Journal of Fourier Analysis and Applications (2024) 30:19
https://doi.org/10.1007/s00041-024-10079-x

Product of Sets on Varieties in Finite Fields

Che-Jui Chang[1] · Ali Mohammadi[2] · Thang Pham[3] · Chun-Yen Shen[1]

Received: 2 January 2023 / Revised: 31 August 2023 / Accepted: 21 February 2024 /
Published online: 27 March 2024

Abstract
Let V be a variety in $\mathbb{F}_q^d$ and $E \subset V$. It is known that if any line passing through the origin contains a bounded number of points from E, then $\left|\prod(E)\right| = |\{x \cdot y : x, y \in E\}| \gg q$ whenever $|E| \gg q^{\frac{d}{2}}$. In this paper, we show that the barrier $\frac{d}{2}$ can be broken when V is a paraboloid in some specific dimensions. The main novelty in our approach is to link this question to the distance problem in one lower dimensional vector space, allowing us to use recent developments in this area to obtain improvements.

Keywords Product of sets · Finite fields · Extension estimates

Mathematics Subject Classification 52C10 · 11T23

1 Introduction

Let $\mathbb{F}_q$ be a finite field of order q, where q is a prime power. For $E, F \subset \mathbb{F}_q^d$, the set of dot products between E and F is defined by

Communicated by Alex Iosevich.

✉ Thang Pham
thangpham.math@vnu.edu.vn

Che-Jui Chang
jerry861021dd@gmail.com

Ali Mohammadi
ali.mohammadi.np@gmail.com

Chun-Yen Shen
cyshen@math.ntu.edu.tw

1 Department of Mathematics, National Taiwan University, Taipei, Taiwan

2 Department of Mathematics and Statistics, UNSW, Kensington, Australia

3 University of Science, Vietnam National University, Hanoi, Vietnam

$$\prod(E, F) := \{x \cdot y : x \in E, y \in F\} \subset \mathbb{F}_q.$$

When $E = F$, we write $\prod(E)$ instead of $\prod(E, F)$. In [3], Hart et al. studied the question of finding the smallest exponent α such that if $|E||F| \gg q^\alpha$, then $|\prod(E, F)| \gg q$. Here and throughout the paper, we use the notation $X \gg Y$ if there exists an absolute constant $c > 0$ such that $X \geq cY$.

By using discrete Fourier analysis, they proved the following result.

Theorem 1.1 (Hart–Iosevich–Koh–Rudnev [3]) *Let E be a set in $\mathbb{F}_q^d$. Suppose that $|E| > q^{\frac{d+1}{2}}$, then*

$$\mathbb{F}_q \setminus \{0\} \subset \prod(E).$$

Moreover, this result is sharp in the following sense:

1. *If $\mathbb{F}_q$ is a quadratic extension, for any $\epsilon > 0$, there exists $E \subset \mathbb{F}_q^d$ of size $q^{\frac{d+1}{2}-\epsilon}$ such that $\left|\prod(E)\right| = o(q)$.*
2. *If $d \equiv 3 \mod 4$ and q is large enough, then for any $t \neq 0$, there exists $E \subset \mathbb{F}_q^d$ of size about $q^{\frac{d+1}{2}}$ such that $t \notin \prod(E)$.*

This theorem says that the exponent $\frac{d+1}{2}$ cannot be improved if we want to have all non-zero dot products. It is natural to ask under what additional conditions, the exponent $\frac{d+1}{2}$ can be improved if we are only interested in a positive proportion of all elements in the field. In the same paper, Hart et al. showed that when E is a subset of the unit sphere, then the exponent $\frac{d}{2}$ is enough. This result can be extended for general sets $E \subset \mathbb{F}_q^d$ whenever E does not contain many points on any lines through the origin. We refer the reader to [3, Section 3.1] and [11, Theorem 1.3] for more details and discussions. To the best of our knowledge, no improvement of $d/2$ has been made in the literature for spheres or other varieties.

In this paper, we are interested in finding varieties V for which the threshold $\frac{d}{2}$ can be further improved. It follows from our main theorem (Theorem 1.2) that paraboloids in some specific dimensions provide the first model for this type question. The main novelty in our approach is to link this question to the distance problem in one lower dimensional vector space, allowing us to use recent developments in this area to obtain improvements. To state our main theorems, we need to recall some notations from Fourier restriction theory.

