

Research Article

Nguyen D. Phuong, Pham Thang and Le A. Vinh*

Incidences between points and generalized spheres over finite fields and related problems

DOI: 10.1515/forum-2015-0024

Received February 5, 2015; revised January 26, 2016

Abstract: Let \mathbb{F}_q be a finite field of q elements, where q is a large odd prime power and

$$Q = a_1x_1^{c_1} + \cdots + a_dx_d^{c_d} \in \mathbb{F}_q[x_1, \dots, x_d],$$

where $2 \leq c_i \leq N$, $\gcd(c_i, q) = 1$, and $a_i \in \mathbb{F}_q$ for all $1 \leq i \leq d$. A Q -sphere is a set of the form

$$\{\mathbf{x} \in \mathbb{F}_q^d \mid Q(\mathbf{x} - \mathbf{b}) = r\},$$

where $\mathbf{b} \in \mathbb{F}_q^d$, $r \in \mathbb{F}_q$. We prove bounds on the number of incidences between a point set \mathcal{P} and a Q -sphere set \mathcal{S} , denoted by $I(\mathcal{P}, \mathcal{S})$, as the following:

$$\left| I(\mathcal{P}, \mathcal{S}) - \frac{|\mathcal{P}||\mathcal{S}|}{q} \right| \leq q^{d/2} \sqrt{|\mathcal{P}||\mathcal{S}|}.$$

We also give a version of this estimate over finite cyclic rings $\mathbb{Z}/q\mathbb{Z}$, where q is an odd integer. As a consequence of the above bounds, we give an estimate for the pinned distance problem and a bound on the number of incidences between a random point set and a random Q -sphere set in \mathbb{F}_q^d . We also study the finite field analogues of some combinatorial geometry problems, namely, the number of generalized isosceles triangles, and the existence of a large subset without repeated generalized distances.

Keywords: Point-circle incidences, sum-product estimate, finite fields

MSC 2010: 52C10

Communicated by: Karl Strambach

1 Introduction

Let \mathbb{F}_q be a finite field of q elements, where q is a large odd prime power. Let P be a set of points, L a set of lines over \mathbb{F}_q^d , and $I(P, L)$ the number of incidences between P and L . Bourgain, Katz, and Tao [4] proved that for any $0 < \alpha < 2$ and $|P|, |L| \leq N = q^\alpha$, $I(P, L) \leq N^{3/2-\epsilon}$, where $\epsilon = \epsilon(\alpha)$. By employing the Erdős–Rényi graph (see Lemma 2.1 for the definition), the third author [17] improved this bound in the case $1 \leq \alpha \leq 2$, and gave the following estimate.

Theorem 1.1. *Let \mathcal{P} be a set of points, and let \mathcal{L} be a set of lines in \mathbb{F}_q^2 . Then we have*

$$I(\mathcal{P}, \mathcal{L}) \leq \frac{|\mathcal{P}||\mathcal{L}|}{q} + q^{1/2} \sqrt{|\mathcal{P}||\mathcal{L}|}.$$

Nguyen D. Phuong: University of Science, Vnu, Hanoi, Vietnam, e-mail: duyphuong@vnu.edu.vn

Pham Thang: Department of Mathematics, EPF Lausanne, Switzerland, e-mail: thang.pham@epfl.ch

***Corresponding author: Le A. Vinh:** University of Education, Vnu, Hanoi, Vietnam, e-mail: vinhla@vnu.edu.vn

The above result was also proved for points and hyperplanes, and for points and k -subspaces (see [3, 17] for more details).

Let $Q = a_1x_1^{c_1} + \dots + a_dx_d^{c_d} \in \mathbb{F}_q[x_1, \dots, x_d]$, where $2 \leq c_i \leq N$, for some constant $N > 0$, $\gcd(c_i, q) = 1$, and $a_i \in \mathbb{F}_q$ for all $1 \leq i \leq d$. We define the *generalized sphere*, or Q -*sphere*, centered at $\mathbf{b} = (b_1, \dots, b_d)$ of radius $r \in \mathbb{F}_q$ to be the set $\{\mathbf{x} \in \mathbb{F}_q^d \mid Q(\mathbf{x} - \mathbf{b}) = r\}$. The main purpose of this paper is to give a similar bound on the number of incidences between points and generalized spheres by employing the spectral graph method. With the same method, we also consider some related problems in Sections 4 and 5. Our main result is the following.

Theorem 1.2. *Let \mathcal{P} be a set of points, and let \mathcal{S} be a set of Q -spheres with arbitrary radii in \mathbb{F}_q^d . Then the number of incidences between points and spheres satisfies*

$$\left| I(\mathcal{P}, \mathcal{S}) - \frac{|\mathcal{P}||\mathcal{S}|}{q} \right| \leq q^{d/2} \sqrt{|\mathcal{P}||\mathcal{S}|}. \tag{1.1}$$

Cilleruelo, Iosevich, Lund, Roche-Newton and Rudnev [8] have independently proved equation (1.1) when $Q(x) = \sum_{i=1}^d x_i^2$. In this case, we also obtain a similar estimate over finite rings (see [16] for the Szemerédi–Trotter theorem over finite rings).

