Incidence bounds and applications over finite fields

Nguyen Duy Phuong * Thang Pham† Nguyen Minh Sang‡
Claudiu Valculescu§ Le Anh Vinh¶

Abstract

In this paper we introduce a unified approach to deal with incidence problems between points and varieties over finite fields. More precisely, we prove that the number of incidences $I(\mathcal{P},\mathcal{V})$ between a set $\mathcal{P}$ of points and a set $\mathcal{V}$ of varieties of a certain form satisfies

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

This result is a generalization of the results of Vinh (2011), Bennett et al. (2014), and Cilleruelo et al. (2015). As applications of our incidence bounds, we obtain results on the pinned value problem and the Beck type theorem for points and spheres.

Using the approach introduced, we also obtain a result on the number of distinct distances between points and lines in $\mathbb{F}_q^2$, which is the finite field analogous of a recent result of Sharir et al. (2015).

1 Introduction

In 1983, Szemerédi and Trotter [30] proved that for any set $\mathcal{P}$ of n points, and any set $\mathcal{L}$ of n lines in the plane, the number of incidences between points of $\mathcal{P}$ and lines from $\mathcal{L}$ is asymptotically at most $n^{4/3}$. Apart from being interesting in itself and being a useful tool for various other discrete mathematics problem, the Szemerédi-Trotter theorem allowed various exentsions and generalizations. Tóth proved that the same bound holds when we work over the complex plane (see [31] for more details). Pach and Sharir [25] generalized the Szemerédi-Trotter theorem to the case of points and curves [25].

*Vietnam National University, Email: duyphuong@vnu.edu.vn

†EPFL, Lausanne, Switzerland. Research partially supported by Swiss National Science Foundation Grants 200020-144531 and 200021-137574. Email: thang.pham@epfl.ch

‡Vietnam National University, Email: sangnmkhtnhn@gmail.com

§EPFL, Lausanne, Switzerland. Research partially supported by Swiss National Science Foundation Grants 200020-144531 and 200021-137574. Email: adrian.valculescu@epfl.ch

¶Vietnam National University, Email: vinhla@vnu.edu.vn

Let $\mathbb{F}_q$ be a finite field of q elements where q is an odd prime power. Let $\mathcal{P}$ be a set of points and $\mathcal{L}$ be a set of lines in $\mathbb{F}_q^2$, and $I(\mathcal{P},\mathcal{L})$ be the number of incidences between $\mathcal{P}$ and $\mathcal{L}$. In [3], Bourgain, Katz, and Tao proved that if one has N lines and N points in the plane $\mathbb{F}_q^2$ for some $1 \ll N \ll q^2$, then there are at most $O(N^{3/2-\epsilon})$ incidences. Here and throughout, $X \gtrsim Y$ 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. The study of incidence problems over finite fields received a considerable amount of attention in recent years [5, 9, 16, 20, 21, 26, 28, 23, 32, 33, 34].

Note that the bound $N^{3/2}$ can be easily obtained from extremal graph theory. The relation between ϵ and α in the result of Bourgain, Katz, and Tao is difficult to determine, and it is far from being tight. If $N = \log_2 \log_6 \log_{18} q - 1$, then Grosu [9] proved that one can embed the point set and the line set to $\mathbb{C}^2$ without changing the incidence structure. Thus it follows from a tight bound on the number of incidences between points and lines in $\mathbb{C}^2$ due to Tóth [31] that $I(\mathcal{P},\mathcal{L}) = O(N^{4/3})$. By using methods from spectral graph theory, the fifth listed author [33] proved the tight bound for the case $N \gg q$ as follows.

Theorem 1.1 (**Vinh**, [33]). *Let $\mathcal{P}$ be a set of points and $\mathcal{L}$ be a set of lines in $\mathbb{F}_q^2$. Then we have*

$$\left| I(\mathcal{P},\mathcal{L}) - \frac{|\mathcal{P}||\mathcal{L}|}{q} \right| \leq q^{1/2}\sqrt{|\mathcal{P}||\mathcal{L}|}. \tag{1.1}$$

It follows from Theorem 1.1 that when $N \geq q^{3/2}$, the number of incidences between $\mathcal{P}$ and $\mathcal{L}$ is asymptotically at most $(1+o(1))N^{4/3}$ (this meets the Szemerédi-Trotter bound). Furthermore, if $|\mathcal{P}||\mathcal{L}| \gg q^3$, then the number of incidences is close to the expected value $|\mathcal{P}||\mathcal{L}|/q$. The lower bound in the theorem is also proved to be sharp up to a constant factor, in the sense that there is a set of points $\mathcal{P}$ and a set of lines $\mathcal{L}$ with $|\mathcal{P}| = |\mathcal{L}| = q^{3/2}$ that determines no incidence (for details see [34]). Theorem 1.1 has various applications in several combinatorial number theory problems (for example [13, 14, 19]).

The main purpose of this paper is to introduce a unified approach, which allows us to deal with incidence problems between points and certain families of varieties. As applications of incidence bounds, we obtain results on the pinned value problem and the Beck type theorem for points and spheres. Using this approach, we also obtain a result on the number of distinct distances between points and lines in $\mathbb{F}_q^2$.

1.1 Incidences between points and varieties

We first need the following definitions.

Definition 1.2. *Let S be a set of polynomials in $\mathbb{F}_q[x_1,\ldots,x_d]$. The variety determined by S is defined as follows*

$$V(S) := \{\mathbf{p} \in \mathbb{F}_q^d \,:\, f(\mathbf{p}) = 0 \text{ for all } \ f \in S\}.$$

Let $h_1(\mathbf{x}),\ldots,h_k(\mathbf{x})$ be fixed polynomials of degree at most $q-1$ in $\mathbb{F}_q[x_1,\ldots,x_d]$, and let $\mathbf{b}_i = (b_{i1},\ldots,b_{id})$, with $1 \leq i \leq k$, be fixed vectors in $(\mathbb{Z}^+)^d$, and $\gcd(b_{ij}, q-1) = 1$

for all $1 \leq j \leq d$. For any k-tuple $(\mathbf{a}_1, \ldots, \mathbf{a}_k)$ with $\mathbf{a}_i = (a_{i1}, \ldots, a_{id}, a_{i(d+1)}) \in \mathbb{F}_q^{d+1}$, we define

$$f_i(\mathbf{x}, \mathbf{a}_i) := h_i(\mathbf{x}) + \mathbf{a}_i \cdot \mathbf{x}^{\mathbf{b}_i}, \text{ where } \mathbf{a}_i \cdot \mathbf{x}^{\mathbf{b}_i} := \sum_{j=1}^{d} a_{ij} x_j^{b_{ij}} + a_{i(d+1)}.$$

Also, we define the corresponding families of varieties as follows:

$$V_{\mathbf{a}_1,\ldots,\mathbf{a}_k} := V\left(x_{d+1} - f_1\left(\mathbf{x}, \mathbf{a}_1\right), \ldots, x_{d+k} - f_k(\mathbf{x}, \mathbf{a}_k)\right) \subseteq \mathbb{F}_q^{d+k}, \text{ and}$$

$$W_{\mathbf{a}_1,\ldots,\mathbf{a}_k} := V\left(f_1(\mathbf{x}, \mathbf{a}_1), \ldots, f_k(\mathbf{x}, \mathbf{a}_k)\right) \subseteq \mathbb{F}_q^{d}.$$

Similarly to incidences between points of lines, given a set $\mathcal{P}$ of points and a set $\mathcal{V}$ of varieties, we define the number of incidences $I(\mathcal{P}, \mathcal{V})$ between $\mathcal{P}$ and $\mathcal{V}$ as the cardinality of the set $\{(p, v) \in \mathcal{P} \times \mathcal{V} \mid p \in v\}$. Our first main result is as follows:

Theorem 1.3. *Let $\mathcal{P}$ be a set of points in $\mathbb{F}_q^d \times \mathbb{F}_q^k$ and $\mathcal{V}$ a set of varieties of the form $V_{\mathbf{a}_1,\ldots,\mathbf{a}_k}$ defined above. Then the number of incidences between $\mathcal{P}$ and $\mathcal{V}$ satisfies*

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

As a consequence of Theorem 1.3, we obtain the following result.

Corollary 1.4. *Let $\mathcal{P}$ be a set of points in $\mathbb{F}_q^d$ and $\mathcal{V}$ be a set of varieties of the form $W_{\mathbf{a}_1,\ldots,\mathbf{a}_k}$ defined above. Then the number of incidences between $\mathcal{P}$ and $\mathcal{V}$ satisfies*

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

Let us observe that if $h_i(\mathbf{x}) \equiv 0$ and $\boldsymbol{b}_i = (1, \ldots, 1)$ for all $1 \leq i \leq k$, then a variety of the form $V_{\mathbf{a}_1,\ldots,\mathbf{a}_k}$ is a k-flat in the vector space $\mathbb{F}_q^{d+k}$. Therefore, we recover the bound established by Bennett et al. [2] on the number of incidences between points and flats:

Corollary 1.5 (**Bennett et al.** [2])**.** *Let $\mathcal{P}$ be a set of points, and $\mathcal{F}$ a set of k-flats in $\mathbb{F}_q^{d+k}$. Then the number of incidences between $\mathcal{P}$ and $\mathcal{F}$ satisfies*

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

It follows from Theorem 1.3 and Theorem 1.4 that if $|\mathcal{P}||\mathcal{V}| \geq 2q^{k(d+2)}$, then $\mathcal{P}$ and $\mathcal{V}$ determine at least one incidence. Also if $|\mathcal{P}||\mathcal{V}| \gg 2q^{k(d+2)}$, then the number of incidences is close to the expected value $|\mathcal{P}||\mathcal{V}|/q^k$.

There are some applications of Corollary 1.5 in combinatorial geometry problems, for instance, the number of congruent classes of triangles determined by a set of points in $\mathbb{F}_q^2$ in [2], and the number of right angles determined by a point set in $\mathbb{F}_q^d$ in [27].

