JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **26**, No. 4, November 2013
http://dx.doi.org/10.14403/jcms.2013.26.4.853

SIZE OF DOT PRODUCT SETS DETERMINED BY PAIRS OF SUBSETS OF VECTOR SPACES OVER FINITE FIELDS

Doowon Koh* and Youngjin Pi**

Abstract. In this paper we study the cardinality of the dot product set generated by two subsets of vector spaces over finite fields. We notice that the results on the dot product problems for one set can be simply extended to two sets. Let E and F be subsets of the d-dimensional vector space $\mathbb{F}_q^d$ over a finite field $\mathbb{F}_q$ with q elements. As a new result, we prove that if E and F are subsets of the paraboloid and $|E||F| \geq Cq^d$ for some large $C > 1$, then $|\Pi(E,F)| \geq cq$ for some $0 < c < 1$. In particular, we find a connection between the size of the dot product set and the number of lines through both the origin and a nonzero point in the given set E. As an application of this observation, we obtain more sharpened results on the generalized dot product set problems. The discrete Fourier analysis and geometrical observation play a crucial role in proving our results.

1. Introduction

How many distinct distances can be determined by a finite subset of $\mathbb{R}^d$? In 1946, this question was addressed by Erdős [3]. This problem is well known as the Erdős distance problem in the Euclidean space. More generally, given $E, F \subset \mathbb{R}^d$ with $|E|, |F| < \infty$, one may ask for the cardinality of the distance set $\Delta(E,F)$ in terms of the sizes of E and F, where $|\cdot|$ denotes the cardinality of a finite set of $\mathbb{R}^d$ and the distance set $\Delta(E,F)$ is defined by

$$\Delta(E,F) = \left\{ \sqrt{(x_1-y_1)^2 + \cdots + (x_d-y_d)^2} : x \in E, y \in F \right\}.$$

Received September 03, 2013; Accepted October 28, 2013.

2010 Mathematics Subject Classification: Primary 52C10; Secondary 11T23.

Key words and phrases: dot product sets, finite fields, paraboloids.

Correspondence should be addressed to Doowon Koh, koh131@chungbuk.ac.kr.

*This work was supported by the research grant of the Chungbuk National University in 2012.

If $E = F$, then we shall write $\Delta(E)$ for $\Delta(E, F)$. The first nontrivial result on this problem was obtained by Erdős [3]. He proved that if $E \subset \mathbb{R}^d$, then $|\Delta(E)| \geq c|E|^{1/d}$ for some constant $0 < c < 1$ independent of $|E|$. In addition, he conjectured that for every $\varepsilon > 0$ there exists $c_\varepsilon > 0$ such that $|\Delta(E)| \geq c_\varepsilon |E|^{2/d-\varepsilon}$. The conjecture on the plane was recently solved by Guth and Katz [6] but it remains open for higher dimensions (see, for example, [14, 11, 13]).

As a continuous version of the Erdős distance problem, the Falconer distance problem has been studied. The Falconer distance conjecture says that if E is a compact subset of $\mathbb{R}^d, d \geq 2$, and the Hausdorff dimension of E is greater than $d/2$, then the distance set $\Delta(E)$ has a positive Lebesgue measure. Since this conjecture was first addressed by Falconer [5], much attention has been given to this problem but it has not been solved for any dimensions. Using the decay estimate of the Fourier transform on the sphere, Falconer [5] firstly obtained that

$$\dim_{\mathcal{H}}(E) > \frac{d+1}{2} \Longrightarrow \mathcal{L}(\Delta(E)) > 0,$$

where $\dim_{\mathcal{H}}(E)$ denotes the Hausdorff dimension of $E \subset \mathbb{R}^d$ and $\mathcal{L}(\Delta(E))$ denotes one-dimensional Lebesgue measure of the distance set $\Delta(E)$. The Falconer's result was generalized by Mattila who proved in [12] that for any compact sets $E, F \subset \mathbb{R}^d$,

$$\dim_{\mathcal{H}}(E) + \dim_{\mathcal{H}}(F) > d + 1 \Longrightarrow \mathcal{L}(\Delta(E, F)) > 0.$$

The currently best known results on the Falconer problem are due to Wolff [15] for two dimensions and Erdoğan [4] for higher dimensions. Their results say that if $E \subset \mathbb{R}^d, d \geq 2$, with $\dim_{\mathcal{H}}(E) > d/2 + 1/3$, then $\mathcal{L}(\Delta(E)) > 0$.

