Michigan Math. J. 62 (2013), 779–792

# On Distance Sets and Product Sets in Vector Spaces over Finite Rings

Do Duy Hieu & Le Anh Vinh

## 1. Introduction

The classical Erdős distance problem asks for the minimal number of distinct distances determined by a finite point set in $\mathbb{R}^n$, $n \geq 2$. This problem in the Euclidean plane was solved by Guth and Katz [9], who showed that a set of $N$ points in $\mathbb{R}^2$ has at least $cN/\log N$ distinct distances. For developments on the Erdős distance problem in higher dimensions, see [13; 15] and the references therein.

Throughout the paper, $q = p^r$ $(r \geq 1)$, where $p$ is a prime large enough to overcome a few minor technical problems. Here and throughout, the notation $X \lesssim Y$ means that there exists a $C > 0$ such that $X \leq CY$. Let $\mathbb{F}_q$ denote a finite field with $q$ elements. For $\mathcal{E} \subset \mathbb{F}_q^n$ $(n \geq 2)$, the finite analogue of the classical Erdős distance problem is to determine the smallest possible cardinality of the set

$$\Delta_{\mathbb{F}_q}(\mathcal{E}) = \{\|\boldsymbol{x} - \boldsymbol{y}\| = (x_1 - y_1)^2 + \cdots + (x_n - y_n)^2 : \boldsymbol{x}, \boldsymbol{y} \in \mathcal{E}\} \subset \mathbb{F}_q.$$

The first nontrivial result on the Erdős distance problem in vector spaces over finite fields is due to Bourgain, Katz, and Tao [3], who showed that if $q$ is a prime, $q \equiv 3 \pmod 4$, then for every $\varepsilon > 0$ and $\mathcal{E} \subset \mathbb{F}_q^2$ with $|\mathcal{E}| \leq C_\varepsilon q^{2-\varepsilon}$ there exists a $\delta > 0$ such that $|\Delta_{\mathbb{F}_q}(\mathcal{E})| \geq C_\delta |\mathcal{E}|^{1/2+\delta}$ for some constants $C_\varepsilon, C_\delta$. However, the relationship between $\varepsilon$ and $\delta$ in their arguments is difficult to determine. In addition, it is quite subtle to address higher-dimensional cases with these arguments. Iosevich and Rudnev [12] used Fourier analytic methods to show that there exist absolute constants $c_1, c_2 > 0$ such that, for any odd prime power $q$ and any set $\mathcal{E} \subset \mathbb{F}_q^d$ of cardinality $|\mathcal{E}| \geq c_1 q^{n/2}$,

$$|\Delta_{\mathbb{F}_q}(\mathcal{E})| \geq c_2 \min\{q, q^{(n-1)/2}|\mathcal{E}|\}. \tag{1.1}$$

In [20], Vu gave another proof of (1.1) using the graph-theoretic method (see also [16] for a similar proof). Iosevich and Rudnev reformulated the question in analogy with the Falconer distance problem: How large must $\mathcal{E} \subset \mathbb{F}_q^n$, $n \geq 2$, be in order to ensure that $\Delta_{\mathbb{F}_q}(\mathcal{E})$ contains a positive proportion of the elements of $\mathbb{F}_q$? The inequality (1.1) implies that if $|\mathcal{E}| \geq 2q^{(n+1)/2}$ then $\Delta_{\mathbb{F}_q}(\mathcal{E}) = \mathbb{F}_q$; this is directly in line with Falconer's result in the Euclidean setting that, for a set $\mathcal{E}$ with Hausdorff dimension greater than $(n+1)/2$, the distance set is of positive measure.

Received October 9, 2012. Revision received March 25, 2013.

Research of the second author is supported by Vietnam National University, Hanoi, under the project "Some Problems on Matrices over Finite Fields".

At first, it seems reasonable that the exponent $(n+1)/2$ may be unprovable—in line with the Falconer distance conjecture just stated. Yet Hart, Iosevich, Koh, and Rudnev [11] discovered that the arithmetic of the problem makes the exponent $(n+1)/2$ best possible in odd dimensions, at least in general fields. In even dimensions it is still possible that the correct exponent is $n/2$, in analogy with the Euclidean case. In [4], Chapman and colleagues took a first step in this direction by showing that, if $\mathcal{E} \subset \mathbb{F}_q^2$ satisfies $|\mathcal{E}| \geq q^{4/3}$, then $|\Delta_{\mathbb{F}_q}(\mathcal{E})| \geq cq$. This is in accordance with Wolff's result for the Falconer conjecture in the plane, which states that the Lebesgue measure of the set of distances determined by a subset of the plane of Hausdorff dimension greater than $4/3$ is positive.

In [6], Covert, Iosevich, and Pakianathan extended (1.1) to the setting of finite cyclic rings $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ ($q = p^r$, $p$ a sufficiently large prime). One reason for considering this situation is that, if one is interested in answering questions about sets $\mathcal{E} \subset \mathbb{Q}^n$ of rational points, then it is possible to ask questions about the distance sets for such sets and how they compare to their counterparts in $\mathbb{R}^n$. By the scale invariance of these questions, the problem of obtaining sharp bounds for the relationship between $|\Delta_{\mathbb{Z}_q}(\mathcal{E})|$ and $|\mathcal{E}|$ for a subset $\mathcal{E}$ of $\mathbb{Q}^n$ would be the same as for subsets of $\mathbb{Z}^n$. Here, the distance set of $\mathcal{E}$ in vector space over a finite ring is defined similarly by

$$\Delta_{\mathbb{Z}_q}(\mathcal{E}) = \{\|\boldsymbol{x} - \boldsymbol{y}\| = (x_1 - y_1)^2 + \cdots + (x_n - y_n)^2 : \boldsymbol{x}, \boldsymbol{y} \in \mathcal{E}\} \subset \mathbb{Z}_q.$$

In [6], a nearly sharp bound was obtained for the distance problem in vector spaces over the finite ring $\mathbb{Z}_q$. More precisely, the authors proved that if $\mathcal{E} \subset \mathbb{Z}_q^n$ is of cardinality

$$|\mathcal{E}| \gtrsim r(r+1)q^{(2r-1)n/2r+1/2r} \tag{1.2}$$

then

$$\mathbb{Z}_q^\times \subset \Delta_{\mathbb{Z}_q}(\mathcal{E}).$$

In [19] this result was extended using graph-theoretic methods. Roughly speaking, it was shown that any sufficiently large subset $\mathcal{E} \subset \mathbb{Z}_q^n$ determines all possible nondegenerated $k$-simplices.