Let $(\mathbb{F}_q^d, dx)$ be the d-dimensional vector space over $\mathbb{F}_q$ endowed with the normalized counting measure dx, and $(\mathbb{F}_q^d, dc)$ be the dual space with the counting measure dc. For complex-valued functions $f : (\mathbb{F}_q^d, dx) \to \mathbb{C}$ and $g : (\mathbb{F}_q^d, dc) \to \mathbb{C}$, we define

$$\int f(x)dx := q^{-d} \sum_{x \in \mathbb{F}_q^d} f(x), \qquad \int g(c)dc := \sum_{c \in \mathbb{F}_q^d} g(c).$$

Let V be an algebraic variety in $(\mathbb{F}_q^d, dx)$, we define the normalized surface measure $d\sigma$ on V by

$$d\sigma(x) := q^d |V|^{-1} 1_V(x) dx.$$

So, for any function $f : V \to \mathbb{C}$,

$$\int f(x) d\sigma(x) := |V|^{-1} \sum_{x \in V} f(x).$$

For a function $f : (\mathbb{F}_q^d, dx) \to \mathbb{C}$, the Fourier transform $\widehat{f}$ is defined on the space $(\mathbb{F}_q^d, dc)$ by

$$\widehat{f}(c) := \int \chi(-x \cdot c) f(x) dx = q^{-d} \sum_{x \in \mathbb{F}_q^d} \chi(-x \cdot c) f(x), \ c \in (\mathbb{F}_q^d, dc).$$

Similarly, for a function $g : (\mathbb{F}_q^d, dc) \to \mathbb{C}$, its Fourier transform is defined on the space $(\mathbb{F}_q^d, dx)$ by

$$\widehat{g}(x) := \int \chi(-x \cdot c) g(c) dc = \sum_{c \in \mathbb{F}_q^d} \chi(-x \cdot c) g(c).$$

With the normalized surface measure $d\sigma$ on V and a function $f : (\mathbb{F}_q^d, dx) \to \mathbb{C}$, we define the inverse Fourier transform $(f d\sigma)^\vee$ of the measure $f d\sigma$ by

$$(f d\sigma)^\vee(c) := \int \chi(c \cdot x) f d\sigma(x) = |V|^{-1} \sum_{x \in V} \chi(c \cdot x) f(x),$$

for $c \in (\mathbb{F}_q^d, dc)$.

The $L^2 \to L^r$ extension problem for the variety V is to determine all ranges of r such that the following inequality

$$||f d\sigma^\vee||_{L^r(\mathbb{F}_q^d, dc)} \leq C ||f||_{L^2(V, d\sigma)} \tag{1}$$

holds for any function f on V. We note that in the above inequality, the constant C is independent of q (the size of $\mathbb{F}_q$). We use the notation $R_V^*(2 \to r) \ll 1$ to indicate that the estimate (1) holds.

There is a series of papers studying $L^2 \to L^r$ estimates for various varieties in the literature, for instance, see [5, 8, 9, 12] and the references therein. In this paper, we require estimates associated to spheres of non-zero radius.

For a positive integer $d \geq 3$ and a non-zero element $r \in \mathbb{F}_q$, the paraboloid P_d and the sphere S_r centered at origin of radius r in $\mathbb{F}_q^d$ are defined by the following

formulas:

$$P_d := \left\{x = (x_1, \dots, x_d) \colon x_d = x_1^2 + \cdots + x_{d-1}^2\right\},$$

and

$$S_r := \left\{x = (x_1, \dots, x_d) \colon x_1^2 + \cdots + x_d^2 = r\right\}.$$

Our main result is as follows.

Theorem 1.2 *Let E be a set in P_d with $d \equiv 3 \mod 4$ and $q \equiv 3 \mod 4$. Assume that the extension conjecture*

$$||f d\sigma^{\vee}||_{L^{\frac{2d+2}{d-1}}(\mathbb{F}_q^{d-1}, dc)} \ll ||f||_{L^2(S_r, d\sigma)},$$

holds for any $S_r \subset \mathbb{F}_q^{d-1}$ and $r \neq 0$, then we have

$$\left|\prod(E)\right| \gg q,$$

whenever $|E| \gg q^{\frac{(d-1)^2+2(d-1)}{2(d-1)+2}} = q^{\frac{d}{2}-\frac{1}{2d}}$.

It is worth noting that the same conclusion does not hold when d is even. When $d \equiv 3 \mod 4$ and $q \equiv 3 \mod 4$, we conjecture that the sharp exponent should be $(d-1)/2$. To support these claims, we provide constructions in the last section. Note that the extension conjecture was proved in [1] to be true in $\mathbb{F}_q^2$. As a result, we have the following corollary.

Corollary 1.3 *Let E be a set in $P_3 \subset \mathbb{F}_q^3$ with $q \equiv 3 \mod 4$. Suppose $|E| \gg q^{\frac{3}{2}-\frac{1}{6}}$, then we have*

$$\left|\prod(E)\right| \gg q,$$

If we assume q is an odd prime number, then by using a recent theorem on *bisector line energy* due to Murphy et al. [10], we can get a better exponent, namely, $\frac{5}{4}$ instead of $\frac{4}{3}$.