In recent years, the Erdős-Falconer distance problems have been reconstructed in the finite field setting. Let $\mathbb{F}_q^d$ denote the d-dimensional vector space over a finite field $\mathbb{F}_q$ with q elements. Throughout the paper, we always assume that the characteristic of $\mathbb{F}_q$ is greater than two. Given $E, F \subset \mathbb{F}_q^d, d \geq 2$, the distance set, denoted by $\mathcal{D}(E, F)$, is defined by

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

where $\|\alpha\| = \alpha_1^2 + \cdots + \alpha_d^2$ for $\alpha = (\alpha_1, \ldots, \alpha_d) \in \mathbb{F}_q^d$. We point out that the function $\| \cdot \|$ on $\mathbb{F}_q^d$ is not a standard norm but its image is invariant under the rotations in $\mathbb{F}_q^d$. The Erdős distance problem in the finite field setting is to find the connection between $|\mathcal{D}(E, F)|$ and cardinalities of $E, F \subset \mathbb{F}_q^d$. In the prime field setting, the Erdős distance problem in two dimensions was initially posed and studied by Bourgain-Katz-Tao [1]. In 2007, Iosevich and Rudnev [8] developed the problem in arbitrary dimensional vector spaces over general finite fields. Using the Kloosterman sum estimate, Iosevich and Rudnev [8] obtained that if $E \subset \mathbb{F}_q^d$, then

$$|\mathcal{D}(E,E)| \gg_c \min\left\{q, \frac{|E|}{q^{\frac{d-1}{2}}}\right\}. \tag{1.1}$$

Remark 1.1. Here and throughout this paper, the notation $A \gg_c B$ for $A, B > 0$ means that there exists a constant $0 < c < 1$ depending only on the dimension d such that $A \geq cB$. On the other hand, we shall use the notation $A \gg_C B$ to indicate that there exists a sufficient large constant $C > 1$ depending only on the dimension d such that $A \geq CB$. The constants $0 < c < 1$ and $C > 1$ may change from one line to another line but they are independent of the size of the underlying finite field $\mathbb{F}_q$. We also write $B \ll_C A$ for $A \gg_c B$. $A \sim B$ means that there exist constants $0 < c < 1, 1 < C$ such that $cB \leq A \leq CB$, where c, C depend only on the dimension d.

As a finite field version of the Falconer distance problem, Iosevich and Rudnev [8] conjectured that if $E \subset \mathbb{F}_q^d$ with $|E| \gg_C q^{d/2}$, then $|\mathcal{D}(E,E)| \gg_c q$. As a corollary of (1.1), they obtained that $|\mathcal{D}(E,E)| \gg_c q$ as long as $|E| \gg_C q^{(d+1)/2}$. The authors in [7] constructed arithmetic examples which show that the conjecture by Iosevich and Rudnev is not true in odd dimensions and the exponent $(d+1)/2$ gives a sharp result on the Falconer distance problem in odd dimensional vector spaces over $\mathbb{F}_q$. However, it has been believed that the conjecture may be true in even dimensions, in part because the authors in [2] recently showed that if $E \subset \mathbb{F}_q^2$ with $|E| \gg_C q^{4/3}$, then $|\mathcal{D}(E,E)| \gg_c q$. When $d = 2$, the exponent $4/3$ is better than the exponent $(d+1)/2$ which gives a sharp exponent in odd dimensions. This result for dimension two was generalized by Koh and Shen [9] who proved that if $E, F \subset \mathbb{F}_q^2$ with $|E||F| \gg_C q^{8/3}$, then $|\mathcal{D}(E,F)| \gg_c q$. In [10], they also stated the following conjecture which generalizes the conjecture originally stated in [8] for even dimensions.

Conjecture 1.2. *Let $d \geq 2$ be an even integer. Suppose $E, F \subset \mathbb{F}_q^d$. If $|E||F| \gg_C q^d$, then $|\mathcal{D}(E,F)| \gg_c q$.*

This conjecture has not been solved but there are some specific sets which yield the conclusion of the conjecture for any dimensions $d \geq 2$.

For example, Iosevich and Rudnev [8] showed that the conclusion of the conjecture holds if $E = F$ and E is a Salem set. Here, we recall that a set $E \subset \mathbb{F}_q^d$ is called a Salem set if $|\widehat{E}(m)| \ll_C \sqrt{|E|}/q^d$ for all $m \in \mathbb{F}_q^d \setminus \{(0, \ldots, 0)\}$. Considering the number of vectors determined by two sets $E, F \subset \mathbb{F}_q^d$, Koh and Shen [9] deduced that if one of sets $E, F \subset \mathbb{F}_q^d$ is a Salem set, then the conclusion of Conjecture 1.2 follows for any dimensions $d \geq 2$.

By analogy with the distance set $\mathcal{D}(E, F)$, if $E, F \subset \mathbb{F}_q^d$, then one can define a set of dot products as

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

In the case when $E = F \subset \mathbb{F}_q^d$, the authors in [7] investigated the cardinality of $|\Pi(E, F)|$. They proved the following result.

Proposition 1.3. *Let $E \subset \mathbb{F}_q^d$. If $|E| \gg_C q^{(d+1)/2}$, then*

$$|\Pi(E, E)| \gg_c q.$$

In addition, they provided an example to show that the exponent $(d + 1)/2$ in Proposition 1.3 can not be improved on a general set E. However, they made a remarkable observation that if E lies on a unit sphere, then Proposition 1.3 can be improved. More precisely, they proved the following.

