

AN EXAMPLE RELATED TO THE ERDŐS–FALCONER QUESTION OVER ARBITRARY FINITE FIELDS

BRENDAN MURPHY AND GIORGIS PETRIDIS

ABSTRACT. There exists an infinite family of examples of subsets of \mathbb{F}_q^2 with $q^{4/3}$ elements whose distance sets are not the whole of \mathbb{F}_q .

1. INTRODUCTION

Iosevich and Rudnev were the first to investigate in [6] the Erdős–Falconer distance set question ([2, 3]) over finite fields. In this context distance is defined algebraically and the *distance set* of a set E is

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

The *distance number* of E is $|\Delta(E)|$. Iosevich and Rudnev studied large subsets of vector spaces over finite fields and sought to find a condition on the cardinality of the subset that guarantees that its distance set is the entire finite field. They proved the following lower bound (\mathbb{F}_q denotes a finite field of q elements).

Theorem 1.1 (Iosevich–Rudnev). *For all $d \geq 2$ and all odd q , if $E \subseteq \mathbb{F}_q^d$ satisfies $|E| > 4q^{(d+1)/2}$, then $\Delta(E) = \mathbb{F}_q$.*

The exponent $(d + 1)/2$ cannot be improved for odd dimensions d . Hart, Iosevich, Koh, and Rudnev proved in [5] that there exists an absolute $c > 0$ and subsets $E \subset \mathbb{F}_q^d$ for any odd d , such that $|E| \geq cq^{(d+1)/2}$ and $\Delta(E) \neq \mathbb{F}_q$. Theorem 1.1 remains the state-of-the-art for even d .

In this short note, we construct an infinite family of examples for $d = 2$, which shows that the exponent in Theorem 1.1 must be at least as big as $4/3$. Our examples disprove Conjecture 1.1 in [6] for $d = 2$.

Theorem 1.2. *Let p be a prime. There exist infinitely many powers q of p and a subset $E \subset \mathbb{F}_q^2$ such that $|E| = q^{4/3}$ and $\Delta(E) \neq \mathbb{F}_q$. In fact, as $q \rightarrow \infty$, $|\Delta(E)|/q \leq 1/2$.*

The construction is very similar to a construction in [7]. Some remarks.

- (1) The examples in Theorem 1.2 stem from properties of vector spaces over subfields. This means that they cannot be extended to prime order fields. They show that vector spaces over subfields (and not only subfields) can obstruct growth in geometric questions.

Date: Received 13 May 2019. Accepted 16 May 2019.

2010 Mathematics Subject Classification. 11B30.

Key words and phrases. distance sets, finite fields.

The first author is supported by the Leverhulme grant RPG 2017-371. The second author is supported by the NSF Award 1723016 and gratefully acknowledges the support from the RTG in Algebraic Geometry, Algebra, and Number Theory at the University of Georgia, and from the NSF RTG grant DMS-1344994.

- (2) The examples in Theorem 1.2 complement results in [1, 4], which show that if $E \subseteq \mathbb{F}_q^2$ and $|E| > q^{4/3}$, then both the distance number and the, intuitively defined, pinned distance number of E is a constant multiple of q . Theorem 1.2 shows that for such E $\Delta(E)$ does not always contain, say, 99% of the elements of \mathbb{F}_q .
- (3) Theorem 1.2 does not rule out the existence of a positive $\delta > 0$ with the property that, for all sufficiently large q , any $E \subseteq \mathbb{F}_q^2$ with $|E| > q^{4/3-\delta}$ elements satisfies $|\Delta(E)| > q/2$. A result along these lines was proved in [7] for an analogous question.

2. PROOF OF THEOREM 1.2

We prove Theorem 1.2 for odd primes p that are congruent to 3 modulo 4. The cases where $p = 2$ or p is congruent to 1 modulo 4 are similar.

We start with \mathbb{F}_p and adjoin a square root of -1 , denoted by i , to get the quadratic extension $\mathbb{F}_p[i]$. Let F be any finite extension of $\mathbb{F}_p[i]$ and \mathbb{F}_q be any cubic extension of F . In other words we may take $q = p^{6r}$ for every positive integer r .

Consider \mathbb{F}_q as a vector space over F and let V be any 2-dimensional vector subspace. It is shown in [7, Proposition 11] that $VV \neq \mathbb{F}_q$ and that $|VV|/q \rightarrow 1/2$ as (r and hence) $q \rightarrow \infty$.

We are now in position to describe E . Set

$$E = \{(u, iv) : u, v \in V\} \subset \mathbb{F}_q^2.$$

Finally note that, because of closure of V under addition and subtraction,

$$\begin{aligned} \Delta(E) &= \{(u_1 - u_2)^2 + (iv_1 - iv_2)^2 : u_1, u_2, v_1, v_2 \in V\} \\ &= \{u^2 - v^2 : u, v \in V\} \\ &= \{(u - v)(u + v) : u, v \in V\} \\ &\subseteq VV. \end{aligned}$$

Therefore $\Delta(E) \neq \mathbb{F}_q$ while $|E| = |V|^2 = |F|^4 = q^{4/3}$.

Note that when q is odd we have $\Delta(E) = VV$.

REFERENCES

- [1] J. Chapman, M. B. Erdoğan, D. Hart, A. Iosevich, and D. Koh. Pinned distance sets, k -simplices, Wolff's exponent in finite fields and sum-product estimates. *Math. Z.*, 271(1-2):63–93, 2012.
- [2] P. Erdős. On sets of distances of n points. *Amer. Math. Monthly*, 53:248–250, 1946.
- [3] K. J. Falconer. On the Hausdorff dimensions of distance sets. *Mathematika*, 32:206–212, 1985.
- [4] B. Hanson, B. Lund, and O. Roche-Newton. On distinct perpendicular bisectors and pinned distances in finite fields. *Finite Fields Appl.*, 37:240–264, 2016.
- [5] 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. *Trans. Amer. Math. Soc.*, 363:3255–3275, 2011.
- [6] A. Iosevich and M. Rudnev. Erdős distance problem in vector spaces over finite fields. *Trans. Amer. Math. Soc.*, 359:6127–6142, 2007.
- [7] B. Murphy and G. Petridis. Products of differences over arbitrary finite fields. *Discrete Analysis*, 18:42 pp., 2018.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRISTOL, AND HEILBRONN INSTITUTE OF MATHEMATICAL RESEARCH, BRISTOL, UK.

E-mail address: brendan.murphy@bristol.ac.uk

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF GEORGIA, ATHENS, GA 30602, USA.

E-mail address: giorgis@cantab.net