Distinct distances on regular varieties over finite fields

Pham Van Thang  Do Duy Hieu

Abstract

In this paper we study some generalized versions of a recent result due to Covert, Koh, and Pi (2015). More precisely, we prove that if a subset \( E \) in a regular variety satisfies \(|E| \gg q^{d^{2}+1/2} + 1\), then

\[
\Delta_k,F(E) := \{F(x^1 + \cdots + x^k) : x^i \in E, 1 \leq i \leq k\} \supseteq F_q \setminus \{0\},
\]

for some certain families of polynomials \( F(x) \in F_q[x_1, \ldots, x_d] \).

1 Introduction

Let \( F_q \) be a finite field of order \( q \), where \( q \) is a prime power. Let \( D(x) = x_1^2 + \cdots + x_d^2 \) be a polynomial in \( F_q[x_1, \ldots, x_d] \). For \( E \subset F_q^d \), we define the distance set of \( E \) to be

\[
\Delta(E) = \{D(x - y) : x, y \in E\}.
\]

There are various papers studying the cardinality \( |\Delta(E)| \), see for example [3, 4, 5, 6] and references therein. In this paper, we are interested in the case when \( E \) is a subset in a regular variety. Let us first start with a definition of regular varieties which is taken from [4].

Definition 1.1. For \( E \subset F_q^d \), let \( 1_E \) denote the characteristic function on \( E \). Let \( F(x) \in F_q[x_1, \ldots, x_d] \) be a polynomial. The variety \( V := \{x \in F_q^d : F(x) = 0\} \) is called a regular variety if \( |V| \asymp q^{d-1} \) and \( 1_V(m) \ll q^{-(d+1)/2} \) for all \( m \in F_q^d \setminus 0 \), where

\[
\hat{1}_V(m) = \frac{1}{q^d} \sum_{x \in F_q^d} \chi(-m \cdot x)1(x).
\]

Here and throughout, \( X \asymp Y \) means that there exist positive constants \( C_1 \) and \( C_2 \) such that \( C_1 Y < X < C_2 Y \), \( X \ll Y \) means that there exists \( C > 0 \) such that \( X \leq CY \), and \( X = o(Y) \) means that \( X/Y \to 0 \) as \( q \to \infty \), where \( X, Y \) are viewed as functions in \( q \).

There are several examples of regular varieties as follows:

1. Spheres of nonzero radii:

\[
S_j = \{x \in F_q^d : ||x|| = j\}, \quad j \in F_q^* := F_q \setminus \{0\}.
\]
2. A paraboloid:

\[ P = \{ x \in \mathbb{F}_q^d : x_1^2 + \cdots + x_{d-1}^2 = x_d \} \]

3. Spheres defined by “Minkowski distance” with nonzero radii:

\[ M_j = \{ x \in \mathbb{F}_q^d : x_1 \cdot x_2 \cdots x_d = j \} , \quad j \in \mathbb{F}_q^* \]

In 2007, Iosevich and Rudnev [9], using Fourier analytic methods, made the first investigation on the distinct distance problem on the unit sphere in \( \mathbb{F}_q^d \). More precisely, they proved the following.

**Theorem 1.2** (Iosevich et al., [9]). For \( \mathcal{E} \subseteq S_1 \) in \( \mathbb{F}_q^d \) with \( d \geq 3 \).

1. If \( |\mathcal{E}| \geq Cq^{d/2} \) with a sufficiently large constant \( C \), then there exists \( c > 0 \) such that \( |\Delta(\mathcal{E})| \geq cq \).

2. If \( d \) is even and \( |\mathcal{E}| \geq Cq^{d/2} \) with a sufficiently large constant \( C \), then \( \Delta(\mathcal{E}) = \mathbb{F}_q \).

3. If \( d \) is even, there exist \( c > 0 \) and \( \mathcal{E} \subset S_1 \) such that \( |\mathcal{E}| \geq cq^{d/2} \) and \( \Delta(\mathcal{E}) \neq \mathbb{F}_q \).

4. If \( d \) is odd and \( |\mathcal{E}| \geq Cq^{d+1} \) with a sufficiently large constant \( C > 0 \), then \( \Delta(\mathcal{E}) = \mathbb{F}_q \).

