

# Dot-product sets and simplices over finite rings

Nguyen Van The <sup>\*</sup>      Le Anh Vinh <sup>†</sup>

## Abstract

In this paper, we study dot-product sets and  $k$ -simplices in  $\mathbb{Z}_n^d$  for odd  $n$ , where  $\mathbb{Z}_n$  is the ring of residues modulo  $n$ . We show that if  $E$  is sufficiently large then the dot-product set of  $E$  covers the whole ring. In higher dimensional cases, if  $E$  is sufficiently large then the set of simplices and the set of dot-product simplices determined by  $E$ , up to congruence, have positive densities.

## 1 Introduction

The Erdős distinct distance problem asks for the minimal number of distinct distances determined by a finite point set in  $\mathbb{R}^d$ ,  $d \geq 2$ . This problem in the Euclidean plane has been solved by Guth and Katz [8]. They show that a set of  $N$  points in  $\mathbb{R}^2$  has at least  $cN/\log N$  distinct distances.

Let  $\mathbb{F}_q$  denote a finite field with  $q$  elements, where  $q$  is an odd prime power. For  $E \subset \mathbb{F}_q^d$  ( $d \geq 2$ ), the finite analogue of the Erdős distinct distance problem is to determine the smallest possible cardinality of the set

$$\Delta(E) = \{\|x - y\| = (x_1 - y_1)^2 + \dots + (x_d - y_d)^2 : x, y \in E\} \subset \mathbb{F}_q.$$

This problem was first studied by Bourgain, Katz, and Tao [3]. They showed that if  $q$  is a prime,  $q \equiv 3 \pmod{4}$ , then for every  $\epsilon > 0$  and  $E \subset \mathbb{F}_q^2$  with  $|E| \ll q^{2-\epsilon}$ , there exists  $\delta > 0$  such that  $|\Delta(E)| \gg |E|^{\frac{1}{2}+\delta}$ . The relationship between  $\epsilon$  and  $\delta$  in their arguments, however,

---

<sup>\*</sup>University of Science, Vietnam National University - Hanoi, Email: nguyenvanthe.t61@hus.edu.vn

<sup>†</sup>Vietnam National University - Hanoi, Email: vinhla@vnu.edu.vn. Vietnam Institute of Educational Sciences. Email: vinhle@vnies.edu.vn

is difficult to determine and to go up to higher dimensional cases. Here and throughout,  $X \gg Y$  means that there exists  $C > 0$  such that  $X \geq CY$ .

Using Fourier analytic methods, Iosevich and Rudnev [13] showed that for any odd prime power  $q$  and any set  $E \subset \mathbb{F}_q^d$  of cardinality  $|E| \gg q^{d/2}$ , we have  $|\Delta(E)| \gg \min \left\{ q, q^{\frac{d-1}{2}} |E| \right\}$ . Iosevich and Rudnev reformulated the question in analogy with the Falconer distance problem: *How large does  $E \subset \mathbb{F}_q^d$ ,  $d \geq 2$ , needed to be ensure that  $\Delta(E)$  contains a positive proportion of the elements of  $\mathbb{F}_q$ ?* The above result implies that if  $|E| \gg q^{\frac{d+1}{2}}$ , then  $\Delta(E) = \mathbb{F}_q$ . This matches with Falconer's result in Euclidean setting that for a set  $E$  with Hausdorff dimension greater than  $(d+1)/2$ , the distance set of  $E$  is of positive measure. Hart, Iosevich, Koh and Rudnev [11] that the exponent  $(d+1)/2$  is sharp in odd dimensions, at least in general fields. In even dimensions, it is still conjectured that the correct exponent is  $d/2$ . Chapman et al. [4] made the first improvement by showing that if  $E \subset \mathbb{F}_q^2$  satisfies  $|E| \geq q^{4/3}$  then  $|\Delta(E)| \gg cq$ . In a recent paper [14], Murphy et al. improved the exponent  $4/3$  to  $5/4$  in the case of prime fields.

In [6], Covert, Iosevich, and Pakianathan extended the Erdős distinct distances problem to the setting of finite cyclic rings  $\mathbb{Z}_{p^l} = \mathbb{Z}/p^l\mathbb{Z}$ , where  $p$  is a fixed odd prime and  $l \geq 2$ . Precisely, they proved that if  $E \subset \mathbb{Z}_{p^l}^d$  of cardinality

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

then the distance set determined by  $E$  will cover all units in  $\mathbb{Z}_{p^l}$ . In [5], Covert extended the problem the ring of residues modulo  $n$  for an arbitrary odd  $n$ . Let  $p$  be the smallest prime divisor of  $n$  and  $\tau(n)$  be the number of divisors of  $n$ , Covert showed that if  $|E| \gg \frac{\tau(n)n^d}{p^{(d-2)/2}}$  then the distance set determined by  $E$  will cover all elements of the ring.

Let  $E \subset \mathbb{F}_q^d$ , we define the dot-product set of  $E$  as follow

$$\Pi(E) := \{x \cdot y : x, y \in E\} \subset \mathbb{F}_q,$$

where  $x \cdot y = x_1y_1 + \dots + x_dy_d$ . Similarly, we can ask a question for the dot-product set instead of the distance set: *How large does  $E$  need to ensure that the dot-product set  $\Pi(E)$  can cover the whole field or at least a positive proportion of the field?* Hart and Iosevich [10], using exponential sums, showed that for the product set to cover the whole field, one can take

$|E| > q^{(d+1)/2}$  for any  $d \geq 2$ . Covert, Iosevich, and Pakianathan [6] extended the problem to the setting of finite cyclic rings  $\mathbb{Z}_{p^t}$ . They proved that if  $E \subset \mathbb{Z}_q^d$  of cardinality

$$|E| \gg rq^{\frac{(2r-1)d}{r} + \frac{1}{2r}},$$

then the dot-product set covers all units in  $\mathbb{Z}_q$ . In [17], the second listed author also studied this result over the ring of residues modulo  $n$  for an arbitrary  $n$ . In this paper, we will further extend the problem to cover the whole ring. Note that, our result is in line with the result of Covert in [5] for the Erdős distinct distances problem.

A classical result due to Furstenberg, Katznelson and Weiss [7] states that if  $E \subset \mathbb{R}^2$  of positive upper Lebesgue density, then for any  $\delta > 0$ , the  $\delta$ -neighborhood of  $E$  contains a congruent copy of a sufficiently large dilate of every three-point configuration. In the case of  $k$ -simplex, using Fourier analytic techniques, Bourgain [2] showed that a set  $E$  of positive upper Lebesgue density always contains a sufficiently large dilate of every non-degenerate  $k$ -point configuration where  $k < d$ . Hart and Iosevich [9] were the first to study an analog of this question in finite field geometries. Let  $P_k$  and  $P'_k$  be two  $k$ -simplices in vector space  $\mathbb{F}_q^d$ . We say that  $P_k \sim P'_k$  if there exist  $\tau \in \mathbb{F}_q^d$ , and  $O \in SO_d(\mathbb{F}_q)$ , the set of  $d$ -by- $d$  orthogonal matrices over  $\mathbb{F}_q$ , such that  $P'_k = O(P_k) + \tau$ . Hart and Iosevich [9] observed that, under this equivalent relation, one may specify a simplex by the distances determined by its vertices. When  $d \geq \binom{k+1}{2}$ , they showed that if  $E \subset \mathbb{F}_q^d$  ( $d \geq \binom{k+1}{2}$ ) of cardinality  $|E| \gg Cq^{\frac{kd}{k+1} + \frac{k}{2}}$  then  $E$  contains a congruent copy of every  $k$ -simplices with the exception of simplices with zero distances. Using spectral graph theory, this lower bound on the set size was improved to  $|E| \gg q^{\frac{d-1}{2} + k}$  by the second listed author [15] for the case of  $d \geq 2k$ .

If we only want to cover a positive proportion of all possible simplices, the above bounds can be further improved. Chapman et al [4] showed that if  $|E| \gtrsim q^{\frac{d+k}{2}}$  ( $d \geq k$ ) then the set of  $k$ -simplices, up to congruence, has density greater than  $c$ . Using group action approach, Bennett et al. [1] proved that if  $E \gg q^{d - \frac{d-1}{k+1}}$  then  $E$  determines a positive proportion of all  $k$ -simplices. In [12], H. Pham, T. Pham and the second listed author gave an improvement of this result in the case when  $E$  is the Cartesian product of sets.

In line with the study of simplices in vector spaces over finite fields, the second listed author [16] also studied the distribution of simplices with respect to the dot-product. Note that, this problem can be viewed as the solvability of systems of bilinear equations over finite fields.

In this paper, we study analogue results of  $k$ -simplices and dot-product  $k$ -simplices in  $\mathbb{Z}_n^d$  for an arbitrary odd integer  $n$ . We will show that any sufficient large subset  $E \subset \mathbb{Z}_n^d$ , the set of  $k$ -simplices and the set of dot-product  $k$ -simplices determined by  $E$ , up to congruence, have positive densities.

## 2 Statements of results

### 2.1 Dot-product sets

Let  $\mathbb{Z}_n$  be the ring of residues mod  $n$  where  $n$  is a large odd integer. Denote  $\mathbb{Z}_n^\times$  be the set of units in  $\mathbb{Z}_n$ . The finite Euclidean space  $\mathbb{Z}_n^d$  consists of column vectors  $x$ , with  $i^{th}$  entry  $x_i \in \mathbb{Z}_n$ . For a subset  $E \subset \mathbb{Z}_n^d$ , we define the *dot-product set* of  $E$  as follows

$$\Pi(E) := \{x \cdot y : x, y \in E\} \subset \mathbb{Z}_n,$$

where

$$x \cdot y = x_1 y_1 + \dots + x_d y_d$$

is the usual dot product. Using Fourier analysis, Covert, Iosevich, and Pakianathan [6] showed that if the set  $E$  is large enough, its product set will cover all units in  $\mathbb{Z}_n$ .

**Theorem 2.1.** (Covert, Iosevich, Pakianathan, [6]) *Let  $E \subset \mathbb{Z}_q^d$ , where  $\ell \geq 2$  and  $q = p^\ell$  is an odd prime power. Suppose that  $|E| \gg \ell q^{\frac{(2\ell-1)d}{2\ell} + \frac{1}{2\ell}}$ . We have*

$$\Pi(E) \supset \mathbb{Z}_q^\times.$$

In [6], it was shown that Theorem 2.1 is close to optimal in the sense that there exist a value  $b = b(p)$  and a subset  $E \subset \mathbb{Z}_q^d$  with cardinality  $|E| = bq^{\left(\frac{2\ell-1}{2\ell}\right)d}$  such that  $\Pi(E) \cap \mathbb{Z}_q^\times = \emptyset$ . For such constructed set  $E$ , we have  $|\Pi(E)| \leq p^{\ell-1} = \underline{q}(q)$ .

