Discrete Applied Mathematics 221 (2017) 95–105

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

An improvement on the number of simplices in $\mathbb{F}_q^d$

Duc Hiep Pham [a], Thang Pham [b,*], Le Anh Vinh [a]

[a] University of Education, Vietnam National University, Viet Nam
[b] Department of Mathematics, EPF Lausanne, Switzerland

ARTICLE INFO

Article history:
Received 30 August 2016
Received in revised form 28 November 2016
Accepted 27 December 2016
Available online 19 January 2017

Keywords:
Finite fields
Simplex
Triangle
Distinct distance subset
Distances

ABSTRACT

Let $\mathcal{E}$ be a set of points in $\mathbb{F}_q^d$. Bennett et al. (2016) proved that if $|\mathcal{E}| \gg q^{d-\frac{d-1}{k+1}}$ then $\mathcal{E}$ determines a positive proportion of all k-simplices. In this paper, we give an improvement of this result in the case when $\mathcal{E}$ is the Cartesian product of sets. Namely, we show that if $\mathcal{E}$ is the Cartesian product of sets and $q^{\frac{kd}{k+1-1/d}} = o(|\mathcal{E}|)$, the number of congruence classes of k-simplices determined by $\mathcal{E}$ is at least $(1-o(1))q^{\binom{k+1}{2}}$, and in some cases our result is sharp.

1. Introduction

Let $\mathbb{F}_q$ be a finite field of order q with $q = p^r$ for some prime p and positive integer r. Denote by $O(d, \mathbb{F}_q)$ the orthogonal group in $\mathbb{F}_q^d$. 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 the same congruence class if 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 all $i = 1, 2, \ldots, k+1$.

Hart and Iosevich [7] 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 $d \geq \binom{k+1}{2}$, then $\mathcal{E}$ contains a copy of all k-simplices with non-zero edges. Here and throughout, $X \ll Y$ means that there exists $C > 0$ such that $X \leq CY$, and $X = o(Y)$ means that $X/Y \to 0$ as $q \to \infty$, where X, Y are viewed as functions in q.

Using methods from spectral graph theory, the third listed author [11] improved this result. In particular, he showed that the same result also holds when $d \geq 2k$ and $|\mathcal{E}| \gg q^{(d-1)/2+k}$. It follows from the results in [7,11] that the most difficulties arise when the size of simplex is large with respect to the dimension of the space, for instance, the result in [11] on the number of congruence classes of triangles is only non-trivial if $d \geq 4$.

In [5], Covert et al. addressed the case of triangles in $\mathbb{F}_q^2$, and they established that if $|\mathcal{E}| \gg \rho q^2$, then $\mathcal{E}$ determines at least $c\rho q^3$ congruence classes of triangles. The author of [12] extended this result to the case $d \geq 3$. Formally, he proved that if $|\mathcal{E}| \gg q^{\frac{d+2}{2}}$, then $\mathcal{E}$ determines a positive proportion of all triangles. Using Fourier analytic techniques, Chapman et al. [4] indicated that the threshold $q^{\frac{d+2}{2}}$ on the cardinality of $\mathcal{E}$ in the triangle case can be replaced by $q^{\frac{d+k}{2}}$ for the case of k-simplices. In a recent result, Bennett et al. [2] improved the threshold $q^{\frac{d+k}{2}}$ to $q^{d-\frac{d-1}{k+1}}$. The precise statement is given by the following theorem.

* Corresponding author.
E-mail addresses: phamduchiepk6@gmail.com (D.H. Pham), thang.pham@epfl.ch (T. Pham), vinhla@vnu.edu.vn (L.A. Vinh).

http://dx.doi.org/10.1016/j.dam.2016.12.023
0166-218X/

Theorem 1.1 (*Bennett et al., [2]*). *Let $\mathcal{E}$ be a subset in $\mathbb{F}_q^d$. Suppose that*

$$|\mathcal{E}| \gg q^{d-\frac{d-1}{k+1}},$$

then, for $1 \leq k \leq d$, the number of congruence classes of k-simplices determined by $\mathcal{E}$ is at least $cq^{\binom{k+1}{2}}$ for some positive constant c.

Note that one of the most important steps in their proof in [2] is to reduce the problem of counting congruence classes of k-simplices to the number of quadruples $(\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}) \in \mathcal{E}^4$ with $\|\mathbf{a} - \mathbf{b}\| = \|\mathbf{c} - \mathbf{d}\|$ by applying Lemma 2.3 and elementary results from group action theory in an ingenious way. It has been shown in [2] that the number of such quadruples in $\mathcal{E}^4$ is at most $|\mathcal{E}|^4/q + q^d|\mathcal{E}|^2$. We remark here that the error term $q^d|\mathcal{E}|^2$ plays an important role in their arguments when $\mathcal{E}$ is large enough. We refer the reader to Section 5 for a detailed explanation and a discussion on a connection between Fourier analytic techniques and methods from spectral graph theory.

