ELEMENTARY METHODS FOR INCIDENCE PROBLEMS IN FINITE FIELDS

JAVIER CILLERUELO, ALEX IOSEVICH, BEN LUND, OLIVER ROCHE-NEWTON AND MISHA RUDNEV

ABSTRACT. We use elementary methods to prove an incidence theorem for points and spheres in $\mathbb{F}_q^n$. As an application, we show that any point set $P \subset \mathbb{F}_q^2$ with $|P| \geq 5q$ determines a positive proportion of all circles. The latter result is an analogue of Beck's Theorem for circles which is optimal up to multiplicative constants.

1. INTRODUCTION

Let $\mathbb{F}_q$ be a field with characteristic strictly greater than 2.[1] In this note, it is established that for a point set $P \subset \mathbb{F}_q^d$ and a family $\mathcal{S}$ of *spheres* in $\mathbb{F}_q^d$, the number of incidences between the points and spheres, which is denoted by $I(P, \mathcal{S}) := |\{(p, S) \in P \times \mathcal{S} : p \in S\}|$, satisfies the bound

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

Many results on incidence problems in finite fields have appeared in recent years; see for example [3, 6, 9, 12]. For relatively large sets of points and surfaces in $\mathbb{F}_q^d$, Fourier analysis and spectral graph theory have been the main tools to deal with these problems. For example, Vinh [12] used the spectral method to prove that, for sets P and $\mathcal{L}$ of points and lines respectively in $\mathbb{F}_q^2$,

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

The result was extended to incidences between points and hyperplanes in $\mathbb{F}_q^d$, and can also be proven using discrete Fourier analysis.

In [5], the first author found an elementary method to prove some results on combinatorial problems in finite fields, including an alternative proof of (1). Here we follow that elementary approach to give an estimate on incidences of points and spheres in $\mathbb{F}_q^d$ and illustrate it with some applications to the pinned distance problem, as well proving a version of Beck's Theorem for circles in $\mathbb{F}_q^2$.

Mathematics Subject Classification 52C10

[1]Whenever a finite field $\mathbb{F}_q$ is mentioned in this paper, it is assumed to have characteristic strictly greater than 2.

In particular, the version of Beck's Theorem for points and circles is tight up to multiplicative constants. In the forthcoming Theorem 3, it is established that any set $P \subset \mathbb{F}_q^2$ such that $|P| \geq 5q$ determines[2] a positive proportion of all circles. On the other hand, if one takes a set P of q points lying on a single line in the plane, then P does not determine any circles. Similarly, if P consists of, say, $q+1$ points on the same circle, then P determines only 1 circle. These degenerate examples are in a sense 1-dimensional, and illustrate the tightness of Theorem 3.

Before saying any more about spheres in finite fields, it is necessary to define what is meant by such an object. We follow the notion of distance introduced in [7]; given a pair of points $x = (x_1, \cdots, x_d)$ and $y = (y_1, \cdots, y_d)$ in $\mathbb{F}_q^d$, the *distance* between x and y is given by

$$||x - y|| := (x_1 - y_1)^2 + \cdots + (x_d - y_d)^2.$$

As one might expect, a *sphere* in $\mathbb{F}_q^d$ is a set of points which are the same distance λ from a given central point $(\alpha_1, \cdots, \alpha_d)$. That is, a sphere is the set of points $x = (x_1, \cdots, x_d)$ which satisfy an equation of the form

$$(x_1 - \alpha_1)^2 + \cdots + (x_d - \alpha_d)^2 = \lambda.$$

These spheres have many natural properties which are analogous with spheres in $\mathbb{R}^d$. For example, given two circles[3] in $\mathbb{F}_q^2$, it is easy to check that the circles intersect in at most two points.

1.1. **Work of Phoung, Thang and Vinh.**

Shortly after an earlier draft of this paper was made available online, we became aware of its overlap with a forthcoming paper of Phoung, Thang and Vinh [11]. The authors in [11] give an independent proof of Theorem 1 via graph theoretic methods similar to those used in [12]. Further applications of the incidence result are also given in [11].

2. Incidences between spheres and points

Given finite sets A, B in a finite group $(G, +)$ we use the notation

$$r_{A+B}(x) = |\{(a,b) \in A \times B : \ a + b = x\}|.$$

We recall the following elementary and well known identities:

$$\sum_{x \in G} r_{A+B}(x) = |A||B|, \qquad (2)$$

$$\sum_{x \in G} r^2_{A+B}(x) = \sum_{x \in G} r_{A-A}(x) r_{B-B}(x). \qquad (3)$$

The quantity in (3) is called the *additive energy* of A and B.

