Rev. Mat. Iberoam. **28** (2012), no. 1, 157–178
DOI 10.4171/RMI/672

Sharp extension theorems and Falconer distance problems for algebraic curves in two dimensional vector spaces over finite fields

Doowon Koh and Chun-Yen Shen

Abstract. In this paper we study extension theorems associated with general varieties in two dimensional vector spaces over finite fields. Applying Bezout's theorem, we obtain the sufficient and necessary conditions on general curves where sharp L^p-L^r extension estimates hold. Our main result can be considered as a nice generalization of works by Mockenhaupt and Tao in [17] and Iosevich and Koh in [10]. As an application of our sharp extension estimates, we also study the Falconer distance problems in two dimensions.

1. Introduction

In the Euclidean setting, the extension theorem is one of the most important, challenging open problems in harmonic analysis. Since this problem was first addressed in 1967 by Stein ([20]), it has been extensively studied in the last few decades, in part because it is closely related to other interesting problems in harmonic analysis, such as Kakeya problems, Falconer distance problems, and Bochner–Riesz summability problems. In the Euclidean case, the extension theorem asks us to determine the optimal range of exponents $1 \leq p, r \leq \infty$ such that the following extension estimate holds:

$$\|(fd\sigma)^{\vee}\|_{L^r(\mathbb{R}^d)} \leq C(p,r,d)\|f\|_{L^p(V,d\sigma)} \quad \text{for all } f \in L^p(V, d\sigma)\,,$$

where $d\sigma$ is a measure on the set V in $\mathbb{R}^d$ and $(fd\sigma)^{\vee}$ denotes the inverse Fourier transform of the measure $fd\sigma$. In the case when the set V is a hypersurface such as the sphere, the paraboloid, or the cone in $\mathbb{R}^d$, the extension problems have received much attention and they were completely solved in lower dimensions. For example, the complete solution for the circle or the parabola in $\mathbb{R}^2$ is due to Zygmund ([27]), and the complete solutions for the cone in $\mathbb{R}^3$ and the cone in $\mathbb{R}^4$

Mathematics Subject Classification (2010): 42B05, 11T24, 52C10.
Keywords: Finite fields, extension/restriction theorems, Falconer distances, Bezout's theorem.

are due to Barceló ([1]) and Wolff ([25]) respectively. Currently, the best known results for the cones in $\mathbb{R}^d, d \geq 5$, and the spheres or the paraboloids in $\mathbb{R}^d, d \geq 3$, are due to Wolff ([25]) and Tao ([22]) respectively, in which they used bilinear approach. However, it has been believed that their results can be improved and new ideas seem to be needed to totally understand the extension problems. For a comprehensive survey of these problems in the Euclidean case, see [23] and the references therein.

In recent year the extension problems have been also investigated in the finite field setting. The finite field case serves as a typical model for the Euclidean case and it also possesses structural advantages which enable us to relate our problems to other well-studied problems in number theory, arithmetic combinatorics, or algebraic geometry. Therefore, we may find useful techniques from these fields to attack our problems. Moreover, the finite field problems display independently interesting features. For these reasons, Mockenhaupt and Tao ([17]) first constructed the extension problems in the finite field setting and they provided us of remarkable facts related to extension theorems for several kinds of algebraic varieties. In particular, they gave us the complete solution for the parabola in two dimensional vector spaces over finite fields. It was Iosevich and Koh that continued the works by Mockenhaupt and Tao. In [11], they studied the L^p-L^r boundedness of the extension operators associated with paraboloids in higher dimensions and partially improved the results by Mockenhaupt and Tao. In [10], they also studied general spherical extension problems and they especially obtained the complete solution for the extension problems related to non-degenerate quadratic curves in two dimension.

In this paper we investigate general properties of algebraic varieties in two dimensional vector space of finite fields on which the extension problems are completely understood. We have the following main theorem which is a generalization of the sharp extension theorems for the parabola in [17] and the non-degenerate quadratic curves in [10] respectively.

Theorem 1.1. *Let $\mathbb{F}_q$ denote a finite field with q elements where we assume that q is a power of odd prime. Suppose that $P(x) \in \mathbb{F}_q[x_1, x_2]$ is non-zero polynomial. Define an algebraic variety $V \subset \mathbb{F}_q^2$ by*

$$V = \{x \in \mathbb{F}_q^2 : P(x) = 0\}.$$

Then, L^2-L^4 extension estimate related to V holds if and only if the polynomial $P(x)$ does not have any linear factor and $|V| \sim q$.

Here and throughout the paper, we denote by $|V|$ the cardinality of V, and $|V| \sim q$ means that there exist $C, c > 0$ depending only on the degree of the polynomial $P(x)$ such that $cq \leq |V| \leq Cq$. We also notice that the norm of the extension operator depends only on the degree of V and on the ratio $|V|/q$. In addition, we assume that the characteristic of the underlying finite field $\mathbb{F}_q$ is greater than the degree of V.

Remark 1.2. In Section 2, the definition of extension problems in finite fields is reviewed and we will give the proof of Theorem 1.1 in Section 3. The L^2-L^4 estimate in Theorem 1.1 gives the critical exponents for all possible exponents where the extension estimate holds (see Remark 2.3 and the necessary conditions (2.9) in Section 2). This presents an interesting fact that there exist some differences between the finite field case and the Euclidean case. For example, let us consider a set V consisting of all zeros of $x_1^4+x_2^4-1=0$. In the Euclidean case, the extension estimate for this variety V is much worse than that for the circle variety, $\{x\in\mathbb{R}^2 : x_1^2+x_2^2=1\}$, because V is a curve with a vanishing Gaussian curvature (see [5], or pages 414 and 418 of [21]). However, Theorem 1.1 says that the circle and the variety V yield the same extension estimate in finite fields. Another difference is that the curve in the finite field case yields much better extension estimate than its counterpart of the Euclidean case. For instance, the L^4-L^4 estimate gives the critical exponents up to the endpoints for the circular extension estimate in $\mathbb{R}^2$ (see [23]). However, this best possible result is much worse than the L^2-L^4 extension estimate which yields sharp exponents in finite fields case.

Another interesting problem in harmonic analysis is the Falconer distance problem which is closely related to the extension problems. Let $E\subset\mathbb{R}^d$, $d\geq 2$ be a compact subset. In the Euclidean setting, the Falconer distance problem is to find $s_0>0$ such that if the Hausdorff dimension of E is greater than s_0, then one-dimensional Lebesgue measure of $\Delta(E,E)$ is positive, where $\Delta(E,E)$ denotes the distance set given by

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

This problem was first addressed by Falconer ([7]) who conjectured that if the Hausdorff dimension of $E\subset\mathbb{R}^d$ is greater than $d/2$, then the Lebesgue measure of $\Delta(E,E)$ is positive. This problem has not been solved in all dimensions. Using the estimates of the Fourier transform of the characteristic function of an annulus in $\mathbb{R}^d$, Falconer in [7] first obtained the following nontrivial result:

$$\text{if } \dim(E)>\frac{d+1}{2}, \quad \text{then } |\Delta(E,E)|>0,$$

where $\dim(E)$ denotes the Hausdorff dimension of $E\subset\mathbb{R}^d$ and $|\Delta(E,E)|$ denotes the one-dimensional Lebesgue measure of the distance set $\Delta(E,E)$. In [16], Mattila generalized the Falconer result by showing that if $\dim(E)+\dim(F)>d+1$ then $|\Delta(E,F)|>0$, where E,F are compact subsets of $\mathbb{R}^d$ and $\Delta(E,F)=\{|x-y|\in\mathbb{R} : x\in E, y\in F\}$. Moreover, he reduced the Falconer distance problem to estimating the spherical means of Fourier transforms of measures. Using Mattila's approach, Wolff ([24]) proved that in two dimension, $\dim(E)>4/3$ implies $|\Delta(E,E)|>0$, which is the best known result in two dimension. Applying Mattila's approach along with the weighted version of Tao's bilinear extension theorem ([22]), Erdoğan in [6] obtained the best known results in higher dimensions: if $\dim(E)>d/2+1/3$, then $|\Delta(E,E)|>0$.

