An Asymmetric Bound for Sum of Distance Sets
Daewoong Cheong\textsuperscript{a}, Doowon Koh\textsuperscript{a}, and Thang Pham\textsuperscript{b,c}

Received July 25, 2020; revised February 25, 2021; accepted June 24, 2021

To the 130th anniversary of I. M. Vinogradov

Abstract—For $E \subseteq \mathbb{F}_q^d$, let $\Delta(E)$ denote the distance set determined by pairs of points in $E$. By using additive energies of sets on a paraboloid, Koh, Pham, Shen, and Vinh (2020) proved that if $E, F \subseteq \mathbb{F}_q^d$ are subsets with $|E| \cdot |F| \gg q^{d+1}/3$, then $|\Delta(E) + \Delta(F)| > q/2$. They also proved that the threshold $q^{d+1}/3$ is sharp when $|E| = |F|$. In this paper, we provide an improvement of this result in the unbalanced case, which is essentially sharp in odd dimensions. The most important tool in our proofs is an optimal $L^2$ restriction theorem for the sphere of zero radius.

DOI: 10.1134/S0081543821040131

1. INTRODUCTION

Let $\mathbb{F}_q$ be a finite field of order $q$, where $q$ is an odd prime power. For $x = (x_1, \ldots, x_d)$ and $y = (y_1, \ldots, y_d)$ in $E$, define a distance between $x$ and $y$ by

$$\|x - y\| := (x_1 - y_1)^2 + \ldots + (x_d - y_d)^2,$$

which is the square of an analog of the Euclidean distance. We denote by $\Delta(E)$ the set of distances determined by pairs of points in $E$, namely,

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

The Erdős–Falconer distance problem in $\mathbb{F}_q^d$ asks for the smallest exponent $N$ such that for any $E \subseteq \mathbb{F}_q^d$ with at least $q^N$ elements, the number of distinct distances determined by pairs of points in $E$ is at least $cq$, for some constant $0 < c < 1$.

Iosevich and Rudnev [6] showed that if $|E| \geq 4q^{(d+1)/2}$, then $|\Delta(E)| = q$, which means that for any $\lambda \in \mathbb{F}_q$, there exist two points $x, y \in E$ such that $\|x - y\| = \lambda$. Hart et al. [1] proved that the exponent $(d + 1)/2$ is essentially sharp in odd dimensions, even though we wish to cover a positive proportion of all distances. However, in even dimensions, it is conjectured that the right exponent should be $d/2$. We refer the interested reader to [8, 11] and references therein for the most recent progress on this conjecture.

Let $E$ and $F$ be sets in $\mathbb{F}_q^d$; in this paper, we focus on the following analog: How large do $E$ and $F$ need to be to guarantee the inequality

$$|\Delta(E) + \Delta(F)| \gg q?$$

\textsuperscript{a}Department of Mathematics, Chungbuk National University, Cheongju, Chungbuk, 28644, Korea.
\textsuperscript{b}Department of Mathematics, HUS, Vietnam National University, 100000 Hanoi, Vietnam.
\textsuperscript{c}The group Theory of Combinatorial Algorithms, ETH Zurich, 8092 Zurich, Switzerland.
E-mail addresses: daewoongc@chungbuk.ac.kr (D. Cheong), koh131@chungbuk.ac.kr (D. Koh), vanthang.pham@inf.ethz.ch (T. Pham).

279
Here, and throughout this paper, for simplicity, we will use $C$ to denote a sufficiently large constant independent of the field size $q$. We also use the following notation: $X \ll Y$ means that there exists some absolute constant $C_1 > 0$ such that $X \leq C_1 Y$, and $X \sim Y$ means $Y \ll X \ll Y$.

Suppose $E, F \subset \mathbb{F}_{q}^{d}$. One can easily check that $\Delta(E) + \Delta(F) = \Delta(E \times F)$, where $\Delta(E \times F)$ is obviously defined as the distance set determined by the product set $E \times F$ in $\mathbb{F}_{q}^{2d}$. Thus, it follows trivially from Iosevich and Rudnev’s result that if $|E| \cdot |F| \geq 4q^{(2d+1)/2}$, then $\Delta(E) + \Delta(F) = \mathbb{F}_{q}$.

It has been proved in [3, 13] that the Iosevich–Rudnev exponent can be decreased for Cartesian product structure sets. Hence, we can expect a smaller exponent for the problem of $\Delta(E) + \Delta(F) = \Delta(E \times F)$ in $\mathbb{F}_{q}^{2d}$.

In a recent paper, by using results on additive energies of sets on a paraboloid, Koh, Pham, Shen, and Vinh [7] showed that the exponent $d + 1/2$ can be decreased to $d + 1/3$ as follows.

**Theorem 1.1** [7]. Let $E$ and $F$ be sets in $\mathbb{F}_{q}^{d}$. Suppose either $d = 4k - 2$ and $q \equiv 3 \mod 4$ or $d \geq 3$ is odd. If $|E| \cdot |F| \geq Cq^{d+1/3}$ for some big positive constant $C$, then $|\Delta(E) + \Delta(F)| > q/2$.

They also constructed examples to show that the exponent $d + 1/3$ is optimal for the case $|E| = |F|$ in odd dimensions. Using the same approach, they indicated that the Erdős–Falconer distance conjecture holds for sets of the form $A^{4} \subset \mathbb{F}_{q}^{4}$, where $q$ is a prime number and $A$ is a multiplicative subgroup in $\mathbb{F}_{q}$.

