Illinois Journal of Mathematics
Volume 61, Numbers 1–2, Spring and Summer 2017, Pages 243–257
S 0019-2082

SOME COMBINATORIAL NUMBER THEORY PROBLEMS OVER FINITE VALUATION RINGS

THANG PHAM AND LE ANH VINH

Abstract. Let $\mathcal{R}$ be a finite valuation ring of order q^r. In this paper, we generalize and improve several well-known results, which were studied over finite fields $\mathbb{F}_q$ and finite cyclic rings $\mathbb{Z}/p^r\mathbb{Z}$, in the setting of finite valuation rings.

1. Introduction

1.1. Dot-product congruence classes of simplices. Let $\mathbb{F}_q$ be a finite field of order q with $q = p^n$ for some prime p and positive integer n. We say that two k-simplices in $\mathbb{F}_q^d$ with vertices $(\mathbf{x}_1, \ldots, \mathbf{x}_{k+1})$, $(\mathbf{y}_1, \ldots, \mathbf{y}_{k+1})$ are in a congruence class if the following condition satisfies

$$\|\mathbf{x}_i - \mathbf{x}_j\| = \|\mathbf{y}_i - \mathbf{y}_j\|, \quad 1 \le i, j \le k+1. \tag{1}$$

Hart and Iosevich [6] made the first investigation on counting the number of congruence classes of simplices determined by a point set in $\mathbb{F}_q^d$. More precisely, they proved that if $|\mathcal{E}| \gg q^{\frac{kd}{k+1} + \frac{k}{2}}$ with $d \ge \binom{k+1}{2}$, then $\mathcal{E}$ contains a copy of all k-simplices with non-zero edges. Several progress on improving this exponent have been made in recent years, for instance, Chapman et al. [3] indicated that one can get a positive proportion of all k-simplices in $\mathbb{F}_q^d$ under the condition $|\mathcal{E}| \gg q^{\frac{d+k}{2}}$, and Bennett et al. [2] improved this condition to $q^{d - \frac{d-1}{k+1}}$. Here, and throughout, $X \ll Y$ means that there exists $C > 0$ such that $X \le CY$, and $X = o(Y)$ means that $X/Y \to 0$ as $q \to \infty$, where X, Y are viewed as functions in q.

A variant of this problem was studied by the second listed author [16] with the condition (1) replaced by

$$\mathbf{x}_i \cdot \mathbf{x}_j = \mathbf{y}_i \cdot \mathbf{y}_j, \quad 1 \le i, j \le k+1. \tag{2}$$

Received September 26, 2016; received in final form December 18, 2017.
2010 *Mathematics Subject Classification.* 05C50, 05C25, 11T24.

In this case, we say that two k-simplices $(\mathbf{x}_1,\ldots,\mathbf{x}_{k+1})$ and $(\mathbf{y}_1,\ldots,\mathbf{y}_{k+1})$ are in a dot-product congruence class.

In [16], the second listed author proved that if $|\mathcal{E}| \gg q^{\frac{d+k}{2}}$, then the number of dot-product congruence classes of k-simplices in $\mathcal{E}$ is at least $(1-o(1))q^{\binom{k+1}{2}}$. This is also an extension of [6, Theorem 1.4], and is the best known result so far. We remark here that the condition (1) is equivalent to the fact that there exist $\theta \in O(d,\mathbb{F}_q)$ (orthogonal group in $\mathbb{F}_q^d$) and $\mathbf{z}\in\mathbb{F}_q^d$ so that $\mathbf{z}+\theta(\mathbf{x}_i)=\mathbf{y}_i$ for $i=1,2,\ldots,k+1$. From this fact, the authors of [2] used ingenious arguments by combining elementary results from group action theory and Fourier analytic methods to get the threshold $q^{d-\frac{d-1}{k+1}}$. However, this approach does not work for the case of dot-product congruence classes of simplices, since we cannot guarantee that there exist $\theta\in O(d,\mathbb{F}_q)$ and $\mathbf{z}\in\mathbb{F}_q^d$ so that $\mathbf{z}+\theta(\mathbf{x}_i)=\mathbf{y}_i$ for $i=1,2,\ldots,k+1$ when two simplices are in a dot-product congruence class.

For the case $k=1$ and $d=2$, it has been shown that if $|\mathcal{E}|\gg q^{4/3}$, then the number of congruence classes of 1-simplices in $\mathcal{E}$ (distinct distances) is at least $\gg q$. However, for the dot-product case, the best known exponent on the cardinality of $\mathcal{E}$ to get $\gg q$ dot-product congruence classes of 1-simplices in $\mathcal{E}$ (distinct dot product values) is $q^{3/2}$. If we assume that any line passing through the origin contains at most $|\mathcal{E}|^{1/2}$ points, then the exponent $q^{4/3}$ also holds for the dot-product problem, see [7], [8] for more details. For general cases, improving the threshold $q^{3/2}$ to $q^{4/3}$ is still an open question.

Let $\mathcal{R}$ be a finite valuation ring of order q^r, where $q=p^n$ is an odd prime power. Throughout, $\mathcal{R}$ is assumed to be commutative, and to have an identity. Let us denote the set of units, non-units in $\mathcal{R}$ by $\mathcal{R}^*$, $\mathcal{R}^0$, respectively. Note that finite fields and finite cyclic rings are special cases of finite valuation rings.

The initial result on the dot product problem in the setting of finite valuation rings was given by Nica in [10]. The precise statement is as follows.

Theorem 1 (Nica, [10]). *Let $\mathcal{E}$, $\mathcal{F}$ be two sets in $\mathcal{R}^d$. For any $\lambda\in\mathcal{R}^*$, let $N_\lambda(\mathcal{E},\mathcal{F})$ be the number of pairs $(\mathbf{a},\mathbf{b})\in\mathcal{E}\times\mathcal{F}$ satisfying $\mathbf{a}\cdot\mathbf{b}=\lambda$. Then we have the following estimate*

$$\left|N_\lambda(\mathcal{E},\mathcal{F})-\frac{|\mathcal{E}||\mathcal{F}|}{q^r}\right|\le q^{(d-1)(r-1/2)}\sqrt{|\mathcal{E}||\mathcal{F}|}.$$

Theorem 1 implies that if $|\mathcal{E}||\mathcal{F}|\ge q^{d(2r-1)+1}$, then for any $\lambda\in\mathcal{R}^*$, the equation $\mathbf{a}\cdot\mathbf{b}=\lambda$ is solvable with $a\in\mathcal{E}$, $b\in\mathcal{F}$.

Motivated by this result, in this paper we prove the following result on the number of dot-product congruence classes of k-simplices over finite valuation rings.