In [13], Iosevich and Rudnev first studied an analog of the Falconer distance problem in the finite field setting and Iosevich and Koh ([9]) studied the problems related to the general cubic distances. Let E be a subset of $\mathbb{F}_q^d$, $d\geq 2$, the d-dimensional vector space over the finite field $\mathbb{F}_q$. For each $x\in\mathbb{F}_q^d$ and a positive integer $n \geq 2$, we define $\|x\|_n = x_1^n + \cdots + x_d^n$. Let $\Delta_n(E,E) = \{\|x-y\|_n \colon x, y \in E\}$ viewed as a subset of $\mathbb{F}_q$. The Falconer distance problem in this context asks for the smallest number s_0 such that $\Delta_n(E,E)$ contains a positive proportion of the elements of $\mathbb{F}_q$ provided that $|E| \geq Cq^{s_0}$. Iosevich and Koh conjectured in [9] that if $|E| \geq Cq^{d/2}$ with C sufficiently large, then $|\Delta_n(E,E)| \gtrsim q$, which generalizes the conjecture originally stated in [13] for $n = 2$. However, it turned out that the conjecture is not true in the case when $n = 2$ and the dimension d is odd. In fact, arithmetic examples constructed by the authors in [8] show that the exponent $(d+1)/2$ is sharp. However, it has been believed that the conjecture may hold if the dimension d is even, in part because the extension theorem for spheres in even dimensions can be better than in odd dimensions for finite fields. The authors in [2] recently showed that if $E \subset \mathbb{F}_q^2$ of cardinality $\geq Cq^{4/3}$, with $C > 0$ large, then we have

$$|\Delta_2(E,E)| \gtrsim q. \tag{1.1}$$

When $d = 2$, the exponent $4/3$ not only matches the one obtained by Wolff in reals, but gives a better result than the exponent $(d+1)/2$ which gives a sharp exponent in odd dimensions. In this paper, we shall show that the general version also holds. Namely, we have the following main theorem for the Falconer distance problem in two dimension.

Theorem 1.3. *Let $E, F \subset \mathbb{F}_q^2$. If $|E||F| \gtrsim q^{\frac{8}{3}}$, then we have*

$$|\Delta(E,F)| := |\{\|x-y\|_2 \in \mathbb{F}_q : x \in E, y \in F\}| \gtrsim q.$$

Here, and throughout the paper, we define $\|x\|_2 = x_1^2 + x_2^2$.

In particular, our result in two dimension improves the Shparlinski's work in [19] which says that

$$|\Delta_2(E,F)| > \frac{|E||F|q}{q^{d+1} + |E||F|}.$$

Here, we recall that for positive numbers X and Y, the notation $X \lesssim Y$ means that there exists a constant $C > 0$ independent of the parameter q such that $X \leq CY$. For a complex number A and a non-negative real number B, the notation $A = O(B)$ is used if $|A| \leq CB$ for some $C > 0$ independent of the size of the underlying finite field $\mathbb{F}_q$.

Remark 1.4. The proof of Theorem 1.3 will be given in Section 4. To prove our main theorem, we mainly follow the methods which the authors in [2] used to obtain the result given in (1.1). However, our Lemma 4.1 which plays a crucial role in the proof was obtained by a new method and it can be also applied to a more general setting. We hope that our Lemmas 4.1 and 4.5 provide a clue to attack the generalized distance problems such as the cubic distance problem which was initially studied by the authors in [9].

Acknowledgment. The authors would like to thank the anonymous referee for useful comments and suggestions to improve this paper.

2. Notation and definitions for extension problems

We review some notation and definitions related to the extension problems in the finite field setting. We shall use the notation and definitions given in [10] or [11]. Let $\mathbb{F}_q$ be a finite field with q elements. We denote by $\mathbb{F}_q^d$ the d-dimensional vector space over the finite field $\mathbb{F}_q$. We shall work on the function space $(\mathbb{F}_q^d, dx)$, where a normalized counting measure dx is always endowed and our algebraic varieties shall be defined. Therefore, given a complex valued function $f : (\mathbb{F}_q^d, dx) \to \mathbb{C}$, the integral of the function f over the function space $(\mathbb{F}_q^d, dx)$ is given by

$$\int_{\mathbb{F}_q^d} f(x)\ dx = \frac{1}{q^d} \sum_{x\in\mathbb{F}_q^d} f(x).$$

We also define the frequency space $(\mathbb{F}_q^d, dm)$ as the dual space of the function space $(\mathbb{F}_q^d, dx)$, where we always endow the frequency space with the counting measure dm. For a fixed non-trivial additive character $\chi : \mathbb{F}_q \to \mathbb{C}$, we therefore define the Fourier transform of the function f on $(\mathbb{F}_q^d, dx)$ by the following formula:

$$\widehat{f}(m) = \int_{\mathbb{F}_q^d} \chi(-m\cdot x) f(x)\ dx = \frac{1}{q^d} \sum_{x\in\mathbb{F}_q^d} \chi(-m\cdot x) f(x), \tag{2.1}$$

where m is an element of the dual space $(\mathbb{F}_q^d, dm)$. Recall that the Fourier transform of the function f on $(\mathbb{F}_q^d, dx)$ is actually defined on the dual space $(\mathbb{F}_q^d, dm)$. Here we endow the dual space $(\mathbb{F}_q^d, dm)$ with a counting measure dm. We therefore see that the Fourier inversion theorem holds:

$$f(x) = \int_{m\in\mathbb{F}_q^d} \chi(m\cdot x)\widehat{f}(m)\ dm = \sum_{m\in\mathbb{F}_q^d} \chi(m\cdot x)\widehat{f}(m), \tag{2.2}$$

where f is the complex valued function defined on $(\mathbb{F}_q^d, dx)$. Using the orthogonality relation of the non-trivial additive character, meaning that $\sum_{x\in\mathbb{F}_q^d} \chi(m\cdot x) = 0$ for $m \neq (0,\dots,0)$, we also see that Plancherel theorem holds:

$$\|\widehat{f}\|_{L^2(\mathbb{F}_q^d, dm)} = \|f\|_{L^2(\mathbb{F}_q^d, dx)}.$$

In other words, the Plancherel theorem takes the following formula:

$$\sum_{m\in\mathbb{F}_q^d} |\widehat{f}(m)|^2 = \frac{1}{q^d} \sum_{x\in\mathbb{F}_q^d} |f(x)|^2. \tag{2.3}$$

Let f and h be the complex valued functions defined on the function space $(\mathbb{F}_q^d, dx)$. The convolution of f and g is defined on the function space $(\mathbb{F}_q^d, dx)$ by the formula

$$f * h(y) = \int_{x\in\mathbb{F}_q^d} f(y-x) g(x)\ dx = \frac{1}{q^d} \sum_{x\in\mathbb{F}_q^d} f(y-x)\ g(x).$$

Then, we can easily check that

$$\widehat{(f*h)}(m)=\widehat{f}(m)\cdot\widehat{h}(m).$$

Remark 2.1. Throughout the paper we always consider the variable "x" as an element of the function space $(\mathbb{F}_q^d, dx)$ with the normalized counting measure dx. On the other hand, we always use the variable "m" for the element of the frequency space $(\mathbb{F}_q^d, dm)$ with the counting measure dm.

2.1. Extension problems for general algebraic varieties in $\mathbb{F}_q^2$

We now introduce algebraic varieties $V\subset(\mathbb{F}_q^2, dx)$ on which we shall work. In addition, we review the definition of extension problems related to the variety V. Let $P(x)\in\mathbb{F}_q[x_1,x_2]$ be a polynomial with degree k. Throughout the paper we always assume that the degree of the polynomial $P(x)$ is less than the characteristic of the underlying finite field $\mathbb{F}_q$. We shall consider the following algebraic variety $V\subset(\mathbb{F}_q^2, dx)$ generated by the polynomial $P(x)\in\mathbb{F}_q[x_1,x_2]$:

$$V=\left\{x\in\mathbb{F}_q^2 : P(x)=0\right\}.$$

We endow the variety V with a normalized surface measure $d\sigma$ defined by the relation

$$\int_V f(x)\, d\sigma(x)=\frac{1}{|V|}\sum_{x\in V} f(x), \tag{2.4}$$

where $|V|$ denotes the number of elements in V. Note that the total mass of V is one and the measure σ is just a function on $(\mathbb{F}_q^2, dx)$ given by

$$d\sigma(x)=\frac{q^2}{|V|}V(x). \tag{2.5}$$

Here, and throughout the paper, we identify the set V with the characteristic function of the set V. For instance, we write $E(x)$ for $\chi_E(x)$ where E is a subset of the function space $(\mathbb{F}_q^2, dx)$. For $1\le p,r\le\infty$, we denote by $R^*(p\to r)$ the smallest constant such that the following extension estimate holds:

$$\|(fd\sigma)^\vee\|_{L^r(\mathbb{F}_q^2,dm)}\le R^*(p\to r)\|f\|_{L^p(V,d\sigma)} \tag{2.6}$$

for every function f defined on V in $(\mathbb{F}_q^2, dx)$, where the inverse Fourier transform of the measure $fd\sigma$ takes the form

$$(fd\sigma)^\vee(m)=\int_V \chi(m\cdot x)f(x)\, d\sigma(x)=\frac{1}{|V|}\sum_{x\in V}\chi(m\cdot x)f(x).$$

By duality, $R^*(p\to r)$ is also defined as the smallest constant such that the following restriction estimate holds:

$$\|\widehat{g}\|_{L^{p'}(V,d\sigma)}\le R^*(p\to r)\|g\|_{L^{r'}(\mathbb{F}_q^2,dm)} \tag{2.7}$$

for all functions g on $(\mathbb{F}_q^2, dm)$ where p' and r' denote the dual exponents of p and r respectively which mean $1/p + 1/p' = 1$ and $1/r + 1/r' = 1$. The constant $R^*(p \to r)$ may depend on q, the size of the underlying finite field $\mathbb{F}_q$. However, the extension problem asks us to determine the exponents $1 \le p, r \le \infty$ such that $R^*(p \to r) \lesssim 1$ where the constant under the notation $\lesssim$ is independent of q and it depends only on the degree of the variety V and on the ratio $|V|/q$.

