International Journal of Number Theory
(2017)
© World Scientific Publishing Company
DOI: 10.1142/S1793042117501275

World Scientific
www.worldscientific.com

The analog of the Erdös distance problem in finite fields

S. D. Adhikari

Harish-Chandra Research Institute, HBNI
Chhatnag Road, Jhusi, Allahabad 211 019, India
adhikari@hri.res.in

Anirban Mukhopadhyay

Institute of Mathematical Sciences, HBNI
CIT Campus, Taramani, Chennai 600113, India
anirban@imsc.res.in

M. Ram Murty

Department of Mathematics and Statistics
Jeffery Hall, Queen's University
Kingston, Ontario, Canada K7L 3N6
murty@mast.queensu.ca

Received 24 November 2015
Accepted 20 October 2016
Published

In this paper, we give a proof of the result of Iosevich and Rudnev [Erdös distance problem in vector spaces over finite fields, *Trans. Amer. Math. Soc.* **359** (2007) 6127–6142] on the analog of the Erdös–Falconer distance problem in the case of a finite field of characteristic p, where p is an odd prime, without using estimates for Kloosterman sums. We also address the case of characteristic 2.

Keywords: Finite-fields; Erdös–Falconer distance problem; Fourier analysis.

Mathematics Subject Classification 2010: 11T24, 52C10

1. Introduction

The finite field analog of the Erdös–Falconer distance problem was investigated by Iosevich and Rudnev [5] by developing the Fourier analytic machinery. More precisely, if $q = p^r$, where p is an odd prime, and $E \subset \mathbb{F}_q^d$, then the minimum cardinality of the set $\Delta(E)$ of distinct distances between points of E was estimated in terms of the cardinality of the set E. The proof of the result of Iosevich and Rudnev uses bounds on Kloosterman sums. In this paper, we give a proof

of their result without using estimates for Kloosterman sums. In the next section, we introduce the relevant terminology and state our result.

In Sec. 5, we take up the Erdös–Falconer distance problem in characteristic 2.

While Iosevich and Rudnev [5] considered the spherical distance problem associated with the polynomial $P(x) = \sum_{j=1}^{d} x_j^2$, later, Iosevich and Koh [4] studied the cubic distance problem associated with the polynomial $P(x) = \sum_{j=1}^{d} x_j^3$ and the problem of Erdös–Falconer distance sets related to general diagonal polynomials were considered by Koh and Shen [6].

We would like to mention that in a forthcoming paper [1], Bennett, Hart, Iosevich, Pakianathan and Rudnev have employed some elementary arguments while establishing the lower bound $|T_d^d(E)| \gg q^{\binom{d+1}{2}}$, where E is a subset of $\mathbb{F}_q^d$ with $d \geq 2$ such that $|E| \gg q^s$ for some $s = s(d) < d$ and $T_k^d(E)$ denotes the set of congruence classes of k-dimensional simplices determined by $(k+1)$-tuples of points from E. Better results are obtained in the special case $d = 2$. They employ the simple observation that if the distance from x to y is equal to the distance from x' to y', then there exists a rotation, unique up to the obvious stabilizer, such that $x - y = \theta(x' - y')$. One observes that with a relatively simpler idea, they improve over some known results and extend some others.

We also mention a result of Le Anh Vinh [7] where graph theoretic tools are used to derive a general version with a non-degenerate quadratic form giving the distance. It is also generalized to "finite non-Euclidean" setting.

2. Preliminaries and the Statement of Our Result

For an odd prime p and $q = p^r$ we consider the finite field $\mathbb{F}_q$ with q elements. Let E be a subset of the vector space $\mathbb{F}_q^d$. We define a distance function

$$|\cdot|^2 : \mathbb{F}_q^d \to \mathbb{F}_q$$

by

$$|x|^2 = x_1^2 + x_2^2 + \cdots + x_d^2,$$

where $x = (x_1, x_2, \ldots, x_d)$. We also set

$$\Delta(E) = |\{|x - y|^2 : (x, y) \in E \times E\}|$$

as the number of distinct distances determined by the set E. Let

$$\nu(j) = |\{(x, y) \in E \times E : |x - y|^2 = j\}|.$$

By Cauchy–Schwarz inequality we get

$$\Delta(E) \geq \frac{|E|^4}{\sum_j \nu^2(j)}.$$

In this paper, we prove the following theorem due to Iosevich and Rudnev [5] without using estimates for Kloosterman sums.

Theorem 1. *Let E be a subset of $\mathbb{F}_q^d$ with $d \geq 3$.*

$$\text{If } |E| \gg q^{(d+1)/2}, \quad \text{then } \Delta(E) \gg q.$$

Fourier transform on vector space over finite fields. Let $\phi : \mathbb{F}_q \to \mathbb{C}$ be defined by

$$\phi(x) = e\left(\frac{\text{tr}(x)}{p}\right),$$

where $e(z) = e^{2\pi iz}$ and $\text{tr}(x)$ denotes the trace of x over $\mathbb{F}_p$.