Proposition 1.4. *Let $E \subset S_1 := \{x \in \mathbb{F}_q^d : x_1^2 + \cdots + x_d^2 = 1\}$. If $|E| \gg_C q^{d/2}$, then $|\Pi(E, E)| \gg_c q$.*

As a direct application of this proposition, they deduced the following Erdős-Falconer distance result on the unit sphere.

Proposition 1.5. *Let $S_1 = \{x \in \mathbb{F}_q^d : x_1^2 + x_2^2 + \cdots + x_d^2 = 1\}$. If $d \geq 3$, $E \subset S_1$, and $|E| \gg_C q^{d/2}$, then $|\mathcal{D}(E, E)| \gg_c q$.*

This proposition implies that the conclusion of Conjecture 1.2 holds for the dimensions $d \geq 3$ if the set E is restricted to the unit sphere.

1.1. Purpose of this paper

For each $x \in \mathbb{F}_q^{d*}$, define

$$l_x = \{sx \in \mathbb{F}_q^d : s \in \mathbb{F}_q^*\}, \tag{1.2}$$

where we denote $\mathbb{F}_q^{d*} = \mathbb{F}_q^d \setminus \{(0, \ldots, 0)\}$ for $d \geq 2$, and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. Estimating $\max_{x \in \mathbb{F}_q^{d*}} |E \cap l_x|$ was one of the most important ingredients in proving Propositions 1.3, 1.4, and 1.5. One of the purposes of this paper is to announce that such an idea enables us to extend results of aforementioned propositions to the general dot product set $\Pi(E,F)$. In particular, we prove that the conclusion of Proposition 1.4 still holds in the case when the unit sphere S_1 is replaced by the paraboloid $P := \{x \in \mathbb{F}_q^d : x_1^2 + \cdots + x_{d-1}^2 = x_d\}$. Furthermore, we observe that if one of the sets E, F is a Salem set, then we are able to obtain extremely good results on the generalized dot product set problem.

The other purpose of this paper is to introduce a new point of view in deriving the results on generalized dot product sets . Roughly speaking, we relate the dot product problem to estimation of the number of lines containing both the origin and an element in a set $E \setminus \{(0,\dots,0)\} \subset \mathbb{F}_q^d$. As a result, we improve statements of aforementioned propositions for general two sets $E, F \subset \mathbb{F}_q^d$. In addition, we classify certain class of the sets $E, F \subset \mathbb{F}_q^d$ which yield much better result than that of Proposition 1.3. For example, assuming that the number of lines both passing through the origin and intersecting with $E \setminus \{(0,\dots,0)\}$ (or $F \setminus \{(0,\dots,0)\}$) is much greater than $|E|/q$ (or $|F|/q$), we shall see that the result of Proposition 1.3 can be improved.

2. Preliminaries

Discrete Fourier analysis is considered as one of the most useful tools in studying problems in the finite field setting. In this section, we briefly review it and derive lemmas which are essential in proving our results.

2.1. Discrete Fourier analysis

We shall denote by ψ a nontrivial additive character of $\mathbb{F}_q$. All results in this paper are independent of the choice of the character ψ. Recall that $\psi : \mathbb{F}_q \to \{u \in \mathbb{C} : |u| = 1\}$ is a group homomorphism. The orthogonality relation of ψ yields that

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

where $m \cdot x$ denotes the usual dot-product notation. Given a function $f : \mathbb{F}_q^d \to \mathbb{C}$, the Fourier transform of the function f is defined by

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

Then the Plancherel theorem in this content says that

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

Thus, it is clear that if $E\subset\mathbb{F}_q^d$, then

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

Here, throughout this paper, we identify the set $E\subset\mathbb{F}_q^d$ with the characteristic function on the set E.

2.2. Key lemmas related to a general dot product set $\Pi(E,F)$

Given $E,F{\subset}F_q^d$, a counting function ν on $\mathbb{F}_q$ is defined by

$$\nu(t)=|\{(x,y)\subset E\times F: x\cdot y=t\}|.$$

By the definition of the dot product set $\Pi(E,F)$, it is clear that

$$|E||F|=\sum_{t\in\Pi(E,F)}1\times\nu(t).$$

Applying the Cauchy-Schwarz inequality, we see that

$$|\Pi(E,F)|\geq\frac{|E|^2|F|^2}{\sum_{t\in\mathbb{F}_q}\nu^2(t)}. \tag{2.1}$$

Following the argument in [7], we obtain the following formula.