We note that in the form of $\Delta(E, F) + \Delta(E, F)$, where $\Delta(E, F) := \{|x - y| : x \in E, y \in F\}$, it was first proved by Shparlinski [14, Corollary 2] that

$$
|\Delta(E, F) + \Delta(E, F)| \geq \frac{1}{3} \min \left\{ \frac{|E| \cdot |F|}{q^{d-1}}, \frac{|E| \cdot |F|^{2}}{q^{3d/2}} \right\},
$$

which is non-trivial when the sizes of sets $E$ and $F$ differ significantly. A simple graph theoretic proof of this result and applications can be found in the work of Hegyvári and Pálffy in [2].

From the Iosevich–Rudnev result [6], we observe that if the size of $E$ (respectively, $F$) is at least $4q^{(d+1)/2}$, then $|\Delta(E)| = q$ (respectively, $|\Delta(F)| = q$), and so we have $|\Delta(E) + \Delta(F)| = q$. Hence, in the rest of this paper, without loss of generality, we assume that $|E|, |F| < 4q^{(d+1)/2}$.

The main purpose of this paper is to give improvements of Theorem 1.1 in the unbalanced case, namely, $|E| \neq |F|$. As mentioned before, Theorem 1.1 was obtained as an application of additive energy estimates on subsets of a paraboloid. However, it turns out that this method is somewhat inefficient in the unbalanced cases of sets. Here, as a main tool, we take advantage of $L^2$-restriction estimates for the sphere of zero radius. As a consequence, we have the following improved result of Theorem 1.1.

**Theorem 1.2.** Let $E$ and $F$ be sets in $\mathbb{F}_{q}^{d}$. Suppose either $d = 4k - 2$ and $q \equiv 3 \mod 4$ or $d \geq 3$ is odd. Then there exists a large positive constant $C$ such that if either $|E| \cdot |F|^{2} \geq Cq^{(3d+1)/2}$ or $|E|^{2}|F| \geq Cq^{(3d+1)/2}$, then we have

$$
|\Delta(E) + \Delta(F)| > \frac{q}{2}.
$$

Let us briefly sketch some ideas in the proof of Theorem 1.2. The main idea is to bound the $L^2$-norm of the distance measure. More precisely, for $t \in \mathbb{F}_{q}$, let $\nu(t)$ be the number of pairs $(x, y) \in (E \times F) \times (E \times F)$ such that $\|x - y\| = t$. By the Cauchy–Schwarz inequality, to prove Theorem 1.2, it is enough to obtain a good upper bound for $\sum_{t \in \mathbb{F}_{q}} \nu(t)^{2}$. In Section 3, we will show that the sum $\sum_{t \in \mathbb{F}_{q}} \nu(t)^{2}$ can be bounded via a sphere restriction estimate, namely,

$$
\sum_{t \in \mathbb{F}_{q}} \nu(t)^{2} \leq \frac{|E|^{4}|F|^{4}}{q} + q^{6d} \left( q^{-3d}|E|^{2}|F| \right) \max_{m \in \mathbb{F}_{q}} \sum_{r \in \mathbb{F}_{q}} |\hat{F}(m)|^{2},
$$
where \( S_r^{d-1} \) is the sphere centered at the origin of radius \( r \) in \( \mathbb{F}_q^d \). The conditions on \( q \) and \( d \) as in Theorem 1.2 are necessary in order to derive a good upper bound for the restriction estimate \( \sum_{m \in S_r^{d-1}} |\hat{\mathcal{F}}(m)|^2 \). For other even dimensions, we will provide more discussion in Remark 3.5.

To see how much Theorem 1.2 is better than Theorem 1.1, let us make a brief comparison.

If \( |E| \cdot |F| \geq C q^{d+1/3} \), then either \( |E| \cdot |F|^2 \geq C q^{(3d+1)/2} \) or \( |E|^2 |F| \geq C q^{(3d+1)/2} \). Indeed, otherwise, one has \( |E| \cdot |F| < C^{2/3} q^{d+1/3} \), a contradiction. When \( |E| = |F| \), both Theorems 1.1 and 1.2 give the same exponent \( d/2 + 1/6 \). For \( 0 < \epsilon < 1/3 \), one can check that for \( E, F \subset \mathbb{F}_q^d \) with \( |E| = q^{(d-1)/2+2\epsilon} \) and \( |F| = q^{(d+1)/2-\epsilon} \), we have \( |E| \cdot |F| = q^{d+\epsilon} \). For these sets, Theorem 1.1 does not tell us about the size of \( \Delta(E) + \Delta(F) \), but Theorem 1.2 gives the expected lower bound \( cq \).

Theorem 1.2 is essentially sharp in odd dimensions. To see this, let us recall the following result from [1, Lemma 5.1]. If either \( n \geq 2 \) is even and \( q \equiv 1 \mod 4 \) or \( n = 4k, k \in \mathbb{N} \), then there exist \( n/2 \) linearly independent vectors \( v_1, \ldots, v_{n/2} \) in \( \mathbb{F}_q^n \) such that \( v_i \cdot v_j = 0 \) for all \( 1 \leq i, j \leq n/2 \). Thus, if either \( d = 4k + 3 \) and \( q \equiv 1 \mod 4 \) or \( d = 4k + 1, k \in \mathbb{N} \), then we can always choose a subspace \( V \) spanned by \( (d-1)/2 \) vectors contained in \( \mathbb{F}_q^{d-1} \times \{0\} \) such that \( u \cdot v = 0 \) for all \( u, v \in V \). Set \( E = V \). It is not hard to check that \( \Delta(E) = \{0\} \). It has also been indicated in the proof of [1, Theorem 2.7] that for any \( \epsilon > 0 \), there exists a set \( F \subset \mathbb{F}_q^d \) such that \( |F| \sim q^{(d+1)/2-\epsilon} \) and \( |\Delta(E)| \sim q^{1-\epsilon} \). In other words, we have \( |E| \cdot |F|^2 \sim q^{(3d+1)/2-2\epsilon} \) and \( |\Delta(E) + \Delta(F)| \sim q^{1-\epsilon} \) for any \( \epsilon > 0 \).

