

ON THE NUMBER OF DOT PRODUCTS DETERMINED BY A LARGE SET AND ONE OF ITS TRANSLATES IN FINITE FIELDS

GIORGIS PETRIDIS

ABSTRACT. Let $E \subseteq \mathbb{F}_q^2$ be a set in the 2-dimensional vector space over a finite field with q elements, which satisfies $|E| > q$. There exist $x, y \in E$ such that $|E \cdot (y - x)| > q/2$. In particular, $(E + E) \cdot (E - E) = \mathbb{F}_q$.

1. INTRODUCTION

The question of determining a lower bound on the cardinality of a set $E \subseteq \mathbb{F}_q^2$ in a 2-dimensional vector space over a finite field \mathbb{F}_q with q elements, which guarantees that the set of dot products determined by E has cardinality strictly greater than $q/2$, goes back at least as far as a paper of Hart and Iosevich [7]. By the *set of dot products determined by E* we mean the following subset of \mathbb{F}_q :

$$E \cdot E = \{u \cdot v : u, v \in E\}.$$

Hart and Iosevich proved that if $|E| > q^{3/2}$, then $E \cdot E = \mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$, with the exponent of $3/2$ in the lower bound for $|E|$ being essentially sharp (see Corollary 2.4 in [8]). For similar results in higher dimensions see [4].

An analogous result was proved in the context of geometric measure theory by Erdoğan, Hart, and Iosevich [5]. The authors showed that if a planar set $E \subset \mathbb{R}^2$ has Hausdorff dimension $\dim_H(E) > 3/2$, then the set $E \cdot E \subset \mathbb{R}$ has positive Lebesgue measure. The result can loosely be interpreted as saying that the set of dot products determined by a “large” planar set is “large”.

The same argument shows that if $\dim_H(E) > 1$, there exists $x \in E$ such that the set

$$E \cdot (E - x) = \{u \cdot (v - x) : u, v \in E\}$$

has positive Lebesgue measure.

Recently, in a breakthrough paper on the Falconer conjecture, Orponen established a similar result. If $E \subset \mathbb{R}^2$ is an Ahlfors-David regular planar set with Hausdorff dimension $\dim_H(E) \geq 1$, then there exists $x \in E$ such that $E \cdot (E - x)$ has packing dimension equal to 1 [13].

Date: June 16, 2017.

1991 Mathematics Subject Classification. 11T99.

Key words and phrases. Finite fields, dot products.

The author is supported by the NSF DMS Grant 1500984.

We prove an analogous result in the context of 2-dimensional vector spaces over finite fields. In fact our result concerns “pinned” dot products.

Theorem 1.1. *Let $E \subseteq \mathbb{F}_q^2$ be a set in the 2-dimensional vector space over a finite field with q elements. Suppose that $|E| > q$. There exist $x, y \in E$ such that*

$$|E \cdot (y - x)| = |\{u \cdot (y - x) : u \in E\}| > \frac{q}{2}.$$

The lower bound is sharp. If $q = p^2$ is the square of a prime p and E is the Cartesian product of a subfield isomorphic to \mathbb{F}_p , then $|E| = p^2 = q$ and $|E \cdot (y - x)| = p = \sqrt{q}$ for all $x, y \in E$.

It is likely that one could prove the existence of $x \in E$ such that $|E \cdot (E - x)| > q/2$ provided that $|E| = \Omega(\sqrt{q} \log(q))$ by combining Theorem 2 in [11] with Theorem 2.6 in [8]. Our proof is different. The advantage of proving a result about “pinned” dot products is illustrated in the following corollary.