[2]Just as in the real plane, three noncollinear points in $\mathbb{F}_q^2$ determine a unique circle. A set of points P determines a given circles if three points from P determine that circle. More details of these basic properties of circles are given in section 3.

[3]Naturally, we call a sphere in $\mathbb{F}_q^2$ a *circle*.

Lemma 1. *Define*

$$A := \{(a_1, a_2, \cdots, a_d, a_1^2 + \cdots + a_d^2) : \ a_1, \cdots, a_d \in \mathbb{F}_q\} \subset \mathbb{F}_q^{d+1}. \tag{4}$$

Then, for all $x = (x_1, \cdots, x_{d+1}) \neq (0, \cdots, 0)$,

$$r_{A-A}(x) \leq q^{d-1}. \tag{5}$$

Proof. This can be calculated directly. Indeed, the quantity $r_{A-A}(x)$ is the number of solutions

$$(a_1, \cdots, a_d, b_1, \cdots, b_d) \in \mathbb{F}_q^{2d}$$

to the system of equations

$$\begin{aligned} a_1 - b_1 &= x_1 \\ a_2 - b_2 &= x_2. \\ &\vdots \\ a_d - b_d &= x_d \\ a_1^2 + \cdots + a_d^2 - b_1^2 - \cdots - b_d^2 &= x_{d+1}. \end{aligned}$$

The b_i variables can be eliminated, and this system of equations reduces to

$$2a_1x_1 + \cdots + 2a_dx_d - x_1^2 - \cdots - x_d^2 = x_{d+1}. \tag{6}$$

If $x \neq 0$ then there is some $1 \leq i \leq d$ such that $x_i \neq 0$. Otherwise $x_{d+1} = 0$ and $x = 0$ is the only choice which admits solutions to (6). Without loss of generality, we may take $i = 1$. If we fix $a_2, \cdots, a_d$, then since the characteristic of the field is not equal to 2, we have $2x_1 \neq 0$ and the value of a_1 is uniquely determined. This gives $r_{A-A}(x) \leq q^{d-1}$.

If $x = 0$, then trivially $r_{A-A}(0) = |A| = q^d$.

□

Lemma 2. *Let A be as defined in* (4)*, and let $B, C \subset \mathbb{F}_q^{d+1}$ be arbitrary. Then*

$$|\{(b, c) \in B \times C : \ b - c \in A\}| = \frac{|B||C|}{q} + \theta |B|^{1/2}|C|^{1/2}q^{d/2},$$

for some $\theta \in \mathbb{R}$ such that $|\theta| < 1$.

Proof. Note that

$$\begin{aligned} |\{(b, c) \in B \times C : \ b - c \in A\}| - \frac{|B||C|}{q} &= \sum_{b \in B} \left(|\{c \in C : \ b - c \in A\}| - \frac{|C|}{q} \right) \\ &= \sum_{b \in B} \left(r_{A+C}(b) - \frac{|C|}{q} \right) := E. \end{aligned}$$

By Cauchy-Schwarz:

$$|E|^2 \leq |B| \sum_{b \in B} \left(r_{A+C}(b) - \frac{|C|}{q} \right)^2 \leq |B| \sum_{x \in \mathbb{F}_q^{d+1}} \left(r_{A+C}(x) - \frac{|C|}{q} \right)^2 .$$

Using (2), (3) and the fact that $|A| = q^d$ we have

$$\begin{aligned} \sum_{x \in \mathbb{F}_q^{d+1}} \left(r_{A+C}(x) - \frac{|C|}{q} \right)^2 &= \sum_{x \in \mathbb{F}_q^{d+1}} r_{A+C}^2(x) - q^{d-1}|C|^2 \\ &= \sum_{x \in \mathbb{F}_q^{d+1}} r_{A-A}(x) r_{C-C}(x) - q^{d-1}|C|^2 \\ &\leq |A||C| + q^{d-1} \sum_{x \neq 0} r_{C-C}(x) - q^{d-1}|C|^2 \\ &= |A||C| + q^{d-1}(|C|^2 - |C|) - q^{d-1}|C|^2 \\ &= |C| q^{d-1}(q-1). \end{aligned}$$

Thus, $|E| < (|B||C|)^{1/2} q^{d/2}$, which completes the proof. □

Theorem 1. *Let $P \subset \mathbb{F}_q^d$ and let $\mathcal{S}$ be a family of spheres in $\mathbb{F}_q^d$. Then*

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

Proof. We denote by $S_{\alpha_1, \cdots, \alpha_d, \lambda}$ the sphere

$$\{(x_1, \cdots, x_d) : \ (x_1 - \alpha_1)^2 + \cdots + (x_d - \alpha_d)^2 = \lambda\}.$$

Define

$$B = \{(p_1, \cdots, p_d, 0) : \ (p_1, \cdots, p_d) \in P\}$$

and

$$C = \{(\alpha_1, \cdots, \alpha_d, -\lambda) : \ S_{\alpha_1, \cdots, \alpha_d, \lambda} \in \mathcal{S}\}.$$

Note that $|B| = |P|$ and $|C| = |\mathcal{S}|$.