Lemma 2.1. *Let $E,F\subset\mathbb{F}_q^d$ with $(0,\dots,0)\notin E$. Then we have*

$$|\Pi(E,F)|\gg_c\min\left\{q,\ \frac{|E||F|^2}{q^{2d-1}\sum\limits_{x\in\mathbb{F}_q^{d*}}\sum\limits_{s\in\mathbb{F}_q^*}E(sx)|\widehat{F}(x)|^2}\right\},$$

where $\mathbb{F}_q^{d*}:=\mathbb{F}_q^d\setminus\{(0,\dots,0)\}$.

Proof. Since $(0,\dots,0)\notin E$, it is enough by (2.1) to show that

$$\sum_{t\in\mathbb{F}_q}\nu^2(t)\leq\frac{|E|^2|F|^2}{q}+q^{2d-1}|E|\sum_{x\in\mathbb{F}_q^d}\sum_{s\in\mathbb{F}_q^*}E(sx)|\widehat{F}(x)|^2.$$

By the Cauchy-Schwarz inequality, it follows that for each $t \in \mathbb{F}_q$,

$$\begin{aligned}\nu^2(t) &= \left(\sum_{x\in E}\sum_{y\in F: x\cdot y=t} 1\right)^2 \leq |E| \sum_{x\in E}\left(\sum_{y\in F: x\cdot y=t} 1\right)^2 \\ &= |E| \sum_{x\cdot y=t=x\cdot y'} E(x)F(y)F(y').\end{aligned}$$

Summing over $t \in \mathbb{F}_q$ and using the orthogonality relation of ψ, it follows

$$\begin{aligned}\sum_{t\in\mathbb{F}_q} \nu^2(t) &\leq |E|q^{-1} \sum_{s\in\mathbb{F}_q}\sum_{x\in E, y, y'\in F} \psi(sx\cdot(y-y')) \\ &= q^{-1}|E|^2|F|^2 + |E|q^{-1}\sum_{s\in\mathbb{F}_q^*}\sum_{x\in E, y, y'\in F} \psi(sx\cdot(y-y')).\end{aligned}$$

By the definition of the Fourier transform and a change of variables,

$$\begin{aligned}\sum_{t\in\mathbb{F}_q} \nu^2(t) &\leq q^{-1}|E|^2|F|^2 + q^{2d-1}|E| \sum_{x\in\mathbb{F}_q^d, s\in\mathbb{F}_q^*} E(x)|\widehat{F}(sx)|^2 \\ &= q^{-1}|E|^2|F|^2 + q^{2d-1}|E| \sum_{x\in\mathbb{F}_q^d, s\in\mathbb{F}_q^*} E(sx)|\widehat{F}(x)|^2,\end{aligned}$$

which completes the proof. □

Definition 2.2. For $E, F \subset \mathbb{F}_q^d$, we define

$$\begin{aligned}\mathfrak{B}(E,F) &= \sum_{x\in\mathbb{F}_q^{d*}}\sum_{s\in\mathbb{F}_q^*} E(sx)|\widehat{F}(x)|^2 \\ &= \sum_{x\in\mathbb{F}_q^{d*}} |E\cap l_x||\widehat{F}(x)|^2,\end{aligned}$$

where l_x is defined as in (1.2).

According to Lemma 2.1, a lower bound of $|\Pi(E,F)|$ can be determined by an upper bound of $\mathfrak{B}(E,F)$. More precisely we have the following result.

Lemma 2.3. *Let $E, F \subset \mathbb{F}_q^d$. Assume that* $\max_{x\in\mathbb{F}_q^{d*}} |E\cap l_x| \ll_C q^\beta$ *for some $0 \leq \beta \leq 1$. Then if $|E||F| \gg_C q^{d+\beta}$, we have*

$$|\Pi(E,F)| \gg_c q.$$

Proof. Without a loss of generality, we may assume that $(0,\ldots,0)\notin E$. Since $\max_{x\in\mathbb{F}_q^{d*}}|E\cap l_x|\ll_C q^{\beta}$, it follows from the Plancherel theorem that

$$\mathfrak{B}(E,F)\ll_C q^{\beta}\sum_{x\in\mathbb{F}_q^d}|\widehat{F}(x)|^2=q^{\beta-d}|F|.$$

Combining this with Lemma 2.1, we conclude that

$$|\Pi(E,F)|\gg_c \min\left\{q,\ \frac{|E||F|}{q^{d+\beta-1}}\right\},$$

which implies the statement of the lemma. □

3. Results on the generalized dot product sets

In this section, we first collect results on the generalized dot product set, which can be obtained by a direct application of Lemma 2.3 or Lemma 2.1. For example, we will be able to simply generalize the results of Propositions 1.3, 1.4, and 1.5. As a core part of this section, we derive a dot product result on subsets of the paraboloid, which may not be obtained by a direct application of Lemma 2.3.

3.1. Direct consequences of Lemma 2.3

The general version of Proposition 1.3 is as follows.