It is worth noting that one cannot hope to deduce the conclusion of Theorem 1.2 in all even dimensions with \( q \equiv 1 \mod 4 \); namely, in Construction 3.4 of Section 3, we will provide examples which tell us that there are sets \( E, F \subset \mathbb{F}_q^d \) with \( d \) even and \( q \equiv 1 \mod 4 \) such that \( |E| \cdot |F|^2 \sim q^{3d/2+2/3} \) and \( |\Delta(E) + \Delta(F)| \leq q/2 \).

While Theorem 1.2 is sharp in odd dimensions, we believe that in the corresponding even dimensions the right condition should be \( |E| \cdot |F|^2 \geq C q^{3d/2} \) or \( |E|^2 |F| \geq C q^{3d/2} \), which is in line with the Erdős–Falconer distance conjecture.

Restricting our attention to prime fields, we obtain an improvement of Theorem 1.2 in two dimensions.

**Theorem 1.3.** Let \( q \equiv 3 \mod 4 \) be a prime number, \( E \) and \( F \) be sets in \( \mathbb{F}_q^2 \), and \( C \) be a large positive constant. If either \( |E|^4 |F|^6 \geq C q^{11} \) or \( |E|^6 |F|^4 \geq C q^{11} \), then we have

\[
|\Delta(E) + \Delta(F)| \gg q.
\]

As in the proof of Theorem 1.2, it is enough to bound \( \sum_{t \in \mathbb{F}_q} \nu(t)^2 \) from above. It has been indicated in [12] that the sum \( \sum_{t \in \mathbb{F}_q} \nu(t)^2 \) can be reduced to the sum \( \sum_{r \in \mathbb{F}_q} \mu(r)^2 \), where \( \mu(r) \) is the number of pairs \( (x, y) \in E \times E \) such that \( \|x - y\| = r \). Using the fact that \( \sum_{r \in \mathbb{F}_q} \mu(r)^2 \) can be bounded by roughly \( |E| T(E) \), where \( T(E) \) denotes the number of non-degenerate isosceles triangles determined by points in \( E \), and a very recent upper bound of \( T(E) \) in [11], we are able to obtain a better upper bound for \( \sum_{t \in \mathbb{F}_q} \nu(t)^2 \).

The following corollary is an immediate consequence of the above theorem.

**Corollary 1.4.** Let \( q \equiv 3 \mod 4 \) be a prime number, \( E \) be a set in \( \mathbb{F}_q^2 \), and \( C \) be a large positive constant. If \( |E| \geq C q^{11/10} \), then we have

\[
|\Delta(E) + \Delta(E)| \gg q.
\]

**Remark 1.5.** It follows from Theorems 1.2 and 1.3 that the sumset of distance sets is large under a weaker assumption on the sets, which implies that if there exists a counter-example to the distance set conjecture, then the critical set does not have much arithmetic structure. The same might also hold for the product of distance sets, which will be addressed in a sequel paper.
The rest of this paper is organized as follows. In Section 2, we recall some notation from discrete Fourier analysis and prove some key lemmas. Theorems 1.2 and 1.3 will be proved in Sections 3 and 4, respectively.

2. PRELIMINARY LEMMAS

2.1. Discrete Fourier analysis and Gauss sums. The Fourier transform is defined by

\[ \hat{f}(\alpha) = q^{-n} \sum_{\beta \in \mathbb{F}_q^n} \chi(-\alpha \cdot \beta) f(\beta), \]

where \( f \) is a complex-valued function on \( \mathbb{F}_q^n \). Here, and throughout this paper, \( \chi \) denotes the principal additive character of \( \mathbb{F}_q \). Recall that the orthogonality of the additive character \( \chi \) says that

\[ \sum_{\alpha \in \mathbb{F}_q^n} \chi(\beta \cdot \alpha) = \begin{cases} 0 & \text{if } \beta \neq (0, \ldots, 0), \\ q^n & \text{if } \beta = (0, \ldots, 0). \end{cases} \]

As a direct application of the orthogonality of \( \chi \), the following Plancherel theorem can be proved: for any set \( \Omega \) in \( \mathbb{F}_q^n \),

\[ \sum_{\alpha \in \mathbb{F}_q^n} |\hat{\Omega}(\alpha)|^2 = q^{-n} |\Omega|. \]

In this paper, we identify a set \( \Omega \) with the indicator function \( 1_\Omega \) on \( \Omega \). It is not hard to prove the following formula which is referred to as the Fourier inversion theorem:

\[ f(\beta) = \sum_{\alpha \in \mathbb{F}_q^n} \chi(\alpha \cdot \beta) \hat{f}(\alpha). \]

Throughout this paper, we denote by \( \eta \) the quadratic character of \( \mathbb{F}_q^* \). For \( a \in \mathbb{F}_q^* \), the Gauss sum \( G_a \) is defined by

\[ G_a = \sum_{s \in \mathbb{F}_q^*} \eta(s) \chi(as). \]

The Gauss sum \( G_a \) is also written as

\[ G_a = \sum_{s \in \mathbb{F}_q} \chi(as^2) = \eta(a) G_1. \]

The absolute value of the Gauss sum \( G_a \) is exactly \( \sqrt{q} \). Moreover, the explicit value of the Gauss sum \( G_1 \) is well-known.