5. If \( d \) is odd, there exist \( c > 0 \) and \( \mathcal{E} \subset S_1 \) such that \( |\mathcal{E}| \geq cq^{d+1} \) and \( \Delta(\mathcal{E}) \neq \mathbb{F}_q \).

Recently, Covert, Koh, and Pi [1] studied a generalization of Theorem 1.2, namely they dealt with the following question: How large does a subset \( \mathcal{E} \) in a regular variety \( \mathcal{V} \) need to be to make sure that \( \Delta_{k,D}(\mathcal{E}) = \mathbb{F}_q \) or \( |\Delta_{k,D}(\mathcal{E})| \gg q \), where

\[ \Delta_{k,D}(\mathcal{E}) := \{ D(x^1 + \cdots + x^k) : x^i \in \mathcal{E}, 1 \leq i \leq k \} \quad (1.1) \]

The main idea in the proof of Theorem 1.2 is to reduce the distance problem to the dot product problem since the distance between two points \( x \) and \( y \) in \( S_1 \) is \( 2 - 2x \cdot y \), where \( x \cdot y = x_1 y_1 + \cdots + x_d y_d \). Therefore

\[ |\Delta(\mathcal{E})| = |\Pi_2(\mathcal{E})| := \{ x \cdot y : x, y \in \mathcal{E} \} . \quad (1.2) \]

For the case \( k \geq 3 \) and \( \mathcal{E} \subset S_1 \), one can check that

\[ |\Delta_{k,D}(\mathcal{E})| = |\Pi_k(\mathcal{E})| := \left| \sum_{i=1}^{k} \sum_{j=1}^{k} a_{ij} \cdot b_{ij} \cdot x^i \cdot x^j : x^i \in \mathcal{E}, 1 \leq l \leq k \right| , \]

where \( a_{ij} = 1 \) if \( i < j \) and 0 otherwise, and \( b_{ij} = 1 \) for \( i = 1 \) and \(-1 \) otherwise.

However, it seems hard to get a good estimate on \( |\Pi_k(\mathcal{E})| \) when \( k \geq 3 \), and if the unit sphere \( S_1 \) is replaced by a general regular variety \( \mathcal{V} \), there is no guarantee that the equality (1.2) will satisfy. Thus, in general, we can not apply the approach of the proof of Theorem 1.2 to estimate the cardinality of \( \Delta_{k,D}(\mathcal{E}) \).

Using a new approach with Fourier analytic techniques, Covert, Koh and Pi [1] established that the condition on the cardinality of \( \mathcal{E} \) in Theorem 1.2 can be improved to get \( \Delta_{k,D}(\mathcal{E}) = \mathbb{F}_q \) with \( k \geq 3 \). The precise statement of their result is as follows.


Theorem 1.3 (Covert et al., [4]). Suppose that $V \subseteq \mathbb{F}^d_q$ is a regular variety, and assume that $k \geq 3$ is an integer and $E \subseteq V$. If $q^{\frac{d-1}{2} + \frac{1}{k-1}} = o(|E|)$, then we have

$$\Delta_{k,D}(E) \supseteq \mathbb{F}^*_q$$

for even $d \geq 2$, and

$$\Delta_{k,D}(E) = \mathbb{F}_q$$

for odd $d \geq 3$.

It follows from Theorem 1.2 that in order to get $\Delta_{2,D}(E) = \mathbb{F}_q$, the sharp exponent of the sets $E$ of $S_1$ must be $d/2$ for even $d \geq 4$, and $(d+1)/2$ for odd $d \geq 3$. Theorem 1.3 implies that the exponent $d/2$ can be decreased to $\frac{d-1}{2} + \frac{1}{k-1}$ for $k \geq 3$ and any regular variety $V \subseteq \mathbb{F}^d_q$.

The main purpose of this note is to prove two generalizations of Theorem 1.3 by employing techniques from spectral graph theory. Our first result is the following.