THEOREM 2. *Let $\mathcal{R}$ be a finite valuation ring of order q^r. Given a set $\mathcal{E}\subseteq\mathcal{R}^d$. Suppose that*

$$|\mathcal{E}|\gg q^{\frac{(d-1)(2r-1)+r(k+1)}{2}}.$$

Then the number of dot-product congruence classes of k-simplices in $\mathcal{E}$ is at least $(1-o(1))q^{r\binom{k+1}{2}}$.

1.2. An improvement on the number of triangle areas. For $\mathcal{E}\subseteq\mathbb{F}_q^d$, we define

$$V_d(\mathcal{E}):=\left\{\det\left(\mathbf{x}^1-\mathbf{x}^{d+1},\ldots,\mathbf{x}^d-\mathbf{x}^{d+1}\right)\colon \mathbf{x}^i\in\mathcal{E},1\le i\le d+1\right\} \tag{3}$$

as the set of d-dimensional volumes determined by $\mathcal{E}$, and the set of pinned volumes at a point $\mathbf{z}\in\mathcal{E}$

$$V_d^{\mathbf{z}}(\mathcal{E}):=\left\{\det\left(\mathbf{x}^1-\mathbf{z},\ldots,\mathbf{x}^d-\mathbf{z}\right)\colon \mathbf{x}^i\in\mathcal{E},1\le i\le d\right\}. \tag{4}$$

In [9], Iosevich, Rudnev, and Zhai showed that if $|\mathcal{E}|\ge 64q\log q$, then there exists a point $\mathbf{z}\in\mathcal{E}$ such that $|V_2^{\mathbf{z}}(\mathcal{E})|\ge q/2$. Note that if we take $\mathcal{E}$ being a set of all points on a line, then there is no non-zero triangle area determined by points in $\mathcal{E}$. Thus this result is sharp up to a factor of $64\log q$.

Note that a construction in Corollary 2.4 in [8] implies that if $|\mathcal{E}|=o(q^{3/2})$, then there exists $\mathbf{z}\in\mathcal{E}$ such that $|V_2^{\mathbf{z}}(\mathcal{E})|=o(q)$. Thus, Iosevich et al.'s result cannot be improved to say that one gets a positive proportion of the areas from any fixed vertex. The interested reader can find more related discussions in [9].

The finite cyclic ring analogue of this problem is recently investigated by Yazici [17]. In particular, she proved that for $\mathcal{E}\subseteq\mathbb{Z}/p^r\mathbb{Z}$, if $|\mathcal{E}|\ge p^{2r-(1/2)}$ then $|V_2(\mathcal{E})|\ge\frac{p^r}{4}\frac{1+p}{p}-1$. This implies that if $r=1$, Yazici's bound is weaker than that of [9]. In this section, we will give an improvement of this result in the setting of finite valuation rings.

THEOREM 3. *Let $\mathcal{R}$ be a finite valuation ring of order q^r. Let $\mathcal{E}$ be a set of points in $\mathcal{R}^2$. If $|\mathcal{E}|\gg q^{2r-1}$, then there exists $\mathbf{z}\in\mathcal{E}$ such that $|V_2^{\mathbf{z}}(\mathcal{E})|\gg q^r$.*

Theorem 3 implies that when $\mathcal{R}$ is a finite field, that is, $r=1$, in order to get $(1-o(1))q$ distinct areas we only need the condition $q=o(|\mathcal{E}|)$. This means that we can chop off the logarithmic term in Iosevich et al.'s result. When $\mathcal{R}$ is a finite cyclic ring, that is, q is a prime p, the bound $p^{2r-\frac{1}{2}}$ in [17] is decreased to p^{2r-1}.

We remark here that if $\mathcal{E}=\{(x,y)\colon x,y\in\mathcal{R}^0\}$, then $|\mathcal{E}|=q^{2r-2}$. One can check that $V_2(\mathcal{E})\subseteq\mathcal{R}^0$, therefore $|V_2(\mathcal{E})|=o(q^r)$. Thus, there is a gap between q^{2r-2} and q^{2r-1} for $r\ge 2$. From this construction, we conjecture that the condition on the size of $\mathcal{E}$ can be improved to $q^{2r-2+\epsilon}$ for any $\epsilon>0$.

By using inductive arguments, one can obtain a similar result for higher dimensional cases, which is also a generalization of the main result in [14].

THEOREM 4. *Let $\mathcal{R}$ be a finite valuation ring of order q^r, and let $\mathcal{E}$ be a set of points in $\mathcal{R}^d$. If $|\mathcal{E}| \gg q^{r-1} \cdot q^{r(d-1)}$, then then there exists a point $\mathbf{z} \in \mathcal{E}$ such that $|V_d^{\mathbf{z}}(\mathcal{E})| \gg q^r$.*

1.3. An improvement on permanents of matrices. Let M be an $k \times k$ matrix. The permanent of M is defined by

$$\mathtt{Per}(M) := \sum_{\sigma \in S_k} \prod_{i=1}^{k} a_{i\sigma(i)}.$$

For $\mathcal{E} \subseteq \mathbb{F}_q^k$, let $M_k(\mathcal{E})$ denote the set of $k \times k$ matrices with rows in $\mathcal{E}$, and $P_k(\mathcal{E}) = \{\mathtt{Per}(M) \colon M \in M_k(\mathcal{E})\}$. In the setting of finite fields, the second listed author [13] proved that for $\mathcal{E} \subseteq \mathbb{F}_q^k$, if $|\mathcal{E}| \gg kq^{k-1}$, then $\mathbb{F}_q \setminus \{0\} \subseteq P_k(\mathcal{E})$. He also indicated that this result is sharp up to a factor of k, for instance, $|\{\mathbf{x} \in \mathbb{F}_q^k \colon x_1 = 0\}| = q^{k-1}$, and $P_k(\{\mathbf{x} \in \mathbb{F}_q^k \colon x_1 = 0\}) = \{0\}$. In the case when $\mathcal{E}$ is the Cartesian product of sets, the author of [13] obtained an improvement. Namely, he showed that for $\mathcal{A} \subseteq \mathbb{F}_q$, if $|\mathcal{A}| \gg q^{\frac{1}{2}+\frac{1}{2k}}$ then $\mathbb{F}_q \setminus \{0\} \subset P_k(\mathcal{A}^k)$. The author of [13] also made a conjecture that the exponent $q^{\frac{1}{2}+\frac{1}{2k}}$ can be decreased to $q^{\frac{1}{2}+\epsilon}$ for any $\epsilon > 0$, when k is sufficiently large.