A related question that has recently received attention is the following. For $\mathcal{A} \subset \mathbb{F}_q$, how large must $\mathcal{A}$ must be in order to ensure that $\mathbb{F}_q^* \subset \mathcal{A} \cdot \mathcal{A} + \cdots + \mathcal{A} \cdot \mathcal{A}$ ($n$ times)? Bourgain [2] showed that if $\mathcal{A} \subset \mathbb{F}_q$ is of cardinality $|\mathcal{A}| \geq Cq^{3/4}$ then $\mathcal{A} \cdot \mathcal{A} + \mathcal{A} \cdot \mathcal{A} + \mathcal{A} \cdot \mathcal{A} = \mathbb{F}_q$. Glibichuk and Konyagin [8] proved in the case of prime fields $\mathbb{Z}_p$ that, for $n = 8$, one can take $|\mathcal{A}| > \sqrt{q}$. Glibichuk [7] then extended this result to arbitrary finite fields. We remark that this question can be stated in a more general setting. If $\mathcal{E} \subset \mathbb{F}_q^n$, then how large must $\mathcal{E}$ be in order to ensure that the equation

$$\boldsymbol{x} \cdot \boldsymbol{y} = \lambda, \quad \boldsymbol{x}, \boldsymbol{y} \in \mathcal{E}, \tag{1.3}$$

is solvable for any $\lambda \in \mathbb{F}_q^*$? Hart and Iosevich [10] used exponential sums to show that one can take $|\mathcal{E}| > q^{(n+1)/2}$ for any $n \geq 2$. Covert, Iosevich, and Pakianathan [6] extended this result to the setting of finite cyclic rings $\mathbb{Z}_q$. They proved that if $\mathcal{E} \subset \mathbb{Z}_q^n$ is of cardinality

$$|\mathcal{E}| \gtrsim rq^{(2r-1)n/2r+1/2r}, \tag{1.4}$$

then (1.3) is solvable for all $\lambda \in \mathbb{Z}_q^{\times}$. Using spectral graph theory, Vinh [19] gave alternative proofs of these theorems. In fact, it is shown there that (almost) all systems of dot-product equations are solvable in any sufficiently large subset $\mathcal{E} \subset \mathbb{Z}_q^n$.

The lower bounds (1.2) and (1.4) establish that there exists a constant $D = D(p,r) > 0$ such that (a) $|\mathcal{E}| > Dq^{n(2r-1)/2r}$ implies $\mathbb{Z}_{p^r}^{\times} \subset \Delta_{\mathbb{Z}_q}(\mathcal{E},\mathcal{E})$ and (b) equation (1.3) is solvable for all $\lambda \in \mathbb{Z}_q^{\times}$. In contrast, it was shown in [6] that for any $n \geq 3$ there exist sets $\mathcal{E} \subset \mathbb{Z}_q^n$ of size $|\mathcal{E}| = bq^{n(2r-1)/2r}$, where

$$b = \begin{cases} 1 & \text{if } n \text{ is even,} \\ 1/\sqrt{p} & \text{if } n \text{ is odd,} \end{cases}$$

yet $|\Delta_{\mathbb{Z}_q}(\mathcal{E})| = o(p^r)$ (1.3) is *not* solvable for any $\lambda \in \mathbb{Z}_q^{\times}$. Since $|\mathbb{Z}_{p^r}^{\times}| = p^r - p^{r-1}$, these bounds are best possible up to the factor of $1/2r$. The main purpose of this paper is to improve the lower bounds (1.2) and (1.4) under the additional assumption that $\mathcal{E}$ is the Cartesian product of sets.

## 2. Statement of Results

### 2.1. Distance Sets and Product Sets over Finite Fields

Let $q = p^r$ $(r \geq 1)$, where $p$ is a sufficiently large prime, and let $\mathbb{F}_q$ be the finite field of $q$ elements. The finite Euclidean space $\mathbb{F}_q^d$ consists of column vectors $\boldsymbol{x}$ with $j$th entry $x_j \in \mathbb{F}_q$. Define the distance between $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^d$ by

$$\|\boldsymbol{x} - \boldsymbol{y}\| = \sum_{j=1}^{d} (x_j - y_j)^2.$$

Given a subset $\mathcal{E} \subset \mathbb{F}_q^d$, we define the *distance set* of $\mathcal{E}$ as

$$\Delta_{\mathbb{F}_q}(\mathcal{E}) = \{\|\boldsymbol{x} - \boldsymbol{y}\| : \boldsymbol{x}, \boldsymbol{y} \in \mathcal{E}\}.$$

Similarly, we define the *product set* of $\mathcal{E}$ as

$$\Pi_{\mathbb{F}_q}(\mathcal{E}) = \{\boldsymbol{x} \cdot \boldsymbol{y} : \boldsymbol{x}, \boldsymbol{y} \in \mathcal{E}\},$$

where $\boldsymbol{x} \cdot \boldsymbol{y} = x_1 y_1 + \cdots + x_d y_d$ is the usual dot product.

Using Fourier analytic methods over finite fields, Iosevich and Rudnev [12] showed that if $|\mathcal{E}| \geq 2q^{(d+1)/2}$ then $\Delta(\mathcal{E}) \equiv \mathbb{F}_q$. Hart and Iosevich [10] improved the threshold to $q^{d^2/(d-1)}$ under the additional assumptions that $\mathcal{E}$ has product structure and that the distance set covers a positive proportion of the field $\mathbb{F}_q$.

THEOREM 2.1 [10, Thm. 1.1, Cor. 1.2]. *Suppose that $\mathcal{E} = E_1 \times \cdots \times E_n$, where $E_1, \ldots, E_n \subset \mathbb{F}_q$, and suppose*

$$|\mathcal{E}| \gtrsim q^{n^2/(2n-1)}.$$

*Then $|\Delta_{\mathbb{F}_q}(\mathcal{E})| \gtrsim q$.*

Hart and colleagues [11] obtained a similar result for the product sets in vector spaces over finite fields.

Theorem 2.2 [11, Thm. 2.5]. *Suppose that* $\mathcal{E} = E_1 \times \cdots \times E_n$, *where* $E_1, \dots, E_n \subset \mathbb{F}_q$, *and suppose*

$$|\mathcal{E}| \gtrsim q^{n^2/(2n-1)}.$$

*Then* $|\Pi_{\mathbb{F}_q}(\mathcal{E})| \gtrsim q$.

