Bull. Aust. Math. Soc. **84** (2011), 1–9
doi:10.1017/S0004972709000537

ON SUM OF PRODUCTS AND THE ERDŐS DISTANCE PROBLEM OVER FINITE FIELDS

LE ANH VINH

(Received 25 February 2009)

Abstract

For a prime power q, let $\mathbb{F}_q$ be the finite field of q elements. We show that $\mathbb{F}_q^* \subseteq d\mathcal{A}^2$ for almost every subset $\mathcal{A} \subset \mathbb{F}_q$ of cardinality $|\mathcal{A}| \gg q^{1/d}$. Furthermore, if $q = p$ is a prime, and $\mathcal{A} \subseteq \mathbb{F}_p$ of cardinality $|\mathcal{A}| \gg p^{1/2}(\log p)^{1/d}$, then $d\mathcal{A}^2$ contains both large and small residues. We also obtain some results of this type for the Erdős distance problem over finite fields.

2000 *Mathematics subject classification*: primary 11B75; secondary 52C10.

Keywords and phrases: sum of products, Erdős distance problem.

1. Introduction

The sum-product phenomenon asserts, roughly speaking, that given a finite nonempty set $\mathcal{A}$ in a ring $\mathcal{R}$, then either the sum set $2\mathcal{A} = \{a + a' \mid a, a' \in \mathcal{A}\}$ or the product set $\mathcal{A}^2 = \{a \cdot a' \mid a, a' \in \mathcal{A}\}$ will be significantly larger than $\mathcal{A}$, unless $\mathcal{A}$ is somehow very close to being a subring of $\mathcal{R}$, or if $\mathcal{A}$ is highly degenerate (for instance, containing a lot of zero divisors). For instance, in the case of the set of integers $\mathcal{R} = \mathbb{Z}$, which has no nontrivial finite subrings, a long-standing conjecture of Erdős and Szemerédi asserts that $|2\mathcal{A}| + |\mathcal{A}^2| \gg_\varepsilon |\mathcal{A}|^{2-\varepsilon}$ for every finite nonempty $\mathcal{A} \subset \mathbb{Z}$ and every $\varepsilon > 0$. (The current best result on this problem is a recent result of Solymosi [14], who showed that the conjecture holds for any ε greater than $\frac{2}{3}$.) A related question, posed in a finite field $\mathbb{F}_q$ with q elements, is how large $\mathcal{A} \subset \mathbb{F}_q$ needs to be to assure that $d\mathcal{A}^2 = \mathcal{A}^2 + \cdots + \mathcal{A}^2 = \mathbb{F}_q$. It is known (see, for example, [5, 6]) that, for any $\varepsilon > 0$, there exists $d = d(\varepsilon)$ such that if $|\mathcal{A}| \gg q^{1/2+\epsilon}$ then $d\mathcal{A}^2 = \mathbb{F}_q$. In particular, Hart and Iosevich [6] have obtained a good lower bound on the size of $\mathcal{A}$ that guarantees $d\mathcal{A}^2 = \mathbb{F}_q$, with the possible exception of 0. They also showed that the lower bound on $\mathcal{A}$ may be relaxed if one settles for a positive proportion of $\mathbb{F}_q$.

THEOREM 1.1. [6] *Let $\mathcal{A} \subseteq \mathbb{F}_q$, where $\mathbb{F}_q$ is an arbitrary finite field with q elements, such that $|\mathcal{A}| > q^{(1/2)+(1/2d)}$. Then*

$$\mathbb{F}_q^* \subset d\mathcal{A}^2.$$

Suppose that

$$|\mathcal{A}| \geq C^{1/d} q^{1/2+1/2(2d-1)}$$

for some constant $C > 0$. Then

$$|d\mathcal{A}^2| \geq \frac{C^{2-1/d}}{C^{2-1/d}+1} q.$$

Motivated by Theorem 1.1, it is plausible to conjecture that if $|\mathcal{A}| \geq q^{1/2+\varepsilon}$ then $2\mathcal{A}^2$ covers $\mathbb{F}_q$ or at least a positive proportion of $\mathbb{F}_q$. When $q = p$ is a prime, the prime field $\mathbb{F}_p$ can be naturally identified with $\mathbb{Z}_p = \{0, 1, \dots, p-1\}$. Garaev and Garcia [4, Theorem 3] showed that the conjecture holds if $\mathcal{A}$ is an interval of length $|\mathcal{A}| \gg p^{1/2}(\log p)^{1/4}$. In the general case, the best known result is still Theorem 1.1. The main purpose of this paper is to present some results in favor of this conjecture. We show that for any $d \geq 2$, for almost every subset $\mathcal{A} \subset \mathbb{F}_q$ of cardinality $|\mathcal{A}| \gg q^{1/d}$, then $\mathbb{F}_q^* \subset d\mathcal{A}^2$. More precisely, our first result is the following.

