

Pinned distance sets, Wolff's exponent in finite fields and improved sum-product estimates

Derrick Hart and Alex Iosevich

April 29, 2008

Abstract

An analog of the Falconer distance problem in vector spaces over finite fields asks for the threshold $\alpha > 0$ such that $|\Delta(E)| \gtrsim q$ whenever $|E| \gtrsim q^\alpha$, where $E \subset \mathbb{F}_q^d$, the d -dimensional vector space over a finite field with q elements (not necessarily prime). Here $\Delta(E) = \{(x_1 - y_1)^2 + \cdots + (x_d - y_d)^2 : x, y \in E\}$. The second listed author and Misha Rudnev ([4]) established the threshold $\frac{d+1}{2}$, and in [3] the authors of this paper, Doowon Koh and Misha Rudnev proved that this exponent is sharp in even dimensions. In this paper we improve the threshold to $\frac{d^2}{2d-1}$ under the additional assumption that E has product structure. In particular, we obtain the exponent $\frac{4}{3}$, consistent with the corresponding exponent in Euclidean space obtained by Wolff ([9]).

1 Introduction

1.1 Distance sets

The classical Erdős distance problem asks for the minimal number of distinct distances determined by a finite point set in \mathbb{R}^d , $d \geq 2$. The continuous analog of this problem, called the Falconer distance problem asks for the optimal threshold such that the set of distances determined by a subset of \mathbb{R}^d , $d \geq 2$, of larger dimension has positive Lebesgue measure. It is conjectured that a set of N points in \mathbb{R}^d , $d \geq 2$, determined $\gtrsim N^{\frac{2}{d}}$ distances and, similarly, that a subset of \mathbb{R}^d , $d \geq 2$, of Hausdorff dimension greater than $\frac{d}{2}$ determines a set of distance of positive Lebesgue measure. Neither problem is close to being completely solved. See [5] and [7], and the references contained therein, on the latest developments on the Erdős distance problem. See [2] and the references contained therein for the best known exponents for the Falconer distance problem.

In vector spaces over finite fields, one may define for $E \subset \mathbb{F}_q^d$,

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

where

$$||x - y|| = (x_1 - y_1)^2 + \cdots + (x_d - y_d)^2,$$

and one may again ask for the smallest possible size of $\Delta(E)$ in terms of the size of E . There are several issues to contend with here. First, E may be the whole vector space, which would result in the rather small size for the distance set:

$$|\Delta(E)| = |E|^{\frac{1}{d}}.$$

Another annoying consideration is that if q is a prime congruent to 1 mod (4), then there exists $i \in \mathbb{F}_q$ such that $i^2 = -1$. This allows us to construct a set

$$Z = \{(t, it) : t \in \mathbb{F}_q\}$$

and one can readily check that

$$\Delta(Z) = \{0\}.$$

The first result in this direction is proved in [1]. The authors get around the first mentioned obstruction by assuming that $|E| \lesssim q^{2-\epsilon}$ for some $\epsilon > 0$. They get around the second mentioned obstruction by mandating that q is a prime $\equiv 3 \pmod{4}$. As a result they prove that

$$|\Delta(E)| \gtrsim |E|^{\frac{1}{2}+\delta},$$

where δ is a function of ϵ .

In [4] the second author along with M. Rudnev went after a distance set result for general fields in arbitrary dimension with explicit exponents. In order to deal with the obstructions outlined above, they reformulated the question in analogy with the Falconer distance problem: how large does $E \subset \mathbb{F}_q^d$, $d \geq 2$, need to be to ensure that $\Delta(E)$ contains a positive proportion of the elements of \mathbb{F}_q . They proved that if $|E| \geq 4q^{\frac{d+1}{2}}$, then $\Delta(E) = \mathbb{F}_q$. At first, it seemed reasonable that the exponent $\frac{d+1}{2}$ may be improvable, in line with the Falconer distance conjecture described above. However, the authors along with D. Koh and M. Rudnev discovered in [3] that the arithmetic of the problem makes the exponent $\frac{d+1}{2}$ best possible in **odd dimensions**, at least in general fields. In even dimensions it is still possible that the correct exponent is $\frac{d}{2}$, in analogy with the Euclidean case.