Theorem 1.4. Let $Q$ be a non-degenerate quadratic form on $\mathbb{F}^d_q$. Suppose that $V \subseteq \mathbb{F}^d_q$ is a regular variety, and assume that $k \geq 3$ is an integer and $E \subseteq V$. If $q^{\frac{d-1}{2} + \frac{1}{k-1}} = o(|E|)$, then for any $t \in \mathbb{F}_q^*$ we have

$$|\{(x_1, \ldots, x_k) \in E^k : Q(x_1 + \cdots + x_k) = t\}| = (1 - o(1))\frac{|E|^k}{q}.$$

Corollary 1.5. Let $Q$ be a non-degenerate quadratic form on $\mathbb{F}^d_q$. Suppose that $V \subseteq \mathbb{F}^d_q$ is a regular variety, and assume that $k \geq 3$ is an integer and $E \subseteq V$. If $q^{\frac{d-1}{2} + \frac{1}{k-1}} = o(|E|)$, then we have

$$\Delta_{k,Q}(E) \supseteq \mathbb{F}^*_q.$$

Let $P(x) = \sum_{j=1}^d a_j x_j^s$ with $s \geq 2, a_j \neq 0$ for all $j = 1, \ldots, d$ be a diagonal polynomial in $\mathbb{F}_q[x_1, \ldots, x_d]$. We obtain the following generalization of Theorem 1.3 which is inspired by the paper [13].

Theorem 1.6. Suppose that $V \subseteq \mathbb{F}^d_q$ is a regular variety, and assume that $k \geq 3$ is an integer and $E \subseteq V$. For $X \subseteq \mathbb{F}_q$, if $|X||E|^{2k-2} \gg q^{(d-1)(k-1)+2}$, we have

$$|X + \Delta_{k,P}(E)| \gg q.$$

Corollary 1.7. Suppose that $V \subseteq \mathbb{F}^d_q$ is a regular variety, and assume that $k \geq 3$ is an integer and $E \subseteq V$. If $|E| \gg q^{\frac{d-1}{2} + \frac{1}{k-1}}$, we have

$$|\Delta_{k,P}(E)| \gg q.$$

The rest of this paper is organized as follows: In Sections 2 and 3, we construct some graphs which are main tools of our later proofs. The proofs of Theorems 1.4 and 1.6 are presented in Sections 4 and 5, respectively.
2 Pseudo-random graphs

For a graph $G$ of order $n$, let $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ be the eigenvalues of its adjacency matrix. The quantity $\lambda(G) = \max\{\lambda_2, -\lambda_n\}$ is called the second eigenvalue of $G$. A graph $G = (V, E)$ is called an $(n, d, \lambda)$-graph if it is $d$-regular, has $n$ vertices, and the second eigenvalue of $G$ is at most $\lambda$.

For two (not necessarily) disjoint subsets of vertices $U, W \subseteq V$, let $e(U, W)$ be the number of ordered pairs $(u, w)$ such that $u \in U$, $w \in W$, and $(u, w)$ is an edge of $G$. It is well known that if $\lambda$ is much smaller than the degree $d$, then $G$ has certain random-like properties. More precisely, we have the following result on the number of edges between subsets in an $(n, d, \lambda)$-graph.

**Lemma 2.1** (Chapter 9, [1]). Let $G = (V, E)$ be an $(n, d, \lambda)$-graph. For any two sets $B, C \subseteq V$, we have

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

In [8], Hanson et al. proved the following version of the expander mixing lemma on the number of edges between multi-sets of vertices in an $(n, d, \lambda)$-graph.

**Lemma 2.2** ([8]). Let $G = (V, E)$ be an $(n, d, \lambda)$-graph. The number of edges between two multi-sets of vertices $B$ and $C$ in $G$, which is denoted by $e(B, C)$, satisfies:

$$\left| e(B, C) - \frac{d|B||C|}{n} \right| \leq \lambda \sqrt{\sum_{b \in B} m_B(b)^2 \sqrt{\sum_{c \in C} m_C(c)^2}},$$

where $m_X(x)$ is the multiplicity of $x$ in $X$.

2.1 Finite Euclidean graphs

Let $Q$ be a non-degenerate quadratic form on $\mathbb{F}_q^d$. For any $t \in \mathbb{F}_q$, the finite Euclidean graph $E_q(d, Q, t)$ is defined as the graph with vertex set $\mathbb{F}_q^d$ and the edge set

$$E = \{(x, y) \in \mathbb{F}_q^d \times \mathbb{F}_q^d | x \neq y, Q(x - y) = t\}.$$  \hfill (2.1)

The $(n, d, \lambda)$ form of the graph $E_q(d, Q, t)$ is estimated in the following theorem.