Theorem 1.4 *Let $\mathbb{F}_p$ be a prime field, and E be a set in P_3 in $\mathbb{F}_p^3$ with $p \equiv 3 \mod 4$. Suppose that $|E| \gg p^{\frac{3}{2}-\frac{1}{4}}$, then*

$$\left|\prod(E)\right| \gg p.$$

Moreover, if $|E| \ll p^{5/4}$ and $|E \backslash \{(x_1, x_2, 0) \colon (x_1, x_2) \in \mathbb{F}_p^2\}| \gg |E|$, then we also have

$$\left|\prod(E)\right| \gg |E|^{\frac{2}{3}}.$$

It is not clear to us how the method of this paper can be adapted for other varieties, say spheres, we hope to address this question in a sequel paper. We also note that for spheres, the dot product set $\prod(E)$ is of the same size as the distance set $\Delta(E)$, where $\Delta(E) := \{||x-y||: x, y \in E\}$. The exponent $d/2$ has been obtained in [3, Theorem 2.8].

2 Preliminary: Extension Estimates

As mentioned in the introduction, the $L^2 \to L^r$ extension problem for the variety V is to determine all ranges of r such that the following inequality

$$\left|\left|fd\sigma^{\vee}\right|\right|_{L^r(\mathbb{F}_q^d,dc)} \leq C||f||_{L^2(V,d\sigma)} \tag{2}$$

holds for any function f on V. The notation $R_V^*(2 \to r) \ll 1$ means the above estimate holds.

In this paper, we only need extension results for spheres. The following is the well-known $L^2 \to L^r$ extension conjecture in $\mathbb{F}_q^n$. We refer the reader to [7] for more discussions.

Conjecture 2.1 *For even $n \geq 2$, let S_r be the sphere centered at the origin of radius r with $r \neq 0$ in $\mathbb{F}_q^n$. We have the following $L^2 \to L^r$ extension estimate*

$$R_{S_r}^*\left(2 \to \frac{2n+4}{n}\right) \ll 1.$$

It was proved in [1] that this conjecture is true for $n = 2$, namely,

Theorem 2.2 *Let C_r be the circle centered at the origin of radius r with $r \neq 0$ in $\mathbb{F}_q^2$. We have the following $L^2 \to L^r$ extension estimate*

$$R_{C_r}^*\left(2 \to 4\right) \ll 1.$$

In higher dimensions, the best current result is

$$R_{S_r}^*\left(2 \to \frac{2n+2}{n-1}\right) \ll 1, \tag{3}$$

which is known to be sharp in odd dimensions. A proof of this estimate can be found in [4].

Although Conjecture 2.1 is still wide open in dimensions $n \geq 4$, for the sphere of radius 0, denoted by S_0, it has been shown in [6] that the conjecture holds true for particular n and q below.

Theorem 2.3 *Let S_0 be the sphere centered at the origin of radius 0. Assume $n \equiv 2 \mod 4$ and $q \equiv 3 \mod 4$, then the following $L^2 \to L^r$ extension estimate holds:*

$$R^*_{S_0}\left(2 \to \frac{2n+4}{n}\right) \ll 1.$$

With these results in hand, we are ready to prove Theorem 1.2 in the next section.

3 Proof of Theorem 1.2

The proof of Theorem 1.2 contains two main steps: reducing to the triangle problem and bounding the number of isosceles triangles.

3.1 Reducing to the Isosceles Triangles Problem

By the Cauchy–Schwarz inequality, we observe that

$$\left|\prod(E)\right| \gg \frac{|E|^3}{|D(E)|}, \tag{4}$$

where $D(E)$ is the number of triples $(x, y, z) \in E^3$ such that $x \cdot y = x \cdot z$. To see this, first, by Cauchy–Schwarz inequality, we have

$$\left|\prod(E)\right| \geq \frac{|E|^4}{|M(E)|}, \tag{5}$$

where $M(E) = \{(x, y, w, z) \in E^4 : x \cdot y = w \cdot z\}$. Thus it suffices to show $|M(E)| \leq |E||D(E)|$. Now for a given t and $x \in E$, write $\pi_x^t(E) = \{y \in E, x \cdot y = t\}$. Then, we observe that

$$|M(E)| = \sum_t \left(\sum_x |\pi_x^t(E)|\right)^2.$$

By Cauchy–Schwarz inequality, we have

$$\sum_t \left(\sum_x |\pi_x^t(E)|\right)^2 \leq \sum_t |E| \sum_x |\{(y, z) \in E^2, x \cdot y = x \cdot z = t\}| = |E||D(E)|.$$

For any point $x = (x_1, \ldots, x_d) \in E \subset P_d$, we define $\overline{x} := (x_1, \ldots, x_{d-1})$, and let $\overline{E} := \{\overline{x} : x \in E\} \subset \mathbb{F}_q^{d-1}$.

Under our assumptions on the set E, without loss of generality, we may assume that $||\overline{x}|| \neq 0$ for all $x \in E$.