In this paper, we extend the method used in [18] to obtain alternative versions of these results. Note that moving from one-set formulations in Theorem 2.3 and Theorem 2.4 to multi-set formulations in Theorem 2.1 and Theorem 2.2 is simply a matter of inserting a different letter in a few places.

Theorem 2.3. *Let* $A \subset \mathbb{F}_q$ *be of cardinality* $|A| \gtrsim q^{1/2}$. *Then*

$$|\Delta_{\mathbb{F}}(A^n)| \gtrsim \min\left\{q, \frac{|A|^{2n-1}}{q^{n-1}}\right\}.$$

Theorem 2.4. *Let* $A \subset \mathbb{F}_q$ *be of cardinality* $|A| \gtrsim q^{1/2}$. *Then*

$$|\Pi_{\mathbb{F}}(A^n)| \gtrsim \min\left\{q, \frac{|A|^{2n-1}}{q^{n-1}}\right\}.$$

In particular, Theorem 2.3 and Theorem 2.4 imply that, if $A \subset \mathbb{F}_q$ is of cardinality $|A| \gtrsim q^{n/(2n-1)}$, then

$$|\Delta_{\mathbb{F}}(A^n)| \gtrsim q \quad \text{and} \quad |\Pi_{\mathbb{F}}(A^n)| \gtrsim q.$$

### 2.2. *Distance Sets and Product Sets over Finite Rings*

Let $q = p^r$ $(r \geq 1)$, where $p$ is a sufficiently large prime, and let $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ be the finite cyclic ring of $q$ elements. The finite Euclidean space $\mathbb{Z}_q^d$ consists of column vectors $\boldsymbol{x}$ with $j$th entry $x_j \in \mathbb{Z}_q$. Similarly, define the distance between $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}_q^d$ by

$$\|\boldsymbol{x} - \boldsymbol{y}\| = \sum_{j=1}^{d} (x_j - y_j)^2.$$

Given a subset $\mathcal{E} \subset \mathbb{Z}_q^d$, we define the distance set of $\mathcal{E}$ as

$$\Delta_{\mathbb{Z}_q}(\mathcal{E}) = \{\|\boldsymbol{x} - \boldsymbol{y}\| : \boldsymbol{x}, \boldsymbol{y} \in \mathcal{E}\}.$$

Similarly, we define the product set of $\mathcal{E}$ as

$$\Pi_{\mathbb{Z}_q}(\mathcal{E}) = \{\boldsymbol{x} \cdot \boldsymbol{y} : \boldsymbol{x}, \boldsymbol{y} \in \mathcal{E}\},$$

where $\boldsymbol{x} \cdot \boldsymbol{y} = x_1 y_1 + \cdots + x_d y_d$ is the usual dot product.

In [6], the following results were obtained using the Fourier analysis method over finite rings.

THEOREM 2.5 [6, Thm. 1.3.1]. *Let $\mathcal{E} \subset \mathbb{Z}_q^n$, where $q = p^r$, $p \geq 3$ is a prime, and $r \geq 2$. Suppose that*

$$|\mathcal{E}| \gtrsim r(r+1)q^{(2r-1)n/2r+1/2r}.$$

*Then*

$$\mathbb{Z}_q^\times \subset \Delta_{\mathbb{Z}_q}(\mathcal{E}),$$

*where $\mathbb{Z}_q^\times$ is the multiplicative group of units modulo $q$.*

THEOREM 2.6 [6, Thm. 1.3.2]. *Let $\mathcal{E} \subset \mathbb{Z}_q^n$, where $q = p^r$, $p \geq 3$ is a prime, and $r \geq 2$. Suppose that*

$$|\mathcal{E}| \gtrsim rq^{(2r-1)n/2r+1/2r}.$$

*Then*

$$\mathbb{Z}_q^\times \subset \Pi_{\mathbb{Z}_q}(\mathcal{E}).$$

Under the additional assumption that the point set is the Cartesian product of sets, we obtain the following stronger results on the distance and product sets in vector spaces over finite fields.

THEOREM 2.7. *Let $A \subset \mathbb{Z}_q$ be of cardinality $|A| \gtrsim q^{1-1/2r}$. Then*

$$|\Delta_{\mathbb{Z}_q}(A^n)| \gtrsim \min\left\{q, \frac{|A|^{2n-1}}{(rq^{2-1/r})^{n-1}}\right\}.$$

THEOREM 2.8. *Let $A \subset \mathbb{Z}_q$ be of cardinality $|A| \gtrsim q^{1-1/2r}$. Then*

$$|\Pi_{\mathbb{Z}_q}(A^n)| \gtrsim \min\left\{q, \frac{|A|^{2n-1}}{(rq^{2-1/r})^{n-1}}\right\}.$$

In particular, Theorem 2.5 and Theorem 2.6 imply that if $A \subset \mathbb{Z}_q$ is of cardinality

$$|A| \gtrsim r^{2/n}q^{1+1/2rn-1/2r} \tag{2.1}$$

then

$$\mathbb{Z}_q^\times \subset \Delta_{\mathbb{Z}_q}(A^n) \quad \text{and} \quad \mathbb{Z}_q^\times \subset \Pi_{\mathbb{Z}_q}(A^n);$$

and Theorem 2.7 and Theorem 2.8 imply that if $A \subset \mathbb{Z}_q$ is of cardinality

$$|A| \gtrsim r^{(n-1)/(2n-1)}q^{1+1/2r(2n-1)-1/2r}$$

then

$$|\Delta_{\mathbb{Z}_q}(A^n)| \gtrsim q \quad \text{and} \quad |\Pi_{\mathbb{Z}_q}(A^n)| \gtrsim q.$$

Recall that, by [6], the bounds in Theorem 2.5 and Theorem 2.6 are best possible up to the factor of $1/2r$. However, the sharpness examples in that paper do not work in the case of product sets. Furthermore, we believe that the bound (4.2) could be improved considerably when $n$ is large.

