepsilon > 0$ such that if $|E| \geq C_\varepsilon q^{\frac{d+1}{2} - \frac{1}{9d-18} + \varepsilon}$, then $|\Delta_3(E)| \geq cq$ for some $0 < c \leq 1$.*

The purpose of this paper is to generalize Theorem 1.3. In particular, in the general setting, we improve the third conclusion of Theorem 1.3 by removing the $\varepsilon > 0$ in the exponent.

The generalized Erdős-Falconer distance problem has been recently studied by considering the distances between any two sets $E_1, E_2 \subset \mathbb{F}_q^d$ (see, for example, [10,13–15,17–19]). Given two sets $E_1, E_2 \subset \mathbb{F}_q^d$, the generalized distance set $\Delta_2(E_1, E_2)$ is defined by

$$\Delta_2(E_1, E_2) = \left\{ \|\mathbf{x}^1 - \mathbf{x}^2\| \in \mathbb{F}_q : \mathbf{x}^1 \in E_1, \ \mathbf{x}^2 \in E_2 \right\}.$$

The generalized Erdős-Falconer distance problem is to determine the smallest exponent $\gamma_2 > 0$ such that if $E_1, E_2 \subset \mathbb{F}_q^d$ with $|E_1||E_2| \geq Cq^{\gamma_2}$ for a sufficiently large constant $C > 0$, then $|\Delta_2(E_1, E_2)| \geq cq$ for some $0 < c \leq 1$. From the Erdős-Falconer distance conjecture, it is natural to conjecture that the smallest exponent γ_2 is $d + 1$ for odd dimension $d \geq 3$ and d for even dimension $d \geq 2$. Shparlinski [17] obtained the exponent $d + 1$ for all dimensions $d \geq 2$. Thus, the generalized Erdős-Falconer distance conjecture was established in odd dimensions. On the other hand, the conjectured exponent d in even dimensions has not been obtained. The currently best known result is the exponent $d + 1$ for even dimensions d except for two dimensions. In dimension two the best known result is the exponent $8/3$ due to Koh and Shen [13].

We now consider a problem which extends both the generalized Erdős-Falconer distance problem and the k-resultant modulus set problem. For k sets $E_j \subset \mathbb{F}_q^d$, $j = 1, 2, \ldots, k$, we define the generalized k-resultant set $\Delta_k(E_1, \ldots, E_k)$ as

$$\Delta_k(E_1, \ldots, E_k) = \left\{ \|\mathbf{x}^1 + \mathbf{x}^2 + \cdots + \mathbf{x}^k\| \in \mathbb{F}_q : \mathbf{x}^j \in E_j, \ j = 1, 2, \ldots, k \right\}.$$

Problem 1.4 Let $k \geq 2$ be an integer. Suppose that $E_j \subset \mathbb{F}_q^d$, $j = 1, 2, \ldots, k$. Determine the smallest exponent $\gamma_k > 0$ such that if $\prod_{j=1}^{k} |E_j| \geq Cq^{\gamma_k}$ for a sufficiently large constant $C > 0$, then $|\Delta_k(E_1, E_2, \ldots, E_k)| \geq cq$ for some $0 < c \leq 1$.

We call this problem the generalized k-resultant modulus problem. As in the k-resultant modulus problem, we are only interested in studying this problem in even dimensions $d \geq 2$. If $q = p^2$ for some odd prime p, then $\mathbb{F}_q$ contains the subfield $\mathbb{F}_p$. In this case, if the dimension d is even and $E_j = \mathbb{F}_p^d$ for all $j = 1, 2, \ldots, k$, then $\prod_{j=1}^{k} |E_j| = q^{dk/2}$ and $|\Delta_k(E_1, E_2, \ldots, E_k)| = |\mathbb{F}_p| = p = \sqrt{q}$. This example proposes the following conjecture.

Conjecture 1.5 *Suppose that $d \geq 2$ is even and $k \geq 2$ is an integer. Then the smallest exponent γ_k in Problem 1.4 must be $\frac{kd}{2}$.*

1.1 Statement of the Main Result

As mentioned before, the known results on the generalized Erdős-Falconer distance problem says that if $k = 2$, then $2 \leq \gamma_k \leq 8/3$ for $d = 2$, and $d \leq \gamma_k \leq d + 1$ for even dimensions $d \geq 4$, where γ_k denotes the smallest exponent in Problem 1.4. In this paper we study the generalized k-resultant modulus problem for $k \geq 3$. Our main result is as follows.

Theorem 1.6 *Let $k \geq 3$ be an integer and $E_j \subset \mathbb{F}_q^d$ for $j = 1, 2, \ldots, k$. Assume that C is a sufficiently large constant. Then the following statements hold:*

(1) *If $d = 4$ or 6, and $\prod_{j=1}^{3} |E_j| \geq Cq^{3\left(\frac{d+1}{2} - \frac{1}{6d+2}\right)}$ then $|\Delta_3(E_1, E_2, E_3)| \gtrsim q$.*

(2) *If $d \geq 8$ is even and $\prod_{j=1}^{4} |E_j| \geq Cq^{4\left(\frac{d+1}{2} - \frac{1}{6d+2}\right)}$ then $|\Delta_4(E_1, E_2, E_3, E_4)| \gtrsim q$.*

(3) *If $d \geq 8$ is even, and $\prod_{j=1}^{3} |E_j| \geq Cq^{3\left(\frac{d+1}{2} - \frac{1}{9d-18}\right)}$, then $|\Delta_3(E_1, E_2, E_3)| \gtrsim q$.*

Taking $E_j = E \subset \mathbb{F}_q^d$ for all $j = 1, 2, \ldots, k$, the first and second conclusions of Theorem 1.3 follow immediately from (1), (2) of Theorem 1.6, respectively. Moreover, the third conclusion of Theorem 1.6 implies that the ε in the statement (3) of Theorem 1.3 is not necessary.

Theorem 1.6 also implies the following result.

Corollary 1.7 *For any integer $k \geq 4$, let $E_j \subset \mathbb{F}_q^d$ for $j = 1, 2, \ldots, k$. Assume that $C > 0$ is a sufficiently large constant. Then if $d \geq 4$ is even, and $\prod_{j=1}^{k} |E_j| \geq Cq^{k\left(\frac{d+1}{2} - \frac{1}{6d+2}\right)}$, we have $|\Delta_k(E_1, E_2, \ldots, E_k)| \gtrsim q$.*

Proof Without loss of generality, we may assume that $|E_1| \geq |E_2| \geq \cdots \geq |E_k|$. Notice that if $\prod_{j=1}^{k} |E_j| \geq Cq^{k\left(\frac{d+1}{2} - \frac{1}{6d+2}\right)}$, then $\prod_{j=1}^{k-1} |E_j| \gtrsim q^{(k-1)\left(\frac{d+1}{2} - \frac{1}{6d+2}\right)}$, and we have $|\Delta_{k-1}(E_1, \ldots, E_{k-1})| \leq |\Delta_k(E_1, \ldots, E_k)|$. Then the statement follows by induction argument with conclusions (1), (2) of Theorem 1.6. $\qquad\square$

2 Discrete Fourier Analysis

We shall use the discrete Fourier analysis to deduce the result of our main theorem, Theorem 1.6. In this section, we recall notation and basic concept in the discrete Fourier analysis. Throughout this paper, we shall denote by χ a nontrivial additive character of $\mathbb{F}_q$. Since our result is independent of the choice of the character χ, we assume that χ is always a fixed nontrivial additive character of $\mathbb{F}_q$. The orthogonality relation of χ states that

$$\sum_{\mathbf{x} \in \mathbb{F}_q^d} \chi(\mathbf{m} \cdot \mathbf{x}) = \begin{cases} 0 & \text{if } \mathbf{m} \neq (0, \ldots, 0) \\ q^d & \text{if } \mathbf{m} = (0, \ldots, 0), \end{cases}$$

where $\mathbf{m} \cdot \mathbf{x} := \sum_{j=1}^{d} \mathbf{m}_j \mathbf{x}_j$ for $\mathbf{m} = (\mathbf{m}_1, \ldots, \mathbf{m}_d)$, $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_d) \in \mathbb{F}_q^d$. Given a function $g : \mathbb{F}_q^d \to \mathbb{C}$, we shall denote by $\widetilde{g}$ the Fourier transform of g which is defined by

$$\widetilde{g}(\mathbf{x}) = \sum_{\mathbf{m}\in\mathbb{F}_q^d} g(\mathbf{m})\,\chi(-\mathbf{x}\cdot\mathbf{m}) \quad \text{for } \mathbf{x}\in\mathbb{F}_q^d. \tag{2.1}$$

On the other hand, we shall denote by $\widehat{f}$ the **normalized** Fourier transform of the function $f : \mathbb{F}_q^d \to \mathbb{C}$. Namely we define that

$$\widehat{f}(\mathbf{m}) = \frac{1}{q^d}\sum_{\mathbf{x}\in\mathbb{F}_q^d} f(\mathbf{x})\,\chi(-\mathbf{x}\cdot\mathbf{m}) \quad \text{for } \mathbf{m}\in\mathbb{F}_q^d.$$

In particular, if $\mathbf{m} = (0,\dots,0)$ and we take f as an indicator function of a set $E \subset \mathbb{F}_q^d$, then we see that

$$\widehat{E}(0,\dots,0) = \frac{|E|}{q^d}.$$

Here, and throughout this paper, we write $E(\mathbf{x})$ for the indicator function $1_E(\mathbf{x})$ of a set $E \subset \mathbb{F}_q^d$. We define the **normalized** inverse Fourier transform of f, denoted by $f^\vee$, as $f^\vee(\mathbf{m}) = \widehat{f}(-\mathbf{m})$ for $\mathbf{m} \in \mathbb{F}_q^d$. It is not hard to see that $\widetilde{(f^\vee)}(\mathbf{x}) = f(\mathbf{x})$ for $\mathbf{x} \in \mathbb{F}_q^d$. Namely, we obtain the Fourier inversion theorem:

$$f(\mathbf{x}) = \sum_{\mathbf{m}\in\mathbb{F}_q^d} \widehat{f}(\mathbf{m})\,\chi(\mathbf{m}\cdot\mathbf{x}) \quad \text{for } \mathbf{x}\in\mathbb{F}_q^d.$$