By employing the same techniques, a similar result was obtained in the setting of finite cyclic rings $\mathbb{Z}/p^r\mathbb{Z}$ in [15]. The author of [15] showed that for any $\mathcal{A} \subseteq \mathbb{Z}/p^r\mathbb{Z}$, if

$$|\mathcal{A}| \gg rp^{r-\frac{1}{2}+\frac{1}{2k}},$$

then $(\mathbb{Z}/p^r\mathbb{Z})^* \subseteq P_k(\mathcal{A}^k)$ with $\gcd(k, p^r) = 1$, where $(\mathbb{Z}/p^r\mathbb{Z})^*$ is the set of all units in $\mathbb{Z}/p^r\mathbb{Z}$

In this paper, we are able to improve the threshold $q^{r-\frac{1}{2}+\frac{1}{2k}}$ to $q^{\frac{(k-1)(2r-1)+r}{2k-1}}$ to get a positive proportion of permanents in a more general setting.

THEOREM 5. *Let $\mathcal{R}$ be a finite valuation rings of order q^r, and k be an integer with* $\gcd(k, q^r) = 1$. *For any $\mathcal{A} \subset \mathcal{R}$, if*

$$|\mathcal{A}| \gg q^{\frac{(k-1)(2r-1)+r}{2k-1}},$$

then $|P_k(\mathcal{A}^k)| \gg q^r$.

1.4. Monochromatic sum-product. For $A_1, A_2 \subset \mathbb{F}_p$, where p is a prime, Shkredov [11] showed that $|A_1||A_2| \geq 20p$, then there exist $x, y \in \mathbb{F}_p$ such that $x + y \in A_1, x \cdot y \in A_2$. Cilleruelo [4] extended this result to arbitrary finite fields $\mathbb{F}_q$ of q elements using Sidon sets as follows.

THEOREM 6 ([4]). *For any $X_1, X_2 \subseteq \mathbb{F}_q$ of cardinality $|X_1||X_2| > 2q$, there exist $x, y \in \mathbb{F}_q$ such that $x + y \in X_1, x \cdot y \in X_2$.*

In this section, we extend Theorem 6 to the setting of finite valuation rings.

Theorem 7. *Let $\mathcal{R}$ be a finite valuation ring of order q^r. For any $X_1, X_2 \subseteq \mathcal{R}^*$ of cardinality*

$$|X_1||X_2| > \frac{q^{4r-1}}{(q^r - q^{r-1})^2},$$

there exist $x, y \in \mathcal{R}^*$ such that $x + y \in X_1$ and $x \cdot y \in X_2$.

The rest of this paper is organized as follows: in Section 2, we recall the definition and some properties of finite valuation rings from [10]. Some tools from spectral graph theory are mentions in Section 3. The proofs of Theorems 2, 3, 5, and 7 are given in Sections 4–7.

2. Preliminaries

We say that a ring $\mathcal{R}$ is *local* if $\mathcal{R}$ has a unique maximal ideal that contains every proper ideal of $\mathcal{R}$. $\mathcal{R}$ is *principal* if every ideal in $\mathcal{R}$ is principal. The following is the definition of finite valuation rings taken from [10].

Definition 8. Finite valuation rings (FVR) are finite rings that are local and principal.

Throughout, rings are assumed to be commutative, and to have an identity. Let $\mathcal{R}$ be a finite valuation ring, then $\mathcal{R}$ has a unique maximal ideal that contains every proper ideals of $\mathcal{R}$. This implies that there exists a non-unit z called *uniformizer* in $\mathcal{R}$ such that the maximal ideal is generated by z. Throughout this paper, we denote the maximal ideal of $\mathcal{R}$ by (z). Moreover, we also note that the uniformizer z is defined up to a unit of $\mathcal{R}$.

There are two structural parameters associated to $\mathcal{R}$ as follows: the cardinality of the residue field $F = \mathcal{R}/(z)$, and the nilpotency degree of z, where the nilpotency degree of z is the smallest integer r such that $z^r = 0$. Let us denote the cardinality of F by q. In this note, q is assumed to be odd, then 2 is a unit in $\mathcal{R}$.

If $\mathcal{R}$ is a finite valuation ring, and r is the nilpotency degree of z, then we have a natural valuation

$$\nu \colon \mathcal{R} \to \{0, 1, \ldots, r\}$$

defined as follows: $\nu(0) = r$, for $x \neq 0$, $\nu(x) = k$ if $x \in (z^k) \setminus (z^{k+1})$. We also note that $\nu(x) = k$ if and only if $x = uz^k$ for some unit u in $\mathcal{R}$. Each Abelian group $(z^k)/(z^{k+1})$ is a one-dimensional linear space over the residue field $F = \mathcal{R}/(z)$, thus its size is q. This implies that $|(z^k)| = q^{r-k}$, $k = 0, 1, \ldots, r$. In particular, $|(z)| = q^{r-1}, |\mathcal{R}| = q^r$ and $|\mathcal{R}^*| = |\mathcal{R}| - |(z)| = q^r - q^{r-1}$. The following are some examples of finite valuation rings:

(1) Finite fields $\mathbb{F}_q$, $q = p^n$ for some $n > 0$.
(2) Finite rings $\mathbb{Z}/p^r\mathbb{Z}$, where p is a prime.

(3) $\mathcal{O}/(p^r)$ where $\mathcal{O}$ is the ring of integers in a number field and $p \in \mathcal{O}$ is a prime.

(4) $\mathbb{F}_q[x]/(f^r)$, where $f \in \mathbb{F}_q[x]$ is an irreducible polynomial.

3. Tools from spectral graph theory

We say that a bipartite graph $G = (A \cup B, E)$ is *biregular* if in both of its two parts, all vertices have the same degree. If A is one of the two parts of a bipartite graph, we write $\deg(A)$ for the common degree of the vertices in A. Label the eigenvalues so that $|\lambda_1| \geq |\lambda_2| \geq \cdots \geq |\lambda_n|$. Note that in a bipartite graph, we have $\lambda_2 = -\lambda_1$. In this paper, we denote the adjacency matrix of G by M. The following is the expander mixing lemma for bipartite graphs. The reader can find a detailed proof in [5].

Lemma 9. *Suppose G is a bipartite graph with parts A, B such that the vertices in A all have degree a and the vertices in B all have degree b. For any two sets $X \subset A$, and $Y \subset B$, the number of edges between X and Y, $e(X,Y)$, satisfies*

$$\left| e(X,Y) - \frac{a}{|B|}|X||Y| \right| \leq \lambda_3 \sqrt{|X||Y|},$$

where λ_3 is the third eigenvalue of G.

The following theorem is an analogue of [1, Theorem 9.2.4].

Theorem 10. *Let $G = (A \cup B, E)$ be a bipartite graph as in Lemma 9, and U, V two subsets in A, B, respectively. Then we have the following estimate*

$$\sum_{u \in U} \left(N_V(u) - \frac{a}{|B|}|V| \right)^2 \leq \lambda_3^2 |V|,$$

where $N_V(u) = N(u) \cap V$, and $N(u)$ is the set of all neighbors of u.