Remark 2.2. Here, we need to be careful with the definition of $\widehat{g}$ in the restriction estimate (2.7). Since g is defined on $(\mathbb{F}_q, dm)$ with a counting measure "dm", the Fourier transform $\widehat{g}$ is actually defined on the dual space $(\mathbb{F}_q^2, dx)$ with the normalized counting measure. Thus, the Fourier transform of the function g takes the following form: for each $x \in (\mathbb{F}_q^2, dx)$,

$$\widehat{g}(x) = \int_{\mathbb{F}_q^d} \chi(-x \cdot m) g(m) dm = \sum_{m \in \mathbb{F}_q^2} \chi(-x \cdot m) g(m), \tag{2.8}$$

which is different from the definition of the Fourier transform in (2.1). Notice that the difference happened because the Fourier transform depends on its domain. Thus, when we compute the Fourier transform, we must carefully check its domain.

Remark 2.3. A direct calculation yields the trivial estimate, $R^*(1 \to \infty) \lesssim 1$. Using Hölder's inequality and the nesting properties of L^p-norms, we also see that

$$R^*(p_1 \to r) \le R^*(p_2 \to r) \quad \text{for} \;\; 1 \le p_2 \le p_1 \le \infty$$

and

$$R^*(p \to r_1) \le R^*(p \to r_2) \quad \text{for} \;\; 1 \le r_2 \le r_1 \le \infty.$$

For any fixed exponent $1 \le p\,(\text{or } r) \le \infty$, we therefore aim to find the smallest exponent $1 \le r\,(\text{or } p) \le \infty$ such that $R^*(p \to r) \lesssim 1$. By interpolating the result $R^*(p \to r) \lesssim 1$ with the trivial bound $R^*(1 \to \infty) \lesssim 1$, further results can be obtained.

2.2. Necessary conditions for $R^*(p \to r) \lesssim 1$

Mockenhaupt and Tao in [17] observed the necessary conditions for the boundedness of extension operators related to general algebraic varieties in d-dimensional vector spaces over finite fields. For example, if $V \subset (\mathbb{F}_q^2, dx)$ is an algebraic variety with $|V| \sim q^s$ for some $0 < s < 2$, then the necessary conditions for $R^*(p \to r) \lesssim 1$ take the following form:

$$r \ge \frac{4}{s} \quad \text{and} \quad r \ge \frac{2p}{s(p-1)}. \tag{2.9}$$

However, if V contains a α-dimensional affine subspace $H(|H| = q^\alpha)$, the necessary conditions in (2.9) can be improved by adding the condition

$$r \ge \frac{p(2-\alpha)}{(p-1)(s-\alpha)}. \tag{2.10}$$

For the proof of above necessary conditions, see pages 41–42 in [17].

Remark 2.4. Let $V = \{x \in \mathbb{F}_q^2 : P(x) = 0\}$ be an algebraic variety in $(\mathbb{F}_q^2, dx)$, where $P(x) \in \mathbb{F}_q[x_1, x_2]$ is a non-zero polynomial. Then it is clear that $|V| \lesssim q$, where the constant depends only on the degree of the polynomial $P(x)$ and the variety V can only contain zero or one dimensional affine subspaces. If V contains a one dimensional affine subspace H (a line) and $|V| \sim q$, then the necessary condition (2.10) says that there are no extension estimates except the trivial cases, $R^*(p \to \infty) \lesssim 1$ for $1 \le p \le \infty$. Thus, we are only interested in the case when our variety V does not contain any line. Namely, the polynomial $P(x)$ generating the variety V does not have any linear factor. In this case, if $|V| \sim q$, then the necessary conditions (2.9) exactly takes the following form:

$$r \ge 4 \quad \text{and} \quad r \ge \frac{2p}{p-1}.$$

In fact, the necessary condition, $r \ge 2p/(p-1)$, can be obtained by testing (2.6) with the function f supported in one point of V. If V contains a large subset H of a line, then this necessary condition must be improved by testing (2.6) with the characteristic function on H. However, Bezout's Theorem (see Theorem 3.1) says that the cardinality of H can not be more than the degree of $P(x)$, because otherwise V must contain the line. This observation leads us to the following conjecture.

Conjecture 2.5. *Given a non-zero polynomial $P(x) \in \mathbb{F}_q[x_1, x_2]$, define an algebraic variety V by*

$$V = \{x \in \mathbb{F}_q^2 : P(x) = 0\}.$$

If $|V| \sim q$ and the polynomial $P(x)$ does not have any linear factor, then the necessary conditions (2.9) *are in fact sufficient conditions for $R^*(p \to r) \lesssim 1$.*

In the case, when $V = \{x \in \mathbb{F}_q^2 : x_1^2 - x_2 = 0\}$ is the parabola, Mockenhaupt and Tao in [17] proved that Conjecture 2.5 holds. Iosevich and Koh in [10] also showed that Conjecture 2.5 is true if $V = \{x \in \mathbb{F}_q^2 : a_1x_1^2 + a_2x_2^2 = j\}$ with $a_1, a_2, j \ne 0$ is the nondegenerate quadratic curve. In fact, Theorem 1.1 shows that Conjecture 2.5 is true for arbitrary algebraic curves. To see this, notice from Remark 2.3 that if $|V| \sim q$, then $R^*(2 \to 4) \lesssim 1$ implies $R^*(p \to r) \lesssim 1$ for all exponents (p, r) satisfying the necessary conditions (2.9).

3. Proof of Theorem 1.1

In this section we shall restate and prove our main theorem for extension problems. The proof is based on the following Bezout's Theorem (see [4]), along with the method used to obtain the sharp extension estimates for the parabola in [17] and for nondegenerate quadratic curves in [10].

Theorem 3.1 (Bezout's Theorem). *Two algebraic curves of degrees K_1 and K_2 can not intersect in more than $K_1 \cdot K_2$ points unless they have a component in common.*

We also need Schwartz–Zippel Lemma (see [26] and [18]).

Lemma 3.2 (Schwartz–Zippel). *Let $P(x) \in \mathbb{F}_q[x_1, x_2]$ be a non zero polynomial with degree k. Then, we have*

$$\big|\{x \in \mathbb{F}_q^2 : P(x) = 0\}\big| \le kq.$$

Now, we restate our main theorem for extension problems and give a complete proof.

Theorem 1.1. *Suppose that $P(x) \in \mathbb{F}_q[x_1, x_2]$ is non-zero polynomial. Define an algebraic variety $V \subset \mathbb{F}_q^2$ by*

$$V = \{x \in \mathbb{F}_q^2 : P(x) = 0\}.$$

Then, $R^*(2 \to 4) \lesssim 1$ if and only if $|V| \sim q$ and the polynomial $P(x)$ does not have any linear factor.

Proof. ($\Longrightarrow$) Suppose that the L^2-L^4 extension estimate holds. By contradiction, assume that $|V|$ is not $\sim q$, or the polynomial $P(x)$ contains a linear factor. If $|V|$ is not $\sim q$, then the Schwartz–Zippel lemma says that $|V| \sim q^\varepsilon$ for some $0 \le \varepsilon < 1$. From the necessary condition (2.9), we therefore see that a L^2-L^4 extension estimate is impossible. On the other hand, if $P(x)$ has a linear factor, then the variety $V = \{x \in \mathbb{F}_q^2 : P(x) = 0\}$ contains a line. In this case, a L^2-L^4 extension estimate is also impossible, as an immediate result from the necessary condition (2.10).

($\Longleftarrow$) Suppose that $|V| \sim q$ and the polynomial $P(x)$ does not have any linear factor. First, we prove the following key lemma.

Lemma 3.3. *For each $j = 1, 2, \ldots, n$, let $P_j(x) \in \mathbb{F}_q[x_1, x_2]$ be an irreducible polynomial with degree ≥ 2. Then, given each variety $V_j := \{x \in \mathbb{F}_q^2 : P_j(x) = 0\}$, we can choose an element $a_j \in \mathbb{F}_q^2$ such that the following estimate holds:*

$$\sum_{x \in V_j} V_j(a - x) \lesssim 1 \quad \text{for all} \;\; a \in \mathbb{F}_q^2 \setminus \{a_j\},$$

where the constant in the estimate depends only on the degree of V_j.