**Lemma 2.1** [9, Theorem 5.15]. Let \( \mathbb{F}_q \) be a finite field with \( q = p^\ell \), where \( p \) is an odd prime and \( \ell \in \mathbb{N} \). Then we have

\[ G_1 = \begin{cases} (-1)^{\ell-1} q^{1/2} & \text{if } p \equiv 1 \text{ mod } 4, \\ (-1)^{\ell-1} \ell q^{1/2} & \text{if } p \equiv 3 \text{ mod } 4. \end{cases} \]

The following corollary follows from the explicit value of the Gauss sum \( G_1 \). For the sake of completeness, we include a proof here.

**Corollary 2.2.** Let \( \eta \) be the quadratic character of \( \mathbb{F}_q^* \). Then, for any positive integer \( n \equiv 2 \text{ mod } 4 \) and \( q \equiv 3 \text{ mod } 4 \), we have

\[ G_1^n = -q^{n/2}. \]
It follows from the definition of the Fourier transform that
\[ G_1^m = (-1)^{(\ell-1)(4k-2)} q^{n/2} = (-1)^\ell q^{n/2} = -q^{n/2}. \]  

Completing the square and using a change of variables, it is not hard to show that
\[ \sum_{s \in \mathbb{F}_q} \chi(as^2 + bs) = \eta(a)G_1 \chi \left( \frac{b^2}{4a} \right), \quad (2.1) \]
for any \( a \in \mathbb{F}_q^* \) and \( b \in \mathbb{F}_q \).

### 2.2. \( L^2 \) Fourier restriction estimates for spheres.
We recall that for each \( r \in \mathbb{F}_q \), the sphere \( S^{d-1}_r \) in \( \mathbb{F}_q^d \) with radius \( r \) is defined by
\[ S^{d-1}_r = \left\{ x \in \mathbb{F}_q^d : \sum_{i=1}^d x_i^2 = r \right\}. \]
Notice that compared to the Euclidean setting, we have no condition on \( r \).

It is well known that the Fourier transform \( S^{d-1}_j(m) \) is closely related to the Kloosterman sum
\[ K(a, b) := \sum_{s \in \mathbb{F}_q^*} \chi(as + b/s), \]
or the twisted Kloosterman sum
\[ TK(a, b) := \sum_{s \in \mathbb{F}_q^*} \eta(s)(as + b/s), \]
where \( a, b \in \mathbb{F}_q \) and \( \eta \) denotes the quadratic character of \( \mathbb{F}_q \). In particular, the next lemma was given in [4, Lemma 4].

**Lemma 2.3.** For \( m \in \mathbb{F}_q^d \), let \( \delta_0(m) = 1 \) if \( m = (0, \ldots, 0) \) and \( \delta_0(m) = 0 \) otherwise.

1. If \( d \geq 3 \) is an odd integer, then for \( m \in \mathbb{F}_q^d \),
\[ \widehat{S}^{d-1}_j(m) = q^{-1} \delta_0(m) + q^{-d-1} \eta(-1)G_1^d TK(j, \frac{\|m\|}{4}). \]

2. If \( d \geq 2 \) is an even integer, then for \( m \in \mathbb{F}_q^d \),
\[ \widehat{S}^{d-1}_j(m) = q^{-1} \delta_0(m) + q^{-d-1} G_1^d K\left(j, \frac{\|m\|}{4}\right). \]

Recall that \( |K(a, b)| \leq 2q^{1/2} \) if \( ab \neq 0 \), and \( |TK(a, b)| \leq 2q^{1/2} \) if \( a, b \in \mathbb{F}_q \) (see, for example, [9]). For \( F \subset \mathbb{F}_q^d \) and \( j \in \mathbb{F}_q \), consider the \( L^2 \) Fourier restriction for the sphere \( S^{d-1}_j \)
\[ \mathcal{M}_j(F) := \sum_{m \in S^{d-1}_j} |\hat{F}(m)|^2. \]
It follows from the definition of the Fourier transform that
\[ \mathcal{M}_j(F) = q^{-d} \sum_{x, y \in F} \widehat{S}^{d-1}_j(x - y). \quad (2.2) \]

In the next result, we give an upper bound for this quantity.
Proposition 2.4. Let $F$ be a subset of $\mathbb{F}_q^d$. Suppose that either $d = 4k - 2$ and $q \equiv 3 \pmod{4}$ or $d \geq 3$ is odd. Then we have
\[
\max_{j \in \mathbb{F}_q^d} \mathcal{M}_j(F) \leq q^{-d-1}|F| + 2q^{(-3d-1)/2}|F|^2.
\]

Proof. Case 1. Suppose that $d$ is odd. Combining (2.2) with the first part of Lemma 2.3, we get
\[
\mathcal{M}_j(F) = q^{-d-1}|F| + q^{-2d-1}G_1^{d} (-1) \sum_{x,y \in F} TK \left( j, \frac{\|x - y\|}{4} \right).
\]
Since the absolute value of the twisted Kloosterman sum is bounded by $2q^{1/2}$ and $|G_1| = q^{1/2}$, we have
\[
\mathcal{M}_j(F) \leq q^{-d-1}|F| + 2q^{(-3d-1)/2}|F|^2.
\]
Since this bound is independent of $r \in \mathbb{F}_q$, we complete the proof.

