ÖAW AUSTRIAN ACADEMY OF SCIENCES

RICAM – JOHANN RADON INSTITUTE FOR COMPUTATIONAL AND APPLIED MATHEMATICS

A Point-Conic Incidence Bound and Applications over $\mathbb{F}_p$

A. Mohammadi, T. Pham, A. Warren

RICAM-Report 2022-18

A Point-Conic Incidence Bound and Applications over $\mathbb{F}_p$

Ali Mohammadi * Thang Pham † Audie Warren ‡

Abstract

In this paper, we prove the first incidence bound for points and conics over prime fields. As applications, we prove new results on expansion of bivariate polynomial images and on certain variations of distinct distances problems. These include new lower bounds on the number of pinned algebraic distances as well as improvements of results of Koh and Sun (2014) and Shparlinski (2006) on the size of the distance set formed by two large subsets of finite dimensional vector spaces over finite fields. We also prove a variant of Beck's theorem for conics.

1 Introduction

For an arbitrary field $\mathbb{F}$ and sets of points $\mathcal{P}$ and algebraic curves $\mathcal{C}$ in $\mathbb{F}^d$, we denote the number of incidences between $\mathcal{P}$ and $\mathcal{C}$ by $I(\mathcal{P},\mathcal{C}) := |\{(\boldsymbol{p}, C) \in \mathcal{P} \times \mathcal{C} : \boldsymbol{p} \in C\}|$. The celebrated Szemerédi–Trotter theorem [26] states that for finite sets of points $\mathcal{P}$ and lines $\mathcal{L}$ over $\mathbb{R}^2$, one has

$$I(\mathcal{P},\mathcal{L}) \ll |\mathcal{P}|^{\frac{2}{3}}|\mathcal{L}|^{\frac{2}{3}} + |\mathcal{P}| + |\mathcal{L}|. \tag{1.1}$$

It is well-known that this bound is sharp up to a constant factor. Many applications of this result can be found in [8, 28], and references therein.

Let $\mathbb{F}_q$ denote a finite field of order q and characteristic p. A finite field analogue of the Szemerédi–Trotter theorem was first studied by Bourgain, Katz and Tao [5] in 2004. They proved that for any point set $\mathcal{P}$ and any line set $\mathcal{L}$ in $\mathbb{F}_p^2$ with $|\mathcal{P}| = |\mathcal{L}| = N = p^\alpha$, $0 < \alpha < 2$, we have

$$I(\mathcal{P},\mathcal{L}) \ll N^{\frac{3}{2}-\varepsilon}, \text{ where } \varepsilon = \varepsilon(\alpha) > 0. \tag{1.2}$$

The study of this type of incidence structure is not only interesting from a geometric perspective, but is also largely motivated by a wide range of applications in different areas, such as arithmetic combinatorics, number theory, restriction theory, and theoretical computer science. Since its appearance nearly two decades ago, only a few quantitative variants of estimate (1.2) have been proved. In particular, when N is large with respect to the order of the field, say $N \geq p$, Vinh [30] showed that

$$\left| I(\mathcal{P},\mathcal{L}) - \frac{|\mathcal{P}||\mathcal{L}|}{p} \right| \leq p^{1/2}\sqrt{|\mathcal{P}||\mathcal{L}|}. \tag{1.3}$$

This was proved using techniques from graph theory. A very short and elementary proof can

*School of Mathematics, Institute for Research in Fundamental Sciences (IPM), Tehran, Iran. Email: a.mohammadi@ipm.ir

†Department of Mathematics, HUS, Vietnam National University. Email: thangpham.math@vnu.edu.vn

‡Johann Radon Institute for Computational and Applied Mathematics (RICAM), Linz, Austria. Email: audie.warren@oeaw.ac.at

also be found in [17]. This result also holds for the setting of arbitrary finite fields $\mathbb{F}_q$. When $|\mathcal{P}| = |\mathcal{L}| = p^{3/2}$, it follows from (1.3) that $I(\mathcal{P}, \mathcal{L}) \sim N^{4/3}$, which matches the bound of (1.1). On the other hand, it has been indicated in [31] that the lower bound of (1.3) is sharp in the sense that there are sets $\mathcal{P}$ and $\mathcal{L}$ with $|\mathcal{P}||\mathcal{L}| \gg p^3$ and there is no incidence between $\mathcal{P}$ and $\mathcal{L}$. When N is extremely small, say, $N \ll \log_2 \log_6 \log_{18} p$, Grosu [9] proved that the point-line incidence structure in $\mathbb{F}_p^2$ is almost the same as that in $\mathbb{C}^2$. As a consequence, relying on the $\mathbb{C}^2$ analogue of estimate (1.1) due to Tóth [29], he obtained $I(\mathcal{P}, \mathcal{L}) \ll N^{4/3}$. Therefore, we are left with the situation that $\log_2 \log_6 \log_{18} p \ll N \ll p^{3/2}$.

In the case $|\mathcal{P}| = |\mathcal{L}| = N \leq p$, Helfgott and Rudnev [10] proved that $I(\mathcal{P}, \mathcal{L}) \ll N^{\frac{3}{2} - \frac{1}{10678}}$. Jones [13] showed that the saving of $\frac{1}{10678}$ can be improved to $\frac{1}{662}$. Both results in [10, 13] were proved by using sum-product type energy inequalities in the field $\mathbb{F}_p$. The best current result is due to Stevens and de Zeeuw [25], who proved that for any set $\mathcal{P}$ of m points in $\mathbb{F}_p^2$ and any set $\mathcal{L}$ of n lines in $\mathbb{F}_p^2$, if $m^{7/8} < n < m^{8/7}$ and $m^{-2}n^{13} \ll p^{15}$, then the number of incidences between $\mathcal{P}$ and $\mathcal{L}$ satisfies $I(\mathcal{P}, \mathcal{L}) \ll m^{11/15}n^{11/15}$. Their proof relies mainly on Rudnev's point-plane incidence bound [21]. We point out that this theorem also holds in the setting of arbitrary fields $\mathbb{F}$. In this case, the condition $m^{-2}n^{13} \ll p^{15}$ is replaced by $m^{-2}n^{13} \ll \texttt{char}(\mathbb{F})^{15}$, and is removed if the characteristic of $\mathbb{F}$ is zero.

In a very recent paper, Rudnev and Wheeler [22] obtained point-hyperbola incidence bounds, that is, incidences between points and hyperbolas of the form $(x-a)(y-b) = 1$ in $\mathbb{F}_p^2$, which improve earlier results due to Shkredov in [23] and Bourgain in [4]. The main idea in their argument is as follows: for a fixed point $\mathbf{q} \in \mathcal{P}$, let $H_{\mathbf{q}}$ be the set of hyperbolas passing through $\mathbf{q}$. They observed that the number of k-rich hyperbolas in $H_{\mathbf{q}}$ can be estimated by using the Stevens–de Zeeuw point-line incidence bound. This observation has been used by Warren and Wheeler [32] to derive an incidence bound between a point set and a set of Möbius transformations in the plane $\mathbb{F}_p^2$.

The main purpose of this paper is to employ this key idea to study a general incidence problem, namely, incidences between points and irreducible conics in the plane $\mathbb{F}_p^2$. We recall that the three types of irreducible conics include parabolas, ellipses and hyperbolas. We also remark that the results in Sections 1.1 and 1.2 can be extended to arbitrary fields, as long as the relevant characteristic condition is satisfied - this is because each of these results relies on the point line incidence bounds of Stevens and de Zeeuw, which hold over arbitrary fields. The results of Warren and Wheeler also rely on these results, and can therefore also be extended to arbitrary fields.

In Section 6, we give various applications of our incidence results. For instance, we prove a pinned algebraic distances result, and an analogue of Beck's theorem for conics in finite fields.

1.1 Point-conic incidence bounds over prime fields

Our first result gives an upper bound on the number of incidences between small sets of points and irreducible conics over $\mathbb{F}_p^2$.