In the general case of the ring of residues modulo  $n$  with  $n$  is a large odd integer, the second listed author obtained the following result ([17]).

**Theorem 2.2.** (Vinh, [17]) *Let  $n$  be a large odd integer. Denote  $\gamma(n)$  be the smallest prime divisor of  $n$  and  $\tau(n)$  be the number of divisors of  $n$ .*

a) Suppose that  $E \subset \mathbb{Z}_n^d$  with cardinality

$$|E| \geq \frac{\sqrt{2}\tau(n)n^d}{\gamma(n)^{(d-1)/2}}.$$

Then, we have  $\mathbb{Z}_n^\times \subset \Pi(E)$ .

b) Suppose that  $E \subset \mathbb{Z}_n^d$  with cardinality

$$|E| \geq \frac{2\sqrt{\tau(n)}n^{d+1}}{\gamma(n)^{d/2}}.$$

Then, we have  $\Pi(E) = \mathbb{Z}_n$ .

The first part of Theorem 2.2 is a generalization of Theorem 2.1. In the second part, to cover the whole ring  $\mathbb{Z}_n$ , we need a weaker condition on the sizes of  $E$ . On the other hand, the result in the second part of Theorem 2.2 is trivial when  $n \geq \gamma(n)^{d/2}$ . More precisely, in the case of finite cyclic rings  $\mathbb{Z}_{p^\ell}$ , the result is non-trivial only if  $\ell < d/2$ .

It is of interest to extend Theorem 2.1 and Theorem 2.2 to cover the whole ring  $\mathbb{Z}_n$ . Our first result is the following.

**Theorem 2.3.** *Let  $E \subset \mathbb{Z}_n^d$  where  $d > 2$  and  $n$  is a large odd integer. Suppose that*

$$|E| > \frac{\tau(n)n^d}{\gamma(n)^{(d-2)/2}}.$$

*Then, we have  $\Pi(E) = \mathbb{Z}_n$ .*

Note that, this result improves the second part of Theorem 2.2 and aligns with Covert's result [5] for Erdős distance problem. Besides, let  $E \subset \mathbb{Z}_n^d$  be the set of all elements in  $\mathbb{Z}_n^d$  with all complements are divisible by  $\gamma(n)$ , then  $|E| = n^d\gamma(n)^{-d}$  and  $\Pi(E)$  contains no non-unit element of  $\mathbb{Z}_n$ . It shows that Theorem 2.3 is asymptotically sharp as we fix  $\gamma(n)$  and  $d$  then let  $n$  goes to infinity. Moreover, this result is non-trivial for  $d \geq 3$  if  $\tau(n) = o(n^\varepsilon)$  for all  $\varepsilon > 0$ .

As a direct consequence, we has the following corollary in the case  $n = p^\ell$ .

**Corollary 2.4.** *Let  $E \subset \mathbb{Z}_q^d$ , where  $q = p^\ell$  and  $d \geq 3$ . Suppose that  $|E| > (\ell + 1)q^{\frac{(2\ell-1)d}{2\ell} + \frac{1}{\ell}}$ . Then, we have  $\Pi(E) = \mathbb{Z}_q$ .*

## 2.2 Distribution of $k$ simplices

Since a geometric justification of the notion of distance is that an orthogonal transformation preserves this distance, a  $k$ -simplex in a subset  $E \subset \mathbb{Z}_n^d$  can be defined recursively by setting

$$\mathcal{T}_{l_k} = \{(\mathbf{x}_0, \dots, \mathbf{x}_{k-1}, \mathbf{x}_k) \in \mathcal{T}_{l_{k-1}} \times E : \|\mathbf{x}_i - \mathbf{x}_k\| = t_{i,k}, i = 0, \dots, k-1\},$$

in which  $l_k = l_{k-1} \cup \{(t_{0,k}, \dots, t_{k-1,k}), t_{i,j} \in \mathbb{Z}_n\}$  and

$$\mathcal{T}_{l_1} = \{(\mathbf{x}_0, \mathbf{x}_1) \in E^2 : \|\mathbf{x}_0 - \mathbf{x}_1\| = t_{0,1}\}.$$

Denote  $\mathcal{T}_k(E) := \{l_k : |\mathcal{T}_{l_k}| > 0\}$  be the set of  $k$ -simplices determined by  $E$ . We have the following the result.

**Theorem 2.5.** *Let  $E \subset \mathbb{Z}_n^d$ . Suppose that*

$$|E| \gg \frac{\sqrt{\tau(n)} n^{d+\frac{k-1}{2}}}{\gamma(n)^{(d-1)/2}}$$

*with  $k \leq d$ , then  $E$  determines a positive proportion of all  $k$ -simplices over  $\mathbb{Z}_n^d$ . In other words,*

$$|\mathcal{T}_k(E)| \gg n^{\binom{k+1}{2}}.$$

Similarly, one can define a  $k$ -simplex with dot-product instead of distance function. A dot-product  $k$ -simplex in a subset  $E \subset \mathbb{Z}_n^d$  can be defined recursively by setting

$$\mathcal{P}_{l_k} = \{(\mathbf{x}_0, \dots, \mathbf{x}_{k-1}, \mathbf{x}_k) \in \mathcal{P}_{l_{k-1}} \times E : \mathbf{x}_i \cdot \mathbf{x}_k = t_{i,k}, i = 0, \dots, k-1\},$$

in which  $l_k = l_{k-1} \cup \{(t_{0,k}, \dots, t_{k-1,k}), t_{i,j} \in \mathbb{Z}_n\}$  and

$$\mathcal{P}_{l_1} = \{(\mathbf{x}_0, \mathbf{x}_1) \in E^2 : \mathbf{x}_0 \cdot \mathbf{x}_1 = t_{0,1}\}.$$

Denote  $\mathcal{P}_k(E) := \{l_k : |\mathcal{P}_{l_k}| > 0\}$  be the set of dot-product  $k$ -simplices determined by  $E$ . We have the following the result.

**Theorem 2.6.** *Let  $E \subset \mathbb{Z}_n^d$ . Suppose that*

$$|E| \gg \frac{\sqrt{\tau(n)} n^{d+\frac{k-1}{2}}}{\gamma(n)^{(d-1)/2}}$$

with  $k \leq d$ , Then,  $E$  determines a positive proportion of all dot-product  $k$ -simplices over  $\mathbb{Z}_n^d$ . In other words,

$$|\mathcal{P}_k(E)| \gg n^{\binom{k+1}{2}}.$$

### 3 Dot-product sets - Proof of Theorem 2.3

We first recall some basic results on Fourier Analysis in  $\mathbb{Z}_n^d$ . For  $f : \mathbb{Z}_n^d \rightarrow \mathbb{C}$ , we define the Fourier transform of  $f$  as

$$\widehat{f}(m) = n^{-d} \sum_{x \in \mathbb{Z}_n^d} f(x) \chi(-x \cdot m),$$

where  $\chi(x) = \exp(2\pi i x/n)$ . Since  $\chi$  is a character on the additive group  $\mathbb{Z}_n$ , we have the following orthogonality property.

**Lemma 3.1.** *We have*

$$n^{-d} \sum_{x \in \mathbb{Z}_n^d} \chi(x \cdot m) = \begin{cases} 1 & m = (0, \dots, 0) \\ 0 & \text{otherwise} \end{cases}$$

The Plancherel and inversion-like identities can be derived from Lemma 3.1.

**Proposition 3.2.** *Let  $f$  and  $g$  be complex-valued functions defined on  $\mathbb{Z}_n^d$ . Then,*

$$f(x) = \sum_{m \in \mathbb{Z}_n^d} \chi(x \cdot m) \widehat{f}(m) \tag{1}$$

$$n^{-d} \sum_{x \in \mathbb{Z}_n^d} f(x) \overline{g(x)} = \sum_{m \in \mathbb{Z}_n^d} \widehat{f}(m) \overline{\widehat{g}(m)} \tag{2}$$

We are now ready to give a proof of Theorem 2.3. We will follow a similar approach as in [6].

**Proof of Theorem 2.3.** Without loss of generality, we suppose that  $n$  has the prime decomposition  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , where  $2 < p_1 < p_2 < \dots < p_k$  and  $\alpha_i > 0$  for each  $i = 1, 2, \dots, k$ . For  $E \subset \mathbb{Z}_n^d$ , we define the incidence function

$$\mu(t) = \{(x, y) \in E \times E : x \cdot y = t\}.$$

In order to show that  $\Pi(E) = \mathbb{Z}_n$ , we will demonstrate that  $\mu(t) > 0$ . We rewrite

$$\begin{aligned}\mu(t) &= n^{-1} \sum_{s \in \mathbb{Z}_n} \sum_{x, y \in E} \chi(s(x \cdot y)) \chi(-st) \\ &= n^{-1} |E|^2 + \mathcal{M}(t),\end{aligned}\tag{3}$$

where

$$\mathcal{M}(t) = n^{-1} \sum_{s \neq 0} \sum_{x, y \in E} \chi(s(x \cdot y)) \chi(-st).$$

Define

$$\text{val}(s) := (\text{val}_{p_1}(s), \dots, \text{val}_{p_k}(s))$$

where  $\text{val}_{p_i}(x) = r$  if  $p_i^r | x$  but  $p_i^{r+1} \nmid x$ . For each  $s \neq 0$ , we write  $s = p_1^{\beta_1} \dots p_k^{\beta_k} \bar{s}$  where  $\bar{s} \in \mathbb{Z}_{n'}^\times$  is uniquely determined for  $n' = p_1^{\alpha_1 - \beta_1} \dots p_k^{\alpha_k - \beta_k}$  and  $\beta_i \geq 0$ . Note that,  $s \neq 0$  so  $\beta_i < \alpha_i$  for some  $i$ . We will use the notation  $\sum_\beta$  to denote the sum over all such  $(\beta_1, \dots, \beta_k)$ 's.