When $k = 1$, varieties of the form $W_{\mathbf{a}_1,\ldots,\mathbf{a}_k}$ become hypersurfaces in $\mathbb{F}_q^d$, so they can be written as

$$W_{\mathbf{a}} = V\left(h(\mathbf{x}) + a_1 x_1^{b_1} + \cdots + a_d x_d^{b_d} + a_{d+1}\right),\ \mathbf{a} = (a_1, \ldots, a_d) \in \mathbb{F}_q^d. \tag{1.2}$$

Therefore, we obtain the following bound on the number of incidences between points and hypersurfaces:

Theorem 1.6. *Let $\mathcal{P}$ be a set of points in $\mathbb{F}_q^d$, and $\mathcal{S}$ a set of hypersurfaces of the form $W_{\mathbf{a}}$. Then the number of incidences between $\mathcal{P}$ and $\mathcal{S}$ satisfies*

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

When $h(\mathbf{x}) = x_1^2 + \cdots + x_d^2$, $\boldsymbol{a} = (1, \ldots, 1)$ and $b_1 = \ldots = b_d = 2$, as a consequence of Theorem 1.6, we recover the bound on the number of incidences between points and spheres obtained in [5, 26].

Corollary 1.7 (**Cilleruelo et al.** [5])**.** *Let $\mathcal{P}$ be a set of points, and $\mathcal{S}$ a set of spheres with arbitrary radii in $\mathbb{F}_q^d$. Then the number of incidences between $\mathcal{P}$ and $\mathcal{S}$ satisfies*

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

Theorem 1.7 also has various applications in several combinatorial problems over finite fields, for instance, Erdős distinct distance problem, the Beck type theorem for points and circles, and subset without repeated distance, see [5, 26] for more details.

1.2 Pinned values and Distinct radii

Pinned values problem: The distance function between two points $\mathbf{x}$ and $\mathbf{y}$ in $\mathbb{F}_q^d$, denoted by $||\mathbf{x} - \mathbf{y}||$, is defined as $||\mathbf{x} - \mathbf{y}|| = (x_1 - y_1)^2 + \cdots + (x_d - y_d)^2$. Although it is not a norm, the function $||\mathbf{x} - \mathbf{y}||$ has properties similar to the Euclidean norm (for example, it is invariant under orthogonal matrices).

Bourgain, Katz, and Tao [3] were the first to consider the the finite analogue of the classical Erdős distinct distance problem, namely to determine the smallest possible cardinality of the set $\Delta_{\mathbb{F}_q}(\mathcal{E}) = \{||\mathbf{x} - \mathbf{y}|| = (x_1 - y_1)^2 + \cdots + (x_d - y_d)^2 \colon \mathbf{x}, \mathbf{y} \in \mathcal{E}\} \subset \mathbb{F}_q$, where $\mathcal{E} \subset \mathbb{F}_q^d$. More precisely, they proved that $|\Delta_{\mathbb{F}_q}(\mathcal{E})| \gtrsim |\mathcal{E}|^{1/2+\epsilon}$, where $|\mathcal{E}| = q^\alpha$ and $\epsilon > 0$ is a small constant depending on α.

Iosevich and Rudnev [17] studied the following question: how large does $\mathcal{E} \subset \mathbb{F}_q^d$, $d \geq 2$ have to be, so that $\Delta_{\mathbb{F}_q}(\mathcal{E})$ contains a positive proportion of the elements of $\mathbb{F}_q$. They proved that if $\mathcal{E} \subset \mathbb{F}_q^d$ such that $|\mathcal{E}| \gtrsim Cq^{d/2}$ for sufficiently large C, then $|\Delta_{\mathbb{F}_q}(\mathcal{E})| = \Omega\left(\min\left\{q, q^{-(d-1)/2}|\mathcal{E}|\right\}\right)$ (in other words, for any sufficiently large $\mathcal{E} \subseteq \mathbb{F}_q^d$, the set $\Delta_{\mathbb{F}_q}(\mathcal{E})$ contains a positive proportion of the elements of $\mathbb{F}_q$). From this, one obtains that that if $|\mathcal{E}| \gtrsim q^{(d+1)/2}$, then $|\Delta_{\mathbb{F}_q}(\mathcal{E})| \gtrsim q$. This is in fact directly related to Falconer's

result [8] in Euclidean space, saying that for every set $\mathcal{E}$ with Hausdorff dimension greater that $(d+1)/2$, the distance set is of positive measure.

Hart et al. [11] proved that the exponent $(d+1)/2$ is the best possible in odd dimensions, although in even dimensions, it might still be place for improvement. Chapman et al. [6] showed that if a set $\mathcal{E} \subseteq \mathbb{F}_q^2$ satisfies $|\mathcal{E}| \geq q^{4/3}$, then $|\Delta_{\mathbb{F}_q}(\mathcal{E})|$ contains a positive proportion of the elements of $\mathbb{F}_q$. In the same paper it was also proved that for any set $\mathcal{P}$ of points in $\mathbb{F}_q^d$ with $|\mathcal{P}| \geq q^{(d+1)/2}$, there exists a subset $\mathcal{P}'$ in $\mathcal{P}$, such that $|\mathcal{P}'| = (1-o(1))|\mathcal{P}|$, and for any $\mathbf{y} \in \mathcal{P}'$, $|\Delta_{\mathbb{F}_q}(\mathcal{P}, \mathbf{y})| \gtrsim q$, where $\Delta_{\mathbb{F}_q}(\mathcal{P}, \mathbf{y}) = \{||\boldsymbol{x} - \boldsymbol{y}||\colon \boldsymbol{x} \in \mathcal{P}\}$. (which is the pinned distance problem)

Let $Q(\mathbf{x})$ be a non-degenerate quadratic form. For a fixed non-square element $\lambda \in \mathbb{F}_q \setminus \{0\}$, the quadraic form $Q(\mathbf{x})$ can be written as

$$Q(\mathbf{x}) = x_1^2 - x_2^2 + x_3^2 - x_4^2 + \cdots + x_{2m-1}^2 - \epsilon x_{2m}^2, \quad \text{if} \quad d = 2m,$$

and

$$Q(\mathbf{x}) = x_1^2 - x_2^2 + x_3^2 - x_4^2 + \cdots + x_{2m-1}^2 - x_{2m}^2 + \epsilon x_{2m+1}^2, \quad \text{if} \quad d = 2m+1,$$

where $\epsilon \in \{1, \lambda\}$, see [18] for more details.

Given a point $\boldsymbol{q} \in \mathbb{F}_q^d$ and a set of points $\mathcal{P} \subseteq \mathbb{F}_q^d$, we define the pinned distance set determined by $Q(\mathbf{x})$ and $\mathbf{q}$ as $\Delta_Q(\mathcal{P}, \boldsymbol{q}) = \{Q(\boldsymbol{p} - \boldsymbol{q})\colon \boldsymbol{p} \in \mathcal{P}\}$. Using methods from spectral graph theory, the fifth listed author obtained the following:

Theorem 1.8 (**Vinh** [35])**.** *Let $\mathcal{P}$ be a set of points in $\mathbb{F}_q^d$ such that $|\mathcal{P}| \geq q^{(d+1)/2}$, then there exists a subset $S \subset \mathcal{P}$ such that $|S| = (1-o(1))|\mathcal{P}|$, and for any $\boldsymbol{y} \in S$, we have $|\Delta_Q(\mathcal{P}, \boldsymbol{y})| \gtrsim q$.*

In our paper, as an application of Theorem 1.3 and using a similar approach to the one in [5], we generalize Theorem 1.8 to *non-degenerate polynomials*. If $F(\mathbf{x}, \mathbf{y})$ is a polynomial in $\mathbb{F}_q[x_1, \ldots, x_d, y_1, \ldots, y_d]$, we say that $F(\mathbf{x}, \mathbf{y})$ is *non-degenerate* if $F(\mathbf{x}, \mathbf{y})$ can be written as

$$F(\mathbf{x}, \mathbf{y}) := g(\mathbf{x}, \mathbf{y}) + (x_1^{b_1}, \ldots, x_d^{b_d}) M (y_1^{c_1}, \ldots, y_d^{c_d})^T,$$

where $g(\mathbf{x}, \mathbf{y}) = g_1(\mathbf{x}) + g_2(\mathbf{y}) \in \mathbb{F}_q[x_1, \ldots, x_d, y_1, \ldots, y_d]$, M is a $d \times d$ invertible matrix, and $\gcd(c_i, q-1) = 1$ for all $1 \leq i \leq d$.

Theorem 1.9. *Let $F(\mathbf{x}, \mathbf{y})$ be a non-degenerate polynomial and $\mathcal{P}$ be a set of points in $\mathbb{F}_q^d$ such that $|\mathcal{P}| \geq (\sqrt{1-c^2}/c^2) q^{(d+1)/2}$ for some constant $0 < c < 1$. Then there is $\mathcal{P}' \subset \mathcal{P}$ such that $|\mathcal{P}'| \geq (1-c)|\mathcal{P}|$, and for any $\boldsymbol{y} \in \mathcal{P}'$, $|\Delta_F(\mathcal{P}, \boldsymbol{y})| \geq (1-c)q$, where $\Delta_F(\mathcal{P}, \boldsymbol{q}) = \{F(\boldsymbol{p}, \boldsymbol{q})\colon \boldsymbol{p} \in \mathcal{P}\}$.*

Corollary 1.10. *Let $F(\mathbf{x}, \mathbf{y})$ be a non-degenerate polynomial and $\mathcal{P}$, $\mathcal{Q}$ be sets of points in $\mathbb{F}_q^d$ such that $|\mathcal{P}||\mathcal{Q}| \geq 2\sqrt{3} q^{d+1}$ for some constant $0 < c < 1$. Then there is $\mathcal{P}' \subset \mathcal{P}$ such that $|\mathcal{P}'| \geq |\mathcal{P}|/2$, and for any $\boldsymbol{y} \in \mathcal{P}'$, $|\Delta_F(\mathcal{Q}, \boldsymbol{y})| \geq q/2$, where $\Delta_F(\mathcal{Q}, \boldsymbol{q}) = \{F(\boldsymbol{p}, \boldsymbol{q})\colon \boldsymbol{p} \in \mathcal{Q}\}$.*

The Beck type theorem for points and spheres: Let $\mathcal{P}$ be a set of points in $\mathbb{F}_q^2$. Iosevich, Rudnev, and Zhai [19] made the first investigation on the finite fields analogue of the Beck type theorem for points and lines in $\mathbb{F}_q^2$. More precisely, they proved that if $|\mathcal{P}| \geq 64q \log q$, then the number of distinct lines determined by $\mathcal{P}$ is at least $q^2/8$. In [23], Lund and Saraf improved the condition of the cardinality of $\mathcal{P}$ to $3q$. Recently, Cilleruelo et al. [5] studied the Beck type theorem for points and circles in $\mathbb{F}_q^2$ by employing the lower bound on the number of incidences between points and circles in $\mathbb{F}_q^2$. Formally, their result is as follows.