Theorem 1.1. *For any set $\mathcal{C}$ of irreducible conics in $\mathbb{F}_p^2$, and any set of points $\mathcal{P} \subseteq \mathbb{F}_p^2$ with $|\mathcal{P}| \ll p^{15/13}$, we have*

$$I(\mathcal{P}, \mathcal{C}) \ll |\mathcal{P}|^{23/27}|\mathcal{C}|^{23/27} + |\mathcal{P}|^{13/9}|\mathcal{C}|^{12/27} + |\mathcal{C}|.$$

To compare with the Cauchy-Schwarz bounds, we note that any conic is determined uniquely by five points, no three of which are collinear, (see [1, Exercise 69]) and by Bézout's theorem, any two distinct conics meet in at most four distinct points. So by the Kővári–Sós–Turán theorem (see [3,

Theorem IV.10]), we have

$$I(\mathcal{P},\mathcal{C}) \ll \min\{|\mathcal{P}||\mathcal{C}|^{4/5} + |\mathcal{C}|, |\mathcal{P}|^{1/2}|\mathcal{C}| + |\mathcal{P}|\}. \tag{1.4}$$

Theorem 1.1 improves the trivial bounds of (1.4), in the range $|\mathcal{P}|^{19/8} \leq |\mathcal{C}| \leq |\mathcal{P}|^{20/7}$, which encompasses the 'balanced Cartesian product' range - that is, when the set of conics $\mathcal{C}$ have coefficients (a, b, c, d, e) coming from a Cartesian product $A \times B \times C \times D \times E$, and the point set $\mathcal{P}$ is also a Cartesian product $F \times G$, and all the sets involved are of the same size N. In this case we have $|\mathcal{C}| = N^5 = |\mathcal{P}|^{5/2}$, and our bound improves on (1.4).

Next, we give an improvement of Theorem 1.1 for the particular case when our point set is a Cartesian product.

Theorem 1.2. *Let $\mathcal{C}$ be a set of irreducible conics in $\mathbb{F}_p^2$. Given any sets $A, B \subset \mathbb{F}_p$ with $|A| \leq |B|$ and $|A||\mathcal{C}| \ll p^2$, we have*

$$I(A \times B,\mathcal{C}) \ll |A|^{\frac{3}{4}}|B|^{\frac{5}{8}}|\mathcal{C}|^{\frac{7}{8}} + |A|^{\frac{1}{2}}|B|^{\frac{3}{4}}|\mathcal{C}|^{\frac{1}{4}} + |\mathcal{C}|.$$

In order to compare these results to what is known over the real numbers, the best analogue is given by the Pach-Sharir theorem [20], which implies that the number of incidences between a point set $\mathcal{P}$ and an arbitrary set of conics $\mathcal{C}$ satisfies

$$I(\mathcal{P},\mathcal{C}) \ll |\mathcal{P}|^{5/9}|\mathcal{C}|^{8/9} + |\mathcal{P}| + |\mathcal{C}|.$$

We refer the reader to [27] for a survey of incidence results and their applications over $\mathbb{R}^d$.

1.2 Point-circle, point-parabola and point-hyperbola incidence bounds over prime fields

When $\mathcal{C}$ is a set of circles, parabolas or hyperbolas, we have the following improvements.

Theorem 1.3. *Let $\mathcal{C}$ be either a set of circles, or of parabolas of the form $y = ax^2 + bx + c$, or of hyperbolas of the form $(x - a)(y - b) = c$ and $\mathcal{P} \subseteq \mathbb{F}_p^2$, with $|\mathcal{P}| \ll p^{15/13}$. If $\mathcal{C}$ is a set of circles suppose that $p \equiv 3 \pmod 4$. Then we have*

$$I(P,\mathcal{C}) \ll |\mathcal{P}|^{15/19}|\mathcal{C}|^{15/19} + |\mathcal{P}|^{23/19}|\mathcal{C}|^{4/19} + |\mathcal{C}|.$$

We remark that any two parabolas or circles meet in at most two points, and that they are determined uniquely by three non-collinear points, as a consequence of the Kővári–Sós–Turán theorem, we have

$$I(\mathcal{P},\mathcal{C}) \ll \min\{|\mathcal{P}||\mathcal{C}|^{2/3} + |\mathcal{C}|, |\mathcal{P}|^{1/2}|\mathcal{C}| + |\mathcal{P}|\}. \tag{1.5}$$

Theorem 1.3 is better than this Cauchy-Schwarz bound in the range $|\mathcal{P}|^{11/8} \ll |\mathcal{C}| \ll |\mathcal{P}|^{12/7}$, again encompassing the balanced Cartesian product range analogous to that described above.

As before, an improved estimate is obtained when $\mathcal{P}$ is a Cartesian product.

Theorem 1.4. *Let $A, B \subset \mathbb{F}_p$, and let $\mathcal{C}$ be either a set of circles, or of parabolas of the form $y = ax^2 + bx + c$, or of hyperbolas of the form $(x - a)(y - b) = c$. If $\mathcal{C}$ is a set of circles, suppose that $p \equiv 3 \pmod 4$. If $|A||\mathcal{C}| \ll p^2$, then we have*

$$I(A \times B,\mathcal{C}) \ll |A|^{4/5}|B|^{3/5}|\mathcal{C}|^{4/5} + |A|^{6/5}|B|^{7/5}|\mathcal{C}|^{1/5} + |\mathcal{C}|.$$

1.3 Incidence bounds over arbitrary finite fields for large sets

Using the same approach, we are able to extend those theorems into arbitrary finite fields for large sets as follows.

Theorem 1.5. *Let $\mathcal{C}$ be a set of irreducible conics in $\mathbb{F}_q^2$ and $\mathcal{P}$ be a set of points in $\mathbb{F}_q^2$. We have*

$$I(\mathcal{P},\mathcal{C}) \ll \frac{|\mathcal{P}||\mathcal{C}|}{q} + q^{1/5}|\mathcal{P}|^{4/5}|\mathcal{C}|^{4/5} + |\mathcal{C}|.$$

Theorem 1.6. *Let $\mathcal{P}$ and $\mathcal{S}$ be sets of points and spheres in $\mathbb{F}_q^d$ respectively and assume $q \equiv 3 \pmod 4$. We have*

$$I(\mathcal{P},\mathcal{S}) \ll \frac{|\mathcal{P}||S|}{q} + q^{\frac{d-1}{3}}|\mathcal{P}|^{2/3}|\mathcal{S}|^{2/3}. \tag{1.6}$$

It is worth noting that Theorem 1.6 improves earlier results in the literature, namely, it is better than the bound

$$\frac{|\mathcal{P}||\mathcal{S}|}{q} + q^{\frac{d}{2}}(|\mathcal{P}||\mathcal{S}|)^{1/2}$$

due to Cilleruelo, Iosevich, Lund, Roche-Newton and Rudnev in [6] when $|\mathcal{P}||\mathcal{S}| \leq q^{d+2}$, and is better than the bound

$$\frac{|\mathcal{P}||\mathcal{S}|}{q} + q^{\frac{d-1}{2}}(|\mathcal{P}||\mathcal{S}|)^{1/2},$$

due to Koh, Lee and Pham [14], which holds for small sets $\mathcal{S}$ with $|\mathcal{P}||\mathcal{S}| \leq q^{d-1}$.

In the range $|\mathcal{P}||\mathcal{S}| \geq q^{d+2}$, Theorem 1.6 implies the same bound as the above-mentioned result of Cilleruelo et al. in [6], which is optimal.

2 Proof of the point-conic bound (Theorem 1.1)

A Möbius transformation (over $\mathbb{F}_q$) is a map f of the form

$$f(x) = \frac{ax+b}{cx+d}, \quad ad - bc \neq 0.$$

We will freely swap between the notion of a Möbius transformation as a map f, and the curve given by $y = f(x)$. We require the following result of [32] on the number of k-rich Möbius transformations, which are defined as

$$T_k := \{f \in T : |f \cap \mathcal{P}| \geq k\},$$

where T is a set of Möbius transformations.