Using the notation as above, we can write  $\mathcal{M}(t) = \sum_\beta \mu_\beta(t)$ , where

$$\mu_\beta(t) = q^{-1} \sum_{s \in \mathbb{Z}_n \setminus \{0\} : \text{val}(s) = \beta} \sum_{x, y \in E} \chi(s(x \cdot y)) \chi(-st).$$

We will find an upper bound of  $\mu_\beta(t)$  for each  $\beta = (\beta_1, \dots, \beta_k)$ . Indeed, viewing the term  $\mu_\beta(t)$  as a sum in  $x$ -variable, applying Cauchy-Schwarz inequality, then extending the sum over  $x \in E$  to the sum over  $x \in \mathbb{Z}_n^d$ , we see that

$$\begin{aligned}|\mu_\beta(t)|^2 &\leq |E| n^{-2} \sum_{x \in \mathbb{Z}_n^d} \sum_{y, y' \in E} \sum_{s, s' \in \mathbb{Z}_{n'}^\times} \chi(p_1^{\beta_1} \dots p_k^{\beta_k} (sy - s'y')x) \chi(p_1^{\beta_1} \dots p_k^{\beta_k} t(s' - s)) \\ &\leq |E| n^{d-2} \sum_{s, s' \in \mathbb{Z}_{n'}^\times} \sum_{\substack{y, y' \in E: \\ p_1^{\beta_1} \dots p_k^{\beta_k} (sy - s'y') = 0}} \chi(p_1^{\beta_1} \dots p_k^{\beta_k} t(s' - s)) \\ &= |E| n^{d-2} \sum_{a, b \in \mathbb{Z}_{n'}^\times} \sum_{\substack{y, y' \in E: \\ p_1^{\beta_1} \dots p_k^{\beta_k} (b(ay - y')) = 0}} \chi(p_1^{\beta_1} \dots p_k^{\beta_k} t(b(1 - a))).\end{aligned}$$



Since  $b$  is a unit in  $\mathbb{Z}_{n'}$ , we have  $ay - y' = \mathbf{0}$  in  $\mathbb{Z}_{n'}^d$ . This implies that

$$\begin{aligned}
|\mu_\beta(t)|^2 &\leq |E|n^{d-2} \sum_{a,b \in \mathbb{Z}_{n'}^\times} \sum_{\substack{y,y' \in \mathbb{Z}_n^d: \\ p_1^{\beta_1} \dots p_k^{\beta_k} (b(ay-y')) = \mathbf{0}}} E(y)E(y')\chi\left(p_1^{\beta_1} \dots p_k^{\beta_k} t(b(1-a))\right) \\
&\leq |E|n^{d-2} \sum_{a,b \in \mathbb{Z}_{n'}^\times} \sum_{\substack{y,y' \in \mathbb{Z}_n^d: \\ p_1^{\beta_1} \dots p_k^{\beta_k} (b(ay-y')) = \mathbf{0}}} \left| E(y)E(y')\chi\left(p_1^{\beta_1} \dots p_k^{\beta_k} t(b(1-a))\right) \right| \\
&= |E|n^{d-2} \sum_{a,b \in \mathbb{Z}_{n'}^\times} \sum_{y \in \mathbb{Z}_n^d} |E(y)| |R(ay)|,
\end{aligned}$$

where  $R(\gamma) = \{y' \in E : y' \equiv \gamma \pmod{n'}\}$ . Since the Kernel of the canonical projection  $K$  from  $\mathbb{Z}_n^d$  to  $\mathbb{Z}_{n'}^d$  defined by

$$K : y \mapsto y \pmod{n'},$$

has size of  $(n/n')^d$ , we have

$$\begin{aligned}
|\mu_\beta(t)|^2 &\leq |E|n^{d-2} \sum_{a,b \in \mathbb{Z}_{n'}^\times} \sum_{y \in \mathbb{Z}_n^d} |E(y)| |R(ay)| \\
&= |E|n^{d-2} \sum_{a,b \in \mathbb{Z}_{n'}^\times} \sum_{y \in \mathbb{Z}_n^d} \left(\frac{n}{n'}\right)^d E(y) \\
&\leq |E|^2 \frac{n^{2d-2}}{n'^d} |\mathbb{Z}_{n'}^\times|^2 \\
&\leq |E|^2 n^{2d-2} n'^{2-d}.
\end{aligned}$$

On the other hand, we know that  $n' = p_1^{\alpha_1 - \beta_1} \dots p_k^{\alpha_k - \beta_k} \geq p_1 = \gamma(n)$  since  $p_1 < p_2 < \dots < p_k$  and  $\beta_i < \alpha_i$  for some  $i$ . Hence,

$$|\mu_\beta(t)| \leq |E|n^{d-1} p_1^{-\frac{d-2}{2}} = \frac{n^{d-1}|E|}{\gamma(n)^{(d-2)/2}}.$$

Therefore, we have

$$|\mathcal{M}(t)| \leq \sum_{\beta} |\mu_\beta(t)| \leq \frac{\tau(n)n^{d-1}|E|}{\gamma(n)^{(d-2)/2}}.$$

It follows from (3) that  $\mu(t) > 0$  whenever

$$|E| > \frac{\tau(n)n^d}{\gamma(n)^{(d-2)/2}}.$$

This completes the proof of Theorem 2.3. □

## 4 Distribution of simplices - Proof of Theorem 2.5

### 4.1 Counting number of $k$ -stars

Define the  $k$ -star set determined by a base of  $k$  points  $y^1, \dots, y^k \in E$  as follows

$$\Delta_{y^1, y^2, \dots, y^k}(E) = \{ (\|x - y^1\|, \dots, \|x - y^k\|) \in \mathbb{Z}_q^k : x \in E \}.$$

The main result of this section is to count the number of  $k$ -stars with bases in a point set  $E$ .

**Theorem 4.1.** *Let  $E \subset \mathbb{Z}_n^d$  with  $n \geq 3$  be an odd integer. Suppose that*

$$|E| \gg \frac{\sqrt{\tau(n)} n^{d + \frac{k-1}{2}}}{\gamma(n)^{(d-1)/2}}.$$

*Then, we have*

$$\frac{1}{|E|^k} \sum_{y^1, \dots, y^k \in E} |\Delta_{y^1, \dots, y^k}(E)| \gg n^k.$$

For  $t_1, \dots, t_k \in \mathbb{Z}_n$  and  $E \subset \mathbb{Z}_n^d$ , we define the counting function

$$\begin{aligned} \nu_{y^1, \dots, y^k}(t_1, \dots, t_k) &:= |\{x \in E : \|x - y^i\| = t_i, \forall i = 1, \dots, k\}| \\ &= \sum_{\|x - y^1\| = t_1, \dots, \|x - y^k\| = t_k} E(x). \end{aligned}$$

The following lemma plays an significant role in proof of Theorem 4.1.

**Lemma 4.2.** *Let  $E \subset \mathbb{Z}_n^d$  where  $n \geq 3$  is an odd integer. Then*

$$\mathcal{M}_k = \sum_{y^1, \dots, y^k \in E} \sum_{t_1, \dots, t_k \in \mathbb{Z}_n} \nu_{y^1, \dots, y^k}^2(t_1, \dots, t_k) \ll \frac{|E|^{k+2}}{n^k} + \frac{\tau(n) n^{2d-1}}{\gamma(n)^{d-1}} |E|^k.$$

*Proof.* We proceed by induction on  $k$ . For the initial case  $k = 1$ , we use the notation  $\nu_y(t)$  instead of  $\nu_{y^1}(t_1)$  for the counting function. We have

$$\nu_y(t)^2 = \sum_{\|x - y\| = \|x' - y\| = t} E(x) E(x').$$

Summing in  $y \in E$  and  $t \in \mathbb{Z}_n$ , then applying Lemma 3.1, we have

$$\begin{aligned}
\sum_{y \in E} \sum_{t \in \mathbb{Z}_n} \nu_y(t)^2 &= \sum_{\|x-y\|=\|x'-y\|} E(x)E(x')E(y) \\
&= n^{-1} \sum_{s \in \mathbb{Z}_n} \sum_{y, x, x' \in \mathbb{Z}_n^d} \chi(s(\|x-y\| - \|x'-y\|)) E(y)E(x)E(x') \\
&= n^{-1}|E|^3 + n^{-1} \sum_{s \neq 0} \sum_{y, x, x' \in \mathbb{Z}_n^d} \chi(s(\|x-y\| - \|x'-y\|)) E(y)E(x)E(x') \\
&= n^{-1}|E|^3 + \mathcal{R}.
\end{aligned}$$

Since  $\|x-y\| - \|x'-y\| = (\|x\| - 2y \cdot x) - (\|x'\| - 2y \cdot x')$ , we can rewrite  $\mathcal{R}$  as

$$\begin{aligned}
\mathcal{R} &= n^{-1} \sum_{s \neq 0} \sum_{x, x', y \in \mathbb{Z}_n^d} \chi(\|x\| - 2y \cdot x) \chi(2y \cdot x' - \|x'\|) E(x)E(x')E(y) \\
&= n^{-1} \sum_{s \neq 0} \sum_{y \in E} \left| \sum_{x \in E} \chi(s(\|x\| - 2y \cdot x)) \right|^2.
\end{aligned}$$

It follows that  $\mathcal{R} \geq 0$  and

$$\begin{aligned}
\mathcal{R} &\leq n^{-1} \sum_{s \neq 0} \sum_{y \in \mathbb{Z}_n^d} \left| \sum_{x \in E} \chi(s(\|x\| - 2y \cdot x)) \right|^2 \\
&= n^{-1} \sum_{s \neq 0} \sum_{y \in \mathbb{Z}_n^d} \sum_{x, x' \in E} \chi(s(\|x\| - \|x'\|)) \chi(-2sy \cdot (x - x')).
\end{aligned}$$

Without loss of generality, we suppose that  $n = p_1^{\alpha_1} \dots p_\ell^{\alpha_\ell}$ . Define

$$val(s) := (val_{p_1}(s), \dots, val_{p_\ell}(s))$$

where  $val_{p_i}(x) = r$  if  $p_i^r | x$  but  $p_i^{r+1} \nmid x$ . For each  $s \neq 0$ , we write  $s = p_1^{\beta_1} \dots p_\ell^{\beta_\ell} \bar{s}$  where  $\bar{s} \in \mathbb{Z}_n^\times$  is uniquely determined for  $n'_\beta = p_1^{\alpha_1 - \beta_1} \dots p_\ell^{\alpha_\ell - \beta_\ell}$  and  $\beta_i \geq 0$ . Since  $s \neq 0$ ,  $\beta_i < \alpha_i$  for some  $i$ . We will use the notation  $\sum_\beta$  to denote the sum over all such  $(\beta_1, \dots, \beta_\ell)$ 's.