Proof. Suppose that $P_j(x)$ is an irreducible polynomial with degree ≥ 2. Then, we aim to prove that there exists a point $a_j \in \mathbb{F}_q^2$ such that the total number of intersection points of the curve $P_j(x) = 0$ and the curve $P_j(a - x) = 0$ is $\lesssim 1$ for all $a \in \mathbb{F}_q^2 \setminus \{a_j\}$. We claim that it suffices to prove that two curves $P_j(x) = 0$ and $P_j(a - x) = 0$ are different for all $a \in \mathbb{F}_q^2 \setminus \{a_j\}$. To see this, assume that the curves $P_j(x) = 0$ and $P_j(a - x) = 0$ are different. Then, $P_j(x)$ and $P_j(a - x)$ can not have a common factor, because the polynomial $P_j(x)$ is irreducible. By Bezout's theorem, we therefore see that the total number of intersection points of two curves can not be greater than the product of the degree of $P_j(x)$ and the degree of $P_j(a - x)$. Thus, it remains to prove that two curves $P_j(x) = 0$ and $P_j(a - x) = 0$ are not same for all $a \in \mathbb{F}_q^2 \setminus \{a_j\}$. Since $P_j(x)$ is an irreducible polynomial with degree ≥ 2, it does not have a linear factor which means that the variety V_j does not contain any line. Without loss of generality, we may assume that there exists $a_j \in \mathbb{F}_q^2$ such that two curves $P_j(x) = 0$ and $P_j(a_j - x) = 0$ are same. Otherwise, there is nothing to prove. To complete the proof, it is enough to show that if $a \neq a_j$, then the curve $P_j(a-x) = 0$ is not same as the curve $P_j(a_j - x) = 0$. To see this, first note that for each $\alpha \in \mathbb{F}_q^2$, the graph of $P_j(\alpha - x) = 0$ can be obtained by reflecting the graph of $P_j(x) = 0$ about the origin and then translating the reflected graph by the vector α. Second, note that the curve given by reflecting the graph of $P_j(x) = 0$ about the origin does not contain any line, because the curve $P_j(x) = 0$ does not. Thus, two graphs obtained by shifting the reflected graph by two different vectors can not be same. This completes the proof. □

We now give the complete proof of Theorem 1.1. Suppose that $|V| \sim q$ and the polynomial $P(x)$ does not have any linear factor. Assume that the polynomial $P(x) \in \mathbb{F}_q[x_1, x_2]$ is completely factored as

$$P(x) = CP_1^{l_1}(x) \cdots P_j^{l_j}(x) \cdots P_n^{l_n}(x),$$

where, for each $j = 1, \dots, n$, $P_j(x)$ is an irreducible polynomial of degree ≥ 2. For each $j = 1, 2, \dots, n$, define the variety $V_j \subset \mathbb{F}_q^2$ as

$$V_j = \{x \in \mathbb{F}_q^2 : P_j(x) = 0\},$$

where $P_j(x)$ is an irreducible polynomial with degree at least two. Then, we see that our variety $V \subset \mathbb{F}_q^2$ is given by $V = \cup_{j=1}^n V_j$. In order to show that $R^*(2 \to 4) \lesssim 1$, we shall show that

$$\|(f d\sigma)^\vee\|^4_{L^4(\mathbb{F}_q^2, dm)} \lesssim \|f\|^4_{L^2(V, d\sigma)} \tag{3.1}$$

for all function f defined on the variety V. Notice from Bezout's Theorem that $|V_i \cap V_j| \sim 1$ for $i \neq j$. Thus, given a function f supported on V, we may write

$$f(x) \sim \sum_{j=1}^n f_j(x),$$

where $f_j(x) = f(x)V_j(x)$; recall that $V_j(x)$ denotes the characteristic function on the variety V_j. In order to prove the mapping property (3.1), it therefore suffices to show that for every $j = 1, \dots, n$,

$$\|(f_j d\sigma)^\vee\|^4_{L^4(\mathbb{F}_q^2, dm)} \lesssim \|f\|^4_{L^2(V, d\sigma)}, \tag{3.2}$$

for all function f defined on the variety V. Recall from (2.5) that the normalized measure $d\sigma$ on V is just a function given by

$$d\sigma(x) = \frac{q^2}{|V|} V(x).$$

For each $j = 1, \dots, n$, define a measure $d\sigma_j$ supported on V_j by

$$d\sigma_j(x) = \frac{q^2}{|V|} V_j(x). \tag{3.3}$$

Then, we see that $f_j d\sigma = f_j d\sigma_j$. From the definition of norms and the Plancherel theorem, we see that for each $j = 1, \dots, n$,

$$\begin{aligned}\|(f_j d\sigma)^\vee\|^4_{L^4(\mathbb{F}_q^2, dm)} &= \|(f_j d\sigma_j)^\vee\|^4_{L^4(\mathbb{F}_q^2, dm)} \\ &= \|[(f_j d\sigma_j)^\vee]^2\|^2_{L^2(\mathbb{F}_q^2, dm)} = \|f_j d\sigma_j * f_j d\sigma_j\|^2_{L^2(\mathbb{F}_q^2, dx)}.\end{aligned}$$

Choose the $a_j \in \mathbb{F}_q^2$ as in Lemma 3.3 and write

$$\begin{aligned}\|f_j d\sigma_j * f_j d\sigma_j\|^2_{L^2(\mathbb{F}_q^2, dx)} &= \frac{1}{q^2} |f_j d\sigma_j * f_j d\sigma_j(a_j)|^2 + \frac{1}{q^2} \sum_{x \in \mathbb{F}_q^2 \setminus \{a_j\}} |f_j d\sigma_j * f_j d\sigma_j(x)|^2 \\ &= \mathrm{I} + \mathrm{II},\end{aligned}$$

where we recall that "dx" is the normalized counting measure. Therefore, our task is to prove that both I and II are $\lesssim \|f\|^4_{L^2(V, d\sigma)}$. From (3.3) and Young's inequality, we observe that

$$\begin{aligned}|f_j d\sigma_j * f_j d\sigma_j(a_j)| \le \|f_j d\sigma_j * f_j d\sigma_j\|_{L^\infty(\mathbb{F}_q^2, dx)} &\le \frac{q^4}{|V|^2} \|f_j \cdot V_j\|^2_{L^2(\mathbb{F}_q^2, dx)} \\ &\le \frac{q^4}{|V|^2} \|f \cdot V\|^2_{L^2(\mathbb{F}_q^2, dx)} = \frac{q^2}{|V|} \|f\|^2_{L^2(V, d\sigma)}.\end{aligned}$$

Since $|V| \sim q$, this implies that $\mathrm{I} \lesssim \|f\|^4_{L^2(V, d\sigma)}$ as required. It remains to prove that $\mathrm{II} \lesssim \|f\|^4_{L^2(V, d\sigma)}$. Without loss of generality, we may assume that $f \ge 0$ and so $f_j \ge 0$. By the Cauchy–Schwarz inequality, we see that for every $x \in \mathbb{F}_q^2$,

$$(f_j d\sigma_j * f_j d\sigma_j)^2(x) \le (d\sigma_j * d\sigma_j)(x) \cdot (f_j^2 d\sigma_j * f_j^2 d\sigma_j)(x). \tag{3.4}$$

From (3.3) and the definition of the convolution of functions, observe that

$$d\sigma_j * d\sigma_j(x) = \frac{q^2}{|V|^2} \sum_{y \in V_j} V_j(x - y)$$

for each $x \in \mathbb{F}_q^2$. By Lemma 3.3, we therefore see that if $x \in \mathbb{F}_q^2 \setminus \{a_j\}$, then

$$d\sigma_j * d\sigma_j(x) \lesssim 1,$$

where we also used the fact that $|V| \sim q$. Putting this together with (3.4), we obtain that, for every $x \in \mathbb{F}_q^2 \setminus \{a_j\}$,

$$(f_j d\sigma_j * f_j d\sigma_j)^2(x) \lesssim (f_j^2 d\sigma_j * f_j^2 d\sigma_j)(x).$$

Thus, we conclude that

$$\begin{aligned}\mathrm{II} &= \frac{1}{q^2}\sum_{x\in\mathbb{F}_q^2\setminus\{a_j\}} |f_j d\sigma_j * f_j d\sigma_j(x)|^2 \lesssim \frac{1}{q^2}\sum_{x\in\mathbb{F}_q^2}(f_j^2 d\sigma_j * f_j^2 d\sigma_j)(x)\\ &= \frac{1}{|V|^2}\Bigg(\sum_{y\in\mathbb{F}_q^2} f_j^2(y)V_j(y)\Bigg)^2 \le \|f^2\|^2_{L^1(V,d\sigma)} = \|f\|^4_{L^2(V,d\sigma)}\end{aligned}$$

where the first equality in the second line follows immediately from Fubini's theorem. This completes the proof of Theorem 1.1. □

4. Distances between two sets

In this section, we shall prove Theorem 1.3 for the Falconer distance problem in two dimensions.