Now, note that

$$\begin{aligned} & |\{(b, c) \in B \times C : \ b - c \in A\}| \\ = \ & |\{((p_1, \cdots, p_d, 0), (\alpha_1, \cdots, \alpha_d, -\lambda)) \in B \times C : (p_1 - \alpha_1, \cdots, p_d - \alpha_d, \lambda) \in A\}| \\ = \ & |\{((p_1, \cdots, p_d, 0), (\alpha_1, \cdots, \alpha_d, -\lambda)) \in B \times C : \ (p_1 - \alpha_1)^2 + \cdots + (p_d - \alpha_d)^2 = \lambda)\}| \\ = \ & I(P, \mathcal{S}). \end{aligned}$$

An application of Lemma 2 completes the proof. □

3. Applications of the incidence bound

3.1. **Pinned distances.** Let P be a set of points in $\mathbb{F}_q^d$, and $y \in \mathbb{F}_q^d$. Following the notation of Chapman et. al. [4], let $\triangle_y(P)$ denote the set of distances between the point y and the set P; that is

$$\triangle_y(P) := \{||x-y|| : x \in P\}.$$

It was established in ([4], Theorem 2.3) that a sufficiently large set of points determines many pinned distances, for many different pins. Here, we use Theorem 1 to give an alternative proof.

Corollary 1. *Let P be a subset of $\mathbb{F}_q^d$ such that $|P| \geq \epsilon^{-1}(1-\epsilon)^{1/2}q^{\frac{d+1}{2}}$ for some $0<\epsilon<1$. Then,*

$$\frac{1}{|P|}\sum_{p\in P}|\triangle_p(P)| > (1-\epsilon)q. \tag{7}$$

Proof. Fix a point $p \in P$, and construct a family of spheres $\mathcal{S}_p$ by minimally covering P by concentric spheres around p. Note that $|\mathcal{S}_p| = |\triangle_p(P)|$, and that $I(P,\mathcal{S}_p) = |P|$. Repeating this process for each point in P, we generate a family of spheres $\mathcal{S}$ defined by the disjoint union

$$\mathcal{S} := \bigcup_{p\in P}\mathcal{S}_p.$$

Observe that $I(P,\mathcal{S}) = \sum_{p\in P} I(P,\mathcal{S}_p) = |P|^2$. On the other hand, Theorem 1 implies that

$$\begin{aligned}|P|^2 = I(P,\mathcal{S}) &< \frac{|P||\mathcal{S}|}{q} + |P|^{1/2}|\mathcal{S}|^{1/2}q^{d/2}\\ &= \frac{|P|\sum_{p\in P}|\triangle_p(P)|}{q} + |P|^{1/2}\left(\sum_{p\in P}|\triangle_p(P)|\right)^{1/2} q^{d/2}.\end{aligned}$$

If $\frac{1}{|P|}\sum_{p\in P}|\triangle_p(P)| \leq (1-\epsilon)q$ the last inequality would imply that $|P| < \epsilon^{-1}(1-\epsilon)^{1/2}q^{\frac{d+1}{2}}$. □

Corollary 2. *Let P be a subset of $\mathbb{F}_q^d$ such that $|P| \geq \alpha^{-2}(1-\alpha^2)^{1/2}q^{\frac{d+1}{2}}$ for some $0<\alpha<1$. Then,*

$$|\triangle_p(P)| > (1-\alpha)q$$

for at least $(1-\alpha)|P|$ points $p \in P$.