Theorem 2.1. *For any set T of Möbius transformations, and any set of points $\mathcal{P} \subseteq \mathbb{F}_p^2$ with $|\mathcal{P}| \ll p^{15/13}$, for all $k \geq 3$ we have*

$$|T_k| \ll \frac{|\mathcal{P}|^{15/4}}{k^{19/4}} + \frac{|\mathcal{P}|^2}{k^2}.$$

Proof of Theorem 1.1. We shall first aim to bound the number of k-rich conics in $\mathcal{C}$, the set of which we denote by $\mathcal{C}_k$. Fix two distinct points $\boldsymbol{q_1}$ and $\boldsymbol{q_2}$ in $\mathcal{P}$. Define the set

$$\mathcal{C}_{\boldsymbol{q_1},\boldsymbol{q_2},k} := \{C \in \mathcal{C} : \boldsymbol{q_1}, \boldsymbol{q_2} \in C, |C \cap \mathcal{P}| \geq k\}.$$

$\mathcal{C}_{\boldsymbol{q_1},\boldsymbol{q_2},k}$ is a set of conics which all pass through the two points $\boldsymbol{q_1}$ and $\boldsymbol{q_2}$. We apply a projective transformation π, with the property that π maps $\boldsymbol{q_1}$ and $\boldsymbol{q_2}$ as follows

$$\boldsymbol{q_1} \to [0:1:0], \qquad \boldsymbol{q_2} \to [1:0:0].$$

Note that such a transformation always exists. We now analyse the image $\pi(C)$ for each $C \in \mathcal{C}_{\boldsymbol{q_1},\boldsymbol{q_2},k}$.

Since π is a projective transformation, these images must all remain degree two algebraic curves, that is, conics. Furthermore, we know that the two points at infinity $[0:1:0]$ and $[1:0:0]$ both lie on $\pi(C)$. We claim that this in fact forces $\pi(C)$ to be a Möbius transformation. Indeed, letting γ denote an irreducible conic over $\mathbb{F}_p$, we have

$$\gamma \text{ is a Möbius transformation} \quad \iff \quad \{[0:1:0],[1:0:0]\} \subseteq \gamma. \tag{2.1}$$

First, we show the implication $\implies$ of (2.1). If γ is Möbius, then since it corresponds to a conic, it is given by an equation of the form

$$y = \frac{ax+b}{x+c}$$

which we then rearrange to

$$xy + cy - ax - b = 0.$$

Projectivising this curve, we have

$$xy + cyz - axz - bz^2 = 0.$$

Upon setting $z = 0$ to find the points at infinity, we have $xy = 0$, and so one of x, y must be zero. This yields the two points as in (2.1).

We now show the reverse implication. Projectivising an arbitrary conic, of the form

$$ax^2 + by^2 + xy + cy + dx + e = 0,$$

we have

$$ax^2 + by^2 + xy + cyz + dxz + ez^2 = 0.$$

Setting $z = 0$ to find the points at infinity, we have the equation $ax^2 + by^2 + xy = 0$. We know that the points $(0,1)$ and $(1,0)$ must lie on this curve. The first implies that $b = 0$, and the second that $a = 0$. Therefore the original curve γ is of the form

$$xy + cy + dx + e = 0.$$

We also must have $dc \neq e$, as otherwise this conic is reducible as $(y+d)(c+x) = 0$. Therefore, we have shown that γ is the general form of a Möbius transformation, concluding the proof of (2.1).

With (2.1) at hand, we know that the set $\pi(\mathcal{C}_{\boldsymbol{q_1},\boldsymbol{q_2},k})$ is a set of Möbius transformations, and so we can apply Theorem 2.1. Therefore, for each distinct pair $(\boldsymbol{q_1},\boldsymbol{q_2}) \in \mathcal{P}^2$, and for each $k \geq 5$, we have

$$|\mathcal{C}_{\boldsymbol{q_1},\boldsymbol{q_2},k}| \ll \frac{|\mathcal{P}|^{15/4}}{k^{19/4}} + \frac{|\mathcal{P}|^2}{k^2}. \tag{2.2}$$

Note that the condition $k \geq 3$ has changed to $k \geq 5$, since the two points at infinity on these conics are now being ignored. In order to alter this bound into a bound on $\mathcal{C}_k$, we sum over each

distinct pairs of points.

$$|\mathcal{C}_k| \leq \binom{k}{2}^{-1} \sum_{\boldsymbol{q_1},\boldsymbol{q_2}\in\mathcal{P}} |\mathcal{C}_{\boldsymbol{q_1},\boldsymbol{q_2},k}| \ll \frac{1}{k^2} \sum_{\boldsymbol{q_1},\boldsymbol{q_2}\in\mathcal{P}} |\mathcal{C}_{\boldsymbol{q_1},\boldsymbol{q_2},k}|.$$

The binomial factor appears since each k-rich conic is being counted at least $\binom{k}{2}$ times, once for each pair of distinct points on the conic. We then bound this by $\binom{k}{2} \gg k^2$ (this is certainly valid in the range $k \geq 5$). Using (2.2), we have

$$|\mathcal{C}_k| \ll \frac{|\mathcal{P}|^{23/4}}{k^{27/4}} + \frac{|\mathcal{P}|^4}{k^4}. \tag{2.3}$$

We proceed to use this estimate to obtain the required incidence bound. We use $\mathcal{C}_{=k}$ to denote $\{C \in \mathcal{C}\colon |C \cap \mathcal{P}| = k\}$.

$$\begin{aligned}
I(\mathcal{P},\mathcal{C}) &= \sum_{k\geq 1} |\mathcal{C}_{=k}|k \\
&= \sum_{k\leq\Delta} |\mathcal{C}_{=k}|k + \sum_{k>\Delta} |\mathcal{C}_{=k}|k \\
&\ll \Delta|\mathcal{C}| + \sum_{i\geq 0} \sum_{\substack{C\in\mathcal{C} \\ 2^i\Delta\leq|C\cap\mathcal{P}|<2^{i+1}\Delta}} (2^i\Delta) \\
&\ll \Delta|\mathcal{C}| + \sum_{i\geq 0} |\mathcal{C}_{2^i\Delta}|(2^i\Delta) \\
&\ll \Delta|\mathcal{C}| + \sum_{i\geq 0} \left(\frac{|\mathcal{P}|^{23/4}}{(2^i\Delta)^{27/4}} + \frac{|\mathcal{P}|^4}{(2^i\Delta)^4} \right) (2^i\Delta) \\
&\ll \Delta|\mathcal{C}| + \frac{|\mathcal{P}|^{23/4}}{\Delta^{23/4}} + \frac{|P|^4}{\Delta^3}.
\end{aligned}$$

In order to optimise the first two terms, we make the choice

$$\Delta = \max\left\{5, \frac{|\mathcal{P}|^{23/27}}{|\mathcal{C}|^{4/27}}\right\}.$$

This maximum is taken to ensure the application of (2.3) was valid. If the maximum above is 5, then we must have

$$\frac{|\mathcal{P}|^{23/27}}{|\mathcal{C}|^{4/27}} \leq 5 \implies |\mathcal{P}|^{23} \ll |\mathcal{C}|^4.$$

The above bound then becomes

$$I(\mathcal{P},\mathcal{C}) \ll |\mathcal{C}| + |\mathcal{P}|^{23/4} \ll |\mathcal{C}|.$$

If the second term in the maximum is taken, we then have

$$I(\mathcal{P},\mathcal{C}) \ll |\mathcal{P}|^{23/27}|\mathcal{C}|^{23/27} + |\mathcal{P}|^{13/9}|\mathcal{C}|^{12/27}.$$

Summing these two bounds to account for either case then gives the result. □

3 Proof of the point-conic bound for Cartesian product sets (Theorem 1.2)

The proof of Theorem 1.2 is similar to that of Theorem 1.1. First, we recall an incidence result of Stevens and de Zeeuw. The following version appears in [18, Theorem 5]. We state the result, more generally, over the two dimensional projective space over $\mathbb{F}_p$, denoted by $\mathbb{P}_2(\mathbb{F}_p)$.