Corollary 1.2. *Let $E \subseteq \mathbb{F}_q^2$ be a set in the 2-dimensional vector space over a finite field with q elements. Suppose that $|E| > q$. There exist $x, y \in E$ such that*

$$\mathbb{F}_q = (E + E) \cdot (y - x) = \{(u + v) \cdot (y - x) : u, v \in E\}.$$

In particular

$$\mathbb{F}_q = (E + E) \cdot (E - E) = \{(u + v) \cdot (z - w) : u, v, z, w \in E\}.$$

When $E = A \times A$ for a symmetric set A (that is, $-A = A$), we recover a result of Glibichuk from [6] that asserts that the 8-fold sumset of AA is the whole of \mathbb{F}_q provided that $|A| > \sqrt{q}$:

$$(1) \quad \mathbb{F}_q = \{a_1 a_2 + a_3 a_4 + \cdots + a_{15} a_{16} : a_1, \dots, a_{16} \in A\}.$$

We conclude the introduction with a short detour on a similar question. As mentioned above, Hart, Iosevich, Koh, and Rudnev showed in [8] that the lower bound $q^{3/2}$ is essentially optimal if we require $E \cdot E$ to be a positive proportion of \mathbb{F}_q . Their example is the union of half-lines and so tells us little about the case where $E = A \times A$ is a Cartesian product. When $E = A \times A$ is a Cartesian product, the set of dot products takes the form $AA + AA$. Bounding from below $|AA + AA|$ has received much attention in the literature and is worth summarising.

(1) Hart and Iosevich proved in [7] that

$$|AA + AA| = \Omega \left(\min \left\{ q, \frac{|A|^3}{q} \right\} \right).$$

A more precise result they proved is that $|AA + AA| > q/2$ when $|A| > q^{2/3}$.

(2) When A is a multiplicative subgroup of \mathbb{F}_q^* we have $AA + AA = A + A$. Heath-Brown and Konyagin proved in [9] the following lower bound for multiplicative

subgroups of prime order fields (we replace q by p for clarity) via an elegant application of Stepanov's method

$$|A + A| = \Omega\left(\min\{p, |A|^{3/2}\}\right).$$

Shkredov and Vyugin improved the lower bound at the cost of the additional assumption $|A| = O(p^{1/2})$ in [16]

$$|A + A| = \Omega(|A|^{5/3} \log(|A|)^{-1/2}).$$

Shkredov recently proved in [15] that under the same hypothesis $|A| = O(p^{1/2})$

$$|A + A + A| = \Omega(|A|^2 / \log(|A|)).$$

This corresponds to $E \cdot E$ for $E = A \times A \times A \subset \mathbb{F}_q^3$.

- (3) Rudnev in [14] generalised the Heath-Brown and Konyagin lower bound to all sets in a prime order field

$$|AA + AA| = \Omega\left(\min\{p, |A|^{3/2}\}\right).$$

It is likely that $AA + AA$ is at least, say, half of \mathbb{F}_q^* for any set A of cardinality a sufficiently large multiple of \sqrt{q} , at least for prime q .

In the next section we offer an overview of the proof of Theorem 1.1 and prove the necessary lemmata. In the final section we prove Theorem 1.1 and Corollary 1.2.

2. FIRST AND SECOND MOMENT CALCULATIONS

The proof of Theorem 1.1 consists of two distinct parts. Before describing them, let us set up some notation. To a direction $\theta \in \mathbb{F}_q \cup \{\infty\}$ we associate the direction vector v_θ , which equals $(1, \theta)$ if $\theta \in \mathbb{F}_q$ and $(0, 1)$ if $\theta = \infty$. A direction $\theta \in \mathbb{F}_q \cup \{\infty\}$ is determined by a set $E \subseteq \mathbb{F}_q^2$ if there exists $\lambda \in \mathbb{F}_q^*$ such that $\lambda v_\theta \in E$.

The two steps of the proof are as follows.

- (1) Let E, F be two sets in \mathbb{F}_q^2 . Suppose that $|E| > q$ and that F determines all directions in $\mathbb{F}_q \cup \{\infty\}$. There exists $v \in F$ such that

$$|E \cdot v| = |\{u \cdot v : u \in E\}| > \frac{q}{2}.$$

- (2) Let E be a set in \mathbb{F}_q^2 . Suppose that $|E| > q$. Every direction in $\mathbb{F}_q \cup \{\infty\}$ is determined by E . This is a result of Iosevich, Morgan, and Pakianathan (Theorem 2 in [10]). It was proved in the case where $E = A \times B$ is a Cartesian product by Bourgain, Glibichuk, and Konyagin in [2].