Proof. Corollary 1 implies that

$$\sum_{p\in P}|\triangle_p(P)| > (1-\alpha^2)q|P|.$$

On the other hand let

$$P' = \{p \in P : |\triangle_p(P)| \geq (1-\alpha)q\}$$

and suppose that $|P'| < (1-\alpha)|P|$. Then we would have

$$\begin{aligned}\sum_{p\in P}|\triangle_p(P)| &= \sum_{p\in P\setminus P'}|\triangle_p(P)| + \sum_{p\in P'}|\triangle_p(P)|\\ &< (1-\alpha)q(|P|-|P'|)+q|P'|\\ &= (1-\alpha)q|P|+\alpha q|P'|\\ &< (1-\alpha^2)q|P|.\end{aligned}$$

□

3.2. **A version of Beck's Theorem for circles.** A result which is closely related to the Szemerédi-Trotter Theorem and incidence geometry is Beck's Theorem [2]. This result states that a set of N points in $\mathbb{R}^2$ determines $\Omega(N^2)$ distinct lines by connecting pairs of points, provided that the set of points does not contain a single line which supports cN points, where c is a small but fixed constant. We say that that P determines a line l if there exist two points p_1 and p_2 belonging to P which both lie on the line l. In finite fields, an analogue of Beck's Theorem was proven by Alon [1], in the form of the following theorem:

Theorem 2. *Let $\epsilon > 0$ and let P be a set of points in the projective plane $\mathbb{PF}_q^2$ such that $|P| > (1+\epsilon)(q+1)$. Then P determines at least*

$$\frac{\epsilon^2(1-\epsilon)}{2+2\epsilon}(q+1)^2$$

distinct straight lines.

Iosevich, Rudnev and Zhai [8] used Fourier analytic techniques to establish a similar result. So, a sufficiently large set of points in the plane determines a positive proportion of all possible lines. The aim here is to establish an analogue of Theorem 2, with the role of lines replaced by circles. Since there are q^2 choices for the location of a circle's centre, and q choices for the radius, we want to generate $\Omega(q^3)$ circles. We first need an obvious definition of what it means for a circle to be generated by a set of points.

Given three non-collinear points in $\mathbb{R}^2$, there exists a unique circle which passes through each of the three points. The same is true of three points in $\mathbb{F}_q^2$:

Lemma 3. *Let (x_1,y_1), (x_2,y_2) and (x_3,y_3) be three distinct non-collinear points in $\mathbb{F}_q^2$. Then there exists a unique circle supporting the three points.*

Proof. We'll show that there exists a unique triple of elements $a,b,c\in\mathbb{F}_q$ such that the system of equations

$$\left\{\begin{array}{ccccc}(x_1-a)^2 &+& (y_1-b)^2 &=& c,\\ (x_2-a)^2 &+& (y_2-b)^2 &=& c,\\ (x_3-a)^2 &+& (y_3-b)^2 &=& c,\end{array}\right. \tag{8}$$

can be realised. Note that we cannot have $x_1 = x_2 = x_3$, since this would contradict the hypothesis that the three points are non-collinear. Therefore, it is assumed without loss of generality that $x_1 \neq x_2$ and $x_1 \neq x_3$.

Subtracting the first equation in (8) from the second and third yields the following system of linear equations:

$$\left\{ \begin{array}{lcl} 2(x_1 - x_2)a + 2(y_1 - y_2)b & = & x_1^2 + y_1^2 - x_2^2 - y_2^2, \\ 2(x_1 - x_3)a + 2(y_1 - y_3)b & = & x_1^2 + y_1^2 - x_3^2 - y_3^2. \end{array} \right. \tag{9}$$

It cannot be the case that both $y_2 = y_1$ and $y_3 = y_1$ (otherwise the three points would be collinear), and so at least one of the b coefficients is non-zero. Therefore, this is a system of two linear equations with two variables (a and b). This system has a unique solution (a, b), unless it is degenerate. This solution can then be plugged into (8) to give a unique solution to the system as required. It remains to show that (9) is non-degenerate.

Suppose for a contradiction that (9) is degenerate. Then there exists $\lambda \in \mathbb{F}_q^*$ such that

$$\left\{ \begin{array}{lcl} \lambda(x_2 - x_1) & = & x_3 - x_1, \\ \lambda(y_2 - y_1) & = & y_3 - y_1, \end{array} \right. \tag{10}$$

Since it is known that at least one of $y_2 - y_1$ and $y_3 - y_1$ is non-zero, and λ is non-zero, it must be the case that both $y_2 - y_1 \neq 0$ and $y_3 - y_1 \neq 0$. Therefore,

$$\lambda = \frac{x_3 - x_1}{x_2 - x_1} = \frac{y_3 - y_1}{y_2 - y_1}.$$

Hence

$$y_3 - y_1 = (x_3 - x_1)\frac{y_2 - y_1}{x_2 - x_1},$$

and clearly

$$y_2 - y_1 = (x_2 - x_1)\frac{y_2 - y_1}{x_2 - x_1}.$$

This implies that $(x_1, y_1), (x_2, y_2)$ and (x_3, y_3) are supported on a line with equation

$$y = \frac{y_2 - y_1}{x_2 - x_1}x + C,$$

where $C = \frac{y_1 x_2 - x_1 y_2}{x_2 - x_1}$. This is a contradiction, and the proof is complete.