THEOREM 1.2. *For a positive integer $d \geq 2$ and for any $\alpha > 0$, there exist an integer $q_0 = q(d, \alpha)$ and a number $C_{d,\alpha} > 0$ with the following property. If one chooses a random subset $\mathcal{A} \subseteq \mathbb{F}_q$ where $|\mathcal{A}| = t \geq C_{d,\alpha} q^{1/d}$, then the probability of $\mathbb{F}_q^* \not\subseteq d\mathcal{A}^2$ is at most $q\alpha^t$, provided that $q \geq q_0$.*

Furthermore, if $q = p$ is a prime, for a sufficiently large subset $\mathcal{A} \subseteq \mathbb{Z}_p$, we show that $d\mathcal{A}^2$ contains both large and small residues.

THEOREM 1.3. *For $\mathcal{A} \subseteq \mathbb{Z}_p \equiv \{0, \dots, p-1\}$ where*

$$\frac{|\mathcal{A}|}{p^{1/2}(\log p)^{1/d}} \to \infty \quad \text{as } p \to \infty,$$

then

$$\max_{x \in d\mathcal{A}^2} x = (1 + o(1))p,$$

and

$$\min_{x \in d\mathcal{A}^2} x = o(p).$$

Another classical problem in combinatorics is the Erdős distance problem. For $\mathcal{E} \subset \mathbb{F}_q^d$, $d \geq 2$, the analog of the classical Erdős distance problem is to determine the smallest possible cardinality of the set

$$\Delta(\mathcal{E}) = \{|x - y|^2 = (x_1 - y_1)^2 + \cdots + (x_d - y_d)^2 : x, y \in \mathcal{E}\},$$

which is viewed as a subset of $\mathbb{F}_q$. Iosevich and Rudnev [8], using Fourier analytic methods, showed that there are absolute constants $c_1, c_2 > 0$ such that for any odd q and any set $\mathcal{E} \subset \mathbb{F}_q^d$ of cardinality $|\mathcal{E}| \geq c_1 q^{d/2}$,

$$|\Delta(\mathcal{E})| \geq c \min\{q, q^{-(d-1)/2}|\mathcal{E}|\}. \tag{1.1}$$

https://doi.org/10.1017/S0004972709000537 Published online by Cambridge University Press

(In fact one can also obtain (see, for example, [12, 13, 15]) more general results for the number of pairwise distances between elements of two sets $\mathcal{E}, \mathcal{F} \subset \mathbb{F}_q^d$.) In view of this result, Iosevich and Rudnev [8] conjectured that for any subset $\mathcal{E} \subset \mathbb{F}_q^d$ with $|\mathcal{E}| \gg q^{d/2+\epsilon}$, $|\Delta(\mathcal{E})| \geq cq$ for some $c > 0$. This conjecture is false in general. Hart *et al.* [7] constructed, for any small $c > 0$, a subset $\mathcal{E} \subset \mathbb{F}_q^d$ of cardinality $1/2cq^{((d+1)/2)}$ such that $\Delta(\mathcal{E}) \leq cq$. They, however, showed [7, Theorem 2.11] that, for any $c > 0$, if $\mathcal{E}$ is uniformly distributed on the sphere and $|\mathcal{E}| \gg q$, then $|\Delta(\mathcal{E})| \geq cq$. We will show that a similar result holds for almost every subset $\mathcal{E} \subset \mathbb{F}_q$ of cardinality $|\mathcal{E}| \gg q$.