## 3. Pseudo-Random Graphs

For a graph $G$, let $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ be the eigenvalues of its adjacency matrix. The quantity $\lambda(G) = \max\{\lambda_2, -\lambda_n\}$ is called the *second eigenvalue* of $G$. A graph $G = (V, E)$ is called an $(n, d, \lambda)$-graph if it is $d$-regular, $G$ has $n$ vertices, and the second eigenvalue of $G$ is at most $\lambda$. It is well known (see [1, Chap. 9] for more details) that if $\lambda$ is much smaller than the degree $d$ then $G$ has certain randomlike properties. For two (not necessarily) disjoint subsets of vertices $U, W \subset V$, let $e(U, W)$ be the number of ordered pairs $(u, w)$ such that $u \in U$, $w \in W$, and $(u, w)$ is an edge of $G$. For a vertex $v$ of $G$, let $N(v)$ denote the set of vertices of $G$ adjacent to $v$ and let $d(v)$ denote this set's degree. Similarly, for a subset $U$ of the vertex set, let $N_U(v) = N(v) \cap U$ and $d_U(v) = |N_U(v)|$. We will need the following well-known fact.

Lemma 3.1 [1, Cor. 9.2.5]. *Let $G = (V, E)$ be an $(n, d, \lambda)$-graph. For any two sets $B, C \subset V$, we have*

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

### *3.1. Sum-Square Graphs over Finite Fields*

The sum-square graph $\mathcal{FS}_q$ over finite field $\mathbb{F}_q$ is defined as follows. The vertex set of the sum-square graph $\mathcal{FS}_q$ is the set $\mathbb{F}_q \times \mathbb{F}_q$. Two vertices $\boldsymbol{a} = (a_1, a_2)$ and $\boldsymbol{b} = (b_1, b_2)$ with $\boldsymbol{a}, \boldsymbol{b} \in V(\mathcal{FS}_q)$ are connected by an edge, $(\boldsymbol{a}, \boldsymbol{b}) \in E(\mathcal{FS}_q)$, if and only if $a_1 + b_1 = (a_2 + b_2)^2$. We have the following pseudo-randomness of the sum-square graph $\mathcal{FS}_q$.

Theorem 3.2. *The graph $\mathcal{FS}_q$ is a $\left(q^2, q, \sqrt{2q}\,\right)$-graph.*

*Proof.* It is clear that $\mathcal{FS}_q$ is a regular graph of order $q^2$ and valency $q$. We now estimate the eigenvalues of this multi-graph (i.e., graph with loops). For any $(\boldsymbol{a}, \boldsymbol{b}) \in V(\mathcal{FS}_q)$ with $\boldsymbol{a} \neq \boldsymbol{b}$, we count the number of solutions of the following system:

$$a_1 + x_1 = (a_2 + x_2)^2, \quad b_1 + x_1 = (b_2 + x_2)^2, \quad \boldsymbol{x} = (x_1, x_2) \in V(\mathcal{FS}_q).$$

This system has the unique solution

$$x_1 = \left(\frac{a_1 - b_1}{a_2 - b_2} + (a_2 - b_2)\right)^2 \Big/ 4 - a_1,$$

$$x_2 = \left(\frac{a_1 - b_1}{a_2 - b_2} - (a_2 + b_2)\right) \Big/ 2$$

if $a_2 \neq b_2$ and has no solution otherwise. In other words, two distinct vertices $\boldsymbol{a} = (a_1, a_2)$ and $\boldsymbol{b} = (b_1, b_2)$ have a unique common vertex if $a_2 \neq b_2$ and otherwise have no common vertex. Let $M$ be the adjacency matrix of $\mathcal{FS}_q$. It follows that

$$M^2 = J + (q - 1)I - E. \tag{3.1}$$

Here $J$ is the all-1 matrix, $I$ is the identity matrix, and $E$ is the adjacency matrix of the graph $\mathcal{S}_E$, where $V(\mathcal{S}_E) = \mathbb{F}_q \times \mathbb{F}_q$ and, for any two distinct vertices $\boldsymbol{a}, \boldsymbol{b} \in V(\mathcal{S}_E)$, $(\boldsymbol{a}, \boldsymbol{b})$ is an edge of $\mathcal{S}_E$ if and only if $a_2 = b_2$. It follows that $\mathcal{S}_E$ is a $(q - 1)$-regular graph. Because $\mathcal{FS}_q$ is a $q$-regular graph, $q$ is an eigenvalue of $M$ with the all-1 eigenvector $\mathbf{1}$. The graph $\mathcal{FS}_q$ is connected and so the eigenvalue $q$

has multiplicity 1. It is clear that the graph $\mathcal{FS}_q$ contains (many) triangles, which implies that the graph is not bipartite. Hence, for any other eigenvalue $\theta$ of the graph $\mathcal{FS}_q$, we have $|\theta| < q$. Let $\boldsymbol{v}_\theta$ denote the corresponding eigenvector of $\theta$. Note that $\boldsymbol{v}_\theta \in \mathbf{1}^\perp$, so $J\boldsymbol{v}_\theta = 0$. It follows from (3.1) that $(\theta^2 - q + 1)\boldsymbol{v}_\theta = -E\boldsymbol{v}_\theta$. Since $\mathcal{S}_E$ is a $(q-1)$-regular graph, absolute values of the eigenvalues of $\mathcal{S}_E$ are bounded by $q-1$. This statement implies that $\theta^2 \leq 2(q-1)$, and the theorem follows. □

### 3.2. Sum-Product Graphs over Finite Fields

For any $\lambda \in \mathbb{F}_q$, the sum-product graph $\mathcal{FP}_q(\lambda)$ is defined as follows. The vertex set of the sum-product graph $\mathcal{FP}_q(\lambda)$ is the set $\mathbb{F}_q \times \mathbb{F}_q$. Two vertices $\boldsymbol{a} = (a_1, a_2)$ and $\boldsymbol{b} = (b_1, b_2)$ with $\boldsymbol{a}, \boldsymbol{b} \in V(\mathcal{FP}_q(\lambda))$ are connected by an edge, $(\boldsymbol{a}, \boldsymbol{b}) \in E(\mathcal{FP}_q(\lambda))$, if and only if $a_1 + b_1 + a_2 b_2 = \lambda$. Our construction is similar to that of Solymosi in [14]. We have the following pseudo-randomness of the sum-product graph $\mathcal{FP}_q(\lambda)$.