Then ϕ defines a character on $\mathbb{F}_q$. Moreover, all the characters of $\mathbb{F}_q$ are given by ψ_a where $a \in \mathbb{F}_q$ and

$$\psi_a(x) = \phi(ax).$$

Now we choose an arbitrary character ψ and fix it for the rest of the section.

For a complex valued function g on $\mathbb{F}_q^d$, we define its Fourier transform, also a function on $\mathbb{F}_q^d$, as

$$\hat{g}(m) = \frac{1}{q^d} \sum_{x \in \mathbb{F}_q^d} g(x)\psi(-x \cdot m),$$

where $x \cdot m$ is the standard inner product. It is easy to see that the Fourier inversion formula and Parseval's equality take the form:

$$g(x) = \sum_{m \in \mathbb{F}_q^d} \hat{g}(m)\psi(x \cdot m),$$

and

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

We define

$$S_j = \{x \in \mathbb{F}_q^d : |x|^2 = j\}.$$

Using Fourier inversion we get

$$\nu(j) = \sum_{x,y \in \mathbb{F}_q^d} E(x)E(y)S_j(x-y) = q^{2d} \sum_{m \in \mathbb{F}_q^d} |\hat{E}(m)|^2 \hat{S}_j(m).$$

Here and throughout the paper we would denote a set and its characteristic function by same notation.

Our goal is to find an upper bound for

$$\sum_{j \in \mathbb{F}_q} \nu^2(j) = q^{4d} \sum_{m_1, m_2 \in \mathbb{F}_q^d} |\hat{E}(m_1)|^2 |\hat{E}(m_2)|^2 \sum_{j \in \mathbb{F}_q} \hat{S}_j(m_1)\hat{S}_j(m_2). \tag{2.1}$$

3. Lemmas

Notations in this section will remain the same as in the previous one.

Lemma 1. *We have*

$$\hat{S}_j(m) = \frac{1}{q}\delta(m) + \frac{\epsilon_d}{q^{d/2+1}} \sum_{t \in \mathbb{F}_q^*} \psi\left(-tj - \frac{|m|^2}{4t}\right),$$

where $\epsilon_d = (\pm i)^d$ *and* $\delta(m)$ *is the delta function at* 0.

We note that the sum on the right-hand side is a Kloosterman sum. Our next lemma which evaluates the inner sum of (2.1) shows that if we average over $j \in \mathbb{F}_q$ then we do not need to use estimates for Kloosterman sums.

Lemma 2. *We have*

$$\sum_{j \in \mathbb{F}_q} \hat{S}_j(m_1)\hat{S}_j(m_2) = \begin{cases} \frac{1}{q} + O\left(\frac{1}{q^{d/2}}\right) & \text{if } m_1 = m_2 = 0, \\ O\left(\frac{1}{q^{d-1}}\right) & \text{if } m_1 = 0 \text{ and } m_2 \neq 0, \\ \frac{-\epsilon_d^2}{q^{d+1}} & \text{if } m_1 \neq 0, m_2 \neq 0 \text{ and } |m_1|^2 \neq |m_2|^2, \\ \frac{\epsilon_d^2(q-1)}{q^{d+1}} & \text{if } m_1 \neq 0, m_2 \neq 0 \text{ and } |m_1|^2 = |m_2|^2. \end{cases}$$

Proof.

Case I: $m_1 = m_2 = 0$**.**

Clearly

$$\hat{S}_j(0) = \frac{1}{q} + O\left(\frac{1}{q^{d/2}}\right)$$

and so

$$\sum_{j \in \mathbb{F}_q} \hat{S}_j{}^2(0) = \frac{1}{q} + O\left(\frac{1}{q^{d/2}}\right).$$

Case II: Either $m_1 = 0$ or $m_2 = 0$, but not both.

$$\begin{aligned} \sum_{j \in \mathbb{F}_q} \hat{S}_j(0)\hat{S}_j(m) &= \sum_{j \in \mathbb{F}_q} \left(\frac{1}{q} + O\left(\frac{1}{q^{d/2}}\right)\right) \frac{\epsilon_d}{q^{d/2+1}} \sum_{t \in \mathbb{F}_q^*} \psi\left(-tj - \frac{|m|^2}{4t}\right) \\ &= \frac{\epsilon_d}{q^{d/2+1}} \sum_{t \in \mathbb{F}_q^*} \psi\left(-\frac{|m|^2}{4t}\right) \sum_{j \in \mathbb{F}_q} \psi(-tj) + O\left(\frac{q^2}{q^{d+1}}\right) = O\left(\frac{1}{q^{d-1}}\right) \end{aligned}$$

since the main term vanishes.