**Theorem 2.3** (Bannai et al. [2], Kwok [11]). Let $Q$ be a non-degenerate quadratic form on $\mathbb{F}_q^d$. For any $t \in \mathbb{F}_q^*$, the graph $E_q(d, Q, t)$ is a $(q^d, (1 + o(1))q^{d-1}, 2q^{(d-1)/2})$-graph.

3 Pseudo-random digraphs

Let $G$ be a directed graph (digraph) on $n$ vertices where the in-degree and out-degree of each vertex are both $d$. 


We define the adjacency matrix of $G$, denoted by $A_G$, as follows: $a_{ij} = 1$ if there is a directed edge from $i$ to $j$ and zero otherwise. Let $\lambda_1 = d, \lambda_2, \ldots, \lambda_n$ be the eigenvalues of $A_G$. These numbers are complex numbers, so we can not order them, but we have $|\lambda_i| \leq d$ for all $1 \leq i \leq n$. We define $\lambda(G) := \max |\lambda_i| \neq d |\lambda_i|$.

An $n \times n$ matrix $A$ is normal if $A^t A = AA^t$, where $A^t$ is the transpose of $A$. We say that a digraph is normal if its adjacency matrix is a normal matrix. There is a simple way to check whether a digraph is normal. In a digraph $G$, let $N^+(x, y)$ be the set of vertices $z$ such that $\vec{zx}, \vec{zy}$ are edges, and $N^-(x, y)$ be the set of vertices $z$ such that $\vec{zx}, \vec{zy}$ are edges. One can easily check that $G$ is normal if and only if $|N^+(x, y)| = |N^-(x, y)|$ for any two vertices $x$ and $y$.

We say that $G$ is an $(n, d, \lambda)$-digraph if $G$ is normal and $\lambda(G) \leq \lambda$. Let $G$ be an $(n, d, \lambda)$-digraph. For two (not necessarily) disjoint subsets of vertices $U, W \subset V$, let $e(U, W)$ be the number of ordered pairs $(u, w)$ such that $u \in U, w \in W$, and $\vec{uw} \in E(G)$ (where $E(G)$ is the edge set of $G$). Vu [14] developed a directed version of the Lemma 2.1 as follows.

**Lemma 3.1** (Vu, [14]). Let $G = (V, E)$ be an $(n, d, \lambda)$-digraph. For any two sets $B, C \subset V$, we have

$$|e(B, C) - \frac{d}{n} |B||C| \leq \lambda \sqrt{|B||C|}.$$  

By using similar arguments as in the proofs of [8, Lemma 16] and [14, Lemma 3.1], we obtain the multiplicity version of Lemma 3.1.

**Lemma 3.2** (Multiplicity version). Let $G = (V, E)$ be an $(n, d, \lambda)$-digraph. For any two multi-sets $B$ and $C$ of vertices, we have

$$|e(B, C) - \frac{d}{n} |B||C| \leq \lambda \sqrt{\sum_{b \in B} m_B(b)^2 \sum_{c \in C} m_C(c)^2},$$  

where $m_X(x)$ is the multiplicity of $x$ in $X$.

We leave the proof of Lemma 3.2 to the interested reader.

4 Proof of Theorem 1.4

Let $H$ be a finite (additive) abelian group and $S$ be a subset of $H$. Define a directed Cayley graph $C_S$ as follows. The vertex of $C_S$ is $H$. There is a directed edge from $x$ to $y$ if and only if $y = x + s \in S$. It is clear that every vertex $C_S$ has out-degree $|S|$. Let $\chi_\alpha, \alpha \in H$, be the additive characters of $H$. It is well known that for any $\alpha \in H, \sum_{s \in S} \chi_\alpha(s)$ is an eigenvalue of $C_S$, with respect the eigenvector $(\chi_\alpha(x))_{x \in H}$.

