Cubic varieties, Erdös-Falconer distance problem, and application of Fourier analysis to a class of Szemeredi-Trotter type incidence theorems in vector spaces over finite fields

Alex Iosevich and Doowon Koh

April 11, 2006

Abstract

We study the Erdos/Falconer distance problem in vector spaces over finite fields with respect to the cubic metric. Estimates for discrete Airy sums and Adolphson/Sperber estimates for exponential sums in terms of Newton polyhedra play a crucial role. Similar techniques are used to study the incidence problem between points and cubic and quadratic curves. As a result we obtain a non-trivial range of exponents that appear to be difficult to attain using combinatorial methods.

Contents

1 Introduction **2**
1.1 The Erdös distance problem 2

2 Previous results **3**

3 Main results of this paper **4**
3.1 Distances determined by a single set 4
3.2 Szemeredi-Trotter type Incidence theorems and distances between pairs of sets 5

4 Fourier analytic preliminaries and notation **6**

5 Proof of Theorem 3.1 **6**

6 Proof of Theorem 5.1 **8**

7 Proof of Theorem 3.4 and Corollary 3.6 **11**

1 Introduction

1.1 The Erdös distance problem

The Erdos distance conjecture in the Euclidean space says that if E is a finite subset of $\mathbb{R}^d$, $d \geq 2$, then

$$\#\Delta(E) \gtrapprox (\#E)^{\frac{2}{d}}, \tag{1.1}$$

where

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

with $|x-y|^2 = (x_1-y_1)^2 + \cdots + (x_d-y_d)^2$ and here, and throughout the paper, $X \lesssim Y$ means that there exists $C > 0$ such that $X \leq CY$, and $X \lessapprox Y$, with the controlling parameter N, means that for every $\epsilon > 0$ there exists $C_\epsilon > 0$ such that $X \leq C_\epsilon N^\epsilon Y$.

Taking $E = \mathbb{Z}^d \cap [0, N^{\frac{1}{d}}]^d$ shows that (1.1) cannot in general be improved. The conjecture has not been solved in any dimension. See, for example, [12]), [1], and the references contained therein for the description of the conjecture, background material, and a survey of recent results.

In this paper we study the Erdös distance problem in vector spaces over finite fields. This problem was recently addressed by Tao ([17]) who relates it to some interesting questions in combinatorics, and, more recently, by Iosevich and Rudnev. We shall describe these results later in the introduction.

Let $\mathbb{F}_q$ denote the finite field with q elements, q prime, and let $\mathbb{F}_q^d$ denote the d-dimensional vector space over this field. While our methods work in more general settings we shall operate in this format for the moment for the sake of clarity. Let $E \subset \mathbb{F}_q^d$, $d \geq 2$. Then the analog of the classical Erdös distance problem is to determine the smallest possible cardinality of the set

$$\Delta_l(E) = \{||x-y|| = (x_1-y_1)^l + \cdots + (x_d-y_d)^l : x, y \in E\},$$

with l a positive integer ≥ 2, viewed as a subset of $\mathbb{F}_q$.

In the finite field setting, the estimate (1.1) cannot hold without further restrictions. To see this, let $E = \mathbb{F}_q^d$. Then $\#E = q^d$ and $\#\Delta(E) = q$. Furthermore, an interesting feature of the Erdös distance problem in the finite field setting with $l = 2$ is the existence of non-trivial spheres of 0 radius. These are sets of the form $\{x \in \mathbb{F}_q^d : x_1^2 + x_2^2 + \cdots + x_d^2 = 0\}$ and several assumptions in the statements of results below are there precisely to deal with issues created by the presence of this object. For example, suppose -1 is a square in $\mathbb{F}_q$. Using spheres of radius 0 one can show, in even dimensions, that there exists a set of cardinality precisely $q^{\frac{d}{2}}$ such that all the distances, $(x_1-y_1)^2 + \cdots + (x_d-y_d)^2$ are 0. What's more, suppose $\mathbb{F}_q$ is a finite field, such that $q = p^2$, where p is a prime. Then

$E = \mathbb{F}_p^d$ is naturally embedded in $\mathbb{F}_q^d$, has cardinality $q^{\frac{d}{2}}$, and determines only $\sqrt{q}$ distances. If $l > 2$, the situation is equally fascinating. For example, if $l = 3$ and $d = 2$, the equation $x_1^3 + x_2^3 = 0$ always has at least q solutions, since cube root of -1 is -1. This equation may have as many as $3q$ solutions if the primitive cube root of -1 is in the field.