The first step can be thought of as a discrete version of a classical theorem of Marstrand about projections in Euclidean space [12] and will be proved by a simple second moment calculation. The second step will be proved by an application of the pigeonhole principle.

2.1. The second moment of a point-line incidence function. Given two sets $E, F \in \mathbb{F}_q^2$ and $t \in F$, there exist $u \in E$ and $v \in F$ such that $u \cdot v = t$ precisely when E is incident to the line $\{w \in \mathbb{F}_q^2 : w \cdot v = t\}$. To motivate the proof of the first step outlined above, suppose for a contradiction that F determines $\Omega(q)$ directions and that $|\mathbb{F}_q \setminus (E \cdot F)| = \Omega(q)$. It follows that $|E|$ is not incident to $\Omega(q^2)$ lines. To show that this is impossible when $|E| = \Omega(q)$ we will prove that “ E is incident to most lines roughly the expected number of times”.

To this end we denote by $i(\ell)$ the number of incidences of a line $\ell \subseteq \mathbb{F}_q^2$ with E

$$(2) \quad i_E(\ell) = i(\ell) = |\ell \cap E|.$$

There are $q(q+1)$ lines in \mathbb{F}_q^2 ($q+1$ possible slopes and q possible y -axis intercepts) and $|E|(q+1)$ point-line incidences between E and the set of all lines with slope in \mathbb{F}_q (there are $q+1$ lines incident to each point of E). Therefore, on average a line is incident to $|E|/q$ points from E . We show that this is typically a very good estimate by obtaining an exact expression for the second moment of $i(\ell)$.

Lemma 2.1. *Let $E \subseteq \mathbb{F}_q^2$ and i be the function defined in (2).*

$$\sum_{\ell} i(\ell)^2 = |E|^2 + q|E|.$$

The sum is over all lines in \mathbb{F}_q^2 .

A few remarks before we prove this lemma. It asserts in probabilistic language that $\text{Var}[i] \leq \mathbb{E}[i]$ and is based on the fact a collection of lines in \mathbb{F}_q^2 is a pseudorandom collection of subsets. It is a generalisation of Lemma 2.1 of Bourgain, Katz, and Tao from [3]. The authors considered the case where $E = A \times B$ is a Cartesian product. It is also very close to a point-line incidence theorem of Vinh [17].

Proof of Lemma 2.1. Sums are over all lines in \mathbb{F}_q^2 . We denote by ℓ the characteristic function of a line ℓ .

$$\begin{aligned} \sum_{\ell} i(\ell)^2 &= \sum_{\ell} \left(\sum_{v \in E} \ell(v) \right)^2 \\ &= \sum_{\ell} \sum_{v, v' \in E} \ell(v) \ell(v') \\ &= \sum_{v \in E} \sum_{\ell} \ell(v) + \sum_{v \neq v' \in E} \sum_{\ell} \ell(v) \ell(v') \\ &= |E|(q+1) + |E|(|E| - 1) \\ &= |E|^2 + q|E|. \end{aligned}$$

In the penultimate line we used the facts that $q+1$ lines are incident to a point and that two distinct points determine a unique line. \square

2.2. Many directions give a good vector to project on. Deducing the first step outlined at the beginning of the section is now only a matter of labelling lines, averaging, and applying the Cauchy-Schwarz inequality.

Corollary 2.2. *Let E, F be two sets in \mathbb{F}_q^2 . Suppose that $|E| > q$ and that F determines all directions in $\mathbb{F}_q \cup \{\infty\}$. There exists $v \in F$ such that*

$$|E \cdot v| = |\{u \cdot v : u \in E\}| > \frac{q}{2}.$$

Proof. We show that there exists $v \in F$ with the property that E is approximately equidistributed on the lines orthogonal to v . The conclusion follows in a straightforward manner by the Cauchy-Schwarz inequality.