For $x, y, z \in P_d$, the identity $x \cdot y = x \cdot z$ can be rewritten as

$$(\overline{x}, ||\overline{x}||) \cdot (\overline{y} - \overline{z}, ||\overline{y}|| - ||\overline{z}||) = 0.$$

This implies that

$$\left(\frac{\overline{x}}{||\overline{x}||}, 1\right) \cdot (\overline{y} - \overline{z}, ||\overline{y}|| - ||\overline{z}||) = 0,$$

which gives

$$\left(\frac{\overline{x}}{||\overline{x}||}, 1\right) \cdot (\overline{y}, ||\overline{y}||) = \left(\frac{\overline{x}}{||\overline{x}||}, 1\right) \cdot (\overline{z}, ||\overline{z}||)\,.$$

So

$$\left\| \frac{-\overline{x}}{2||\overline{x}||} - \overline{y} \right\| = \left\| \frac{-\overline{x}}{2||\overline{x}||} - \overline{z} \right\|. \tag{6}$$

Set $F' := \left\{ \frac{-\overline{x}}{2||\overline{x}||} : \overline{x} \in \overline{E} \right\} \subset \mathbb{F}_q^{d-1}$.

The Eq. (6) counts the number of isosceles triangles with one vertex from F' and the two other vertices (base) from $\overline{E}$.

In other words, to bound the size of $D(E)$ from above, it is enough to count the number of isosceles triangles with vertices in F' and $\overline{E}$ satisfying the relation (6).

3.2 Bounding the Number of Isosceles Triangles

Given $X \subset \mathbb{F}_q^d$ and $y \in \mathbb{F}_q^d$, we first count the number of isosceles triangles with a given apex.

Lemma 3.1 *Let $X \subset \mathbb{F}_q^n$ and $y \in X$. Then we have*

$$\sum_{x,z \in X : ||x-y|| = ||z-y|| \neq 0} 1 \ll \frac{|X|^2}{q} + q^n \sum_{r \in \mathbb{F}_q^*} \left| \sum_{m \in S_r} \widehat{X}(m) \chi(y \cdot m) \right|^2 + q^n \left| \sum_{||m||=0, m \neq 0} \widehat{X}(m) \chi(y \cdot m) \right|^2.$$

Proof Let $O(n)$ be the orthogonal group of $n \times n$ matrices in $\mathbb{F}_q$. It is well-known that $|O(n)| = (1 + o(1))q^{\frac{n^2}{2}}$, and the stabilizer of any non-zero vector in $\mathbb{F}_q^n$ is of the size $|O(n-1)|$. It is not hard to prove that $|O(n)| = |S_1||O(n-1)| = (1 + o(1))q^{n-1}|O(n-1)|$. We note that $O(d)$ acts transitively on the set of non-zero vectors of any given norm.

We first note that if there is an $x \in X$ with $y - x \in S_r$, the sphere with radius r in $\mathbb{F}_q^n$, then writing $y - x = x'$, we have a one-to-one correspondence between $x' \in S_r$ and $y - x' \in X$. Hence, we can write

$$\begin{aligned}\sum_{x,z\in X:||x-y||=||z-y||\neq 0} 1 &= \sum_{r\in\mathbb{F}_q^*}\sum_{x\in S_r} X(y-x)\sum_{z\in S_r} X(y-z)\\ &\leq \frac{1}{|O(n-1)|}\cdot\sum_{\theta\in O(n)}\sum_{r\in\mathbb{F}_q^*}\sum_{x\in S_r} X(y-x)X(y-\theta x).\end{aligned}$$

Applying the Fourier inversion theorem to functions $X(y-x)$, $X(y-\theta x)$, that is

$$X(y-x) = \sum_{m\in\mathbb{F}_q^n} \widehat{X}(m)\chi(m(y-x))$$

and

$$X(y-\theta x) = \sum_{m'\in\mathbb{F}_q^n} \widehat{X}(m')\chi(m'(y-\theta x)).$$

We have

$$\begin{aligned}\sum_{x,z\in X:||x-y||=||z-y||\neq 0} 1 \leq \frac{1}{|O(n-1)|}\cdot\sum_{\theta\in O(n)}\sum_{m,m'\in\mathbb{F}_q^n} &\widehat{X}(m)\widehat{X}(m')\chi(y\cdot(m+m'))\\ &\sum_{x\in\mathbb{F}_q^n}\chi(-m\cdot x - m'\cdot\theta x).\end{aligned}$$