Using this notation, we have  $\mathcal{R} \leq \sum_\beta \mathcal{R}_\beta$ , where

$$\mathcal{R}_\beta = n^{-1} \sum_{\substack{s \in \mathbb{Z}_n \setminus \{0\} \\ val(s) = \beta}} \sum_{y \in \mathbb{Z}_n^d} \sum_{x, x' \in E} \chi(s(\|x\| - \|x'\|)) \chi(-2sy \cdot (x - x')).$$

For each  $\beta = (\beta_1, \dots, \beta_\ell)$ , denote  $n'_\beta = p_1^{\alpha_1 - \beta_1} \dots p_\ell^{\alpha_\ell - \beta_\ell}$  and  $n_\beta = p_1^{\beta_1} \dots p_\ell^{\beta_\ell}$ . Now, we will bound  $\mathcal{R}_\beta$ . Applying the orthogonality property (Lemma 3.1), we have

$$\begin{aligned}
\mathcal{R}_\beta &= n^{-1} \sum_{\bar{s} \in \mathbb{Z}_{n'_\beta}^\times} \sum_{y \in \mathbb{Z}_n^d} \sum_{x, x' \in E} \chi \left( p_1^{\beta_1} \dots p_\ell^{\beta_\ell} \bar{s} (\|x\| - \|x'\|) \right) \chi \left( -2p_1^{\beta_1} \dots p_\ell^{\beta_\ell} \bar{s} y \cdot (x - x') \right) \\
&= n^{-1} \sum_{\bar{s} \in \mathbb{Z}_{n'_\beta}^\times} \sum_{y \in \mathbb{Z}_n^d} \sum_{\substack{x, x' \in E: \\ p_1^{\beta_1} \dots p_\ell^{\beta_\ell} (x - x') = \mathbf{0}}} \chi \left( p_1^{\beta_1} \dots p_\ell^{\beta_\ell} \bar{s} (\|x\| - \|x'\|) \right) \\
&\leq n^{d-1} \sum_{\bar{s} \in \mathbb{Z}_{n'_\beta}^\times} \left| \left\{ x, x' \in E : p_1^{\beta_1} \dots p_\ell^{\beta_\ell} (x - x') = \mathbf{0} \right\} \right| \\
&< n^{d-1} n'_\beta \sum_{x' \in E} \left| \left\{ x \in E : p_1^{\beta_1} \dots p_\ell^{\beta_\ell} (x - x') = \mathbf{0} \right\} \right|.
\end{aligned}$$

On the other hand, since the Kernel of the canonical projection  $K$  from  $\mathbb{Z}_n^d$  to  $\mathbb{Z}_{n'_\beta}^d$  defined by

$$K : y \mapsto y \bmod n'_\beta,$$

has the size of  $(n/n'_\beta)^d$ , for each  $x' \in E$ , there exist  $(n/n'_\beta)^d = n_\beta^d$  solutions to the equation  $n_\beta(x - x') = p_1^{\beta_1} \dots p_\ell^{\beta_\ell} (x - x') = 0$ . Therefore, we obtain

$$\left| \left\{ x \in E : p_1^{\beta_1} \dots p_\ell^{\beta_\ell} (x - x') = \mathbf{0} \right\} \right| \leq \left( \frac{n}{n'_\beta} \right)^d. \quad (4)$$

It follows that

$$\mathcal{R}_\beta < n^{d-1} n'_\beta \sum_{x' \in E} \left( \frac{n}{n'_\beta} \right)^d = \frac{n^{2d-1}}{n_\beta^{d-1}} |E| \leq \frac{n^{2d-1}}{\gamma(n)^{d-1}} |E|.$$

Putting all together, we have

$$\begin{aligned}
\sum_{y \in E} \sum_{t \in \mathbb{Z}_n} \nu_y(t)^2 &< n^{-1} |E|^3 + \sum_{\beta} \mathcal{R}_\beta \\
&\leq n^{-1} |E|^3 + \frac{\tau(n) n^{2d-1}}{\gamma(n)^{d-1}} |E|.
\end{aligned}$$

This completes the proof of the initial case.

Now, suppose that the statement holds for  $k - 1$

$$\sum_{y^1, \dots, y^{k-1} \in E} \sum_{t_1, \dots, t_{k-1} \in \mathbb{Z}_n} \nu_{y^1, \dots, y^{k-1}}^2(t_1, \dots, t_{k-1}) \ll \frac{|E|^{k+1}}{n^{k-1}} + \frac{\tau(n)n^{2d-1}}{\gamma(n)^{d-1}} |E|^{k-1}.$$

We will show that the statement holds for  $k$ . We have

$$\begin{aligned} \sum_{y^1, \dots, y^{k-1}, y^k \in E} \sum_{t_1, \dots, t_{k-1}, t_k \in \mathbb{Z}_n} \nu_{y^1, \dots, y^{k-1}, y^k}^2(t_1, \dots, t_{k-1}, t_k) = \\ \sum_{\|x-y^1\|=\|x'-y^1\|, \dots, \|x-y^k\|=\|x'-y^k\|} \dots \sum E(y^1) \dots E(y^k) E(x) E(x'). \end{aligned}$$

Applying the orthogonality property (Lemma 3.1), we obtain

$$\begin{aligned} \sum_{y^1, \dots, y^{k-1}, y^k \in E} \sum_{t_1, \dots, t_{k-1}, t_k \in \mathbb{Z}_n} \nu_{y^1, \dots, y^{k-1}, y^k}^2(t_1, \dots, t_{k-1}, t_k) = \\ n^{-1} \sum_{\substack{s \in \mathbb{Z}_n, \\ x, x', y^1, \dots, y^k \in E}} \sum_{\|x-y^1\|=\|x'-y^1\|, \dots, \|x-y^{k-1}\|=\|x'-y^{k-1}\|} \dots \sum \chi(s(\|x\| - 2y^k \cdot x)) \chi(-s(\|x'\| - 2y^k \cdot x')) \end{aligned}$$

since

$$\|x - y^k\| - \|x' - y^k\| = (\|x\| - 2y^k \cdot x) - (\|x'\| - 2y^k \cdot x').$$

Separating the term  $s = 0$  then applying the induction hypothesis, we have

$$\mathcal{M}_k \ll \frac{|E|^{k+2}}{n^k} + \frac{\tau(n)n^{2d-2}}{\gamma(n)^{d-1}} |E|^k + \mathcal{N},$$

where

$$\begin{aligned}
\mathcal{N} &= n^{-1} \sum_{\substack{s \neq 0, \\ x, x', y^1, \dots, y^{k-1} \in E \\ y^k \in E}} \sum_{\|x-y^1\|=\|x'-y^1\|, \dots, \|x-y^{k-1}\|=\|x'-y^{k-1}\|} \cdots \sum \chi(s(\|x\| - 2y^k \cdot x)) \chi(-s(\|x'\| - 2y^k \cdot x')) \\
&= n^{-1} \sum_{\substack{s \neq 0, \\ y^1, \dots, y^{k-1} \in E \\ y^k \in E}} \sum_{t_1, \dots, t_{k-1} \in \mathbb{Z}_n} \left| \sum_{x \in E} \sum_{\|x-y^1\|=t_1, \dots, \|x-y^{k-1}\|=t_{k-1}} \cdots \sum \chi(s(\|x\| - 2y^k \cdot x)) \right|^2 \\
&\leq n^{-1} \sum_{y^k \in \mathbb{Z}_n^d} \sum_{\substack{s \neq 0, \\ y^1, \dots, y^{k-1} \in E}} \sum_{t_1, \dots, t_{k-1} \in \mathbb{Z}_n} \left| \sum_{x \in E} \sum_{\|x-y^1\|=t_1, \dots, \|x-y^{k-1}\|=t_{k-1}} \cdots \sum \chi(s(\|x\| - 2y^k \cdot x)) \right|^2 \\
&= n^{-1} \sum_{y^k \in \mathbb{Z}_n^d} \sum_{\substack{s \neq 0, \\ y^1, \dots, y^{k-1} \in E}} \sum_{\|x-y^1\|=\|x'-y^1\|, \dots, \|x-y^{k-1}\|=\|x'-y^{k-1}\|} \cdots \sum_{x, x' \in E} \chi(s(\|x\| - 2y^k \cdot x)) \chi(-s(\|x'\| - 2y^k \cdot x')) \\
&= n^{-1} \sum_{y^k \in \mathbb{Z}_n^d} \sum_{\substack{s \neq 0, \\ y^1, \dots, y^{k-1} \in E}} \sum_{\|x-y^1\|=\|x'-y^1\|, \dots, \|x-y^{k-1}\|=\|x'-y^{k-1}\|} \cdots \sum_{x, x' \in E} \chi(s(\|x\| - \|x'\|)) \chi(-2sy^k \cdot (x - x')).
\end{aligned}$$

It follows that  $\mathcal{N} \leq \sum_{\beta} \mathcal{N}_{\beta}$ , where

$$\mathcal{N}_{\beta} = n^{-1} \sum_{y^k \in \mathbb{Z}_n^d} \sum_{\substack{s \neq 0: \text{val}(s)=\beta \\ y^1, \dots, y^{k-1} \in E}} \sum_{\|x-y^1\|=\|x'-y^1\|, \dots, \|x-y^{k-1}\|=\|x'-y^{k-1}\|} \cdots \sum_{x, x' \in E} \chi(s(\|x\| - \|x'\|)) \chi(-2sy^k \cdot (x - x')).$$

Now, we will bound  $\mathcal{N}_{\beta}$ . We proceed similarly as in the initial case. More precisely, applying the orthogonality property (Lemma 3.1), we have

$$\begin{aligned}
\mathcal{N}_{\beta} &= n^{-1} \sum_{y^k \in \mathbb{Z}_n^d} \sum_{\substack{\bar{s} \in \mathbb{Z}_{n_{\beta}}^{\times}, \\ y^1, \dots, y^{k-1} \in E}} \sum_{\|x-y^1\|=\|x'-y^1\|, \dots, \|x-y^{k-1}\|=\|x'-y^{k-1}\|} \cdots \sum_{x, x' \in E} \chi(n_{\beta}\bar{s}(\|x\| - \|x'\|)) \chi(-2n_{\beta}\bar{s}y^k \cdot (x - x')) \\
&= n^{-1} \sum_{y^k \in \mathbb{Z}_n^d} \sum_{\substack{\bar{s} \in \mathbb{Z}_{n_{\beta}}^{\times}, \\ y^1, \dots, y^{k-1} \in E}} \sum_{\|x-y^1\|=\|x'-y^1\|, \dots, \|x-y^{k-1}\|=\|x'-y^{k-1}\|} \cdots \sum_{x, x' \in E: n_{\beta}(x-x')=\mathbf{0}} \chi(n_{\beta}\bar{s}(\|x\| - \|x'\|)) \\
&= n^{d-1} \sum_{\substack{\bar{s} \in \mathbb{Z}_{n_{\beta}}^{\times}, \\ y^1, \dots, y^{k-1} \in E}} \sum_{\|x-y^1\|=\|x'-y^1\|, \dots, \|x-y^{k-1}\|=\|x'-y^{k-1}\|} \cdots \sum_{x, x' \in E: n_{\beta}(x-x')=\mathbf{0}} \chi(n_{\beta}\bar{s}(\|x\| - \|x'\|)).
\end{aligned}$$

Therefore, we obtain

$$\begin{aligned}
|\mathcal{N}_\beta| &\leq n^{d-1} \sum_{\substack{\vec{s} \in \mathbb{Z}_{n'_\beta}^\times, \\ y^1, \dots, y^{k-1} \in E}} \sum_{\substack{\|x-y^1\|=\|x'-y^1\|, \dots, \|x-y^{k-1}\|=\|x'-y^{k-1}\| \\ x, x' \in E: n_\beta(x-x')=\mathbf{0}}} \cdots \sum 1 \\
&\leq n^{d-1} n'_\beta |E|^{k-1} |\{x, x' \in E : n_\beta(x-x') = \mathbf{0}\}|.
\end{aligned}$$