With these examples as guide, we generalize the conjecture originally stated in ([9]) in the case $l = 2$ as follows.

Conjecture 1.1. *Let $E \subset \mathbb{F}_q^d$ of cardinality $\geq Cq^{\frac{d}{2}}$, with C sufficiently large. Then*

$$\#\Delta_l(E) \gtrapprox q.$$

The authors conjecture in [9] that the constant C that appears above may be taken to be one in the case $l = 2$. It is interesting to note that if $l > 2$, the situation becomes more complicated. For example, as we pointed out above, if $l = 3$ and $d = 2$, the number of points on the curve $x_1^3 + x_2^3 = 0$ may be as high as $3q$, depending on whether or not the primitive cube root of -1 is in the field. Thus a corresponding conjecture in the case $l > 2$ must be designed with these issues in mind.

2 Previous results

A Euclidean plane argument due to Erdös ([5]) can be applied to the finite field set-up under the assumption of Conjecture 1.1 to show that if $d = 2$ and $\#E \geq Cq$, with C sufficiently large, then

$$\#\Delta_l(E) \gtrsim (\#E)^{\frac{1}{2}}. \tag{2.1}$$

This result was improved by Bourgain, Katz and Tao ([3]) who showed using intricate incidence geometry that for every $\epsilon > 0$, there exists $\delta > 0$, such that if $\#E \lesssim q^{2-\epsilon}$, then

$$\#\Delta_2(E) \gtrsim q^{\frac{1}{2}+\delta}.$$

The relationship between ϵ and δ in the above argument is difficult to determine. Moreover, matters are even more subtle in higher dimensions the context of vector spaces over finite fields because intersection of analogs of spheres, both quadratic and cubic, in $\mathbb{F}_q^d$ may be quite complicated, and the standard induction on the dimension argument in $\mathbb{R}^d$ (see e.g. [1]) that allows one to bootstrap the estimate (2.1) into the estimate

$$\#\Delta_{\mathbb{R}^d}(E) \gtrsim (\#E)^{\frac{1}{d}} \tag{2.2}$$

does not immediately go through. We establish the finite field analog of the estimate (2.2) below using Fourier analytic methods and number theoretic properties of Kloosterman sums and its more general analogs.

Another way of thinking of Conjecture 1.1 is in terms of the Falconer distance conjecture ([6]) in the Euclidean setting which says that if the Hausdorff dimension of a set in $\mathbb{R}^d$ exceeds $\frac{d}{2}$, then the Lebesgue measure of the distance set is positive. Conjecture 1.1 implies that if the size of the set is greater than $q^{\frac{d}{2}}$, then the distance set contains a positive proportion of all the possible distances, an analogous statement.

In ([9]) the authors proved the following result.

Theorem 2.1. *Let $E \subset \mathbb{F}_q^d$, $d \geq 2$, such that $\#E \geq Cq^{\frac{d+1}{2}}$. Then if C is sufficiently large, $\Delta_2(E)$ contains every element of $\mathbb{F}_q$.*

3 Main results of this paper

3.1 Distances determined by a single set

Our first result is the version of Theorem 2.1 for cubic metrics.

Theorem 3.1. *Suppose that q is a prime number congruent to 1 modulo 3. Let $E \subset \mathbb{F}_q^d$, such that $\#E \gtrsim Cq^{\frac{d+1}{2}}$. Then if C is sufficiently large, $\Delta_3(E)$ contains every element of $\mathbb{F}_q$.*

Corollary 3.2. *Suppose that q is a prime number congruent to 1 modulo 3. Let $E \subset \mathbb{F}_q^d$, $d \geq 2$, such that $\#E = Cq^{\frac{d+1}{2}}$. Then if C is sufficiently large,*

$$\#\Delta_3(E) \approx (\#E)^{\frac{2}{d+1}}.$$

Note that in the case $d = 2$, the exponent $\frac{2}{3}$ obtained via the corollary, for the given range of parameters, is a much better exponent than the one obtained by the incidence argument due to Erdos described in (2.1) above. Also, we point out once more that Erdos' argument does not generalize to higher dimensions, at least not very easily, due to the possibly complicated intersection properties of cubic varieties.