Theorem 3.1. *Given $A, B \subset \mathbb{F}_p$ with $|A| \leq |B|$, let $\mathcal{P} = \{[a : b : 1] : (a, b) \in A \times B\} \subset \mathbb{P}_2(\mathbb{F}_p)$ and let $\mathcal{L}$ be a set of lines over $\mathbb{P}_2(\mathbb{F}_p)$. Suppose $|A||\mathcal{L}| \ll p^2$. Then*

$$I(\mathcal{P}, \mathcal{L}) \ll |A|^{3/4}|B|^{1/2}|\mathcal{L}|^{3/4} + |\mathcal{L}| + |A||B|.$$

Corollary 3.2. *Let the sets $\mathcal{P}, \mathcal{L}$ be as in Theorem 3.1 and let π be a projective transformation of $\mathbb{P}_2(\mathbb{F}_p)$. Then*

$$I(\pi(\mathcal{P}), \mathcal{L}) \ll |A|^{3/4}|B|^{1/2}|\mathcal{L}|^{3/4} + |\mathcal{L}| + |A||B|.$$

Proof. First note that $I(\pi(\mathcal{P}), \mathcal{L}) = I(\mathcal{P}, \pi^{-1}(\mathcal{L}))$. Then the result follows from Lemma 3.1 noting that $|\mathcal{L}| = |\pi^{-1}(\mathcal{L})|$. □

Corollary 3.3. *For $A, B \subset \mathbb{F}_p$, with $|A| \leq |B|$, let $\mathcal{P} = \{[a : b : 1] : (a, b) \in A \times B\} \subset \mathbb{P}_2(\mathbb{F}_p)$ and let $\mathcal{L}$ denote a set of lines over $\mathbb{P}_2(\mathbb{F}_p)$. Suppose π is a projective transformation and for $k \geq 2$, let $\mathcal{L}_k$ denote the set of k-rich lines of $\mathcal{L}$ with respect to $\pi(P)$. Suppose $|A||\mathcal{L}| \ll p^2$. Then*

$$|\mathcal{L}_k| \ll \frac{|A|^3|B|^2}{k^4} + \frac{|A||B|}{k}.$$

Proof. The result follows from Corollary 3.2, using the observation that $k|\mathcal{L}_k| \ll I(\pi(\mathcal{P}), \mathcal{L}_k)$. □

By following the arguments of [32], one obtains the following result on the number of k-rich Möbius transformations.

Corollary 3.4. *For $A, B \subset \mathbb{F}_p$, with $|A| \leq |B|$, let $\mathcal{P} = A \times B$ and let T denote a set of Möbius transformations. Suppose π is a projective transformation and for $k \geq 3$, let T_k be a the set of k-rich transformations of T, with respect to $\pi(P)$. If $|A||T| \ll p^2$, then*

$$|T_k| \ll \frac{|A|^4|B|^3}{k^5} + \frac{|A|^2|B|^2}{k^2}.$$

Proof of Theorem 1.2. Corollary 3.4 may be used, in a similar manner as in the proof of Theorem 1.1, to bound the number of k-rich conics $\mathcal{C}_k$, for $k \geq 5$. This gives

$$|\mathcal{C}_k| \ll \frac{|A|^6|B|^5}{k^7} + \frac{|A|^4|B|^4}{k^4}.$$

This can then be converted into the required incidence bound in a similar fashion to the proof of Theorem 1.1. □

4 Proof of Theorems 1.3 and 1.4

We begin this section by giving the proof of the circles part of Theorem 1.3, and then explain the alterations necessary to deal with parabolas and hyperbolas.

Proof of Theorem 1.3. Fix a point $\boldsymbol{q} \in \mathcal{P}$. We aim to bound the number of k-rich circles passing through $\boldsymbol{q}$, for $k \geq 3$. After translating the points and circles, we may assume $\boldsymbol{q} = (0,0)$ without altering the incidences. We rename the translated sets of points and circles as $\mathcal{P}$ and $\mathcal{C}$ respectively. A circle of the form

$$(x-c)^2 + (y-d)^2 = r$$

for some c, d, r before this translation, is now of the form

$$C_{a,b}: \quad (x-a)^2 + (y-b)^2 = a^2 + b^2$$

for some $a, b \in \mathbb{F}_p$; this is due to the fact that $(0,0)$ must lie on the translated circle. Let us take a k-rich circle C. Then there exist points (α_1, β_1),...,$(\alpha_{k-1}, \beta_{k-1}) \in \mathcal{P} \setminus \{(0,0)\}$ which all lie on C. Each such point can be associated with a line of the form

$$-2\alpha_i X - 2\beta_i Y + \alpha_i^2 + \beta_i^2 = 0.$$

We show that these lines are not defined with multiplicity. Suppose that the two points (α, β) and (α', β') define the same line. Without loss of generality, we may assume that assume $\beta \neq 0$, since at least one of α or β is non-zero. After rearranging, we come to the equation

$$Y = \frac{-\alpha}{\beta} X + \frac{\alpha^2 + \beta^2}{2\beta}.$$

We must therefore have

$$\frac{\alpha}{\beta} = \frac{\alpha'}{\beta'}, \quad \frac{\alpha^2 + \beta^2}{2\beta} = \frac{\alpha'^2 + \beta'^2}{2\beta'}$$

setting $\lambda := \frac{\alpha}{\beta} = \frac{\alpha'}{\beta'}$, we must have $\alpha = \lambda\beta$ and $\alpha' = \lambda\beta'$. Substituting this into the second equation then gives

$$\beta(\lambda^2 + 1) = \beta'(\lambda^2 + 1).$$

Recalling our assumption $p \equiv 3 \pmod 4$, it follows that -1 is a non-square, and so we conclude that $\beta = \beta'$, which implies $\alpha = \alpha'$, and so we are done.

As we have just seen, the point set $\mathcal{P}$ gives rise to a set of lines $\mathcal{L}$, each of the form above, and $|\mathcal{P}| = |\mathcal{L}|$. Furthermore, a circle $C_{a,b}$ as defined above can be associated with the point (a,b). The set of circles $\mathcal{C}$ therefore gives rise to a set of points $\mathcal{Q} \subseteq \mathbb{F}_p^2$. Finally, the k-rich circle $C_{a,b}$ above, corresponds to a $(k-1)$-rich point $(a,b) \in \mathcal{Q}$, with respect to the set of lines $\mathcal{L}$. We can see these as the lines corresponding to the points (α_i, β_i) all passing the point (a,b). Now, we use the following corollary of the Stevens–de Zeeuw incidence bound [25, Theorem 3] to bound the number of such $(k-1)$-rich points. Note that this corollary is the dual of [32, Corollary 5].

Corollary 4.1. *Let $\mathcal{L}$ be a set of lines over $\mathbb{F}_p^2$, with $|\mathcal{L}| \ll p^{15/13}$, and for $k \geq 2$ let $\mathcal{P}_k$ denote the number of k-rich points with respect to $\mathcal{L}$. Then*

$$|\mathcal{P}_k| \ll \frac{|\mathcal{L}|^{11/4}}{k^{15/4}} + \frac{|\mathcal{L}|}{k}.$$

Corollary 4.1 and the above argument immediately yields the bound

$$|\mathcal{C}_{\boldsymbol{q},k}| \ll \frac{|\mathcal{L}|^{11/4}}{k^{15/4}} + \frac{|\mathcal{L}|}{k} = \frac{|\mathcal{P}|^{11/4}}{k^{15/4}} + \frac{|\mathcal{P}|}{k}$$

where $\mathcal{C}_{\boldsymbol{q},k}$ denotes the set of k-rich circles, for $k \geq 3$, containing $\boldsymbol{q}$. Then summing the contribution over all points of $\mathcal{P}$ and noting that each k-rich circle gets overcounted by at least a factor of $k-1$ in this way, we have

$$|\mathcal{C}_k| \ll \frac{1}{k} \sum_{\boldsymbol{q} \in \mathcal{P}} |\mathcal{C}_{\boldsymbol{q},k}| \ll \frac{|\mathcal{P}|^{15/4}}{k^{19/4}} + \frac{|\mathcal{P}|^2}{k^2}.$$

This can then be used to bound $I(\mathcal{P}, \mathcal{C})$ in a similar manner as in the proofs of Theorem 1.1 or [32, Theorem 2].

For parabolas, a similar argument works. After fixing a point $\boldsymbol{q}$ and translating so that $\boldsymbol{q} = (0,0)$, we find parabolas of the form

$$y = ax^2 + bx.$$

A k-rich parabola then yields a $(k-1)$-rich point (a,b), with respect to the lines given by

$$\beta = X\alpha^2 + Y\alpha$$

which are again defined with no multiplicity, and the rest of the argument follows similarly to above.