Case 2. Assume that $d$ is even with $d = 4k - 2$, and $q \equiv 3 \pmod{4}$. By combining (2.2) with the second part of Lemma 2.3, we have
\[
\mathcal{M}_j(F) = q^{-d-1}|F| + q^{-2d-1}G_1^{d} \sum_{x,y \in F} K \left( j, \frac{\|x - y\|}{4} \right).
\]
If $j \neq 0$, then the Kloosterman sum $|K(j, \|x - y\|/4)|$ is bounded by $2q^{1/2}$. Hence, as in case 1, we obtain
\[
\max_{j \neq 0} \mathcal{M}_j(F) \leq q^{-d-1}|F| + 2q^{(-3d-1)/2}|F|^2.
\]
To complete the proof, it therefore remains to show that
\[
\mathcal{M}_0(F) \leq q^{-d-1}|F| + 2q^{(-3d-1)/2}|F|^2.
\]
(2.3)
In fact, we can prove that
\[
\mathcal{M}_0(F) \leq q^{-d-1}|F| + q^{(-3d-2)/2}|F|^2,
\]
(2.4)
which is much stronger. Indeed,
\[
\mathcal{M}_0(F) = q^{-d-1}|F| + q^{-2d-1}G_1^{d} \sum_{x,y \in F} K \left( 0, \frac{\|x - y\|}{4} \right)
\]
\[
= q^{-d-1}|F| + q^{-2d-1}G_1^{d} \sum_{x,y \in F:\|x - y\|=0} K(0,0) + q^{-2d-1}G_1^{d} \sum_{x,y \in F:\|x - y\|\neq 0} (-1) K \left( 0, \frac{\|x - y\|}{4} \right).
\]
Using the facts that $K(0,0) = q - 1$ and $K(0,s) = -1$ for $s \neq 0$,
\[
\mathcal{M}_0(F) = q^{-d-1}|F| + q^{-2d-1}G_1^{d} \sum_{x,y \in F:\|x - y\|=0} (q - 1) + q^{-2d-1}G_1^{d} \sum_{x,y \in F:\|x - y\|\neq 0} 1.
\]
\[
= q^{-d-1}|F| + q^{-2d}G_1^{d} \sum_{x,y \in F:\|x - y\|=0} 1 - q^{-2d-1}G_1^{d} \sum_{x,y \in F} 1.
\]
Since $G_1^{d} = -q^{d/2}$ by Corollary 2.2, the second term above is negative and the third term equals $q^{(-3d-2)/2}|F|^2$. Thus, we obtain
\[
\mathcal{M}_0(F) \leq q^{-d-1}|F| + q^{(-3d-2)/2}|F|^2,
\]
as required.

We remark here that one can apply directly Theorem 1.3 in [5] for characteristic functions to give a bound which is better than (2.3), but weaker than (2.4).
3. PROOF OF THEOREM 1.2

In this section, we devote ourselves to giving a proof of Theorem 1.2. Our idea is to involve a suitable algebraic variety in the Fourier analysis. An advantage in using an algebraic variety argument is that it offers a new form for the upper bound of the $L^2$-norm of a certain counting function, which is more manageable for our purpose afterwards.

**Algebraic variety and related Fourier transform.** Let $X = (x, y)$ be the coordinates of $\mathbb{F}_q^{2d} \times \mathbb{F}_q^{2d} = \mathbb{F}_q^{4d}$, and let $\|X\|_*$ be the homogeneous polynomial defined by

$$
\|X\|_* := \|x\| - \|y\| = x_1^2 + \ldots + x_{2d}^2 - z_1^2 - \ldots - z_{2d}^2.
$$

**Definition 3.1.** Let $V_0$ be the subvariety of $\mathbb{F}_q^{4d}$ cut out by the equation $\|X\|_* = 0$, i.e.,

$$
V_0 := \{ X \in \mathbb{F}_q^{4d} : \|X\|_* = 0 \}.
$$

We need the following Fourier transform of the variety $V_0$ in $\mathbb{F}_q^{4d}$.

**Lemma 3.2.** If $M \in \mathbb{F}_q^{4d}$, then we have

$$
\hat{V}_0(M) := q^{-4d} \sum_{X \in V_0} \chi(-M \cdot X) = \begin{cases} 
q^{-1}\delta_0(M) + q^{-2d-1}(q - 1) & \text{if } \|M\|_* = 0, \\
-q^{-2d-1} & \text{if } \|M\|_* \neq 0.
\end{cases}
$$

**Proof.** It follows from the orthogonality of $\chi$ that

$$
\hat{V}_0(M) = q^{-4d} \sum_{X \in V_0} \chi(-M \cdot X) = q^{-1}\delta_0(M) + q^{-4d-1} \sum_{X \in \mathbb{F}_q^{4d}} \sum_{s \neq 0} \chi(s\|X\|_* - M \cdot X).
$$

From formula (2.1), it follows that

$$
\hat{V}_0(M) = q^{-1}\delta_0(M) + q^{-4d-1}G_{1d}^d \sum_{s \neq 0} \eta^{2d}(s)\eta^{2d}(-s)\chi\left(\frac{\|M\|_*}{4s}\right).
$$

Since $\eta^{2d} = 1$, by a change of variables, one has

$$
\hat{V}_0(M) = q^{-1}\delta_0(M) + q^{-4d-1}G_{1d}^d \sum_{r \neq 0} \chi(r\|M\|_*).
$$

By the orthogonality of $\chi$,

$$
\hat{V}_0(M) = \begin{cases} 
q^{-1}\delta_0(M) + G_{1d}^d q^{-4d-1}(q - 1) & \text{if } \|M\|_* = 0, \\
-G_{1d}^d q^{-4d-1} & \text{if } \|M\|_* \neq 0.
\end{cases}
$$

Since $G_{1d}^d = q^{2d}$, the proof is complete. □

By invoking Lemma 3.2, we are able to deduce the following lemma.