Using the orthogonality relation of the character χ, we see that

$$\sum_{\mathbf{m}\in\mathbb{F}_q^d} |\widehat{f}(\mathbf{m})|^2 = \frac{1}{q^d}\sum_{\mathbf{x}\in\mathbb{F}_q^d} |f(\mathbf{x})|^2.$$

We shall call this formula the Plancherel theorem. Notice that if we take f as an indicator function of a set $E \subset \mathbb{F}_q^d$, then the Plancherel theorem yields that

$$\sum_{\mathbf{m}\in\mathbb{F}_q^d} |\widehat{E}(\mathbf{m})|^2 = \frac{|E|}{q^d}.$$

Recall from Hölder's inequality that if $f_1, f_2 : \mathbb{F}_q^d \to \mathbb{C}$, then we have

$$\sum_{\mathbf{m}\in\mathbb{F}_q^d} |f_1(\mathbf{m})|\,|f_2(\mathbf{m})| \le \left(\sum_{\mathbf{m}\in\mathbb{F}_q^d} |f_1(\mathbf{m})|^{p_1}\right)^{\frac{1}{p_1}} \left(\sum_{\mathbf{m}\in\mathbb{F}_q^d} |f_2(\mathbf{m})|^{p_2}\right)^{\frac{1}{p_2}},$$

where $1 < p_1, p_2 < \infty$ and $1/p_1 + 1/p_2 = 1$. Applying Hölder's inequality repeatedly, we obtain that if $f_i : D \subset \mathbb{F}_q^d \to \mathbb{C}$ and $1 \le p_i < \infty$ for $i = 1, 2, \dots, k$ with $\sum_{i=1}^k \frac{1}{p_i} = 1$, then

$$\sum_{\mathbf{m}\in D}\left(\prod_{i=1}^{k}|f_i(\mathbf{m})|\right)\leq\prod_{i=1}^{k}\left(\sum_{\mathbf{m}\in D}|f_i(\mathbf{m})|^{p_i}\right)^{\frac{1}{p_i}}. \tag{2.2}$$

We refer to this formula as the generalized Hölder's inequality.

Lemma 2.1 *Let $k \geq 2$ be an integer. If $E_j \subset \mathbb{F}_q^d$ for all $j = 1, 2, \ldots, k$, then we have*

$$\sum_{\mathbf{m}\in\mathbb{F}_q^d}\left(\prod_{j=1}^{k}|\widehat{E_j}(\mathbf{m})|\right)\leq q^{-dk+d}\left(\prod_{j=1}^{k}|E_j|\right)^{\frac{k-1}{k}}.$$

Proof Notice that if $E \subset \mathbb{F}_q^d$ and $\mathbf{m} \in \mathbb{F}_q^d$, then $|\widehat{E}(\mathbf{m})| \leq |\widehat{E}(0, \ldots, 0)| = \frac{|E|}{q^d}$. Since $\sum_{j=1}^{k}\frac{1}{k} = 1$, applying generalized Hölder's inequality yields the desirable result:

$$\sum_{\mathbf{m}\in\mathbb{F}_q^d}\left(\prod_{j=1}^{k}|\widehat{E_j}(\mathbf{m})|\right)\leq\prod_{j=1}^{k}\left(\sum_{\mathbf{m}\in\mathbb{F}_q^d}|\widehat{E_j}(\mathbf{m})|^k\right)^{\frac{1}{k}}$$

$$\leq\prod_{j=1}^{k}\left(|\widehat{E_j}(0, \ldots, 0)|^{\frac{k-2}{k}}\left(\sum_{\mathbf{m}\in\mathbb{F}_q^d}|\widehat{E_j}(\mathbf{m})|^2\right)^{\frac{1}{k}}\right)$$

$$=\prod_{j=1}^{k}\left(\left(\frac{|E_j|}{q^d}\right)^{\frac{k-2}{k}}\left(\frac{|E_j|}{q^d}\right)^{\frac{1}{k}}\right)=q^{-dk+d}\left(\prod_{j=1}^{k}|E_j|\right)^{\frac{k-1}{k}}$$

$\square$

To estimate a lower bound of $|\Delta_k(E_1, \ldots, E_k)|$, we shall utilize the Fourier decay estimate on spheres. Recall that the sphere $S_t \subset \mathbb{F}_q^d$ for $t \in \mathbb{F}_q$ is defined by

$$S_t = \{\mathbf{x} \in \mathbb{F}_q^d : x_1^2 + \cdots + x_d^2 = t\}. \tag{2.3}$$

It is not hard to see that $|S_t| = q^{d-1}(1+o(1))$ for $d \geq 3$ and $t \in \mathbb{F}_q$ (see Theorem 6.26 and Theorem 6.27 in [16]). It is well known that the value of $\widehat{S_t}(\mathbf{m})$ can be written in terms of the Gauss and the Kloosterman sum. In particular, when the dimension d is even, the following result can be obtained from Lemma 4 in [11].

Lemma 2.2 *Let $d \geq 2$ be even. If $t \in \mathbb{F}_q$ and $\boldsymbol{m} \in \mathbb{F}_q^d$, then we have*

$$\widehat{S_t}(\boldsymbol{m}) = q^{-1}\delta_0(\boldsymbol{m}) + q^{-d-1} G^d \sum_{\ell\in\mathbb{F}_q^*}\chi\left(t\ell + \frac{\|\boldsymbol{m}\|}{4\ell}\right),$$

where $\delta_0(\boldsymbol{m}) = 1$ for $\boldsymbol{m} = (0, \ldots, 0)$ and $\delta_0(\boldsymbol{m}) = 0$ otherwise, and G denotes the Gauss sum

$$G = \sum_{s \in \mathbb{F}_q^*} \eta(s) \, \chi(s),$$

where η is the quadratic character of $\mathbb{F}_q$, and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. In particular, we have

$$\widehat{S_0}(\boldsymbol{m}) = q^{-1}\delta_0(\boldsymbol{m}) + q^{-d-1} G^d \sum_{\ell \in \mathbb{F}_q^*} \chi(\|\boldsymbol{m}\|\ell) \quad \text{for } \boldsymbol{m} \in \mathbb{F}_q^d. \tag{2.4}$$

We shall invoke the following result which was given in Proposition 2.2 in [15].

Lemma 2.3 *If $\boldsymbol{m}, \boldsymbol{v} \in \mathbb{F}_q^d$, then we have*

$$\sum_{t \in \mathbb{F}_q} \widehat{S_t}(\boldsymbol{m}) \, \overline{\widehat{S_t}}(\boldsymbol{v}) = q^{-1}\delta_0(\boldsymbol{m}) \, \delta_0(\boldsymbol{v}) + q^{-d-1} \sum_{s \in \mathbb{F}_q^*} \chi(s(\|\boldsymbol{m}\| - \|\boldsymbol{v}\|)).$$

3 Formula for a Lower Bound of $|\Delta_k(E_1, \ldots, E_k)|$

This section devotes to proving the following result which is useful to deduce a lower bound of $|\Delta_k(E_1, \ldots, E_k)|$.

Theorem 3.1 *Let $d \geq 2$ be even and $k \geq 2$ be an integer. If $E_j \subset \mathbb{F}_q^d$ for $j = 1, 2, \ldots, k$ and $\prod_{j=1}^k |E_j| \geq 3^k q^{\frac{dk}{2}}$, then we have*

$$|\Delta_k(E_1, \ldots, E_k)| \gtrsim \min \left\{ q, \; \frac{\left(\prod_{j=1}^k |E_j|\right)^{\frac{k+1}{k}}}{q^{dk}\left(\max_{r \in \mathbb{F}_q^*} \prod_{j=1}^k \left(\sum_{\boldsymbol{v} \in S_r} |\widehat{E_j}(\boldsymbol{v})|^k\right)^{\frac{1}{k}}\right)} \right\}.$$

Proof For each $t \in \mathbb{F}_q$, we define a counting function $\nu_k(t)$ by

$$\nu_k(t) = \left| \{(\mathbf{x}^1, \mathbf{x}^2, \ldots, \mathbf{x}^k) \in E_1 \times \cdots \times E_k : \|\mathbf{x}^1 + \cdots + \mathbf{x}^k\| = t\} \right|.$$

Since $\prod_{j=1}^k |E_j| = \sum_{t \in \mathbb{F}_q} \nu_k(t)$, and $\nu_k(t) = 0$ if $t \notin \Delta_k(E_1, \ldots, E_k)$, we see that

$$\prod_{j=1}^k |E_j| - \nu_k(0) = \sum_{0 \neq t \in \Delta_k(E_1, \ldots, E_k)} \nu_k(t).$$

Square both sides of this equation and use the Cauchy-Schwarz inequality. Then we see that

$$\left(\prod_{j=1}^{k}|E_j| - v_k(0)\right)^2 = \left(\sum_{0 \neq t \in \Delta_k(E_1,\ldots,E_k)} v_k(t)\right)^2 \leq |\Delta_k(E_1,\ldots,E_k)|\left(\sum_{t \in \mathbb{F}_q^*} v_k^2(t)\right).$$

Thus, we obtain

$$|\Delta_k(E_1,\ldots,E_k)| \geq \frac{\left(\prod_{j=1}^{k}|E_j| - v_k(0)\right)^2}{\sum_{t \in \mathbb{F}_q^*} v_k^2(t)}. \tag{3.1}$$

Now, we claim three facts below.