Proof. Let denote $c = |V|/|B|$, and x be a vector, where $x_i = I_{i \in V} - c\mathbf{1}_B$. We note that $\sqrt{a}\mathbf{1}_A \pm \sqrt{b}\mathbf{1}_B$ are eigenvectors corresponding to λ_1, λ_n. It follows from the definition of x that $\langle x, \mathbf{1}_A \rangle = 0$ and $\langle x, \mathbf{1}_B \rangle = 0$. Then $x \in W$, and $\|Mx\|^2 \leq \lambda_3^2 \|x\|^2$. We note that

$$\langle Mx, Mx \rangle = \sum_{u \in A} \left(N_V(u) - \frac{a|V|}{|B|} \right)^2,$$

and $\|x\|^2 = (1-c)^2|V| + (|B| - |V|)c^2 = (1-c)|V| < |V|$, then the lemma follows from the fact that

$$\sum_{u \in U} \left(N_V(u) - \frac{a|V|}{|B|} \right)^2 \leq \sum_{u \in A} \left(N_V(u) - \frac{a|V|}{|B|} \right)^2. \qquad \square$$

3.1. Product graphs over finite valuation rings. We define the product graphs $\mathcal{P}_{q,r}(\mathcal{R}) = (A \cup B, E)$ over finite valuation rings $\mathcal{R}$ as follows: $A = B = \mathcal{R}^d \setminus (\mathcal{R}^0)^d$, and there is an edge between $\mathbf{x} \in A$ and $\mathbf{y} \in B$ if and only if $\mathbf{x} \cdot \mathbf{y} = 1$. The spectrum of this graph was given by Nica [10].

Theorem 11 (Nica, [10]). *The cardinality of each vertex part of $\mathcal{P}_{q,r}(\mathcal{R})$ is $q^{dr} - q^{d(r-1)} = (1 - o(1))q^{dr}$, and $\deg(A) = \deg(B) = q^{(d-1)r}$. The third eigenvalue of $\mathcal{P}_{q,r}(\mathcal{R})$ is at most $\sqrt{q^{(d-1)(2r-1)}}$.*

3.2. Erdős–Rényi graphs over FVR. For any $\mathbf{x}$ in $\mathcal{R}^d \backslash (\mathcal{R}^0)^d$, we denote $[\mathbf{x}]$ the equivalence class of $\mathbf{x}$ in $\mathcal{R}^d \backslash (\mathcal{R}^0)^d$, where $\mathbf{x}, \mathbf{y} \in \mathcal{R}^d \backslash (\mathcal{R}^0)^d$ are equivalent if and only if $\mathbf{x} = t\mathbf{y}$ for some $t \in \mathcal{R}^*$. Let $\mathcal{E}_{q,d}(\mathcal{R})$ denote the Erdős–Rényi bipartite graph $\mathcal{E}_{q,d}(\mathcal{R}) = (A \cup B, E)$ whose vertices in each part are the points of the projective space over $\mathcal{R}$, where two vertices $[\mathbf{x}]$ and $[\mathbf{y}]$ are connected if and only if $\mathbf{x} \cdot \mathbf{y} = 0$. We have the following theorem on the spectrum of $\mathcal{E}_{q,d}(\mathcal{R})$.

Theorem 12 (Nica, [10]). *The cardinality of each vertex part of $\mathcal{E}_{q,d}(\mathcal{R})$ is $q^{(d-1)(r-1)}(q^d - 1)/(q - 1)$, and $\deg(A) = \deg(B) = q^{(d-2)(r-1)}(q^{d-1} - 1)/(q - 1)$. The third eigenvalue of $\mathcal{E}_{q,d}(\mathcal{R})$ is at most $\sqrt{q^{(d-2)(2r-1)}}$.*

As an application of the Erdős–Rényi graph $\mathcal{E}_{q,2d}(\mathcal{R})$, we obtain the following theorem which is a generalization of [9, Theorem 9]. Some of its applications over finite fields can be found in [8], [9].

Theorem 13. *Let F and G be subsets in $\mathcal{R}^d$. Suppose that $F \cap (\mathcal{R}^0)^d = \emptyset$. Let, for $t \in \mathcal{R}$,*

$$\nu(t) := \left|\left\{(\mathbf{x}, \mathbf{y}) \in F \times G \colon \mathbf{x} \cdot \mathbf{y} = t\right\}\right|,$$

where $\mathbf{x} \cdot \mathbf{y} = x_1 y_1 + \cdots + x_d y_d$. Then

$$\sum_{t \in \mathcal{R}} \nu(t)^2 \leq \frac{|F|^2 |G|^2}{q^r} + q^{(d-1)(2r-1)} |F||G| \cdot \max_{\mathbf{x} \in \mathcal{R}^d \backslash (\mathcal{R}^0)^d} |F \cap l_{\mathbf{x}}|,$$

where

$$l_{\mathbf{x}} := \left\{s\mathbf{x} \colon s \in \mathcal{R}^*\right\},$$

with $\mathbf{x} \in \mathcal{R}^d \setminus (\mathcal{R}^0)^d$.

Proof. For any pair of points $(\mathbf{a}, \mathbf{b}) \in \mathcal{R}^d \times \mathcal{R}^d$, we define

$$p_{\mathbf{a},\mathbf{b}} := (a_1, \ldots, a_d, b_1, \ldots, b_d),$$

and

$$U := \left\{p_{\mathbf{x},-\mathbf{t}} \colon (\mathbf{x}, \mathbf{t}) \in F \times G\right\} \subseteq \mathcal{R}^{2d},$$
$$V := \left\{p_{\mathbf{y},\mathbf{z}} \colon (\mathbf{y}, \mathbf{z}) \in G \times F\right\} \subseteq \mathcal{R}^{2d}.$$

Since $F \cap (\mathcal{R}^0)^d = \emptyset$, U and V are sets of points in $\mathcal{R}^{2d} \backslash (\mathcal{R}^0)^{2d}$. It follows from the definition of $\nu(t)$ that $\sum_{t \in \mathcal{R}} \nu(t)^2$ is the number of quadruples $(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{t}) \in$

$F \times G \times F \times G$ satisfying $\mathbf{x}\cdot\mathbf{y} = \mathbf{z}\cdot\mathbf{t}$. It is clear that if $\mathbf{x}\cdot\mathbf{y} = \mathbf{z}\cdot\mathbf{t}$, then there is an edge between two vertices $[p_{\mathbf{x},-\mathbf{t}}]$ and $[p_{\mathbf{y},\mathbf{z}}]$ in the Erdős–Rényi graph $\mathcal{E}_{q,2d}(\mathcal{R})$. However, we cannot make sure that the number of edges between $[U] := \{[u] \colon u \in U\}$ and $[V] := \{[v] \colon v \in V\}$ in the Erdős–Rényi graph $\mathcal{E}_{q,2d}(\mathcal{R})$ is an upper bound for the sum $\sum_{t\in\mathcal{R}} \nu(t)^2$, since there might exist two points in U determining the same congruence class, that is, the same vertex in the Erdős–Rényi graph $\mathcal{E}_{q,2d}(\mathcal{R})$, for example, $u \in U$ and $\lambda u \in U$ with $\lambda \in \mathcal{R}^* \setminus \{1\}$.