Case III: $m_1 \neq 0,\ m_2 \neq 0.$

$$\begin{aligned}\sum_{j\in\mathbb{F}_q} \hat{S}_j(m_1)\hat{S}_j(m_2) &= \sum_{j\in\mathbb{F}_q}\left(\frac{\epsilon_d}{q^{d/2+1}}\right)^2 \sum_{t_1,t_2\in\mathbb{F}_q^*} \psi\left(-t_1 j - t_2 j - \frac{|m_1|^2}{4t_1} - \frac{|m_2|^2}{4t_2}\right)\\ &= \frac{\epsilon_d^2}{q^{d+2}} \sum_{t_1,t_2\in\mathbb{F}_q^*} \psi\left(-\frac{|m_1|^2}{4t_1} - \frac{|m_2|^2}{4t_2}\right) \sum_{j\in\mathbb{F}_q} \psi(-j(t_1+t_2))\\ &= \frac{\epsilon_d^2}{q^{d+1}} \sum_{t\in\mathbb{F}_q^*} \psi\left(-\frac{(|m_1|^2 - |m_2|^2)}{4t}\right)\\ &= \begin{cases} \dfrac{-\epsilon_d^2}{q^{d+1}} & \text{if } |m_1|^2 \neq |m_2|^2,\\ \dfrac{\epsilon_d^2(q-1)}{q^{d+1}} & \text{if } |m_1|^2 = |m_2|^2. \end{cases}\end{aligned}$$

This finishes the proof of the lemma.

We note the following observation from Fourier analysis as defined in the last section.

Lemma 3. *For a set $E \subset \mathbb{F}_q^d$ we have*

$$\sum_{m\in\mathbb{F}_q^d} |\hat{E}(m)|^2 = \frac{1}{q^d} \sum_{x\in\mathbb{F}_q^d} |E(x)|^2 = \frac{|E|}{q^d} \quad \textit{and} \quad \hat{E}(0) = \frac{|E|}{q^d}.$$

Lemma 4. *For a set $E \subset \mathbb{F}_q^d$ we have*

$$\sum_{\substack{m_1,m_2\in\mathbb{F}_q^d\setminus\{0\}\\ |m_1|^2=|m_2|^2}} |\hat{E}(m_1)|^2|\hat{E}(m_2)|^2 = O\left(\frac{|E|^2}{q^{2d}}\right).$$

Proof. We bound the left-hand sides trivially as

$$\sum_{\substack{m_1,m_2\in\mathbb{F}_q^d\setminus\{0\}\\ |m_1|^2=|m_2|^2}} |\hat{E}(m_1)|^2|\hat{E}(m_2)|^2 \leq \left(\sum_{m\in\mathbb{F}_q^d\setminus\{0\}} |\hat{E}(m)|^2\right)^2.$$

Hence the lemma follows by Plancherel's theorem. □

4. Proof of Theorem 1

Using Lemma 2 we get

$$\sum_{j\in\mathbb{F}_q} \nu^2(j) = q^{4d} \sum_{m_1,m_2\in\mathbb{F}_q^d\setminus\{0\}} |\hat{E}(m_1)|^2|\hat{E}(m_2)|^2 \sum_{j\in\mathbb{F}_q} \hat{S}_j(m_1)\hat{S}_j(m_2)$$

$$
\begin{aligned}
&= q^{4d}|\hat{E}(0)|^2|\hat{E}(0)|^2\left(\frac{1}{q}+O\left(\frac{1}{q^{d/2}}\right)\right)\\
&\quad + q^{4d}|\hat{E}(0)|^2\sum_{m\in\mathbb{F}_q^d\setminus\{0\}}|\hat{E}(m)|^2 O\left(\frac{1}{q^{d-1}}\right)\\
&\quad + q^{4d}\sum_{\substack{m_1,m_2\in\mathbb{F}_q^d\setminus\{0\}\\ |m_1|^2\neq|m_2|^2}}|\hat{E}(m_1)|^2|\hat{E}(m_2)|^2\frac{(-\epsilon_d^2)}{q^{d+1}}\\
&\quad + q^{4d}\sum_{\substack{m_1,m_2\in\mathbb{F}_q^d\setminus\{0\}\\ |m_1|^2=|m_2|^2}}|\hat{E}(m_1)|^2|\hat{E}(m_2)|^2\frac{\epsilon_d^2(q-1)}{q^{d+1}}\\
&= \epsilon_d^2 q^{3d}\sum_{\substack{m_1,m_2\in\mathbb{F}_q^d\setminus\{0\}\\ |m_1|^2=|m_2|^2}}|\hat{E}(m_1)|^2|\hat{E}(m_2)|^2\\
&\quad + O\left(\frac{|E|^4}{q}\right)+O(q|E|^3)+O(q^{d-1}|E|^2).
\end{aligned}
$$

Now we use Lemma 4 to conclude

$$\sum_{j\in\mathbb{F}_q}\nu^2(j)\ll\frac{|E|^4}{q}+q|E|^3+q^d|E|^2.$$

Since we are considering set E such that $|E|\geq q^2$, the second term is dominated by the first, so

$$\sum_{j\in\mathbb{F}_q}\nu^2(j)\ll\frac{|E|^4}{q}+q^d|E|^2.$$

Finally

$$\Delta(E)\geq\frac{|E|^4}{\sum_j\nu^2(j)}\gg\frac{|E|^4}{|E|^4/q+q^d|E|^2}.$$

Thus

$$|E|\gg q^{(d+1)/2}\quad\text{implies }\Delta(E)\gg q,$$

completing the proof of the theorem.