Theorem 1.3. *Let \mathcal{P} be a set of points, and let \mathcal{S} be a set of spheres with arbitrary radii in \mathbb{Z}_q^d , q is an odd integer. Then the number of incidences between points and spheres satisfies*

$$\left| I(\mathcal{P}, \mathcal{S}) - \frac{|\mathcal{P}||\mathcal{S}|}{q} \right| \leq \sqrt{2\tau(q)} \frac{q^d}{\gamma(q)^{d/2}} \sqrt{|\mathcal{P}||\mathcal{S}|},$$

where $\gamma(q)$ is the smallest prime divisor of q , and $\tau(q)$ the number of divisors of q .

Generalized pinned distances. Let $P(\mathbf{x}) \in \mathbb{F}_q[x_1, \dots, x_d]$ be a polynomial and $\mathcal{E} \subset \mathbb{F}_q^d$. Given $\mathbf{x} \in \mathbb{F}_q^d$, we denote the pinned P -distance set determined by \mathcal{E} and \mathbf{x} by $\Delta_P(\mathcal{E}, \mathbf{x}) = \{P(\mathbf{y} - \mathbf{x}) \in \mathbb{F}_q \mid \mathbf{y} \in \mathcal{E}\}$. We are interested in finding the elements $\mathbf{x} \in \mathbb{F}_q^d$ and the size of $\mathcal{E} \subset \mathbb{F}_q^d$ such that $|\Delta_P(\mathcal{E}, \mathbf{x})| \geq q$. In the case $P(\mathbf{x}) = x_1^2 + \dots + x_d^2$, Chapman, Erdoğan, Hart, Iosevich and Koh [5] proved that for any subset $\mathcal{E} \subset \mathbb{F}_q^d$ such that $|\mathcal{E}| \geq q^{(d+1)/2}$, there exists a subset $\mathcal{E}' \subset \mathcal{E}$ such that $|\mathcal{E}'| \sim |\mathcal{E}|$, and for every $\mathbf{y} \in \mathcal{E}'$ we have $|\Delta_P(\mathcal{E}, \mathbf{y})| > \frac{q}{2}$. Cilleruelo, Iosevich, Lund, Roche-Newton and Rudnev [8] reproved the same result using their bound on number of incidences between points and spheres.

In this general setting, the main difficulty in this problem is that we do not know the explicit form of the polynomial $P(\mathbf{x})$. Koh and Shen [10] found some conditions on $P(\mathbf{x})$ to obtain the desired bound. We remark that if P is a diagonal polynomial of the form $\sum_{j=1}^d a_j x_j^{c_j}$, the conditions of Koh and Shen are satisfied. However, if we consider the polynomial $Q(\mathbf{x}) = \sum_{j=1}^d a_j x_j^{c_j}$, where the exponents c_j are distinct, then we have not found any reference which shows that those conditions are satisfied.

As a consequence of Theorem 1.2, the following result can be derived in a similar way to how [8] derived their result from their bound on the number of incidences between points and spheres. It generalizes the pinned distance results of [5].

Theorem 1.4. *Let $\mathcal{E} \subset \mathbb{F}_q^d$ with $|\mathcal{E}| > \sqrt{(1 - c^2)/c^d} \cdot q^{(d+1)/2}$ for some $0 < c < 1$. Then the number of points $\mathbf{p} \in \mathcal{E}$ satisfying $|\Delta_Q(\mathcal{E}, \mathbf{p})| > (1 - c)q$ is at least $(1 - c)|\mathcal{E}|$.*

Incidences between a random point set and a random Q -sphere set. It follows from Theorem 1.2 that if \mathcal{P} is a set of points and \mathcal{S} is a set of Q -spheres such that $|\mathcal{P}||\mathcal{S}| > q^{d+2}$, then there exists at least one incidence pair $(\mathbf{p}, \mathbf{S}) \in \mathcal{P} \times \mathcal{S}$ with $\mathbf{p} \in \mathbf{S}$. We improve the bound q^{d+2} in the sense that for any $\alpha \in (0, 1)$ it suffices to take $t \geq C_\alpha q$ randomly chosen points and spheres over \mathbb{F}_q^d to guarantee that the probability of no incidences is exponentially small, namely α^t , when q is large enough. We remark that the ideas in this part are similar to the case between points and lines in [20]. More precisely, our result is the following theorem.

Theorem 1.5. *For any $\alpha > 0$, there exist an integer $q_0 = q_0(\alpha)$ and a number $C_\alpha > 0$ with the following property: When a point set \mathcal{P} and a Q -sphere set \mathcal{S} , where $|\mathcal{P}| = |\mathcal{S}| = t \geq C_\alpha q$ are chosen randomly in \mathbb{F}_q^d , the probability of $\{(\mathbf{p}, \mathbf{S}) \in \mathcal{P} \times \mathcal{S} \mid \mathbf{p} \in \mathbf{S}\} = \emptyset$ is at most α^t , provided that $q \geq q_0$.*