Claim 3.2 *Suppose that $d \geq 2$ is even and $k \geq 2$ is an integer. If $E_j \subset \mathbb{F}_q^d$ for $j = 1, 2, \ldots, k$ with $\prod_{j=1}^{k}|E_j| \geq 3^k q^{\frac{dk}{2}}$, then we have*

$$\left(\prod_{j=1}^{k}|E_j| - v_k(0)\right)^2 \geq \frac{1}{9}\left(\prod_{j=1}^{k}|E_j|\right)^2.$$

Claim 3.3 *Let $d \geq 2$ and $k \geq 2$ be integers. If $E_j \subset \mathbb{F}_q^d$ for $j = 1, 2, \ldots, k$, then we have*

$$\sum_{t \in \mathbb{F}_q} v_k^2(t) \leq \frac{1}{q}\left(\prod_{j=1}^{k}|E_j|\right)^2 + q^{2dk-d}\sum_{r \in \mathbb{F}_q}\left|\sum_{\mathbf{v} \in S_r}\left(\prod_{j=1}^{k}\widehat{E_j}(\mathbf{v})\right)\right|^2.$$

Claim 3.4 *Assume that $d \geq 2$ is even and $k \geq 2$ is an integer. If $E_j \subset \mathbb{F}_q^d$ for $j = 1, 2, \ldots, k$ with $\prod_{j=1}^{k}|E_j| \geq q^{\frac{dk}{2}}$, then we have*

$$q^{2dk-d}\left|\sum_{\mathbf{m} \in S_0}\left(\prod_{j=1}^{k}\widehat{E_j}(\mathbf{m})\right)\right|^2 - v_k^2(0) \leq \frac{4}{q}\left(\prod_{j=1}^{k}|E_j|\right)^2.$$

For a moment, let us accept Claims 3.2, 3.3, and 3.4 which shall be proved in the following subsections (see Sects. 3.1, 3.2, and 3.3). From (3.1) and Claim 3.2, we see that if $\prod_{j=1}^{k}|E_j| \geq 3^k q^{\frac{dk}{2}}$, then

$$|\Delta_k(E_1,\ldots,E_k)| \gtrsim \frac{\left(\prod_{j=1}^{k}|E_j|\right)^2}{\sum_{t \in \mathbb{F}_q^*} v_k^2(t)}. \tag{3.2}$$

Observe from Claims 3.3 and 3.4 that if $\prod_{j=1}^{k} |E_j| \geq 3^k q^{\frac{dk}{2}}$, then

$$
\begin{aligned}
\sum_{t \in \mathbb{F}_q^*} v_k^2(t) = \sum_{t \in \mathbb{F}_q} v_k^2(t) - v_k^2(0) &\leq \frac{5}{q} \left(\prod_{j=1}^{k} |E_j| \right)^2 + q^{2dk-d} \sum_{r \neq 0} \left| \sum_{\mathbf{v} \in S_r} \left(\prod_{j=1}^{k} \widehat{E_j}(\mathbf{v}) \right) \right|^2 \\
&\lesssim \frac{1}{q} \left(\prod_{j=1}^{k} |E_j| \right)^2 + q^{2dk-d} \sum_{r \neq 0} \left(\sum_{\mathbf{v} \in S_r} \left(\prod_{j=1}^{k} |\widehat{E_j}(\mathbf{v})| \right) \right)^2 \\
&\leq \frac{1}{q} \left(\prod_{j=1}^{k} |E_j| \right)^2 + q^{2dk-d} \left(\max_{r \neq 0} \sum_{\mathbf{v} \in S_r} \left(\prod_{j=1}^{k} |\widehat{E_j}(\mathbf{v})| \right) \right) \left(\sum_{\mathbf{v} \in \mathbb{F}_q^d} \left(\prod_{j=1}^{k} |\widehat{E_j}(\mathbf{v})| \right) \right) \\
&\leq \frac{1}{q} \left(\prod_{j=1}^{k} |E_j| \right)^2 + q^{dk} \left(\prod_{j=1}^{k} |E_j| \right)^{\frac{k-1}{k}} \left(\max_{r \neq 0} \sum_{\mathbf{v} \in S_r} \left(\prod_{j=1}^{k} |\widehat{E_j}(\mathbf{v})| \right) \right),
\end{aligned}
$$

where Lemma 2.1 was used to obtain the last inequality. From this estimate and (3.2), it follows that

$$
|\Delta_k(E_1, \ldots, E_k)| \gtrsim \frac{\left(\prod_{j=1}^{k} |E_j| \right)^2}{\frac{1}{q} \left(\prod_{j=1}^{k} |E_j| \right)^2 + q^{dk} \left(\prod_{j=1}^{k} |E_j| \right)^{\frac{k-1}{k}} \left(\max_{r \in \mathbb{F}_q^*} \sum_{\mathbf{v} \in S_r} \left(\prod_{j=1}^{k} |\widehat{E_j}(\mathbf{v})| \right) \right)}
$$

$$
\gtrsim \min \left\{ q, \frac{\left(\prod_{j=1}^{k} |E_j| \right)^{\frac{k+1}{k}}}{q^{dk} \left(\max_{r \in \mathbb{F}_q^*} \sum_{\mathbf{v} \in S_r} \left(\prod_{j=1}^{k} |\widehat{E_j}(\mathbf{v})| \right) \right)} \right\}.
$$

Then the statement of Theorem 3.1 follows by applying generalized Hölder's inequality (2.2):

$$
\max_{r \in \mathbb{F}_q^*} \sum_{\mathbf{v} \in S_r} \left(\prod_{j=1}^{k} |\widehat{E_j}(\mathbf{v})| \right) \leq \max_{r \in \mathbb{F}_q^*} \prod_{j=1}^{k} \left(\sum_{\mathbf{v} \in S_r} |\widehat{E_j}(\mathbf{v})|^k \right)^{\frac{1}{k}}.
$$

$\square$

3.1 Proof of Claim 3.2

Suppose that $d \geq 2$ is even and $k \geq 2$ is an integer. Let $E_j \subset \mathbb{F}_q^d$ for $j = 1, 2, \ldots, k$ with $\prod_{j=1}^{k} |E_j| \geq 3^k q^{\frac{dk}{2}}$. We aim to show that

$$\left(\prod_{j=1}^{k}|E_j| - v_k(0)\right)^2 \geq \frac{1}{9}\left(\prod_{j=1}^{k}|E_j|\right)^2. \tag{3.3}$$

To prove this, we begin by estimating the counting function $v_k(t)$ for $t \in \mathbb{F}_q$. For each $t \in \mathbb{F}_q$, it follows that

$$v_k(t) = \left|\{(\mathbf{x}^1, \mathbf{x}^2, \dots, \mathbf{x}^k) \in E_1 \times \dots \times E_k : \|\mathbf{x}^1 + \dots + \mathbf{x}^k\| = t\}\right|$$

$$= \sum_{(\mathbf{x}^1,\mathbf{x}^2,\dots,\mathbf{x}^k)\in E_1\times E_2\times\dots\times E_k} S_t(\mathbf{x}^1 + \mathbf{x}^2 + \dots + \mathbf{x}^k).$$

Applying the Fourier inversion theorem to the indicate function $S_t(\mathbf{x}^1 + \mathbf{x}^2 + \dots + \mathbf{x}^k)$, it follows that

$$v_k(t) = \sum_{(\mathbf{x}^1,\mathbf{x}^2,\dots,\mathbf{x}^k)\in\mathbb{F}_q^d\times\dots\times\mathbb{F}_q^d} E_1(\mathbf{x}^1) \cdots E_k(\mathbf{x}^k) \sum_{\mathbf{m}\in\mathbb{F}_q^d} \widehat{S}_t(\mathbf{m})\,\chi(\mathbf{m}\cdot(\mathbf{x}^1 + \dots + \mathbf{x}^k)).$$

By the definition of the normalized Fourier transform, we can write

$$v_k(t) = q^{dk} \sum_{\mathbf{m}\in\mathbb{F}_q^d} \widehat{S}_t(\mathbf{m})\left(\prod_{j=1}^{k}\overline{\widehat{E}_j}(\mathbf{m})\right). \tag{3.4}$$

To prove (3.3), we first find an upper bound of $v_k(0) = q^{dk} \sum_{\mathbf{m}\in\mathbb{F}_q^d} \widehat{S}_0(\mathbf{m})\left(\prod_{j=1}^{k}\overline{\widehat{E}_j}(\mathbf{m})\right).$

By (2.4) of Lemma 2.2, we can write

$$v_k(0) = q^{dk} \sum_{\mathbf{m}\in\mathbb{F}_q^d} \left(\prod_{j=1}^{k}\overline{\widehat{E}_j}(\mathbf{m})\right)\left(q^{-1}\delta_0(\mathbf{m}) + q^{-d-1}\,G^d\sum_{\ell\in\mathbb{F}_q^d}\chi(\|\mathbf{m}\|\ell)\right)$$

$$= q^{dk-1}\left(\prod_{j=1}^{k}\overline{\widehat{E}_j}(0,\dots,0)\right) + q^{dk-d-1}\,G^d \sum_{\mathbf{m}\in\mathbb{F}_q^d}\left(\prod_{j=1}^{k}\overline{\widehat{E}_j}(\mathbf{m})\right)\sum_{\ell\in\mathbb{F}_q^*}\chi(\|\mathbf{m}\|\ell) \tag{3.5}$$

Since $\overline{\widehat{E}_j}(0,\dots,0) = \frac{|E_j|}{q^d}$, $|G| = q^{1/2}$ and $|\sum_{\ell\in\mathbb{F}_q^*}\chi(\|\mathbf{m}\|\ell)| \leq q$,

$$v_k(0) \leq q^{-1}\prod_{j=1}^{k}|E_j| + q^{dk-d/2}\sum_{\mathbf{m}\in\mathbb{F}_q^d}\prod_{j=1}^{k}|\widehat{E}_j(\mathbf{m})|$$

Applying Lemma 2.1,

$$v_k(0) \leq q^{-1} \prod_{j=1}^{k} |E_j| + q^{\frac{d}{2}} \left(\prod_{j=1}^{k} |E_j| \right)^{\frac{k-1}{k}}.$$

Since $q \geq 3$, it follows that

$$\prod_{j=1}^{k} |E_j| - v_k(0) \geq \prod_{j=1}^{k} |E_j| - q^{-1} \prod_{j=1}^{k} |E_j| - q^{\frac{d}{2}} \left(\prod_{j=1}^{k} |E_j| \right)^{\frac{k-1}{k}}$$

$$\geq \frac{1}{3} \prod_{j=1}^{k} |E_j| + \left(\frac{1}{3} \prod_{j=1}^{k} |E_j| - q^{\frac{d}{2}} \left(\prod_{j=1}^{k} |E_j| \right)^{\frac{k-1}{k}} \right).$$

Note that if $\prod_{j=1}^{k} |E_j| \geq 3^k q^{\frac{dk}{2}}$, then the second term above is nonnegative. Thus we obtain that

$$\prod_{j=1}^{k} |E_j| - v_k(0) \geq \frac{1}{3} \prod_{j=1}^{k} |E_j|.$$

Squaring the both sizes, we complete the proof of Claim 3.2.