5. The Erdös Distance Problem in Characteristic 2

In this section, we consider an analog of Erdös distance problem in a vector space over a finite field of characteristic 2. Let $E\subset\mathbb{F}_N^d$ where $N=2^n$. The distance

function now is

$$|x-y|^2 = \sum_{i=1}^{d} x_i^2 + \sum_{i=1}^{d} y_i^2,$$

where $x = (x_1, x_2, \ldots, x_d)$ and $y = (y_1, y_2, \ldots, y_d)$ are elements of $\mathbb{F}_N^d$.

We define

$$\mathrm{Ad}(E,E) = |\{(x,y,z,w) \in E^4 : x+y = z+w\}|.$$

This number is usually called the *Additive Energy* of the set E.

We start by considering an example. Let E be a subset of $\mathbb{F}_N^d$ defined as follows:

$$E = \{(x_1, \ldots, x_{d-1}, x_d) \,|\, x_1, \ldots, x_{d-1} \in \mathbb{F}_N, x_d^2 = x_1^2 + \cdots + x_{d-1}^2\}.$$

Since every element in a field of characteristic 2 is a square, we have $|E| = N^{d-1}$. However, we note that $\Delta(E) = 1$. So, the situation in characteristic 2 is quite different from that in odd characteristics. By imposing a condition on additive energy of the set E we could prove the following theorem.

Theorem 2. *For a subset E of $\mathbb{F}_N^d$:*

$$\textit{If } \mathrm{Ad}(E,E) \leq \frac{|E|^3}{N} \quad \textit{and} \quad |E| \geq N^{d-1}, \quad \textit{then } \Delta(E) \gg N.$$

Definitions of the sets $\nu(j)$ and S_j remain the same as in the previous section. Proof of the theorem also starts in a similar way but deviates considerably as many of the arguments leading to the proof of Theorem 1 do not remain valid in characteristic 2.

The following lemma is a special case of the Artin–Schreier theorem in characteristic 2 (see [2, Theorem 6.69, p. 166]).

Lemma 5. *Let $f(T) = aT^2 + bT + c$ be a polynomial in $\mathbb{F}_N[T]$. Then*

- *f has exactly one root in $\mathbb{F}_N$ if and only if $b = 0$.*
- *f has exactly two roots in $\mathbb{F}_N$ if and only if $b \neq 0$ and $\mathrm{tr}(ac/l^2) = 0$.*
- *f has no root in $\mathbb{F}_N$ if and only if $b \neq 0$ and $\mathrm{tr}(ac/l^2) = 1$.*

The next lemma computes the Fourier transform of S_j.

Lemma 6.

$$\hat{S}_j(m) = \begin{cases} \dfrac{1}{N} & \textit{if } m = (0, \ldots, 0), \\ \dfrac{1}{N}\psi(m_0^2 j) & \textit{if } m = (m_0, \ldots, m_0), \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. We have

$$\begin{aligned}\hat{S}_j(m) &= \frac{1}{N^d}\sum_{x\in\mathbb{F}_N^d} S_j(x)\psi(-x\cdot m)\\ &= \frac{1}{N^d}\sum_{x\in\mathbb{F}_N^d}\psi(-x\cdot m)\frac{1}{N}\sum_{l\in\mathbb{F}_N}\psi(l(|x|^2+j))\\ &= \frac{1}{N^{d+1}}\sum_{l\in\mathbb{F}_N}\psi(lj)\sum_{x\in\mathbb{F}_N^d}\psi(-x\cdot m+l|x|^2)\\ &= \frac{1}{N}\delta(m)+\frac{1}{N^{d+1}}\sum_{l\in\mathbb{F}_N^*}\psi(lj)\prod_{i=1}^{d}\sum_{t\in F_N}\psi(m_it+lt^2)\end{aligned}$$

since the summand corresponding to $l=0$ vanishes unless $m=0$.