Hyperbolas defined by the equation $(x-a)(y-b) = c$, passing through the point $\mathbf{q} = (q_1, q_2)$, can be written as

$$xy - b(x - q_1) - a(y - q_2) = q_1 q_2.$$

By setting $x' = x - q_1$ and $y' = y - q_2$, our hyperbolas are represented by

$$x'y' + x'(q_2 - b) + y'(q_1 - a) = 0.$$

This equation can be viewed as an incidence between the point $(q_2 - b, q_1 - a)$ and the line

$$x' \cdot X + y' \cdot Y = -x'y'.$$

Thus, we are now in the same situation as before for circles, and the same argument works. □

The proof of Theorem 1.4 follows from almost exactly the same argument as that of Theorem 1.3, with the only exception being that the dual form of Theorem 3.1 (using point-line duality) replaces Corollary 4.1 to bound the number of k-rich points corresponding to the k-rich circles of $\mathcal{C}$. This is based on the observation that the line set $\mathcal{L}$, as defined in the proof of Theorem 1.3 (corresponding to the point set $\mathcal{P}$ in the statement of Theorem 1.4), now has a Cartesian product structure.

5 Proofs of incidence bounds for large sets (Theorems 1.5 and 1.6)

To prove Theorem 1.5, we recall the following point-line incidence bound for large sets in [30].

Theorem 5.1. *Let $\mathcal{P}$ be a set of points and $\mathcal{L}$ be a set of lines in $\mathbb{F}_q^2$. Then*

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

Corollary 5.2. *Let $\mathcal{P}$ be a set of points and $\mathcal{L}_k$ be the set of k-rich lines over $\mathbb{F}_q^2$. Suppose that*

$k > |\mathcal{P}|/q$, then we have

$$|\mathcal{L}_k| \leq \frac{q|\mathcal{P}|}{k^2}.$$

Utilising Corollary 5.2 and the arguments of [32, Theorem 2], one obtains the following bound on the number of k-rich Möbius transformations, which is an analogue of Theorem 2.1 for large sets.

Corollary 5.3. *Let $\mathcal{P}$ be a set of points and T a set of Möbius transformations over $\mathbb{F}_q^2$. Let T_k be the set of k-rich transformations in T and suppose that $k > \max\{2, |\mathcal{P}|/q\}$. Then*

$$|T_k| \leq \frac{q|\mathcal{P}|^2}{k^3}.$$

Proof of Theorem 1.5. The proof follows the same approach as in the proof of Theorem 1.1, essentially only replacing Theorem 2.1 by Corollary 5.3 to bound the number of k-rich transformations. In particular, we are able to show that

$$|\mathcal{C}_k| \ll \frac{|\mathcal{P}|^2}{k^2} \cdot \frac{q|\mathcal{P}|^2}{k^3} = \frac{q|\mathcal{P}|^4}{k^5},$$

whenever $k > \max\{4, |\mathcal{P}|/q\}$. Then, writing

$$I(\mathcal{P}, \mathcal{C}) \leq \sum_{k \leq \frac{|\mathcal{P}|}{q}} |\mathcal{C}_{=k}|k + \sum_{k > \max\{4, \frac{|\mathcal{P}|}{q}\}} |\mathcal{C}_{=k}|k + \sum_{k \leq 4} |\mathcal{C}_{=k}|k,$$

we may bound the second sum similarly to the proof of Theorem 1.1, and the first sum trivially, to obtain

$$I(\mathcal{P}, \mathcal{C}) \ll \frac{|\mathcal{P}||\mathcal{C}|}{q} + q^{1/5}|\mathcal{P}|^{4/5}|\mathcal{C}|^{4/5} + |\mathcal{C}|.$$

□

To prove Theorem 1.6, we require the following bound on incidences between large sets of points and hyperplanes due to Vinh [30].

Theorem 5.4. *Let $\mathcal{P}$ be a set of points and $\mathcal{H}$ be a set of hyperplanes in $\mathbb{F}_q^d$. The number of incidences between $\mathcal{P}$ and $\mathcal{H}$ satisfies*

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

Proof of Theorem 1.6. The proof uses the same framework as the proof of Theorem 1.3 and so we skip the overly similar details. We begin by fixing a point $\boldsymbol{q}$ aiming to bound the number of k-rich spheres passing through it. After a translation, we assume $\boldsymbol{q} = \mathbf{0}$ and so each sphere passing through $\boldsymbol{q}$ takes the form

$$S_{\boldsymbol{a}}: \quad (x_1 - a_1)^2 + (x_2 - a_2)^2 + \cdots + (x_d - a_d)^2 = a_1^2 + a_2^2 + \cdots + a_d^2,$$

for some $\boldsymbol{a} = (a_1, a_2, \ldots, a_d) \in \mathbb{F}_q^d$. Let $\boldsymbol{q_1}, \ldots, \boldsymbol{q_{k-1}}$ denote the $k-1$ points on $S_{\boldsymbol{a}}$ other than $\mathbf{0}$ and write $\boldsymbol{q_i} = (\alpha_{(i,1)}, \alpha_{(i,2)}, \ldots, \alpha_{(i,d)})$. For each $1 \leq i \leq k-1$, the point $\boldsymbol{q_i}$ can be associated with the hyperplane

$$-2\alpha_{(i,1)}X_1 - 2\alpha_{(i,2)}X_2 - \cdots - 2\alpha_{(i,d)}X_d + \alpha_{(i,1)}^2 + \alpha_{(i,2)}^2 + \cdots + \alpha_{(i,d)}^2 = 0.$$

Arguing similarly as in the proof of Theorem 1.3, since -1 is a non-square, these hyperplanes are defined without multiplicity.

Now, having established the correspondence between our original sets of points and spheres to new sets of hyperplanes and points respectively, in order to bound the number, $|\mathcal{S}_{\boldsymbol{q},k}|$, of k-rich spheres through $\boldsymbol{q}$, we require a bound on the number, $|\mathcal{P}_k|$, of k-rich points in terms of hyperplanes over $\mathbb{F}_q^d$. To this end, we use Theorem 5.4, to obtain

$$|\mathcal{P}_k| \leq \frac{q^{d-1}|\mathcal{H}|}{k^2}$$

if $k > |\mathcal{H}|/q$. As in the proof of Theorem 1.3, we use the above estimate to bound the number of k-rich spheres, obtaining

$$|\mathcal{S}_k| \leq \frac{q^{d-1}|\mathcal{P}|^2}{k^3}$$

if $k > |\mathcal{P}|/q$. This can then be easily converted into the required incidence bound. □

6 Applications

6.1 Pinned algebraic distances

Our first application is to the pinned algebraic distance problem.

Theorem 6.1. *Let $f(x,y)$ be one of the following polynomials: x^2+y^2 (usual distance function), xy (Minkowski distance function) or $y+x^2$ (parabola distance function). For $\mathcal{E} \subset \mathbb{F}_p^2$ with $|\mathcal{E}| \ll p^{15/13}$ and $p \equiv 3 \pmod 4$, there exists a point $\boldsymbol{p} \in \mathcal{E}$ such that $|f(\boldsymbol{p}-\mathcal{E})| \gg |\mathcal{E}|^{\frac{8}{15}}$, where*

$$f(\boldsymbol{p}-\mathcal{E}) := \{f(\boldsymbol{p}-\boldsymbol{e})\colon \boldsymbol{e} \in \mathcal{E}\}.$$

Remark 6.2. When $f(x,y) = x^2+y^2$, Theorem 6.1 was first proved by Stevens and de Zeeuw in [25] by using a point-line incidence bound. The exponent $\frac{8}{15}$ was improved to $\frac{1}{2}+\frac{149}{4214}$ by Iosevich, Koh, Pham, Shen and Vinh [12], then to $\frac{1}{2}+\frac{3}{74}$ by Lund and Petridis [16] and to $\frac{1}{2}+\frac{69}{1558}$ by Iosevich, Koh and Pham [11]. The best current lower bound is $|\mathcal{E}|^{2/3}$ due to Murphy, Petridis, Pham, Rudnev and Stevens [19]. We also note that it seems very difficult to extend the methods in [12, 16, 11, 19] to the Minkowski and parabola distance functions.