The example that shows that the $\frac{d+1}{2}$ is sharp in odd dimensions is very radial in nature and this led the authors of this paper to consider classes of sets that possess a certain amount of product structure. In particular, we shall that if $|E| \subset \mathbb{F}_q^2$ satisfies $|E| \geq Cq^{\frac{4}{3}}$ and E is a product set, then $|\Delta(E)| \geq cq$. This is in line with Wolff's result for the Falconer conjecture in the plane which says that the Lebesgue measure of the set of distances determined by a subset of the plane of Hausdorff dimension greater than $\frac{4}{3}$. In higher dimensions we shall obtain a positive proportion of the distances for products sets of size $\gtrsim q^{\frac{d^2}{2d-1}}$, improving an analog of Erdogan's ([2]) exponent in Euclidean space for general sets.

1.2 Pinned distance sets

Let $\pi_j(x) = (x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_d)$ and define

$$E_z^j = \pi_j(E) \times \{z\},$$

where z is an element of

$$\{z \in \mathbb{F}_q : (x_1, x_2, \dots, x_{j-1}, z, x_{j+1}, \dots, x_d) \in E\}.$$

Define

$$\Delta_z^j(E) = \{||x - y|| : x \in E, y \in E_z^j\}.$$

Our first main result is the following.

Theorem 1.1. *Let $E \subset \mathbb{F}_q^d$ and let E_z^j be defined with respect to a projection π_j , for some $1 \leq j \leq d$ and an element $z \in \{z \in \mathbb{F}_q : (x_1, x_2, \dots, z, x_{j+1}, \dots, x_d) \in E\}$ as above. Suppose that*

$$|E||E_z^j| \geq Cq^d.$$

Then

$$|\Delta_z^j(E)| \geq q \frac{3C}{3C+1}. \quad (1.1)$$

Observe that if E is a product set, then $\Delta_z^j(E) \subset \Delta(E)$. This leads us to the following consequence of Theorem 1.1.

Corollary 1.2. *Suppose that $E = E_1 \times E_2 \times \dots \times E_d$, where E_j is contained in \mathbb{F}_q . Suppose that*

$$|E| \geq Cq^{\frac{d^2}{2d-1}}.$$

Then

$$|\Delta(E)| \geq q \frac{3C}{3C+1}.$$

The Corollary follows immediately from Theorem 1.1 since, after perhaps relabeling some coordinates, we may assume, using straightforward pigeon-holing, that $E = E' \times E''$, where $E' \subset \mathbb{F}_q^{d-1}$ and $|E'| \geq |E|^{\frac{d-1}{d}}$. Observe that we could have made a much weaker, though more technical, assumption on the structure of E . We shall attempt to classify this notion in a precise way in a subsequent paper.

1.3 Sums and products

A related question that has recently been attacked using a similar Fourier-geometric framework is the problem of sums and products in \mathbb{F}_q in the following form. Let $A \subset \mathbb{F}_q$. How large does A need to be to ensure that

$$\mathbb{F}_q^* \subset A \cdot A + A \cdot A,$$

or, more modestly,

$$|A \cdot A + A \cdot A| \geq cq$$

for some $c > 0$.

The authors of this paper have recently proved the following result.

Theorem 1.3. *Let $A \subset \mathbb{F}_q$.*

- *If $|A| > q^{\frac{3}{4}}$, then*

$$\mathbb{F}_q^* \subset A \cdot A + A \cdot A.$$

- *If $|A| \geq C_{size}^{\frac{1}{2}} q^{\frac{2}{3}}$, then*

$$|A \cdot A + A \cdot A| \geq q \frac{C_{size}^{\frac{3}{2}}}{1 + C_{size}^{\frac{3}{2}}}.$$

We use the method of proof of Theorem 1.1 above to obtain the following.