4.1. Key estimates for the proof of Theorem 1.3

The proof of Theorem 1.3 calls for lots of estimates which are related to discrete Fourier analysis. Here, we collect some useful lemmas needed to complete the proof of Theorem 1.3. Given $t \in \mathbb{F}_q$ and a polynomial $P(x) \in \mathbb{F}_q[x_1, x_2]$, define a variety V_t by

$$V_t = \{x \in \mathbb{F}_q^2 : P(x) = t\}. \tag{4.1}$$

Then, we have the following lemma:

Lemma 4.1. *If $P(x) = a_1x_1^d + a_2x_2^d \in \mathbb{F}_q[x_1, x_2]$ of degree $d \ge 2$, and $a_1, a_2 \in \mathbb{F}_q \setminus \{0\}$, then we have*

$$\sum_{t\in\mathbb{F}_q} \widehat{V_t}(m)|V_t| \lesssim 1 \quad \textit{for all} \;\; m \in \mathbb{F}_q^2 \setminus \{(0,0)\},$$

where $\widehat{V_t}$ is the Fourier transform of the characteristic function on the variety V_t defined by $\widehat{V_t}(m) = \frac{1}{q^2}\sum_{x\in\mathbb{F}_q^2}\chi(-x\cdot m)V_t(x)$.

Before we proceed to prove Lemma 4.1, we recall some well-known facts related to the polynomial $P(x) = a_1x_1^d + a_2x_2^d$. Lemma 1 in [3] says that the polynomial $P(x)-t$ is irreducible for any $t \in \mathbb{F}_q \setminus \{0\}$. From Theorem 6.37 in [15], we see that for every $t \in \mathbb{F}_q \setminus \{0\}$,

$$|V_t| = \big|\{x \in \mathbb{F}_q^2 : P(x) = t\}\big| = q + O(q^{\frac{1}{2}}). \tag{4.2}$$

We also recall a theorem by N. Katz ([14]).

Theorem 4.2. *Assume that a polynomial $\Lambda(x) \in \mathbb{F}_q[x_1, x_2]$ does not contain a linear factor. Then, for any $m \in \mathbb{F}_q^2 \setminus \{(0,0)\}$, we have that*

$$\Big|\sum_{x\in V} \chi(x\cdot m)\Big| \lesssim q^{\frac{1}{2}},$$

where $V = \{x \in \mathbb{F}_q^2 : \Lambda(x) = 0\}$.

Proof of Lemma 4.1. First, let us write $|V_t| = q + R_t$. From (4.2), we have that $R_t = O(q^{1/2})$ for $t \neq 0$. Moreover, it is clear from Schwartz–Zippel lemma that $R_0 = O(q)$. Using Theorem 4.2, we see that, for $t \neq 0$ and $m \neq (0,0)$,

$$\sum_{x\in\mathbb{F}_q^2 : P(x)=t} \chi(-x\cdot m) = O(q^{\frac{1}{2}}).$$

If $t = 0$, then we use Schwartz–Zippel lemma to bound

$$\sum_{x\in\mathbb{F}_q^2 : P(x)=0} \chi(-x\cdot m) = O(q).$$

Therefore, we obtain

$$\begin{aligned}\sum_{t\in\mathbb{F}_q} |V_t| \sum_{x\in\mathbb{F}_q^2 : P(x)=t} \chi(-x\cdot m) &= \\ = q\sum_{t\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_q^2 : P(x)=t} \chi(-x\cdot m) &+ \sum_{t\in\mathbb{F}_q} R_t \sum_{x\in\mathbb{F}_q^2 : P(x)=t} \chi(-x\cdot m).\end{aligned}$$

The first sum vanishes because $m \neq (0,0)$, and the second sum can be written as

$$\sum_{t\neq 0} R_t \sum_{x\in\mathbb{F}_q^2 : P(x)=t} \chi(-x\cdot m) + R_0 \sum_{x\in\mathbb{F}_q^2 : P(x)=0} \chi(-x\cdot m),$$

which is bounded by

$$O(qq^{1/2}q^{1/2} + qq) = O(q^2),$$

which in turn shows that

$$\sum_{t\in\mathbb{F}_q} \widehat{V}_t(m)|V_t| \lesssim 1.$$

□

In particular, we can take the polynomial $P(x)$ as $\|x\|_2 = x_1^2 + x_2^2$. In this case, the variety V_t in (4.1) is called a circle with radius $t \in \mathbb{F}_q$ and we can observe some specific properties on the circle V_t. For example, in [12] the Fourier transform on V_t is given by the formula

$$\widehat{V}_t(m) = q^{-2}\sum_{x\in\mathbb{F}_q^2} \chi(-m\cdot x)V_t(x) = q^{-1}\delta_0(m) + q^{-3}G_1^2 \sum_{s\in\mathbb{F}_q\setminus\{0\}} \chi\Big(\frac{\|m\|_2}{4s} + st\Big), \tag{4.3}$$

where $\delta_0(m) = 1$ if $m = (0,0)$ and $\delta_0(m) = 0$ if $m \neq (0,0)$, and we denote by G_1 the usual Gauss sum. It is known that the Gauss sum G_1 can be explicitly computed. If η is the quadratic character of $\mathbb{F}_q$ and χ is the canonical additive character of $\mathbb{F}_q$, then the Gauss sum $G_1 = \sum_{t\neq 0} \eta(t)\chi(t)$ takes the following value (see Theorem 5.15 in [15]):

$$G_1 = \begin{cases} (-1)^{k-1} q^{\frac{1}{2}} & \text{if} \quad p = 1 \ (mod\ 4), \\ (-1)^{k-1} i^k q^{\frac{1}{2}} & \text{if} \quad p = 3 \ (mod\ 4), \end{cases}$$

where k is a natural number and p is an odd prime with $q = p^k$. Thus, if $q = 1$ $(mod\ 4)$, then the square of the Gauss sum G_1 is exactly q. From this observation and (4.3), we see that if $q = 1\ (mod\ 4), m \in \mathbb{F}_q^2$, and $V_t = \{x \in \mathbb{F}_q^2 : \|x\|_2 = t\}$, then

$$\widehat{V_t}(m) = q^{-1}\delta_0(m) + q^{-2} \sum_{s\in\mathbb{F}_q\setminus\{0\}} \chi\left(\frac{\|m\|_2}{4s} + st\right). \tag{4.4}$$

However, observe that G_1^4 is always q^2, which yields the following lemma.

Lemma 4.3. *For each $t \in \mathbb{F}_q$, let $V_t = \{x \in \mathbb{F}_q^2 : \|x\|_2 = t\}$. For each $m, \xi \in \mathbb{F}_q^2 \setminus \{(0,0)\}$, we have*

$$\sum_{t\in\mathbb{F}_q} \widehat{V_t}(m)\widehat{V_t}(\xi) = q^{-3} \sum_{s\in\mathbb{F}_q\setminus\{0\}} \chi\left(s(\|m\|_2 - \|\xi\|_2)\right).$$

Proof. Since $m, \xi \neq (0,0)$ and $G_1^4 = q^2$, the estimate (4.3) implies that

$$\begin{aligned} \sum_{t\in\mathbb{F}_q} \widehat{V_t}(m)\widehat{V_t}(\xi) &= q^{-4} \sum_{s,s'\in\mathbb{F}_q\setminus\{0\}} \chi\left(\frac{\|m\|_2}{4s} + \frac{\|\xi\|_2}{4s'}\right) \sum_{t\in\mathbb{F}_q} \chi((s+s')t) \\ &= q^{-3} \sum_{s\in\mathbb{F}_q\setminus\{0\}} \chi\left(\frac{\|m\|_2}{4s} - \frac{\|\xi\|_2}{4s}\right), \end{aligned}$$

where the last line follows from the orthogonality relation of χ. Using a change of variables, $1/(4s) \to s$, we complete the proof. □

Let $E, F \subset \mathbb{F}_q^2$. We now consider the counting function $\nu : \mathbb{F}_q \to \mathbb{N} \cup \{0\}$, given by

$$\nu(t) = \left|\{(x,y) \in E \times F : \|x-y\|_2 = t\}\right|.$$

In particular, we have the following lemma.

Lemma 4.4. *Let $E, F \subset \mathbb{F}_q^2$. If $|E||F| \gtrsim q^2$ and $q = 1\ (mod\ 4)$, then we have*

$$\nu(0) = O(q^{-1}|E||F|) + q^3 \sum_{m\in V_0} \overline{\widehat{E}}(m)\,\widehat{F}(m),$$

where $V_0 = \{x \in \mathbb{F}_q^2 : \|x\|_2 = 0\}$.