By the orthogonality of χ, we compute the above sum in $x \in \mathbb{F}_q^d$, then the size of the right-hand side inequality becomes

$$\frac{q^n}{|O(n-1)|}\cdot\sum_{\theta\in O(n)}\sum_{m\in\mathbb{F}_q^n}\widehat{X}(m)\widehat{X}(-\theta m)\chi(y\cdot(m-\theta m)),$$

which can be decomposed as the sum of

$$\frac{q^n}{|O(n-1)|}\sum_{\theta\in O(n)}\sum_{m\in S_0}\widehat{X}(m)\widehat{X}(-\theta m)\chi(y\cdot(m-\theta m))$$

and

$$\frac{q^n}{|O(n-1)|}\sum_{\theta\in O(n)}\sum_{r\in\mathbb{F}_q^*}\sum_{m\in S_r}\widehat{X}(m)\widehat{X}(-\theta m)\chi(y\cdot(m-\theta m)),$$

which is equal to

$$= \frac{q^n}{|O(n-1)|} \sum_{\theta \in O(n)} \sum_{m \in S_0} \widehat{X}(m)\widehat{X}(-\theta m)\chi(y \cdot (m - \theta m)) + q^n \sum_{r \in \mathbb{F}_q^*} \left| \sum_{m \in S_r} \widehat{X}(m)\chi(y \cdot m) \right|^2$$

$$\ll \frac{|X|^2}{q} + q^n \sum_{r \in \mathbb{F}_q^*} \left| \sum_{m \in S_r} \widehat{X}(m)\chi(y \cdot m) \right|^2 + q^n \left| \sum_{||m||=0, m \neq 0} \widehat{X}(m)\chi(y \cdot m) \right|^2.$$

□

Lemma 3.1 shows that the number of isosceles triangles can be reduced to extension-type estimates associated to spheres. Thus, we now can apply results in Sect. 2 to derive the next theorem.

Theorem 3.2 *For $n \equiv 2 \mod 4$ and $X \subset \mathbb{F}_q^n$ with $q \equiv 3 \mod 4$. Assume that Conjecture 2.1 holds, then the number of isosceles triangles is bounded by*

$$\ll \frac{|X|^3}{q} + q^{d-1}|X|^{\frac{n+4}{n+2}} + q^{\frac{n-2}{2}}|X|^2.$$

Proof Let $T^{\mathtt{nde}}(X)$ be the number of isosceles triangles in E of the form $(x, y, z) \in X^3$ such that $||x - y|| = ||x - z|| \neq 0$. Let $T^{\mathtt{de}}(X)$ be the number of triangles with at least one side of zero length.

To bound $T^{\mathtt{de}}(X)$, we will show that the number of pairs $(x, y) \in X \times X$ such that $||x - y|| = 0$ is at most

$$\frac{|X|^2}{q} + q^{\frac{n-2}{2}}|X|.$$

Once we have the bound above, then

$$\sum_{x,y,z \in X : ||x-y||=||z-y||=0} 1 \leq \sum_{z \in X} \sum_{x,y \in X : ||x-y||=0} 1 \leq \frac{|X|^3}{q} + q^{\frac{n-2}{2}}|X|^2.$$

Now write

$$\sum_{x,y \in X : ||x-y||=0} 1 = \sum_{x,y \in \mathbb{F}_q^n} X(x)X(y)S_0(x - y),$$

which, by the Fourier inversion formula, becomes

$$\sum_{x,y \in \mathbb{F}_q^n} X(x)X(y) \sum_{m \in \mathbb{F}_q^n} \widehat{S_0}(m)\chi((x - y)m),$$

which is $\sum_{m\in\mathbb{F}_q^n} |\widehat{X}(m)|^2 \widehat{S}_0(m)$. In order to proceed further, we recall the following lemma on the Fourier transform of the sphere of zero radius from [6].

Lemma 3.3 [6] *Let S_0 be the sphere with zero radius in $\mathbb{F}_q^n$. Assume that $n = 4k+2$ for $k \in \mathbb{N}$ and $q \equiv 3 \mod 4$. Then we have*

$$\widehat{S_0}(m) := q^{-n} \sum_{y\in S_0} \chi(m\cdot y) = q^{-1}\delta_0(m) - q^{\frac{-(n+2)}{2}} \sum_{r\neq 0} \chi(r\|m\|),$$

where $\delta_0(m) = 1$ for $m = (0,\dots,0)$, and 0 otherwise.