Let $V$ be a regular variety defined by

$$V := \{x \in \mathbb{F}_q^d : F(x) = 0\},$$
for some polynomial $F \in \mathbb{F}_q[x_1, \ldots, x_d]$.

The Cayley graph $C_V$ is defined with $H = \mathbb{F}_q^d$ and $S = V$. In particular, the edge set of the Cayley graph $C_V$ is defined by

$$E(C_V) = \{(\overrightarrow{x, y}) \in H \times H : y - x \in V\}.$$  

For any two vertices $x$ and $y$ in $H$, we have

$$|N^+(x, y)| = |N^-(x, y)| = |(x + V) \cap (y + V)|,$$

which implies that $C_V$ is normal. We now study the $(n, d, \lambda)$ form of this digraph in the next theorem.

**Theorem 4.1.** The Cayley graph $C_V$ is a $(q^d, |V|, cq^{d-1}/2)$-digraph for some positive constant $c$.

**Proof.** It is clear that $C_V$ has $q^d$ vertices and the in-degree and out-degree of each vertex are both $|V|$. Next, we will estimate eigenvalues of $C_V$. The exponentials (or characters of the additive group $\mathbb{F}_q^d$)

$$\chi_m(x) = \chi(x \cdot m),$$

for $x, m \in \mathbb{F}_q^d$, are eigenfunctions of the adjacency operator for the graph $C_V$ corresponding to the eigenvalue

$$\lambda_m = \sum_{x \in V} \chi_m(x) = \sum_{x \in V} \chi(x \cdot m) = q^d \mathbf{1}_V(-m) \ll q^{(d-1)/2},$$

when $m \neq 0$. If $m = 0$, then $\lambda_0 = |V|$, which is the largest eigenvalue of $C_V$. In other words, $C_V$ is a $(q^d, |V|, cq^{d-1}/2)$-digraph for some positive constant $c$. \hfill $\Box$

In order to prove Theorem 4.1, we need the following notations.

For an even integer $k = 2m \geq 2$ and $E \subseteq \mathbb{F}_q^d$, the $k$-energy is defined by

$$\Lambda_k(E) = \left| \{(x^1, \ldots, x^k) \in E^k : x^1 + \cdots + x^m = x^{m+1} + \cdots + x^k \} \right|.$$  

For $E \subseteq \mathbb{F}_q^d$, we define

$$\nu_k(t) = \left| \{(x^1, \ldots, x^k) \in E^k : Q(x^1 + \cdots + x^k) = t \} \right|.$$  

In our next lemmas, we give estimates on the magnitude of $\nu_k(t)$.
Lemma 4.2. For $E \subset \mathbb{F}_q^d$ and $k \geq 2$ even, we have

$$\left| \nu_k(t) - (1 + o(1)) \frac{|E|^k}{q} \right| \leq q^{(d-1)/2} \Lambda_k(E).$$

Proof. Suppose that $k = 2m$. Let $A$ and $B$ be multi-sets of points in $\mathbb{F}_q^d$ defined as follows

$$A = \{ x_1 + \ldots + x_m : x_i \in E, 1 \leq i \leq m \}, \quad B = \{ -x_{m+1} - \ldots - x_k : x_i \in E, m+1 \leq i \leq k \}.$$

It is easy to check that

$$\sum_{a \in A} m_A(a)^2 = \Lambda_k(E), \quad \sum_{b \in B} m_B(b)^2 = \Lambda_k(E),$$

and $\nu_k(t)$ is equal to the number of edges between $A$ and $B$ in the graph $E_q(d, Q, t)$. Thus the lemma follows immediately from Lemma 2.2 and Theorem 2.3.

By using the same techniques, we get a similar result for the case $k$ odd.

Lemma 4.3. For $E \subset \mathbb{F}_q^d$ and $k \geq 3$ odd, we have

$$\left| \nu_k(t) - (1 + o(1)) \frac{|E|^k}{q} \right| \leq 2q^{(d-1)/2} \Lambda_k(E)^{1/2} \Lambda_{k+1}(E)^{1/2}.$$

Combining Lemmas 4.2 and 4.3 leads to the following theorem.