**Lemma 3.3.** Let $D \subset \mathbb{F}_q^{2d}$. For each $t \in \mathbb{F}_q$, let $\nu(t)$ be the number of pairs $(x, y) \in D \times D$ such that $\|x - y\| = t$. Then we have

$$
\sum_{t \in \mathbb{F}_q} \nu(t)^2 \leq \frac{|D|^4}{q} + q^{6d} \sum_{\|M\|_* = 0} |\overline{D \times D}(M)|^2.
$$

**Proof.** Since $\nu(t) = \sum_{x,y \in D: \|x - y\|=t} 1$, we have

$$
\sum_{t \in \mathbb{F}_q} \nu(t)^2 = \sum_{t \in \mathbb{F}_q} \left(\sum_{x,y \in D: \|x - y\|=t} 1\right)^2 = \sum_{x,y,z,w \in D: \|x - y\|=\|z - w\|} 1.
$$
We will relate the value \( \sum_t \nu(t)^2 \) to the Fourier transform on the variety \( V_0 \) in \( \mathbb{F}_q^{4d} \). To do this, we let \( X = (x, z), Y = (y, w) \in \mathcal{D} \times \mathcal{D} \). Using this notation with \( \| \cdot \|_s \), we can write

\[
\sum_{t \in \mathbb{F}_q} \nu(t)^2 = \sum_{X, Y \in \mathcal{D} \times \mathcal{D}} \frac{1}{\|X-Y\|_s} V_0(X-Y),
\]

where we recall from Definition 3.1 that the variety \( V_0 \) is given by

\[
V_0 = \{ X \in \mathbb{F}_q^{4d} : \|X\|_s = 0 \}.
\]

Applying the Fourier inversion theorem to the characteristic function \( V_0(X-Y) \), we get

\[
\sum_{t \in \mathbb{F}_q} \nu(t)^2 = \sum_{X, Y \in \mathcal{D} \times \mathcal{D}} V_0(X-Y) = q^{8d} \sum_{M \in \mathbb{F}_q^{4d}} \hat{V}_0(M)|\hat{D} \times \hat{D}(M)|^2.
\]

Replacing \( \hat{V}_0(M) \) by the explicit value given in Lemma 3.2, we get

\[
\sum_{t \in \mathbb{F}_q} \nu(t)^2 = q^{8d-1} \sum_{\|M\|_s=0} \delta_0(M)|\hat{D} \times \hat{D}(M)|^2 + q^{6d} \sum_{\|M\|_s=0} |\hat{D} \times \hat{D}(M)|^2 - q^{6d-1} \sum_{M \in \mathbb{F}_q^{4d}} |\hat{D} \times \hat{D}(M)|^2.
\]

Since the last term on the right-hand side is negative and the first term is \( |\mathcal{D}|^4/q \), we arrive at (3.1), as desired. □

We are ready to prove Theorem 1.2.

**Proof of Theorem 1.2.** Define \( \mathcal{D} = E \times F \subset \mathbb{F}_q^d \times \mathbb{F}_q^d \). For \( t \in \mathbb{F}_q \), let \( \nu(t) \) be the number of pairs \( (x, y) \in \mathcal{D} \times \mathcal{D} \) such that \( \|x-y\| = t \). By the Cauchy–Schwarz inequality, we have

\[
|\Delta(E) + \Delta(F)| = |\Delta(E \times F)| \geq \left| \frac{|E|^4|F|^4}{\sum_{t \in \mathbb{F}_q} \nu(t)^2} \right|.
\]

Since \( |\mathcal{D}| = |E| \cdot |F| \), Lemma 3.3 implies that

\[
\sum_{t \in \mathbb{F}_q} \nu(t)^2 \leq \frac{|E|^4|F|^4}{q} + q^{6d} \sum_{M \in \mathbb{F}_q^{4d}} |E \times F \times E(M')|^2 \cdot \max_{r \in \mathbb{F}_q} \sum_{m \in S_r^{d-1}} |\hat{F}(m)|^2.
\]

Using Proposition 2.4 and the Plancherel theorem, we get

\[
\sum_{t \in \mathbb{F}_q} \nu(t)^2 \leq \frac{|E|^4|F|^4}{q} + q^{6d} (q^{-3d}|E|^2|F|) (q^{-d-1}|F| + 2q^{-(3d-1)/2}|F|^2).
\]

Simplifying the right-hand side gives us

\[
\sum_{t \in \mathbb{F}_q} \nu(t)^2 \leq \frac{|E|^4|F|^4}{q} + q^{2d-1}|E|^2|F|^2 + 2q^{(3d-1)/2}|E|^2|F|^3.
\]