Thus, we will partition U and V to subsets such that no two points in each subset determine the same vertex in the Erdős–Rényi graph.

Since $m = \max_{\mathbf{x}\in\mathcal{R}^d\setminus(\mathcal{R}^0)^d} |F \cap l_{\mathbf{x}}|$, we can partition U into m subsets $U_1,\dots,U_m$ of distinct vertices of the Erdős–Rényi graph $\mathcal{ER}_{q,2d}(\mathcal{R})$. Similarly, we also can partition V into m subsets $V_1,\dots,V_m$ of distinct vertices of the Erdős–Rényi graph $\mathcal{ER}_{q,2d}(\mathcal{R})$. Then, it is clear that

$$\sum_{t\in\mathcal{R}} \nu(t)^2 \le \sum_{i,j} e(U_i,V_j) = \sum_{j=1}^m e(U_1,V_j) + \cdots + \sum_{j=1}^m e(U_m,V_j).$$

On the other hand, for each $1 \le i \le m$, it follows from Lemma 9 and Theorem 12 that

$$\begin{aligned}\sum_{j=1}^m e(U_i,V_j) &\le \frac{|U_i||V|}{q^r} + q^{(d-1)(2r-1)}\sqrt{|U_i}\big(\sqrt{|V_1|} + \cdots + \sqrt{|V_m|}\big)\\ &\le \frac{|U_i||V|}{q^r} + \sqrt{m}q^{(d-1)(2r-1)}\sqrt{|U_i|V|},\end{aligned}$$

where the second inequality follows from the Cauchy–Schwarz inequality. Thus

$$\sum_{t\in\mathcal{R}} \nu(t)^2 \le \frac{|U||V|}{q^r} + q^{(d-1)(2r-1)} m\sqrt{|U||V|}.$$

From the definitions of U and V, we get $|U| = |F||G|$ and $|V| = |F||G|$. Therefore, the theorem follows. □

Now we prove the following theorem that will be used many times in this paper.

THEOREM 14. *Let F and G be subsets in $\mathcal{R}^d$. Suppose that*

$$m = \max_{\mathbf{x}\in\mathcal{R}^d\setminus(\mathcal{R}^0)^d} |F \cap l_{\mathbf{x}}|,$$

then we have

$$\big|\{\mathbf{x}\cdot\mathbf{y} \colon \mathbf{x} \in F, \mathbf{y} \in G\}\big| \gg q^r,$$

when $|F||G| \gg mq^{(d-1)(2r-1)+r}$.

Proof. We first have

$$\big|\{\mathbf{x}\cdot\mathbf{y} \colon \mathbf{x} \in F, \mathbf{y} \in G\}\big| = \big|\{t \colon \nu(t) > 0\}\big|,$$

and

$$\sum_{t\in\mathcal{R}} \nu(t) = |F||G|.$$

On the other hand, let

$$T = \left|\left\{(\mathbf{x}_1, \mathbf{y}_1, \mathbf{x}_2, \mathbf{y}_2) \in F \times G \times F \times G \colon \mathbf{x}_1 \cdot \mathbf{y}_1 = \mathbf{x}_2 \cdot \mathbf{y}_2\right\}\right|,$$

which implies that

$$T = \sum_{t\in\mathcal{R}} \nu(t)^2.$$

It follows from the Cauchy–Schwarz inequality that

$$\left|\left\{t \colon \nu(t) > 0\right\}\right| \sum_{t\in\mathcal{R}} \nu(t)^2 \geq \left(\sum_{t\in\mathcal{R}} \nu(t)\right)^2.$$

Therefore, we obtain

$$\left|\left\{t \colon \nu(t) > 0\right\}\right| \geq \frac{|F|^2|G|^2}{T}. \tag{5}$$

On the other hand, it follows from Theorem 13 that

$$T \leq \frac{|F|^2|G|^2}{q^r} + mq^{(d-1)(2r-1)}|F||G|. \tag{6}$$

Putting (5) and (6) together gives us

$$\left|\left\{\mathbf{x}\cdot\mathbf{y} \colon \mathbf{x} \in F, \mathbf{y} \in G\right\}\right| \gg q^r,$$

when $|F||G| \gg mq^{(d-1)(2r-1)+r}$. This concludes the proof of the theorem. □

4. Proof of Theorem 2

A graph $G = (V, E)$ is called an (n, d, λ)-graph if it is d-regular, has n vertices, and the second eigenvalue of G is at most λ. Suppose that a graph G is edge-colored by a set of finite colors. We say that G is an (n, d, λ)-colored graph if the induced subgraph of G on each color is an $(n, d(1+o(1)), \lambda)$-graph. In [16], the second listed author proved that any large induced subgraph of an (n, d, λ)-colored graph contains almost all possible colorings of small complete subgraphs.

THEOREM 15 ([16, Theorem 2.7]). *For any $t \geq 2$. Let $G = (V, E)$ be an (n, d, λ)-colored graph, and let $m < n$ such that $m \gg \lambda(n/d)^{t/2}$. Suppose that the color set of $\mathcal{C}$ has cardinality $|\mathcal{C}| = (1 - o(1))n/d$, then for every subset $U \subset V$ with cardinality m, the induced subgraph G on U contains at least $(1 - o(1))|\mathcal{C}|^{\binom{t}{2}}$ possible colorings of K_t.*

Let $\mathcal{C} = \mathcal{R}^*$, we now define a graph $G(\mathcal{R})$ as follows: the vertex set of $G(\mathcal{R})$ is $\mathcal{R}^d$ and the edge between $\mathbf{x}$ and $\mathbf{y}$ is colored by the β-color with $\beta \in \mathcal{C}$, if and only of $\mathbf{x} \cdot \mathbf{y} = \beta$.

One can follow the proof of [16, Theorem 2.7] step by step by using Lemma 9, Theorem 10, and Theorem 11 to get a version of Theorem 15 for $G(\mathcal{R})$ as follows.