Theorem 4.4. Let $E$ be a set in $\mathbb{F}_q^d$. Then we have

1. If $q^{\frac{d+1}{2}}\Lambda_k(E) = o(|E|^k)$ and $k$ is even, then

$$\left| \left\{ (x_1, \ldots, x_k) \in E^k : Q(x_1 + \cdots + x_k) = t \right\} \right| = (1 + o(1)) \frac{|E|^k}{q}.$$

2. If $q^{\frac{d+1}{2}}(\Lambda_{k-1}(E))^{1/2}(\Lambda_{k+1}(E))^{1/2} = o(|E|^k)$ and $k$ is odd, then

$$\left| \left\{ (x_1, \ldots, x_k) \in E^k : Q(x_1 + \cdots + x_k) = t \right\} \right| = (1 + o(1)) \frac{|E|^k}{q}.$$

Theorem 4.4 implies that in order to prove Theorem 1.4, it is sufficient to bound $\Lambda_k(E)$.

Lemma 4.5. For a regular variety $V \subset \mathbb{F}_q^d$. If $k \geq 4$ is even, and $E \subset V$, we have

$$\left| \Lambda_k(E) - (1 + o(1)) \frac{|E|^{k-1}}{q} \right| \ll q^{(d-1)/2}(\Lambda_{k-2}(E))^{1/2}(\Lambda_k(E))^{1/2}.$$
Proof. Since $E$ is a subset in the variety $V$, we have the following estimate

$$
\Lambda_k(E) \leq \sum_{x_1, \ldots, x_{k-1} \in E} \mathbf{1}_V(x_1 + \cdots + x_{k/2} - x_{k/2+1} - \cdots - x_{k-1}).
$$

Let $A$ and $B$ be two multi-sets defined by

$$
A := \{x_1 + \cdots + x_{k/2} : x_i \in E, 1 \leq i \leq k/2\},
$$

and

$$
B := \{-x_{k/2+1} - \cdots - x_{k-1} : x_i \in E, k/2 + 1 \leq i \leq k - 1\}.
$$

It is clear that

$$
\sum_{a \in A} m_A(a)^2 = \Lambda_k(E), \quad \sum_{b \in B} m_B(b)^2 = \Lambda_{k-2}(E).
$$

On the other hand, $\Lambda_k(E)$ is equal to the number of edges between $A$ and $B$ in the Cayley graph $C_V$. Thus the lemma follows from Lemmas 3.2 and 4.1.

For $E \subseteq V$ and $k \geq 4$ even, it follows from Lemma 4.5 that

$$
\Lambda_k(E) \ll \frac{|E|^{k-1}}{q} + q^{(d-1)/2}(\Lambda_{k-2}(E))^{1/2}(\Lambda_k(E))^{1/2}.
$$

Solving this inequality in terms of $\Lambda_k(E)$ gives us

$$
\Lambda_k(E) \ll q^{d-1} \Lambda_{k-2}(E) + \frac{|E|^{k-1}}{q}.
$$

Using inductive arguments, we obtain the following estimate for $E \subseteq V$ and $k \geq 4$ even

$$
\Lambda_k(E) \ll q^{(d-1)(k-2)/2} \Lambda_2(E) + \frac{|E|^{k-1}}{q} \sum_{j=0}^{(k-4)/2} \left(\frac{q}{|E|^2}\right)^j.
$$

(4.2)

If we assume that $|E| > q^{(d-1)/2}$, then the inequality (4.2) implies the following theorem.

**Theorem 4.6.** Let $E$ be a subset of a regular variety $V$ in $\mathbb{F}_q^d$ with $|E| > q^{(d-1)/2}$.

1. If $k \geq 2$ is even, then

$$
\Lambda_k(E) \ll q^{(d-1)(k-2)/2} |E| + \frac{|E|^{k-1}}{q}.
$$

2. If $k \geq 3$ is odd, then

$$
\Lambda_{k-1}(E)\Lambda_{k+1}(E) \ll q^{(d-1)(k-2)} |E|^2 + q^{(d-1)(k-3)/2} |E|^{k+1} + \frac{|E|^{2k-2}}{q^2}.
$$
Note that the first statement of Theorem 4.6 follows from (4.2) with the facts that
\( \Lambda_2(E) = |E| \) and \( \frac{q^{d-1}}{p^2} < 1 \), and the second is a consequence of the first one.