On the other hand, it follows from (4) that

$$|\{x, x' \in E : n_\beta(x-x') = \mathbf{0}\}| \leq n_\beta^d |E| = \left(\frac{n}{n'_\beta}\right)^d |E|.$$

Hence, we obtain that

$$|\mathcal{N}_\beta| \leq \frac{n^{2d-1}}{n_\beta'^{d-1}} |E|^k \leq \frac{n^{2d-1}}{\gamma(n)^{d-1}} |E|^k.$$

Putting all together, we conclude that

$$\begin{aligned}
\mathcal{M}_k &\ll \frac{|E|^{k+2}}{n^k} + \frac{\tau(n)n^{2d-2}}{\gamma(n)^{d-1}} |E|^k + \mathcal{N} \\
&\ll \frac{|E|^{k+2}}{n^k} + \frac{\tau(n)n^{2d-2}}{\gamma(n)^{d-1}} |E|^k + \sum_{\beta} |\mathcal{N}_\beta| \\
&\ll \frac{|E|^{k+2}}{n^k} + \frac{\tau(n)n^{2d-2}}{\gamma(n)^{d-1}} |E|^k + \frac{\tau(n)n^{2d-1}}{\gamma(n)^{d-1}} |E|^k \\
&\ll \frac{|E|^{k+2}}{n^k} + \frac{\tau(n)n^{2d-1}}{\gamma(n)^{d-1}} |E|^k.
\end{aligned}$$

This concludes the proof of Lemma 4.2. □

We are now ready to give a proof of Theorem 4.1.

**Proof of Theorem 4.1.** By the Cauchy-Schwarz inequality, we have

$$\begin{aligned}
|E|^{2k+2} &= \left( \sum_{y^1, \dots, y^k \in E} \sum_{t_1, \dots, t_k \in \mathbb{Z}_n} \nu_{y^1, \dots, y^k}(t_1, \dots, t_k) \right)^2 \\
&\leq \sum_{y^1, \dots, y^k \in E} |\Delta_{y^1, \dots, y^k}(E)| \cdot \sum_{y^1, \dots, y^k \in E} \sum_{t_1, \dots, t_k \in \mathbb{Z}_n} \nu_{y^1, \dots, y^k}^2(t_1, \dots, t_k).
\end{aligned}$$

It follows from Lemma 4.2 that

$$|E|^{2k+2} \ll \sum_{y^1, \dots, y^k \in E} |\Delta_{y^1, \dots, y^k}(E)| \cdot \left( \frac{|E|^{k+2}}{n^k} + \frac{\tau(n)n^{2d-1}}{\gamma(n)^{d-1}} |E|^k \right).$$

Therefore, we have

$$\frac{1}{|E|^k} \sum_{y^1, \dots, y^k} |\Delta_{y^1, \dots, y^k}(E)| \gg \frac{|E|^{k+2}}{\frac{|E|^{k+2}}{n^k} + \frac{\tau(n)n^{2d-1}}{\gamma(n)^{d-1}} |E|^k} \gg n^k$$

under the assumption

$$|E| \gg \frac{\sqrt{\tau(n)} n^{d+\frac{k-1}{2}}}{\gamma(n)^{(d-1)/2}}.$$

This concludes the proof of Theorem 4.1.  $\square$

## 4.2 Distribution of $k$ -simplices

Applying Lemma 4.2, we obtain the following result.

**Lemma 4.3.** *Given  $E \subset \mathbb{Z}_n^d$ , let  $X \subset E \times E \times \dots \times E = E^u$ ,  $u \geq 2$  with  $X \sim |E|^u$ . Define*

$$X' = \{(y^1, \dots, y^{u-1}) : (y^1, \dots, y^u) \in X \text{ for some } y^u \in E\}.$$

For each  $(y^1, \dots, y^{u-1}) \in X'$ , we define

$$X(y^1, \dots, y^{u-1}) = \{y^u \in E : (y^1, \dots, y^u) \in X\}.$$

If

$$|E| \gg \frac{\sqrt{\tau(n)} n^{d+\frac{u-2}{2}}}{\gamma(n)^{(d-1)/2}}$$

then

$$\frac{1}{|X'|} \sum_{(y^1, \dots, y^{u-1}) \in X'} |\Delta_{y^1, \dots, y^{u-1}}(X(y^1, \dots, y^{u-1}))| \gg n^{u-1},$$

where

$$\Delta_{y^1, \dots, y^{u-1}}(X(y^1, \dots, y^{u-1})) = \{(\|y^u - y^1\|, \dots, \|y^u - y^{u-1}\|) \in (\mathbb{Z}_n)^{u-1} : y^u \in X(y^1, \dots, y^{u-1})\}.$$

*Proof.* For each  $(t_1, \dots, t_{u-1}) \in (\mathbb{Z}_n)^{u-1}$ , define the incidence function on  $X(y^1, \dots, y^{u-1})$



as follows

$$\nu_{y^1, \dots, y^{u-1}}^{X(y^1, \dots, y^{u-1})}(t_1, \dots, t_{u-1}) = |\{y^u \in X(y^1, \dots, y^{u-1}) : \|y^u - y^1\| = t_1, \dots, \|y^u - y^{u-1}\| = t_{u-1}\}|.$$

It is easy to see that

$$\nu_{y^1, \dots, y^{u-1}}^{X(y^1, \dots, y^{u-1})}(t_1, \dots, t_{u-1}) \leq \nu_{y^1, \dots, y^{u-1}}(t_1, \dots, t_u),$$

where

$$\nu_{y^1, \dots, y^{u-1}}(t_1, \dots, t_{u-1}) = |\{y^u \in E : \|y^u - y^1\| = t_1, \dots, \|y^u - y^{u-1}\| = t_{u-1}\}|.$$

By the Cauchy-Schwarz inequality, we have

$$\begin{aligned} |E|^2 &= \left( \sum_{(y^1, \dots, y^{u-1}) \in X'} \sum_{t_1, \dots, t_{u-1} \in \mathbb{Z}_n} \nu_{y^1, \dots, y^{u-1}}^{X(y^1, \dots, y^{u-1})}(t_1, \dots, t_{u-1}) \right)^2 \\ &\leq \left( \sum_{(y^1, \dots, y^{u-1}) \in X'} |\Delta_{y^1, \dots, y^{u-1}}(X(y^1, \dots, y^{u-1}))| \right) \left( \sum_{(y^1, \dots, y^{u-1}) \in E} \sum_{t_1, \dots, t_{u-1} \in \mathbb{Z}_n} \nu_{y^1, \dots, y^{u-1}}^2(t_1, \dots, t_u) \right). \end{aligned}$$

Using Lemma 4.2, we have

$$|E|^2 \leq \left( \sum_{(y^1, \dots, y^{u-1}) \in X'} |\Delta_{y^1, \dots, y^{u-1}}(X(y^1, \dots, y^{u-1}))| \right) \cdot \left( \frac{|E|^{u+1}}{n^{u-1}} + \frac{\tau(n)n^{2d-1}}{\gamma(n)^{d-1}} |E|^{u-1} \right).$$

On the other hand, since  $X' \sim |E|^{u-1}$ , we have

$$\frac{1}{|X'|} \sum_{(y^1, \dots, y^{u-1}) \in X'} |\Delta_{y^1, \dots, y^{u-1}}(X(y^1, \dots, y^{u-1}))| \gg \frac{|E|^{u+1}}{\frac{|E|^{u+1}}{n^{u-1}} + \frac{\tau(n)n^{2d-1}}{\gamma(n)^{d-1}} |E|^{u-1}} \gg n^{u-1}$$

under the assumption

$$|E| \gg \frac{\sqrt{\tau(n)} n^{d + \frac{u-2}{2}}}{\gamma(n)^{(d-1)/2}}.$$

This concludes the proof of Lemma 4.3. □

As a direct consequence, we have the following corollary.

**Corollary 4.4.** *Let  $E \subset \mathbb{Z}_n^d$  and  $X \subset E \times \cdots \times E = E^u$ ,  $u \geq 2$ , with  $|X| \sim |E|^u$ . If*

$$|E| \gg \frac{\sqrt{\tau(n)} n^{d+\frac{u-2}{2}}}{\gamma(n)^{(d-1)/2}},$$

*then there exists  $\mathcal{X}^{(1)} \subset X' \subset E^{u-1}$  with  $|\mathcal{X}^{(1)}| \sim |X'| \sim |E|^{u-1}$  such that for every  $(y^1, \dots, y^{u-1}) \in \mathcal{X}^{(1)}$ , we have*

$$|\Delta_{y^1, \dots, y^{u-1}}(X(y^1, \dots, y^{u-1}))| \gg n^{u-1}.$$

*Namely, the elements in  $X$  determine a positive proportion of all  $(u-1)$ -simplices which are based on a  $(u-2)$ -simplex given by any element  $(y^1, \dots, y^{u-1}) \in \mathcal{X}^{(1)}$ .*

**Proof of Theorem 2.5.** Firstly, by Theorem 4.1, there exists a subset  $\mathcal{X}^{(0)} \subset E \times \cdots \times E = E^k$  with  $|\mathcal{X}^{(0)}| \sim |E|^k$  such that for every  $(y^1, \dots, y^k) \in \mathcal{X}^{(0)}$ , we have

$$|\Delta_{y^1, \dots, y^k}(E)| = \left| \left\{ (\|y^0 - y^1\|, \dots, \|y^0 - y^k\|) \in (\mathbb{Z}_n)^k : y^0 \in E \right\} \right| \gg n^k.$$

This implies that the set  $E$  determines a positive proportion of all  $k$ -simplices which are based on a  $(k-1)$ -simplex given by any element  $(y^1, \dots, y^k) \in \mathcal{X}^{(0)}$ .

Since

$$|E| \gg \frac{\sqrt{\tau(n)} n^{d+\frac{k-1}{2}}}{\gamma(n)^{(d-1)/2}} \gg \frac{\sqrt{\tau(n)} n^{d+\frac{k-2}{2}}}{\gamma(n)^{(d-1)/2}}$$

and  $|\mathcal{X}^{(0)}| \sim |E|^k$ , by Corollary 4.4 where  $u$  is replaced by  $k$ , there exists a set  $\mathcal{X}^{(1)} \subset (\mathcal{X}^{(0)})' \subset E^{k-1}$  with  $|\mathcal{X}^{(1)}| \sim |(\mathcal{X}^{(0)})'| \sim |E|^{k-1}$  such that for every  $(y^1, \dots, y^{k-1}) \in \mathcal{X}^{(1)}$ , we have

$$|\Delta_{y^1, \dots, y^{k-1}}(\mathcal{X}^{(0)}(y^1, \dots, y^{k-1}))| \gg n^{k-1}.$$

This implies that the set  $\mathcal{X}^{(0)}$  determines a positive proportion of all  $(k-1)$ -simplices which are based on a  $(k-2)$ -simplex given by any element  $(y^1, \dots, y^{k-1}) \in \mathcal{X}^{(1)}$ .