For each direction $\theta \in \mathbb{F} \cup \{\infty\}$ let $v_\theta \in F$ be the vector that determines θ , described at the beginning of the section. Next label by $\ell_{\theta,t}$ the line $\{w \in \mathbb{F}^2 : w \cdot v_\theta = t\}$. Lemma 2.1 implies

$$\sum_{\theta \in \mathbb{F} \cup \{\infty\}} \sum_{t \in \mathbb{F}} i(\ell_{\theta,t})^2 = \sum_{\ell} i(\ell)^2 = |E|^2 + q|E| < 2|E|^2.$$

Therefore, noting that $i(\ell_{\theta,t}) = 0$ unless $t \in v_\theta \cdot E$, there exists $\theta \in \mathbb{F}$ such that

$$\sum_{t \in v_\theta \cdot E} i(\ell_{\theta,t})^2 = \sum_{t \in \mathbb{F}} i(\ell_{\theta,t})^2 < \frac{2|E|^2}{q}.$$

By the Cauchy-Schwarz inequality

$$\frac{2|E|^2}{q} > \sum_{t \in v_\theta \cdot E} i(\ell_{\theta,t})^2 \geq \frac{(\sum_{t \in v_\theta \cdot E} i(\ell_{\theta,t}))^2}{|v_\theta \cdot E|} = \frac{|E|^2}{|v_\theta \cdot E|},$$

which implies $|v_\theta \cdot E| > q/2$. Finally, $v_\theta = \lambda v$ for some $v \in F$ and $\lambda \in \mathbb{F}^*$ and so

$$|E \cdot v| = |\lambda(E \cdot v)| = |E \cdot (\lambda v)| = |E \cdot v_\theta| > q/2.$$

□

2.3. A result of Iosevich, Morgan, and Pakianathan. We now turn our attention to the second step outlined at the beginning of the section and prove the result of Iosevich, Morgan, and Pakianathan. The special case when $E = A \times B$ is a Cartesian product was proved by Bourgain, Glibichuk, and Konyagin (statement (9) in the proof of Theorem 3 in [2]). For completeness, we provide a proof communicated by Rudnev that is along the lines of the Bourgain, Glibichuk, and Konyagin. It should also be noted that considerations of Alon at the end of Section 4 of [1] imply a similar result.

Lemma 2.3 (Iosevich, Morgan, and Pakianathan, Theorem 2 in [10]). *Let E be a set in \mathbb{F}_q^2 . Suppose that $|E| > q$. The difference set $E - E = \{u - w : u, w \in E\}$ determines all directions in $\mathbb{F}_q \cup \{\infty\}$.*

Proof. Let θ be a direction in $\mathbb{F}_q \cup \{\infty\}$, v_θ be a vector determining it, and $\ell_\theta = \{\mu v_\theta : \mu \in \mathbb{F}_q\}$ a line with direction θ .

Note that $|E||\ell| > q^2$ and so the pairwise products $u + \mu v_\theta$ with $v \in E$ and $\mu \in \mathbb{F}_q$ cannot all be distinct. Therefore there exist distinct $u, w \in E$ and $\mu, \mu' \in \mathbb{F}_q$ such that $u + \mu v_\theta = w + \mu' v_\theta$ or equivalently $u - w = (\mu' - \mu)v_\theta$. In other words, $E - E$ determines the direction θ . \square

3. PROOFS OF THEOREM 1.1 AND COROLLARY 1.2

Proof of Theorem 1.1. The hypothesis $|E| > q$ and Lemma 2.3 every direction is determined by $E - E$. Corollary 2.2 and the hypothesis $|E| > q$ now imply there exists $y - x \in E - E$ such that $|E \cdot (y - x)| > q/2$. \square

Proof of Corollary 1.2. Let $S = E \cdot (y - x) \subseteq \mathbb{F}_q$. $|S| > q/2$ and so $S + S = \mathbb{F}_q$ (for each $\xi \in \mathbb{F}_q$, the sets S and $\xi - S$ must intersect because the sum of their cardinalities exceeds q). Therefore $\mathbb{F}_q = E \cdot (y - x) + E \cdot (y - x) = (E + E) \cdot (y - x)$. \square

When $E = A \times A$ we instantly get equality (1).