Generalized isosceles triangles. Given a set \mathcal{E} of n points in \mathbb{R}^2 , let $h(\mathcal{E})$ be the number of isosceles triangles determined by \mathcal{E} . Define $h(n) = \min_{|\mathcal{E}|=n} h(\mathcal{E})$. Pach and Tardos [13] proved that $h(n) = O(n^{2.136})$. In the present paper, we consider the finite field version of this problem. Let us give some notation: A Q -isosceles triangle at a vertex \mathbf{x} is a triple of distinct elements $(\mathbf{x}, \mathbf{y}, \mathbf{z}) \in \mathbb{F}_q^d \times \mathbb{F}_q^d \times \mathbb{F}_q^d$ such that $Q(\mathbf{x} - \mathbf{y}) = Q(\mathbf{x} - \mathbf{z})$. We will show that for any subset \mathcal{E} in \mathbb{F}_q^d such that its cardinality is large enough, the number of isosceles triangles determined by \mathcal{E} is $(1 + o(1))|\mathcal{E}|^3/q$. This result is a generalization of previous results in [5, 18, 21].

Theorem 1.6. *Given a set of n points \mathcal{E} in \mathbb{F}_q^d , $d \geq 2$. If $|\mathcal{E}| \gg q^{\frac{2(d+1)}{3}}$, then the number of isosceles triangles determined by \mathcal{E} is $(1 + o(1))|\mathcal{E}|^3/q$.*

Here and throughout, $X \geq Y$ means that $X \geq CY$ for some constant C and $X \gg Y$ means that $Y = o(X)$, where X, Y are viewed as functions of the parameter q .

Distinct distance subset. Given a set \mathcal{E} of n points in \mathbb{R}^2 , let $g(\mathcal{E})$ be the maximal cardinality of a subset U in \mathcal{E} such that no distance determined by U occurs twice. Define $g(n) = \min_{|\mathcal{E}|=n} g(\mathcal{E})$. Charalambides [6] proved that $n^{1/3}/(\log n) \leq g(n) \leq n^{1/2}/(\log n)^{1/4}$, where the upper bound is obtained from the Erdős distinct distance problem (see [9, 11] for more details, earlier results, and results in higher dimensions). In this paper, we study the finite field analogue of this problem.

Given a set of n points $\mathcal{E} \subset \mathbb{F}_q^d$, a subset $U \subset \mathcal{E}$ is called a *distinct Q -distance subset* if there are no four distinct points $\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{t} \in U$ such that $Q(\mathbf{x} - \mathbf{y}) = Q(\mathbf{z} - \mathbf{t})$. Using the same method that Thiele used in \mathbb{R}^2 (see [1, p. 191] for more details), we show that for any large enough set \mathcal{E} in \mathbb{F}_q^d , there exists a distinct Q -distance subset of cardinality at least $Cq^{1/3}$, for some constant C . More precisely, we have the following estimate:

Theorem 1.7. *Let \mathcal{E} be a subset in \mathbb{F}_q^d , $d \geq 2$, satisfying $|\mathcal{E}| \gg q^{2(d+1)/3}$. If $U_Q \subset \mathcal{E}$ is a maximal distinct Q -distance subset of \mathcal{E} , then $q^{1/3} \lesssim |U_Q| \lesssim q^{1/2}$.*

About the work of Cilleruelo, Iosevich, Lund, Roche-Newton and Rudnev. After we finished a draft of this paper, we learned that Cilleruelo, Iosevich, Lund, Roche-Newton and Rudnev [8] had independently obtained the same bound for the number of incidences between points and spheres in the case $Q(\mathbf{x}) = \sum_{i=1}^d x_i^2$, using the elementary method introduced in [7].

2 Spectra of graphs and digraphs

2.1 Pseudo-random graphs

Let us recall some notions about (n, d, λ) -graphs from Alon and Spencer in [2]. Given an undirected graph G , let $\lambda_1(G) \geq \lambda_2(G) \geq \dots \geq \lambda_n(G)$ be the eigenvalues of its adjacency matrix. The quantity

$$\lambda(G) = \max\{\lambda_2(G), -\lambda_n(G)\}$$

is called the second eigenvalue of G . 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 . It is well known (see [2, Chapter 9] for more details) that if λ is much smaller than the degree d , then G has certain random-like properties. For two (not necessarily disjoint) subsets of vertices $U, W \subset V$, let $e(U, W)$ be the number of ordered pairs (u, w) such that $u \in U, w \in W$, and (u, w) is an edge of G . We first recall the following well-known lemma (see, for example, [2, Corollary 9.2.5]).

Lemma 2.1. *Let $G = (V, E)$ be an (n, d, λ) -graph. For any two sets $B, C \subset V$, we have*

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

Let $PG(q, d)$ denote the projective space of dimension $d - 1$ over the finite field \mathbb{F}_q . Let $\mathcal{ER}(\mathbb{F}_q^d)$ denote the graph with vertex set $PG(q, d)$, and two vertices \mathbf{x}, \mathbf{y} are connected by an edge if $\mathbf{x} \cdot \mathbf{y} = 0$. In the case $d = 2$,

this graph is called *Erdős–Rényi graph*. The third author used the spectrum of $\mathcal{ER}(\mathbb{F}_q^d)$ and Lemma 2.1 to prove Theorem 1.1 (see [17] for more details).