3.2 Proof of Claim 3.3

We want to prove the following L^2 estimate of the counting function $v(t)$:

$$\sum_{t \in \mathbb{F}_q} v_k^2(t) \leq \frac{1}{q} \left(\prod_{j=1}^{k} |E_j| \right)^2 + q^{2dk-d} \sum_{r \in \mathbb{F}_q} \left| \sum_{\mathbf{v} \in S_r} \left(\prod_{j=1}^{k} \widehat{E_j}(\mathbf{v}) \right) \right|^2. \qquad (3.6)$$

By (3.4), we see that

$$\sum_{t \in \mathbb{F}_q} v_k^2(t) = \sum_{t \in \mathbb{F}_q} v_k(t) \overline{v_k}(t)$$

$$= q^{2dk} \sum_{\mathbf{m}, \mathbf{v} \in \mathbb{F}_q^d} \left(\prod_{j=1}^{k} \overline{\widehat{E_j}}(\mathbf{m}) \right) \left(\prod_{j=1}^{k} \widehat{E_j}(\mathbf{v}) \right) \sum_{t \in \mathbb{F}_q} \widehat{S_t}(\mathbf{m}) \overline{\widehat{S_t}}(\mathbf{v}).$$

Using Lemma 2.3, we see that

$$
\sum_{t\in\mathbb{F}_q} v_k^2(t) = q^{2dk-1} \sum_{\mathbf{m},\mathbf{v}\in\mathbb{F}_q^d} \left(\prod_{j=1}^{k} \overline{\widehat{E_j}}(\mathbf{m})\right)\left(\prod_{j=1}^{k} \widehat{E_j}(\mathbf{v})\right)\delta_0(\mathbf{m})\,\delta_0(\mathbf{v})
$$

$$
+ q^{2dk-d-1} \sum_{\mathbf{m},\mathbf{v}\in\mathbb{F}_q^d} \left(\prod_{j=1}^{k} \overline{\widehat{E_j}}(\mathbf{m})\right)\left(\prod_{j=1}^{k} \widehat{E_j}(\mathbf{v})\right)\left(\sum_{s\in\mathbb{F}_q} \chi\left(s(\|\mathbf{m}\|-\|\mathbf{v}\|)\right)-1\right)
$$

$$
= q^{2dk-1}\left(\prod_{j=1}^{k} \overline{\widehat{E_j}}(0,\ldots,0)\right)\left(\prod_{j=1}^{k} \widehat{E_j}(0,\ldots,0)\right)
$$

$$
+ q^{2dk-d-1} \sum_{\mathbf{m},\mathbf{v}\in\mathbb{F}_q^d} \left(\prod_{j=1}^{k} \overline{\widehat{E_j}}(\mathbf{m})\right)\left(\prod_{j=1}^{k} \widehat{E_j}(\mathbf{v})\right)\sum_{s\in\mathbb{F}_q} \chi\left(s(\|\mathbf{m}\|-\|\mathbf{v}\|)\right)
$$

$$
- q^{2dk-d-1} \sum_{\mathbf{m},\mathbf{v}\in\mathbb{F}_q^d} \left(\prod_{j=1}^{k} \overline{\widehat{E_j}}(\mathbf{m})\right)\left(\prod_{j=1}^{k} \widehat{E_j}(\mathbf{v})\right).
$$

By the definition of the normalized Fourier transform, the orthogonality relation of χ, and basic property of summation, it follows that

$$
\sum_{t\in\mathbb{F}_q} v_k^2(t) = q^{2dk-1}\left(\prod_{j=1}^{k} \frac{|E_j|}{q^d}\right)^2
$$

$$
+ q^{2dk-d} \sum_{\mathbf{m},\mathbf{v}\in\mathbb{F}_q^d:\|\mathbf{m}\|=\|\mathbf{v}\|} \left(\prod_{j=1}^{k} \overline{\widehat{E_j}}(\mathbf{m})\right)\left(\prod_{j=1}^{k} \widehat{E_j}(\mathbf{v})\right)
$$

$$
- q^{2dk-d-1}\left|\sum_{\mathbf{v}\in\mathbb{F}_q^d} \left(\prod_{j=1}^{k} \widehat{E_j}(\mathbf{v})\right)\right|^2.
$$

Since the third term above is not positive, we obtain that

$$
\sum_{t\in\mathbb{F}_q} v_k^2(t) \le q^{2dk-1}\left(\prod_{j=1}^{k} \frac{|E_j|}{q^d}\right)^2 + q^{2dk-d} \sum_{\mathbf{m},\mathbf{v}\in\mathbb{F}_q^d:\|\mathbf{m}\|=\|\mathbf{v}\|} \left(\prod_{j=1}^{k} \overline{\widehat{E_j}}(\mathbf{m})\right)\left(\prod_{j=1}^{k} \widehat{E_j}(\mathbf{v})\right)
$$

$$
= q^{-1}\left(\prod_{j=1}^{k} |E_j|\right)^2 + q^{2dk-d} \sum_{r\in\mathbb{F}_q} \left|\sum_{\mathbf{v}\in\mathbb{F}_q^d:\|\mathbf{v}\|=r} \left(\prod_{j=1}^{k} \widehat{E_j}(\mathbf{v})\right)\right|^2,
$$

which completes the proof of Claim 3.3.

3.3 Proof of Claim 3.4

For even $d \geq 2$ and an integer $k \geq 2$, let $E_j \subset \mathbb{F}_q^d$ for $j = 1, 2, \ldots, k$ with $\prod_{j=1}^k |E_j| \geq q^{\frac{dk}{2}}$. We must show that

$$q^{2dk-d} \left| \sum_{\mathbf{m} \in S_0} \left(\prod_{j=1}^k \widehat{E_j}(\mathbf{m}) \right) \right|^2 - v_k^2(0) \leq \frac{4}{q} \left(\prod_{j=1}^k |E_j| \right)^2. \tag{3.7}$$

We begin by recalling from (3.5) that if $d \geq 2$ is even, then

$$v_k(0) = q^{dk-1} \left(\prod_{j=1}^k \overline{\widehat{E_j}}(0, \ldots, 0) \right) + q^{dk-d-1} G^d \sum_{\mathbf{m} \in \mathbb{F}_q^d} \left(\prod_{j=1}^k \overline{\widehat{E_j}}(\mathbf{m}) \right) \sum_{\ell \in \mathbb{F}_q^*} \chi(\|\mathbf{m}\|\ell).$$

It follows that

$$v_k(0) = q^{-1} \left(\prod_{j=1}^k |E_j| \right) + q^{dk-d-1} G^d \sum_{\mathbf{m} \in \mathbb{F}_q^d} \left(\prod_{j=1}^k \overline{\widehat{E_j}}(\mathbf{m}) \right) \left(-1 + \sum_{\ell \in \mathbb{F}_q} \chi(\|\mathbf{m}\|\ell) \right)$$

$$= \left[q^{-1} \left(\prod_{j=1}^k |E_j| \right) - q^{dk-d-1} G^d \sum_{\mathbf{m} \in \mathbb{F}_q^d} \left(\prod_{j=1}^k \overline{\widehat{E_j}}(\mathbf{m}) \right) \right]$$

$$+ q^{dk-d} G^d \sum_{\mathbf{m} \in S_0} \left(\prod_{j=1}^k \overline{\widehat{E_j}}(\mathbf{m}) \right) := A + B.$$

Thus we can write

$$v_k^2(0) = v_k(0) \, \overline{v_k(0)} = (A + B)(\overline{A} + \overline{B}) = |A|^2 + |B|^2 + A\overline{B} + \overline{A}B$$

Since the absolute value of the Gauss sum G is $\sqrt{q}$, we have

$$v_k^2(0) = q^{2dk-d} \left| \sum_{\mathbf{m} \in S_0} \left(\prod_{j=1}^k \widehat{E_j}(\mathbf{m}) \right) \right|^2 + |A|^2 + A\overline{B} + \overline{A}B.$$

It follows that

$$q^{2dk-d} \left| \sum_{\mathbf{m} \in S_0} \left(\prod_{j=1}^k \widehat{E_j}(\mathbf{m}) \right) \right|^2 - v_k^2(0) \leq -A\overline{B} - \overline{A}B \leq 2|A||B|. \tag{3.8}$$

Now, notice that

$$|A| \leq q^{-1} \left(\prod_{j=1}^{k} |E_j| \right) + q^{dk-d-1} |G|^d \sum_{\mathbf{m} \in \mathbb{F}_q^d} \left(\prod_{j=1}^{k} |\widehat{E_j}(\mathbf{m})| \right)$$

and

$$|B| \leq q^{dk-d} |G|^d \sum_{\mathbf{m} \in \mathbb{F}_q^d} \left(\prod_{j=1}^{k} |\widehat{E_j}(\mathbf{m})| \right).$$

Since $|G| = \sqrt{q}$, using Lemma 2.1 yields the following two estimates:

$$|A| \leq q^{-1} \left(\prod_{j=1}^{k} |E_j| \right) + q^{\frac{d}{2}-1} \left(\prod_{j=1}^{k} |E_j| \right)^{\frac{k-1}{k}}$$

and

$$|B| \leq q^{\frac{d}{2}} \left(\prod_{j=1}^{k} |E_j| \right)^{\frac{k-1}{k}}.$$

From these estimates and (3.8), we have

$$q^{2dk-d} \left| \sum_{\mathbf{m} \in S_0} \left(\prod_{j=1}^{k} \widehat{E_j}(\mathbf{m}) \right) \right|^2 - v_k^2(0)$$

$$\leq 2 \left(q^{\frac{d}{2}-1} \left(\prod_{j=1}^{k} |E_j| \right)^{\frac{2k-1}{k}} + q^{d-1} \left(\prod_{j=1}^{k} |E_j| \right)^{\frac{2k-2}{k}} \right).$$

Finally, we obtain the estimate (3.7) by observing that if $\prod_{j=1}^{k} |E_j| \geq q^{\frac{dk}{2}}$, then

$$\max \left\{ q^{\frac{d}{2}-1} \left(\prod_{j=1}^{k} |E_j| \right)^{\frac{2k-1}{k}}, q^{d-1} \left(\prod_{j=1}^{k} |E_j| \right)^{\frac{2k-2}{k}} \right\} \leq q^{-1} \left(\prod_{j=1}^{k} |E_j| \right)^2.$$

Thus the proof of Claim 3.4 is complete.