THEOREM 1.4. *For any $\alpha > 0$, there exist an integer $q_0 = q(\alpha)$ and a number $C_\alpha > 0$ with the following property. When a subset $\mathcal{E} \subseteq \mathbb{F}_q^d$, where $|\mathcal{E}| = t \geq C_\alpha q$, is chosen randomly, the probability of $\mathbb{F}_q \nsubseteq \Delta(\mathcal{E})$ is at most $q\alpha^t$, provided that $q \geq q_0$.*

Note that the implied constants in the symbols 'o' and '$\gg$' may depend on an integer parameter d. We recall that the notation $U \gg V$ is equivalent to the assertion that the inequality $U \gg c|V|$ holds for some constant $c > 0$. The rest of this paper is organized as follows. In Section 2, we summarize several useful lemmas, which will be used throughout the paper. The proofs of Theorems 1.2, 1.3 and 1.4 are given in Sections 3–5, respectively.

2. Preliminaries

2.1. Incidence geometry. One of our main tools is the following geometric incidence estimate, which was developed and used in [6] (see also [2] for a functional version).

LEMMA 2.1. [6] *Let $B(\cdot,\cdot)$ be a nondegenerate bilinear form in $\mathbb{F}_q^d$. For any $\lambda \in \mathbb{F}_q$ and two subsets $\mathcal{E}, \mathcal{F} \subseteq \mathbb{F}_q^d$, we define*

$$v_\lambda(\mathcal{E}, \mathcal{F}) = \sum_{B(\boldsymbol{x},\boldsymbol{y})=\lambda} \mathcal{E}(\boldsymbol{x})\mathcal{F}(\boldsymbol{y}),$$

where $\mathcal{E}(\cdot)$ and $\mathcal{F}(\cdot)$ are the characteristic functions of $\mathcal{E}$ and $\mathcal{F}$, respectively. For any $\lambda \in \mathbb{F}_q^*$,

$$v_\lambda(\mathcal{E}, \mathcal{F}) = \frac{|\mathcal{E}||\mathcal{F}|}{q} + R(\lambda),$$

where

$$|R(\lambda)| \leq \sqrt{q^{d-1}|\mathcal{E}||\mathcal{F}|}.$$

2.2. Finite Euclidean graphs. For a fixed $a \in \mathbb{F}_q$, the finite Euclidean graph $E_{q,d}(a)$ in $\mathbb{F}_q^d$ is defined as the graph with the vertex set $\mathbb{F}_q^d$ and the edge set

$$\{(x, y) \in \mathbb{F}_q^d \times \mathbb{F}_q^d : x \neq y, |x - y|^2 = (x_1 - y_1)^2 + \cdots + (x_d - y_d)^2 = a\}.$$

In [10], Medrano *et al.* studied the spectrum of these graphs and showed that they are asymptotically Ramanujan graphs.

https://doi.org/10.1017/S0004972709000537 Published online by Cambridge University Press

THEOREM 2.2. [10] *The finite Euclidean graph $E_{q,d}(a)$ is a regular graph with q^d vertices of valency*

$$k(q,a)=\begin{cases} q^{d-1}+\chi((-1)^{(d-1)/2}a)q^{(d-1)/2} & a\neq 0,\ d \text{ odd},\\ q^{d-1}-\chi((-1)^{d/2})q^{(d-2)/2} & a\neq 0,\ d \text{ even},\\ q^{d-1} & a=0,\ d \text{ odd},\\ q^{d-1}-\chi((-1)^{d/2})(q-1)q^{(d-2)/2} & a=0,\ d \text{ even}\end{cases}$$

where χ is the quadratic character

$$\chi(a)=\begin{cases} 1 & a\neq 0, \quad a \text{ is square in } \mathbb{F}_q,\\ -1 & a\neq 0, \quad a \text{ is nonsquare in } \mathbb{F}_q,\\ 0 & a=0.\end{cases}$$

Let λ be any eigenvalues of the graph $E_{q,d}(a)$ with $\lambda \neq$ valency of the graph. Then

$$|\lambda| \leq 2q^{(d-1)/2}. \tag{2.1}$$

2.3. Eigenvalues and expanders. We call a graph $G=(V,E)$ an (n,d,λ)-graph if G is a d-regular graph on n vertices where the absolute values of each of its eigenvalues except for the largest one are at most λ. It is well known that if $\lambda \ll d$, then an (n,d,λ)-graph behaves similarly to a random graph $G_{n,d/n}$. Specifically, we have the following result.