We now continue the proof of Theorem 3.2 by inserting the formula for $\widehat{S_0}(m)$. Thus we get

$$\sum_{m\in\mathbb{F}_q^n} |\widehat{X}(m)|^2 q^{-1}\delta_0(m) - q^{\frac{-(n+2)}{2}} \sum_{m\in\mathbb{F}_q^n} |\widehat{X}(m)|^2 \sum_{r\neq 0} \chi(r\|m\|).$$

Applying the orthogonality relation of χ to the sum over $r \neq 0$, we obtain

$$\begin{aligned} &|\widehat{X}(0,\dots,0)|^2 q^{-1} - q^{\frac{-(n+2)}{2}}(q-1) \sum_{\|m\|=0} |\widehat{X}(m)|^2 + q^{\frac{-(n+2)}{2}} \sum_{\|m\|\neq 0} |\widehat{X}(m)|^2 \\ &= q^{-1}|X|^2 - q^{\frac{-(n+2)}{2}} q \sum_{\|m\|=0} |\widehat{X}(m)|^2 + q^{\frac{-(n+2)}{2}} \sum_{m\in\mathbb{F}_q^n} |\widehat{X}(m)|^2. \end{aligned}$$

Since $\sum_{m\in\mathbb{F}_q^n} |\widehat{X}(m)|^2 = q^n|X|$ and the middle term above is negative, we get that

$$\sum_{m\in\mathbb{F}_q^n} |\widehat{X}(m)|^2 \widehat{S}_0(m) \leq \frac{|X|^2}{q} + q^{\frac{n-2}{2}}|X|.$$

Hence,

$$T^{\mathrm{de}}(X) \ll \frac{|X|^3}{q} + q^{\frac{n-2}{2}}|X|^2.$$

To bound T^{nde}, we observe that

$$T^{\mathrm{nde}}(X) = \sum_{y\in X} \sum_{\substack{x,z\in X:\\ ||x-y||=||z-y||}} 1.$$

Thus, applying Lemma 3.1, it suffices to bound the following sums:

$$\sum_{y\in X} \left| \sum_{m\in S_r} \widehat{X}(m)\chi(y\cdot m) \right|^2 \quad \text{with } r \neq 0,$$

and

$$\sum_{y\in X}\left|\sum_{m\in S_0}\widehat{X}(m)\chi(y\cdot m)\right|^2.$$

Set $f=\widehat{X}$ and use Fourier inversion formula, the first sum becomes

$$\begin{aligned}\sum_{y\in X}\left|\sum_{m\in S_r}\widehat{X}(m)\chi(y\cdot m)\right|^2 &= |S_r|^2\sum_{y\in X}|fd\sigma^\vee(y)|^2\\ &\le |S_r|^2\cdot|X|^{\frac{2}{n+2}}\cdot||fd\sigma^\vee||^2_{L^{\frac{2n+4}{n}}(\mathbb{F}_q^n,dc)}.\end{aligned}$$

Assuming Conjecture 2.1 holds, i.e.

$$\left|\left|fd\sigma^\vee\right|\right|_{L^{\frac{2n+4}{n}}(\mathbb{F}_q^n,dc)}\ll||f||_{L^2(S_r,d\sigma)},$$

then we get

$$\begin{aligned}\sum_{y\in X}\left|\sum_{m\in S_r}\widehat{X}(m)\chi(y\cdot m)\right|^2 &= |S_r|^2\sum_{y\in X}|fd\sigma^\vee(y)|^2\\ &\le |S_r|^2\cdot|X|^{\frac{2}{n+2}}\cdot\left|\left|fd\sigma^\vee\right|\right|^2_{L^{\frac{2n+4}{n}}(\mathbb{F}_q^n,dc)}\\ &\le |S_r|^2\cdot|X|^{\frac{2}{n+2}}\cdot||f||^2_{L^2(S_r,d\sigma)}\\ &= |S_r|\cdot|X|^{\frac{2}{n+2}}\sum_{m\in S_r}|\widehat{X}(m)|^2.\end{aligned}$$

Similarly, using Theorem 2.3, we have the same bound for the second sum. Using the fact that $|S_r|=(1+o(1))q^{n-1}$, we have

$$\begin{aligned}T^{\mathrm{nde}}(X) &\ll \frac{|X|^3}{q}+q^{n-1}\sum_{r\in\mathbb{F}_q}|X|^{\frac{2}{n+2}}\sum_{m\in S_r}|\widehat{X}(m)|^2\\ &= \frac{|X|^3}{q}+q^{n-1}|X|^{\frac{n+4}{n+2}}.\end{aligned}$$

Putting the bounds of $T^{\mathrm{nde}}(X)$ and $T^{\mathrm{de}}(X)$ together gives us the desired estimate. □

3.3 Concluding the Proof

Setting $X=E'\cup F'\subset\mathbb{F}_q^{d-1}$. We have $|X|\le 2|E|$. It is not hard to see that $D(E)$ is bounded by the number of isosceles triangles in X. So applying Theorem 3.2 and (5) concludes the proof.

Remark 3.1 If we use the estimate (3) in place of Conjecture 2.1 in the above argument, then we obtain the condition $|E| \gg q^{\frac{d}{2}}$ in the statement of Theorem 1.2.

4 Proof of Theorem 1.4

We follow the proof of Theorem 1.2 identically, except that we have a more effective bound on the number of isosceles triangles in two dimensions due to Murphy et al. [10].