Proof of Theorem 6.1. For $\boldsymbol{p} \in \mathcal{E}$, let $\mathcal{C}_{\boldsymbol{p}}$ be the set of conics defined by the equation $f(\boldsymbol{p}-\boldsymbol{x}) = t$, with $t \in f(\boldsymbol{p}-\mathcal{E}) \setminus \{\boldsymbol{0}\}$. Let $\mathcal{C} = \bigcup_{\boldsymbol{p}\in\mathcal{E}} \mathcal{C}_{\boldsymbol{p}}$. We observe that $I(\mathcal{E},\mathcal{C}) \gg |\mathcal{E}|^2$. On the other hand, applying Theorem 1.3, we have

$$I(\mathcal{E},\mathcal{C}) \ll (|\mathcal{E}||\mathcal{C}|)^{15/19} + |\mathcal{E}|^{23/19}|\mathcal{C}|^{4/19} + |\mathcal{C}|.$$

Putting the lower and upper bounds of $I(\mathcal{E},\mathcal{C})$ together and using the fact that $|\mathcal{C}| \leq \sum_{\boldsymbol{p}\in\mathcal{E}} |f(\boldsymbol{p}-\mathcal{E})|$, the theorem follows. □

We now take advantage of the generality of Theorem 1.1 to study algebraic distances between two sets in $\mathbb{F}_p^3$, where one set lies on a plane and the other set is arbitrary.

More precisely, let $f \in \mathbb{F}_p[x,y,z]$ and $\mathcal{E},\mathcal{F} \subset \mathbb{F}_p^3$, with $\mathcal{E}$ lying on the plane $z=0$. As above, the

set of f-algebraic distances between $\mathcal{E}$ and $\mathcal{F}$ is defined by

$$f(\mathcal{E}-\mathcal{F}) := \{f(\boldsymbol{x}-\boldsymbol{y})\colon \boldsymbol{x}\in\mathcal{E}, \boldsymbol{y}\in\mathcal{F}\}.$$

Theorem 6.3. *Let $\mathcal{E},\mathcal{F}\subset\mathbb{F}_p^3$, with $\mathcal{E}$ lying on the plane $z=0$. Suppose $f\in\mathbb{F}_p[x,y,z]$ satisfies the property that, for each $\boldsymbol{p}\in\mathcal{F}$, the polynomial $f(\boldsymbol{x}-\boldsymbol{p})-t$ is of degree two and irreducible for all $t\in f(\mathcal{E}-\boldsymbol{p})$. We have*

$$|f(\mathcal{E}-\mathcal{F})| \gg \min\left\{|\mathcal{E}|^{4/23}|\mathcal{F}|^{4/23},\ \frac{|\mathcal{F}|^{5/4}}{|\mathcal{E}|},\ \frac{|\mathcal{E}|^{20/7}}{|\mathcal{F}|}, |\mathcal{E}|\right\}.$$

The following is an example of this theorem.

Corollary 6.4. *Let $f(x,y,z)=x^2y^2+z^2$. For a set $\mathcal{E}$ on the plane $z=0$ and a set $\mathcal{F}\subset\mathbb{F}_p^3$ with $|\mathcal{F}|\geq|\mathcal{E}|^{\frac{405}{216}}$ and $p\equiv 3 \pmod 4$, we have*

$$|f(\mathcal{E}-\mathcal{F})| \gg \min\left\{|\mathcal{E}|^{4/23}|\mathcal{F}|^{4/23},\ \frac{|\mathcal{F}|^{5/4}}{|\mathcal{E}|},\ \frac{|\mathcal{E}|^{20/7}}{|\mathcal{F}|}, |\mathcal{E}|\right\}.$$

Remark 6.5. We note that similar questions for some specific polynomials f have been considered in the literature. For instance, the set of distances between a set on a line and an arbitrary set in $\mathbb{F}_p^2$ was studied by Iosevich, Koh, Pham, Shen and Vinh in [12] as the key step in their improvement of Stevens–de Zeeuw's result on the original distance problem in two dimensions.

Proof of Theorem 6.3. If $|f(\mathcal{E}-\mathcal{F})| > \frac{|\mathcal{E}|^{20/7}}{|\mathcal{F}|}$, then we are done. Thus, assuming otherwise, we have $|f(\mathcal{E}-\mathcal{F})|\cdot|\mathcal{F}|\leq|\mathcal{E}|^{20/7}$.

For each $\boldsymbol{p}\in\mathcal{F}$, let $\mathcal{C}_{\boldsymbol{p}}$ be the set of irreducible conics defined by $f(\boldsymbol{x}-\boldsymbol{p})=t$ where $t\in f(\mathcal{E}-\boldsymbol{p})$.

Let $\mathcal{C}=\bigcup_{\boldsymbol{p}}\mathcal{C}_{\boldsymbol{p}}$. We observe that $I(\mathcal{E},\mathcal{C})\gg|\mathcal{E}||\mathcal{F}|$. On the other hand, applying Theorem 1.1 implies

$$|\mathcal{E}||\mathcal{F}| \ll |\mathcal{E}|^{\frac{23}{27}}\left(\sum_{\boldsymbol{p}\in\mathcal{F}}|f(\mathcal{E}-\boldsymbol{p})|\right)^{23/27} + |\mathcal{E}|^{13/9}\left(\sum_{\boldsymbol{p}\in\mathcal{F}}|f(\mathcal{E}-\boldsymbol{p})|\right)^{12/27} + \sum_{\boldsymbol{p}\in\mathcal{F}}|f(\mathcal{E}-\boldsymbol{p})|.$$

Rearranging this inequality gives

$$|f(\mathcal{E}-\mathcal{F})| \gg \min\left\{|\mathcal{E}|^{4/23}|\mathcal{F}|^{4/23},\ \frac{|\mathcal{F}|^{5/4}}{|\mathcal{E}|}, |\mathcal{E}|\right\}.$$

We note that the assumption $|\mathcal{F}|\geq|\mathcal{E}|^{\frac{405}{216}}$ is needed to ensure that $|\mathcal{E}|^{19/8}\leq|\mathcal{C}|\leq|\mathcal{E}|^{20/7}$ and so the bound on $I(\mathcal{E},\mathcal{C})$, given by Theorem 1.1, is better than the trivial bound (1.4). □

6.2 Polynomial images

Theorem 6.6. *Let $f(x,y)$ be either x^2+y^2 (usual distance function) or $y+x^2$ (parabola distance function). In the former case, assume $p\equiv 3 \pmod 4$. For $\mathcal{E},\mathcal{F}\subset\mathbb{F}_p^2$ with $|\mathcal{E}+\mathcal{F}|\ll p^{15/13}$, we*

have

$$|f(\mathcal{E})| \gg \min\left\{\frac{|\mathcal{E}|^{19/15}|\mathcal{F}|^{4/15}}{|\mathcal{E}+\mathcal{F}|},\ \frac{|\mathcal{E}|^{19/4}|\mathcal{F}|^{15/4}}{|\mathcal{E}+\mathcal{F}|^{23/4}}, |\mathcal{E}|\right\}.$$

Proof. We consider the following equation

$$f(\boldsymbol{x}-\boldsymbol{y}) = t,$$

where $\boldsymbol{x} \in \mathcal{E}+\mathcal{F}$, $\boldsymbol{y} \in \mathcal{F}$ and $t \in f(\mathcal{E})$.

Let $\mathcal{C}$ be the set of curves defined by $f(\boldsymbol{x}-\boldsymbol{q}) = t$ with $\boldsymbol{q} \in \mathcal{F}$ and $t \in f(\mathcal{E})$. It is not hard to see that if $f(x,y) = x^2+y^2$ or $f(x,y) = y+x^2$, then the curves in $\mathcal{C}$ are irreducible. Note that

$$|\mathcal{E}||\mathcal{F}| \leq I(\mathcal{E}+\mathcal{F}, \mathcal{C}).$$

Since $|\mathcal{C}| = |\mathcal{F}||f(\mathcal{E})|$, using the incidence bound of Theorem 1.3, one has

$$|\mathcal{E}||\mathcal{F}| \ll |\mathcal{E}+\mathcal{F}|^{15/19}(|\mathcal{F}||f(\mathcal{E})|)^{15/19} + |\mathcal{E}+\mathcal{F}|^{23/19}(|\mathcal{F}||f(\mathcal{E})|)^{4/19} + |\mathcal{F}||f(\mathcal{E})|.$$

Solving this inequality completes the proof. □

Theorem 6.7. *Let $f(x,y) = xy$ (Minkowski distance function). For $\mathcal{E}, \mathcal{F} \subset \mathbb{F}_p^2$ with $|\mathcal{E}+\mathcal{F}| \ll p^{15/13}$. Assuming that the two lines $x=0$ and $y=0$ contain at most $|\mathcal{E}|/2$ points from $\mathcal{E}$, we have*

$$|f(\mathcal{E})| \gg \min\left\{\frac{|\mathcal{E}|^{19/15}|\mathcal{F}|^{4/15}}{|\mathcal{E}+\mathcal{F}|},\ \frac{|\mathcal{E}|^{19/4}|\mathcal{F}|^{15/4}}{|\mathcal{E}+\mathcal{F}|^{23/4}}, |\mathcal{E}|\right\}.$$

Proof. Let $\mathcal{E}' = \mathcal{E} \setminus \{(a,b) \in \mathcal{E} : a = 0 \text{ or } b = 0\}$.