LEMMA 2.3. [1, Corollary 9.2.5] *Let G be an (n,d,λ)-graph. For every set of vertices B and C of G,*

$$\left|e(B,C)-\frac{d}{n}|B||C|\right| \leq \lambda\sqrt{|B||C|}, \tag{2.2}$$

where $e(B,C)$ is the number of edges in the induced bipartite subgraph of G on (B,C) (that is, the number of ordered pairs (u,v) where $u\in B$, $v\in C$ and uv is an edge of G).

2.4. A graph theory lemma. Let $G(X,Y)$ be a bipartite graph. We denote the number of edges going through X and Y by $e(X,Y)$. The average degree $\bar{d}(G)$ of G is defined as

$$\bar{d}(G)=\frac{2e(X,Y)}{|X|+|Y|}.$$

We will need the following bound on the probability of an induced bipartite subgraph being empty.

LEMMA 2.4. [11, Lemma 2.1] *Let $\{G_n=G(V_n,V_n)\}_{n=1}^{\infty}$ be a sequence of bipartite graphs with $|V_n|\to\infty$ as $n\to\infty$. Assume that for any $\varepsilon>0$, there exist an integer $v(\varepsilon)$ and a number $c(\varepsilon)>0$ such that $e(A,A)\geq c(\varepsilon)|A|^2\bar{d}(G_n)/|V_n|$ for all $|V_n|\geq v(\varepsilon)$ and all $A\subset V_n$ satisfying $|A|\geq\varepsilon|V_n|$. Then for any $\alpha>0$, there exist an integer $v(\alpha)$ and a number $C(\alpha)$ with the following property. If one chooses a random subset S of V_n of cardinality s, then the probability of $G(S,S)$ being empty is at most α^s, provided that $|S|=s\geq C(\alpha)|V_n|/\bar{d}(G)$ and $|V_n|\geq v(\alpha)$.*

https://doi.org/10.1017/S0004972709000537 Published online by Cambridge University Press

2.5. Character sums for bilinear forms over finite fields. The next lemma is an estimate of a character sum with bilinear forms over finite fields.

LEMMA 2.5. *Let $B(\cdot, \cdot)$ be a nondegenerate bilinear form in the d-dimensional vector space $\mathbb{F}_q^d$, and ψ be a nontrivial additive character on $\mathbb{F}_q$. For any two sets $\mathcal{E}, \mathcal{F} \subset \mathbb{F}_q^n$ with $|\mathcal{E}| = E$, $|\mathcal{F}| = F$,*

$$\left| \sum_{\boldsymbol{u} \in \mathcal{E}, \boldsymbol{v} \in \mathcal{F}} \psi(B(\boldsymbol{u}, \boldsymbol{v})) \right| \le \sqrt{q^d |\mathcal{E}||\mathcal{F}|}. \tag{2.3}$$

PROOF. Viewing $\sum_{\boldsymbol{u} \in \mathcal{E}, \boldsymbol{v} \in \mathcal{F}} \psi(B(\boldsymbol{u}, \boldsymbol{v}))$ as a sum in $\boldsymbol{v}$, applying the Cauchy–Schwarz inequality and dominating the sum over $\boldsymbol{v} \in \mathcal{F}$ by the sum over $\boldsymbol{v} \in \mathbb{F}_q^d$, we see that

$$\begin{aligned} \left| \sum_{\boldsymbol{u} \in \mathcal{E}, \boldsymbol{v} \in \mathcal{F}} \psi(B(\boldsymbol{u}, \boldsymbol{v})) \right|^2 &\le |\mathcal{F}| \sum_{\boldsymbol{v} \in \mathbb{F}_q^d} \sum_{\boldsymbol{u}, \boldsymbol{u}' \in \mathcal{E}} \psi(B(\boldsymbol{u} - \boldsymbol{u}', \boldsymbol{v})) \\ &\le |\mathcal{F}| \sum_{\boldsymbol{u}, \boldsymbol{u}' \in \mathcal{E}} \sum_{\boldsymbol{v} \in \mathbb{F}_q^d} \psi(B(\boldsymbol{u} - \boldsymbol{u}', \boldsymbol{v})) \\ &\le q^d |\mathcal{E}||\mathcal{F}|, \end{aligned}$$

since the inner sum over $\boldsymbol{v}$ vanishes unless $\boldsymbol{u} = \boldsymbol{u}'$. □