This estimate can be combined with (3.2) to deduce that

\[
|\Delta(E) + \Delta(F)| > \frac{q}{2}
\]

under the conditions that \( |E| \cdot |F| \geq 2q^d \) and \( |E|^2|F| \geq Cq^{(3d+1)/2} \) for a sufficiently large constant \( C \). Now we show that the condition \( |E| \cdot |F| \geq 2q^d \) is not necessary. Recall that we can assume that \( |E| < 4q^{(d+1)/2} \), for otherwise \( |\Delta(E)| = q \), which is a consequence due to Iosevich and Rudnev [6]. We claim that if \( |E|^2|F| \geq Cq^{(3d+1)/2} \), then \( |E| \cdot |F| \geq 2q^d \). If not, then \( |E| \cdot |F| < 2q^d \) and \( |E|^2|F| < Cq^{(3d+1)/2} \). These two conditions clearly imply that \( |E| > Cq^{(d+1)/2}/2 \), which contradicts our assumption that \( |E| < 4q^{(d+1)/2} \).
A symmetric argument switching the roles of $E$ and $F$ also shows that if $|E| \cdot |F|^2 \geq C q^{(3d+1)/2}$, then $|\Delta(E) + \Delta(F)| > q/2$. This completes the proof. □

In the following construction, we show that Theorem 1.2 cannot hold when $d \geq 2$ is even and $q \equiv 1 \mod 4$.

**Construction 3.4.** Let $d \geq 2$ be even.

(1) Suppose that $q = p^l$ with $p \equiv 1 \mod 4$ and $l = 3k$. There exist sets $E, F \subset \mathbb{F}_q^d$ such that $|E| \cdot |F|^2 \sim q^{d+2/3}$ and $|\Delta(E) + \Delta(F)| \leq q/2$.

(2) Suppose that $q = p^l$ with $p \equiv 3 \mod 4$ and $l = 6k$. There exist sets $E, F \subset \mathbb{F}_q^d$ such that $|E| \cdot |F|^2 \sim q^{d+2/3}$ and $|\Delta(E) + \Delta(F)| \leq q/2$.

**Proof.** We first recall the following result from [10, Theorem 2] due to Murphy and Petridis:

- If $q = p^l$ with $p \equiv 1 \mod 4$ and $l = 3k$, then there exists a set $A \subset \mathbb{F}_q^2$ such that $|A| \sim q^{4/3}$ and $|\Delta(A)| \leq q/2$.
- If $q = p^l$ with $p \equiv 3 \mod 4$ and $l = 6k$, then there exists a set $A \subset \mathbb{F}_q^3$ such that $|A| \sim q^{4/3}$ and $|\Delta(A)| \leq q/2$.

We note that $q = p^l \equiv 3 \mod 4$ if and only if $p \equiv 3 \mod 4$ and $l$ is odd.

Since $d \geq 2$ is even and $q \equiv 1 \mod 4$, it is known in [1, Lemma 5.1] that one can find $d/2$ linearly independent vectors in $\mathbb{F}_q^d$, say $\{v_1, \ldots, v_{d/2}\}$, such that $v_i \cdot v_j = 0$ for all $1 \leq i, j \leq d/2$, and $(d-2)/2$ linearly independent vectors in $\mathbb{F}_q^{d/2}$, say $\{v'_1, \ldots, v'_{(d-2)/2}\}$, such that $v'_i \cdot v'_j = 0$ for all $1 \leq i, j \leq (d-2)/2$. Define $E = \text{Span}(v_1, \ldots, v_{d/2})$ and $F = \text{Span}(v'_1, \ldots, v'_{(d-2)/2}) \times A$. It is clear that $|E| = q^{d/2}$ and $|F| \sim q^{(d-2)/2+4/3}$. So, $|E| \cdot |F|^2 \sim q^{3d/2+2/3}$. It follows from the definitions of $E$ and $F$ that $\Delta(E) = \{0\}$ and $\Delta(F) = \Delta(A)$. Thus, $|\Delta(E) + \Delta(F)| = |\Delta(A)| \leq q/2$. □

**Remark 3.5.** We remark here that in other even dimensions, using Lemma 2.3, we have the following bound in place of Proposition 2.4:

$$\max_{j \in \mathbb{F}_q} \mathcal{M}_j(F) \ll \min \left\{ \frac{|F|}{q^{d}}, \frac{|F|^2}{q^{3d/2}} \right\}.$$ 

Plugging this bound into the proof of Theorem 1.2 and assuming that $|E| \geq |F|$, we have

$$\sum_{t \in \mathbb{F}_q} \nu(t)^2 \leq \frac{|E|^4 |F|^4}{q} + C \min \left\{ q^{2d} |E|^2 |F|^2, q^{3d/2} |E|^2 |F|^3 \right\} \leq 2 \frac{|E|^4 |F|^4}{q}$$

if either $|E| \cdot |F| \gg q^{d+1/2}$ or $|E|^2 |F| > q^{3d+2/3}$. This result is of course weaker than Theorem 1.2 since $|E| \gg q^{d/2}$.

4. PROOF OF THEOREM 1.3

In this section, we give a proof of Theorem 1.3. To do this, we first recall the following proposition from [12], which essentially says that the $L^2$-norm of the distance measure on the Cartesian product set $E \times F$ can be reduced to the $L^2$-norm of the distance measure on each component.