Theorem 3.1. *Let $E,F\subset\mathbb{F}_q^d$. If $|E||F|\gg_C q^{d+1}$, then we have $|\Pi(E,F)|\gg_c q$.*

Proof. Since every line contains exactly q points, it is clear that

$$\max_{x\in\mathbb{F}_q^{d*}}|E\cap l_x|\le q.$$

Thus, the result follows immediately by using Lemma 2.3 with $\beta=1$. □

The following theorem is a generalization of Proposition 1.4.

Theorem 3.2. *Let $F\subset\mathbb{F}_q^d$ and $E\subset S_j:=\{x\in\mathbb{F}_q^d: x_1^2+\cdots+x_d^2=j\in\mathbb{F}_q^*\}$. Then if $|E||F|\gg_C q^d$, we have $|\Pi(E,F)|\gg_c q$.*

Proof. Since $j\ne 0$, it follows that

$$\max_{x\in\mathbb{F}_q^{d*}}|E\cap l_x|\le 2.$$

Therefore, the statement of the theorem follows by applying Lemma 2.3 with $\beta=0$. □

We now give the generalization of Proposition 1.5 .

Theorem 3.3. *Let $S_j = \{x \in \mathbb{F}_q^d : x_1^2 + x_2^2 + \cdots + x_d^2 = j\}$. Suppose that $E \subset S_i$ and $F \subset S_j$ for some $i, j \in \mathbb{F}_q^*$. Then if $d \geq 3$, and $|E||F| \gg_C q^d$, we have $|\mathcal{D}(E, F)| \gg_c q$.*

Proof. Notice that if $x \in E \subset S_i$ and $y \in F \subset S_j$, then

$$\|x - y\| = x \cdot x - 2x \cdot y + y \cdot y = i + j - 2x \cdot y.$$

Thus, we see that $|D(E, F)| = |\Pi(E, F)|$ and it suffices to prove that $|\Pi(E, F)| \gg_c q$ as long as $|E||F| \gg_C q^d$. However, this follows immediately from Theorem 3.2. □

Now we address a result on the dot product set $\Pi(E, F)$ in the case when one of sets $E, F \subset \mathbb{F}_q^d$ is a Salem set. Recall that a set $F \subset \mathbb{F}_q^d$ is a Salem set if $|\widehat{F}(m)| \ll_C q^{-d}\sqrt{|F|}$ for all $m \neq (0, \ldots, 0)$.

Theorem 3.4. *Let $E, F \subset \mathbb{F}_q^d$. If F is a Salem set and $|F| \gg_C q$, then*

$$|\Pi(E, F)| \gg_c q.$$

Proof. Notice that we may assume that $(0, \ldots, 0) \notin E$. Since F is a Salem set, we see that

$$\max_{x \in \mathbb{F}_q^{d*}} |\widehat{F}(x)|^2 \ll_C q^{-2d}|F|.$$

It therefore follows that

$$\mathfrak{B}(E, F) \ll_C q^{-2d}|F| \sum_{x \in \mathbb{F}_q^{d*}} \sum_{s \in \mathbb{F}_q^*} E(sx) < q^{-2d}|F||E|q = q^{1-2d}|E||F|.$$

By this and Lemma 2.1, we obtain that

$$|\Pi(E, F)| \gg_c \min\{q,\ |F|\},$$

which implies the statement of the theorem. □

3.2. Dot product sets determined by subsets of the paraboloid

In the finite field setting, the paraboloid in $\mathbb{F}_q^d$, denoted by P, is defined by

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

which is an analog of the Euclidean paraboloid.

Unlike the sphere S_j with nonzero radius, the paraboloid $P \subset \mathbb{F}_q^d, d \geq 3$, contains lines through the origin. For example, the set $H := \{x \in P : x_d = 0\}$ consists of some of lines through the origin. Thus, if $E \subset P$

contains some of such lines, then $\max_{x\in\mathbb{F}_q^{d*}} |E\cap l_x| = q-1$. In this case, if we simply use Lemma 2.3 , then we only get that if $|E||F| \gg_C q^{d+1}$, then $|\Pi(E,F)| \gg_c q$. This result is much weaker than the dot product result on spheres with nonzero radius, but there are no known good results for sets in the paraboloid. In this subsection, we prove that if $E,F\subset P$ and $|E||F| \gg_C q^d$, then $|\Pi(E,F)| \gg_c q$. We begin with a definition. Let $\pi : \mathbb{F}_q^d \to \mathbb{F}_q^{d-1}$ be a projection map defined as

$$\pi(x) = (x_1,\ldots,x_{d-1}) \quad \text{for } x=(x_1,\ldots,x_{d-1},x_d).$$

We have the following result.

Lemma 3.5. *Let $E\subset P$ and $F\subset \mathbb{F}_q^d$. If $|E||\pi(F)| \gg_C q^d$, then $|\Pi(E,F)| \gg_c q$.*

Proof. Write that $E=G\cup B$ where

$$G=\{x\in E : x_d\neq 0\} \quad \text{and} \quad B=\{x\in E : x_d=0\}.$$

We may assume that either $|G|\ge |E|/2$ or $|B|\ge |E|/2$.