Theorem 1.4. *Let $E \subset \mathbb{F}_q^d$ and let E_z^j be defined as above. Then*

$$|\{x \cdot y : x \in E_z, y \in E\}| \geq q \frac{2C}{2C + 1} \tag{1.2}$$

whenever

$$|E_z^j| |E| \geq Cq^d.$$

Setting $E = A \times A \times A$, we obtain the following consequence recently obtained by Shparlinski ([6]) in the case $d = 2$.

Corollary 1.5. *Let A, B be subsets of \mathbb{F}_q . Suppose that*

$$|A| \geq C^{\frac{1}{3}} q^{\frac{2}{3}}.$$

Then for any $z \in A$,

$$|A \cdot A + zA| \geq \frac{2C}{2C + 1} q.$$

2 Proof of Theorem 1.1

We drop the exponent j in the sequel for the sake of convenience. Define

$$\nu(t) = |\{(x, y) \in E_z \times E : \|x - y\| = t\}|,$$

where, as usual

$$\|x\| = x_1^2 + \cdots + x_d^2.$$

By Cauchy-Schwartz,

$$\nu^2(t) \leq |E_z| \cdot \sum_{\|x-y\|=\|x-y'\|=t} E_z(x)E(y)E(y'),$$

so

$$\begin{aligned} \sum_t \nu^2(t) &\leq |E_z| \cdot \sum_{\|x-y\|=\|x-y'\|} E_z(x)E(y)E(y') \\ &= q^{-1}|E_z| \cdot \sum_s \sum_{x,y,y'} \chi(s(\|x-y\| - \|x-y'\|)) E_z(x)E(y)E(y') \\ &= q^{-1}|E_z|^2|E|^2 + R, \end{aligned}$$

and

$$R = q^{-1}|E_z| \sum_{s \neq 0} \sum_{x \in E_z} \left| \sum_{y \in E} \chi(s(\|y\| - 2x \cdot y)) \right|^2,$$

since

$$\|x - y\| - \|x - y'\| = (\|y\| - 2x \cdot y) - (\|y'\| - 2x \cdot y').$$

It follows that

$$\begin{aligned} R &\leq q^{-1}|E_z| \sum_{s \neq 0} \sum_{x \in \mathbb{F}_q^{d-1} \times \{z\}} \sum_{y,y' \in E} \chi(-2sx \cdot (y - y')) \chi(s(\|y\| - \|y'\|)) \\ &= q^{d-2}|E_z| \sum_{s \neq 0} \sum_{\pi_d(y)=\pi_d(y')} E(y)E(y') \chi(-2sz(y_d - y'_d)) \chi(s(y_d^2 - y'^2_d)) \\ &= q^{d-2}|E_z| \sum_s \sum_{\pi_d(y)=\pi_d(y')} E(y)E(y') \chi(-2sz(y_d - y'_d)) \chi(s(y_d^2 - y'^2_d)) \\ &\quad - q^{d-2}|E_z| \sum_{\pi_d(y)=\pi_d(y')} E(y)E(y') = A - B. \end{aligned}$$

Now,

$$B \leq q^{d-2}|E_z||E|q = q^{d-1}|E_z||E|$$

because one coordinate can contribute at most a factor of q . On the other hand,

$$\begin{aligned}
A &= q^{d-1}|E_z| \cdot \sum_{2z(y_d - y'_d) = y_d^2 - y'^2_d; \pi_d(y) = \pi_d(y')} E(y)E(y') \\
&= q^{d-1}|E_z| \cdot \sum_{2z = y_d + y'_d; y_d \neq y'_d; \pi_d(y) = \pi_d(y')} E(y)E(y') \\
&\quad + q^{d-1}|E_z| \sum_{y=y'} E(y)E(y') \\
&\leq 2q^{d-1}|E_z||E|.
\end{aligned}$$