**Proposition 4.1.** Let $E, F \subset \mathbb{F}_q^d$. In addition, for any $r \in \mathbb{F}_q$, let $\nu(r)$ be the number of pairs $((e_1, f_1), (e_2, f_2)) \in (E \times F)^2$ such that $\|e_1-e_2\| + \|f_1-f_2\|=r$, and let $\mu(r)$ be the number of pairs $(x, y) \in E \times E$ such that $\|x-y\|=r$. Then we have

$$\sum_{r \in \mathbb{F}_q} \nu(r)^2 \leq \frac{|E|^4 |F|^4}{q} + q^d |F|^2 \sum_{r \in \mathbb{F}_q} \mu(r)^2.$$
Proof of Theorem 1.3. If $|E| \geq q^{5/4}$, then it has been proved in [11, Theorem 1] that $|\Delta(E)| \gg q$. Therefore, without loss of generality, we can assume that $|E| \leq q^{5/4}$.

Let $T(E)$ be the number of triples $(x,y,z) \in E \times E \times E$ such that $\|x-y\| = \|x-z\|$ with $\|y-z\| \neq 0$. Since $q \equiv 3 \mod 4$, there are no two distinct points $y,z \in E$ such that $\|y-z\| = 0$. It has been proved in [11, Theorem 4] that there exists a large enough constant $C_2$ such that

$$T(E) \leq C_2 \left( \frac{|E|^3}{q} + q^{2/3}|E|^{5/3} + q^{1/4}|E|^2 \right) \ll q^{2/3}|E|^{5/3} \quad (4.1)$$

for $|E| \leq q^{5/4}$. By the Cauchy–Schwarz inequality, we have

$$\sum_{r \in \mathbb{F}_q} \mu(r)^2 \leq |E|(T(E) + |E|^2) \leq C_2 \left( \frac{|E|^4}{q} + q^{2/3}|E|^{8/3} + q^{1/4}|E|^3 \right) + |E|^3 \ll q^{2/3}|E|^{8/3}$$

for $|E| \leq q^{5/4}$. By Proposition 4.1, it follows that

$$\sum_{r \in \mathbb{F}_q} \nu(r)^2 \leq \frac{|E|^4|F|^4}{q} + q^2|F|^2 \sum_{r \in \mathbb{F}_q} \mu(r)^2.$$

Therefore,

$$\sum_{r \in \mathbb{F}_q} \nu(r)^2 \ll \frac{|E|^4|F|^4}{q} + q^{8/3}|F|^2|E|^{8/3} \ll \frac{|E|^4|F|^4}{q}$$

whenever $|E|^4|F|^6 \gg q^{11}$.

As in the proof of Theorem 1.2, we have

$$|\Delta(E) + \Delta(F)| \geq \frac{|E|^4|F|^4}{\sum_r \nu(r)^2} \gg q$$

under the condition $|E|^4|F|^6 \gg q^{11}$.

We also change the roles of $E$ and $F$ in the above proof. Hence, we also see that if $|E|^6|F|^4 \gg q^{11}$, then $|\Delta(E) + \Delta(F)| \gg q/2$. This completes the proof. \quad \square

ACKNOWLEDGMENTS

We are grateful to the reviewers for useful comments and suggestions. We would also like to thank the Vietnam Institute for Advanced Study in Mathematics for hospitality during our visit.

FUNDING

Daewoong Cheong and Doowon Koh were supported by Basic Science Research Programs through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2018R1D1A3B07045594 and NRF-2018R1D1A1B07044469, respectively). Thang Pham was supported by the Swiss National Science Foundation grants P400P2-183916 and P4P4P2-191067.

REFERENCES

1. D. Hart, A. Iosevich, D. Koh, and M. Rudnev, “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).
2. N. Hegyvári and M. Pálfy, “Note on a result of Shparlinski and related results,” Acta Arith. 193 (2), 157–163 (2020).
3. D. D. Hieu and L. A. Vinh, “On distance sets and product sets in vector spaces over finite rings,” Mich. Math. J. 62 (4), 779–792 (2013).
4. A. Iosevich and D. Koh, “Extension theorems for spheres in the finite field setting,” Forum Math. 22 (3), 457–483 (2010).
5. A. Iosevich, D. Koh, S. Lee, T. Pham, and C.-Y. Shen, “On restriction estimates for the zero radius sphere over finite fields,” Can. J. Math. 73 (3), 769–786 (2021).
6. A. Iosevich and M. Rudnev, “Erdős distance problem in vector spaces over finite fields,” Trans. Am. Math. Soc. 359 (12), 6127–6142 (2007).
7. D. Koh, T. Pham, C.-Y. Shen, and L. A. Vinh, “A sharp exponent on sum of distance sets over finite fields,” Math. Z. 297 (3–4), 1749–1765 (2021).
8. D. Koh, T. Pham, and L. A. Vinh, “Extension theorems and a connection to the Erdős–Falconer distance problem over finite fields,” J. Funct. Anal. 281 (8), 109137 (2021); arXiv:1809.08699 [math.CA].
9. R. Lidl and H. Niederreiter, Finite Fields (Cambridge Univ. Press, Cambridge, 1997), Encycl. Math. Appl. 20.
10. B. Murphy and G. Petridis, “An example related to the Erdős–Falconer question over arbitrary finite fields,” Bull. Hell. Math. Soc. 63, 38–39 (2019).
11. B. Murphy, G. Petridis, T. Pham, M. Rudnev, and S. Stevens, “On the pinned distances problem over finite fields,” arXiv:2003.00510 [math.CO].
12. T. Pham, “Erdős distinct distances problem and extensions over finite spaces,” PhD thesis (EPFL, Lausanne, 2017).
13. T. Pham and L. A. Vinh, “Distribution of distances in positive characteristic,” Pac. J. Math. 309 (2), 437–451 (2020).
14. I. E. Shparlinski, “On the additive energy of the distance set in finite fields,” Finite Fields Appl. 42, 187–199 (2016).