Proof. It follows that

$$\nu(0)=\sum_{x,y\in\mathbb{F}_q^2}E(x)F(y)V_0(x-y).$$

Applying the Fourier inversion theorem (2.2) to $V_0(x-y)$ and using the definition of the Fourier transform, we have

$$\nu(0)=q^4\sum_{m\in\mathbb{F}_q^2}\overline{\widehat{E}}(m)\widehat{F}(m)\widehat{V_0}(m).$$

Since $q=1$ (*mod* 4), the formula (4.4) can be used to observe the following:

$$\begin{aligned}\nu(0)&=q^4\sum_{m\in\mathbb{F}_q^2}\overline{\widehat{E}}(m)\widehat{F}(m)\left(q^{-1}\delta_0(m)+q^{-2}\sum_{s\in\mathbb{F}_q\setminus\{0\}}\chi\left(\frac{\|m\|_2}{4s}\right)\right)\\&=q^3\overline{\widehat{E}}(0,0)\widehat{F}(0,0)+q^2\sum_{m\in\mathbb{F}_q^2}\overline{\widehat{E}}(m)\widehat{F}(m)\sum_{s\in\mathbb{F}_q\setminus\{0\}}\chi\left(\frac{\|m\|_2}{4s}\right).\end{aligned}$$

Computing the sum over $s\in\mathbb{F}_q\setminus\{0\}$, it follows that

$$\nu(0)=q^{-1}|E||F|+q^3\sum_{\|m\|_2=0}\overline{\widehat{E}}(m)\widehat{F}(m)-q^2\sum_{m\in\mathbb{F}_q^2}\overline{\widehat{E}}(m)\widehat{F}(m).$$

By the Cauchy–Schwarz inequality and the Plancherel theorem (2.3), the absolute value of the third term above is less than equal to $|E|^{\frac{1}{2}}|F|^{\frac{1}{2}}$. Since $|E||F|\gtrsim q^2$, the first term dominates the third term and the proof is complete. □

We now address the most important lemma for the proof of Theorem 1.3. The following lemma below may be hard to obtain if we use the direct computation, in part because we do not know the explicit form of the variety. Using the dual extension theorem, we can overcome the problem.

Lemma 4.5. *Let $\Gamma(x)\in\mathbb{F}_q[x_1,x_2]$ be a non-zero polynomial. For each $t\in\mathbb{F}_q$, let $V_t=\{x\in\mathbb{F}_q^2:\Gamma(x)=t\}$. Suppose that a set $T\subset\mathbb{F}_q$ satisfies the following conditions: if $t\in T$, then $|V_t|\sim q$ and $\Gamma(x)-t$ does not contain a linear factor. Then, we have that for every set $H\subset\mathbb{F}_q^2$,*

$$\max_{t\in T}\sum_{m\in V_t}|\widehat{H}(m)|^2\lesssim q^{-3}|H|^{\frac{3}{2}},\tag{4.5}$$

where we recall that $\widehat{H}(m)=q^{-2}\sum_{x\in H}\chi(-x\cdot m)$ and the constant in the estimate depends only on the degree of V_t and on the ratio $|V_t|/q$. In particular, if $\Gamma(x)=\|x\|_2=x_1^2+x_2^2$, then above conclusion holds with $T=\mathbb{F}_q\setminus\{0\}$.

Proof. For every $t\in T$, we must show that

$$q^{-4}\sum_{m\in V_t}\left|\sum_{x\in H}\chi(-x\cdot m)\right|^2\lesssim q^{-3}|H|^{\frac{3}{2}},$$

where the constant in "$\lesssim$" depends only on the degree of V_t and on the ratio $|V_t|/q$. Since the forms of variables m, x do not affect the above estimate, we can change the variables, $x \leftrightarrow m$. Thus, it suffices to show that

$$q^{-1} \sum_{x \in V_t} \left| \sum_{m \in H} \chi(-x \cdot m) \right|^2 \lesssim |H|^{\frac{3}{2}}. \tag{4.6}$$

From Theorem 1.1, we see that for every $t \in T$,

$$\|\widehat{fd\sigma}\|_{L^4(\mathbb{F}_q^2, dm)} \lesssim \|f\|_{L^2(V_t, d\sigma)}$$

for all functions f on $(V_t, d\sigma)$, where $d\sigma$ is the normalized measure on V_t defined as in (2.4). By duality (see (2.7)), this implies that

$$\|\widehat{g}\|_{L^2(V_t, d\sigma)} \lesssim \|g\|_{L^{\frac{4}{3}}(\mathbb{F}_q^2, dm)}$$

for all functions g on $(\mathbb{F}_q^2, dm)$. If we take g as the characteristic function on the set H, then we have

$$\|\widehat{H}\|^2_{L^2(V_t, d\sigma)} \lesssim \|H\|^2_{L^{\frac{4}{3}}(\mathbb{F}_q^2, dm)}.$$

To complete the proof, we shall show that this inequality is same as in (4.6). Namely, it suffices to prove that

$$\|H\|^2_{L^{\frac{4}{3}}(\mathbb{F}_q^2, dm)} = |H|^{\frac{3}{2}} \tag{4.7}$$

and

$$\|\widehat{H}\|^2_{L^2(V_t, d\sigma)} \sim q^{-1} \sum_{x \in V_t} \left| \sum_{m \in H} \chi(-x \cdot m) \right|^2. \tag{4.8}$$

The equality (4.7) is clear because "dm" is the counting measure. To see that (4.8) holds, observe from (2.4) that

$$\|\widehat{H}\|^2_{L^2(V_t, d\sigma)} = \frac{1}{|V_t|} \sum_{x \in V_t} |\widehat{H}(x)|^2.$$

From (2.8) observed in Remark 2.2, we see that the Fourier transform of H takes the following form:

$$\widehat{H}(x) = \sum_{m \in H} \chi(-x \cdot m).$$

□

Thus, the statement (4.8) follows immediately from the fact that $|V_t| \sim q$. Thus, the proof of (4.5) is complete. In particular, if $\Gamma(x) = x_1^2 + x_2^2$, then $\Gamma(x) - t$ for $t \neq 0$ is irreducible which implies that the polynomial $\Gamma(x) - t$ for $t \neq 0$ does not have a linear factor. Moreover, $|V_t| \sim q$ for $t \neq 0$. In this case, we can therefore take $T = \mathbb{F}_q \setminus \{0\}$.

4.2. Proof of Theorem 1.3

We shall provide the proof of Theorem 1.3. Let $E, F \subset \mathbb{F}_q^2$ with $|E||F| \gtrsim q^{\frac{8}{3}}$. For each $x \in \mathbb{F}_q^2$, recall that $\|x\|_2 = x_1^2 + x_2^2$. We must prove that

$$\big|\Delta(E,F)\big| = \big|\{\|x-y\|_2 \in \mathbb{F}_q : x \in E, y \in F\}\big| \gtrsim q. \tag{4.9}$$

For each $t \in \mathbb{F}_q$, define a variety $V_t = \{x \in \mathbb{F}_q^2 : \|x\|_2 = t\}$ and consider a counting function $\nu(t)$ given by

$$\nu(t) = \big|\{(x,y) \in E \times F : \|x-y\|_2 = t\}\big| = \sum_{x \in E, y \in F} V_t(x-y).$$

Applying the Fourier inversion theorem (2.2) to the function $V_t(x-y)$ and using the definition of the Fourier transform, we see that

$$\nu(t) = q^4 \sum_{m \in \mathbb{F}_q^2} \overline{\widehat{E}}(m)\widehat{F}(m)\widehat{V_t}(m) = \frac{|E||F||V_t|}{q^2} + q^4 \sum_{m \in \mathbb{F}_q^2 \setminus \{(0,0)\}} \overline{\widehat{E}}(m)\widehat{F}(m)\widehat{V_t}(m).$$

Squaring the $\nu(t)$ and summing over $t \in \mathbb{F}_q$, we obtain

$$\begin{aligned}\sum_{t \in \mathbb{F}_q} \nu^2(t) &= q^{-4}|E|^2|F|^2 \sum_{t \in \mathbb{F}_q} |V_t|^2 + 2q^2|E||F| \sum_{m \in \mathbb{F}_q^2 \setminus \{(0,0)\}} \overline{\widehat{E}}(m)\widehat{F}(m) \sum_{t \in \mathbb{F}_q} |V_t|\widehat{V_t}(m) \\ &\quad + q^8 \sum_{m,\xi \in \mathbb{F}_q^2 \setminus \{(0,0)\}} \overline{\widehat{E}}(m)\widehat{F}(m)\overline{\widehat{E}}(\xi)\widehat{F}(\xi) \sum_{t \in \mathbb{F}_q} \widehat{V_t}(m)\widehat{V_t}(\xi) = \mathrm{I} + \mathrm{II} + \mathrm{III}.\end{aligned}$$

The Schwartz–Zippel Lemma says that $|V_t| \lesssim q$ for all $t \in \mathbb{F}_q$. Therefore, the term I is clearly given by

$$|\mathrm{I}| = O(q^{-1}|E|^2|F|^2).$$

From Lemma 4.1 and Cauchy–Schwarz inequality, the second term can be estimated by

$$|\mathrm{II}| \lesssim q^2|E||F|\Big(\sum_{m \in \mathbb{F}_q^2} \big|\overline{\widehat{E}}(m)\big|^2\Big)^{\frac{1}{2}} \Big(\sum_{m \in \mathbb{F}_q^2} \big|\widehat{F}(m)\big|^2\Big)^{\frac{1}{2}}.$$