Theorem 3.3. *The graph $\mathcal{FP}_q(\lambda)$ is a $\left(q^2, q, \sqrt{2q}\,\right)$-graph.*

*Proof.* It is clear that $\mathcal{FP}_q(\lambda)$ is a regular graph of order $q^2$ and valency $q$. We now estimate the eigenvalues of this multi-graph. For any $(\boldsymbol{a}, \boldsymbol{b}) \in V(\mathcal{FP}_q(\lambda))$ with $\boldsymbol{a} \neq \boldsymbol{b}$, we count the number of solutions of the following system:

$$a_1 + x_1 + a_2 x_2 = b_1 + x_1 + b_2 x_2 = \lambda, \qquad \boldsymbol{x} = (x_1, x_2) \in V(\mathcal{FP}_q(\lambda)).$$

This system has the unique solution

$$x_1 = \lambda - \frac{a_2 b_1 - a_1 b_2}{a_2 - b_2},$$
$$x_2 = \frac{b_1 - a_1}{a_2 - b_2}$$

if $a_2 \neq b_2$ and has no solution otherwise. In other words, two distinct vertices $\boldsymbol{a} = (a_1, a_2)$ and $\boldsymbol{b} = (b_1, b_2)$ have a unique common vertex if $a_2 \neq b_2$ and otherwise have no common vertex. Let $M$ be the adjacency matrix of $\mathcal{FP}_q(\lambda)$. It follows that

$$M^2 = J + (q-1)I - E.$$

Here $J$ is the all-1 matrix, $I$ is the identity matrix, and $E$ is the adjacency matrix of the graph $\mathcal{S}_E$, where $V(\mathcal{S}_E) = \mathbb{F}_q \times \mathbb{F}_q$ and, for any two distinct vertices $\boldsymbol{a}, \boldsymbol{b} \in V(\mathcal{S}_E)$, $(\boldsymbol{a}, \boldsymbol{b})$ is an edge of $\mathcal{S}_E$ if and only if $a_2 = b_2$. It follows that $\mathcal{S}_E$ is a $(q-1)$-regular graph. Since the graph $\mathcal{FP}_q(\lambda)$ is a $q$-regular graph, $q$ is an eigenvalue of $M$ with the all-1 eigenvector $\mathbf{1}$. The graph $\mathcal{FP}_q(\lambda)$ is connected, so the eigenvalue $q$ has multiplicity 1. Much as in the proof of Theorem 3.2, for any other eigenvalue $\theta$ of $\mathcal{FP}_q$ we have $\theta^2 < 2q - 1$. The theorem follows. □

### 3.3. Sum-Square Graphs over Finite Rings

Suppose that $q = p^r$ for a sufficiently large prime $p$. The sum-square graph $\mathcal{SR}_q$ is defined as follows. The vertex set of the sum-product graph $\mathcal{SR}_q$ is the set

$V(\mathcal{SR}_q) = \mathbb{Z}_q \times \mathbb{Z}_q$. Two vertices $(a,b)$ and $(c,d)$ in $V(\mathcal{SR}_q)$ are connected by an edge in $E(\mathcal{SR}_q)$ if and only if $a + c = (b + d)^2$. We have the following pseudo-randomness of the sum-square graph $\mathcal{SR}_q$.

THEOREM 3.4. *The sum-square graph $\mathcal{SR}_q$ is a $\big(p^{2r}, p^r, \sqrt{2rp^{2r-1}}\big)$-graph.*

*Proof.* It is easy to see that $\mathcal{SR}_q$ is a regular graph of order $p^{2r}$ and valency $p^r$. We now compute the eigenvalues of this multi-graph. For any $(a,b),(c,d) \in \mathbb{Z}_{p^r} \times \mathbb{Z}_{p^r}$, we count the number of solutions of the following system:

$$a + u = (b + v)^2, \quad c + u = (d + v)^2, \quad u, v \in \mathbb{Z}_{p^r}. \tag{3.2}$$

For each solution $v$ of

$$(b - d)(2v + b + d) = a - c, \tag{3.3}$$

there exists a unique $u$ satisfying the system (3.5). Therefore, we need only count the number of solutions of (3.6).

Let $0 \le \alpha \le r$ be the largest power such that $b - d$ is divisible by $p^\alpha$. Suppose that $p^\alpha|(a - c)$. Let $\gamma = (a - c)/p^\alpha$ and $\beta = (b - d)/p^\alpha$. Since $\beta \in \mathbb{Z}^\times_{p^{r-\alpha}}$, there exists a unique solution $v \in \mathbb{Z}_{p^{r-\alpha}}$ of $\beta v = \gamma$. Substituting back into (3.6) yields $p^\alpha$ solutions. Hence (3.5) has $p^\alpha$ solutions if $p^\alpha|(a - c)$ and has no solution otherwise.

So for any two vertices $(a,b)$ and $(c,d)$ in $V(\mathcal{SR}_q)$, let $p^\alpha = \gcd(b - d, p^r)$; then $(a,b)$ and $(c,d)$ have $p^\alpha$ common neighbors if $p^\alpha|(c - a)$ and have no common neighbors otherwise. Let $A$ be the adjacency matrix of $\mathcal{SR}_q$. It follows that

$$A^2 = J + (p^r - 1)I - \sum_{\alpha=0}^{r-1} E_\alpha + \sum_{\alpha=1}^{r-1}(p^\alpha - 1)F_\alpha. \tag{3.4}$$

Here $J$ is the all-1 matrix, $I$ is the identity matrix, and $E_\alpha$ is the adjacency matrix of the graph $B_{E,\alpha}$, where the vertex set of $B_{E,\alpha}$ is $\mathbb{Z}_q \times \mathbb{Z}_q$ and, for any two vertices $U = (a,b)$ and $V = (c,d)$ with $U, V \in V(B_{E,\alpha})$, we have that $(U,V)$ is an edge of $B_{E,\alpha}$ if and only if $p^\alpha = \gcd(b - d, p^r) > \gcd(a - c, p^r)$; also, $F_\alpha$ is the adjacency matrix of the graph $B_{F,\alpha}$, where the vertex set of $B_{F,\alpha}$ is $\mathbb{Z}_q \times \mathbb{Z}_q$ and, for any two vertices $U = (a,b)$ and $V = (c,d)$ with $U, V \in V(B_{F,\alpha})$, we have that $(U,V)$ is an edge of $B_{F,\alpha}$ if and only if $p^\alpha = \gcd(b - d, p^r) \le \gcd(a - c, p^r)$. Hence for any $\alpha > 0$ it follows that $B_{E,\alpha}$ is a regular graph of order less than $p^{2r-\alpha}$ and that $B_{F,\alpha}$ is a regular graph of order less than $p^{2(r-\alpha)}$. Therefore, all eigenvalues of $E_\alpha$ are at most $p^{2r-\alpha}$ and all eigenvalues of $F_\alpha$ are at most $p^{2(r-\alpha)}$. Note that $E_0$ is a zero matrix.