Theorem 1.11 (**Cilleruelo et al.** [5]). *Let $\mathcal{P}$ be a set of points in $\mathbb{F}_q^2$. If $|\mathcal{P}| \geq 5q$, then the number of distinct circles determined by $\mathcal{P}$ is at least $4q^3/9$.*

As a consequence of Theorem 1.11, we obtain the following result.

Theorem 1.12. *Let $\mathcal{P}$ be a set of $5q$ points in $\mathbb{F}_q^2$. Then the number of distinct radii of circles determined by $\mathcal{P}$ is at least $4q/9$.*

Note that it is hard to generalize Theorem 1.11 in higher dimensional cases by their arguments. In the following theorem, we will give an approach to address this problem by using a result on the number of pinned distinct distances.

Theorem 1.13. *Let $\mathcal{P}$ be a set of $8q^2$ points in $\mathbb{F}_q^3$. Then the number of distinct spheres determined by $\mathcal{P}$ is at least $q^4/9$.*

As a consequence of Theorem 1.13, we obtain the following result on the number of distinct radii of spheres determined by a set of points in $\mathbb{F}_q^3$.

Theorem 1.14. *Let $\mathcal{P}$ be a set of $8q^2$ points in $\mathbb{F}_q^3$. Then the number of distinct radii of spheres determined by $\mathcal{P}$ is at least $q/9$.*

Remark 1.15. *We note that one can follow the proof of Theorem 1.13 to prove that there exist constants $c = c(d)$ and $c' = c'(d)$ such that there are at least cq^{d+1} d-dimensional spheres determined by a set of $c'q^{d-1}$ points in $\mathbb{F}_q^d$.*

1.3 Distinct distances between points and lines

As already mentioned in the abstract, we use the same approach to address the finite field variants of two recent results due to Sharir et al. [29], involving distances between points and lines. The first bound is a lower bound for the minimum number of distinct distances between a set of points and a set of lines, both in the plane. A second result is a lower bound for the minimum number of distinct distances between a set of non-collinear points and the lines that they span.

Theorem 1.16 (**Sharir et al.** [29]). *For $m^{1/2} \leq n \leq m^2$, the minimum number $D(m, n)$ of point-line distances between m points and n lines in $\mathbb{R}^2$ satisfies $D(m, n) = \Omega(m^{1/5}n^{3/5})$*

Theorem 1.17 (**Sharir et al.** [29]). *The minimum number $H(m)$ of point-line distances between m non-collinear points and their spanned lines satisfies $H(m) = \Omega(m^{4/3})$.*

In the plane over finite fields, a line $ax+by+c=0$ is *degenerate* if and only if $a^2+b^2=0$. Similarly, a hyperplane $a_1x_1+\cdots+a_dx_d+a_{d+1}=0$ in $\mathbb{F}_q^d$ is *degenerate* if and only if $a_1^2+\cdots+a_d^2=0$. For a point $p=(x_p,y_p)\in\mathbb{F}_q^2$ and a non-degenerate line $l:\ ax+by+c=0$ in $\mathbb{F}_q^2$, let $d(p,l)$ denote the distance function between p and l, defined as

$$d(p,l)=\frac{(ax_p+by_p+c)^2}{a^2+b^2}.$$

For a set of points $\mathcal{P}$ in $\mathbb{F}_q^2$ and a line l, set $\Delta_{\mathbb{F}_q}(\mathcal{P},l)=\{d(p,l):p\in\mathcal{P}\}$. Distances between points and non-degenerate lines are preserved under rotations and translations.

Similarly, for a point $p=(x_p^1,x_p^2,\ldots,x_p^d)\in\mathbb{F}_q^d$ and a non-dengenerate hyperplane $h:a_1x_1+\cdots+a_dx_d+a_{d+1}=0$, we define the point-hyperplane distance

$$d(p,h)=(a_1x_p^1+\cdots+a_dx_p^d+a_{d+1})^2/(a_1^2+\cdots+a_d^2).$$

For a set of points $\mathcal{P}$ in $\mathbb{F}_q^d$ and a hyperplane h, we let $\Delta_{\mathbb{F}_q}(\mathcal{P},h)=\{d(p,h):p\in\mathcal{P}\}$.

We prove that under a similar condition as in the result due to Chapman et al. [6] on the number of distinct distances between points in $\mathbb{F}_q^2$, the set of distances between $\mathcal{P}$ and $\mathcal{L}$ contains a positive proportion of the elements of $\mathbb{F}_q$.

Theorem 1.18. *Let $\mathcal{P}$ be a set of points and $\mathcal{L}$ be a set of non-degenerate lines in $\mathbb{F}_q^2$, such that*

$$|\mathcal{P}||\mathcal{L}|\geq\frac{4(1-c^2)}{(1/2-(1-c^2))^2}q^{8/3}$$

with $1-c^2<1/4$. Then there exists a subset $\mathcal{L}'$ of $\mathcal{L}$ with $|\mathcal{L}'|=(1-o(1))|\mathcal{L}|$, so that $|\Delta_{\mathbb{F}_q}(\mathcal{P},l)|\gtrsim q$, for each line l in $\mathcal{L}'$.

Combining a finite field variant of Beck's theorem (which can be found in [23]) with Theorem 1.18, we obtain the following bound on the number of distinct distances between a set of points and their spanned lines.

Corollary 1.19. *Let $\mathcal{P}$ be a set of points in $\mathbb{F}_q^2$ with $|\mathcal{P}|\geq 3q$, and let $\mathcal{L}$ be the set of lines spanned by $\mathcal{P}$ in $\mathbb{F}_q^2$. Then there exists a subset $\mathcal{L}'$ of $\mathcal{L}$ with $|\mathcal{L}'|=(1-o(1))|\mathcal{L}|$, so that $|\Delta_{\mathbb{F}_q}(\mathcal{P},l)|\gtrsim q$, for each line l in $\mathcal{L}'$.*

By similar arguments as in the proof of Theorem 1.18, we obtain a similar result on the number of distinct distances between points and hyperplanes in d-dimensional vector space over finite fields as follows.

Theorem 1.20. *Let $\mathcal{P}$ be a set of points in $\mathbb{F}_q^d$, and $\mathcal{H}$ be a set of non-degenerate hyperplanes in $\mathbb{F}_q^d$, such that*

$$|\mathcal{P}||\mathcal{H}|\geq\frac{4(1-c^2)}{(1/2-(1-c^2))^2}q^{4d/3},$$

with $1-c^2<1/4$. Then there exists a subset $\mathcal{H}'$ of $\mathcal{H}$ with $|\mathcal{H}'|=(1-o(1))|\mathcal{H}|$, so that $|\Delta_{\mathbb{F}_q}(\mathcal{P},h)|\gtrsim q$, for each line h in $\mathcal{H}'$.

2 Tools

This section contains a couple of notions and theorems that we use as tools in the proofs of our main results. We fist state the well-known Schwartz-Zippel Lemma (for proof refer to Theorem 6.13 in [24]).

Lemma 2.1 (**Schwartz-Zippel**). *Let $P(\boldsymbol{x})$ be a non-zero polynomial of degree k. Then*

$$\left|\{\boldsymbol{x} \in \mathbb{F}_q^d : P(\boldsymbol{x}) = 0\}\right| \leq kq^{d-1}.$$

We say that a bipartite graph is *biregular* if in both of its two parts, all vertices have the same degree. If A is one of the two parts of a bipartite graph, we write $\deg(A)$ for the common degree of the vertices in A. Label the eigenvalues so that $|\lambda_1| \geq |\lambda_2| \geq \cdots \geq |\lambda_n|$. Note that in a bipartite graph, we have $\lambda_2 = -\lambda_1$. The following variant of the expander mixing lemma is proved in [7]. We include the proof of this result for the sake of completeness of the paper.

Lemma 2.2 (**Expander mixing lemma**). *Let G be a bipartite graph with parts A, B such that the vertices in A all have degree a and the vertices in B all have degree b. Then, for any two sets $X \subset A$ and $Y \subset B$, the number of edges between X and Y, denoted by $e(X, Y)$, satisfies*

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

where λ_3 is the third eigenvalue of G.

Proof. We assume that the vertices of G are labeled from 1 to $|A| + |B|$, and we denote by M the adjacency matrix of G having the form

$$M = \begin{bmatrix} 0 & N \\ N^t & 0 \end{bmatrix},$$

where N is the $|A| \times |B|$ $0-1$ matrix, with $N_{ij} = 1$ if and only if there is an edge between i and j. First, let us recall some properties of the eigenvalues of the matrix M. Since all vertices in A have degree a and all vertices in B have degree b, all eigenvalues of M are bounded by $\sqrt{ab}$. Indeed, let us denote the L_1 vector norm by $||\cdot||_1$, and let $\mathbf{e}_v$ be the unit vector having 1 in the position corresponding to vertex v and zeroes elsewhere. One can observe that $||M^2 \cdot \mathbf{e}_v||_1 \leq ab$, so the absolute value of each eigenvalue of M is bounded by $\sqrt{ab}$. Let $\mathbf{1}_X$ denote the column vector of size $|A| + |B|$ having 1s in the positions corresponding to the set of vertices X and 0s elsewhere. Then, we have that

$$M(\sqrt{a}\mathbf{1}_A + \sqrt{b}\mathbf{1}_B) = b\sqrt{a}\mathbf{1}_B + a\sqrt{b}\mathbf{1}_A = \sqrt{ab}(\sqrt{a}\mathbf{1}_A + \sqrt{b}\mathbf{1}_B),$$

$$M(\sqrt{a}\mathbf{1}_A - \sqrt{b}\mathbf{1}_B) = b\sqrt{a}\mathbf{1}_B - a\sqrt{b}\mathbf{1}_A = -\sqrt{ab}(\sqrt{a}\mathbf{1}_A - \sqrt{b}\mathbf{1}_B),$$

which implies that $\lambda_1 = \sqrt{ab}$ and $\lambda_2 = -\sqrt{ab}$ are the first and second eigenvalues, corresponding to the eigenvectors $(\sqrt{a}\mathbf{1}_A + \sqrt{b}\mathbf{1}_B)$ and $(\sqrt{a}\mathbf{1}_A - \sqrt{b}\mathbf{1}_B)$.