Given a set $X \subset \mathbb{F}_p^2$, we say that a triple $(x, y, z) \in X^3$ forms a *non-degenerate* isosceles triangle if $||x - y|| = ||x - z||$ and $||y - z|| \neq 0$. If $||x - y|| = ||x - z||$ and $||y - z|| = 0$, we say the triangle is *degenerate*.

Theorem 4.1 (Non-degenerate isosceles triangles) *Let X be a set in $\mathbb{F}_p^2$ with $|X| \leq p^{4/3}$. Let $T^*(X)$ be the number of non-degenerate isosceles triangles in X. We have*

$$T^*(X) - \frac{|X|^3}{p} \ll \min\left\{p^{2/3}|X|^{5/3} + p^{1/4}|X|^2,\ |X|^{7/3}\right\}$$

Hence,

1. if $|X| \gg p^{5/4}$,

$$T^*(X) \ll \frac{|X|^3}{p}.$$

2. if $|X| \ll p^{5/4}$, then

$$T^*(X) \ll |X|^{7/3}.$$

Since we assumed that $p \equiv 3 \mod 4$, the number of degenerate isosceles triangles is at most $\ll |E|^2$. Hence,

1. if $|E| \gg p^{5/4}$,

$$|D(E)| \ll \frac{|E|^3}{p} + |E|^2$$

2. if $|E| \ll p^{5/4}$, then

$$|D(E)| \ll |E|^{7/3}.$$

These give us the desired bounds of Theorem 1.4. The first construction tells us that it is impossible to break $\frac{d}{2}$ in even dimensions.

5 Constructions and Remarks

We have the following constructions on the sharpness of Theorem 1.2.

Construction 5.1 *Assume d is even, for any $\epsilon > 0$, there exists a set $E \subset P_d$ such that $|E| \sim q^{\frac{d}{2}-\epsilon}$ such that $|\prod(E)| = o(q)$.*

Proof We first consider the case $d \equiv 2 \mod 4$. We know from Lemma 5.1 in [3] that there exist $\frac{d-2}{2}$ nonzero vectors $v_1, \ldots, v_{\frac{d-2}{2}}$ in $\mathbb{F}_q^{d-2}$ which are mutually orthogonal, i.e. $v_i \cdot v_j = 0$ for all $1 \le i \le j \le \frac{d-2}{2}$. Let S be the subspace spanned by these $(d-2)/2$ vectors. Set $E = S \times \{(x, x^2) : x \in A\}$, where A is a multiplicative subgroup of $\mathbb{F}_q^*$ of size $q^{1-\epsilon}$. Then one can directly check that

$$\prod(E) \subset a + a^2,$$

for $a \in A$. This shows that $|\prod(E)| \sim q^{1-\epsilon}$ and $|E| \sim q^{\frac{d}{2}-\epsilon}$.

When $d \equiv 0 \mod 4$, we use Lemma 5.1 from [3] again to obtain $\frac{d}{2}$ vectors that are mutually orthogonal in $\mathbb{F}_q^d$. We denote these vectors by $u_1, \ldots, u_{\frac{d}{2}}$. Let A be a multiplicative subgroup of $\mathbb{F}_q^*$ of size $q^{1-\epsilon}$. We note that $v_{\frac{d}{2}}$ is of the form $(0, \ldots, 0, 1, i)$, where $i^2 = -1$. Define

$$S := \mathbb{F}_q v_1 + \cdots + \mathbb{F}_q v_{\frac{d}{2}-1} + A v_{\frac{d}{2}}.$$

Set

$$E = \left\{\left(x_1, \ldots, x_{d-1}, -x_d^2\right) : (x_1, \ldots, x_d) \in S\right\}.$$

Since $|S| \sim q^{\frac{d}{2}-\epsilon}$, we have $|E| \sim q^{\frac{d}{2}-\epsilon}$.

For $(x_1, \ldots, x_{d-1}, -x_d^2)$ and $(y_1, \ldots, y_{d-1}, -y_d^2)$ in E, we have their product is

$$x_1 y_1 + \cdots + x_{d-1} y_{d-1} - x_d^2 y_d^2 = -x_d y_d - x_d^2 y_d^2.$$

So the product value becomes $x + x^2$ for $x \in A$. This implies $|\prod(E)| \sim q^{1-\epsilon}$. □

The next construction provides the information that the best exponent of Theorem 1.2 one can expect is $\frac{d-1}{2}$.