Since $\mathcal{SR}_q$ is a $p^r$-regular graph, $p^r$ is an eigenvalue of $A$ with the all-1 eigenvector $\mathbf{1}$. The graph $\mathcal{SR}_q$ is connected, so the eigenvalue $p^r$ has multiplicity 1. Since the graph $\mathcal{SR}_q$ contains (many) triangles, it is not bipartite. As a result, $|\theta| < p^r$ for any other eigenvalue $\theta$. Let $\boldsymbol{v}_\theta$ denote the corresponding eigenvector of $\theta$. Note that $\boldsymbol{v}_\theta \in \mathbf{1}^\perp$, so $J\boldsymbol{v}_\theta = 0$. It then follows from (3.7) that

$$(\theta^2 - p^r + 1)\boldsymbol{v}_\theta = \bigg(-\sum_{\alpha=1}^{r-1} E_\alpha + \sum_{\alpha=1}^{r-1}(p^\alpha - 1)F_\alpha\bigg)\boldsymbol{v}_\theta.$$

Thus $\boldsymbol{v}_\theta$ is also an eigenvalue of

$$\sum_{\alpha=1}^{r-1}(p^\alpha - 1)F_\alpha - \sum_{\alpha=1}^{r-1} E_\alpha.$$

Since eigenvalues of the sum of the matrices are bounded by the sum of the largest eigenvalues of the summands, we have

$$\begin{aligned}\theta^2 &\leq p^r - 1 + \sum_{\alpha=1}^{r-1} p^{2r-\alpha} + \sum_{\alpha=1}^{r-1}(p^\alpha - 1)p^{2(r-\alpha)} \\ &< 2rp^{2r-1}.\end{aligned}$$

The lemma follows. □

### 3.4. Sum-Product Graphs over Finite Rings

Suppose that $q = p^r$ for some odd prime $p$ and integer $r \geq 2$. The sum-product graph $\mathcal{RP}_q$ is defined as follows. The vertex set of the sum-product graph $\mathcal{RP}_q$ is the set $V(\mathcal{RP}_q) = \mathbb{Z}_q \times \mathbb{Z}_q$. Two vertices $(a, b)$ and $(c, d)$ in $V(\mathcal{RP}_q)$ are connected by an edge in $E(\mathcal{RP}_q)$ if and only if $a + c = bd$. We have the following pseudo-randomness of the sum-product graph $\mathcal{RP}_q$.

Theorem 3.5 [17, Thm. 2.3]. *The sum-product graph $\mathcal{RP}_q$ is a $\left(p^{2r}, p^r, \sqrt{2rp^{2r-1}}\right)$-graph.*

*Proof.* It is easy to see that $\mathcal{RP}_q$ is a regular graph of order $p^{2r}$ and valency $p^r$. We now compute the eigenvalues of this multi-graph. For any $(a, b), (c, d) \in \mathbb{Z}_{p^r} \times \mathbb{Z}_{p^r}$, we count the number of solutions of the following system:

$$a + u = bv, \quad c + u = dv, \quad u, v \in \mathbb{Z}_{p^r}. \tag{3.5}$$

For each solution $v$ of

$$(b - d)v = a - c, \tag{3.6}$$

there exists a unique $u$ satisfying the system (3.5). Therefore, we need only count the number of solutions of (3.6).

Let $0 \leq \alpha \leq r$ be the largest power such that $b - d$ is divisible by $p^\alpha$. Suppose that $p^\alpha | (a - c)$. Let $\gamma = (a - c)/p^\alpha$ and $\beta = (b - d)/p^\alpha$. Since $\beta \in \mathbb{Z}_{p^{r-\alpha}}^\times$, there exists a unique solution $v \in \mathbb{Z}_{p^{r-\alpha}}$ of $\beta v = \gamma$. Substituting back into (3.6) yields $p^\alpha$ solutions. Hence (3.5) has $p^\alpha$ solutions if $p^\alpha | (a - c)$ and has no solution otherwise.

So for any two vertices $(a, b)$ and $(c, d)$ in $V(\mathcal{RP}_q)$, let $p^\alpha = \gcd(b - d, p^r)$; then $(a, b)$ and $(c, d)$ have $p^\alpha$ common neighbors if $p^\alpha | (c - a)$ and otherwise have no common neighbors. Let $A$ be the adjacency matrix of $\mathcal{RP}_q$. It follows that

$$A^2 = J + (p^r - 1)I - \sum_{\alpha=0}^{r-1} E_\alpha + \sum_{\alpha=1}^{r-1}(p^\alpha - 1)F_\alpha. \tag{3.7}$$

Here $J$ is the all-1 matrix, $I$ is the identity matrix, and $E_\alpha$ is the adjacency matrix of the graph $B_{E,\alpha}$, where the vertex set of $B_{E,\alpha}$ is $\mathbb{Z}_q \times \mathbb{Z}_q$ and, for any two vertices $U = (a, b)$ and $V = (c, d)$ with $U, V \in V(B_{E,\alpha})$, we have that $(U, V)$ is an edge of $B_{E,\alpha}$ if and only if $p^\alpha = \gcd(b-d, p^r) > \gcd(a-c, p^r)$; also, $F_\alpha$ is the adjacency matrix of the graph $B_{F,\alpha}$, where the vertex set of $B_{F,\alpha}$ is $\mathbb{Z}_q \times \mathbb{Z}_q$ and, for any two vertices $U = (a,b)$ and $V = (c,d)$ with $U, V \in V(B_{F,\alpha})$, we have that $(U,V)$ is an edge of $B_{F,\alpha}$ if and only if $p^\alpha = \gcd(b-d, p^r) \le \gcd(a-c, p^r)$. Hence for any $\alpha > 0$ it follows that $B_{E,\alpha}$ is a regular graph of order less than $p^{2r-\alpha}$ and that $B_{F,\alpha}$ is a regular graph of order less than $p^{2(r-\alpha)}$. Therefore, all eigenvalues of $E_\alpha$ are at most $p^{2r-\alpha}$ and all eigenvalues of $F_\alpha$ are at most $p^{2(r-\alpha)}$. Note that $E_0$ is a zero matrix.