In order to prove Theorem 1.3, we use the *sum-product graph* defined as the following. The vertex set of the sum-product graph $\mathcal{SP}(\mathbb{Z}_q^{d+1})$ is the set $V(\mathcal{SP}(\mathbb{Z}_q^{d+1})) = \mathbb{Z}_q \times \mathbb{Z}_q^d$. Two vertices $U = (a, \mathbf{b})$ and $V = (c, \mathbf{d}) \in V(\mathcal{SP}(\mathbb{Z}_q^{d+1}))$ are connected by an edge, $(U, V) \in E(\mathcal{SP}(\mathbb{Z}_q^{d+1}))$, if and only if $a + c = \mathbf{b} \cdot \mathbf{d}$. Our construction is similar to that of Solymosi in [14]. We have the following lemma about the spectrum of the sum-product graph $\mathcal{SP}(\mathbb{Z}_q^{d+1})$.

Lemma 2.2 ([22, Lemma 4.1]). *For any $d \geq 1$, the sum-product graph $\mathcal{SP}(\mathbb{Z}_q^{d+1})$ is a*

$$\left(q^{d+1}, q^d, \sqrt{2\tau(q)} \frac{q^d}{\gamma(q)^{d/2}} \right)\text{-graph.}$$

However, it seems difficult to use the spectrum of an undirected graph to analyze the number of incidences between points and Q -spheres, where $Q(x) \in \mathbb{F}_q[x_1, \dots, x_d]$ is an arbitrary diagonal polynomial. In the next subsection, we will introduce the Cayley graph and some notions from Vu [23] to deal with this problem.

2.2 Pseudo-random digraphs

Let G be a directed graph (digraph) on n vertices where the in-degree and out-degree of each vertex are both d . The adjacency matrix A_G is defined as follows: $a_{ij} = 1$ if there is a directed edge from i to j , and zero otherwise. Let $\lambda_1(G), \dots, \lambda_n(G)$ be the eigenvalues of A_G . These numbers are complex numbers, so we cannot order them, but we have $|\lambda_i| \leq d$ for any $1 \leq i \leq n$. Define $\lambda_1(G) = d, \lambda(G) := \max_{|\lambda_i(G)| \neq d} |\lambda_i(G)|$.

A digraph G is called an (n, d, λ) -digraph if it has n vertices, the in-degree and out-degree of each vertex is d , and $\lambda(G) \leq \lambda$.

Let G be an (n, d, λ) -digraph. For any two (not necessarily disjoint) subsets $U, W \subset V$, let $e(U, W)$ be the number of ordered pairs $(u, w) \in U \times W$ such that \overrightarrow{uw} is an edge of G . Vu [23, Lemma 3.1] developed a directed version of Lemma 2.1.

Lemma 2.3. *Let $G = (V, E)$ be an (n, d, λ) -digraph. For any two sets $B, C \subset V$, we have*

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

Let H be a finite abelian group, and let S be a subset of H . The *Cayley graph* is the digraph $C_S(H) = (H, E)$, where the vertex set is H , and there is a directed edge from vertex x to vertex y if and only if $y - x \in S$. It is clear that every vertex of $C_S(H)$ has out-degree $|S|$. We define the graph $C_Q(\mathbb{F}_q^{d+1})$ to be the Cayley graph with $H = \mathbb{F}_q \times \mathbb{F}_q^d$ and $S = \{(x_0, \mathbf{x}) \in \mathbb{F}_q \times \mathbb{F}_q^d \mid x_0 + Q(\mathbf{x}) = 0\}$, i.e.

$$E(C_Q(\mathbb{F}_q^{d+1})) = \{(x_0, \mathbf{x}), (y_0, \mathbf{y}) \in H \times H \mid x_0 - y_0 + Q(\mathbf{x} - \mathbf{y}) = 0\}.$$

We have the following result on the spectrum of $C_Q(\mathbb{F}_q^{d+1})$:

Lemma 2.4 (see [19, Lemma 3.2]). *For any odd prime power $q, d \geq 1, C_Q(\mathbb{F}_q^{d+1})$ is a $(q^{d+1}, q^d, q^{d/2})$ -digraph.*

As a corollary, we obtain the following result for the graph we use in the proof of Theorem 1.6:

Lemma 2.5. *For any odd prime power $q, d \geq 1$, let $Q'(x_1, \dots, x_{2d})$ be a polynomial in $\mathbb{F}_q[x_1, \dots, x_{2d}]$ defined by $Q' = Q(x_1, \dots, x_d) - Q(x_{d+1}, \dots, x_{2d})$. Then $C_{Q'}(\mathbb{F}_q^{2d+1})$ is a (q^{2d+1}, q^{2d}, q^d) -digraph.*

3 Proofs of Theorem 1.2 and Theorem 1.3

Proof of Theorem 1.2. We use the Cayley graph $C_Q(\mathbb{F}_q^{d+1})$ to prove Theorem 1.2. Let $\mathcal{P} = \{(x_{i1}, \dots, x_{id})\}_i$ be a set of n points in \mathbb{F}_q^d , and let $S = \{(r_i, (y_{i1}, \dots, y_{id}))\}_i$ be a set of pairs of radii and centers representing