Applying Plancherel's theorem (2.3), we obtain

$$|\mathrm{II}| = O\big(|E|^{\frac{3}{2}}|F|^{\frac{3}{2}}\big).$$

Thus, if $|E||F| \gtrsim q^{\frac{8}{3}}$, the first term I dominates the second term II. It therefore follows that

$$|\mathrm{I}| + |\mathrm{II}| = O(q^{-1}|E|^2|F|^2). \tag{4.10}$$

We explicitly estimate the third term III. From Lemma 4.3 and the orthogonality relation of the character χ, we observe that

$$\begin{aligned}
\mathrm{III} &= q^8 \sum_{m,\xi\in\mathbb{F}_q^2\setminus\{(0,0)\}} \overline{\widehat{E}}(m)\widehat{F}(m)\overline{\widehat{E}}(\xi)\widehat{F}(\xi) \sum_{t\in\mathbb{F}_q} \widehat{V_t}(m)\widehat{V_t}(\xi)\\
&= q^5 \sum_{m,\xi\in\mathbb{F}_q^2\setminus\{(0,0)\}} \overline{\widehat{E}}(m)\widehat{F}(m)\overline{\widehat{E}}(\xi)\widehat{F}(\xi) \Big(-1 + \sum_{s\in\mathbb{F}_q} \chi\left(s(\|m\|_2 - \|\xi\|_2)\right)\Big)\\
&= -q^5 \sum_{m,\xi\in\mathbb{F}_q^2\setminus\{(0,0)\}} \overline{\widehat{E}}(m)\widehat{F}(m)\overline{\widehat{E}}(\xi)\widehat{F}(\xi) + q^6 \sum_{m,\xi\neq(0,0):\|m\|_2=\|\xi\|_2} \overline{\widehat{E}}(m)\widehat{F}(m)\overline{\widehat{E}}(\xi)\widehat{F}(\xi)\\
&= \mathrm{III}_1 + \mathrm{III}_2.
\end{aligned}$$

By the trivial bound and the Cauchy–Schwarz inequality, we have

$$|\mathrm{III}_1| \le q^5 \Big(\sum_{m\in\mathbb{F}_q^2} \Big|\overline{\widehat{E}}(m)\Big| \Big|\widehat{F}(m)\Big| \Big)^2 \le q^5 \Big(\sum_{m\in\mathbb{F}_q^2} \Big|\overline{\widehat{E}}(m)\Big|^2 \Big) \Big(\sum_{m\in\mathbb{F}_q^2} \Big|\widehat{F}(m)\Big|^2 \Big).$$

Applying Plancherel's theorem (2.3), the term III_1 is estimated by

$$|\mathrm{III}_1| = O(q|E||F|).$$

To estimate III_2, observe that

$$\begin{aligned}
\mathrm{III}_2 &= q^6 \sum_{k\in\mathbb{F}_q} \Big(\sum_{m\neq(0,0):\|m\|_2=k\}} \overline{\widehat{E}}(m)\widehat{F}(m) \Big)^2\\
&= q^6 \Big(\sum_{m\neq(0,0):\|m\|_2=0} \overline{\widehat{E}}(m)\widehat{F}(m) \Big)^2 + q^6 \sum_{k\in\mathbb{F}_q\setminus\{0\}} \Big(\sum_{\|m\|_2=k} \overline{\widehat{E}}(m)\widehat{F}(m) \Big)^2\\
&= q^6 \Big(\sum_{m\in V_0} \overline{\widehat{E}}(m)\widehat{F}(m) - \overline{\widehat{E}}(0,0)\widehat{F}(0,0) \Big)^2 + q^6 \sum_{k\in\mathbb{F}_q\setminus\{0\}} \Big(\sum_{m\in V_k} \overline{\widehat{E}}(m)\widehat{F}(m) \Big)^2.
\end{aligned}$$

Since $\overline{\widehat{E}}(0,0)\widehat{F}(0,0) = q^{-4}|E||F|$, expanding the first term above and putting it together with the second term, we have

$$\mathrm{III}_2 = q^6 \sum_{k\in\mathbb{F}_q} \Big(\sum_{m\in V_k} \overline{\widehat{E}}(m)\widehat{F}(m) \Big)^2 - 2q^2|E||F| \sum_{m\in V_0} \overline{\widehat{E}}(m)\widehat{F}(m) + q^{-2}|E|^2|F|^2.$$

Putting this estimate together with the estimate (4.10), we obtain

$$\begin{aligned}
\sum_{t\in\mathbb{F}_q} \nu^2(t) = q^6 \sum_{k\in\mathbb{F}_q} \Big(\sum_{m\in V_k} \overline{\widehat{E}}(m)\widehat{F}(m) \Big)^2 &- 2q^2|E||F| \sum_{m\in V_0} \overline{\widehat{E}}(m)\widehat{F}(m)\\
&+ O(q^{-1}|E|^2|F|^2).
\end{aligned}$$

Observe that the absolute value of the second term above is less than equal to the number

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

Using Cauchy–Schwarz inequality and Plancherel's theorem (2.3), this value is dominated by $2|E|^{\frac{3}{2}}|F|^{\frac{3}{2}}$. Since we have assumed that $|E||F|\gtrsim q^{\frac{8}{3}}$, the third term dominates the second term and so we obtain that

$$\sum_{t\in\mathbb{F}_q}\nu^2(t)=q^6\sum_{k\in\mathbb{F}_q}\Big(\sum_{m\in V_k}\overline{\widehat{E}}(m)\widehat{F}(m)\Big)^2+O(q^{-1}|E|^2|F|^2). \tag{4.11}$$

We are ready to prove that the statement (4.9) holds. First we assume that $q=3$ $(mod\ 4)$. In this case, -1 is not a square number in $\mathbb{F}_q$, because $\eta(-1)=-1$ where η is the quadratic character of $\mathbb{F}_q$ (see Remark 5.13 in [15]). Thus, we see that $V_0=\{x\in\mathbb{F}_q^2:\|x\|_2=0\}=\{(0,0)\}$. Therefore, we see that

$$\begin{aligned}\sum_{t\in\mathbb{F}_q}\nu^2(t)=q^6\left(\overline{\widehat{E}}(0,0)\widehat{F}(0,0)\right)^2+q^6\sum_{k\in\mathbb{F}_q\setminus\{0\}}\Big(\sum_{m\in V_k}\overline{\widehat{E}}(m)\widehat{F}(m)\Big)^2\\ +O(q^{-1}|E|^2|F|^2).\end{aligned} \tag{4.12}$$

Note that the first term is same as $q^{-2}|E|^2|F|^2$ which is dominated by the third term. In addition, observe that the absolute value of the second term is less than equal to the value

$$q^6\Big(\max_{k\in\mathbb{F}_q\setminus\{0\}}\Big|\sum_{m\in V_k}\overline{\widehat{E}}(m)\widehat{F}(m)\Big|\Big)\Big(\sum_{m\in\mathbb{F}_q^2}\Big|\overline{\widehat{E}}(m)\Big|\Big|\widehat{F}(m)\Big|\Big).$$

In order to get the upper bound of the maximum value, we use the Cauchy–Schwarz inequality and apply Lemma 4.5. Then, we see that

$$\Big(\max_{k\in\mathbb{F}_q\setminus\{0\}}\Big|\sum_{m\in V_k}\overline{\widehat{E}}(m)\widehat{F}(m)\Big|\Big)\lesssim q^{-3}|E|^{\frac{3}{4}}|F|^{\frac{3}{4}}.$$

On the other hand, using Cauchy–Schwarz inequality and Plancherel's theorem (2.3) yield that

$$\Big(\sum_{m\in\mathbb{F}_q^2}\Big|\overline{\widehat{E}}(m)\Big|\Big|\widehat{F}(m)\Big|\Big)\le q^{-2}|E|^{\frac{1}{2}}|F|^{\frac{1}{2}}.$$

Therefore, the second term in (4.12) can be estimated by

$$\Big|q^6\sum_{k\in\mathbb{F}_q\setminus\{0\}}\Big(\sum_{m\in V_k}\overline{\widehat{E}}(m)\widehat{F}(m)\Big)^2\Big|\lesssim q|E|^{\frac{5}{4}}|F|^{\frac{5}{4}}. \tag{4.13}$$

Putting together all the estimates, we see that

$$\sum_{t\in\mathbb{F}_q}\nu^2(t)\lesssim q|E|^{\frac{5}{4}}|F|^{\frac{5}{4}}+q^{-1}|E|^2|F|^2.$$