We are now ready to prove Theorem 1.4.

**Proof of Theorem 1.4.** We now consider two following cases:

**Case 1:** If \( k \geq 2 \) is even and \( q^{\frac{d-1}{k-1}} = o(|E|) \), then it follows from Theorem 4.6 that
\[
q^{\frac{d+1}{2}} \Lambda_k(E) = o(|E|^k).
\]

**Case 2:** If \( k \geq 3 \) is odd and \( q^{\frac{d-1}{k-1}} = o(|E|) \), then it follows from Theorem 4.6 that
\[
q^{\frac{d+1}{2}} (\Lambda_{k-1}(E))^{1/2} (\Lambda_{k+1}(E))^{1/2} = o(|E|^k).
\]

In other words, Theorem 1.4 follows immediately from Theorem 4.4.

---

**5 Proof of Theorem 1.6**

To prove Theorem 1.6, we need to construct a new Cayley graph as follows.

Let \( P(x) = \sum_{j=1}^{d} a_j x_j^s \in \mathbb{F}_q[x_1, \ldots, x_d] \) with \( s \geq 2 \), \( a_j \neq 0 \) for all \( j = 1, \ldots, d \), and
\[
P'(x_1, \ldots, x_{2d}) = P(x_1, \ldots, x_d) - P(x_{d+1}, \ldots, x_{2d}) \in \mathbb{F}_q[x_1, \ldots, x_d].
\]

We define the graph \( C_{P'}(\mathbb{F}_q^{2d+1}) \) to be the Cayley graph with \( H = \mathbb{F}_q \times \mathbb{F}_q^{2d} \) and \( S = \{(x_0, x) \in \mathbb{F}_q \times \mathbb{F}_q^{2d} : x_0 + P'(x) = 0\} \), i.e.
\[
E(C_{P'}(\mathbb{F}_q^{2d+1})) = \left\{ ((x_0, x), (y_0, y)) \in H \times H : y_0 - x_0 + P'(y - x) = 0 \right\}.
\]

The \((n, d, \lambda)\) form of \( C_{P'}(\mathbb{F}_q^{2d+1}) \) was studied in [13].

**Lemma 5.1 ([13]).** For any odd prime power \( q \), \( d \geq 1 \), then \( C_{P'}(\mathbb{F}_q^{2d+1}) \) is a
\[
(q^{2d+1}, q^2, q^d) - \text{digraph}.
\]

For \( E \subseteq \mathbb{F}_q^d \) and \( X \subseteq \mathbb{F}_q^d \), define
\[
\nu_{P,k}(t) = \left| \{(a, x_1, \ldots, x_k) \in X \times E^k : a + P(x_1 + \cdots + x_k) = t\} \right|.
\]

Our next lemmas are the main steps in the proof of Theorem 1.6.

**Lemma 5.2.** For \( E \subseteq \mathbb{F}_q^d \) and \( k \geq 2 \) even, we have the following estimate
\[
\sum_{t \in \mathbb{F}_q} \nu_{P,k}(t)^2 \leq \frac{|E|^{2k}|X|^2}{q} + q^d|X|\Lambda_k(E)^2.
\]
Proof. Let $A$ and $B$ be multi-sets defined by:

$$A := \{ (a, -x_1 - \cdots - x_{k/2}, -y_1 - \cdots - y_{k/2}) : a \in X, x_i, y_i \in E \},$$

and

$$B := \{ (b, x_{k/2+1} + \cdots + x_k, y_{k/2+1} + \cdots + y_{k/2+1}) : b \in X, x_i, y_i \in E \}.$$

One can check that

$$\sum_{x \in A} m_A(x)^2 = |X| \Lambda_k(E)^2,$$

$$\sum_{x \in B} m_B(x)^2 = |X| \Lambda_k(E)^2,$$

and

$$|A| = |B| = |X||E|^k.$$

On the other hand, it is clear that $\sum_{t \in \mathbb{F}_q} \nu_{P,k}(t)^2$ is equal to the number of edges from $A$ to $B$ in the graph $C_{P'}(\mathbb{F}_q^{2d+1})$. Thus it follows from Lemma 3.2 and Theorem 5.1 that

$$\sum_{t \in \mathbb{F}_q} \nu_{P,k}(t)^2 \leq \frac{|E|^2|X|^2}{q} + q^d |X| \Lambda_k(E)^2.$$

This ends the proof of the lemma.