Let $W^\perp$ be a subspace spanned by the vectors $\mathbf{1}_A$ and $\mathbf{1}_B$. Since M is a symmetric matrix, the eigenvectors of M, except $\sqrt{a}\mathbf{1}_A + \sqrt{b}\mathbf{1}_B$ and $\sqrt{a}\mathbf{1}_A - \sqrt{b}\mathbf{1}_B$, span W. Therefore, for any $u \in W$, $Mu \in W$, and $||Mu|| \leq \lambda_3||u||$. Let us now remark the following facts:

1. Let K be a matrix of the form $\begin{bmatrix} 0 & J \\ J & 0 \end{bmatrix}$, where J is the $|A| \times |B|$ all-ones matrix. If $u \in W$, then $Ku = 0$ since every row of K is either $\mathbf{1}_A^T$ or $\mathbf{1}_B^T$.
2. If $w \in W^\perp$, then $(M - (a/|B|)K)w = 0$. Indeed, it follows from the facts that $a|A| = b|B|$, and $M\mathbf{1}_A = b\mathbf{1}_B = (a/|B|)K\mathbf{1}_A$, $M\mathbf{1}_B = a\mathbf{1}_A = (a/|B|)K\mathbf{1}_B$.

Since $e(X,Y) = \mathbf{1}_Y^T M \mathbf{1}_X$ and $|X||Y| = \mathbf{1}_Y^T K \mathbf{1}_X$,

$$\left| e(X,Y) - \frac{a}{|B|}|X||Y| \right| = \left| \mathbf{1}_Y^T (M - \frac{a}{|B|}K)\mathbf{1}_X \right|.$$

For any vector v, let $\bar{v}$ be the orthogonal projection onto W, so that $\overline{v} \in W$, and $v - \overline{v} \in W^\perp$. Thus

$$\mathbf{1}_Y^T (M - \frac{a}{|B|}K)\mathbf{1}_X = \mathbf{1}_Y^T (M - \frac{a}{|B|}K)\overline{\mathbf{1}_X} = \mathbf{1}_Y^T M \overline{\mathbf{1}_X} = \overline{\mathbf{1}_Y}^T M \overline{\mathbf{1}_X}, \text{ so}$$

$$\left| e(X,Y) - \frac{a}{|B|}|X||Y| \right| \leq \lambda_3 ||\overline{\mathbf{1}_X}||\ ||\overline{\mathbf{1}_Y}||.$$

Since

$$\overline{\mathbf{1}_X} = \mathbf{1}_X - ((\mathbf{1}_X \cdot \mathbf{1}_A)/(\mathbf{1}_A \cdot \mathbf{1}_A))\,\mathbf{1}_A = \mathbf{1}_X - (|X|/|A|)\mathbf{1}_A,$$

we have $||\overline{\mathbf{1}_X}|| = \sqrt{|X|(1 - |X|/|A|)}$. Similarly, $||\overline{\mathbf{1}_Y}|| = \sqrt{|Y|(1 - |Y|/|B|)}$.

In other words,

$$\left| e(X,Y) - \frac{a}{|B|}|X||Y| \right| \leq \lambda_3 \sqrt{|X||Y|(1 - |X|/|A|)(1 - |Y|/|B|)},$$

which completes the proof of the lemma. □

3 Proofs of Theorems 1.3, 1.4, and Corollary 1.7

We start by proving the following lemma.

Lemma 3.1. *For any two k-tuples of vectors $(\mathbf{a}_1, \ldots, \mathbf{a}_k) \neq (\mathbf{c}_1, \ldots, \mathbf{c}_k)$, we have $V_{\mathbf{a}_1,\ldots,\mathbf{a}_k} \neq V_{\mathbf{c}_1,\ldots,\mathbf{c}_k}$.*

Proof. Since $(\mathbf{a}_1, \ldots, \mathbf{a}_k) \neq (\mathbf{c}_1, \ldots, \mathbf{c}_k)$, without loss of generality, we can assume that $\mathbf{a}_1 \neq \mathbf{c}_1$. Therefore,

$$f_1(\mathbf{x}, \mathbf{a}_1) - f_1(\mathbf{x}, \mathbf{c}_1) = (a_{11} - c_{11})x_1^{b_{11}} + \cdots + (a_{1d} - c_{1d})x_d^{b_{1d}} + a_{1(d+1)} - c_{1(d+1)},$$

is a non-zero polynomial of degree at most $q-1$ in $\mathbb{F}_q[x_1, \ldots, x_d]$.

By Lemma 2.1, the cardinality of $V(f_1(\mathbf{x}, \mathbf{a}_1) - f_1(\mathbf{x}, \mathbf{c}_1))$ is at most $(q-1)q^{d-1} < q^d$. Let us observe that if $V_{\mathbf{a}_1,\ldots,\mathbf{a}_k} \equiv V_{\mathbf{c}_1,\ldots,\mathbf{c}_k}$, then $|V(f_1(\mathbf{x}, \mathbf{a}_1) - f_1(\mathbf{x}, \mathbf{c}_1))| = q^d$. This is indeed the case since each variety contains exactly q^d points in $\mathbb{F}_q^d \times \mathbb{F}_q^k$. Thus, we obtain

$$V\left(x_{d+1} - f_1(\mathbf{x}, \mathbf{a}_1), \ldots, x_{d+k} - f_k(\mathbf{x}, \mathbf{a}_k)\right) \neq V\left(x_{d+1} - f_1(\mathbf{x}, \mathbf{c}_1), \ldots, x_{d+k} - f(\mathbf{x}, \mathbf{c}_k)\right),$$

which completes the proof of the lemma. □

We define the bipartite graph $G = (A \cup B, E)$ as follows. The first vertex part A is $(\mathbb{F}_q)^d \times (\mathbb{F}_q)^k$ and the second vertex part B is the set of all varieties $V_{\mathbf{a_1},\ldots,\mathbf{a_k}}$ with $(\mathbf{a_1},\ldots,\mathbf{a_k}) \in \left(\mathbb{F}_q^{d+1}\right)^k$. We draw an edge between a point $\mathbf{p} \in A$ and a variety $\mathbf{v} \in B$ if and only if $\mathbf{p} \in \mathbf{v}$. It is easy to check that G is biregular with $\deg(A) = q^{dk}$ and $\deg(B) = q^d$.

Lemma 3.2. *Let λ_3 be the third eigenvalue of the adjacency matrix of G. Then $|\lambda_3| \leq q^{dk/2}$.*

Proof. Let M be the adjacency matrix of G, so $M = \begin{bmatrix} 0 & N \\ N^T & 0 \end{bmatrix}$, where N is a $q^{d+k} \times q^{(d+1)k}$ matrix, with $N_{\mathbf{pv}} = 1$ if $\mathbf{p} \in \mathbf{v}$, $N_{\mathbf{pv}} = 0$ if $\mathbf{p} \notin \mathbf{v}$.

Let J be the $q^{d+k} \times q^{k(d+1)}$ all-one matrix and $K = \begin{bmatrix} 0 & J \\ J^T & 0 \end{bmatrix}$. We prove that M satisfies

$$M^3 = q^{dk}M + (q^d - 1)q^{k(d-1)}K.$$

If $\mathbf{v}$ is an eigenvector corresponding to the third eigenvalue λ_3, then $K\mathbf{v} = 0$. Therefore from the equation above one obtains that $\lambda_3^3 = q^{dk}\lambda_3$, which implies that $|\lambda_3| = \sqrt{q^{dk}}$.

Let us observe that the $(\mathbf{p}, \mathbf{v})$-entry of M^3 equals the number of walks of length three from $\mathbf{p} \in A$ to $\mathbf{v} \in B$, that is the number of quadruples $(\mathbf{p}, \mathbf{v}', \mathbf{p}', \mathbf{v})$, where $\mathbf{p}, \mathbf{p}' \in A, \mathbf{v}, \mathbf{v}' \in B$, and $(\mathbf{p}, \mathbf{v}'), (\mathbf{p}', \mathbf{v}'), (\mathbf{p}', \mathbf{v})$ are edges of G.

Given two points $\mathbf{p} = (p_1, \ldots, p_{d+k})$ and $\mathbf{p}' = (p'_1, \ldots, p'_{d+k})$, the varieties containing both $\mathbf{p}$ and $\mathbf{p}'$, and corresponding to k-tuples $(\mathbf{a_1}, \ldots, \mathbf{a_k}) \in \mathbb{F}_q^{(d+1)k}$ satisfies

$$\begin{array}{rcl} p_{d+i} & = & h_i(p_1, \ldots, p_d) + a_{i1}p_1^{b_{i1}} + \cdots + a_{id}p_d^{b_{id}} + a_{id+1}, \\ p'_{d+i} & = & h_i(p'_1, \ldots, p'_d) + a_{i1}(p'_1)^{b_{i1}} + \cdots + a_{id}(p'_d)^{b_{id}} + a_{id+1}, \end{array} \tag{3.1}$$

for all $1 \leq i \leq k$. Thus, for each $1 \leq i \leq k$, we have

$$p_{d+i} - p'_{d+i} = h_i(p_1, \ldots, p_d) - h_i(p'_1, \ldots, p'_d) + a_{i1}(p_1^{b_{i1}} - (p'_1)^{b_{i1}}) + \cdots + a_{id}(p_d^{b_{id}} - (p'_d)^{b_{id}}). \tag{3.2}$$

Let us observe that for each $a \in \mathbb{F}_q$, if $\gcd(r, q-1) = 1$, then the equation $x^r = a^r$ has the unique solution $x = a$. Thus if $p_i = p'_i$ for all $1 \leq i \leq d$, then there exists at least one variety containing both p and p' if and only if $p_{d+i} = p'_{d+i}$ for all $1 \leq i \leq k$. This implies that $\mathbf{p} = \mathbf{p}'$.