3.2 Szemeredi-Trotter type Incidence theorems and distances between pairs of sets

As in the case $l = 2$, the proof of Theorem 3.1 can be modified to yield a good upper bound on the number of incidences between points and cubic surfaces in vector spaces over finite fields. It is an analog, and a higher dimensional generalization, of the following classical result due to Szemeredi and Trotter.

Theorem 3.3. *The number of incidences between N points and M lines (or circles of the same radius) in the plane is*

$$\lesssim N + M + (NM)^{\frac{2}{3}}.$$

Our incident estimate is the following.

Theorem 3.4. *Let $E, F \subset \mathbb{F}_q^d$, $d \geq 2$. Then if $j \neq 0$,*

$$\#\{(x,y) \in E \times F : (x_1 - y_1)^3 + \cdots + (x_d - y_d)^3 = j\}$$

$$\lesssim \#E \cdot \#F \cdot q^{-1} + q^{\frac{d-1}{2}} \cdot (\#E)^{\frac{1}{2}} \cdot (\#F)^{\frac{1}{2}}.$$

Similarly,

$$\#\{(x,y) \in E \times F : (x_1 - y_1)^2 + \cdots + (x_d - y_d)^2 = j\}$$
$$\lesssim \#E \cdot \#F \cdot q^{-1} + q^{\frac{d-1}{2}} \cdot (\#E)^{\frac{1}{2}} \cdot (\#F)^{\frac{1}{2}}.$$

Remark 3.5. In particular, that if $\#E \approx \#F \approx q^{\frac{d+1}{2}}$, then the number of incidences between points in E and "spheres", quadratic or cubic, centered at elements of F is $\lesssim q^d$.

To make the numerology more transparent, Theorem 3.4 says that if $N \approx q^{\frac{d+1}{2}}$, the number of incidences between $\approx N$ points and $\approx N$ spheres, cubic or quadratic, in $\mathbb{F}_q^d$ is $\lesssim q^d = N^{\frac{2d}{d+1}}$. In two dimensions this says that the number of incidences between N points and N circles is $\lesssim N^{\frac{4}{3}}$, provided that $N \approx q^{\frac{d+1}{2}}$, matching in this setting the exponent in the following celebrated result due to Szemeredi and Trotter in the Euclidean plane.

An easy modification of the method used to prove Theorem 3.4 above yields the following distance set result.

Corollary 3.6. *Let $E, F \subset \mathbb{F}_q^d$, $d \geq 2$. Suppose that $\#E \cdot \#F \geq Cq^{d+1}$. Let $\Delta_3(E,F) = \{||x-y|| : x \in E, y \in F\}$. Then if C is sufficiently large, then $\Delta_3(E,F)$ contains every element of $\mathbb{F}_q$.*

An analogous version of this result was independently obtained by Shparlinski in [15].

4 Fourier analytic preliminaries and notation

Let $\mathbb{F}_q$ be a finite field with q elements, where q is a prime number. Let

$$\chi(t) = e^{\frac{2\pi i}{q}t}.$$

Given a complex valued function f on $\mathbb{F}_q^d$, define the Fourier transform of f by the equation

$$\widehat{f}(m) = q^{-d} \sum_{x \in \mathbb{F}_q^d} \chi(-x \cdot m) f(x) dx.$$

And, perhaps the most important identity in mathematics :) is the following. Let f be as above. Then

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

5 Proof of Theorem 3.1

Let $\chi(s) = e^{\frac{2\pi i}{q}s}$. Let S_j denote the characteristic function of the cubic "sphere"

$$\{x \in \mathbb{F}_q^d : ||x|| = j\},$$

where, as above,

$$||x|| = x_1^3 + \cdots + x_d^3.$$

The key estimate of the paper is the following.