Case 1. Assume that $|G|\ge|E|/2$. Since $G\subset P$, it is not hard to see that $|G\cap l_x|\le 1$ for all $x\in\mathbb{F}_q^{d*}$. By Lemma 2.3, we see that if $|G||F|\gg_C q^d$, then $|\Pi(G,F)|\gg_c q$. Since $2|G||F| \ge |E||\pi(F)| \gg_C q^d$, and $|\Pi(E,F)|\ge|\Pi(G,F)|$, the statement of the lemma follows.

Case 2. Assume that $|B|\ge|E|/2$. By the definitions of B and the dot product, notice that

$$\begin{aligned}\Pi(B,F) &= \Pi(B,\pi(F)\times\{0\}) = \Pi(\pi(B),\pi(F))\\ &:= \{\alpha\cdot\beta\in\mathbb{F}_q : \alpha\in\pi(B)\subset\mathbb{F}_q^{d-1},\ \beta\in\pi(F)\subset\mathbb{F}_q^{d-1}\}.\end{aligned}$$

Since $\pi(B),\pi(F)\subset\mathbb{F}_q^{d-1}$, we can use Theorem 3.1 for dimension $d-1$ to deduce that

$$|\Pi(B,F)| = |\Pi(\pi(B),\pi(F))| \gg_c q \quad \text{if } |\pi(B)||\pi(F)| \gg_C q^d.$$

Since B is a subset of the paraboloid P, it is clear that $|\pi(B)| = |B| \ge |E|/2$, where the inequality follows by our case assumption. Since $|\Pi(E,F)|\ge|\Pi(B,F)|$, we complete the proof. □

Since $|\Pi(F)| = |F|$ for $F\subset P$, the following result follows immediately from Lemma 3.5.

Theorem 3.6. *Let $E,F\subset P\subset\mathbb{F}_q^d$. If $|E||F|\gg_C q^d$, then we have $|\Pi(E,F)|\gg_c q$.*

Remark 3.7. Let $E \subset P \subset \mathbb{F}_q^d$, and $F \subset \mathbb{F}_q^d$ with $|\pi(F)| \gg_c |F|/q^\gamma$ for some $0 \leq \gamma \leq 1$. In this case, Lemma 3.5 implies that if $|E||F| \gg_C q^{d+\gamma}$, then $|\Pi(E,F)| \gg_c q$.

Here we may have a natural question.

Question 3.8. *Let $E \subset P$ and $F \subset \mathbb{F}_q^d$. Is it true that if $|E||F| \gg_C q^d$, then $|\Pi(E,F)| \gg_c q$?*

Considering Remark 3.7, it seems that the answer is negative. However, Theorem 3.2 says that if we replace the paraboloid P by the sphere S_j with nonzero radius, then the answer is positive. Now, we show that if the paraboloid P is appropriately translated, then the answer to Question 3.8 is also positive.

Theorem 3.9. *Let $a \in \mathbb{F}_q^d \setminus \overline{P} := \{x \in \mathbb{F}_q^d : x_1^2 + \cdots + x_{d-1}^2 = -x_d\}$. Suppose that $E \subset P + a := \{x + a : x \in P\}$ and $F \subset \mathbb{F}_q^d$. Then if $|E||F| \gg_C q^d$, we have $|\Pi(E,F)| \gg_c q$.*

Proof. By Lemma 2.3, it suffices to prove that for every $a \in \mathbb{F}_q^d \setminus \overline{P}$, and $x \neq (0, \ldots, 0)$,

$$|(P+a) \cap l_x| \ll_C 1, \tag{3.1}$$

where we recall that $l_x = \{sx \in \mathbb{F}_q^{d*} : s \in \mathbb{F}_q^*\}$. Fix $x \in P + a$. Then it follows that

$$(x_1 - a_1)^2 + \cdots + (x_{d-1} - a_{d-1})^2 = x_d - a_d.$$

With this assumption, it is enough to prove that

$$|\{s \in \mathbb{F}_q^* : sx \in P + a\}| \leq 2.$$

It follows from a routine algebra that if $a \notin \overline{P}$, then

$$|\{s \in \mathbb{F}_q^* : (sx_1 - a_1)^2 + \cdots + (sx_{d-1} - a_{d-1})^2 = sx_d - a_d\}| \leq 2.$$

Thus, the proof is complete. □

Observe that $(0, \ldots, 0) \in P$, but the sphere S_j for $j \neq 0$ or $P + a$ for $a \notin P$ does not contain $(0, \ldots, 0)$. From Theorem 3.2 and Theorem 3.9, this observation may lead us to the following conjecture.