4 Connection Between Restriction Estimates for Spheres and $|\Delta_k(E_1, \ldots, E_k)|$

Theorem 3.1 shows that a good lower bound of $|\Delta_k(E_1, E_2, \ldots, E_k)|$ can be obtained by estimating an upper bound of the quantity

$$\max_{r \in \mathbb{F}_q^*} \prod_{j=1}^{k} \left(\sum_{\mathbf{v} \in S_r} |\widehat{E_j}(\mathbf{v})|^k \right)^{\frac{1}{k}} . \tag{4.1}$$

This quantity is closely related to the restriction estimates for spheres with non-zero radius. In this section, we introduce the restriction problem for spheres and we restate Theorem 3.1 in terms of the restriction estimates for spheres. We begin by reviewing the extension problem for spheres which is also called the dual restriction problem for spheres. We shall use the notation $(\mathbb{F}_q^d, d\mathbf{x})$ to denote the d-dimensional vector space over the finite field $\mathbb{F}_q$ where a normalized counting measure $d\mathbf{x}$ is given. On the other hand, we denote by $(\mathbb{F}_q^d, d\mathbf{m})$ the dual space of the vector space $(\mathbb{F}_q^d, d\mathbf{x})$, where we endow the dual space $(\mathbb{F}_q^d, d\mathbf{m})$ with the counting measure $d\mathbf{m}$. Since the space $(\mathbb{F}_q^d, d\mathbf{x})$ can be identified with its dual space $(\mathbb{F}_q^d, d\mathbf{m})$ as an abstract group, we shall use the notation $\mathbb{F}_q^d$ to indicate both the space and its dual space. To distinguish the space with its dual space, we always use the variable $\mathbf{x}$ for the element of the space $(\mathbb{F}_q^d, d\mathbf{x})$ with the normalized counting measure $d\mathbf{x}$. On the other hand, the variable $\mathbf{m}$ will be used to denote the element of the dual space $(\mathbb{F}_q^d, d\mathbf{m})$ with the counting measure $d\mathbf{m}$. For example, we write $\mathbf{x} \in \mathbb{F}_q^d$ and $\mathbf{m} \in \mathbb{F}_q^d$ for $\mathbf{x} \in (\mathbb{F}_q^d, d\mathbf{x})$ and $\mathbf{m} \in (\mathbb{F}_q^d, d\mathbf{m})$, respectively. With these notations, the classical norm notation can be used to indicate the following sums: for $1 \leq r < \infty$,

$$\|g\|_{L^r(\mathbb{F}_q^d, d\mathbf{m})}^r = \sum_{\mathbf{m} \in \mathbb{F}_q^d} |g(\mathbf{m})|^r,$$

$$\|f\|_{L^r(\mathbb{F}_q^d, d\mathbf{x})}^r = q^{-d} \sum_{\mathbf{x} \in \mathbb{F}_q^d} |f(\mathbf{x})|^r,$$

and

$$\|g\|_{L^\infty(\mathbb{F}_q^d, d\mathbf{m})} = \max_{\mathbf{m} \in \mathbb{F}_q^d} |g(\mathbf{m})|.$$

where g is a function on $(\mathbb{F}_q^d, d\mathbf{m})$ and f is a function on $(\mathbb{F}_q^d, d\mathbf{x})$. For each $t \in \mathbb{F}_q^*$, let $S_t \subset (\mathbb{F}_q^d, dx)$ be the sphere defined as in (2.3). We endow the sphere S_t with the normalized surface measure $d\sigma$ which is defined by measuring the mass of each point on S_t as $1/|S_t|$. Notice that the total mass of S_t is 1 and we have

$$\|f\|_{L^r(S_t, d\sigma)}^r = \frac{1}{|S_t|} \sum_{\mathbf{x} \in S_t} |f(\mathbf{x})|^r \quad \text{for } 1 \leq r < \infty,$$

$$\|f\|_{L^\infty(S_t, d\sigma)} = \max_{\mathbf{x} \in S_t} |f(\mathbf{x})|. \tag{4.2}$$

We also recall that if $f : (S_t, d\sigma) \to \mathbb{C}$, then the inverse Fourier transform of $f d\sigma$ is defined by

$$(f d\sigma)^\vee(\mathbf{m}) = \frac{1}{|S_t|} \sum_{\mathbf{x} \in S_t} f(\mathbf{x}) \chi(\mathbf{m} \cdot \mathbf{x}) \quad \text{for } \mathbf{m} \in (\mathbb{F}_q^d, d\mathbf{m}).$$

Since the sphere S_t is symmetric about the origin, we can write

$$(d\sigma)^\vee(\mathbf{m}) = \frac{q^d}{|S_t|} \widehat{S_t}(\mathbf{m}) \quad \text{for } \mathbf{m} \in (\mathbb{F}_q^d, d\mathbf{m}).$$

With the above notation, the extension problem for the sphere S_t asks us to determine $1 \leq p, r \leq \infty$ such that there exists $C > 0$ satisfying the following extension estimate:

$$\|(f d\sigma)^\vee\|_{L^r(\mathbb{F}_q^d, d\mathbf{m})} \leq C \|f\|_{L^p(S_t, d\sigma)} \quad \text{for all } f : S_t \to \mathbb{C}, \qquad (4.3)$$

where the constant $C > 0$ may depend on p, r, d, S_t, but it must be independent of the functions f and the size of the underlying finite field $\mathbb{F}_q$. By duality, this extension estimate is the same as the following restriction estimate (see [?,?]) :

$$\|\widetilde{g}\|_{L^{p'}(S_t, d\sigma)} \leq C \|g\|_{L^{r'}(\mathbb{F}_q^d, d\mathbf{m})} \quad \text{for all } g : \mathbb{F}_q^d \to \mathbb{C}, \qquad (4.4)$$

where $\widetilde{g}$ is defined as in (2.1), and p', r' denote the Hölder conjugates of p and r, respectively (namely, $1/p + 1/p' = 1$ and $1/r + 1/r' = 1$).

Now, we address the relation between the restriction estimates for spheres with non-zero radius and a lower bound of $|\Delta_k(E_1, \ldots, E_k)|$. By Theorem 3.1 and the definition of the restriction estimates for spheres in (4.4), we obtain the following result.

Lemma 4.1 *For even $d \geq 2$ and an integer $k \geq 2$, let $E_j \subset \mathbb{F}_q^d$ for $j = 1, 2, \ldots, k$. Assume that $\prod_{j=1}^k |E_j| \geq 3^k q^{\frac{dk}{2}}$ and the following restriction estimate holds for some $1 \leq \ell < \infty$ and $\alpha \in \mathbb{R}$:*

$$\|\widetilde{E_j}\|_{L^k(S_r, d\sigma)} \lesssim q^\alpha \|E_j\|_{L^\ell(\mathbb{F}_q^d, d\mathbf{m})} \quad \text{for all } r \in \mathbb{F}_q^*, \quad j = 1, 2, \ldots, k. \qquad (4.5)$$

Then we have

$$|\Delta_k(E_1, \ldots, E_k)| \gtrsim \min \left\{ q, \frac{\left(\prod_{j=1}^k |E_j| \right)^{\frac{k+1}{k} - \frac{1}{\ell}}}{q^{k\alpha + d - 1}} \right\}.$$

Proof By Theorem 3.1, it suffices to prove that

$$q^{dk}\left(\max_{r\in\mathbb{F}_q^*}\prod_{j=1}^{k}\left(\sum_{\mathbf{v}\in S_r}|\widehat{E_j}(\mathbf{v})|^k\right)^{\frac{1}{k}}\right)\lesssim q^{k\alpha+d-1}\left(\prod_{j=1}^{k}|E_j|\right)^{\frac{1}{\ell}}. \qquad (4.6)$$

Since $\widehat{E_j}(\mathbf{v}) = q^{-d}\widetilde{E_j}(\mathbf{v})$ for $j = 1,\ldots,k$, we see that

$$q^{dk}\left(\max_{r\in\mathbb{F}_q^*}\prod_{j=1}^{k}\left(\sum_{\mathbf{v}\in S_r}|\widehat{E_j}(\mathbf{v})|^k\right)^{\frac{1}{k}}\right)=\left(\max_{r\in\mathbb{F}_q^*}\prod_{j=1}^{k}\left(\sum_{\mathbf{v}\in S_r}|\widetilde{E_j}(\mathbf{v})|^k\right)^{\frac{1}{k}}\right).$$

Using the definition of $\|\widetilde{E_j}\|_{L^k(S_r,d\sigma)}$ in (4.2) and the fact that $|S_r|\sim q^{d-1}$, the above quantity is similar to the following value:

$$q^{d-1}\left(\max_{r\in\mathbb{F}_q^*}\prod_{j=1}^{k}\|\widetilde{E_j}\|_{L^k(S_r,d\sigma)}\right).$$

By assumption (4.5), this can be dominated by

$$q^{d-1}\left(\prod_{j=1}^{k}\left(q^{\alpha}\|E_j\|_{L^\ell(\mathbb{F}_q^d,d\mathbf{m})}\right)\right)=q^{k\alpha+d-1}\left(\prod_{j=1}^{k}|E_j|^{\frac{1}{\ell}}\right)=q^{k\alpha+d-1}\left(\prod_{j=1}^{k}|E_j|\right)^{\frac{1}{\ell}}.$$

Putting all estimates together yields the inequality (4.6), which completes the proof.
□

5 Restriction Theorems for Spheres

We see from Lemma 4.1 that the restriction estimates for spheres play an important role in determining lower bounds of the cardinality of the generalized k-resultant set $\Delta_k(E_1,\ldots,E_k)$. In particular, our main result (Theorem 1.6) will be proved by making an effort on finding possibly large exponent $\ell \geq 1$ such that the restriction inequality (4.5) holds for $k = 3$ or $k = 4$. In this section, we shall obtain such restriction estimates. To this end, we shall apply the following dual restriction estimate for spheres with non-zero radius due to the authors in [11].