Since $\mathcal{RP}_q$ is a $p^r$-regular graph, $p^r$ is an eigenvalue of $A$ with the all-1 eigenvector $\mathbf{1}$. The graph $\mathcal{RP}_q$ is connected, so the eigenvalue $p^r$ has multiplicity 1. Since the graph $\mathcal{RP}_q$ contains (many) triangles, it is not bipartite. As a result, $|\theta| < p^r$ for any other eigenvalue $\theta$. Let $\boldsymbol{v}_\theta$ denote the corresponding eigenvector of $\theta$. Note that $\boldsymbol{v}_\theta \in \mathbf{1}^\perp$, so $J\boldsymbol{v}_\theta = 0$. It then follows from (3.7) that

$$(\theta^2 - p^r + 1)\boldsymbol{v}_\theta = \left(-\sum_{\alpha=1}^{r-1} E_\alpha + \sum_{\alpha=1}^{r-1} (p^\alpha - 1)F_\alpha\right)\boldsymbol{v}_\theta.$$

Thus $\boldsymbol{v}_\theta$ is also an eigenvalue of

$$\sum_{\alpha=1}^{r-1} (p^\alpha - 1)F_\alpha - \sum_{\alpha=1}^{r-1} E_\alpha.$$

Since eigenvalues of the sum of the matrices are bounded by the sum of the largest eigenvalues of the summands, we have

$$\begin{aligned}\theta^2 &\le p^r - 1 + \sum_{\alpha=1}^{r-1} p^{2r-\alpha} + \sum_{\alpha=1}^{r-1} (p^\alpha - 1)p^{2(r-\alpha)}\\ &< 2rp^{2r-1}.\end{aligned}$$

The lemma follows. □

## 4. Distance Sets

### *4.1. Proof of Theorem 2.3*

As a consequence of Theorem 3.2, we have the following lemma.

LEMMA 4.1. *For any $A, B, C \subseteq \mathbb{F}_q$,*

$$|\{a + (b-c)^2 : a \in A,\ b \in B,\ c \in C\}| \gtrsim \min\left\{q, \frac{|A||B||C|}{q}\right\}.$$

*Proof.* Let $D = \{a + (b-c)^2 : a \in A,\ b \in B,\ c \in C\} \subset \mathbb{F}_q$. Let $N$ be the number of solutions of the equation $-d + a + (b-c)^2 = 0$, where $(a,b,c,d) \in A \times B \times C \times D$. It is clear that $N = |A||B||C|$. Moreover, $N$ is the number of edges between $(-D) \times B$ and $A \times (-C)$ of the sum-square graph $\mathcal{FS}_q$. From Lemma 3.1 and Theorem 3.2 it now follows that

$$\left| |A||B||C| - \frac{|A||B||C||D|}{q} \right| \leq \sqrt{2q|A||B||C||D|}$$

or, equivalently,

$$|A||B||C| \leq \frac{|A||B||C||D|}{q} + \sqrt{2q|A||B||C||D|}.$$

Let $t = \sqrt{|D|} \geq 0$. Then

$$\frac{\sqrt{|A||B||C|}}{q} t^2 + \sqrt{2q}t - \sqrt{|A||B||C|} \geq 0,$$

which implies that

$$\begin{aligned}\sqrt{|D|} &\geq \frac{-\sqrt{2q} + \sqrt{2q + 4|A||B||C|/q}}{2\sqrt{|A||B||C|/q}} \\ &= \frac{2\sqrt{|A||B||C|}}{\sqrt{2q} + \sqrt{2q + 4|A||B||C|/q}} \\ &\gtrsim \min\left\{\sqrt{q}, \sqrt{\frac{|A||B||C|}{q}}\right\}.\end{aligned}$$

This concludes the proof of the lemma. □

We are now ready to prove Theorem 2.3. We proceed by induction on $n$. For the base case $n = 2$, let $X = \{(a-b)^2 : a, b \in A\}$ and let $Y = Z = A$. Since $|X| \geq |A|/2$, it follows from Lemma 4.1 that

$$\begin{aligned}|\Delta_{\mathbb{F}}(A^2)| &= |\{x + (y-z)^2 : x \in X,\ y \in Y,\ z \in Z\}| \\ &\gtrsim \min\left\{q, \frac{|X||Y||Z|}{q}\right\} \\ &\gtrsim \min\left\{q, \frac{|A|^3}{q}\right\}.\end{aligned}$$

Suppose the statement holds for $n$; we show that it holds also for $n+1$. Let $X = \Delta_{\mathbb{F}}(A^n)$ and $Y = Z = A$. By the induction hypothesis, we have

$$|X| \gtrsim \min\left\{q, \frac{|A|^{2n-1}}{q^{n-1}}\right\}. \tag{4.1}$$

From (4.2) and Lemma 4.1 it follows that

$$\begin{aligned}|\Delta_{\mathbb{F}}(A^{n+1})| &= |\{x + (y-z)^2 : x \in X,\ y \in Y,\ z \in Z\}| \\ &\gtrsim \min\left\{q, \frac{|X||Y||Z|}{q}\right\} \\ &\gtrsim \min\left\{q, \frac{|A|^{2n+1}}{q^n}\right\},\end{aligned}$$

which concludes the proof of the theorem.

### 4.2. Proof of Theorem 2.7

LEMMA 4.2. *Let $q = p^r$ for $p$ an odd prime and $r \geq 2$ an integer. For any $A, B, C \subseteq \mathbb{Z}_q$,*

$$|\{a + (b-c)^2 : a \in A,\ b \in B,\ c \in C\}| \gtrsim \min\left\{q, \frac{|A||B||C|}{rq^{2-1/r}}\right\}.$$

*Proof.* Let $D = \{a + (b-c)^2 : a \in A,\ b \in B,\ c \in C\} \subset \mathbb{Z}_q$. Let $N$ be the number of solutions of the equation $-d + a + (b-c)^2 = 0$, where $(a, b, c, d) \in A \times B \times C \times D$. It is clear that $N = |A||B||C|$. Moreover, $N$ is the number of edges between $(-D) \times B$ and $A \times (-C)$ of the sum-square graph $\mathcal{SR}_q$. From Lemma 3.1 and Theorem 3.4 it now follows that

$$\left| |A||B||C| - \frac{|A||B||C||D|}{q} \right| \leq \sqrt{2rq^{2-1/r}|A||B||C||D|}$$

or, equivalently,

$$|A||B||C| \leq \frac{|A||B||C||D|}{q} + \sqrt{2rq^{2-1/r}|A||B||C||D|}.$$

Let $t = \sqrt{|D|} \geq 0$. Then

$$\frac{\sqrt{|A||B||C|}}{q} t^2 + \sqrt{2rq^{2-1/r}}\, t - \sqrt{|A||B||C|} \geq 0,$$

which implies that

$$\begin{aligned}\sqrt{|D|} &\geq \frac{-\sqrt{2rq^{2-1/r}} + \sqrt{2rq^{2-1/r} + 4|A||B||C|/q}}{2\sqrt{|A||B||C|/q}} \\ &= \frac{2\sqrt{|A||B||C|}}{\sqrt{2rq^{2-1/r}} + \sqrt{2rq^{2-1/r} + 4|A||B||C|/q}} \\ &\gtrsim \min\left\{\sqrt{q}, \sqrt{\frac{|A||B||C|}{rq^{2-1/r}}}\right\}.\end{aligned}$$