Q -spheres in \mathcal{S} . Let $U = \{(0, x_{i1}, \dots, x_{id})\}_i \subset \mathbb{F}_q^{d+1}$ and $W = \{(r_i, y_{i1}, \dots, y_{id})\}_i \subset \mathbb{F}_q^{d+1}$. Then the number of incidences between points and Q -spheres is the number of edges between U and W in $C_Q(\mathbb{F}_q^{d+1})$. Using Lemmas 2.3 and 2.4, Theorem 1.2 follows. \square

Proof of Theorem 1.3. We use the sum-product graph $\mathcal{SP}(\mathbb{Z}_q^{d+1})$ to prove Theorem 1.3. We identify each point (b_1, \dots, b_d) in \mathcal{P} with a vertex $(-b_1^2 - \dots - b_d^2, b_1, \dots, b_d) \in \mathbb{Z}_q^{d+1}$ of $\mathcal{SP}(\mathbb{Z}_q^{d+1})$, and each sphere $(x_1 - a_1)^2 + \dots + (x_d - a_d)^2 = r$ in \mathcal{S} with a vertex $(r - a_1^2 - \dots - a_d^2, -2a_1, \dots, -2a_d) \in \mathbb{Z}_q^{d+1}$ of $\mathcal{SP}(\mathbb{Z}_q^{d+1})$. Let $U \subset \mathbb{Z}_q^{d+1}$ be the set of points corresponding to \mathcal{P} , and $W \subset \mathbb{Z}_q^{d+1}$ the set of points corresponding to \mathcal{S} . Then the number of incidences between points and spheres is the number of edges between U and W in the sum-product graph $\mathcal{SP}(\mathbb{Z}_q^{d+1})$. By Lemma 2.1 and Lemma 2.2, Theorem 1.3 follows. \square

Remark. The authors have not found any reference for a version of Weil’s theorem over finite rings \mathbb{Z}_m^d , which is the crucial component of the proof of Lemma 2.4. Therefore, it seems hard to prove Theorem 1.2 for a more general polynomial $Q(x)$ over finite rings using directed graphs. We note that Lemmas 2.4 and 2.5 also hold for the general case $Q(x_1, \dots, x_d) = \sum_{i=1}^d f_i(x_i)$, where $\deg(f_i) \geq 2$, $\gcd(\deg(f_i), q) = 1$ for all i . Therefore, all of the results in this paper over finite fields also hold for this case.

4 Generalized pinned distance problem

In this section, we give a proof of Theorem 1.4. Our proof is similar to the proof of [8, Corollary 1, Corollary 2]. First we prove that

$$\frac{1}{|\mathcal{E}|} \sum_{\mathbf{p} \in \mathcal{E}} |\Delta_Q(\mathcal{E}, \mathbf{p})| > (1 - c^2)q.$$

We identify each point $\mathbf{p} = (b_1, \dots, b_d) \in \mathcal{E}$ with a point $(0, b_1, \dots, b_d) \in \mathbb{F}_q^{d+1}$, and each pair

$$(\mathbf{p} = (b_1, \dots, b_d), t),$$

where $t \in \Delta_Q(\mathcal{E}, \mathbf{p})$ with a point $(t, b_1, \dots, b_d) \in \mathbb{F}_q^{d+1}$. Let $U \subset \mathbb{F}_q^{d+1}$ be the set of points corresponding to \mathcal{E} , and let $W \subset \mathbb{F}_q^{d+1}$ be the set of points corresponding to point-distance pairs. Then we have $|U| = |\mathcal{E}|$, and $|W| = \sum_{\mathbf{p} \in \mathcal{E}} |\Delta_Q(\mathcal{E}, \mathbf{p})|$. Moreover, one can easily see that U, W are vertex subsets of the Cayley digraph $C_Q(\mathbb{F}_q^{d+1})$. The number of edges between U and W is $|\mathcal{E}|^2$, since each point in \mathcal{E} contributes $|\mathcal{E}|$ edges between U and W . It follows from Lemmas 2.3 and 2.4 that

$$\begin{aligned} |\mathcal{E}|^2 \leq e(U, W) &\leq \frac{|U||W|}{q} + q^{d/2} \sqrt{|U||W|} \\ &= \frac{|\mathcal{E}| \sum_{\mathbf{p} \in \mathcal{E}} |\Delta_Q(\mathcal{E}, \mathbf{p})|}{q} + q^{d/2} \sqrt{|\mathcal{E}| \sum_{\mathbf{p} \in \mathcal{E}} |\Delta_Q(\mathcal{E}, \mathbf{p})|}. \end{aligned} \tag{4.1}$$

If $\frac{1}{|\mathcal{E}|} \sum_{\mathbf{p} \in \mathcal{E}} |\Delta_Q(\mathcal{E}, \mathbf{p})| \leq (1 - c^2)q$, it follows from (4.1) that

$$\begin{aligned} |\mathcal{E}|^2 &\leq |\mathcal{E}|^2(1 - c^2) + q^{(d+1)/2} |\mathcal{E}| \sqrt{(1 - c^2)}, \\ |\mathcal{E}| &\leq \sqrt{\frac{(1 - c^2)}{c^4}} q^{(d+1)/2}. \end{aligned}$$