Lemma 5.1 ([11], Theorem 1) *If $d \geq 4$ is even, then*

$$\|(Fd\sigma)^\vee\|_{L^4(\mathbb{F}_q^d,d\mathbf{m})}\lesssim\|F\|_{L^{(12d-8)/(9d-12)}(S_t,d\sigma)} \quad \text{for all } F\subset S_t,\ t\neq 0. \qquad (5.1)$$

To obtain a restriction estimate for spheres, we shall use the dual estimate of (5.1). To this end, it is useful to review Lorentz spaces in our setting. For a function $f : (S_t, d\sigma) \to \mathbb{C}$, we denote by d_f the distribution function on $[0, \infty)$:

$$d_f(a) := \frac{1}{|S_t|} |\{\mathbf{x} \in S_t : |f(\mathbf{x})| > a\}| .$$

We see that for $1 \le r \le \infty$,

$$\|f\|^r_{L^r(S_t, d\sigma)} = r \int_0^\infty s^{r-1} d_f(s) \, ds.$$

The function f^* is defined on $[0, \infty)$ by

$$f^*(s) := \inf\{a > 0 : d_f(a) \le s\}.$$

For $1 \le p, r \le \infty$ and a function $f : (S_t, d\sigma) \to \mathbb{C}$, define

$$\|f\|_{L^{p,r}(S_t, d\sigma)} := \begin{cases} \left(\int_0^\infty \left(s^{1/p} f^*(s) \right)^r \frac{ds}{s} \right)^{1/r} & \text{for } 1 \le r < \infty \\ \sup_{s>0} s^{1/p} f^*(s) & \text{for } r = \infty. \end{cases}$$

In particular, we see that

$$\|f\|_{L^{p,1}(S_t, d\sigma)} = \int_0^\infty s^{1/p-1} f^*(s) \, ds.$$

It is not hard to see that for $1 \le p \le \infty$ and $1 \le r_1 \le r_2 \le \infty$,

$$\|f\|_{L^{p,r_2}(S_t, d\sigma)} \lesssim \|f\|_{L^{p,r_1}(S_t, d\sigma)} \quad \text{and} \quad \|f\|_{L^{p,p}(S_t, d\sigma)} = \|f\|_{L^p(S_t, d\sigma)}.$$

See [6] for further information about Lorentz spaces. With the above notation, the following fact can be deduced.

Lemma 5.2 *Let $d\sigma$ be the normalized surface measure on the sphere $S_t \subset (\mathbb{F}_q^d, d\mathbf{x})$. Assume that the estimate*

$$\|(Fd\sigma)^\vee\|_{L^r(\mathbb{F}_q^d, d\mathbf{m})} \lesssim \|F\|_{L^p(S_t, d\sigma)} \tag{5.2}$$

holds for all subsets F of S_t. Then we have

$$\|(fd\sigma)^\vee\|_{L^r(\mathbb{F}_q^d, d\mathbf{m})} \lesssim \|f\|_{L^{p,1}(S_t, d\sigma)}$$

for all functions $f : (S_t, d\sigma) \to \mathbb{C}$.

Proof Without loss of generality, we may assume that f is a nonnegative simple function given by the form

$$f = \sum_{j=1}^N a_j 1_{F_j} \tag{5.3}$$

where $F_N \subset F_{N-1} \subset \cdots \subset F_2 \subset F_1$ and $a_j > 0$ for all $j = 1, 2, \ldots, N$. Notice that

$$f^*(s) = \sum_{j=1}^{N} a_j \, 1_{\left[0, \frac{|F_j|}{|S_t|}\right]}(s).$$

It follows that

$$\int_0^\infty s^{\frac{1}{p}-1} f^*(s) \, ds = \int_0^\infty s^{\frac{1}{p}-1} \sum_{j=1}^{N} a_j \, 1_{\left[0, \frac{|F_j|}{|S_t|}\right]}(s) \, ds$$

$$= \sum_{j=1}^{N} a_j \int_0^{\frac{|F_j|}{|S_t|}} s^{\frac{1}{p}-1} \, ds = p \sum_{j=1}^{N} a_j \left(\frac{|F_j|}{|S_t|}\right)^{\frac{1}{p}} = p \sum_{j=1}^{N} a_j \|F_j\|_{L^p(S_t, d\sigma)}.$$

Namely, we see that

$$\int_0^\infty s^{\frac{1}{p}-1} f^*(s) \, ds \sim \sum_{j=1}^{N} a_j \|F_j\|_{L^p(S_t, d\sigma)}.$$

Using this estimate along with (5.3) and the hypothesis (5.2), we see that

$$\|(f d\sigma)^\vee\|_{L^r(\mathbb{F}_q^d, d\mathbf{m})} \le \sum_{j=1}^{N} a_j \, \|(F_j d\sigma)^\vee\|_{L^r(\mathbb{F}_q^d, d\mathbf{m})}$$

$$\lesssim \sum_{j=1}^{N} a_j \, \|F_j\|_{L^p(S_t, d\sigma)} \sim \int_0^\infty s^{\frac{1}{p}-1} f^*(s) \, ds = \|f\|_{L^{p,1}(S_t, d\sigma)}.$$

Hence, the proof is complete. $\qquad\square$

We shall invoke the following weak-type restriction estimate.

Lemma 5.3 *If $d \ge 4$ is even and we put $r_0 = (12d - 8)/(3d + 4)$, then the weak-type restriction estimate*

$$\|\widetilde{g}\|_{L^{r_0, \infty}(S_t, d\sigma)} \lesssim \|g\|_{L^{\frac{4}{3}}(\mathbb{F}_q^d, d\mathbf{m})} \tag{5.4}$$

holds for all $t \in \mathbb{F}_q^*$ and for all functions $g : (\mathbb{F}_q^d, d\mathbf{m}) \to \mathbb{C}$.

Proof Since $r_0 = (12d - 8)/(3d + 4)$, its dual exponent r_0' is given by

$$r_0' = (12d - 8)/(9d - 12).$$

Combining Lemma 5.1 with Lemma 5.2, it follows that

$$\|(f d\sigma)^\vee\|_{L^4(\mathbb{F}_q^d, d\mathbf{m})} \lesssim \|f\|_{L^{r_0', 1}(S_t, d\sigma)}$$

for all functions $f : (S_t, d\sigma) \to \mathbb{C}$ with $t \in \mathbb{F}_q^*$. By duality, this estimate is same as (5.4), which completes the proof. □

The following restriction estimate will play an important role in proving the third part of Theorem 1.6.

Lemma 5.4 *If $E \subset (\mathbb{F}_q^d, d\mathbf{m})$ and $|E| \geq q^{\frac{d-1}{2}}$, then we have*

$$\|\widetilde{E}\|_{L^2(S_t, d\sigma)} \lesssim \frac{|E|}{q^{\frac{d-1}{4}}} \quad \text{for all } t \in \mathbb{F}_q^*.$$

Proof Since $\|\widetilde{E}\|_{L^2(S_t, d\sigma)}^2 = \frac{1}{|S_t|} \sum_{\mathbf{x} \in S_t} |\widetilde{E}(\mathbf{x})|^2$ and $|S_t| \sim q^{d-1}$ for $t \in \mathbb{F}_q^*$, it is enough to show that if $E \subset \mathbb{F}_q^d$ with $|E| \geq q^{\frac{d-1}{2}}$, then

$$\sum_{\mathbf{x} \in S_t} |\widetilde{E}(\mathbf{x})|^2 \lesssim q^{\frac{d-1}{2}} |E|^2. \tag{5.5}$$

Notice from the definition of the Fourier transforms that

$$\sum_{\mathbf{x} \in S_t} |\widetilde{E}(\mathbf{x})|^2 = \sum_{\mathbf{x} \in S_t} \sum_{\mathbf{m}, \mathbf{m}' \in E} \chi(-\mathbf{x} \cdot (\mathbf{m} - \mathbf{m}')) = \sum_{\mathbf{m}, \mathbf{m}' \in E} q^d \widehat{S_t}(\mathbf{m} - \mathbf{m}')$$

$$= q^d |E| \widehat{S_t}(0, \dots, 0) + \sum_{\mathbf{m}, \mathbf{m}' \in E : \mathbf{m} \neq \mathbf{m}'} q^d \widehat{S_t}(\mathbf{m} - \mathbf{m}')$$

$$\leq |E||S_t| + \left(\max_{\mathbf{n} \in \mathbb{F}_q^d \setminus \{(0, \dots, 0)\}} |\widehat{S_t}(\mathbf{n})| \right) \sum_{\mathbf{m}, \mathbf{m}' \in E : \mathbf{m} \neq \mathbf{m}'} q^d$$

$$\lesssim |E| q^{d-1} + |E|^2 q^d \left(\max_{\mathbf{n} \in \mathbb{F}_q^d \setminus \{(0, \dots, 0)\}} |\widehat{S_t}(\mathbf{n})| \right).$$

Now, we apply the well known fact (Lemma 2.2 in [12]) that if $S_t \subset \mathbb{F}_q^d$ for $t \in \mathbb{F}_q^*$ and $d \geq 2$, then

$$\left(\max_{\mathbf{n} \in \mathbb{F}_q^d \setminus \{(0, \dots, 0)\}} |\widehat{S_t}(\mathbf{n})| \right) \lesssim q^{-\frac{d+1}{2}}.$$

Then we see that

$$\sum_{\mathbf{x} \in S_t} |\widetilde{E}(\mathbf{x})|^2 \lesssim |E| q^{d-1} + q^{\frac{d-1}{2}} |E|^2 \lesssim q^{\frac{d-1}{2}} |E|^2,$$

where the last inequality follows from our assumption that $|E| \geq q^{\frac{d-1}{2}}$. Thus, (5.5) holds and we complete the proof. □

Now, we introduce the interpolation theorem which enables us to derive the restriction estimates we need for the proof of our main results.