We now count the number of walks of length three as follows. If $\mathbf{p} \notin \mathbf{v}$, then we can choose $\mathbf{p}' \neq \mathbf{p}$ in v such that $p_i \neq p'_i$ for some $1 \leq i \leq d$ (otherwise, there is no v' containing both $\mathbf{p}$ and $\mathbf{p}'$). We assume that $p_1 \neq p'_1$, so $p_1^{b_{i1}} \neq (p'_1)^{b_{i1}}$. Therefore, for each choice of $(a_{i2}, \ldots, a_{id})$, a_{i1} is determined uniquely by (3.2), and a_{id+1} is determined by any equation in (3.1). In this case, the number of walks of length three is $(q^d - 1)q^{k(d-1)}$.

If $\mathbf{p} \in \mathbf{v}$, then again there are $(q^d - 1)q^{k(d-1)}$ walks with $\mathbf{p} \neq \mathbf{p}'$. Now we can choose $\mathbf{p} = \mathbf{p}'$. In this case, the number of walks equals the degree of $\mathbf{p}$. Thus if $\mathbf{p} \in \mathbf{v}$, then the number of walks of length three from $\mathbf{p}$ to $\mathbf{v}$ is $(q^d - 1)q^{k(d-1)} + q^{dk}$.

In conclusion, M satisfies $M^3 = q^{dk}M + (q^d - 1)q^{k(d-1)}K$, which completes the proof of the lemma. □

Combining Lemma 2.2 and Lemma 3.2, Theorem 1.3 follows. We are now ready to prove Theorem 1.4.

Proof of Theorem 1.4. Let $\mathcal{P}' = \{p \times (0)^k : p \in \mathcal{P}\}$, then $|\mathcal{P}'| = |\mathcal{P}|$. Note that the number of incidences between points in $\mathcal{P}$ and varieties $W_{\mathbf{a}_1,\ldots,\mathbf{a}_k}$ is the number of incidences between points in $\mathcal{P}'$ and varieties $V_{\mathbf{a}_1,\ldots,\mathbf{a}_k}$. Therefore, Theorem 1.4 follows immediately from Theorem 1.3. □

Proof of Corollary 1.7. Let s be the sphere of radius r with the center $\mathbf{a} \in \mathbb{F}_q^d$, that is the set of points $(x_1, \cdots, x_d) \in \mathbb{F}_q^d$ satisfying $(x_1 - a_1)^2 + \cdots + (x_d - a_d)^2 = r$. Therefore, we can re-write the formula for the points contained in s as

$$x_1^2 + \cdots x_d^2 + \sum_{i=1}^{d} a_i x_i - (r - \sum_{i=1}^{d} a_i^2) = 0.$$

Let $h(\mathbf{x}) = x_1^2 + \cdots + x_d^2$, $\mathbf{b} = (1, \ldots, 1)$, and $\mathbf{a} = \left(a_1, \ldots, a_d, -\left(r - \sum_{i=1}^{d} a_i^2\right)\right)$. Then Corollary 1.7 follows immediately from Theorem 1.6. □

4 Proof of Theorem 1.9

Let us define

$$\mathcal{S} := \left\{x_{d+1} = F(\mathbf{x}, \mathbf{q}) \colon \mathbf{q} \in \mathcal{P}\right\}, \ \mathcal{P}' := \left\{(\mathbf{p}, t) \in \mathbb{F}_q^{d+1} \colon (\mathbf{p}, t) \in \mathcal{P} \times \Delta_F(\mathcal{P}, \mathbf{p})\right\}.$$

Since $F(\mathbf{x}, \mathbf{y})$ is non-degenerate, $\mathcal{S}$ is a set of hypersurfaces. It follows from Theorem 1.3 for the case $k = 1$ that

$$e(\mathcal{P}', \mathcal{S}) \leq \frac{|\mathcal{P}'||\mathcal{S}|}{q} + q^{d/2}\sqrt{|\mathcal{P}'||\mathcal{S}|}.$$

On the other hand, we have $e(\mathcal{P}', \mathcal{S}) = |\mathcal{P}|^2$, thus

$$\begin{aligned} |\mathcal{P}|^2 \leq e(\mathcal{P}', \mathcal{S}) &\leq \frac{|\mathcal{P}'||\mathcal{S}|}{q} + q^{d/2}\sqrt{|\mathcal{P}'||\mathcal{S}|}. \\ &= \frac{|\mathcal{P}| \sum_{\mathbf{p} \in \mathcal{P}} |\Delta_F(\mathcal{P}, \mathbf{p})|}{q} + q^{d/2}\sqrt{|\mathcal{P}| \sum_{\mathbf{p} \in \mathcal{P}} |\Delta_F(\mathcal{P}, \mathbf{p})|}. \end{aligned} \tag{4.1}$$

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

$$|\mathcal{P}|^2 \leq |\mathcal{P}|^2(1 - c^2) + q^{(d+1)/2}|\mathcal{P}|\sqrt{(1 - c^2)}.$$

This implies that

$$|\mathcal{P}| < \sqrt{\frac{(1 - c^2)}{c^4}} q^{(d+1)/2},$$

which is a contradiction. Therefore,

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

Let $\mathcal{P}' := \{\mathbf{p}\in\mathcal{P}\colon |\Delta_F(\mathcal{P},\mathbf{p})| > (1-c)q\}$. Suppose that $|\mathcal{P}'| < (1-c)|\mathcal{P}|$, we have

$$\sum_{\mathbf{p}\in\mathcal{P}\setminus\mathcal{P}'}|\Delta_F(\mathcal{P},\mathbf{p})| \le (|\mathcal{P}|-|\mathcal{P}'|)(1-c)q, \text{ and } \sum_{\mathbf{p}\in\mathcal{P}'}|\Delta_F(\mathcal{P},\mathbf{p})| \le q|\mathcal{P}'|.$$

Putting everything together, we obtain

$$\sum_{\mathbf{p}\in\mathcal{P}}|\Delta_F(\mathcal{P},\mathbf{p})| \le (1-c)q|\mathcal{P}| + cq|\mathcal{P}'| < (1-c)q|\mathcal{P}| + cq(1-c)|\mathcal{P}| = (1-c^2)q|\mathcal{P}|,$$

which contradicts (4.2), and the theorem follows.

5 Proofs of Theorem 1.13 and Theorem 1.14

We first need the following lemma.

Lemma 5.1. *There is a unique sphere in $\mathbb{F}_q^3$ passing through four given non-coplanar points.*

Proof. Let $\mathbf{p}_1 = (a_1,a_2,a_3)$, $\mathbf{p}_2 = (b_1,b_2,b_3)$, $\mathbf{p}_3 = (c_1,c_2,c_3)$, and $\mathbf{p}_4 = (d_1,d_2,d_3)$ be given non-coplanar points. We will show that there exists a unique sphere in $\mathbb{F}_q^3$ containing $\mathbf{p}_1$, $\mathbf{p}_2$, $\mathbf{p}_3$, and $\mathbf{p}_4$. In fact, a sphere passing through these four points can be written as

$$(x-e_1)^2+(y-e_2)^2+(z-e_3)^2 = r, \text{ with } e_1,e_2,e_3,r\in\mathbb{F}_q.$$

Let $e_1' = -2e_1, e_2' = -2e_2, e_3' = -2e_3$, and $r' = e_1^2+e_2^2+e_3^2-r$. Then we obtain the following system of four equations

$$\begin{aligned}
a_1e_1'+a_2e_2'+a_3e_3'+r' &= -a_1^2-a_2^2-a_3^2\\
b_1e_1'+b_2e_2'+b_3e_3'+r' &= -b_1^2-b_2^2-b_3^2\\
c_1e_1'+c_2e_2'+c_3e_3'+r' &= -c_1^2-c_2^2-c_3^2\\
d_1e_1'+d_2e_2'+d_3e_3'+r' &= -d_1^2-d_2^2-d_3^2
\end{aligned}$$

This system can be written as

$$\begin{pmatrix} a_1 & a_2 & a_3 & 1\\ b_1 & b_2 & b_3 & 1\\ c_1 & c_2 & c_3 & 1\\ d_1 & d_2 & d_3 & 1\end{pmatrix}\begin{pmatrix} e_1'\\ e_2'\\ e_3'\\ r'\end{pmatrix} = \begin{pmatrix} -a_1^2-a_2^2-a_3^2\\ -b_1^2-b_2^2-b_3^2\\ -c_1^2-c_2^2-c_3^2\\ -d_1^2-d_2^2-d_3^2\end{pmatrix} \tag{5.1}$$

Since $\mathbf{p}_i$'s are non-coplannar points, the determinant of the matrix on the left hand side of (5.1) is not equal to 0. Therefore, the system 5.1 has an unique solution. In short, there is a unique sphere passing through any four given non-coplanar points. □

Proof of Theorem 1.13. Since $|\mathcal{P}| \geq 8q^2$, by the pigeon-hole principle, there exist two parallel planes U and V satisfying $|U \cap \mathcal{P}| \geq 5q$ and $|V \cap \mathcal{P}| \geq 8q$. Let γ be the direction which is orthogonal to U and V. We set $E_1 := U \cap \mathcal{P}$ and $E_2 := V \cap \mathcal{P}$. It follows from Theorem 1.11 that there are at least $4q^3/9$ distinct circles in U determined by E_1. We denote the set of centers of these circles by F_1.

Let f be the projection from U to V in the direction γ, and $F_2 := f(F_1)$. Then we have $|F_1| = |F_2| \geq 4q^2/9$. It follows from Corollary 1.10 that there exists a set $F_2' \subseteq F_2$ such that, for each point $\mathbf{p} \in F_2'$, we have $|\Delta_{\mathbb{F}_q}(F_2, \mathbf{p})| \geq q/2$. Thus, for each point $\mathbf{p} \in F_2'$, there exist at least $q/2$ circles centered at $\mathbf{p}$ of radii in $\Delta_{\mathbb{F}_q}(F_2, \mathbf{p})$. We denote the set of these circles by $C_{\mathbf{p}}$.