Conjecture 3.10. *Let $V = \{x \in \mathbb{F}_q^d : Q(x) = 0\}$ be a variety where $Q(x) \in \mathbb{F}_q[x_1, \ldots, x_d]$ is a polynomial. In addition, assume that $(0, \ldots, 0) \notin V$. If $E \subset V$ and $F \subset \mathbb{F}_q^d$ with $|E||F| \gg_C q^d$, then we have*

$$|\Pi(E,F)| \gg_c q.$$

4. Sharpened results on the generalized dot product set

In the previous section, we deduced the results on the dot product set by considering $\max_{x\in\mathbb{F}_q^{d*}} |E\cap l_x|$. This method may give us a sharp result for the set $E\subset\mathbb{F}_q^d$ in the case when $|E\cap l_x|\sim|E\cap l_y|$ for almost elements $x,y\in\mathbb{F}_q^{d*}$. However, it may not be efficient in the case when the variation of $|E\cap l_x|$ for $x\in\mathbb{F}_q^{d*}$ is relatively large. In this section, we introduce a new approach to compensate the defect of the previous method and provide improved statements of the results in the previous section.

Now, we derive a new formula to determine $|\Pi(E,F)|$, which is much stronger than Lemma 2.3.

Lemma 4.1. *Let $E,F\subset\mathbb{F}_q^d$. Assume that the number of lines through the origin and a point in $E\setminus\{(0,\dots,0)\}$ is at least $\sim q^{-\alpha}|E|$ for some $0\le\alpha\le 1$. If $|E||F|\gg_C q^{d+\alpha}$ then there exists a set $E_0\subset E$ with $|E_0|\sim q^{-\alpha}|E|$ such that*

$$|\Pi(E_0,F)|\gg_c q.$$

Proof. Note that we may assume that $(0,\dots,0)\notin E$. Let n be an integer with $n\sim q^{-\alpha}|E|$. By assumption, we may choose n lines, say that $l_j, j=1,2,\dots,n$, such that each of them contains at least one point in E, and is also passing through the origin. For each $j=1,2,\dots,n$, choose exactly an element $x^j\in l_j\cap E$ and define

$$E_0=\{x^j: j=1,2,\dots,n\}.$$

Since $|E_0|=n\sim q^{-\alpha}|E|$ for some $0\le\alpha\le 1$, it suffices to prove that $|\Pi(E_0,F)|\gg_c q$ as long as $|E||F|\gg_C q^{d+\alpha}$. By the definition of E_0, it is clear that $\sum_{s\in\mathbb{F}_q^*}E_0(sx)=1$ for each $x\ne(0,\dots,0)$. This implies that $\mathfrak{B}(E_0,F)\le\sum_{x\in\mathbb{F}_q^d}|\widehat{F}(x)|^2=q^{-d}|F|$. Now applying Lemma 2.1 with E_0,F yields that

$$|\Pi(E_0,F)|\gg_c \min\left\{q,\ \frac{|E_0||F|}{q^{d-1}}\right\}.$$

Since $|E_0|\sim q^{-\alpha}|E|$, the statement of the theorem follows immediately from the assumption that $|E||F|\gg_C q^{d+\alpha}$. □

The value α given in Lemma 4.1 must be contained in $[0,1]$. For example, if E lies on a unit sphere $S_1:=\{x\in\mathbb{F}_q^d:\|x\|=1\}$, then α can be taken as zero. In addition, observe that for each $E\setminus\{(0,\dots,0)\}$, there are at least $\sim q^{-1}|E|$ such lines, because a line contains exactly q

points. Namely, α must be less than or equal to one. Also notice from Lemma 4.1 that we can expect better dot product results whenever the set E intersects with lots of such lines. In order words, the smaller α is, the better the result is. As mentioned before, the $(d+1)/2$ is the optimal exponent to obtain the conclusion of Proposition 1.3 for arbitrary set E. Thus, the exponent $d+1$ in the assumption of Theorem 3.1 is also optimal in general. However, Lemma 4.1 illustrates that the exponent $d+1$ can be improved in the case when the set $E \setminus \{(0, \ldots, 0)\}$ intersects with at least $|E|/q^{1-\varepsilon}$ lines through the origin for some $0 < \varepsilon \leq 1$.

Now, we claim that Lemma 4.1 is much superior to Lemma 2.3. Indeed, an upgraded version of Lemma 2.3 can be given by a corollary of Lemma 4.1. More precisely, we can derive the following fact.