This concludes the proof of the lemma. □

Next we prove Theorem 2.7; we proceed by induction on $n$. For the base case $n = 2$, let $X = \{(a-b)^2 : a, b \in A\}$, $X' = X \cap \mathbb{Z}_q^\times$, and $Y = Z = A$. Since $a, b \in \mathbb{Z}_q^\times$ we have $a^2 = b^2$. Then, for $a = \pm b$,

$$|X| \geq |X'| \geq \frac{|A - A| - |\mathbb{Z}_q^0|}{2} \geq \frac{|A| - p^{r-1}}{2} \gtrsim |A|.$$

It follows from Lemma 4.2 that

$$\begin{aligned}|\Delta_{\mathbb{Z}_q}(A^2)| &= |\{x+(y-z)^2 : x\in X,\ y\in Y,\ z\in Z\}|\\ &\gtrsim \min\left\{q, \frac{|X||Y||Z|}{rq^{2-1/r}}\right\}\\ &\gtrsim \min\left\{q, \frac{|A|^3}{rq^{2-1/r}}\right\}.\end{aligned}$$

Suppose the statement holds for $n$; we show that it holds also for $n+1$. Let $X = \Delta_{\mathbb{Z}_n}(A^n)$ and $Y = Z = A$. By the induction hypothesis, we have

$$|X| \gtrsim \min\left\{q, \frac{|A|^{2n-1}}{(rq^{2-1/r})^{n-1}}\right\}. \tag{4.2}$$

From (4.2) and Lemma 4.1 it follows that

$$\begin{aligned}|\Delta_{\mathbb{Z}_q}(A^{n+1})| &= |\{x+(y-z)^2 : x\in X,\ y\in Y,\ z\in Z\}|\\ &\gtrsim \min\left\{q, \frac{|X||Y||Z|}{rq^{2-1/r}}\right\}\\ &\gtrsim \min\left\{q, \frac{|A|^{2n+1}}{(rq^{2-1/r})^{n}}\right\},\end{aligned}$$

which concludes the proof of the theorem.

## 5. Product Sets: Proof of Theorems 2.4 and 2.8

Similarly to the previous section, we obtain the following lemmas from Theorem 3.3 and Theorem 3.5.

Lemma 5.1. *For any $A, B, C \subseteq \mathbb{F}_q$,*

$$|\{a+bc : a\in A,\ b\in B,\ c\in C\}| \gtrsim \min\left\{q, \frac{|A||B||C|}{q}\right\}.$$

Lemma 5.2. *Let $q = p^r$ for $p$ an odd prime and $r \geq 2$ an integer. Then, for any $A, B, C \subseteq \mathbb{Z}_q$,*

$$|\{a+bc : a\in A,\ b\in B,\ c\in C\}| \gtrsim \min\left\{q, \frac{|A||B||C|}{rq^{2-1/r}}\right\}.$$

Theorem 2.4 and Theorem 2.8 follow from Lemma 5.1 and Lemma 5.2, respectively.

## References

[1] N. Alon and J. H. Spencer, *The probabilistic method,* 2nd ed., Wiley, New York, 2000.

[2] J. Bourgain, *Mordell's exponential sum estimate revisited,* J. Amer. Math. Soc. 18 (2005), 477–499.

[3] J. Bourgain, N. Katz, and T. Tao, *A sum product estimate in finite fields and applications,* Geom. Funct. Anal. 14 (2004), 27–57.

[4] J. Chapman, M. B. Erdogan, 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), 63–93.

[5] D. Covert, D. Hart, A. Iosevich, and I. Uriarte-Tuero, *A Furstenberg–Katznelson–Weiss type theorem on* $(d+1)$*-point configurations in sets of positive density in finite field geometries,* Discrete Math. 311 (2011), 423–430.

[6] D. Covert, A. Iosevich, and J. Pakianathan, *Geometric configurations in the ring of integers modulo* $p^l$, Indiana Univ. Math. J. (to appear).

[7] A. A. Glibichuk, *Additive properties of product sets in an arbitrary finite field,* preprint.

[8] A. A. Glibichuk and S. V. Konyagin, *Additive properties of product sets in fields of prime order,* Additive combinatorics, CRM Proc. Lecture Notes, 43, pp. 279–286, Amer. Math. Soc., Providence, RI, 2007.

[9] L. Guth and N. Katz, *On the Erdős distinct distances problem in the plane,* preprint, arXiv:1011.4105.

[10] D. Hart and A. Iosevich, *Sum and products in finite fields: An integral geometric viewpoint,* Contemp. Math., 464, pp. 129–135, Amer. Math. Soc., Providence, RI, 2008.

[11] 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.

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

[13] N. H. Katz and G. Tardos, *A new entropy inequality for the Erdős distance problem,* Towards a theory of geometric graphs, Contemp. Math., 342, pp. 119–126, Amer. Math. Soc., Providence, RI, 2004.

[14] J. Solymosi, *Incidences and the spectra of graphs,* Building bridges, Bolyai Soc. Math. Stud., 19, pp. 499–513, Springer-Verlag, Berlin, 2008.

[15] J. Solymosi and V. Vu, *Near optimal bounds for the Erdős distinct distances problem in high dimensions,* Combinatorica 28 (2008), 113–125.

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

[17] ———, *Sum and shifted-product subsets of product-sets over finite rings,* Electron. J. Combin. 19 (2012), #P33.

[18] ———, *The solvability of norm, bilinear and quadratic equations over finite fields via spectra of graphs,* Forum Mathematicum (to appear).

[19] ———, *Pinned distance sets and k-simplices in vector spaces over finite rings,* preprint.

[20] V. H. Vu, *Sum-product estimates via directed expanders,* Math. Res. Lett. 15 (2008), 375–388.

D. D. Hieu
Faculty of Mathematics,
Mechanics and Informatics
University of Science
Vietnam National University
Hanoi

duyhieua1t@gmail.com

L. A. Vinh
University of Education
Vietnam National University
Hanoi

vinhla@vnu.edu.vn