Construction 5.2 *Assume $d \equiv 3 \mod 4$ and $q \equiv 3 \mod 4$, for any $\epsilon > 0$, there exists a set $E \subset P_d$ such that $|E| \sim q^{\frac{d-1}{2}-\epsilon}$ such that $|\prod(E)| = o(q)$.*

Proof Following the first case of Construction 5.1, we may find a subspace $S' \subset \mathbb{F}_q^{d-3}$ of size $q^{\frac{d-3}{2}}$, with the property that any pair of its vectors are mutually orthogonal. Let $S \subset \mathbb{F}_q^{d-2}$ be the set one gets by adjoining 0 as the last entry of elements of S'. Then, by choosing E in the same way as the first case of Construction 5.1, we get $|\prod(E)| \sim q^{1-\epsilon}$ while $|E| \sim q^{\frac{d-1}{2}-\epsilon}$ □

Remark 5.1 It is well-known that the L^2-norm of the distance problem, i.e. the number of quadruples $(x, y, z, w) \in E^4$ such that $||x - y|| = ||z - w||$, can be bounded by using extension estimates, see [7, Theorem 1.7] for example. By using the Cauchy–Schwarz inequality, the number of such quadruples is at most $|E|$ times the number of isosceles triangles in E. In other words, Theorem 3.2, provided in Sect. 3, offers a stronger form of this problem.

Remark 5.2 In the statement of Corollary 1.3, if $q \equiv 1 \mod 4$ then we find that the exponent $\frac{4}{3}$ is not good enough to guarantee that the number of isosceles triangles (including both degenerate and non-degenerate) is at most $\ll |E|^3/q$. Let $i^2 = -1$ and E be a set of points on $|E|/M$ parallel lines of slope i, where each line contains exactly M points. So, the number of degenerate isosceles triangles is at least $M^3 \cdot \frac{|E|}{M} = M^2|E|$, which is bigger than $|E|^3/q$ if $|E| \leq q^{1/2}M$. For example, if $|E| \sim q^{4/3}$, one can take $M = q^{\frac{5}{6}+\epsilon}$ for any $\epsilon > 0$. The same happens for the case of Theorem 1.4. In other words, if one wishes to remove the condition $q \equiv 1 \mod 4$, then the best hope with this approach is to show that the inequality (5) still holds when replace $D(E)$ by $D^*(E)$, where $D^*(E)$ is the set of triples $(x, y, z) \in D(E)$ with $||\overline{y} - \overline{z}|| \neq 0$.

Remark 5.3 We note that by using a bisector line energy estimate due to Hanson et al. [2, Theorem 3], the proof of Theorem 1.4 also implies Corollary 1.3. However, the method in [2] is very difficult to extend to higher dimensions. This explains why we need to employ techniques from Fourier extension/restriction theory to prove Theorem 1.2.

Remark 5.3 leads us to the following question:

Question: Is it possible to use results from Fourier extension/restriction theory to get a non-trivial result on bisector hyperplane energy in $\mathbb{F}_q^d$?

Acknowledgements T. Pham would like to thank to the VIASM for the hospitality and for the excellent working conditions.

Funding C.-Y. Shen was partially supported by NSTC grant 111-2115-M-002-010-MY5.

References

1. Chapman, J., Erdogan, M.B., Hart, D., Iosevich, A., Koh, D.: Pinned distance sets, k-simplices, Wolff's exponent in finite fields and sum-product estimates. Math. Z. **271**(1–2), 63–93 (2012)
2. Hanson, B., Lund, B., Roche-Newton, O.: On distinct perpendicular bisectors and pinned distances in finite fields. Finite Fields Appl. **37**, 240–264 (2016)
3. 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)
4. Iosevich, A., Koh, D.: Extension theorems for spheres in the finite field setting. Forum Math. **22**(3), 457–483 (2010)
5. Iosevich, A., Koh, D.: Extension theorems for the Fourier transform associated with nondegenerate quadratic surfaces in vector spaces over finite fields. Ill. J. Math. **52**(2), 611–628 (2008)
6. Iosevich, A., Koh, D., Lee, S., Pham, T., Shen, C.-Y.: On restriction estimates for the zero radius sphere over finite fields. Can. J. Math. **73**(3), 769–786 (2021)
7. Koh, D., Pham, T., Vinh, L.A.: Extension theorems and a connection to the Erdős-Falconer distance problem over finite fields. J. Funct. Anal. **281**(8), 109–137 (2021)

8. Lewko, M.: Finite field restriction estimates based on Kakeya maximal operator estimates. J. Eur. Math. Soc. **21**(12), 3649–3707 (2019)
9. Mockenhaupt, G., Tao, T.: Restriction and Kakeya phenomena for finite fields. Duke Math. J. **121**(1), 35–74 (2004)
10. Murphy, B., Petridis, G., Pham, T., Rudnev, M., Stevens, S.: On the pinned distances problem over finite fields. J. Lond. Math. Soc. **105**(1), 469–499 (2022)
11. Pham, T., Vinh, L.A.: Some combinatorial number theory problems over finite valuation rings. Ill. J. Math. **61**(1–2), 243–257 (2017)
12. Rudnev, M., Shkredov, I.D.: On the restriction problem for discrete paraboloid in lower dimension. Adv. Math. **339**, 657–671 (2018)