Again, applying Corollary 4.4 where  $u$  is replaced by  $(k-1)$ , there exists a set  $\mathcal{X}^{(2)} \subset (\mathcal{X}^{(1)})' \subset E^{k-2}$  with  $|\mathcal{X}^{(2)}| \sim |(\mathcal{X}^{(1)})'| \sim |E|^{k-2}$  such that for every  $(y^1, \dots, y^{k-2}) \in \mathcal{X}^{(2)}$ , we have

$$|\Delta_{y^1, \dots, y^{k-2}}(\mathcal{X}^{(1)}(y^1, \dots, y^{k-2}))| \gg n^{k-2}.$$

This implies that the set  $\mathcal{X}^{(1)}$  determines a positive proportion of all  $(k-2)$ -simplices which

are based on a  $(k-3)$ -simplex given by any element  $(y^1, \dots, y^{k-2}) \in \mathcal{X}^{(2)}$ .

Repeating the above process, there exists a sequence of sets  $\mathcal{X}^{(0)}, \mathcal{X}^{(1)}, \dots, \mathcal{X}^{(k-2)}$  with  $|\mathcal{X}^{(s)}| = |E|^{k-s}$  for all  $s = 0, 1, \dots, k-2$  such that the set  $\mathcal{X}^{(s)}$  determines a positive proportion of all  $(k-1-s)$ -simplices which are based on a  $(k-2-s)$ -simplex given by any element  $(y^1, \dots, y^{k-1-s}) \in \mathcal{X}^{(s+1)}$ .

Finally, let  $u = 2, X = \mathcal{X}^{(k-2)}$ . Applying Lemma 4.4, we have the set  $\mathcal{X}^{(k-2)} \subset E \times E$  determines a positive proportion of all 1-simplices. This implies that the set  $\mathcal{X}^{(0)}$  determines a positive proportion of all  $(k-1)$ -simplices.

On the other hand, since the set  $E$  determines a positive proportion of all  $k$ -simplices whose bases are fixed as a  $(k-1)$ -simplex given by any element  $(y^1, \dots, y^k) \in \mathcal{X}^{(0)}$ , we conclude that the set  $E$  determines a positive proportion of all  $k$ -simplices. It means that

$$|\mathcal{T}_k(E)| \geq n^{\binom{k+1}{2}},$$

concluding the proof of Theorem 2.5. □

## 5 Dot-product simplices - Proof of Theorem

### 5.1 Counting dot-product stars

Define dot-product  $k$ -star set determined by  $k$  points  $y^1, \dots, y^k \in E$  as follows

$$\Pi_{y^1, y^2, \dots, y^k}(E) = \{(x \cdot y^1, \dots, x \cdot y^k) \in \mathbb{Z}_q^k : x \in E\}.$$

The main result of this section is to count the number of dot-product  $k$ -stars with bases in a point set  $E$ .

**Theorem 5.1.** *Let  $E \subset \mathbb{Z}_n^d$  with  $n \geq 3$  be an odd integer. Suppose that*

$$|E| \gg \frac{\sqrt{\tau(n)} n^{d + \frac{k-1}{2}}}{\gamma(n)^{(d-1)/2}}.$$

*Then, we have*

$$\frac{1}{|E|^k} \sum_{y^1, \dots, y^k \in E} |\Pi_{y^1, \dots, y^k}(E)| \gg n^k.$$

For  $t_1, \dots, t_k \in \mathbb{Z}_n$  and  $E \subset \mathbb{Z}_n^d$ , we define the counting function

$$\begin{aligned}\mu_{y^1, \dots, y^k}(t_1, \dots, t_k) &:= |\{x \in E : x \cdot y^i = t_i, \forall i = 1, \dots, k\}| \\ &= \sum_{x \in E} \prod_{i=1}^k \left( n^{-1} \sum_{s \in \mathbb{Z}_n} \chi(s(t_i - x \cdot y^i)) \right).\end{aligned}$$

The following lemma plays an significant role in the proof of Theorem 5.1.

**Lemma 5.2.** *Let  $E \subset \mathbb{Z}_n^d$  with odd integer  $n \geq 3$ . Then*

$$\mathcal{K}_k = \sum_{y^1, \dots, y^k \in E} \sum_{t_1, \dots, t_k \in \mathbb{Z}_n} \mu_{y^1, \dots, y^k}^2(t_1, \dots, t_k) \ll \frac{|E|^{k+2}}{n^k} + \frac{\tau(n)n^{2d-1}}{\gamma(n)^{d-1}} |E|^k.$$

*Proof.* We proceed by induction on  $k$ . For the initial case  $k = 1$ , we use the notation  $\mu_y(t)$  instead of  $\mu_{y^1}(t_1)$ . More precisely, define the counting function

$$\mu_y(t) := |\{x \in E : x \cdot y = t\}|.$$

Applying the orthogonality property, we have

$$\mu_y(t) = \sum_{x \in E} n^{-1} \sum_{s \in \mathbb{Z}_n} \chi(s(t - x \cdot y)) = n^{-1} \sum_{x \in \mathbb{Z}_n^d} \sum_{s \in \mathbb{Z}_n} \chi(s(t - x \cdot y)) E(x).$$

It follows that

$$\begin{aligned}\widehat{\mu_y}(s) &= n^{-1} \sum_{t \in \mathbb{Z}_n} \chi(-ts) \mu_y(t) = n^{-2} \sum_{t \in \mathbb{Z}_n} \chi(-ts) \sum_{x \in \mathbb{Z}_n^d} \sum_{s' \in \mathbb{Z}_n} \chi(s'(t - x \cdot y)) E(x) \\ &= n^{-2} \sum_{x \in \mathbb{Z}_n^d} E(x) \sum_{s' \in \mathbb{Z}_n} \chi(-s'x \cdot y) \sum_{t \in \mathbb{Z}_n} \chi(t(s' - s)) \\ &= n^{-1} \sum_{x \in \mathbb{Z}_n^d} E(x) \chi(-sx \cdot y). \quad (\text{If } s' \neq s, \text{ the sum is vanished by Lemma 3.1.})\end{aligned}$$

Therefore, we obtain  $\widehat{\mu_y}(s) = n^{d-1} \widehat{E}(sy)$ . Hence,

$$\sum_{y \in E} \sum_{s \in \mathbb{Z}_n} |\widehat{\mu_y}(s)|^2 = n^{2(d-1)} \sum_{y \in E} \sum_{s \in \mathbb{Z}_n} \left| \widehat{E}(sy) \right|^2 = q^{-2} |E|^3 + \mathcal{K}$$

where  $\mathcal{K} = n^{2(d-1)} \sum_{s \neq 0} \sum_{y \in E} \left| \widehat{E}(sy) \right|^2$ .

Without loss of generality, we suppose that  $n$  has the prime decomposition  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_\ell^{\alpha_\ell}$ ,

where  $2 < p_1 < p_2 < \dots < p_k$  and  $\alpha_i > 0$  for each  $i = 1, 2, \dots, \ell$ . Define

$$\text{val}(s) := (\text{val}_{p_1}(s), \dots, \text{val}_{p_\ell}(s))$$

where  $\text{val}_{p_i}(x) = r$  if  $p_i^r | x$  but  $p_i^{r+1} \nmid x$ . For each  $s \neq 0$ , we write  $s = p_1^{\beta_1} \dots p_\ell^{\beta_\ell} \bar{s}$  where  $\bar{s} \in \mathbb{Z}_{n'}^\times$  is uniquely determined for  $n' = p_1^{\alpha_1 - \beta_1} \dots p_\ell^{\alpha_\ell - \beta_\ell}$  and  $\beta_i \geq 0$ . Since  $s \neq 0$ ,  $\beta_i < \alpha_i$  for some  $i$ . We will use the notation  $\sum_\beta$  to denote the sum over all such  $(\beta_1, \dots, \beta_\ell)$ 's. Now, rewrite  $\mathcal{K}$  as  $\mathcal{K} = \sum_\beta \mathcal{K}_\beta$ , where

$$\mathcal{K}_\beta = n^{2(d-1)} \sum_{s \in \mathbb{Z}_n : \text{val}(s) = \beta} \sum_{y \in E} \left| \widehat{E}(sy) \right|^2.$$

For each  $\beta = (\beta_1, \dots, \beta_\ell)$ , denote  $n'_\beta = p_1^{\alpha_1 - \beta_1} \dots p_\ell^{\alpha_\ell - \beta_\ell}$  and  $n_\beta = p_1^{\beta_1} \dots p_\ell^{\beta_\ell}$ . Now, we will bound  $\mathcal{K}_\beta$ . Applying the orthogonality property (Lemma 3.1), we have

$$\begin{aligned} \mathcal{K}_\beta &= n^{2(d-1)} \sum_{\bar{s} \in \mathbb{Z}_{n'_\beta}^\times} \sum_{y \in E} \left| \widehat{E} \left( p_1^{\beta_1} \dots p_\ell^{\beta_\ell} \bar{s} y \right) \right|^2 \\ &= n^{2(d-1)} \sum_{\bar{s} \in \mathbb{Z}_{n'_\beta}^\times} \sum_{y \in \mathbb{Z}_n^d} E(y/\bar{s}) \left| \widehat{E} \left( p_1^{\beta_1} \dots p_\ell^{\beta_\ell} y \right) \right|^2. \end{aligned}$$

Set  $\rho(x) = \left| \left\{ y \in \mathbb{Z}_n^d : p_1^{\beta_1} \dots p_\ell^{\beta_\ell} y = x \right\} \right|$ . Since  $\sum_{\bar{s} \in \mathbb{Z}_{n'_\beta}^\times} E(y/\bar{s}) \leq n'_\beta$ , we obtain

$$\begin{aligned} \mathcal{K}_\beta &\leq n^{2(d-1)} n'_\beta \sum_{y \in \mathbb{Z}_n^d} \left| \widehat{E} \left( p_1^{\beta_1} \dots p_\ell^{\beta_\ell} y \right) \right|^2 \\ &\leq n'_\beta n^{2(d-1)} \sum_{x \in \mathbb{Z}_n^d} \rho(x) \left| \widehat{E}(x) \right|^2 \\ &\leq \left( \max_{x \in \mathbb{Z}_n^d} \rho(x) \right) n'_\beta n^{2(d-1)} \sum_{x \in \mathbb{Z}_n^d} \left| \widehat{E}(x) \right|^2 \\ &= \left( \max_{x \in \mathbb{Z}_n^d} \rho(x) \right) n'_\beta n^{d-2} |E|, \end{aligned}$$

where the last line follows by (2). On the other hand, similarly to the proof of (4), it is not hard to show that

$$\rho(x) = \left| \left\{ y \in \mathbb{Z}_n^d : p_1^{\beta_1} \dots p_\ell^{\beta_\ell} y = x \right\} \right| \leq \left( p_1^{\beta_1} \dots p_\ell^{\beta_\ell} \right)^d = n_\beta^d.$$

It implies that

$$\mathcal{K}_\beta \leq n_\beta^d n'_\beta n^{d-2} |E| = \frac{n^{2d-2} |E|}{n_\beta^{d-1}} \leq \frac{n^{2d-2} |E|}{\gamma(n)^{d-1}}.$$

Therefore, applying Plancherel identity (2) again, we have

$$\sum_{t \in \mathbb{Z}_n} \sum_{y \in E} \mu_y^2(t) = n \sum_{s \in \mathbb{Z}_n} \sum_{y \in E} |\widehat{\mu_y}(s)|^2 \leq n^{-1} |E|^3 + \frac{n^{2d-1} |E|}{\gamma(n)^{d-1}}.$$

This concludes the proof for the initial case  $k = 1$  of Lemma 5.2.