We note that $|F_2 \setminus F_2'| = o(q^2)$, so the number of circles in U with centers in $F_1 \setminus f^{-1}(F_2')$ is $o(q^3)$. Therefore, the number of circles in U with centers in $f^{-1}(F_2')$ is at least $2q^3/9$.

On the other hand, for each point $\mathbf{p} \in F_2'$, the spheres determined by a circle center at $f^{-1}(\mathbf{p}) \in U$ and circles in $C_{\mathbf{p}}$ are distinct. Let $S_{\mathbf{p}}$ denote the set of the spheres associating $\mathbf{p} \in F_2'$. Then $S_{\mathbf{p}} \cap S_{\mathbf{q}} = \emptyset$ for any two points $\mathbf{p}$ and $\mathbf{q}$ in F_2'. Hence, the number of distinct spheres determined by $\mathcal{P}$ is at least $q^4/9$, and the theorem follows. □

Proof of Theorem 1.14. It follows from Theorem 1.13 that if $|\mathcal{P}| \geq 8q^2$, then the number of spheres determined by $\mathcal{P}$ is at least $q^4/9$. Since the cardinality of the set of centers of these spheres is at most q^3, the number of distinct radii of spheres determined by $\mathcal{P}$ is at least $q/9$, and the theorem follows. □

6 Distinct distances between points and lines

To prove results on the number of distinct distances between points and lines, we construct the *point-line distance bipartite graph* as follows.

6.1 Point-line distance bipartite graph

Let $SQ := \{x^2 \colon x \in \mathbb{F}_q\} \setminus \{0\}$. We define the point-line distance bipartite graph $PL(\mathbb{F}_q^2) = (A \cup B, E)$ as follows. The first vertex part, A, is the set of all quadruples $(a, b, c, \lambda) \in \mathbb{F}_q^4$ satisfying $(a^2+b^2)\lambda \in SQ$. The second vertex part, B, is the set of all points in $\mathbb{F}_q^2$. There is an edge between (a, b, c, λ) and (x, y) if and only if $(ax+by+c)^2 = \lambda(a^2+b^2)$. We have the following properties of the point-line distance bipartite graph $PL(\mathbb{F}_q^2)$.

Lemma 6.1. *The degree of each vertex in A is $2q$, and the degree of each vertex in B is $2|S|$, where*

$$S = \left\{(a, b, \lambda) \in \mathbb{F}_q^3 \colon \lambda(a^2 + b^2) \in SQ\right\}.$$

Proof. Let (a, b, c, λ) be a vertex in A. The degree of (a, b, c, λ) is the number of solutions $(x, y) \in \mathbb{F}_q^2$ of the equation

$$(ax + by + c)^2 = \lambda(a^2 + b^2). \tag{6.1}$$

Since $\lambda(a^2+b^2) \in SQ$, there exists $m \in \mathbb{F}_q \backslash \{0\}$ such that $\lambda(a^2+b^2) = m^2$. Since (a, b, c, λ) is fixed, it follows from the equation (6.1) that (x, y) is a solution of either equations of the following system

$$ax + by + c = m,\ ax + by + c = -m.$$

Since $(a^2 + b^2) \neq 0$, we can assume that $a \neq 0$. Therefore, for any choice of y from $\mathbb{F}_q$, x is determined uniquely, so the degree of (a, b, c, λ) is $2q$.

Let (x, y) be a vertex in B. The degree of (x, y) is the number of solutions $(a, b, c, \lambda) \in A$ satisfying the equation (6.1). Note that if there is an edge between (x, y) and (a, b, c, λ), then $\lambda(a^2 + b^2) \in SQ$ (this follows from the definition of A). Thus, for each triple $(a, b, \lambda) \in S$, we assume that $\lambda(a^2 + b^2) = m^2$ for some $m \in \mathbb{F}_q$. It follows from the equation (6.1) that c is a solution of either equations of the following system

$$ax + by + c = m,\ ax + by + c = -m.$$

This implies that, for each triple $(a, b, \lambda) \in S$, there are exactly two values of c such that (a, b, c, λ) is adjacent to (x, y). In short, the degree of each vertex in B is $2|S|$. □

Lemma 6.2. *Let (a, b, c, λ) and (d, e, f, β) be two distinct vertices in A, and N be the number of common neighbors of (a, b, c, λ) and (d, e, f, β). Then we have*

$$N = \begin{cases} q, \text{ if } (d, e) = k(a, b) \text{ and } f \neq kc, \text{ for some } k \in \mathbb{F}_q \backslash \{0\} \\ 0, \text{ if } (d, e, f) = k(a, b, c) \text{ and } \lambda \neq \beta, \text{ for some } k \in \mathbb{F}_q \backslash \{0\} \\ 2q, \text{ if } (d, e, f) = k(a, b, c) \text{ and } \lambda = \beta, \text{ for some } k \in \mathbb{F}_q \backslash \{0\} \\ 4, \text{ otherwise} \end{cases}$$

Proof. The number of common neighbors of (a, b, c, λ) and (d, e, f, β) is the number of solutions $(x, y) \in \mathbb{F}_q^2$ of the following system

$$\begin{array}{rcl} (ax + by + c)^2 & = & \lambda(a^2 + b^2) = m_1^2 \\ (dx + ey + f)^2 & = & \beta(d^2 + e^2) = m_2^2, \end{array} \tag{6.2}$$

for some $m_1, m_2 \in \mathbb{F}_q \setminus \{0\}$. This implies that (x, y) is a solution of one of the following 4 systems formed of the following 2 equations, each system corresponding to a choice of $\pm$.

$$ax + by + c = \pm m_1,\ dx + ey + f = \pm m_2$$

Since $m_1, m_2 \in \mathbb{F}_q \setminus \{0\}$, two such systems do not have a common solution. We have the two following cases:

1. If (a, b) and (d, e) are linearly independent, then each system has unique solution, so the number of common neighbors of (a, b, c, λ) and (d, e, f, β) is 4.

2. If (a, b) and (d, e) are linearly dependent, then we assume that $(d, e) = k(a, b)$ for some $k \in \mathbb{F}_q \backslash \{0\}$. It follows from the system (6.2) that

$$\begin{array}{rcl} k^2(ax + by + c)^2 & = & k^2\lambda(a^2 + b^2) \\ (kax + kby + f)^2 & = & k^2\beta(a^2 + b^2) \end{array}$$

Subtracting the first equation from the second equation, we obtain

$$(f - kc)(2kax + 2kby + f + kc) = (a^2 + b^2)k^2(\lambda - \beta). \tag{6.3}$$

If $f = kc$ and $\lambda = \beta$, then the number of solutions (x, y) of the system (6.2) is $\deg(a, b, c, \lambda)$, which by Lemma 6.1 equals $2q$.

If $f = kc$ and $\lambda \neq \beta$, then the number of solutions (x, y) of the system (6.2) is 0.

If $f \neq kc$, then from equation (6.3) follows that

$$2kax + 2kby + f + kc = (f - kc)^{-1}(a^2 + b^2)k^2(\lambda - \beta). \tag{6.4}$$

Since $a^2 + b^2 \neq 0$, we assume that $a \neq 0$. Therefore, the number of solutions of the equation (6.4) is q, since we can choose y arbitrary, and for each choice of y, x is determined uniquely by the equation (6.4). In other words, in this case, the number of common neighbors of (a, b, c, λ) and (d, e, f, β) is q.

□

In the following two lemmas, we count the number of walks of length three between a vertex (a, b, c, λ) from A and a vertex (z, t) from B. This will be directly related to obtaining the value for the third eigenvalue corresponding to the point-line distance graph. The first lemma treats the case when (a, b, c, λ) and (z, t) are not adjacent, while the second lemma deals with the case when the two vertices are adjacent.

Lemma 6.3. *Given a pair of non-adjacent vertices (a, b, c, λ) and (z, t), let N be the number of walks of length three between them. Then we have*

$$N = \begin{cases} 4\left(2|S| - (q-1)^2\right) + q\left(q-1\right)^2, \text{ if } az + bt + c = 0 \\ 4\left(2|S| - (q-1)^2\right) + q\left((q-1)^2 - (q-1)\right), \text{ otherwise} \end{cases}$$

Proof. We can distinguish two cases:

1. The point (z, t) lies on the line $ax + by + c = 0$.

   (a) First we count the number of neighbors (d, e, f, β) of (z, t) satisfying $(d, e) \neq k(a, b)$ for all $k \in \mathbb{F}_q \backslash \{0\}$. It follows from the definition of S that the number of triples (d, e, β) satisfying $\beta(d^2 + e^2) \in SQ$ and $d^2 + e^2 \neq k^2(a^2 + b^2)$ for all $k \in \mathbb{F}_q \backslash \{0\}$ is $|S| - (q-1)^2/2$. Moreover, with each triple (d, e, β) satisfying $\beta(d^2 + e^2) \in SQ$, there are two solutions of f such that (d, e, f, β) is a neighbor of (z, t). Thus, the number of neighbors (d, e, f, β) of (z, t) satisfying $(d, e) \neq k(a, b)$ for all $k \in \mathbb{F}_q \backslash \{0\}$ is $2|S| - (q-1)^2$.

   (b) We now count the number of neighbors (d, e, f, β) of (z, t) satisfying $(d, e, f) = k(a, b, c)$, for some $k \in \mathbb{F}_q \backslash \{0\}$, and $\lambda \neq \beta$. If (d, e, f, β) is a neighbor of (z, t), then $(dz + et + f)^2 = \beta(d^2 + e^2)$, which implies that $k^2(az + bt + c)^2 = \beta k^2(a^2 + b^2)$. Since (z, t) lies on the line $ax + by + c = 0$, we have $\beta = 0$. Thus there is no neighbor (d, e, f, β) of (z, t) satisfying $(d, e, f) = k(a, b, c)$, and $\lambda \neq \beta$ for some $k \in \mathbb{F}_q \backslash \{0\}$.