By our assumption, we know that $|\mathcal{E}'| \gg |\mathcal{E}|$. We note that $0 \notin f(\mathcal{E}')$, so the curves defined by

$$(x-a)(y-b) = t,$$

with $(a,b) \in \mathcal{F}$ and $t \in f(\mathcal{E}')$ are irreducible. So, we can use the same argument as in the proof of Theorem 6.6 to conclude the proof of the theorem. □

Remark 6.8. We note that the assumption that there is at most a proportion of points from $\mathcal{E}$ belonging to the two lines $x=0$ and $y=0$ is necessary, for instance, if $\mathcal{E} \subset \{x=0\} \cup \{y=0\}$, then it is clear that $f(\mathcal{E}) = \{0\}$.

6.3 An improvement of Koh-Sun's result on distances for large sets

For $\mathcal{E}, \mathcal{F} \subset \mathbb{F}_q^d$, we denote the set of distances between $\mathcal{E}$ and $\mathcal{F}$ by the set $\Delta(\mathcal{E}, \mathcal{F})$.

We recall results of Koh and Sun [15], which remove the logarithmic factor in a result due to Dietmann [7]. In [15, Theorems 3.3], the authors prove that if $d \geq 3$ is odd, then

$$|\Delta(\mathcal{E},\mathcal{F})| \geq \begin{cases} \min\left\{\frac{q}{2}, \frac{|\mathcal{E}||\mathcal{F}|}{8q^{d-1}}\right\} & \text{if } 1 \leq |\mathcal{E}| < q^{\frac{d-1}{2}} \\ \min\left\{\frac{q}{2}, \frac{|F|}{8q^{\frac{d-1}{2}}}\right\} & \text{if } q^{\frac{d-1}{2}} \leq |E| < q^{\frac{d+1}{2}} \\ \min\left\{\frac{q}{2}, \frac{|\mathcal{E}||\mathcal{F}|}{2q^d}\right\} & \text{if } q^{\frac{d+1}{2}} \leq |\mathcal{E}| \leq q^d \end{cases}. \tag{6.1}$$

For even $d \geq 2$, under the assumption $|\mathcal{E}||\mathcal{F}| \geq 16q^d$, by [15, Theorems 3.5], one has

$$|\Delta(\mathcal{E},\mathcal{F})| \geq \begin{cases} \frac{q}{144} & \text{for } \ 1 \leq |\mathcal{E}| < q^{\frac{d-1}{2}} \\ \frac{1}{144}\min\left\{q, \frac{|\mathcal{F}|}{2q^{\frac{d-1}{2}}}\right\} & \text{for } \ q^{\frac{d-1}{2}} \leq |\mathcal{E}| < q^{\frac{d+1}{2}} \\ \frac{1}{144}\min\left\{q, \frac{2|\mathcal{E}||\mathcal{F}|}{q^d}\right\} & \text{for } \ q^{\frac{d+1}{2}} \leq |\mathcal{E}| \leq q^d \end{cases}. \tag{6.2}$$

We mention that, in comparison to estimate (6.1) (for odd d), the additional condition $|\mathcal{E}||\mathcal{F}| \geq 16q^d$ for estimate (6.2) (for even d) is necessary in Koh and Sun's proof. This is due to the fact that the Fourier decay of the sphere of zero radius in even dimensions is much worse than in odd dimensions. We also note that in the range $q^{\frac{d+1}{2}} \leq |\mathcal{E}| \leq q^d$, the lower bound $\gg \min\left\{q, \frac{|\mathcal{E}||\mathcal{F}|}{q^d}\right\}$ was obtained by Shparlinski [24] without the condition $|\mathcal{E}||\mathcal{F}| \gg q^d$.

As a direct consequence of Theorem 1.6, we are able to remove the condition $|\mathcal{E}||\mathcal{F}| \gg q^d$ for the range $q^{\frac{d-1}{2}} \leq |\mathcal{E}| \leq q^{\frac{d+1}{2}}$.

Theorem 6.9. *Let $\mathcal{E}, \mathcal{F}$ be sets in $\mathbb{F}_q^d$. Assume that $|\mathcal{E}| \sim |\mathcal{F}| \leq q^{\frac{d+1}{2}}$, then we have*

$$|\Delta(\mathcal{E},\mathcal{F})| \gg \min\left\{q, \frac{|\mathcal{E}|^{1/2}|\mathcal{F}|^{1/2}}{q^{\frac{d-1}{2}}}\right\}.$$

Proof. For $\boldsymbol{p} \in \mathcal{F}$, let $\mathcal{C}_{\boldsymbol{p}}$ be the set of spheres centered at $\boldsymbol{p}$ of radius in $\Delta(\boldsymbol{p},\mathcal{E})$, and let $\mathcal{C} = \bigcup_{\boldsymbol{p}\in\mathcal{F}} \mathcal{C}_{\boldsymbol{p}}$. We have $|\mathcal{C}| = \sum_{\boldsymbol{p}\in\mathcal{F}} |\Delta(\boldsymbol{p},\mathcal{E})|$, and $I(\mathcal{E},\mathcal{C}) \gg |\mathcal{E}||\mathcal{F}|$. Therefore, applying Theorem 1.6 gives

$$|\mathcal{E}||\mathcal{F}| \ll \frac{|\mathcal{E}|\sum_{\boldsymbol{p}\in\mathcal{F}} |\Delta(\boldsymbol{p},\mathcal{E})|}{q} + q^{\frac{d-1}{3}}|\mathcal{E}|^{2/3}\left(\sum_{\boldsymbol{p}\in\mathcal{F}} |\Delta(\boldsymbol{p},\mathcal{E})|\right)^{2/3}.$$

Solving this inequality, there exists $\boldsymbol{p} \in \mathcal{F}$ such that

$$|\Delta(\boldsymbol{p},\mathcal{E})| \gg \min\left\{q, \frac{|\mathcal{E}|^{1/2}|\mathcal{F}|^{1/2}}{q^{\frac{d-1}{2}}}\right\}.$$

□

6.4 Conical Beck's Theorem

A well-known result of Beck [2] states that for a finite point set $\mathcal{P} \subset \mathbb{R}^2$, either a positive proportion of $\mathcal{P}$ is collinear or there exist $\Omega(|\mathcal{P}|^2)$ distinct lines supported on 2-tuples of (distinct) points of $\mathcal{P}$. See [25, Corollary 14] for a quantitatively weaker analogue of this result, which holds over arbitrary fields.

We proceed to prove a finite field analogue of Beck's theorem, replacing the notion of lines by irreducible conics. See also [32, Corollary 2] for a similar result involving Möbius transformations. In the following, an irreducible conic is said to be defined by a point set $\mathcal{P}$ if it passes through at least five points of $\mathcal{P}$.

Theorem 6.10. *Let $\mathcal{P} \subseteq \mathbb{F}_p^2$ be a set of points with $|\mathcal{P}| \ll p^{15/13}$, with no positive proportion of $\mathcal{P}$ collinear. Then either there exists a conic C such that $|C \cap \mathcal{P}| \gg |\mathcal{P}|$, or $\mathcal{P}$ defines at least $|\mathcal{P}|^{20/7}$ irreducible conics.*

We note that this theorem implies that any point set $\mathcal{P} \subseteq \mathbb{F}_p^2$ with $p^{1+\varepsilon} < |\mathcal{P}| \ll p^{15/13}$, for some

$\varepsilon > 0$, must define at least $|\mathcal{P}|^{20/7}$ irreducible conics, since no conic or line can contain a positive proportion of this point set. We further point out that proof of this theorem relies on a bound on the number of k-rich conics obtained as part of the proof of Theorem 1.1. Moreover, note that a collinearity restriction is necessary in this theorem; an irreducible conic is only defined by five points which lie in general position. Through essentially the same scheme, one may replace this bound by the one obtained in the proof of Theorem 1.3 to give an improved result, concerning circles, parabolas and hyperbolas.