Theorem 5.5 *Let Ω be a collection of subsets E of $(\mathbb{F}_q^d, d\mathbf{m})$. Assume that the following two restriction estimates hold for all sets $E \in \Omega$ and $1 \le r_0 < r_1 \le \infty$:*

$$\|\widetilde{E}\|_{L^{r_0,\infty}(S_t, d\sigma)} \lesssim A_0(q, |E|) := A_0$$

and

$$\|\widetilde{E}\|_{L^{r_1,\infty}(S_t, d\sigma)} \lesssim A_1(q, |E|) := A_1.$$

Then for $r_0 < r < r_1$, we have

$$\|\widetilde{E}\|_{L^r(S_t, d\sigma)} \lesssim \left(\max\left\{ \frac{2r}{r-r_0}, \frac{2r}{r_1-r} \right\} \right)^{\frac{1}{r}} A_0^{\frac{r_0(r_1-r)}{r(r_1-r_0)}} A_1^{\frac{r_1(r-r_0)}{r(r_1-r_0)}}. \tag{5.6}$$

Namely, if $\frac{1}{r} = \frac{1-\theta}{r_0} + \frac{\theta}{r_1}$ for some $0 < \theta < 1$, then we have

$$\|\widetilde{E}\|_{L^r(S_t, d\sigma)} \lesssim A_0^{1-\theta} A_1^{\theta}. \tag{5.7}$$

Proof Let $\delta > 0$ which will be chosen later.

$$
\begin{aligned}
\|\widetilde{E}\|_{L^r(S_t,d\sigma)}^r &= r \int_0^\infty s^{r-1} d_{\widetilde{E}}(s) \, ds \\
&= r \int_0^\delta s^{r-1} d_{\widetilde{E}}(s) \, ds + r \int_\delta^\infty s^{r-1} d_{\widetilde{E}}(s) \, ds \\
&= r \int_0^\delta s^{r-r_0-1} s^{r_0} d_{\widetilde{E}}(s) \, ds + r \int_\delta^\infty s^{r-r_1-1} s^{r_1} d_{\widetilde{E}}(s) \, ds \\
&\le r \left(\sup_{0<s<\infty} s^{r_0} d_{\widetilde{E}}(s) \right) \int_0^\delta s^{r-r_0-1} \, ds \\
&\quad + r \left(\sup_{0<s<\infty} s^{r_1} d_{\widetilde{E}}(s) \right) \int_\delta^\infty s^{r-r_1-1} \, ds \\
&= \frac{r}{r-r_0} \|\widetilde{E}\|_{L^{r_0,\infty}(S_t,d\sigma)}^{r_0} \delta^{r-r_0} + \frac{r}{r_1-r} \|\widetilde{E}\|_{L^{r_1,\infty}(S_t,d\sigma)}^{r_1} \delta^{r-r_1} \\
&\lesssim \max\left\{ \frac{r}{r-r_0}, \frac{r}{r_1-r} \right\} \left(A_0^{r_0} \delta^{r-r_0} + A_1^{r_1} \delta^{r-r_1} \right).
\end{aligned}
$$

Now we choose δ such that

$$A_0^{r_0} \delta^{r-r_0} = A_1^{r_1} \delta^{r-r_1}.$$

Namely, we choose

$$\delta = A_0^{\frac{r_0}{r_0 - r_1}} A_1^{\frac{r_1}{r_1 - r_0}}.$$

It follows that

$$\|\widetilde{E}\|_{L^r(S_t,d\sigma)}^r \lesssim \max\left\{\frac{2r}{r - r_0}, \frac{2r}{r_1 - r}\right\} A_0^{r_0} \delta^{r - r_0}$$

$$\lesssim \max\left\{\frac{2r}{r - r_0}, \frac{2r}{r_1 - r}\right\} A_0^{r_0} A_0^{\frac{r_0(r - r_0)}{r_0 - r_1}} A_1^{\frac{r_1(r - r_0)}{r_1 - r_0}}$$

$$= \max\left\{\frac{2r}{r - r_0}, \frac{2r}{r_1 - r}\right\} A_0^{\frac{r_0(r_1 - r)}{r_1 - r_0}} A_1^{\frac{r_1(r - r_0)}{r_1 - r_0}},$$

which implies (5.6). By a direct computation, (5.7) follows from (5.6).   □

Remark 5.6 The new ingredient of this paper is to eliminate the ε appearing in the third part of Theorem 1.3 which was previously obtained in [3]. This can be done by proceeding as follows. Combining Lemma 5.3 with Lemma 5.4, Theorem 5.5 yields the improved strong L^3-restriction estimate (see Lemma 6.3 in the next section).

6 Proof of Main Theorem (Theorem 1.6)

In this section, we shall give the complete proof of Theorem 1.6. Since $\|\widetilde{g}\|_{L^{\infty,\infty}(S_t,d\sigma)} = \|\widetilde{g}\|_{L^\infty(S_t,d\sigma)} = \max_{\mathbf{x} \in S_t} |\widetilde{g}(\mathbf{x})| \le \|g\|_{L^1(\mathbb{F}_q^d, d\mathbf{m})}$, it is clear that

$$\|\widetilde{E}\|_{L^{\infty,\infty}(S_t,d\sigma)} \lesssim \|E\|_{L^1(\mathbb{F}_q^d,d\mathbf{m})} = |E| \quad \text{for all } E \subset \mathbb{F}_q^d, \ t \neq 0. \quad (6.1)$$

On the other hand, it follows from Lemma 5.3 that if $d \geq 4$ is even, then

$$\|\widetilde{E}\|_{L^{\frac{12d-8}{3d+4},\infty}(S_t,d\sigma)} \lesssim \|E\|_{L^{\frac{4}{3}}(\mathbb{F}_q^d,d\mathbf{m})} = |E|^{\frac{3}{4}} \quad \text{for all } E \subset \mathbb{F}_q^d, \ t \neq 0. \quad (6.2)$$

6.1 Proof of Statement (1)

We need the following lemma to prove the statement (1) of Theorem 1.6.

Lemma 6.1 *If $d = 4$ or 6, then we have*

$$\|\widetilde{E}\|_{L^3(S_t,d\sigma)} \lesssim \|E\|_{L^{\frac{9d+12}{6d+14}}(\mathbb{F}_q^d,dm)} \quad \text{for all } E \subset \mathbb{F}_q^d, \ t \neq 0.$$

Proof Note that if $d = 4$ or 6, then $\frac{12d-8}{3d+4} < 3 < \infty$. Therefore, using Theorem 5.5, we are able to interpolate (6.1) and (6.2) so that we obtain

$$\|\widetilde{E}\|_{L^3(S_t,d\sigma)} \lesssim |E|^{1-\theta} |E|^{\frac{3\theta}{4}} \quad \text{with } \theta = \frac{12d-8}{9d+12}.$$

Namely, we see that

$$\|\widetilde{E}\|_{L^3(S_t,d\sigma)} \lesssim |E|^{\frac{6d+14}{9d+12}} = \|E\|_{L^{\frac{9d+12}{6d+14}}(\mathbb{F}_q^d,dm)}.$$

Thus, the proof is complete. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

We are ready to prove statement (1) of Theorem 1.6. We aim to prove that if $d = 4$ or $d = 6$, and $E_1, E_2, E_3 \subset \mathbb{F}_q^d$ with $|E_1||E_2||E_3| \gtrsim q^{3\left(\frac{d+1}{2} - \frac{1}{6d+2}\right)}$, then $|\Delta_3(E_1, E_2, E_3)| \gtrsim q$. Combining Lemmas 4.1 and 6.1, we see that

$$|\Delta_3(E_1, E_2, E_3)| \gtrsim \min\left\{q, \frac{\left(\prod_{j=1}^3 |E_j|\right)^{\frac{4}{3} - \frac{6d+14}{9d+12}}}{q^{d-1}}\right\}.$$

Since $|E_1||E_2||E_3| \geq Cq^{3\left(\frac{d+1}{2} - \frac{1}{6d+2}\right)}$ for a sufficiently large $C > 0$, we see from a direct computation that

$$|\Delta_3(E_1, E_2, E_3)| \gtrsim q.$$

6.2 Proof of Statement (2) of Theorem 1.6

The following lemma shall be used to prove the statement (2) of Theorem 1.6.