Theorem 5.1. *Let $||x|| = x_1^3 + \cdots + x_d^3$. Suppose that q is a prime number congruent to 1 modulo 3 and $j \neq 0$. Then if $m \neq (0, \ldots, 0)$, then*

$$\left|\widehat{S}_j(m)\right| = \left| q^{-d} \sum_{\{x \in \mathbb{F}_q^d : ||x|| = j\}} \chi(x \cdot m) \right| \lesssim q^{-\frac{d+1}{2}},$$

and if $m = (0, \ldots, 0)$, then

$$\begin{aligned} \widehat{S}_j(m) &= q^{-1} + O(q^{-\frac{d+1}{2}}) \\ &\approx O(q^{-1}). \end{aligned}$$

With Theorem 5.1 in tow,

$$\#\{(x,y)\in E\times E: ||x-y||=j\}$$
$$=\sum_{x,y} E(x)E(y)S_j(x-y)$$
$$=q^{2d}\sum_m |\widehat{E}(m)|^2 \widehat{S}_j(m) = I + II,$$

where

$$I = q^{2d}|\widehat{E}(0,\dots,0)|^2 \widehat{S}_j(0,\dots,0),$$

and

$$II = q^{2d}\sum_{m\neq(0,\dots,0)} |\widehat{E}(m)|^2 \widehat{S}_j(m).$$

Now,

$$I = q^{2d}q^{-2d}(\#E)^2\cdot q^{-d}\#S_j,$$

whereas using Theorem 5.1,

$$II \lesssim q^{2d}q^{-\frac{d+1}{2}}\sum_{m\neq(0,0)} |\widehat{E}(m)|^2$$
$$\lesssim q^{2d}q^{-\frac{d+1}{2}}q^{-2}\sum_{x\in\mathbb{F}_q^2} E^2(x)$$
$$= q^{\frac{d-1}{2}}\cdot\#E.$$

We need the following estimate on S_j.

Corollary 5.2. *Let S_j be defined as above. Suppose that $j\neq 0$. Then*

$$\#S_j \approx q^{d-1}.$$

Corollary 5.2 is an immediate consequence of Theorem 5.1.

Using Lemma 5.2 we see that

$$\#\{(x,y)\in E\times E: ||x-y||=j\} = I + II,$$

where

$$I \gtrsim (\#E)^2 q^{-1},$$

and

$$II \lesssim \#E\cdot q^{\frac{d-1}{2}}.$$

We conclude that if $\#E \geq Cq^{\frac{d+1}{2}}$, with C sufficiently large, then

$$\#\{(x,y) \in E \times E : ||x-y|| = j\} > 0$$

for each $j \neq 0$. This completes the proof of Theorem 3.1.

6 Proof of Theorem 5.1

We have

$$\widehat{S}_j(m) = q^{-d} \sum_{\{x \in \mathbb{F}_q^2 : ||x|| = j\}} \chi(x \cdot m)$$

$$= q^{-1}\delta(m) + q^{-d-1} \sum_x \sum_{t \in \mathbb{F}_q^*} \chi(t(||x|| - j))\chi(x \cdot m),$$

where $\delta(m) = 1$ if $m = (0, \dots, 0)$ and 0 otherwise.

Lemma 6.1. *Let χ be a nontrivial additive character of F_q with $q \equiv 1 \mod (3)$. Suppose that $m = (m_1, \cdots, m_l) \in (\mathbb{F}_q^*)^l$. Then for any multiplicative character ψ of F_q of order 3 and $t \neq 0$, we have*

$$\prod_{j=1}^{l} \sum_{s_j \in F_q} \chi(s_j m_j + s_j^3 t)$$

$$= \psi^{-l}(t) \sum_{s_1, \cdots, s_l \in F_q^*} \chi(s_1 + \cdots + s_l - m_1^3 t^{-1} s_1^{-1} - \cdots - m_l^3 t^{-1} s_l^{-1}) \psi(s_1) \cdots \psi(s_l).$$

We shall also need the following result due to Duke and Iwaniec ([4]).

Theorem 6.2. *Suppose that $q \equiv 1 \mod (3)$ and let ψ be a multiplicative character of order three. Then*

$$\sum_{s \in \mathbb{F}_q} \chi(as^3 + s) = \sum_{s \in \mathbb{F}_q^*} \psi(sa^{-1})\chi(s - (3^3 as)^{-1}),$$

for any $a \in \mathbb{F}_q^*$.

It follows that

$$\sum_{s \in \mathbb{F}_q} \chi(sm_j + s^3 t) = \sum_{s \in \mathbb{F}_q} \chi(s + s^3 t m_j^{-3})$$

$$= \sum_{s \in \mathbb{F}_q^*} \psi(st^{-1})\chi(s - m_j^3 t^{-1} 3^{-3} s^{-1}).$$

since ψ is a multiplicative character of F_q of order three and $m_j \neq 0$. Absorbing 3^3 into m_j to make the notations simple, we complete the proof of Lemma 6.1.