We write

$$\sum_{t\in F_N}\psi(m_it+lt^2)=\sum_{a\in\mathbb{F}_N}N_a\psi(a),$$

where

$$N_a=|\{t\in\mathbb{F}_N : lt^2+m_it+a=0\}|.$$

From Lemma 5 we get

$$N_a=\begin{cases}1 & \text{if } m_i=0,\\ 2 & \text{if } m_i\neq 0, \operatorname{tr}(la/m_i^2)=0,\\ 0 & \text{if } m_i\neq 0, \operatorname{tr}(la/m_i^2)=1.\end{cases}\tag{5.1}$$

Note that if $m_i=0$,

$$\sum_{t\in F_N}\psi(m_it+lt^2)=\sum_{t\in F_N}\psi(lt^2)=0$$

since all the elements in a field of characteristic 2 are squares.

Therefore

$$\sum_{a\in\mathbb{F}_N}N_a\psi(a)=2\sum_{\substack{a\in\mathbb{F}_N\\ \operatorname{tr}(la/m_i^2)=0}}\psi(a).$$

Let ϕ be the additive character of F_N defined by

$$\phi(x)=e\left(\frac{\operatorname{tr}(x)}{2}\right),$$

where the exponential function being $e(z)=e^{2\pi iz}$. We note that

$$\frac{1}{2}(1+\phi(x))=\begin{cases}1 & \text{if } \operatorname{tr}(x)=0,\\ 0 & \text{otherwise.}\end{cases}$$

We have done the Fourier analysis with an arbitrary but fixed non-principal character ψ. From here onwards we choose $\psi = \phi$. Thus

$$\begin{aligned}\sum_{a\in\mathbb{F}_N} N_a\psi(a) &= \sum_{a\in\mathbb{F}_N} \phi(a)(1+\phi(la/m_i^2))\\ &= \sum_{a\in\mathbb{F}_N} \phi(a)\phi(la/m_i^2)\\ &= \sum_{a\in\mathbb{F}_N} e\left(\frac{\mathrm{tr}(a(1+l/m_i^2))}{2}\right).\end{aligned}$$

We note that all the characters on $\mathbb{F}_N$ are given by

$$\psi_a : x \to e\left(\frac{\mathrm{tr}(ax)}{2}\right)$$

and $a \to \psi_a$ defines an isomorphisms between $\mathbb{F}_N$ and its dual as an additive group. Hence following this notation we can write

$$\sum_{a\in\mathbb{F}_N} N_a\psi(a) = \sum_{a\in\mathbb{F}_N} \psi_k(a),$$

where $k = 1+l/m_i^2$. The last sum vanishes unless ψ_k is a principal character and that happens only if $\mathrm{tr}(a(1+l/m_i^2)) = 0$ for all $a \in \mathbb{F}_N$. Since $\mathbb{F}_N$ is a separable extension of $\mathbb{F}_2$, the bilinear form given by $(x, y) \to \mathrm{tr}(xy)$ is non-degenerate. Therefore $1 + l/m_i^2 = 0$ which implies $l = m_i^2$. We get

$$\sum_{t\in F_N} \psi(m_i t + lt^2) = \begin{cases} N & \text{if } l = m_i^2,\\ 0 & \text{otherwise.}\end{cases}$$

Hence we conclude

$$\hat{S}_j(m) = \begin{cases} \dfrac{1}{N} & \text{if } m = (0,\ldots,0),\\ \dfrac{1}{N}\psi(m_0^2 j) & \text{if } m = (m_0,\ldots,m_0),\\ 0 & \text{otherwise.}\end{cases}$$

□

The following lemma is a general fact about the l^4 norm of a Fourier transform.

Lemma 7. *Let f be a complex valued function on $\mathbb{F}_N^d$. For $y \in \mathbb{F}_N^d$, we define $f_y(x) = f(x + y)$ and also $F(y)$ to be the inner product (f, f_y). Then*

$$(F, F) = N^{3d} \sum_{m\in\mathbb{F}_N^d} |\hat{f}(m)|^4.$$

Proof. We note that by Fourier inversion

$$f_y(x) = \sum_{m\in\mathbb{F}_N^d} \hat{f}(m)\psi(y\cdot m)\psi(x\cdot m).$$

Thus $\hat{f}_y(m) = \hat{f}(m)\psi(y \cdot m)$. Hence by Parseval's equality

$$F(y) = N^d \sum_{m \in \mathbb{F}_N^d} \hat{f}_y(m)\overline{\hat{f}(m)} = N^d \sum_{m \in \mathbb{F}_N^d} |\hat{f}(m)|^2 \psi(y \cdot m).$$

Therefore

$$(F, F) = N^{3d} \sum_{m \in \mathbb{F}_N^d} |\hat{f}(m)|^4. \qquad \square$$

Our last lemma is about additive energy.