In this paper, by employing spectral graph theory techniques, we are able to get a better estimate on the number of quadruples $(\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}) \in \mathcal{E}^4$ with $\|\mathbf{a} - \mathbf{b}\| = \|\mathbf{c} - \mathbf{d}\|$ in the case $\mathcal{E}$ is a Cartesian product of sets. This allows us to obtain the following improvement of Theorem 1.1.

Theorem 1.2. *Let $\mathcal{E} = \mathcal{A}_1 \times \cdots \times \mathcal{A}_d$ be a subset in $\mathbb{F}_q^d$. Suppose that*

$$(\min_{1\leq i\leq d} |\mathcal{A}_i|)^{-1}|\mathcal{E}|^{k+1} \gg q^{kd},$$

then for $1 \leq k \leq d$, the number of congruence classes of k-simplices determined by $\mathcal{E}$ is at least $cq^{\binom{k+1}{2}}$ for some positive constant c.

Corollary 1.3. *Let $\mathcal{E} = \mathcal{A}^d$ be a subset in $\mathbb{F}_q^d$. If $|\mathcal{E}| \gg q^{\frac{kd}{k+1-1/d}}$ then the number of congruence classes of k-simplices determined by $\mathcal{E}$ is at least $cq^{\binom{k+1}{2}}$ for some positive constant c.*

As a consequence of Corollary 1.3, we recover the following result in [8].

Theorem 1.4. *Let $\mathcal{A}$ be a subset in $\mathbb{F}_q$. If $|\mathcal{A}| \gg q^{\frac{d}{2d-1}}$, then the number of distinct distances determined by points in $\mathcal{A}^d \subseteq \mathbb{F}_q^d$ is at least $\gg q$.*

On the number of congruence classes of triangles in $\mathbb{F}_q^2$.

For the case of triangles in $\mathbb{F}_q^2$, in 2012 Bennett, Iosevich, and Pakianathan [3], using Elekes–Sharir paradigm and an estimate on the number of incidences between points and lines in $\mathbb{F}_q^3$, improved significantly the result in [5]. In particular, they proved that if $|\mathcal{E}| \gg q^{7/4}$ and $q \equiv 3 \bmod 4$, then the number of triangles determined by $\mathcal{E}$ is at least cq^3 for some positive constant c. The authors of [2] recently improved the exponent $7/4$ to $8/5$ in the following.

Theorem 1.5 (*Bennett et al. [2]*). *Let $\mathcal{E}$ be a set of points in $\mathbb{F}_q^2$. If $|\mathcal{E}| \gg q^{8/5}$, then $\mathcal{E}$ determines a positive proportion of all triangles.*

We will give a graph-theoretic proof for this theorem in Section 4. If $\mathcal{E}$ has Cartesian product structure of sets with different sizes, as a consequence of Theorem 1.2, we are able to obtain a much stronger result as follows.

Theorem 1.6. *Let $\mathcal{A}, \mathcal{B}$ be subsets in $\mathbb{F}_q$. If $|\mathcal{A}| \geq q^{\frac{1}{2}+\epsilon}$ and $|\mathcal{B}| \geq q^{1-\frac{2\epsilon}{3}}$ for some $\epsilon \geq 0$, then the number of congruence classes of triangles determined by $\mathcal{A} \times \mathcal{B} \subseteq \mathbb{F}_q^2$ is at least cq^3 for some positive constant c.*

Note that if $\mathcal{A}$ and $\mathcal{B}$ are arbitrary sets in $\mathbb{F}_q$, then it follows from Theorem 1.2 that in order to prove that there exist at least cq^3 congruence classes of triangles, we need the condition $|\mathcal{A}|^2|\mathcal{B}|^3 \gg q^4$. In particular, if $|\mathcal{A}| < q^{1/2}$ then we must have $|\mathcal{B}| > q$. In fact, one cannot expect to get a positive proportion of congruence of triangles in the set $\mathcal{A} \times \mathcal{B}$ with arbitrary sets $\mathcal{A}$ and $\mathcal{B}$ satisfying $|\mathcal{A}| = o(q^{1/2})$ and $|\mathcal{B}| < q$, since the authors of [2] gave a construction with $|\mathcal{A}| = q^{1/2-\epsilon'}$ and $|\mathcal{B}| = q$, and the number of congruence classes triangles determined by $\mathcal{E}$ is at most $cq^{3-\epsilon''}$ for $\epsilon'' > 0$. For the sake of completeness, we reproduce their construction here:

A construction for the triangle case.

Let $\epsilon \in (0, 1/2)$ and τ be a non-null vector. We use the orthogonal decomposition $\tau^\perp \oplus \langle\tau\rangle$ to identify $\mathbb{F}_q^2 = \mathbb{F}_q \oplus \mathbb{F}_q$. Suppose that $q = p^r$ for some prime p, so $\mathbb{F}_q$ can be viewed as a r-dimensional space over $\mathbb{F}_p$. Thus for any $y \in \mathbb{F}_q$, we can write y as $(y(1), \ldots, y(r)) \in \mathbb{F}_p^r$ where $y(i)$ are the $\mathbb{F}_p$ coordinates of $y \in \mathbb{F}_q$ with respect to a $\mathbb{F}_p$-basis.