Lemma 6.3. *Let χ be a nontrivial additive character of F_q with $q \equiv 1 \mod (3)$. Then for any multiplicative character ψ of F_q of order 3 and $t \neq 0$, we have*

$$\Big(\sum_{s\in F_q} \chi(ts^3)\Big)^l = \sum_{r=0}^{l} \left(\begin{array}{c} l \\ r \end{array}\right) q^l\, \psi^{-(l+r)}(t)\Big(\widehat{\psi}(-1)\Big)^{l-r} \Big(\widehat{\psi^2}(-1)\Big)^r,$$

where $\left(\begin{array}{c} \cdot \\ \cdot \end{array}\right)$ is a binomial coefficient and l is a positive integer.

To prove this, we need the following theorem. For the proof, see the ([19], page 217, Thm 5.30.).

Theorem 6.4. *Let χ be a nontrivial additive character of F_q, $n \in \mathbb{N}$, and ψ a multiplicative character of F_q of order $h =$gcd$(n, q-1)$. Then*

$$\sum_{s\in F_q} \chi(ts^n + b) = \chi(b) \sum_{k=1}^{h-1} \psi^{-k}(t)\, G(\psi^k, \chi)$$

for any $t, b \in F_q$ with $t \neq 0$, where $G(\psi^k, \chi) = \sum_{s\in F_q^*} \psi^k(s)\chi(s)$.

By using Theorem (6.4), we see that for any multiplicative character ψ of order three,

$$\begin{aligned} &\Big(\sum_{s\in F_q} \chi(ts^3)\Big)^l \\ &= \Big(\sum_{k=1}^{2} \psi^{-k}(t) \sum_{s\in F_q^*} \psi^k(s)\,\chi(s)\Big)^l \\ &= \Big(\psi^{-1}(t) \sum_{s\in F_q^*} \psi(s)\,\chi(s) + \psi^{-2}(t) \sum_{s\in F_q^*} \psi^2(s)\chi(s)\Big)^l \\ &= \Big(G_1(t) + G_2(t)\Big)^l \\ &= \sum_{r=0}^{l} \left(\begin{array}{c} l \\ r \end{array}\right) G_1(t)^{l-r} G_2(t)^r, \end{aligned}$$

where

$$G_1(t) = \psi^{-1}(t) \sum_{s\in F_q^*} \psi(s)\chi(s)$$

and

$$G_2(t) = \psi^{-2}(t) \sum_{s\in F_q^*} \psi^2(s)\chi(s).$$

Note that $G_1(t) = q\psi^{-1}(t)\,\widehat{\psi}(-1)$ and $G_2(t) = q\psi^{-2}(t)\,\widehat{\psi^2}(-1)$.

Thus we conclude that

$$\Big(\sum_{s\in F_q}\chi(ts^3)\Big)^l = \sum_{r=0}^{l}\left(\begin{array}{c} l \\ r \end{array}\right) q^l\psi^{-(l+r)}(t)\Big(\widehat{\psi}(-1)\Big)^{l-r}\Big(\widehat{\psi^2}(-1)\Big)^r.$$

We are now ready to prove Theorem 5.1. First, we assume that $m = (0,\cdots,0) \in F_q^d$. Then, using Lemma 6.3, we see that

$$\widehat{S}_j(0,\cdots,0) = q^{-d}\sum_{\{x\in\mathbb{F}_q^d:||x||=j\}} 1$$

$$= q^{-1} + q^{-d-1}\sum_{t\in\mathbb{F}_q^*}\chi(-tj)\sum_{x}\chi(t(||x||))$$

$$= q^{-1} + q^{-d-1}\sum_{t\in\mathbb{F}_q^*}\chi(-tj)\sum_{r=0}^{d}\left(\begin{array}{c} d \\ r \end{array}\right) q^d\psi^{-(d+r)}(t)\Big(\widehat{\psi}(-1)\Big)^{d-r}\Big(\widehat{\psi^2}(-1)\Big)^r$$

$$= q^{-1} + q^{-1}\sum_{r=0}^{d}\left(\begin{array}{c} d \\ r \end{array}\right)\Big(\widehat{\psi}(-1)\Big)^{d-r}\Big(\widehat{\psi^2}(-1)\Big)^r\sum_{t\in\mathbb{F}_q^*}\chi(-tj)\psi^{-(d+r)}(t)$$