2.6. Discrepancy of sequences. For any real number x, set $e(x) = e^{2\pi i x}$. The fraction part $\{x\}$ of x is defined by $\{x\} = x - [x]$, where $[x]$ denotes the integral part of x, that is, the greatest integer less than or equal to x. For any interval $\mathcal{I} \subseteq [0, 1)$ and a sequence $\{x_n\}_{n \ge 1}$, $x_n \in \mathbb{R}$, let $A(\mathcal{I}, N, x_n)$ be the number of x_n, $1 \le n \le N$, for which $\{x_n\} \in \mathcal{I}$, that is,

$$A(\mathcal{I}, N, x_n) = \sum_{n=1}^{N} \chi_{\mathcal{I}}(\{x_n\}), \tag{2.4}$$

where $\chi_{\mathcal{I}}$ is the characteristic function of $\mathcal{I}$. The discrepancy $D_N(x_n)$ of a finite sequence $\{x_n\}_{1 \le n \le N}$ is defined as follows.

DEFINITION 2.6. Let $x_1, \ldots, x_N$ be a finite sequence of real numbers. Then the number

$$D_N = D_N(x_n) = \sup_{I \subseteq [0,1)} \left| \frac{A(\mathcal{I}, N, x_n)}{N} - |\mathcal{I}| \right|$$

is called the discrepancy of the given sequence.

We will need the following variant of the Erdős–Turán–Koksma inequality.

LEMMA 2.7. [3, Equation (1.62)] *Let $x_1, \ldots, x_N$ be a finite sequence of real numbers. For any $H > 2$,*

$$D_N(x_n) \le \frac{1}{H+1} + \sum_{0 < h \le H} \frac{1}{h} \left| \frac{1}{N} \sum_{n=1}^{N} e(hx_n) \right|. \tag{2.5}$$

https://doi.org/10.1017/S0004972709000537 Published online by Cambridge University Press

3. Sum of products in random sets

In this section, we mimic the proof of [11, Lemma 2.1] to give a proof of Theorem 1.2. Let $\mathcal{A}$ be an ordered random subset, whose elements are chosen in order (a_1 first and a_t last). For any $\lambda \in \mathbb{F}_q^*$, we compute the probability that $\lambda \notin d\mathcal{A}^2$. For $1 \leq s < t$, let

$$\mathcal{N}_s = \{a \in \mathbb{F}_q : ay_1 + x_2y_2 + \cdots + x_dy_d = \lambda,\\ \text{for some } x_2, \ldots, x_d, y_1, \ldots, y_d \in \{a_1, \ldots, a_s, a\}\}.$$

Since $\lambda \notin d\mathcal{A}^2$, $a_{s+1} \notin \mathcal{N}_s$. Let

$$\mathcal{M}_{s+1} = \{a_{s+1} \in \mathbb{F}_q \setminus \{a_1, \ldots, a_s\} : |\mathcal{N}_{s+1} \setminus \mathcal{N}_s| \leq \varepsilon q^{1/d}/2\},$$

where ε later will be chosen to be small enough. Suppose that $|\mathcal{M}_{s+1}| > \varepsilon q$ for some $1 \leq s < t$. From Lemma 2.1,

$$v_\lambda(\mathcal{M}_{s+1}^d, \mathcal{M}_{s+1}^d) \geq \frac{|\mathcal{M}_{s+1}|^{2d}}{q} - q^{(d-1)/2}|\mathcal{M}_{s+1}|^d. \tag{3.1}$$

Since $\mathcal{M}_{s+1} \cap \mathcal{N}_s = \emptyset$, it follows that

$$v_\lambda(\mathcal{M}_{s+1}^d, \mathcal{M}_{s+1}^d) \leq v_\lambda(\mathcal{M}_{s+1}^d, (\mathbb{F}_q \setminus \mathcal{N}_s)^d) \leq |\mathcal{M}_{s+1}|^d(\varepsilon q^{1/d}/2)^d < \frac{\varepsilon^d q|\mathcal{M}_{s+1}|^d}{2^d}. \tag{3.2}$$

Putting (3.1) and (3.2) together leads to a contradiction. Therefore, $|\mathcal{M}_{s+1}| \leq \varepsilon q$ for $1 \leq s < t$. Let $t \geq 4q^{1/d}/\varepsilon$, and assume that the set $\mathcal{A}$ has been chosen such that $\lambda \notin d\mathcal{A}^2$. Let t_1 be the number of a_{s+1} that do not belong to $\mathcal{M}_{s+1}$. Then

$$q \geq |\mathcal{N}_t| \geq \sum_{a_{s+1} \notin \mathcal{M}_{k+1}} |\mathcal{N}_{k+1} \setminus \mathcal{N}_k| \geq \varepsilon t_1 q^{1/d}/2.$$