Lemma 4.2. *Let* $E, F \subset \mathbb{F}_q^d$. *Assume that* $\max_{x \in \mathbb{F}_q^{d*}} |E \cap l_x| \ll_C q^\beta$ *for some* $0 \leq \beta \leq 1$. *Then if* $|E||F| \gg_C q^{d+\beta}$, *there exists a set* $E_0 \subset E$ *with* $|E_0| \sim q^{-\beta}|E|$ *such that*

$$|\Pi(E_0, F)| \gg_c q.$$

Proof. Since $\max_{x \in \mathbb{F}_q^{d*}} |E \cap l_x| \ll_C q^\beta$, it is clear that the number of lines through the origin and a point in $E \setminus \{(0, \ldots, 0)\}$ is at least $\sim q^{-\beta}|E|$. Hence, the statement of the lemma follows immediately by Lemma 4.1. □

Lemma 4.2 enables us to deduce stronger conclusion than Lemma 2.1, because $|\Pi(E_0, F)| \leq |\Pi(E, F)|$ for $E_0 \subset E$. For example, Theorem 3.1 can be improved by the following statement.

Theorem 4.3. *Let* $E, F \subset \mathbb{F}_q^d$. *It* $|E||F| \gg_C q^{d+1}$, *then there exists a set* $E_0 \subset E$ *with* $|E_0| \sim q^{-1}|E|$ *such that*

$$|\Pi(E_0, F)| \gg_c q.$$

Proof. Since $|E \cap l_x| \leq q$, this theorem is an immediate consequence of Lemma 4.2. □

Notice that Lemma 4.2 can be also used to deduce the improved conclusions of Theorem 3.2 and Theorem 1.5. We close this paper with an important remark on Theorem 4.3.

Remark 4.4. The authors in [2] studied the pinned distance sets and proved the following strong result (Theorem 2.2 in [2]).

Proposition 4.5. *Let* $E \subset \mathbb{F}_q^d, d \geq 2$. *If* $|E| \geq q^{(d+1)/2}$, *then there exists a set* $E' \subset E$ *with* $|E'| \gg_c |E|$ *such that if* $x \in E'$, *then* $|\Pi(x, E)| > q/2$, *where* $\Pi(x, E) := \{x \cdot y : y \in E\}$.

This proposition is much superior to our Theorem 4.3 in the case when $E = F$. The existence of such set E' in Proposition 4.5 was proved by using an averaging argument. Therefore, there is no information about how to choose an exact element x of E' so that $|\Pi(x, E)| \gg_c q$. On the other hand, the proof of our Theorem 4.3 clearly indicates how to choose the set E_0. In practice, our Theorem 4.3 can be very useful.

Acknowledgments

The authors would like to thank referees for helpful comments on this paper which enable us to complete this paper.

References

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

[2] J. Chapman, M. Erdoğan, D. Hart, A. Iosevich, and D. Koh, *Pinned distance sets, Wolff's exponent in finite fields and sum-product estimates*, Math. Z. **271** (2012), 63-93.

[3] P. Erdős, *On sets of distances of n points*, Amer. Math. Monthly **53** (1946), 248-250.

[4] M. Erdoğan, *A bilinear Fourier extension theorem and applications to the distance set problem,* Internat. Math. Res. Notices **23** (2005), 1411-1425.

[5] K. Falconer, *On the Hausdorff dimension of distance sets,* Mathematika **32** (1985), 206-212.

[6] L. Guth and N. Katz, *On the Erdős distinct distance problem in the plane,* preprint.

[7] D. Hart, A. Iosevich, D. Koh, and M. Rudnev, *Averages over hyperplanes, sum-product theory in vector spaces over finite fields and the Erdös-Falconer distance conjecture*, Trans. Amer. Math. Soc. **363** (2011), no. 6, 3255-3275.

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

[9] D. Koh and C. Shen, *Sharp extension theorems and Falconer distance problems for algebraic curves in two dimensional vector spaces over finite fields,* Revista Matematica Iberoamericana **28** (2012), no. 1, 157-178.

[10] D. Koh and C. Shen, *Additive energy and the Falconer distance problem in finite fields,* Integers **13** (2013), 1-10.

[11] N. Katz and G. Tardos, *A new entropy inequality for the Erdős distance problem*, In: Contemp. Math. Towards a Theory of Geometric Graphs, **342** Amer. Math. Soc. Providence (2004), 119–126.

[12] P. Mattila, *Spherical averages of Fourier transforms of measures with finite energy: dimension of intersections and distance sets,* Mathematika **34** (1987), 207-228.

[13] J. Solymosi and V. Vu, *D*istinct distances in high dimensional homogeneous sets in: Towards a Theory of Geometric Graphs (J. Pach, ed.), Contemporary Mathematics **342** Amer. Math. Soc. (2004), 259-268.

[14] J. Solymosi and V. Vu, *N*ear optimal bounds for the number of distinct distances in high dimensions, Combinatorica **28** (2008), no. 1, 113-125.

[15] T. Wolff, *Decay of circular means of Fourier transforms of measures,* Internat. Math. Res. Notices (1999), 547-567.

*
Department of Mathematics
Chungbuk National University
Cheongju 361-763, Republic of Korea
E-mail: koh131@chungbuk.ac.kr

**
Department of Mathematics
Chungbuk National University
Cheongju 361-763, Republic of Korea
E-mail: pi@chungbuk.ac.kr