Lemma 8. *For a subset E of $\mathbb{F}_N^d$ we have*

$$\sum_{m \in \mathbb{F}_N^d} |\hat{E}(m)|^4 = \sum_{y \in E-E} |(y+E) \cap E|^2 = \frac{\mathrm{Ad}(E,E)}{N^{3d}}.$$

Proof. We take $f = E$ in the last lemma to prove this equality. $\square$

Proof of Theorem 2. As earlier by the Cauchy–Schwarz inequality we get

$$\Delta(E) \geq \frac{|E|^4}{\sum_j \nu(j)^2}.$$

The Fourier inversion formula gives

$$\nu(j) = N^{2d} \sum_{m \in \mathbb{F}_N^d} |\hat{E}(m)|^2 \hat{S}_j(m).$$

Hence

$$\begin{aligned}\sum_{j \in \mathbb{F}_N} \nu(j)^2 &= N^{4d} \sum_{m,n \in \mathbb{F}_N^d} |\hat{E}(m)|^2 |\hat{E}(n)|^2 \sum_{j \in \mathbb{F}_N} \hat{S}_j(m)\hat{S}_j(n) \\ &= N^{4d} |\hat{E}(0)|^4 \frac{1}{N} \\ &\quad + N^{4d} \sum_{\substack{m_0 \in \mathbb{F}_N \setminus \{0\} \\ n_0 \in \mathbb{F}_N \setminus \{0\}}} |\hat{E}(m_0, m_0, \ldots, m_0)|^2 |\hat{E}(n_0, n_0, \ldots, n_0)|^2 \\ &\quad \times \frac{1}{N^2} \sum_{j \in \mathbb{F}_N} \psi(m_0^2 j)\psi(n_0^2 j).\end{aligned}$$

By orthogonality of characters we get

$$\sum_{j \in \mathbb{F}_N} \psi(m_0^2 j)\psi(n_0^2 j) = \begin{cases} N & \text{if } m_0 = n_0, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore

$$\sum_{j \in \mathbb{F}_N} \nu(j)^2 = \frac{|E|^4}{N} + N^{4d-1} \sum_{m \in \mathbb{F}_N \setminus \{0\}} |\hat{E}(m, m, \ldots, m)|^4.$$

The last sum is trivially bounded above as

$$\sum_{m\in\mathbb{F}_N\setminus\{0\}} |\hat{E}(m,m,\ldots,m)|^4 \leq \sum_{m\in\mathbb{F}_N^d} |\hat{E}(m)|^4 = \frac{\mathrm{Ad}(E,E)}{N^{3d}},$$

where the last inequality is a consequence of Lemma 8.

Thus we have

$$\sum_{j\in\mathbb{F}_N} \nu(j)^2 \leq \frac{|E|^4}{N} + N^{d-1}\mathrm{Ad}(E,E).$$

If

$$\mathrm{Ad}(E,E) \leq \frac{|E|^3}{N},$$

then

$$\sum_{j\in\mathbb{F}_N} \nu(j)^2 \leq \frac{|E|^4}{N} + N^{d-2}|E|^3.$$

Hence we get

$$\Delta(E) \geq \frac{|E|^4}{\frac{|E|^4}{N} + \frac{|E|^4}{N}} \geq \frac{N}{2},$$

whenever $|E| \geq N^{d-1}$. Taking $|E| \geq cN^{d-1}$, for some $c \geq 1$, we have $\Delta(E) \geq \frac{N}{1+\frac{1}{c}}$.

Hence the theorem.

6. A Variant of the Sum-Product Problem

Here we consider finite fields $\mathbb{F}_q$ with q elements where q is a power of an odd prime. Let $E \subset \mathbb{F}_q^2$. For $j \in \mathbb{F}_q$ define

$$A(j) = |\{(x,y) \in E \times E : (x_1 - y_1)(x_2 - y_2) = j\}|.$$

Let

$$\Omega(E) = |\{(x_1 - y_1)(x_2 - y_2) : (x,y) \in E\}|.$$

By the Cauchy–Schwarz inequality we get

$$\Omega(E) \geq \frac{|E|^4}{\sum_j A(j)^2}.$$

The aim of this section is to prove the following theorem due to Iosevich–Hart–Solymosi [3] without using estimates on Kloosterman sums.

Theorem 3. *Let $E \subset \mathbb{F}_q^2$ be such that $|E| \gg q^{3/2}$ then $\Omega(E) \gg q$.*

Before we begin the proof, we need the following lemmas. We define

$$H_j = \{x \in \mathbb{F}_q^2 : x_1 x_2 = j\}.$$

Then

$$A(j) = \sum_{x,y\in\mathbb{F}_q^2} E(x)E(y)H_j(x-y) = q^4 \sum_m |\hat{E}(m)|^2 \hat{H}_j(m).$$

Our first lemma evaluates $\hat{H}_j(m)$.