Now, suppose that the statement holds for  $k - 1$

$$\mathcal{K}_{k-1} = \sum_{y^1, \dots, y^{k-1} \in E} \sum_{t_1, \dots, t_{k-1} \in \mathbb{Z}_n} \mu_{y^1, \dots, y^{k-1}}^2(t_1, \dots, t_{k-1}) \ll \frac{|E|^{k+1}}{n^{k-1}} + \frac{\tau(n) n^{2d-1}}{\gamma(n)^{d-1}} |E|^{k-1}.$$

We will show that the statement holds for  $k$ . Firstly, set  $\mathbf{s} = (s_1, \dots, s_k) \in \mathbb{Z}_n^k$ , we have

$$\begin{aligned} \widehat{\mu}_{y^1, \dots, y^k}(s_1, \dots, s_k) &= n^{-k} \sum_{t_1, \dots, t_k \in \mathbb{Z}_n} \chi(-t_1 s_1 - \dots - t_k s_k) \mu_{y^1, \dots, y^k}(t_1, \dots, t_k) \\ &= n^{-k} \sum_{t_1, \dots, t_k \in \mathbb{Z}_n} \chi(-t_1 s_1 - \dots - t_k s_k) \sum_{x \in E} \prod_{i=1}^k \left( n^{-1} \sum_{s' \in \mathbb{Z}_n} \chi(s'(t_i - x \cdot y^i)) \right) \\ &= n^{-2k} \sum_{\mathbf{t}=(t_1, \dots, t_k) \in \mathbb{Z}_n^k} \chi(-\mathbf{t} \cdot \mathbf{s}) \sum_{x \in E} \sum_{\mathbf{s}'=(s'_1, \dots, s'_k) \in \mathbb{Z}_n^k} \prod_{i=1}^k \chi(s'_i t_i - s'_i x \cdot y^i) \\ &= n^{-2k} \sum_{x \in E} \sum_{\mathbf{s}'=(s'_1, \dots, s'_k) \in \mathbb{Z}_n^k} \sum_{\mathbf{t}=(t_1, \dots, t_k) \in \mathbb{Z}_n^k} \chi(\mathbf{t} \cdot (\mathbf{s}' - \mathbf{s})) \chi(-x \cdot (s'_1 y^1 + \dots + s'_k y^k)). \end{aligned}$$

Applying the orthogonality property, we have

$$\sum_{\mathbf{s}' \in \mathbb{Z}_n^k : \mathbf{s}' \neq \mathbf{s}} \sum_{\mathbf{t} \in \mathbb{Z}_n^k} \chi(\mathbf{t} \cdot (\mathbf{s}' - \mathbf{s})) = 0.$$

Therefore, we obtain

$$\begin{aligned} \widehat{\mu}_{y^1, \dots, y^k}(s_1, \dots, s_k) &= n^{-k} \sum_{x \in E} \chi(-x \cdot (s_1 y^1 + \dots + s_k y^k)) \\ &= n^{d-k} \widehat{E}(s_1 y^1 + \dots + s_k y^k). \end{aligned}$$

It follows that

$$\sum_{y^1, \dots, y^k \in E} \sum_{s_1, \dots, s_k \in \mathbb{Z}_n} \left| \widehat{\mu}_{y^1, \dots, y^k}(s_1, \dots, s_k) \right|^2 = n^{2(d-k)} \sum_{y^1, \dots, y^k \in E} \sum_{s_1, \dots, s_k \in \mathbb{Z}_n} \left| \widehat{E}(s_1 y^1 + \dots + s_k y^k) \right|^2.$$

Separating the case  $s_k \neq 0$ , we have

$$\sum_{y^1, \dots, y^k \in E} \sum_{s_1, \dots, s_k \in \mathbb{Z}_n} \left| \widehat{\mu}_{y^1, \dots, y^k}(s_1, \dots, s_k) \right|^2 = I + II,$$

where

$$\begin{aligned} I &= n^{2(d-k)} \sum_{\substack{y^1, \dots, y^{k-1} \in E \\ y^k \in E}} \sum_{s_1, \dots, s_{k-1} \in \mathbb{Z}_n} \left| \widehat{E}(s_1 y^1 + \dots + s_{k-1} y^{k-1}) \right|^2, \\ II &= n^{2(d-k)} \sum_{s_k \neq 0} \sum_{y^1, \dots, y^k \in E} \sum_{s_1, \dots, s_{k-1} \in \mathbb{Z}_n} \left| \widehat{E}(s_1 y^1 + \dots + s_k y^k) \right|^2. \end{aligned}$$

Using the above estimation, applying Plancherel identity and the induction hypothesis, we have

$$\begin{aligned} I &= n^{2(d-k)} |E| \sum_{y^1, \dots, y^{k-1} \in E} \sum_{s_1, \dots, s_{k-1} \in \mathbb{Z}_n} \left| \widehat{E}(s_1 y^1 + \dots + s_{k-1} y^{k-1}) \right|^2 \\ &= |E| \sum_{y^1, \dots, y^{k-1} \in E} \sum_{s_1, \dots, s_{k-1} \in \mathbb{Z}_n} \left| \widehat{\mu}_{y^1, \dots, y^{k-1}}(s_1, \dots, s_{k-1}) \right|^2 \\ &= n^{-k-1} |E| \mathcal{K}_{k-1} \\ &\ll \frac{|E|^{k+2}}{n^{2k}} + \frac{\tau(n) n^{2d-k-2}}{\gamma(n)^{d-1}} |E|^k. \end{aligned}$$

Now, we will bound the second term  $II$ . Note that  $II = \sum_{\beta} II_{\beta}$  where

$$II_{\beta} = n^{2(d-k)} \sum_{\substack{s_k \neq 0: \\ \text{val}(s_k) = \beta}} \sum_{y^1, \dots, y^k \in E} \sum_{s_1, \dots, s_{k-1} \in \mathbb{Z}_n} \left| \widehat{E}(s_1 y^1 + \dots + s_k y^k) \right|^2.$$

We proceed similar to the initial case. We have

$$\begin{aligned}
II_\beta &= n^{2(d-k)} \sum_{y^1, \dots, y^{k-1} \in E} \sum_{s_1, \dots, s_{k-1} \in \mathbb{Z}_n} \left( \sum_{\bar{s}_k \in \mathbb{Z}_{n'_\beta}^\times} \sum_{y^k \in \mathbb{Z}_n^d} E(y^k) \left| \widehat{E}(s_1 y^1 + \dots + s_{k-1} y^{k-1} + n_\beta \bar{s}_k y^k) \right|^2 \right) \\
&= n^{2(d-k)} \sum_{y^1, \dots, y^{k-1} \in E} \sum_{s_1, \dots, s_{k-1} \in \mathbb{Z}_n} \left( \sum_{\bar{s}_k \in \mathbb{Z}_{n'_\beta}^\times} \sum_{y^k \in \mathbb{Z}_n^d} E(y^k / \bar{s}_k) \left| \widehat{E}(s_1 y^1 + \dots + s_{k-1} y^{k-1} + n_\beta y^k) \right|^2 \right) \\
&< n'_\beta n^{2(d-k)} \sum_{y^1, \dots, y^{k-1} \in E} \sum_{s_1, \dots, s_{k-1} \in \mathbb{Z}_n} \sum_{y^k \in \mathbb{Z}_n^d} \left| \widehat{E}(s_1 y^1 + \dots + s_{k-1} y^{k-1} + n_\beta y^k) \right|^2 \\
&\leq n'_\beta n^{2(d-k)} \sum_{y^1, \dots, y^{k-1} \in E} \sum_{s_1, \dots, s_{k-1} \in \mathbb{Z}_n} \sum_{x \in \mathbb{Z}_n^d} \rho(x - s_1 y^1 - \dots - s_{k-1} y^{k-1}) \left| \widehat{E}(x) \right|^2 \\
&\leq \left( \max_{x \in \mathbb{Z}_n^d} \rho(x) \right) n'_\beta n^{2d-k-1} |E|^{k-1} \sum_{x \in \mathbb{Z}_n^d} \left| \widehat{E}(x) \right|^2.
\end{aligned}$$

Using  $\rho(x) \leq n_\beta^d$  and applying Plancherel identity, we obtain

$$II_\beta \leq n_\beta^d n'_\beta n^{2d-k-1} |E|^{k-1} (n^{-d} |E|) = \frac{n^{2d-k-1} |E|^k}{n'^{d-1}_\beta} \leq \frac{n^{2d-k-1}}{\gamma(n)^{d-1}} |E|^k.$$

Therefore, we have

$$II = \sum_{\beta} II_\beta \leq \frac{\tau(n) n^{2d-k-1}}{\gamma(n)^{d-1}} |E|^k.$$

Finally, applying Plancherel identity, we have

$$\begin{aligned}
\mathcal{K}_k &= n^k (I + II) \\
&\ll n^k \left( \frac{|E|^{k+2}}{n^{2k}} + \frac{\tau(n) n^{2d-k-2}}{\gamma(n)^{d-1}} |E|^k + \frac{\tau(n) n^{2d-k-1}}{\gamma(n)^{d-1}} |E|^k \right) \\
&\ll \frac{|E|^{k+2}}{n^k} + \frac{\tau(n) n^{2d-1}}{\gamma(n)^{d-1}} |E|^k.
\end{aligned}$$

This concludes the proof of Lemma 5.2. □

We are now ready to give a proof of Theorem 5.1.