Theorem 16. *For any $t \geq 2$, and for every subset $U \subset V(G(\mathcal{R}))$ of cardinality $m \gg q^{\frac{(d-1)(2r-1)+rt}{2}}$, the induced subgraph of $G(\mathcal{R})$ on U contains at least $(1 - o(1))q^{r\binom{t}{2}}$ possible colorings of K_t.*

We are now ready to prove Theorem 2.

Proof of Theorem 2. Since $|\mathcal{E}| \gg q^{\frac{(d-1)(2r-1)+r(k+1)}{2}}$, it follows from Theorem 16 that the induced subgraph $G(\mathcal{R})$ on $\mathcal{E}$ contains at least $(1-o(1))q^{r\binom{k+1}{2}}$ possible colorings of K_{k+1}. Moreover, each coloring is corresponding to a dot-product congruence class, thus the number of dot-product congruence classes of k-simplices in $\mathcal{E}$ is at least $(1 - o(1))q^{r\binom{k+1}{2}}$. This ends the proof of the theorem. □

5. Proofs of Theorems 3 and 4

Before giving a proof of Theorem 3, we have the following observation: Since the area of triangle is invariant under translations, we can assume that $\mathbf{0} \in \mathcal{E}$, and the formula of area of the triangle formed by three vertices $\mathbf{0}$, $\mathbf{a} = (a_1, a_2)$ and $\mathbf{b} = (b_1, b_2)$ is $a_1b_2 - a_2b_1$. Let S be the set of triangles in $\mathcal{E}$ which share a common vertex at $\mathbf{0}$. Then the number of distinct areas of triangles in S is at least the cardinality of

$$\mathcal{E} \cdot \mathcal{E}' := \left\{\mathbf{x} \cdot \mathbf{y} \colon \mathbf{x} \in \mathcal{E}, \mathbf{y} \in \mathcal{E}'\right\},$$

where $\mathcal{E}' = \{(y, -x) \colon (x, y) \in \mathcal{E}\}$.

A result of Nica in [10], that is, Theorem 1, states that if $|\mathcal{E}||\mathcal{E}'| > q^{4r-1}$, then $|\mathcal{E} \cdot \mathcal{E}'| \gg q^r - q^{r-1}$. It is clear that $|\mathcal{E}| = |\mathcal{E}'|$. Thus if $|\mathcal{E}| > q^{2r-\frac{1}{2}}$, then the number of distinct areas of triangles in $\mathcal{E}$ is at least $q^r - q^{r-1}$. In fact, the result of Nica [10] gives us even more information, for instance, the number of triangles of area $t \in \mathcal{R}^*$ is at least $(1 - o(1))\frac{|\mathcal{E}|^2}{q^r}$ when $q^{2r-\frac{1}{2}} = o(|\mathcal{E}|)$.

However, in order to decrease from the exponent $q^{2r-\frac{1}{2}}$ to q^{2r-1}, we need to use more complicated and tricky arguments. First, we need to prove the following lemma.

Lemma 17. *Let $\mathcal{R}$ be a finite valuation ring of order q^r, and let $\mathcal{E}$ be a set of $8q^{2r-1}$ points in $\mathcal{R}^2$. Then there exists a point $\mathbf{z}$ of $\mathcal{E}$ such that $\mathbf{z}$ is contained in at least $q^r/8$ lines, and each of these lines passes through at least $q^{r-1} + 1$ points from $\mathcal{E}$.*

Proof of Lemma 17. To prove Lemma 17, we make use of the following theorem on the number of incidences between points and lines in $\mathcal{R}^2$, where a line in $\mathcal{R}^2$ is of the form $ax+by+c=0$ with $(a,b,c)\in R^3\setminus(\mathcal{R}^0)^3$. We will follow the argument of Solymosi [12] in its proof.

Theorem 18. *Let $\mathcal{R}$ be a finite valuation ring of order q^r, $\mathcal{E}$ be a set of points in $\mathcal{R}^2$ and $\mathcal{L}$ be a set of lines in $\mathcal{R}^2$. Then the number of incidences between the point set $\mathcal{E}$ and the line set $\mathcal{L}$, denoted by $I(\mathcal{E},\mathcal{L})$, satisfies*

$$\left|I(\mathcal{E},\mathcal{L})-\frac{|\mathcal{E}||\mathcal{L}|}{q^r}\right|\le q^{(2r-1)/2}\sqrt{|\mathcal{E}||\mathcal{L}|}.$$

Proof. We identify each point $(x_1,x_2)\in\mathcal{E}$ with a vertex $[x_1,x_2,1]$ of the Erdős–Rényi graph $\mathcal{E}_{q,3}(\mathcal{R})$. Let $\mathcal{E}'$ be the set of corresponding vertices. Similarly, we identify each line $ax+by=c$ in $\mathcal{L}$, $(a,b,c)\notin(\mathcal{R}^0)^3$, with a vertex $[a,b,-c]$ of the Erdős–Rényi graph $\mathcal{E}_{q,3}(\mathcal{R})$. Let $\mathcal{L}'$ be the set of corresponding vertices. Then $\mathcal{E}'$ and $\mathcal{L}'$ are sets of distinct vertices with $|\mathcal{E}'|=|\mathcal{E}|$ and $|\mathcal{L}'|=|\mathcal{L}|$.

It is easy to see that the number of incidences between $\mathcal{E}$ and $\mathcal{L}$ equals the number of edges between $\mathcal{E}'$ and $\mathcal{L}'$ in the Erdős–Rényi graph $\mathcal{E}_{q,3}(\mathcal{R})$. It follows from Lemma 9 and Theorem 12 that

$$\left|I(\mathcal{E},\mathcal{L})-\frac{|\mathcal{E}||\mathcal{L}|}{q^r}\right|\le q^{(2r-1)/2}\sqrt{|\mathcal{E}||\mathcal{L}|}.$$

This concludes the proof of the theorem. □

The following is a corollary of Theorem 18.

Corollary 19. *Let $\mathcal{R}$ be a finite valuation ring of order q^r, and let $\mathcal{E}$ be a set of $3q^{2r-1}$ points in $\mathcal{R}^2$. Then the number of distinct lines spanned by $\mathcal{E}$ containing at least $q^{r-1}+1$ points from $\mathcal{E}$ is at least $q^{2r}/4$.*

Proof. Let $\mathcal{L}_1$ be the set of lines in $\mathcal{R}^2$ such that each line contains at most q^{r-1} points from $\mathcal{E}$. We now show that $|\mathcal{L}_1|\le 3q^{2r}/4$. Indeed, we first have $I(\mathcal{E},\mathcal{L}_1)\le q^{r-1}|\mathcal{L}_1|$, and it follows from Theorem 18 that

$$I(\mathcal{E},\mathcal{L}_1)\ge\frac{|\mathcal{E}||\mathcal{L}_1|}{q^r}-q^{(2r-1)/2}\sqrt{|\mathcal{E}||\mathcal{L}_1|}\ge 3q^{r-1}|\mathcal{L}_1|-\sqrt{3}q^{2r-1}\sqrt{|\mathcal{L}_1|}.$$

This implies that

$$2q^{r-1}|\mathcal{L}_1|\le\sqrt{3}q^{2r-1}\sqrt{|\mathcal{L}_1|}.$$

Thus, we obtain

$$|\mathcal{L}_1|\le\frac{3q^{2r}}{4}.$$

On the other hand, the number of lines of the form $y=ax+b$ in $\mathcal{R}^2$ is q^{2r}, then the number of lines of the form $y=ax+b$ containing at least $q^{r-1}+1$ points from $\mathcal{E}$ is at least $q^{2r}/4$. Since any two lines in $\mathcal{R}^2$ have at most q^{r-1}

points in common, these lines are distinct. This completes the proof of the corollary. □

We are ready to give a proof of Lemma 17.