By employing the same techniques, we get a similar result for the case $k \geq 3$ odd.

Lemma 5.3. For $E \subseteq \mathbb{F}_q^d$ and $k \geq 3$ odd, we have the following estimate

$$\sum_{t \in \mathbb{F}_q} \nu_{P,k}(t)^2 \leq \frac{|E|^{2k}|X|^2}{q} + q^d |X| \Lambda_{k-1}(E) \Lambda_{k+1}(E).$$

We are now ready to prove Theorem 1.6.

Proof of Theorem 1.6. It follows from the proof of Theorem 2.6 in [13] that

$$|X + \Delta_{k,P}(E)| \gtrsim \frac{|X|^2|E|^{2k}}{\sum_{t \in \mathbb{F}_q} \nu_{P,k}(t)^2}.$$ 

Therefore from Lemma 3.2 and Lemma 5.3 we get two following cases:

1. If $k \geq 2$ is even, we obtain

$$|X + \Delta_{k,P}(E)| \gtrsim \min \left\{ \frac{|X||E|^{2k}}{q^d \Lambda_k(E)^2}, q \right\}.$$

2. If $k \geq 3$ is odd, we obtain

$$|X + \Delta_{k,P}(E)| \gtrsim \min \left\{ \frac{|X||E|^{2k}}{q^d \Lambda_k(E) \Lambda_{k-1}(E)}, q \right\}.$$

Thus Theorem 1.6 follows immediately from Theorem 4.6 which concludes the proof of the theorem.
Acknowledgements.

The first author was partially supported by Swiss National Science Foundation grants 200020-162884 and 200020-144531.

References

[1] N. Alon and J. H. Spencer, *The probabilistic method*, 2nd ed., Willey-Interscience, 2000.

[2] E. Bannai, O. Shimabukuro and H. Tanaka, *Finite analogues of non-Euclidean spaces and Ramanujan graphs*, European Journal of Combinatorics 25 (2004), 243–259.

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

[4] D. Covert, D. Koh, Y. Pi, *The k-resultant modulus set problem on algebraic varieties over finite fields*, arXiv: 1508.02688 (2015).

[5] D. Covert, D. Koh, and Y. Pi, *On the sums of any k points in finite fields*, accepted in SIAM 2016.

[6] G. Mockenhaupt, T. Tao, *Restriction and Kakeya phenomena for finite fields*, Duke Math. J. 121 (2004), no. 1, 35–74.

[7] D. Hart, A. Iosevich, J. Solymosi, *Sum-product estimates in finite fields via Kloosterman sums*, Int. Math. Res. Not. no. 5, (2007) Art. ID rnm007.

[8] B. Hanson, B. Lund, and O. Roche-Newton, *On distinct perpendicular bisectors and pinned distances in finite fields*, Finite Fields and Their Applications, 37 (2016), 240–264.

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

[10] D. Koh and H. Sun, *Distance sets of two subsets of vector spaces over finite fields*, PAMS, to appear, [arXiv:1212.5305](https://arxiv.org/abs/1212.5305).

[11] W.M. Kwok, *Character tables of association schemes of affine type*, European J. Combin. 13 (1992) 167–185.

[12] D. Koh and C-Y. Shen, *The generalized Erdős-Falconer distance problems in vector spaces over finite fields*, Journal of Number Theory, 132(11) (2012): 2455–2473.

[13] L.A.Vinh, *On the generalized Erdős–Falconer distance problems over finite fields*, J. Number Theory, 133 (2013) 2939–2947.
[14] Vu Ha Van, *Sum-product estimates via directed expanders*, Mathematical research letters, 15(2) (2008): 375–388.

Department of Mathematics,  
EPF Lausanne  
Switzerland  
E-mail: thang.pham@epfl.ch

Institute of Mathematics,  
Vietnam Academy of Science and Technology  
E-mail: ddhieu@math.ac.vn