2.1 Conclusion of the proof:

We have

$$\begin{aligned}
|E|^2|E_z|^2 &= \left(\sum_t \nu(t) \right)^2 \leq |\Delta_z(E)| \cdot \sum_t \nu^2(t) \\
&\leq |\Delta_z(E)| \cdot (|E|^2|E_z|^2 q^{-1} + 3q^{d-1}|E_z||E|).
\end{aligned}$$

It follows that

$$|\Delta_z(E)| \geq cq$$

if

$$|E||E_z| \geq Cq^d.$$

3 Proof of Theorem 1.4

Without loss of generality that $j = d$ in the argument below. Consider the incidence function

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

Then

$$\begin{aligned}
\sum_t \nu^2(t) &\leq |E_z| \sum_{x \cdot y = x \cdot y'} E_z(x)E(y)E(y') \\
&= |E_z|^2|E|^2 q^{-1} + |E_z| q^{-1} \sum_{s \neq 0} \sum_{\substack{x \in E_z \\ y, y' \in E}} \chi(sx \cdot (y - y')) \\
&= I + II
\end{aligned}$$

Now

$$\begin{aligned}
II &= |E_z|q^{-1} \sum_{s \neq 0} \sum_{x \in E_z} \left| \sum_{y \in E} \chi(sx \cdot y) \right|^2 \\
&\leq |E_z|q^{-1} \sum_{s \neq 0} \sum_{x \in \mathbb{F}_q^{d-1} \times \{z\}} \left| \sum_{y \in E} \chi(sx \cdot y) \right|^2 \\
&= |E_z|q^{d-2} \sum_{s \neq 0} \sum_{\pi_d(y) = \pi_d(y')} \chi(sz(y_d - y'_d)) E(y) E(y') \\
&= |E_z| |E| q^{d-1} - |E_z| q^{d-2} \sum_{\pi_d(y) = \pi_d(y')} E(y) E(y') \\
&= A - B.
\end{aligned}$$

We conclude that

$$B \leq |E_z| |E| q^{d-1},$$

which implies that

$$|II| \leq 2|E| |E_z| q^{d-1}$$

and

$$\sum_t \nu^2(t) \leq |E_z|^2 |E|^2 q^{-1} + 2|E| |E_z| q^{d-1},$$

and the conclusion follows in the same way as in the proof of Theorem 1.1.

References

- [1] J. Bourgain, N. Katz, and T. Tao, *A sum-product estimate in finite fields, and applications* Geom. Funct. Anal. **14** (2004), 27-57.
- [2] B. Erdoğın *A bilinear Fourier extension theorem and applications to the distance set problem* IMRN (accepted for publication) (2005).
- [3] D. Hart, A. Iosevich, D. Koh and M. Rudnev *Averages over hyperplanes, sum-product theory in vector spaces over finite fields and the Erdős-Falconer distance conjecture*, submitted for publication (2007).
- [4] A. Iosevich and M. Rudnev. *Erdős distance problem in vector spaces over finite fields*. Trans. Amer. Math. Soc. (2007).
- [5] N. Katz and G. Tardos *A new entropy inequality for the Erdős distance problem* Contemp. Math. **342**, Towards a theory of geometric graphs, 119-126, Amer. Math. Soc., Providence, RI (2004).
- [6] I. Shparlinski, *On The Solvability of Bilinear Equations in Finite Fields*. (preprint), (2007)
- [7] J. Solymosi and V. Vu *Near optimal bounds for the number of distinct distances in high dimensions* Combinatorica (2005).
- [8] T. Wolff *Lecture notes on harmonic analysis. With a foreword by C. Fefferman and preface by I. Łaba. Edited by I. Łaba and C. Shubin*. University Lecture Series, **29**. American Mathematical Society, Providence, RI, 2003.
- [9] T. Wolff, *Decay of circular means of Fourier transforms of measures*, Internation Math Research Notices, **10**, 547-567, (1999).