This would be a contradiction. Therefore,

$$\sum_{\mathbf{p} \in \mathcal{E}} |\Delta_Q(\mathcal{E}, \mathbf{p})| > (1 - c^2)q|\mathcal{E}|. \tag{4.2}$$

Let us define $\mathcal{E}' := \{\mathbf{p} \in \mathcal{E} : |\Delta_Q(\mathcal{E}, \mathbf{p})| > (1 - c)q\}$. Suppose that $|\mathcal{E}'| < (1 - c)|\mathcal{E}|$, hence

$$\sum_{\mathbf{p} \in \mathcal{E} \setminus \mathcal{E}'} |\Delta_Q(\mathcal{E}, \mathbf{p})| \leq (|\mathcal{E}| - |\mathcal{E}'|)(1 - c)q, \tag{4.3}$$

and

$$\sum_{\mathbf{p} \in \mathcal{E}'} |\Delta_Q(\mathcal{E}, \mathbf{p})| \leq q|\mathcal{E}'|. \tag{4.4}$$

Putting inequalities (4.3) and (4.4) together, we obtain

$$\sum_{\mathbf{p} \in \mathcal{E}} |\Delta_Q(\mathcal{E}, \mathbf{p})| \leq (1 - c)q|\mathcal{E}| + cq|\mathcal{E}'| < (1 - c)q|\mathcal{E}| + cq(1 - c)|\mathcal{E}| = (1 - c^2)q|\mathcal{E}|.$$

The theorem follows because this contradicts inequality (4.2).

5 Related problems

5.1 Incidences between random points and Q -spheres

To prove Theorem 1.5, we need the following lemma (see [12, Lemma 8], and [20, Lemma 2.3] for more details).

Lemma 5.1. *Let $\{G_n = G(U_n, V_n)\}_{n=1}^\infty$ be a sequence of bipartite graphs with $|V_n| = |U_n| \rightarrow \infty$ as $n \rightarrow \infty$, and let $\bar{d}(G_n)$ be the average degree of G_n . Assume that for any $\epsilon > 0$, there exists an integer $\nu(\epsilon)$ and a number $c(\epsilon) > 0$ such that*

$$e(A, B) \geq c(\epsilon)|A||B| \frac{\bar{d}(G_n)}{|V_n|}$$

for all $|V_n| = |U_n| \geq \nu(\epsilon)$ and all $A \subset V_n, B \subset U_n$ satisfying $|A||B| \geq \epsilon|V_n|^2$. Then for any $\alpha > 0$, there exists an integer $\nu(\alpha)$ and a number $C(\alpha)$ with the following property: if one chooses a random subset S of V_n of cardinality t and a random subset T of U_n of the same cardinality t , then the probability of $G(S, T)$ being empty is at most α^t provided that $t \geq C(\alpha)|V_n|/\bar{d}(G_n)$ and $|V_n| \geq \nu(\alpha)$.

We notice that the Lemma 5.1 also holds when $\{G_n\}_n$ is a sequence of digraphs.

Proof of Theorem 1.5. Let $B_{q,d}$ be a bipartite digraph with vertex set $V(C_Q(\mathbb{F}_q^{d+1})) \times V(C_Q(\mathbb{F}_q^{d+1}))$, where $C_Q(\mathbb{F}_q^{d+1})$ is the Cayley graph defined as in Lemma 2.4 and the edge set

$$\{((x_0, \mathbf{x}), (y_0, \mathbf{y})) \in \mathbb{F}_q^{d+1} \times \mathbb{F}_q^{d+1} \mid (x_0 - y_0) + Q(\mathbf{x} - \mathbf{y}) = 0\}.$$

With the same identification of the point set and the Q -sphere set as in proof of Theorem 1.2, we obtain two corresponding sets U and W , where $|U| = |\mathcal{P}|, |W| = |\mathcal{S}|$. Thus, the number of incidences between points and spheres is the number of edges between U and W . By Lemmas 2.3 and 2.4, we obtain

$$\left| e(U, W) - \frac{|U||W|}{q} \right| \leq q^{d/2} \sqrt{|U||W|}. \tag{5.1}$$

For any $\epsilon > 0$ such that $|U||W| \geq \epsilon q^{2d+2}$ and $q^d \geq \frac{4}{\epsilon}$, we have from inequality (5.1) that

$$e(U, W) > \frac{q^d}{2q^{d+1}} |U||W| = \frac{\bar{d}(B_{q,d})}{|V(B_{q,d})|} |U||W|.$$

Let $c(\epsilon) = 1, \nu(\epsilon) \geq (\frac{4}{\epsilon})^{(d+1)/d}$. Then the theorem follows from Lemma 5.1. □

5.2 Generalized isosceles triangles

We give a proof of Theorem 1.6. Let

$$U = \{(1, \mathbf{x}, \mathbf{x}) \in \{1\} \times \mathcal{E} \times \mathcal{E}\}, \quad W = \{(1, \mathbf{y}, \mathbf{z}) \in \{1\} \times \mathcal{E} \times \mathcal{E}\}.$$