This implies that

$$t_1 \leq 2q^{1/d}/\varepsilon \leq t/2.$$

Therefore, there are $t - t_1 \geq t/2$ elements a_{k+1} that belong to $\mathcal{M}_{k+1}$ where $|\mathcal{M}_{k+1}| \leq \varepsilon q$. Hence, the number of ordered subsets $\mathcal{A} \subseteq \mathbb{F}_q$ such that $\lambda \notin d\mathcal{A}^2$ is bounded by

$$\sum_{t_1 \leq t/2} \binom{t}{t_1} q^{t_1}(\varepsilon q)^{t-t_1} \leq (6\varepsilon)^{t/2} q(q-1)\cdots(q-t+1).$$

Choosing $\varepsilon = \alpha^2/6$, we complete the proof of the theorem.

4. Largest and smallest residues

We give a proof of Theorem 1.3 in this section. Choose $H := p - 1$, $N := |\mathcal{A}|^{2d}$ and

$$\{x_1, \ldots, x_N\} := \left\{\frac{\sum_{i=1}^d a_ib_i}{p} : a_1, \ldots, a_d, b_1, \ldots, b_d \in \mathcal{A}\right\}.$$

https://doi.org/10.1017/S0004972709000537 Published online by Cambridge University Press

From Lemma 2.7,

$$D_N(x_n) \leq \frac{1}{p} + \sum_{1 \leq h \leq p-1} \frac{1}{h|\mathcal{A}|^{2d}} \left| \sum_{n=1}^{N} e(hx_n) \right|. \tag{4.1}$$

Applying Lemma 2.5 for additive character $\psi(x) = e(hx/p)$ and $\mathcal{E} = \mathcal{F} = \mathcal{A}^d$,

$$\left| \sum_{n=1}^{N} e(hx_n) \right| \leq p^{d/2} |\mathcal{A}|^d, \tag{4.2}$$

for $1 \leq h \leq p - 1$. It follows from (4.1) and (4.2) that

$$D_N(x_n) \leq \frac{1}{p} + \frac{p^{d/2}}{|\mathcal{A}|^d} \sum_{1 \leq h \leq p-1} \frac{1}{h} \leq \frac{1}{p} + \frac{p^{d/2} \log p}{|\mathcal{A}|^d}. \tag{4.3}$$

Let $\mathcal{I}_1 = [1 - (2p^{d/2} \log p/|\mathcal{A}|^d), 1)$; then

$$\left| \frac{A(\mathcal{I}_1, N, x_n)}{N} - \frac{2p^{d/2} \log p}{|\mathcal{A}|^d} \right| \leq D_N(x_n) \leq \frac{1}{p} + \frac{p^{d/2} \log p}{|\mathcal{A}|^d}.$$

Therefore, $A(\mathcal{I}_1, N, x_n) > 0$, or equivalently

$$\max_{x \in d\mathcal{A}^2} x \geq \left(1 - \frac{2p^{d/2} \log p}{|\mathcal{A}|^d} \right) p = (1 + o(1))p.$$

Similarly, let $\mathcal{I}_2 = [0, 2p^{d/2} \log p/|\mathcal{A}|^d]$; then $A(\mathcal{I}_2, N, x_n) > 0$, or

$$\min_{x \in d\mathcal{A}^2} x \leq \frac{2p^{d/2} \log p}{|\mathcal{A}|^d} p = o(p).$$

This completes the proof of Theorem 1.3.