**Proof of Theorem 5.1.** Applying the Cauchy-Schwarz inequality, we have

$$\begin{aligned} |E|^{2k+2} &= \left( \sum_{y^1, \dots, y^k \in E} \sum_{t_1, \dots, t_k \in \mathbb{Z}_n} \mu_{y^1, \dots, y^k}(t_1, \dots, t_k) \right)^2 \\ &\leq \sum_{y^1, \dots, y^k \in E} |\Pi_{y^1, \dots, y^k}(E)| \cdot \sum_{y^1, \dots, y^k \in E} \sum_{t_1, \dots, t_k \in \mathbb{Z}_n} \mu_{y^1, \dots, y^k}^2(t_1, \dots, t_k). \end{aligned}$$

It follows from Lemma 5.2 that

$$|E|^{2k+2} \ll \sum_{y^1, \dots, y^k \in E} |\Pi_{y^1, \dots, y^k}(E)| \cdot \left( \frac{|E|^{k+2}}{n^k} + \frac{\tau(n)n^{2d-1}}{\gamma(n)^{d-1}} |E|^k \right).$$

Therefore, we have

$$\frac{1}{|E|^k} \sum_{y^1, \dots, y^k} |\Pi_{y^1, \dots, y^k}(E)| \gg \frac{|E|^{k+2}}{\frac{|E|^{k+2}}{n^k} + \frac{\tau(n)n^{2d-1}}{\gamma(n)^{d-1}} |E|^k} \gg n^k$$

under the assumption

$$|E| \gg \frac{\sqrt{\tau(n)} n^{d+\frac{k-1}{2}}}{\gamma(n)^{(d-1)/2}}.$$

This concludes the proof of Theorem 5.1. □

## 5.2 Distribution of dot-product simplices

If  $k = 1$ , Theorem 2.6 follows directly from Theorem 5.1. We only need to consider the case  $k \geq 2$ . We will need the following generalization of Theorem 5.1.

**Lemma 5.3.** *Given  $E \subset \mathbb{Z}_n^d$ , let  $Y \subset E \times E \times \dots \times E = E^u$ ,  $u \geq 2$  with  $Y \sim |E|^u$ . Define*

$$Y' = \{(y^1, \dots, y^{u-1}) : (y^1, \dots, y^u) \in Y \text{ for some } y^u \in E\}.$$

*For each  $(y^1, \dots, y^{u-1}) \in Y'$ , we define*

$$Y(y^1, \dots, y^u) = \{y^u \in E : (y^1, \dots, y^u) \in Y^u\}.$$

*If*

$$|E| \gg \frac{\sqrt{\tau(n)} n^{d+\frac{u-2}{2}}}{\gamma(n)^{(d-1)/2}},$$

then we have

$$\frac{1}{|Y'|} \sum_{(y^1, \dots, y^{u-1}) \in Y'} |\Pi_{y^1, \dots, y^{u-1}}(Y(y^1, \dots, y^{u-1}))| \gg n^{u-1},$$

where

$$\Pi_{y^1, \dots, y^{u-1}}(Y(y^1, \dots, y^{u-1})) = \{(y^u \cdot y^1, \dots, y^u \cdot y^{u-1}) \in (\mathbb{Z}_n)^{u-1} : y^u \in Y(y^1, \dots, y^{u-1})\}.$$

*Proof.* For each  $(t_1, \dots, t_{u-1}) \in (\mathbb{Z}_n)^{u-1}$ , define the incidence function on  $Y(y^1, \dots, y^{u-1})$  as follows

$$\mu_{y^1, \dots, y^{u-1}}^{Y(y^1, \dots, y^{u-1})}(t_1, \dots, t_{u-1}) = |\{y^u \in Y(y^1, \dots, y^{u-1}) : y^u \cdot y^1 = t_1, \dots, y^u \cdot y^{u-1} = t_{u-1}\}|.$$

It is easy to see that

$$\mu_{y^1, \dots, y^{u-1}}^{Y(y^1, \dots, y^{u-1})}(t_1, \dots, t_{u-1}) \leq \mu_{y^1, \dots, y^{u-1}}(t_1, \dots, t_u),$$

where

$$\mu_{y^1, \dots, y^{u-1}}(t_1, \dots, t_{u-1}) = |\{y^u \in E : y^u \cdot y^1 = t_1, \dots, y^u \cdot y^{u-1} = t_{u-1}\}|.$$

By the Cauchy-Schwarz inequality, we have

$$\begin{aligned} |E|^2 &= \left( \sum_{(y^1, \dots, y^{u-1}) \in Y'} \sum_{t_1, \dots, t_{u-1} \in \mathbb{Z}_n} \mu_{y^1, \dots, y^{u-1}}^{Y(y^1, \dots, y^{u-1})}(t_1, \dots, t_{u-1}) \right)^2 \\ &\leq \left( \sum_{(y^1, \dots, y^{u-1}) \in Y'} |\Pi_{y^1, \dots, y^{u-1}}(Y(y^1, \dots, y^{u-1}))| \right) \cdot \left( \sum_{(y^1, \dots, y^{u-1}) \in E} \sum_{t_1, \dots, t_{u-1} \in \mathbb{Z}_n} \mu_{y^1, \dots, y^{u-1}}^2(t_1, \dots, t_{u-1}) \right). \end{aligned}$$

Using Lemma 5.2, we obtain

$$|E|^2 \leq \left( \sum_{(y^1, \dots, y^{u-1}) \in Y'} |\Pi_{y^1, \dots, y^{u-1}}(Y(y^1, \dots, y^{u-1}))| \right) \cdot \left( \frac{|E|^{u+1}}{n^{u-1}} + \frac{\tau(n)n^{2d-1}}{\gamma(n)^{d-1}} |E|^{u-1} \right).$$

On the other hand, since  $Y' \sim |E|^{u-1}$ , we have

$$\frac{1}{|Y'|} \sum_{(y^1, \dots, y^{u-1}) \in Y'} |\Pi_{y^1, \dots, y^{u-1}}(Y(y^1, \dots, y^{u-1}))| \gg \frac{|E|^{u+1}}{\frac{|E|^{u+1}}{n^{u-1}} + \frac{\tau(n)n^{2d-1}}{\gamma(n)^{d-1}} |E|^{u-1}} \gg n^{u-1}$$

under the assumption

$$|E| \gg \frac{\sqrt{\tau(n)}n^{d+\frac{u-2}{2}}}{\gamma(n)^{(d-1)/2}}.$$

This completes the proof of Lemma 5.3.  $\square$

As a direct consequence, we have the following corollary.

**Corollary 5.4.** *Let  $E \subset \mathbb{Z}_n^d$  and  $Y \subset E \times \cdots \times E = E^u$ ,  $u \geq 2$ , with  $|Y| \sim |E|^u$ . If*

$$|E| \gg \frac{\sqrt{\tau(n)}n^{d+\frac{u-2}{2}}}{\gamma(n)^{(d-1)/2}},$$

*then there exists  $\mathcal{Y}^{(1)} \subset Y' \subset E^{u-1}$  with  $|\mathcal{Y}^{(1)}| \sim |Y'| \sim |E|^{u-1}$  such that for every  $(y^1, \dots, y^{u-1}) \in \mathcal{Y}^{(1)}$ , we have*

$$|\Pi_{y^1, \dots, y^{u-1}}(Y(y^1, \dots, y^{u-1}))| \gg n^{u-1}.$$

*Namely, the set  $Y$  determines a positive proportion of all dot-product  $(u-1)$ -simplices which are based on a  $(u-2)$ -simplex given by any element  $(y^1, \dots, y^{u-1}) \in \mathcal{Y}^{(1)}$ .*

**Proof of Theorem 2.6.** The proof of Theorem 2.6 is similiary to the proof of Theorem 2.5, in which we use Theorem 5.1 and Corollary 5.4 instead of Theorem 4.1 and Corollary 4.4.  $\square$

## References

- [1] M. Bennett, D. Hart, A. Iosevich, J. Pakianathan, and M. Rudnev, *Group actions and geometric combinatorics in  $\mathbb{F}_q^d$* , Forum Mathematicum, **29**(1) (2017), 91 – 110.
- [2] J. Bourgain, *A Szemerédi type theorem for sets of positive density*, Israel J. Math., **54** (1986), no. 3, 307–331.
- [3] J. Bourgain, N. Katz, and T. Tao, *A sum product estimate in finite fields and Applications*, Geom. Funct. Analysis, **14** (2004), 27–57.
- [4] J. Chapman, M. Erdogan, D. Hart, A. Iosevich, and D. Koh, *Pinned distance sets,  $k$ -simplices, Woff’s exponent in finite fields and sum-product estimates*, Math. Z. **271** (2012), 63–93.

- [5] D. Covert, *Results on the Erdős-Falconer distance problem in  $\mathbb{Z}_q^d$  for odd  $q$* , Journal of Mathematical Analysis and Applications, **426** (2015), 727–733.
- [6] D. Covert, A. Iosevich, and J. Pakianathan, *Geometric configurations in the ring of integers modulo  $p^\ell$* , Indiana Univ. Math. J., **61**(5) (2012), 1949–1969.
- [7] H. Furstenberg, Y. Katznelson, and B. Weiss, *Ergodic theory and configurations in sets of positive density*, Mathematics of Ramsey theory, 184–198, Algorithms Combin., 5, Springer, Berlin (1990).
- [8] L. Guth and N. Katz, *On the Erdős distinct distances problem in the plane*, Annals of Mathematics, **181**(2014), 1–36.
- [9] D. Hart and A. Iosevich, *Ubiquity of simplices in subsets of vector spaces over finite fields*, Analysis Mathematica, **34**(2007).
- [10] D. Hart and A. Iosevich, *Sums and products in finite fields: An integral geometric viewpoint*, in: Radon Transforms, Geometry, and Wavelets, Contemp. Math. 464, American Mathematical Society, Providence (2008), 129–135.
- [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*, Transactions of the AMS, **363** (2011) 3255–3275.
- [12] D. H. Pham, T. Pham, and L. A. Vinh, *An improvement on the number of simplices in  $\mathbb{F}_q^d$* , Discrete Applied Mathematics, **221** (2017), 95–105.
- [13] A. Iosevich and M. Rudnev, *Erdős distance problem in vector spaces over finite fields*, Trans. Amer. Math. Soc., **359** (2007), 6127–6142.
- [14] B. Murphy, G. Petridis, T. Pham, M. Rudnev, and S. Stevents, *On the pinned distances problem over finite fields*, arXiv:2003.00510 [math.CO], 2020.
- [15] L. A. Vinh, *On kaleidoscopic pseudo-randomness of finite Euclidean graphs*, Discussiones Mathematicae Graph Theory, **32**(2012), 279–297.
- [16] L. A. Vinh, *The solvability of norm, bilinear and quadratic equations over finite fields via spectral of graphs*, Forum Mathematicum, **26**(1) (2014), 141–175.
- [17] L. A. Vinh, *Product graphs, sum-product graphs and sum-product estimates over finite rings*, Forum Mathematicum, 27(3) (2014), 1639–1655.