Proof of Lemma 17. Let $\mathcal{L}$ be the set of lines in $\mathcal{R}^2$ such that each line in $\mathcal{L}$ contains at least $q^{r-1}+1$ points from $\mathcal{E}$. It follows from Corollary 19 that $|\mathcal{L}| \geq q^{2r}/4$. From the lower bound of Theorem 18, we have if $|\mathcal{E}||\mathcal{L}| \geq 2q^{4r-1}$, then $I(\mathcal{E},\mathcal{L}) \geq |\mathcal{E}||\mathcal{L}|/q^r$. Thus, it implies that $I(\mathcal{E},\mathcal{L}) \geq q^{3r-1}$. Therefore, by the pigeon-hole principle, there exists a point $\mathbf{z} \in \mathcal{E}$ such that $\mathbf{z}$ is contained in at least $q^r/8$ lines from $\mathcal{L}$, and each of these lines contains at least $q^{r-1}+1$ points from $\mathcal{E}$. □

Proofs of Theorems 3 and 4.

Proof of Theorem 3. Since $|\mathcal{E}| \gg q^{2r-1}$, we may suppose that $|\mathcal{E}| \geq 8q^{2r-1}$. We have $|(\mathcal{R}^0)^2| = o(|\mathcal{E} \cap \mathcal{R}^2 \setminus (\mathcal{R}^0)^2|)$, thus without loss of generality, we can assume that $\mathcal{E} \subseteq \mathcal{R}^2 \setminus (\mathcal{R}^0)^2$. Lemma 17 implies that there exists a point $\mathbf{z} \in \mathcal{E}$ such that $\mathbf{z}$ is contained in at least $q^r/8$ lines, and each of these lines passes through least $q^{r-1}+1$ points from $\mathcal{E}$. We denote the set of these lines by $\mathcal{L}'$.

We now consider the set of triangles in $\mathcal{E}$ which share a common vertex at $\mathbf{z}$. Since the area of a triangle is invariant under translations, we assume that $\mathbf{z} = \mathbf{0}$, and all lines in $\mathcal{L}'$ are of the form $l_k := \{y = kx\}$ with $k \in \mathcal{R}$. It is easy to see that for a fixed $a \in \mathcal{R}$, the points $(x, ax) \notin l_b$ for all $b \neq a$ and $x \in \mathcal{R}^*$. Thus, we can choose $q^r/8$ points of $\mathcal{E}$ from the lines in $\mathcal{L}'$ such that no two points belong to the same line. Let F be the set of such points, and $G := \{(-p_2, p_1) \colon (p_1, p_2) \in \mathcal{E}\}$. Then the number of distinct areas of triangles formed by three vertices $(\mathbf{0}, \mathbf{a}, \mathbf{b}) \in \{\mathbf{0}\} \times F \times G$ is the cardinality of the set $F \cdot G = \{\mathbf{a} \cdot \mathbf{b} \colon \mathbf{a} \in F, \mathbf{b} \in G\}$.

Applying Theorem 14 with $|F| = q^r/8, |G| = 8q^{2r-1}$, $d = 2$, and $m = 1$, we get

$$|F \cdot G| \gg q^r.$$

This implies that the number of distinct areas determined by $\mathcal{E}$ is at least $\gg q^r$. This concludes the proof of the theorem. □

Proof of Theorem 4. We prove Theorem 4 by induction on d. The base case $d = 2$ follows from Theorem 3. Suppose that the statement is true for all $2 < i \leq d-1$, we now show that it also holds for d. Indeed, suppose $|\mathcal{E}| \geq 8q^{r-1}q^{r(d-1)}$, there exists a hyperplane $H_t := \{\mathbf{x} \in \mathcal{R}^d \colon x_d = t\}$ such that $|\mathcal{E} \cap H_t| \geq 8q^{r-1}q^{r(d-2)}$. By induction hypothesis, we have $|V_{d-1}(\mathcal{E} \cap H_t)| \geq q^r/2$.

Since $V_d(\mathcal{E})$ is invariant under translations, we can assume that $t = 0$. Moreover, the number of points of $\mathcal{E}$ satisfying $x_d \in \mathcal{R}^0$ is at most $q^{r-1} \cdot q^{r(d-1)}$.

Thus, there exists a point $\mathbf{z} \in \mathcal{E}$ such that $z_d \in \mathcal{R}^*$. On the other hand, $V_d^{\mathbf{z}}(\mathcal{E})$ are determinants of size $d+1$ of the form

$$\det \begin{pmatrix} 1 & \dots & 1 & 1 \\ x_1^1 & \dots & x_1^d & z_1 \\ \vdots & \ddots & \vdots & \vdots \\ x_{d-1}^1 & \dots & x_{d-1}^d & z_{d-1} \\ 0 & \dots & 0 & z_d \end{pmatrix} = z_d \cdot \det \begin{pmatrix} 1 & \dots & 1 \\ x_1^1 & \dots & x_1^d \\ \vdots & \dots & \vdots \\ x_{d-1}^1 & \dots & x_{d-1}^d \end{pmatrix}.$$

This completes the proof of the Theorem 4. □

6. Proof of Theorem 5

Since $|\mathcal{A}| \gg q^{\frac{(k-1)(2r-1)+r}{2k-1}} > q^{r-1} = |\mathcal{R}^0|$, there exists a unit $u \in \mathcal{A} \cap \mathcal{R}^*$. Let $\mathbf{1} := (1, \dots, 1) \in \mathcal{R}^k$, $\mathbf{u} = (u, \dots, u) \in \mathcal{R}^k$. For any two points $\mathbf{x}$ and $\mathbf{y}$ in $\mathcal{A}^k$, let $M(\mathbf{u}, \mathbf{x}, \mathbf{y})$ denote the matrix whose rows are $\mathbf{x}$, $\mathbf{y}$ and $(k-2)$ $\mathbf{u}$'s.