Since $|E||F| \gtrsim q^{\frac{8}{3}}$, it follows that

$$\sum_{t\in\mathbb{F}_q} \nu^2(t) \lesssim q^{-1}|E|^2|F|^2.$$

It is clear that

$$(|E||F|)^2 = \Bigg(\sum_{t\in\Delta(E,F)} \nu(t)\Bigg)^2 \le |\Delta(E,F)| \sum_{t\in\mathbb{F}_q} \nu^2(t),$$

where we used the Cauchy–Schwarz inequality. Thus, we have proved that if $q = 3$ (mod 4) and $|E||F| \gtrsim q^{\frac{8}{3}}$, then

$$|\Delta(E,F)| \gtrsim q.$$

It remains to prove that if $q = 1$ (mod 4) and $|E||F| \gtrsim q^{\frac{8}{3}}$, then the estimate (4.9) holds. Assume that $q = 1$ (mod 4). Since $|E||F| = \sum_{t\in\Delta(E,F)} \nu(t)$, it follows that

$$(|E||F| - \nu(0))^2 = \Bigg(\sum_{t\in\Delta(E,F)\setminus\{0\}} \nu(t)\Bigg)^2 \le |\Delta(E,F)| \sum_{t\in\mathbb{F}_q\setminus\{0\}} \nu^2(t). \tag{4.14}$$

From Lemma 4.4, recall that

$$\nu(0) = O(q^{-1}|E||F|) + q^3 \sum_{m\in V_0} \overline{\widehat{E}}(m)\widehat{F}(m). \tag{4.15}$$

Thus, using the estimate (4.11),

$$\begin{aligned}\sum_{t\in\mathbb{F}_q\setminus\{0\}} \nu^2(t) &= \sum_{t\in\mathbb{F}_q} \nu^2(t) - \nu^2(0)\\ &= q^6 \sum_{k\in\mathbb{F}_q\setminus\{0\}} \Bigg(\sum_{m\in V_k} \overline{\widehat{E}}(m)\widehat{F}(m)\Bigg)^2 + O(q^2|E||F|)\Bigg(\sum_{m\in V_0} \overline{\widehat{E}}(m)\widehat{F}(m)\Bigg)\\ &\quad + O(q^{-1}|E|^2|F|^2)\end{aligned}$$

As in (4.13), the absolute value of the first term is $\lesssim q|E|^{\frac{5}{4}}|F|^{\frac{5}{4}}$, which is dominated by the third term, because we have assumed that $|E||F| \gtrsim q^{\frac{8}{3}}$. To estimate the absolute value of the second term, notice that

$$\Bigg|\sum_{m\in V_0} \overline{\widehat{E}}(m)\widehat{F}(m)\Bigg| \le \sum_{m\in\mathbb{F}_q^2} \Big|\overline{\widehat{E}}(m)\Big|\,\Big|\widehat{F}(m)\Big| \le q^{-2}|E|^{\frac{1}{2}}|F|^{\frac{1}{2}}, \tag{4.16}$$

where the last inequality can be obtained using the Cauchy–Schwarz inequality and Plancherel's theorem (2.3). Thus, the absolute value of the second term is $\lesssim |E|^{\frac{3}{2}}|F|^{\frac{3}{2}}$, which is also dominated by the third term if $|E||F| \gtrsim q^{\frac{8}{3}}$. Thus, we obtain that

$$\sum_{t\in\mathbb{F}_q\setminus\{0\}} \nu^2(t) \lesssim q^{-1}|E|^2|F|^2. \tag{4.17}$$

Next, we claim that

$$(|E||F| - \nu(0))^2 \sim |E|^2|F|^2. \tag{4.18}$$

To see this, observe from (4.15) and (4.16) that

$$|\nu(0)| \lesssim q^{-1}|E||F| + q|E|^{\frac{1}{2}}|F|^{\frac{1}{2}} \sim q|E|^{\frac{1}{2}}|F|^{\frac{1}{2}},$$

where the last estimate is clear because $|E||F| \leq q^4$. Since $|E||F| \gtrsim q^{\frac{8}{3}}$, it therefore is clear that $|E||F|$ dominates $|\nu(0)|$ and the estimate (4.18) holds. Finally, from (4.14), (4.17), and (4.18), we conclude that if $q = 1$ $(mod\ 4)$ and $|E||F| \gtrsim q^{\frac{8}{3}}$, then

$$|\Delta(E,F)| \gtrsim q.$$

This completes the proof of Theorem 1.3.

References

[1] Barceló, B.: On the restriction of the Fourier transform to a conical surface. *Trans. Amer. Math. Soc.* **292** (1985), no. 1, 321–333.

[2] Chapman, J., Erdoğan, M., Hart, D., Iosevich, A. and Koh, D.: Pinned distance sets, Wolff's exponent in finite fields and sum-product estimates. *Math. Z.*, published online, March 22 (2011).

[3] Cochrane, T.: Bounds on complete exponential sums. In *Analytic number theory, Vol. 1 (Allerton Park, IL, 1995),* 211–224. Prog. Math. 138, Birkhäuser-Boston, Boston, MA, 1996.

[4] Coolidge, J.: *A treatise on algebraic plane curves.* Dover Publications, New York, 1959.

[5] DeCarli, L. and Iosevich, A.: A restriction theorem for flat manifolds of codimension two. *Illinois J. Math.* **39** (1995), no. 4, 576–585.

[6] Erdoğan, M.: A bilinear Fourier extension theorem and applications to the distance set problem. *Int. Math. Res. Not.* **2005**, no. 23, 1411–1425.

[7] Falconer, K.: On the Hausdorff dimension of distance sets. *Mathematika* **32** (1985), no. 2, 206–212.

[8] Hart, D., Iosevich, A., Koh, D. and Rudnev, M.: 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.

[9] Iosevich, A. and Koh, D.: The Erdös–Falconer distance problem, exponential sums, and Fourier analytic approach to incidence theorems in vector spaces over finite fields. *SIAM J. Discrete Math.* **23** (2008/09), no. 1, 123–135.

[10] Iosevich, A. and Koh, D.: Extension theorems for the Fourier transform associated with nondegenerate quadratic surfaces in vector spaces over finite fields. *Illinois J. Math.* **52** (2008), no. 2, 611–628.

[11] Iosevich, A. and Koh, D.: Extension theorems for paraboloids in the finite field setting. *Math. Z.* **266** (2010), no. 2, 471–487.

[12] Iosevich, A. and Koh, D.: Extension theorems for spheres in the finite field setting. *Forum Math.* **22** (2010), no. 3, 457–483.

[13] Iosevich, A. and Rudnev, M.: Erdös distance problem in vector spaces over finite fields. *Trans. Amer. Math. Soc.* **359** (2007), no. 12, 6127–6142.

[14] Katz, N.: *Sommes exponentielles.* Astérisque 79, Société Mathématique de France, Paris, 1980.

[15] Lidl, R. and Niederreiter, H.: *Finite fields.* Encyclopedia of Mathematics and its Applications 20, Cambridge University Press, Cambridge, 1997.

[16] Mattila, P.: Spherical averages of Fourier transforms of measures with finite energy; dimension of intersections and distance sets. *Mathematika* **34** (1987), no. 2, 207–228.

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

[18] Schwartz, J.: Fast probabilistic algorithms for verification of polynomial identities. *J. Assoc. Comput. Mach.* **27** (1980), no. 4, 701–717.

[19] Shparlinski, I.: On the set of distance between two sets over finite fields. *Int. J. Math. Math. Sci.* (2006), Art. ID 59482, 1–5.

[20] Stein, E. M.: Some problems in harmonic analysis. In *Harmonic analysis in Euclidean spaces (Proc. Sympos. Pure Math., Williamstown, Mass., 1978), Part 1*, 3–20. Proc. Sympos. Pure Math., XXXV, Amer. Math. Soc., Providence, RI, 1979.

[21] Stein, E. M.: *Harmonic analysis: real-variable methods, orthogonality, and oscillatory integrals.* Princeton Mathematical Series 43, Monographs in Harmonic Analysis III, Princeton University Press, Princeton, NJ, 1993.

[22] Tao, T.: A sharp bilinear restriction estimate for paraboloids. *Geom. Funct. Anal.* **13** (2003), no. 6, 1359–1384.

[23] Tao, T.: Some recent progress on the restriction conjecture. In *Fourier analysis and convexity*, 217–243. Appl. Numer. Harmon. Anal., Birkhäuser, Boston, MA, 2004.

[24] Wolff, T.: Decay of circular means of Fourier transforms of measures. *Internat. Math. Res. Notices* **1999**, no. 10, 547–567.

[25] Wolff, T.: A sharp bilinear cone restriction estimate. *Ann. of Math. (2)* **153** (2001), no. 3, 661–698.

[26] Zippel, R.: Probabilistic algorithms for sparse polynomials. In *Symbolic and algebraic computation (EUROSAM'79, Internat. Sympos., Marseille, 1979)*, 216–226. Lecture Notes in Comput. Sci. 72, Springer, Berlin-New York, 1979.

[27] Zygmund, A.: On Fourier coefficients and transforms of functions of two variables. *Studia Math.* **50** (1974), 189–201.

Received April 3, 2010; revised November, 28, 2010.

Doowon Koh: Department of Mathematics, Chungbuk National University, Cheongju city, Chungbuk-Do 361-736, Korea.
E-mail: `koh131@chungbuk.ac.kr`

Chun-Yen Shen: Department of Mathematics and Statistics, McMaster University, Hamilton L8S 4K1, Canada.
E-mail: `shenc@umail.iu.edu`