Lemma 9. *For $m \in \mathbb{F}_q^2$ we have*

$$\hat{H}_j(m) = \frac{1}{q}\delta(m) + \frac{1}{q^2}\sum_{l\in\mathbb{F}_q^*} \psi\left(-lj - \frac{m_1m_2}{l}\right).$$

Proof. Using the definition of Fourier transform and the orthogonality of characters we can write

$$\begin{aligned}
\hat{H}_j(m) &= \frac{1}{q^2}\sum_{x\in\mathbb{F}_q^2} H_j(x)\psi(-x\cdot m)\\
&= \frac{1}{q^2}\sum_{x\in\mathbb{F}_q^2} \psi(-x\cdot m)\frac{1}{q}\sum_{l\in\mathbb{F}_q}\psi(l(x_1x_2-j))\\
&= \frac{1}{q^3}\sum_{l\in\mathbb{F}_q}\psi(-lj)\sum_{x\in\mathbb{F}_q^2}\psi(-x\cdot m + lx_1x_2)\\
&= \frac{1}{q}\delta(m) + \frac{1}{q^3}\sum_{l\in\mathbb{F}_q^*}\psi(-lj)\sum_{x\in\mathbb{F}_q^2}\psi(-x_1m_1 - x_2m_2 + lx_1x_2).
\end{aligned}$$

We observe that for $l \in \mathbb{F}_q^*$ we get the inner sum

$$\begin{aligned}
&\sum_{x_1,x_2\in\mathbb{F}_q}\psi(-x_1m_1 - x_2m_2 + lx_1x_2)\\
&\quad= \psi\left(-\frac{m_1m_2}{l}\right)\sum_{x_1,x_2\in\mathbb{F}_q}\psi\left(l\left(x_1 - \frac{m_2}{l}\right)\left(x_2 - \frac{m_1}{l}\right)\right).
\end{aligned}$$

We note that

$$\sum_{y_1,y_2\in\mathbb{F}_q}\psi(ly_1y_2) = q.$$

By change of variable

$$\sum_{x_1,x_2\in\mathbb{F}_q}\psi(-x_1m_1 - x_2m_2 + lx_1x_2) = q\psi\left(-\frac{m_1m_2}{l}\right)$$

which completes the proof. □

Lemma 10. *We have*

$$\sum_{j\in\mathbb{F}_q}\hat{H}_j(m)\hat{H}_j(n)=\begin{cases}\dfrac{1}{q}+O\left(\dfrac{1}{q^2}\right) & \text{if } m=n=0,\\ O\left(\dfrac{1}{q^2}\right) & \text{if } m=0 \text{ and } n\neq 0,\\ \dfrac{-1}{q^3} & \text{if } m_1\neq 0, m_2\neq 0 \text{ and } m_1m_2\neq n_1n_2,\\ \dfrac{(q-1)}{q^3} & \text{if } m_1\neq 0, m_2\neq 0 \text{ and } m_1m_2=n_1n_2.\end{cases}$$

Proof. We first calculate that

$$\hat{H}_j(0)=\begin{cases}\dfrac{2}{q}-\dfrac{1}{q^2} & \text{if } j=0,\\ \dfrac{1}{q}-\dfrac{1}{q^2} & \text{if } j\neq 0.\end{cases}$$

Now it is easy to show that

$$\sum_{j\in\mathbb{F}_q}\hat{H}_j(0)^2=\frac{1}{q}+O\left(\frac{1}{q^2}\right).$$

For $m\neq 0$, we have

$$\begin{aligned}\sum_{j\in\mathbb{F}_q}\hat{H}_j(0)\hat{H}_j(m)&=\frac{1}{q^3}\left(2-\frac{1}{q}\right)\sum_{l\in\mathbb{F}_q^*}\psi\left(-\frac{m_1m_2}{l}\right)\\ &\quad+\frac{1}{q^3}\left(1-\frac{1}{q}\right)\sum_{l\in\mathbb{F}_q^*}\psi\left(-\frac{m_1m_2}{l}\right)\sum_{j\in\mathbb{F}_q^*}\psi(-lj)\\ &=\frac{1}{q^3}\sum_{l\in\mathbb{F}_q^*}\psi\left(-\frac{m_1m_2}{l}\right)\\ &=O\left(\frac{1}{q^2}\right).\end{aligned}$$

Let $m,n\in\mathbb{F}_q^2$ such that $m\neq 0$ and $n\neq 0$. We see that

$$\sum_{j\in\mathbb{F}_q}\hat{H}_j(m)\hat{H}_j(n)=\frac{1}{q^3}\sum_{l\in\mathbb{F}_q^*}\psi\left(\frac{-m_1m_2+n_1n_2}{l}\right).$$

The conclusion follows by orthogonality of character. □

Proof of Theorem 3. We observe that

$$\sum_{j\in\mathbb{F}_q^2}A(j)^2=q^8\sum_{m,n\in\mathbb{F}_q^2}|\hat{E}(m)|^2|\hat{E}(n)|^2\sum_{j\in\mathbb{F}_q^2}\hat{H}_j(m)\hat{H}_j(n).$$