$$\begin{aligned} (E + E) \cdot (E - E) &= [(A + A) \times (A + A)] \cdot [(A - A) \times (A - A)] \\ &= (A + A)(A - A) + (A + A)(A - A) \\ &\subseteq AA - AA + AA - AA + AA - AA + AA - AA. \end{aligned}$$

Remark. *The arguments presented in this note highlight the importance of the direction set of E in dot-product related questions. They suggest that when looking to bound $|AA + AA|$ from below, the case where $E = A \times A$ for a multiplicative subgroup $A \subseteq \mathbb{F}_q^*$ might, in a sense, be extremal.*

ACKNOWLEDGEMENTS

The research for this work was completed while the author was working at the University of Rochester. The author would like to thank Alex Iosevich, Jonathan Pakianathan, and Misha Rudnev for helpful conversations. Misha Rudnev suggested using Lemma 2.3, which simplified the original argument and yielded the optimal lower bound on $|E|$ in Theorem 1.1.

REFERENCES

- [1] N. Alon, *Eigenvalues, geometric expanders, sorting in rounds, and Ramsey theory*, *Combinatorica* 6 (2004), pp. 207–219.
- [2] J. Bourgain, A. A. Glibichuk, and S. V. Konyagin, *On a variant of sum-product estimates and explicit exponential sum bounds in prime fields*, *Math. Proc. Camb. Phil. Soc.* 146 (2006), pp. 1–21.
- [3] J. Bourgain, N. H. Katz, and T. Tao, *A sum-product estimate in finite fields, and applications*, *Geom. Funct. Anal.* 14 (2004), pp. 27–57.
- [4] 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 (2012), pp. 63–93.

- [5] M. B. Erdoğan, D. Hart, and A. Iosevich, *Multiparameter projection theorems with applications to sums-products and finite point configurations in the Euclidean setting*, in *Recent Advances in Harmonic Analysis and Applications*, Springer NY, (2013), pp. 93–103.
- [6] A. A. Glibichuk, *Combinational properties of sets of residues modulo a prime and the Erdős–Graham problem*, *Mat. Zametki* 79 (2006), pp. 384–395.
- [7] D. Hart and A. Iosevich, *Sums and products in finite fields: an integral geometric viewpoint*, in *Radon Transforms, Geometry, and Wavelets*, AMS RI, (2008), pp. 129–136.
- [8] 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 (2011), pp. 3255–3275.
- [9] D. R. Heath-Brown and S. V. Konyagin, *New bounds for Gauss sums derived from k th powers, and for Heilbronn’s exponential sum*, *Q. J. Math.* 52 (2000), pp. 221–235.
- [10] A. Iosevich, H. Morgan and J. Pakianathan, *On directions determined by subsets of vector spaces over finite fields*, *Integers* 11 (2011), A39.
- [11] A. Iosevich, M. Rudnev and Y. Zhai, *Areas of triangles and Beck’s theorem in planes over finite fields*, *Combinatorica* 35 (2015), pp. 295–308.
- [12] J. M. Marstrand, *Some fundamental geometrical properties of plane sets of fractional dimensions*, *Proc. London Math. Soc.*(3) s3-4 (1954), pp. 257–302.
- [13] T. Orponen, *On the distance sets of Ahlfors–David regular sets*, *Adv. Math.* 307 (2017), pp. 1029–1045.
- [14] M. Rudnev, *On the number of incidences between planes and points in three dimensions*, *Combinatorica* (2017), pp.1–36.
- [15] I. D. Shkredov, *On tripling constant of multiplicative subgroups*, *Integers* 16 (2016), p. A75.
- [16] I. D. Shkredov and I. V. Vyugin, *On additive shifts of multiplicative subgroups*, *Sb. Math.* 203 (2012), pp. 844–863.
- [17] L. A. Vinh, *The Szemerédi–Trotter type theorem and the sum-product estimate in finite fields*, *European J. Combin.* 8 (201), pp. 1177–1181.

EXCEPT WHERE OTHERWISE NOTED, CONTENT IN THIS ARTICLE IS LICENSED UNDER A CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL LICENSE.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF GEORGIA, ATHENS, GA 30602, USA
E-mail address: giorgis@cantab.net