Lemma 6.2 *If $d \geq 4$ is even, then we have*

$$\|\widetilde{E}\|_{L^4(S_t,d\sigma)} \lesssim \|E\|_{L^{\frac{12d+16}{9d+18}}(\mathbb{F}_q^d,dm)} \quad \text{for all } E \subset \mathbb{F}_q^d, \ t \neq 0.$$

Proof Since $\frac{12d-8}{3d+4} < 4 < \infty$ for all even $d \geq 4$, interpolating (6.1) and (6.2) yields

$$\|\widetilde{E}\|_{L^4(S_t,d\sigma)} \lesssim |E|^{1-\theta}|E|^{\frac{3\theta}{4}} \quad \text{with } \theta = \frac{3d-2}{3d+4}.$$

Since $|E|^{1-\theta}|E|^{\frac{3\theta}{4}} = |E|^{\frac{9d+18}{12d+16}} = \|E\|_{L^{\frac{12d+16}{9d+18}}(\mathbb{F}_q^d,dm)}$, the statement follows. $\quad\square$

Let us prove statement (2) of Theorem 1.6. Recall that we must show that if $d \geq 8$ is even and $E_1, E_2, E_3, E_4 \subset \mathbb{F}_q^d$ with $\prod_{j=1}^4 |E_j| \gtrsim q^{4\left(\frac{d+1}{2} - \frac{1}{6d+2}\right)}$, then $|\Delta_4(E_1, E_2, E_3, E_4)| \gtrsim q$. Combining Lemmas 4.1 and 6.2, we obtain that

$$|\Delta_4(E_1, E_2, E_3, E_4)| \gtrsim \min\left\{q, \frac{\left(\prod_{j=1}^4 |E_j|\right)^{\frac{5}{4} - \frac{9d+18}{12d+16}}}{q^{d-1}}\right\}.$$

Since $|E_1||E_2||E_3||E_4| \geq Cq^{4\left(\frac{d+1}{2} - \frac{1}{6d+2}\right)}$ for a sufficiently large $C > 0$, it follows from a direct computation that

$$|\Delta_4(E_1, E_2, E_3, E_4)| \gtrsim q.$$

6.3 Proof of Statement (3) of Theorem 1.6

We begin by proving the following lemma.

Lemma 6.3 *Let $E \subset \mathbb{F}_q^d$. If $d \geq 8$ is even and $|E| \geq q^{\frac{d-1}{2}}$, then we have*

$$\|\widetilde{E}\|_{L^3(S_t, d\sigma)} \lesssim q^{\frac{-3d^2+23d-20}{36d-96}} \|E\|_{L^{\frac{18d-48}{15d-46}}(\mathbb{F}_q^d, d\mathbf{m})} \quad \text{for all } t \in \mathbb{F}_q^*.$$

Proof Since $\|\widetilde{E}\|_{L^{2,\infty}(S_t, d\sigma)} \leq \|\widetilde{E}\|_{L^2(S_t, d\sigma)}$, and $|E| \geq q^{\frac{d-1}{2}}$, we see from Lemma 5.4 that

$$\|\widetilde{E}\|_{L^{2,\infty}(S_t, d\sigma)} \lesssim q^{-\frac{(d-1)}{4}}|E| \quad \text{for all } t \in \mathbb{F}_q^* \quad \text{and } E \subset \mathbb{F}_q^d \text{ with } |E| \geq q^{\frac{d-1}{2}}. \quad (6.3)$$

As in (6.2), we also see that

$$\|\widetilde{E}\|_{L^{\frac{12d-8}{3d+4},\infty}(S_t, d\sigma)} \lesssim |E|^{\frac{3}{4}} \quad \text{for all } E \subset \mathbb{F}_q^d, \ t \in \mathbb{F}_q^*. \quad (6.4)$$

Since $2 < 3 < \frac{12d-8}{3d+4}$ for $d \geq 8$, by using Theorem 5.5 we are able to interpolate (6.3) and (6.4). Hence, if $d \geq 8$ is even and $|E| \geq q^{\frac{d-1}{2}}$, then we have

$$\|\widetilde{E}\|_{L^3(S_t, d\sigma)} \lesssim \left(q^{-\frac{(d-1)}{4}}|E|\right)^{1-\theta}|E|^{\frac{3\theta}{4}} \quad \text{with } \theta = \frac{6d-4}{9d-24}.$$

By a direct computation, we conclude

$$\|\widetilde{E}\|_{L^3(S_t, d\sigma)} \lesssim q^{\frac{-3d^2+23d-20}{36d-96}}|E|^{\frac{15d-46}{18d-48}} = q^{\frac{-3d^2+23d-20}{36d-96}} \|E\|_{L^{\frac{18d-48}{15d-46}}(\mathbb{F}_q^d, d\mathbf{m})},$$

which completes the proof of the lemma. $\square$

Let us prove the statement (3) of Theorem 1.6 which states that if $d \geq 8$ is even, and $\prod_{j=1}^3 |E_j| \gtrsim q^{3\left(\frac{d+1}{2} - \frac{1}{9d-18}\right)}$, then $|\Delta_3(E_1, E_2, E_3)| \gtrsim q$. To prove this, let us first assume that one of $|E_1|, |E_2|, |E_3|$ is less than $q^{\frac{d-1}{2}}$, say that $|E_3| < q^{\frac{d-1}{2}}$. Then by our hypothesis that $|E_1||E_2||E_3| \gtrsim q^{3\left(\frac{d+1}{2} - \frac{1}{9d-18}\right)}$, it must follow that

$$|E_1||E_2| \gtrsim q^{-\frac{(d-1)}{2}} q^{3\left(\frac{d+1}{2} - \frac{1}{9d-18}\right)} = q^{(d+1)+\frac{3d-7}{3d-6}} > q^{d+1}.$$

This implies that $|\Delta_2(E_1, E_2)| \gtrsim q$, which was proved by Shparlinski [17]. Thus it is clear that $|\Delta_3(E_1, E_2, E_3)| \gtrsim q$, because $|\Delta_3(E_1, E_2, E_3)| \geq |\Delta_2(E_1, E_2)|$. For this reason, we may assume that all of $|E_1|, |E_2|, |E_3|$ are greater than or equal to $q^{\frac{d-1}{2}}$, and $|E_1||E_2||E_3| \gtrsim q^{3\left(\frac{d+1}{2} - \frac{1}{9d-18}\right)}$. Combining Lemma 4.1 with Lemma 6.3 , we obtain that

$$|\Delta_3(E_1, E_2, E_3)| \gtrsim \min \left\{ q, \ \frac{\left(\prod_{j=1}^3 |E_j|\right)^{\frac{4}{3} - \frac{1}{\ell}}}{q^{3\alpha+d-1}} \right\},$$

where we take $\alpha = \frac{-3d^2+23d-20}{36d-96}$ and $\ell = \frac{18d-48}{15d-46}$. By a direct comparison, it is not hard to see that if $|E_1||E_2||E_3| \gtrsim q^{3\left(\frac{d+1}{2} - \frac{1}{9d-18}\right)} = q^{\frac{9d^2-9d-20}{6d-12}}$, then we have $|\Delta_3(E_1, E_2, E_3)| \gtrsim q$. We have finished the proof of the third part of Theorem 1.6.

References

1. Bourgain, J., Katz, N., Tao, T.: A sum-product estimate in finite fields, and applications. Geom. Funct. Anal. **14**, 27–57 (2004)
2. Chapman, J., Erdoǧan, M., Hart, D., Iosevich, A., Koh, D.: Pinned distance sets, Wolff's exponent in finite fields and sum-product estimates. Math. Z. **271**, 63–93 (2012)
3. Covert, D., Koh, D., Pi, Y.: On the sums of any k points in finite fields. SIAM J. Discret. Math. **30**(1), 367–382 (2016)
4. Covert, D., Koh, D., Pi, Y.: The k-resultant modulus set problem on algebraic varieties over finite fields. Finite Fields Appl. **48**, 68–86 (2017)
5. Erdös, P.: On sets of distances of n points. Amer. Math. Mon. **53**, 248–250 (1946)
6. Grafakos, L.: Classical and Modern Fourier Analysis. Pearson Education, Inc., New York (2004)
7. Guth, L., Katz, N.: On the Erdős distinct distance problem in the plane. Ann. Math. **181**, 155–190 (2015)
8. Hanson, B., Lund, B., Roche-Newton, O.: On distinct perpendicular bisectors and pinned distances in finite fields. Finite Fields Their Appl. **37**, 240–264 (2016)
9. Hart, D., Iosevich, A., Koh, D., Rudnev, M.: Averages over hyperplanes, sum-product theory in vector spaces over finite fields and the Erdős-Falconer distance conjecture. Trans. Am. Math. Soc. **363**(6), 3255–3275 (2011)
10. Hart, D., Li, L., Shen, C.: Fourier analysis and expanding phenomena in finite fields. Proc. Am. Math. Soc. **141**(2), 461–473 (2013)
11. Iosevich, A., Koh, D.: Extension theorems for spheres in the finite field setting. Forum Math. **22**(3), 457–483 (2010)
12. Iosevich, A., Rudnev, M.: Erdős distance problem in vector spaces over finite fields. Trans. Am. Math. Soc. **359**, 6127–6142 (2007)
13. Koh, D., Shen, C.: Sharp extension theorems and Falconer distance problems for algebraic curves in two dimensional vector spaces over finite fields. Rev. Mat. Iberoam. **28**(1), 157–178 (2012)
14. Koh, D., Shen, C.: The generalized Erdős-Falconer distance problems in vector spaces over finite fields. J. Number Theory **132**(11), 2455–2473 (2012)
15. Koh, D., Sun, H.: Distance sets of two subsets of vector spaces over finite fields. Proc. Am. Math. Soc. **143**(4), 1679–1692 (2015)
16. Lidl, R., Niederreiter, H.: Finite Fields. Cambridge University Press, Cambridge (1997)

17. Shparlinski, I.: On the set of distance between two sets over finite fields. Int. J. Math. Math. Sci. **59482**, 1–5 (2006)
18. Vinh, L.A.: Explicit Ramsey graphs and Erdős distance problem over finite Euclidean and non-Euclidean spaces. Electron. J. Comb. **15**, 1 (2008)
19. Vinh, L.A.: On the generalized Erdős distance problems over finite fields. J. Number Theory **133**(9), 2939–2947 (2013)