From the previous lemmas we have

$$\sum_j A(j)^2 = q^8|\hat{E}(0)|^4\left(\frac{1}{q}+O\left(\frac{1}{q^2}\right)\right)$$
$$+q^8|\hat{E}(0)|^2\sum_m|\hat{E}(m)|^2O\left(\frac{1}{q^2}\right)-q^5\sum_{\substack{m,n\in\mathbb{F}_q^2\\ m_1m_2\neq n_1n_2}}|\hat{E}(m)|^2\hat{E}(n)|^2$$
$$+(q-1)q^5\sum_{\substack{m,n\in\mathbb{F}_q^2\\ m_1m_2=n_1n_2}}|\hat{E}(m)|^2\hat{E}(n)|^2.$$

Now

$$\sum_{\substack{m,n\in\mathbb{F}_q^2\\ m_1m_2=n_1n_2}}|\hat{E}(m)|^2\hat{E}(n)|^2\leq\left(\sum_m|\hat{E}(m)|^2\right)^2=\frac{|E|^2}{q^4}.$$

Therefore

$$\sum_j A(j)^2\ll\frac{|E|^4}{q}+|E|^3+q^2|E|^2.$$

We get

$$\Omega(E)\gg\frac{|E|^4}{\frac{|E|^4}{q}+|E|^3+q^2|E|^2}$$

and the theorem follows.

Application. Suppose $A\subset\mathbb{F}_q$. Let $E=A\times A$, then $\Omega(E)=(A-A)(A-A)$. Applying the last theorem we get:

$$\text{If } |A|\gg q^{3/4},\quad \text{then } |(A-A)(A-A)|\gg q.$$

7. Connection to Restriction Theory Over Finite Fields

For a subset S of $F=\mathbb{F}_q^d$ and a complex valued function g on S, we define

$$\|g\|_{L^p(S)}=\left(\sum_{\xi\in S}|g(\xi)|^p\right)^{1/p}.$$

We also define $\check{g}$ to be a function on $\mathbb{F}_q^d$ by

$$\check{g}(x)=\sum_{\xi\in S}g(\xi)\psi(x\cdot\xi).$$

For any two exponents p,q, $1\leq p,q\leq\infty$. The function $g\to\check{g}$ is a linear transformation between $L^p(S)$ and $L^q(F)$.

Let $R_S(p \to q)$ be the smallest real number satisfying

$$\|\check{g}\|_{L^q(F)} \leq R_S(p \to q)\|g\|_{L^p(S)}$$

for all function g on S. By duality for all function $f \in L^{q'}(F)$

$$\|\hat{f}\|_{L^{p'}(S)} \leq R_S(p \to q)\|f\|_{L^p(F)}.$$

Now we consider $f = E$, indicator function of the set $E \subset \mathbb{F}_q^d$ and let S_k denote the circle of radius k.

We note that

$$\begin{aligned}\sum_{\substack{m_1,m_2\in\mathbb{F}_q^d\setminus\{0\}\\ |m_1|^2=|m_2|^2}} |\hat{E}(m_1)|^2|\hat{E}(m_2)|^2 &= \sum_{k\in\mathbb{F}_q^*}\left(\sum_{|m|^2=k}|\hat{E}(m)|^2\right)^2\\ &= \sum_{k\in\mathbb{F}_q^*}\|\hat{E}\|^4_{L^2(S_k)}\\ &\leq \sum_{k\in\mathbb{F}_q^*} R_{S_k}(2\to 2)^4\|E\|^4_{L^2(\mathbb{F}_q^d)}\\ &= \frac{|E|^2}{q^{2d}}\sum_{k\in\mathbb{F}_q^*} R_{S_k}(2\to 2)^4.\end{aligned}$$

Hence analog of Erdös distance conjecture for $\mathbb{F}_q$ follows if

$$\sum_{k\in\mathbb{F}_q^*} R_{S_k}(2\to 2)^4 \ll \frac{1}{q}.$$

Presently we do not have any heuristic to support this assertion.

References

[1] M. Bennett, D. Hart, A. Iosevich, J. Pakianathan and M. Rudnev, Group actions and geometric combinatorics in $\mathbb{F}_q^d$, *Forum Math.* **29**(1) (2017) 91–110.

[2] E. R. Berlekamp, *Algebraic Coding Theory* (McGraw-Hill, 1968).

[3] D. Hart, A. Iosevich and J. Solymosi, Sum-product estimates in finite fields via Kloosterman sums, *Int. Math. Res. Notices*, **2007**(5) (2007), Article ID: rnm007.

[4] A. Iosevich and D. Koh, 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**(1) (2008) 123–135.

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

[6] D. Koh and C.-Y. Shen, The generalized Erdös–Falconer distance problems in vector spaces over finite fields, *J. Number Theory* **132** (2012) 2455–2473.

[7] L. A. Vinh, Explicit Ramsey graphs and Erdös distance problem over finite Euclidean and non-Euclidean spaces, *Electron. J. Combin.* **15**(1) (2008), Research Paper 5, 18 pp.