We have

$$\mathtt{Per}\big(M(\mathbf{u}, \mathbf{x}, \mathbf{y})\big) = u^k \mathtt{Per}\big(M(\mathbf{1}, \mathbf{x}/u, \mathbf{y}/u)\big) = u^k \sum_{i=1}^{k} \frac{x_i}{u} \sum_{j \neq i} \frac{y_j}{u}. \tag{7}$$

Thus, we are able to reduce the permanent problem to the dot product problem of two following sets:

$$F := \left\{ \left(\frac{x_1}{u}, \dots, \frac{x_k}{u} \right) : (x_1, \dots, x_k) \in \mathcal{A}^k \right\},$$
$$G := \left\{ \left(\sum_{j \neq 1} \frac{y_j}{u}, \dots, \sum_{j \neq k} \frac{y_j}{u} \right) : (y_1, \dots, y_k) \in \mathcal{A}^k \right\}.$$

It is clear that $|F| = |\mathcal{A}|^k$ and $|G| = |\mathcal{A}|^k$ since $\gcd(k, q^r) = 1$. From (7) we get

$$\big|\mathtt{Per}\big(M(\mathbf{u}, \mathbf{x}, \mathbf{y})\big)\big| = |F \cdot G|,$$

then the theorem follows immediately from Theorem 14 with $m = |\mathcal{A}|$.

7. Proof of Theorem 7

The proof of Theorem 7 is based on the study of the equation $(x_1/2 - z)(x_1/2 + z) = x_2$ where $x_1 \in X_1, x_2 \in X_2$ and $z \in X_3$. Here, $X_3 \equiv \mathcal{R}^*$. This equation is equivalent to the equation $(x_1/2)^2 - x_2 = z^2$. We set

$$A_1 = \big\{(x_1/2)^2 \mid x_1 \in X_1\big\}, \qquad A_2 = \{-x_2 \mid x_2 \in X_2\},$$
$$A_3 = \big\{z^2 \mid z \in X_3\big\}, \qquad A_4 = \big\{z^2 \mid z \in X_3\big\}.$$

Note that the equation $x^2 = a^2$ has at most two solutions in $\mathcal{R}$ for any $a \in \mathcal{R}^*$. Thus, we have

$$|A_1| \geq |X_1|/2, \qquad |A_2| = |X_2|, \qquad |A_3| \geq |X_3|/2, \qquad |A_4| \geq |X_3|/2.$$

The equation $(x_1/2)^2 - x_2 = z^2$ has a solution $x_1 \in X_1, x_2 \in X_2, z \in X_3$ if and only if there exists an edge between two vertex sets

$$U := \big\{[a_3, 1, a_1] \colon (a_3, 1, a_1) \in A_3 \times \{1\} \times A_1\big\},$$

and

$$V := \big\{[a_4, 1, a_2] \colon (a_4, 1, a_2) \in A_4 \times \{1\} \times A_2\big\}$$

in the Erdős–Rényi graph $\mathcal{E}_{q,3}(\mathcal{R})$. Therefore, from Lemma 9 and Lemma 12 that

$$e(U,V) \geq \frac{|A_1||A_2||A_3||A_4|}{q^r} - q^{(2r-1)/2}\sqrt{|A_1||A_2||A_3||A_4|}.$$

Thus, if

$$|X_1||X_2| > \frac{q^{4r-1}}{(q^r - q^{r-1})^2},$$

then $e(U,V) > 0$, and the theorem follows.

Acknowledgments. The first listed author was partially supported by Swiss National Science Foundation grants 200020-162884 and 200020-144531. The authors would like to thank the referee for valuable comments and suggestions which improved the presentation of this paper considerably.

References

[1] N. Alon and J. H. Spencer, *The probabilistic method*, 2nd ed., Willey-Interscience, 2000. MR 1885388

[2] M. Bennett, D. Hart, A. Iosevich, J. Pakianathan and M. Rudnev, *Group actions and geometric combinatorics in $\mathbb{F}_q^d$*, Forum Math. **29** (2017), no. 1, 91–110. MR 3592595

[3] 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), no. 1–2 63–93.

[4] J. Cilleruelo, *Combinatorial problems in finite fields and Sidon sets*, Combinatorica **32** (2012), no. 5, 497–511.

[5] A. Eustis, *Hypergraph Independence Numbers*, Ph.D. thesis, University of California, San Diego, 2013.

[6] D. Hart and A. Iosevich, *Ubiquity of simplices in subsets of vector spaces over finite fields*, Anal. Math. **34** (2008), no. 1, 29–38.

[7] D. Hart and A. Iosevich, *Sums and products in finite fields: An integral geometric viewpoint*, Radon transforms, geometry, and wavelets, Contemp. Math., vol. 464, Amer. Math. Soc., Providence, RI, 2008, pp. 129–135.

[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), 3255–3275.

[9] A. Iosevich, M. Rudnev and Y. Zhai, *Areas of triangles and Beck's theorem in planes over finite fields*, Combinatorica **35** (2015), no. 3, 295–308.

[10] B. Nica, *Unimodular graphs and Eisenstein sums*, J. Algebraic Combin. **45** (2017), no. 2, 423–454.

[11] I. Shkredov, *On monochromatic solutions of some nonlinear equations in $\mathbb{Z}/p\mathbb{Z}$*, Math. Notes **88** (2010), no. 3–4, 603–611.

[12] J. Solymosi, *Incidences and the spectra of graphs, combinatorial number theory and additive group theory*, Advanced Courses in Mathematics—CRM Barcelona, Birkhauser-Verlag, Basel, 2009.

[13] L. A. Vinh, *On the permanents of matrices with restricted entries over finite fields*, SIAM J. Discrete Math. **26** (2012), no. 3, 997–1007. MR 3022119

[14] L. A. Vinh, *On the volume set of point sets in vector spaces over finite fields*, Proc. Amer. Math. Soc. **141** (2013), no. 9, 3067–3071.

[15] L. A. Vinh, *Spectra of product graphs and permanents of matrices over finite rings*, Pacific J. Math. **267** (2014), no. 2, 479–487.

[16] L. A. Vinh, *The solvability of norm, bilinear and quadratic equations over finite fields via spectra of graph*, Forum mathematicum, vol. 26, 2014.

[17] E. A. Yazici, *Erdős type problems in modules over cyclic rings*, J. Fourier Anal. Appl. **22** (2016), no. 2, 237–250. MR 3471300

Thang Pham, Department of Mathematics, EPF Lausanne, Switzerland

E-mail address: phamanhthang.vnu@gmail.com; v9pham@ucsd.edu

Le Anh Vinh, University of Education, Vietnam National University, Vietnam

E-mail address: vinhla@vnu.edu.vn