(c) Combining two above cases, we obtain that the number of neighbors (d, e, f, β) of (z, t) satisfying $(d, e) = k(a, b)$, $f \neq kc$ for some $k \in \mathbb{F}_q \backslash \{0\}$ is $(q-1)^2$.

Thus, if $az + bt + c = 0$, the number of walks of length three between (z, t) and (a, b, c, λ) is $q\,(q-1)^2 + 4\,(2|S| - (q-1)^2)$, which finishes this case.

2. The point (z, t) does not lie on $ax + by + c = 0$.

   (a) By the same arguments as above, the number of neighbors (d, e, f, β) of (z, t) satisfying $(d, e) \neq k(a, b)$ for all $k \in \mathbb{F}_q \backslash \{0\}$ is $2|S| - (q-1)^2$.

   (b) The number of neighbors (d, e, f, β) of (z, t) satisfying $(d, e, f) = k(a, b, c), k \in \mathbb{F}_q \backslash \{0\}$, and $\lambda \neq \beta$ is $(q-1)$. Indeed, if (d, e, f, β) is a neighbor of (z, t), then $(dz + et + f)^2 = \beta(d^2 + e^2)$, which implies that $k^2(az + bt + c)^2 = \beta k^2(a^2 + b^2)$. Since (z, t) does not lie on the line $ax+by+c = 0$, $\beta = (az+bt+c)^{-2}(a^2+b^2) \neq 0$. It is easy to see that $\beta \neq \lambda$. Since there are $q-1$ choices of k, the number of neighbors (d, e, f, β) of (z, t) satisfying $(d, e, f) = k(a, b, c), k \in \mathbb{F}_q \backslash \{0\}$, and $\lambda \neq \beta$ is $(q-1)$.

   (c) Combining above cases implies that the number of neighbors (d, e, f, β) of (z, t) satisfying $(d, e) = k(a, b)$, $f \neq kc$ for some $k \in \mathbb{F}_q \backslash \{0\}$ is $(q-1)^2 - (q-1)$.

   In other words, if $az + bt + c \neq 0$, then the number of walks of length three between (z, t) and (a, b, c, λ) is $q\,((q-1)^2 - (q-1)) + 4\,(2|S| - (q-1)^2)$.

□

Lemma 6.4. *Given a pair of adjacent vertices (a, b, c, λ) and (z, t), the the number of walks of length three between them is* $4\,(2|S| - (q-1)^2) + 2q(q-1) + q\,((q-1)^2 - (q-1))$.

Proof. We now consider the following cases:

1. As in the proof of Lemma 6.3, we obtain that the number of neighbors (d, e, f, β) of (z, t) satisfying $(d, e) \neq k(a, b)$ for all $k \in \mathbb{F}_q \backslash \{0\}$ is $2|S| - (q-1)^2$.

2. The number of neighbors (d, e, f, β) of (z, t) satisfying $(d, e, f) = k(a, b, c)$ and $\lambda = \beta$ (for some $k \in \mathbb{F}_q \backslash \{0\}$) is $(q-1)$, since (a, b, c, λ) is a neighbor of (z, t).

3. The number of neighbors (d, e, f, β) of (z, t) satisfying $(d, e, f) = k(a, b, c)$, and $\lambda \neq \beta$, for some $k \in \mathbb{F}_q \backslash \{0\}$ is 0 since (a, b, c, λ) is a neighbor of (z, t).

4. Combining above cases implies that the number of neighbors (d, e, f, β) of (z, t) satisfying $(d, e) = k(a, b)$, $f \neq kc$ for some $k \in \mathbb{F}_q \backslash \{0\}$ is $(q-1)^2 - (q-1)$.

In other words, this gives that the number of walks of length three from (a, b, c, λ) to (z, t) is $q((q-1)^2 - (q-1)) + 2q(q-1) + 4\,(2|S| - (q-1)^2)$, which completes the proof. □

Theorem 6.5. *The absolute value of the third eigenvalue of the point-line distance graph $PL(\mathbb{F}_q^2)$ is at most $2q^{4/3}$.*

Proof. Let M be the adjacency matrix of $PL(\mathbb{F}_q^2)$, which has the form

$$M = \begin{bmatrix} 0 & N \\ N^T & 0 \end{bmatrix},$$

where N is a $|A| \times |B|$ matrix, and $N_{(a,b,c,\lambda),(x,y)} = 1$ if there is an edge between $(a,b,c,\lambda) \in A$ and (x,y) in B, and zero otherwise. Therefore,

$$M^3 = \begin{bmatrix} 0 & NN^TN \\ N^TNN^T & 0 \end{bmatrix}.$$

Let J be the $|A| \times |B|$ all-one matrix. We set

$$K = \begin{bmatrix} 0 & J \\ J^T & 0 \end{bmatrix}.$$

It follows from Lemma 6.3 and Lemma 6.4 that

$$M^3 = \left(4\left(2|S| - (q-1)^2\right) + q((q-1)^2 - (q-1))\right)K + 2q(q-1)M + q(q-1)A_{\mathcal{IN}}, \quad (6.5)$$

where $A_{\mathcal{IN}}$ is the adjacency matrix of the bipartite graph $\mathcal{IN} = (A \cup B, E_{\mathcal{IN}})$ defined as follows: there is an edge between $(z,t) \in B$ and $(a,b,c,\lambda) \in A$ if and only if (z,t) lies on the line $ax + by + c = 0$. It is easy to check that in the graph $\mathcal{IN}$, the degree of each vertex (z,t) is $|S|$, and the degree of each vertex (a,b,c,λ) is q. Thus, the largest eigenvalue of $\mathcal{IN}$ is bounded from above by $\sqrt{q|S|}$.

Let $\mathbf{v_3}$ be an eigenvector corresponding to the third eigenvalue of the point-line distance graph $PL(\mathbb{F}_q^2)$. Then it follows from the equation (6.5) that

$$(\lambda_3^3 - 2q(q-1)\lambda_3)\mathbf{v_3} = q(q-1)A_{\mathcal{IN}}\mathbf{v_3},$$

since $K\mathbf{v_3} = 0$. This implies that $\mathbf{v_3}$ is an eigenvector of the matrix $q(q-1)A_{\mathcal{IN}}$, with the corresponding eigenvalue

$$\lambda_3^3 - 2q(q-1)\lambda_3 \leq q(q-1)\sqrt{q|S|}.$$

Note that if -1 is not a square in $\mathbb{F}_q$, then $|S| = (q-1)^2(q+1)/2$, and if -1 is a square in $\mathbb{F}_q$, then $|S| = (q-1)(q^2-2q+1)/2$. Thus, in both cases, we have $|S| \leq q^3$. This implies that

$$\lambda_3^3 - 2q(q-1)\lambda_3 \leq q^4,$$

Let $f(x) = x^3 - 2q(q-1)x - q^4 = 0$, so $f'(x) = 3x^2 - 2q(q-1)$. Thus, $f'(x) \geq 0$ if $x \geq \sqrt{2q(q-1)/3}$. On the other hand, if $x = 2q^{4/3}$, then $f(x) > 0$, which implies that $f(x) \leq 0$ if $x < 2q^{4/3}$. Therefore, $\lambda_3 \leq 2q^{4/3}$, which concludes the proof of the theorem. □

6.2 Proofs of Theorem 1.18 and Corollary 1.19

In order to prove Theorem 1.18, we need the following result, proved in [33], which is also a corollary of Theorem 1.3.

Theorem 6.6 (**Vinh**, [33])**.** *Let $\mathcal{P}$ be a set of points and $\mathcal{L}$ a set of lines. Then*

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

where $I(\mathcal{P},\mathcal{L})$ represents the number of incidences between points in $\mathcal{P}$ and lines in $\mathcal{L}$.

Proof of Theorem 1.18. First we prove that

$$\frac{1}{|\mathcal{L}|}\sum_{l\in\mathcal{L}}|\Delta_{\mathbb{F}_q}(l,\mathcal{P})| > (1-c^2)q.$$

For each $l \in \mathcal{L}$, let denote the set of non-zero distances between l and $\mathcal{P}$ by $\Delta_{\mathbb{F}_q}(l,\mathcal{P})$. For each line $l = \{ax + by + c = 0\}$, we define

$$D_l := \{(a,b,c,\lambda)\colon \lambda \in \Delta_{\mathbb{F}_q}(l,\mathcal{P})\}.$$

Let $D = \cup_{l\in\mathcal{L}} D_l$. Since $\mathcal{L}$ is a set of lines in $\mathbb{F}_q^2$, D becomes a set of points in $\mathbb{F}_q^4$. Therefore, $|D_l| = |\Delta_{\mathbb{F}_q}(l,\mathcal{P})|$, and $|D| = \sum_{l\in\mathcal{L}}|\Delta_{\mathbb{F}_q}(l,\mathcal{P})|$. One can observe that each point (a,b,c,λ) in D satisfies the condition $\lambda(a^2+b^2) \in SQ$. It follows from the definition of D and Theorem 6.6 that

$$e(D,\mathcal{P}) = |\mathcal{P}||\mathcal{L}| - I(\mathcal{P},\mathcal{L}) \geq \frac{|\mathcal{P}||\mathcal{L}|}{2}, \tag{6.6}$$

where $e(D,\mathcal{P})$ is the number of edges between D and $\mathcal{P}$ in the point-line graph. On the other hand, we now prove that

$$e(D,\mathcal{P}) \leq 2(1-c^2)|\mathcal{P}||\mathcal{L}| + q^{4/3}\sqrt{(1-c^2)|\mathcal{P}||\mathcal{L}|}.$$

Let $U = \{(ka,kb,kc,\lambda)\colon k \in \mathbb{F}_q\backslash\{0\}, (a,b,c,\lambda) \in D\}$. Since the lines in $\mathcal{L}$ are distinct, no two points from U coincide, so $|U| = (q-1)|D|$. If there is an edge between a point $p \in \mathcal{P}$ and a point (a,b,c,λ) in D, then there is also an edge between p and each point $(ka,kb,kc,\lambda) \in U$ where $k \in \mathbb{F}_q\backslash\{0\}$. Therefore, $e(U,\mathcal{P}) = (q-1)e(D,\mathcal{P})$. On the other hand, it follows from Lemma 2.2 and Lemma 6.5 that

$$\begin{aligned} e(U,\mathcal{P}) \leq \frac{2|U||\mathcal{P}|}{q} + 2q^{4/3}\sqrt{|U||\mathcal{P}|} &= \frac{2|\mathcal{P}|(q-1)\sum_{l\in\mathcal{L}}|\Delta_{\mathbb{F}_q}(l,\mathcal{P})|}{q} \\ &+ 2q^{4/3}\sqrt{|\mathcal{P}|(q-1)\sum_{l\in\mathcal{L}}|\Delta_{\mathbb{F}_q}(l,\mathcal{P})|}. \end{aligned}$$