$$= q^{-1} + q^{-1}\sum_{r=0}^{d}\left(\begin{array}{c} d \\ r \end{array}\right)\Big(\widehat{\psi}(-1)\Big)^{d-r}\Big(\widehat{\psi^2}(-1)\Big)^r q\widehat{\psi^{-(d+r)}}(j)$$

$$= q^{-1} + O(q^{-\frac{d+1}{2}}) \approx O(q^{-1}).$$

In the last equality, we used the fact that $\widehat{\psi}(k) = O(q^{-\frac{1}{2}})$ for any multiplicative character of F_q. Thus the second part of Theorem 5.1 is proved. Now we shall deal with the problem in case $m = (m_1,\cdots,m_d) \neq (0,\cdots,0)$. Suppose that $m_j \neq 0$ for $j \in J \subset \{1,2,\cdots,d\}$ and $m_j = 0$ for $j \in \{1,2,\cdots,d\}\setminus J = J^{'}$. Without loss of generality, we may assume that $J = \{1,2,\cdots,l\}$ and $J^{'} = \{l+1,\cdots,d\}$for some $l = 1,2,\cdots,d$. Using Lemma (6.1) and Lemma (6.3),we see that

$$\widehat{S_j}(m) = q^{-d-1}\sum_{t\in F_q^*}\chi(-tj)\sum_{x\in F_q^d}\chi(t||x|| + m\cdot x)$$

$$= q^{-d-1}\sum_{t\in F_q^*}\chi(-tj)\Big(\prod_{k=1}^{l}\sum_{s_k\in F_q}\chi(ts_k^3 + m_ks_k)\Big)\Big(\prod_{k=l+1}^{d}\sum_{s_k\in F_q}\chi(ts_k^3)\Big)$$

$$= q^{-d-1} \sum_{t \in F_q^*} \chi(-tj)\, \psi^{-l}(t) \sum_{s_1,\cdots,s_l \in F_q^*} \chi(s_1+\cdots+s_l-m_1^3t^{-1}s_1^{-1}-\cdots-m_l^3t^{-1}s_l^{-1})\psi(s_1)\cdots\psi(s_l)$$

$$\times \sum_{r=0}^{d-l} \begin{pmatrix} d-l \\ r \end{pmatrix} q^{d-l}\, \psi^{-(d-l+r)}(t) \left(\widehat{\psi}(-1)\right)^{d-l-r} \left(\widehat{\psi^2}(-1)\right)^{r}$$

$$= q^{-1-l} \sum_{r=0}^{d-l} \begin{pmatrix} d-l \\ r \end{pmatrix} \left(\widehat{\psi}(-1)\right)^{d-l-r} \left(\widehat{\psi^2}(-1)\right)^{r} \sum_{t \in F_q^*} \chi(-tj)\, \psi^{-(d+r)}(t)$$

$$\times \sum_{s_1,\cdots,s_l \in F_q^*} \chi(s_1+\cdots+s_l-m_1^3t^{-1}s_1^{-1}-\cdots-m_l^3t^{-1}s_l^{-1})\psi(s_1)\cdots\psi(s_l)$$

Since $\begin{pmatrix} d-l \\ r \end{pmatrix} \left(\widehat{\psi}(-1)\right)^{d-l-r} \left(\widehat{\psi^2}(-1)\right)^{r} = O(q^{-\frac{1}{2}(d-l)})$, we obtain that

$$\left|\widehat{S_j}(m)\right| \lesssim q^{-1-\frac{d+l}{2}} \sum_{r=0}^{d-l} |A_r(\chi,\psi)|,$$

where $A_r(\chi,\psi)$ is given by

$$\sum_{t \in F_q^*} \chi(-tj)\, \psi^{-(d+r)}(t) \sum_{s_1,\cdots,s_l \in F_q^*} \chi(s_1+\cdots+s_l-m_1^3t^{-1}s_1^{-1}-\cdots-m_l^3t^{-1}s_l^{-1})\psi(s_1)\cdots\psi(s_l).$$

We now apply the result of Adolphson and Sperber ([2], Theorem 4.2, Corollary 4.3) to see that for all $r = 0, 1, \cdots, d-l$,

$$|A_r(\chi,\psi)| \lesssim q^{\frac{l+1}{2}}.$$

This completes the proof.