One can easily see that $|U| = |\mathcal{E}|$, $|W| = |\mathcal{E}|^2$. Let

$$T_1 = \{(1, \mathbf{x}, \mathbf{x}, 1, \mathbf{y}, \mathbf{z}) \in \{1\} \times \mathcal{E} \times \mathcal{E} \times \{1\} \times \mathcal{E} \times \mathcal{E} \mid Q(\mathbf{x} - \mathbf{y}) = Q(\mathbf{x} - \mathbf{z})\}.$$

Then the cardinality of T_1 is the number of edges between the sets U and W in the graph $C_{Q'}(\mathbb{F}_q^{2d+1})$ (defined as in Lemma 2.5). It follows from Lemmas 2.3 and 2.5 that

$$\left| |T_1| - \frac{|U||W|}{q} \right| \leq q^d \sqrt{|U||W|}.$$

Thus, if $|\mathcal{E}| \gg q^{2(d+1)/3}$, then we have $|T_1| = (1 + o(1))|\mathcal{E}|^3/q$. We notice that T_1 also contains the tuples $(1, \mathbf{x}, \mathbf{x}, 1, \mathbf{x}, \mathbf{y})$ with $Q(\mathbf{x} - \mathbf{y}) = 0$ which correspond to the edges between the vertices $(1, \mathbf{x}, \mathbf{x}) \in U$ and $(1, \mathbf{x}, \mathbf{y}) \in W$. Let us denote the set of such tuples by T_{err} , then one can easily see that $\frac{1}{2}|T_{\text{err}}|$ is the number of pairs $(\mathbf{x}, \mathbf{y}) \in \mathcal{E} \times \mathcal{E}$ such that $Q(\mathbf{x} - \mathbf{y}) = 0$, since each pair (\mathbf{x}, \mathbf{y}) with $Q(\mathbf{x} - \mathbf{y}) = 0$ contributes two edges $((1, \mathbf{x}, \mathbf{x}), (1, \mathbf{x}, \mathbf{y}))$ and $((1, \mathbf{x}, \mathbf{x}), (1, \mathbf{y}, \mathbf{x}))$. It follows from Lemmas 2.3 and 2.4 that

$$\left| |T_{\text{err}}| - \frac{|\mathcal{E}|^2}{q} \right| \leq q^{d/2} \sqrt{|\mathcal{E}|^2}.$$

Thus, if $|\mathcal{E}| \gg q^{2(d+1)/3}$, $d \geq 2$, then $|T_{\text{err}}| = |\mathcal{E}|^2/q = o(1)|\mathcal{E}|^3/q$. Therefore, the number of Q -isosceles triangles determined by \mathcal{E} is $(1 + o(1))|\mathcal{E}|^3/q$.

5.3 Distinct distance subset

In order to prove Theorem 1.7, we need the following theorem on the cardinality of a maximal independent set of a hypergraph due to Spencer [15].

Theorem 5.2. *Let H be a k -uniform hypergraph with n vertices and $m \geq n/k$ edges, and let $\alpha(H)$ denote the independence number of H . Then*

$$\alpha(H) \geq \left(1 - \frac{1}{k}\right) \left[\left(\frac{1}{k} \frac{n^k}{m}\right)^{\frac{1}{k-1}} \right].$$

Proof of Theorem 1.7. Let

$$T_2 = \{(1, \mathbf{p}_1, \mathbf{q}_1, 1, \mathbf{p}_2, \mathbf{q}_2) \in \{1\} \times \mathcal{E} \times \mathcal{E} \times \{1\} \times \mathcal{E} \times \mathcal{E} \mid Q(\mathbf{p}_1 - \mathbf{q}_1) = Q(\mathbf{p}_2 - \mathbf{q}_2)\}.$$

With the same arguments in the proof of Theorem 1.6, we obtain $|T_2| \leq \frac{|\mathcal{E}|^4}{q} + q^d |\mathcal{E}|^2$. Thus, if $|\mathcal{E}| \gg q^{(d+1)/2}$, then

$$|T_2| = (1 + o(1)) \frac{|\mathcal{E}|^4}{q}.$$

A 4-tuple of distinct elements in \mathcal{E}^4 is called *regular* if all six generalized distances determined are distinct. Otherwise, it is called *singular*. Let H be the 4-uniform hypergraph on the vertex set $V(H) = \mathcal{E}$, whose edges are the singular 4-tuples of \mathcal{E} .

It follows from Theorem 1.6 that the number of 4-tuples containing a triple induced an isosceles triangle is at most $((1 + o(1))|\mathcal{E}|^3/q) \cdot |\mathcal{E}| = (1 + o(1))|\mathcal{E}|^4/q$ when $|\mathcal{E}| \gg q^{2(d+1)/3}$. Thus the number of edges of H containing a triple induced an isosceles triangle is at most $(1 + o(1))|\mathcal{E}|^4/q$. On the other hand, since $T_2 = (1 + o(1))|\mathcal{E}|^4/q$ when $|\mathcal{E}| \gg q^{(d+1)/2}$, the number of 4-tuples $(\mathbf{p}_1, \mathbf{q}_1, \mathbf{p}_2, \mathbf{q}_2)$ in \mathcal{E}^4 satisfying

$$Q(\mathbf{p}_1 - \mathbf{q}_1) = Q(\mathbf{p}_2 - \mathbf{q}_2)$$

equals $(1 + o(1))|\mathcal{E}|^4/q$ when $|\mathcal{E}| \gg q^{(d+1)/2}$. Thus, if $|\mathcal{E}| \gg q^{2(d+1)/3}$ with $d \geq 2$, then

$$|E(H)| \leq \frac{2|\mathcal{E}|^4}{q}.$$

It follows from Theorem 5.2 that

$$\alpha(H) \geq C \left[\frac{|\mathcal{E}|^4}{|E(H)|} \right]^{1/3} = Cq^{1/3}.$$