Proof of Theorem 6.10. We begin by claiming that a positive proportion of the 5-tuples defined by $\mathcal{P}$ are in general position. Indeed, if we let L be the maximum number of collinear points in $\mathcal{P}$, we have

$$\#\text{5-tuples in GP} = |\mathcal{P}|(|\mathcal{P}|-1)(|\mathcal{P}|-L)(|\mathcal{P}|-3L)(|\mathcal{P}|-6L) = |\mathcal{P}|^5 - O(L|\mathcal{P}|^4) \gg |\mathcal{P}|^5,$$

where the last inequality follows from $L = o(|\mathcal{P}|)$. From this point we focus only on 5-tuples of points from $\mathcal{P}$ which are in general position.

With a slight abuse of notation, we write $\mathcal{C}_k$ to denote the set of irreducible conics over $\mathbb{F}_p^2$ containing at least k and at most $2k-1$ points of $\mathcal{P}$. The number of 5-tuples of points of $\mathcal{P}$ contained in elements of $\mathcal{C}_k$ is at most $O(k^5|\mathcal{C}_k|)$ which, by (2.3), is bounded by $O(|\mathcal{P}|^{23/4}k^{-7/4} + |\mathcal{P}|^4 k)$.

Let $I = \{k \geq 5 : \lambda|\mathcal{P}|^{3/7} \leq k \leq \lambda^{-7/4}|\mathcal{P}|\}$ for some constant $\lambda > 0$ to be determined. Then, by the above estimate, the total number of 5-tuples of $\mathcal{P}$ contained in the conics $\cup_{k\in I}\mathcal{C}_k$ is at most $O(\lambda^{-7/4}|\mathcal{P}|^5)$. Taking λ to be sufficiently large, we may assume these account for less than, say, half of the total number of 5-tuples of $\mathcal{P}$. Moreover, we may assume there exists no irreducible conic containing more than $\lambda^{-7/4}|\mathcal{P}|$ points of $\mathcal{P}$, since otherwise there is nothing to prove.

We conclude that a positive proportion of the 5-tuples of $\mathcal{P}$ lie on conics belonging to the set

$$\mathcal{C} := \bigcup_{k<\lambda|\mathcal{P}|^{3/7}} \mathcal{C}_k.$$

Consequently, we have

$$|\mathcal{P}|^5 \approx \sum_{C\in\mathcal{C}} |C\cap\mathcal{P}|^5 \ll |\mathcal{C}||\mathcal{P}|^{15/7},$$

which gives the second possibility claimed by the theorem, concluding the proof. □

Acknowledgements

Thang Pham would like to thank to the VIASM for the hospitality and for the excellent working condition. Audie Warren was supported by Austrian Science Fund FWF grant P-34180. We thank Oliver Roche-Newton for helpful discussions, and two reviewers for many valuable comments.

References

[1] S. Ball, *Finite Geometry and Combinatorial Applications*, London Mathematical Society Student Texts 82, Cambridge University Press, Cambridge, 2015.

[2] J. Beck, 'On the lattice property of the plane and some problems of Dirac, Motzkin and Erdős in combinatorial geometry', *Combinatorica* **3** (1983), 281–297.

[3] B. Bollobás, 'Modern Graph Theory', Springer, Berlin, 1998.

[4] J. Bourgain, 'A modular Szemerédi-Trotter theorem for hyperbolas', *C. R. Math. Acad. Sci. Paris* **350** (2012), 793–796.

[5] J. Bourgain, N. Katz and T. Tao, 'A sum-product estimate in finite fields, and applications', *Geom. Funct. Anal.* **14**(1) (2004), 27–57.

[6] J. Cilleruelo, A. Iosevich, B. Lund, O. Roche-Newton and M. Rudnev, 'Elementary methods for incidence problems in finite fields', *Acta Arith.* **177** (2017), 133–142.

[7] R. Dietmann, 'On the Erdős–Falconer distance problem for two sets of different size in vector spaces over finite fields', *Monatsh. Math.* **170** (2013), 343–359.

[8] Z. Dvir, 'Incidence theorems and their applications', *Foundations and Trends in Theoretical Computer Science* **6** (2012), 257–393.

[9] C. Grosu, '$\mathbb{F}_p$ is locally like $\mathbb{C}$', *J. London Math. Soc.* **89**(3) (2014), 724–744.

[10] H. Helfgott, M. Rudnev, 'An explicit incidence theorem in $\mathbb{F}_p$', *Mathematika* **57** (2011), 135–156.

[11] A. Iosevich, D. Koh and T. Pham, 'New bounds for distance-type problems over prime fields', *Eur. J. Combin.* **86** (2020), 103080.

[12] A. Iosevich, D. Koh, T. Pham, C-Y Shen and L. A. Vinh, 'A new bound on Erdős distinct distances problem in the plane over prime fields', *Acta Arith.* **193** (2020), 165–174.

[13] T. G. F. Jones, 'An improved incidence bound for fields of prime order', *Eur. J. Combin.* **52** (2016), 136–145.

[14] D. Koh, S. Lee and T. Pham, 'On the finite field cone restriction conjecture in four dimensions and applications in incidence geometry', *Int. Math. Res. Not.* (to appear) (2021).

[15] D. Koh and H-S. Sun, 'Distance sets of two subsets of vector spaces over finite fields', *Proc. Amer. Math. Soc.* **143** (2015), 1679-1692.

[16] B. Lund and G. Petridis, 'Bisectors and pinned distances', *Discrete Comput. Geom.* **64** (2020), 995–1012.

[17] B. Murphy and G. Petridis, 'A point-line incidence identity in finite fields, and applications', *Mosc. J. Comb. Number Theory* **6**(1) (2016), 64–95.

[18] B. Murphy and G. Petridis, 'A second wave of expanders', in *Combinatorial and Additive Number Theory II* Springer International Publishing, New York, 2017.

[19] B. Murphy, G. Petridis, T. Pham, M. Rudnev and S. Stevens, 'On the pinned distances problem over finite fields', *J. London Math. Soc.* (to appear), arXiv:2003.00510 (2020).

[20] J. Pach and M. Sharir, 'On the number of incidences between points and curves', *Combin. Probab. Comput.*, **7** (1998), 121–127.

[21] M. Rudnev, 'On the number of incidences between points and planes in three dimensions', *Combinatorica* **38** (2018), 219–238.

[22] M. Rudnev and J. Wheeler, 'Incidence bounds with Möbius hyperbolae in positive characteristic', arXiv preprint `arXiv:2104.10534` (2021).

[23] I. D. Shkredov, 'Modular hyperbolas and bilinear forms of Kloosterman sums', *J. Number Theory* **220** (2020), 182–211.

[24] I. E. Shparlinski, 'On the set of distances between two sets over finite fields', *Int. J. Math. Math. Sci.* (2006) Art. ID 59482.

[25] S. Stevens and F. de Zeeuw, 'An improved point-line incidence bound over arbitrary fields', *Bull. London Math. Soc.* **49** (2017), 842–858.

[26] E. Szemerédi and W.T. Trotter, 'Extremal problems in discrete geometry', *Combinatorica* **3** (1983), 381–392.

[27] A. Sheffer, *Polynomial Methods and Incidence Theory*, Cambridge University Press, 2022.

[28] T. Tao and V. Vu, Additive Combinatorics, Cambridge University Press, Cambridge, 2006.

[29] C. D. Tóth, 'The Szemerédi–Trotter theorem in the complex plane', *Combinatorica* **35** (2015), 95–126.

[30] L. A. Vinh, 'Szemerédi-Trotter type theorems and sum-product estimates in finite fields', *Eur. J. Combin.* **32** (2011), 1177–1181.

[31] L. A.Vinh, 'On point-line incidences in vector spaces over finite fields', *Discrete Appl. Math.* **177**(1) (2014), 146–151.

[32] A. Warren and J. Wheeler, 'Incidences of Möbius transformations in $\mathbb{F}_p$', arXiv preprint `arXiv:2107.12286` (2021).