5. Distances in random sets

Let $G_{q,d}(a)$ be a bipartite graph with the vertex set $\mathbb{F}_q^d \times \mathbb{F}_q^d$ and the edge set

$$\{(x, y) \in \mathbb{F}_q^d \times \mathbb{F}_q^d : |x - y|^2 = (x_1 - y_1)^2 + \cdots + (x_d - y_d)^2 = a\}.$$

Then

$$\bar{d}(G_{q,d}(a)) = k(q, a) + \delta_0(a),$$

where $\delta_0(a) = 1$ if $a = 0$, and 0 otherwise. From Theorem 2.2 and Lemma 2.3, for any $A \subset \mathbb{F}_q^d$,

$$\left| e(A, A) - \frac{k(q, a)}{q^d} |A|^2 \right| \leq 2q^{(d-1)/2} |A|.$$

https://doi.org/10.1017/S0004972709000537 Published online by Cambridge University Press

Hence, it is easy to check that, for any $\varepsilon > 0$, if $|A| \gg \varepsilon q^d$ and $q \gg (2/\varepsilon)^{2/(d-1)}$, then

$$e(A, A) \geq \frac{\bar{d}(G_{q,d}(a))}{2q^d}|A|^2.$$

Let $c(\varepsilon) = 1/2$ and $n(\varepsilon) = \lceil (2/\varepsilon)^{2/(d-1)} \rceil$. Theorem 1.4 now follows immediately from Lemma 2.4.

6. Remarks

For a prime number p and a sufficiently large subset $\mathcal{E} \subseteq \mathbb{Z}_p^d$, similar to Section 4, we can show that $\Delta(\mathcal{E})$ contains both large and small distances.

THEOREM 6.1. [9] *For $\mathcal{E} \subseteq \mathbb{Z}_p^d$ and $|\mathcal{E}| \geq p^{d/2} \log p$,*

$$\max \Delta(\mathcal{E}) = (1 + o(1))p,$$

and

$$\min \Delta(\mathcal{E}) = o(p).$$

Theorem 6.1 and other general results are given in [9]. Theorem 1.3 was inspired by that paper.

References

[1] N. Alon and J. H. Spencer, *The Probabilistic Method*, 2nd edn. (Wiley-Interscience, New York, 2000).

[2] D. Covert, D. Hart, A. Iosevich, D. Koh and M. Rudnev, ‘Generalized incidence theorems, homogeneous forms and sum–product estimates in finite fields’, *European J. Combin.* **31** (2010), 306–319.

[3] M. Drmota and R. Tichy, *Sequence, Discrepancies and Applications* (Springer, Berlin, 1997).

[4] M. Z. Garaev and V. C. Garcia, ‘The equation $x_1x_2 = x_3x_4 + \lambda$ in fields of prime order and applications’, *J. Number Theory* **128** (2008), 2520–2537.

[5] A. A. Glibichuk and S. V. Konyagin, ‘Additive properties of product sets in fields of prime order’, in: *Additive Combinatorics*, CRM Proceedings and Lecture Notes, 43 (American Mathematical Society, Providence, RI, 2007), pp. 279–286.

[6] D. Hart and A. Iosevich, ‘Sums and products in finite fields: an integral geometric viewpoint’, in: *Radon Transforms, Geometry, and Wavelets*, Contemporary Mathematics, 464 (American Mathematical Society, Providence, RI, 2008), pp. 129–135.

[7] 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), 3255–3275.

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

[9] N. M. Katz, I. E. Shparlinski and M. Xiong, ‘On character sums with distances on the upper half plane over a finite field’, Preprint, 2009.

[10] A. Medrano, P. Myers, H. M. Stark and A. Terras, ‘Finite analogues of Euclidean space’, *J. Comput. Appl. Math.* **68** (1996), 221–238.

[11] H. H. Nguyen, ‘On two-point configurations in a random set’, *Integers* **9** (2009), 41–45.

[12] I. E. Shparlinski, ‘On some generalisations of the Erdős distance problem over finite fields’, *Bull. Aust. Math. Soc.* **73** (2006), 285–292.

https://doi.org/10.1017/S0004972709000537 Published online by Cambridge University Press

[13] I. E. Shparlinski, ‘On the set of distances between two sets over finite fields’, *Int. J. Math. Math. Sci.* **2006** (2006), Article ID 59482.

[14] J. Solymosi, Bounding multiplicative energy by the sumset, arXiv:0806.1040.

[15] L. A. Vinh, ‘Explicit Ramsey graphs and Erdős distance problem over finite Euclidean and non-Euclidean spaces’, *Electron. J. Combin.* **15** (2008), Article R5.

LE ANH VINH, Mathematics Department, Harvard University, Cambridge,
MA, 20138, USA
e-mail: vinh@math.harvard.edu

https://doi.org/10.1017/S0004972709000537 Published online by Cambridge University Press