Since there is no repeated generalized distance determined by the independent set of H , we have

$$|U_Q| \geq \alpha(H) \geq Cq^{1/3}.$$

Moreover, it is easy to see that there is at least one repeated generalized distance determined by any set of $\sqrt{2}q^{1/2} + 1$ elements since there are only $q = |\mathbb{F}_q|$ distances over \mathbb{F}_q^d . Thus, the theorem follows. \square

Acknowledgment: The authors would like to thank János Pach and Frank de Zeeuw for many useful discussions and helpful comments. The authors are grateful to the referee for useful comments and suggestions.

Funding: The first and third author were supported by Vietnam National Foundation for Science and Technology grant 101.99-2013.21. The work of the second author was partially supported by Swiss National Science Foundation grants 200020-144531 and 200021-137574.

References

- [1] P. K. Agarwal and J. Pach, *Combinatorial Geometry*, John Wiley, New York, 1995.
- [2] N. Alon and J. H. Spencer, *The Probabilistic Method*, 2nd ed., Wiley-Interscience, Hoboken, 2000.
- [3] M. Bennett, A. Iosevich and J. Pakianathan, Three-point configurations determined by subsets of \mathbb{F}_q^2 via the Elekes–Sharir paradigm, *Combinatorica* **34** (2014), no. 6, 689–706.
- [4] J. Bourgain, N. Katz and T. Tao, A sum-product estimate in finite fields, and applications, *Geom. Funct. Anal.* **14** (2004), 27–57.
- [5] J. Chapman, M. Erdoğ an, 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.
- [6] M. Charalambides, A note on distinct distance subsets, *J. Geom.* **104** (2013), 439–442.
- [7] J. Cilleruelo, Combinatorial problems in finite fields and Sidon sets, *Combinatorica* **32** (2012), no. 5, 497–511.
- [8] J. Cilleruelo, A. Iosevich, B. Lund, O. Roche-Newton and M. Rudnev, Elementary methods for incidence problems in finite fields, preprint (2014), <http://arxiv.org/abs/1407.2397>.
- [9] D. Conlon, J. Fox, W. Gasarch, D. G. Harris, D. Ulrich and S. Zbarsky, Distinct volume subsets, *SIAM J. Discrete Math.* **29** (2015), no. 1, 472–480.
- [10] D. Koh and C.-Y. Shen, The generalized Erdős–Falconer distance problems in vector spaces over finite fields, *J. Number Theory* **132** (2012), no. 11, 2455–2473.
- [11] H. Lefmann and T. Thiele, Point sets with distinct distances, *Combinatorica* **15** (1995), 379–408.
- [12] H. H. Nguyen, On two-point configurations in a random set, *Integers* **9** (2009), 41–45.
- [13] J. Pach and G. Tardos, Isosceles triangles determined by a planar point set, *Graphs Combin.* **18** (2002), 769–779.
- [14] J. Solymosi, Incidences and the spectra of graphs, in: *Building Bridges Between Mathematics and Computer Science*, Bolyai Soc. Math. Stud. 19, Springer, Berlin (2008), 499–513.
- [15] J. Spencer, Turán’s theorem for k -graphs, *Discrete Math.* **2** (1972), 183–186.
- [16] P. V. Thang and L. A. Vinh, Erdős–Rényi graph, Szemerédi–Trotter type theorem, and sum-product estimates over finite rings, *Forum Math.* **27** (2015), no. 1, 331–342.
- [17] L. A. Vinh, A Szemerédi–Trotter type theorem and sum-product estimate over finite fields, *European J. Combin.* **32** (2011), no. 8, 1177–1181.
- [18] L. A. Vinh, On a Furstenberg–Katznelson–Weiss type theorem over finite fields, *Ann. Comb.* **15** (2011), 541–547.
- [19] L. A. Vinh, On the generalized Erdős–Falconer distance problems over finite fields, *J. Number Theory* **133** (2013), 2939–2947.
- [20] L. A. Vinh, On point-line incidences in vector spaces over finite fields, *Discrete Appl. Math.* **177** (2014), 146–151.
- [21] L. A. Vinh, The solvability of norm, bilinear and quadratic equations over finite fields via spectra of graph, *Forum Math.* **26** (2014), no. 1, 141–175.
- [22] L. A. Vinh, Product graphs, sum-product graphs and sum-product estimate over finite rings, *Forum Math.* **27** (2015), no. 3, 1639–1655.
- [23] V. Vu, Sum-product estimates via directed expanders, *Math. Res. Lett.* **15** (2008), 375–388.