If $\sum_{l\in\mathcal{L}}|\Delta_{\mathbb{F}_q}(l,\mathcal{P})|<(1-c^2)q|\mathcal{L}|$ with $2(1-c^2)<1/2$, then we obtain

$$\begin{aligned} e(U,\mathcal{P}) &\leq \frac{2|\mathcal{P}|(q-1)\sum_{l\in\mathcal{L}}|\Delta_{\mathbb{F}_q}(l,\mathcal{P})|}{q}+2q^{4/3}\sqrt{|\mathcal{P}|(q-1)\sum_{l\in\mathcal{L}}|\Delta_{\mathbb{F}_q}(l,\mathcal{P})|} \\ &< 2(1-c^2)|\mathcal{P}|(q-1)|\mathcal{L}|+2q^{4/3+1}\sqrt{(1-c^2)|\mathcal{P}||\mathcal{L}|}. \end{aligned} \tag{6.7}$$

Since $e(U,\mathcal{P})=(q-1)e(D,\mathcal{P})$, we obtain

$$e(D,\mathcal{P})\leq 2(1-c^2)|\mathcal{P}||\mathcal{L}|+2q^{4/3}\sqrt{(1-c^2)|\mathcal{P}||\mathcal{L}|}. \tag{6.8}$$

Combining the equation (6.6) and the equation (6.8), we obtain

$$\left(1/2-2(1-c^2)\right)|\mathcal{P}||\mathcal{L}|\leq 2\sqrt{1-c^2}q^{4/3}\sqrt{|\mathcal{P}||\mathcal{L}|},$$

which implies that

$$|\mathcal{P}||\mathcal{L}|\leq\frac{4(1-c^2)}{(1/2-2(1-c^2))^2}q^{8/3},$$

which contradicts the assumption in the hypothesis. In other words, we have that

$$\frac{1}{|\mathcal{L}|}\sum_{l\in\mathcal{L}}|\Delta_{\mathbb{F}_q}(l,\mathcal{P})|>(1-c^2)q. \tag{6.9}$$

Let $\mathcal{L}':=\{l\in\mathcal{L}:|\Delta_{\mathbb{F}_q}(\mathcal{P},l)|>(1-c)q\}$. Suppose that $|\mathcal{L}'|<(1-c)|\mathcal{L}|$, so

$$\sum_{l\in\mathcal{L}\setminus\mathcal{L}'}|\Delta_{\mathbb{F}_q}(\mathcal{P},l)|\leq(|\mathcal{L}|-|\mathcal{L}'|)(1-c)q, \text{ and} \tag{6.10}$$

$$\sum_{l\in\mathcal{L}'}|\Delta_{\mathbb{F}_q}(\mathcal{P},l)|\leq q|\mathcal{L}'|. \tag{6.11}$$

Putting (6.10) and (6.11) together, we obtain

$$\sum_{l\in\mathcal{L}}|\Delta_{\mathbb{F}_q}(\mathcal{P},l)|\leq(1-c)q|\mathcal{L}|+cq|\mathcal{L}'|<(1-c)q|\mathcal{L}|+cq(1-c)|\mathcal{L}|=(1-c^2)q|\mathcal{L}|,$$

which contradicts (6.9). Therefore, there exists a subset $\mathcal{L}'$ of $\mathcal{L}$ such that $|\mathcal{L}'|=(1-o(1))|\mathcal{L}|$, and $|\Delta_{\mathbb{F}_q}(\mathcal{P},l)|\gtrsim q$, for each $l\in\mathcal{L}'$, which completes the proof. □

In order to prove Corollary 1.19, we need the following result, which as already mentioned in the introduction, is a variant of Beck's theorem over finite fields.

Theorem 6.7. *([23, Corollary 5]) Let $\mathcal{P}$ be a set of points in $\mathbb{F}_q^2$. If $|\mathcal{P}|\geq 3q$, then the number of distinct lines determined by $\mathcal{P}$ is at least $q^2/3$.*

Proof of Corollary 1.19. One can check that the number of degenerate lines is at most $2q$. Therefore, the proof of Corollary 1.19 follows immediately from Theorem 1.18 and Theorem 6.7. □

References

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

[2] 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**(6) (2014): 689-706.

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

[4] J. Cilleruelo, *Combinatorial problems in finite fields and Sidon sets*, Combinatorica, **32**(5), 497-511.

[5] J. Cilleruelo, A. Iosevich, B. Lund, O. Roche-Newton, M. Rudnev, *Elementary methods for incidence problems in finite fields*, arXiv:1407.2397 (2014).

[6] J. Chapman, M. B. Erdogan, D. Hart, A. Iosevich, and D. Koh, *Pinned distance sets, k-simplices, Wolffs exponent in finite fields and sum-product estimates*, Mathematische Zeitschrift **271** (1)(2012): 63–93.

[7] A. Eustis, Hypergraph Independence Numbers, PHD thesis, University of California San Diego, 2013.

[8] K. Falconer, *On the Hausdorff dimensions of distance sets*, Mathematika **32**(1986), 206–212.

[9] C. Grosu, $\mathbb{F}_q$ *is locally like* $\mathbb{C}$, Journal of the London Mathematical Society **89**(3) (2014):724-744.

[10] D. Hart, A. Iosevich, D. Koh, S. Senger, and I. Uriarte-Tuero, *Distance graphs in vector spaces over finite fields, coloring, pseudo-randomness and arithmetic progressions*, preprint 2008, arXiv:0804.3036.

[11] D. Hart, A. Iosevich, D. Koh, and M. Rudnev, *Averages over hyperplanes, sum-product theory in vector spaces over finite fields and the Erdős-Falconer distance conjecture*, Trans. Amer. Math. Soc., **363** (2011), 3255–3275.

[12] D. Hart and A. Iosevich, *Ubiquity of simplices in vector spaces over finite fields*, Anal. Math. **34**(1) (2008).

[13] F. Hennecart, N. Hegyvári, *Explicit constructions of extractors and expanders*, Acta Arith. **140**(2009) 233–249.

[14] F. Hennecart, N. Hegyvári,*A note on Freiman models in Heisenberg groups*, Israel Journal of Mathematics, **189**(1), 397–411.

[15] Hegyvári, Norbert, F. Hennecart, *A structure result for bricks in Heisenberg groups*, Journal of Number Theory, **133**(9) (2013), 2999–3006.

[16] H. Helfgott and M. Rudnev, *An explicit incidence theorem in F_p*, Mathematika **57**(1) (2011), 135–145.

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

[18] A. Iosevich, I. Shparlinski, M. Xiong, *Sets with integral distances in finite fields*, Transactions of the American Mathematical Society, **362**(4) (2010), 2189–2204.

[19] A. Iosevich, M. Rudnev, Y. Zhai, *Areas of triangles and Becks theorem in planes over finite fields*. Combinatorica, 1-14.(2012)

[20] T. G. F. Jones, *Further improvements to incidence and Beck-type bounds over prime finite fields*, arXiv:1206.4517, (2012)

[21] J. Kollár, *Szemerédi–Trotter-type theorems in dimension* 3, Advances in Mathematics **271** (2015): 30–61.

[22] M. Krivelevich and B. Sudakov, *Pseudo-random graphs*, in More Sets, Graphs and Numbers, Bolyai Soc. Math. Studies 15, Springer, 2006, 199–262.

[23] B. Lund and S. Saraf, *Incidence bounds for block designs*, arXiv:1407.7513, (2014).

[24] R. Lidl and H. Niederreiter, Finite fields, *Cambridge University Press*, (1993).

[25] J. Pach, and M. Sharir, *On the number of incidences between points and curves*, Combinatorics, Probability and Computing, **7**(01) (1998): 121–127.

[26] N.D. Phuong, P.V. Thang, L.A. Vinh, *Incidences between points and generalized spheres over finite fields and related problems*, arXiv:1410.7899 (2014).

[27] N. M. Sang, T. Pham, G. Tardos, *Right angles in vector spaces*, forthcoming, 2016.

[28] J. Solymosi, *Incidences and the Spectra of Graphs*, Building Bridges between Mathematics and Computer Science, Vol. **19.** Ed. Martin Groetschel and Gyula Katona. Series: Bolyai Society Mathematical Studies. Springer, 2008. 499 – 513.

[29] M. Sharir, S. Smorodinsky, C. Valculescu, and F. de Zeeuw, *Distinct distances between points and lines*, arXiv:1512.09006.

[30] E. Szemerédi, W. Trotter, *Extremal problems in discrete geometry*, Combinatorica, **3**.3-4 (1983): 381–392.

[31] C. D. Tóth, *The Szemerédi–Trotter theorem in the complex plane*. Combinatorica, **35**(1), 95-126.

[32] P.V. Thang, L.A. Vinh, *Erdös-Rényi graph, Szemerédi-Trotter type theorem, and sum-product estimates over finite rings*, Forum Mathematicum, **27**(1) (2015), 331–342.

[33] L.A. Vinh, *A Szemerédi-Trotter type theorem and sum-product estimate over finite fields*, Eur. J. Comb. **32**(8) (2011), 1177–1181.

[34] L. A. Vinh, *On point-line incidences in vector spaces over finite fields*, Discrete applied mathematics **177**(2014): 146–151.

[35] L. A. Vinh, *The solvability of norm, bilinear and quadratic equations over finite fields via spectra of graphs*, Forum Mathematicum, **26** (1) (2014), 141–175.

[36] L. A. Vinh, *Graphs generated by Sidon sets and algebraic equations over finite fields*, Journal of Combinatorial Theory Series B, **103**(6) (2013), 651–657.