7 Proof of Theorem 3.4 and Corollary 3.6

As we mentioned in the introduction, this a simple variation on the proof of Theorem 3.1. Indeed,

$$\#\{(x,y) \in E \times F : ||x-y|| = j\}$$
$$= q^{2d} \sum_m \widehat{E}(m)\overline{\widehat{F}(m)}\widehat{S}_j(m)$$
$$= \#E \cdot \#F \cdot q^{-d} \cdot \#S_j + q^{2d} \sum_{m \neq (0,\dots,0)} \widehat{E}(m)\overline{\widehat{F}(m)}\widehat{S}_j(m) = I + II.$$

By Lemma 5.2,

$$I \lesssim \#E \cdot \#F \cdot q^{-1}.$$

Applying Cauchy-Schwartz, Theorem 5.1 and Plancherel, we see that

$$II \lesssim q^{2d} q^{-\frac{d+1}{2}} \sum_{m \neq (0,\ldots,0)} \widehat{E}(m)\overline{\widehat{F}(m)}$$

$$\leq q^{2d} q^{-\frac{d+1}{2}} \left(\sum_m |\widehat{E}(m)|^2 \right)^{\frac{1}{2}} \cdot \left(\sum_m |\widehat{F}(m)|^2 \right)^{\frac{1}{2}}$$

$$\leq q^{2d} q^{-\frac{d+1}{2}} q^{-d} \left(\sum_x |E(x)|^2 \right)^{\frac{1}{2}} \cdot \left(\sum_x |\widehat{F}(x)|^2 \right)^{\frac{1}{2}}$$

$$= q^{\frac{d-1}{2}} \cdot \sqrt{\#E} \cdot \sqrt{\#F}.$$

This completes the proof of Theorem 3.4.

The proof of Corollary 3.6 we observe that by Lemma 5.2

$$I \gtrsim \#E \cdot \#F \cdot q^{-1}.$$

On the other hand, we have seen above that

$$II \lesssim q^{\frac{d-1}{2}} \cdot \sqrt{\#E} \cdot \sqrt{\#F},$$

and the result follows by a direct comparison.

References

[1] J. Pach, and P. Agarwal, *Combinatorial geometry,* Wiley-Interscience Series in Discrete Mathematics and Optimization. A Wiley-Interscience Publication. John Wiley and Sons, Inc., New York (1995).

[2] A. Adolphson and S. Sperber, *Exponential sums and Newton polyhedra: cohomology and estimates*, (1989), **130**, 367-406.

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

[4] W. Duke and H. Iwaniec, *A relation between cubic exponential and Kloosterman sums*, Contemp. Math. **143**, (1993), 255-258.

[5] P. Erdös *On sets of distances of n points,* Amer. Math. Monthly. **53** (1946), 248–250.

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

[7] B. J. Green, *Restriction and Kakeya phonomena,* Lecture notes (2003).

[8] H. Iwaniec, and E. Kowalski, *Analytc Number Theory,* Colloquium Publications **53** (2004).

[9] A. Iosevich and M. Rudnev, *Erdos/Falconer distance problem in vector spaces over finite fields*, TAMS (to appear), (2006).

[10] N. Katz, *Gauss sums, Kloosterman sums, and monodromy groups,* Ann. Math. Studies **1**16, Princeton (1988).

[11] M. Lacey and W. McClain, it On an argument of Shkredov in the finite field setting, (2006), On-line journal of analytic combinatorics (http://www.ojac.org).

[12] J. Matousek, *Lectures on Discrete Geometry,* Graduate Texts in Mathematics, Springer **202** (2002).

[13] G. Mockenhaupt, and T. Tao, *Restriction and Kakeya phenomena for finite fields,* Duke Math. J. **121** (2004), 35–74.

[14] H. Niederreiter, *The distribution of values of Kloosterman sums,* Arch. Math. **56** (1991), 270–277.

[15] I. Shparlinski, *On the set of distances between two sets in vector spaces over finite fields*, (2006), (preprint).

[16] E. Stein, and R. Shakarchi, *Fourier analysis,* Princeton Lectures in Analysis, (2003).

[17] T. Tao, *Finite field analogues of Erdös, Falconer, and Furstenberg problems,* preprint.

[18] A. Weil, *On some exponential sums,* Proc. Nat. Acad. Sci. U.S.A. **34** (1948), 204–207.

[19] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge Univ. Press (1997).