□

We say that a circle C is determined by P if there exist three points from P which determine the circle C. We are now ready to state our version of Beck's Theorem for circles:

Theorem 3. *Let $P \subset \mathbb{F}_q^2$ such that $|P| \geq 5q$. Then P determines at least $\frac{4q^3}{9}$ distinct circles.*

Note that in the statement of Theorems 2 and 3, the conclusion is that we determine a positive proportion of all possible lines and circles respectively. If one asks how many points are needed to generate *all* lines (respectively circles), then the problem becomes rather different, since one can take a point set $P = \mathbb{F}_q^2 \setminus l$ where l is a line (respectively $P = \mathbb{F}_q^2 \setminus C$ where C is a circle), and the line l (respectively the circle C) is not determined by the point set P. So, we cannot hope to show that a set of $o(q^2)$ points determine all possible lines or circles.

3.3. **Proof of Theorem 3.** At the outset, identify a subset $P' \subset P$ such that $|P'| = 5q$. The aim is to show that P', and hence also P, determines many circles.

Let $\mathcal{S}$ be the set of all circles which contain less than or equal to 3 points from P'. We will show that

$$|\mathcal{S}| < \frac{5q^3}{9}, \tag{11}$$

and then since there are q^3 circles, it must be the case that there are at least $\frac{4}{9}q^3$ circles which contain at least 3 points from P'. These $4q^3/9$ circles are therefore spanned by P.

It remains to prove (11), and to do this we will make use of the lower bound on $I(P', \mathcal{S})$ from Theorem 1. We have

$$\begin{aligned} 5|\mathcal{S}| - |P'|^{1/2}|\mathcal{S}|^{1/2}q = \frac{|P'||\mathcal{S}|}{q} - |P'|^{1/2}|\mathcal{S}|^{1/2}q \\ < I(P', \mathcal{S}) \\ \leq 2|\mathcal{S}|, \end{aligned}$$

a rearrangement of which gives

$$|\mathcal{S}| < \frac{|P'|q^2}{9} = \frac{5q^3}{9},$$

as required.

□

Arguments similar to the proof above can be found in [10]. Note that, using a lower bound on the number of incidences between sets of points and lines in $\mathbb{F}_q^2$ which follows from the proof of the main result in [12], it is straightforward to adapt the proof of Theorem 3 with lines in the place of circles in order to prove a version of Theorem 2.

Acknowledgements. J. Cilleruelo was supported by grants MTM 2011-22851 of MICINN and ICMAT Severo Ochoa project SEV-2011-0087. Oliver Roche-Newton was supported by EPSRC Doctoral Prize Scheme (Grant Ref: EP/K503125/1) and by the Austrian Science Fund (FWF): Project F5511-N26, which is part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications.

References

[1] N. Alon 'Eigenvalues, geometric expanders, sorting in rounds, and Ramsey theory', *Combinatorica* **6** (1986), no. 3, 207-219.

[2] J. Beck, 'On the lattice property of the plane and some problems of Dirac, Motzkin and Erdős in combinatorial geometry', *Combinatorica* **3** (1983), no. 3-4, 281-297.

[3] J. Bourgain, N. H. Katz and T. Tao, 'A sum-product estimate in finite fields, and applications', *Geom. Funct. Anal.* **14** (2004), no. 1, 27-57.

[4] J. Chapman, M. Erdoğan, D. Hart, A. Iosevich and D.Koh, 'Pinned distance sets, k-simplices, Wolff's exponent in finite fields and sum-product estimates', *Math. Z.* **271** (2012), no. 1-2, 63-93.

[5] J. Cilleruelo, 'Combinatorial problems in finite fields and Sidon sets', *Combinatorica* **32** (2012), no.5, 497-511.

[6] H. Helfgott and M. Rudnev, 'An explicit incidence theorem in $\mathbb{F}_p$', *Mathematika* **57** (2011), no. 1, 135-145.

[7] A. Iosevich and M. Rudnev, 'Erdős distance problem in vector spaces over finite fields', *Trans. Amer. Math. Soc.* **359** (2007), no. 12, 6127-6142.

[8] A. Iosevich, M. Rudnev and Y. Zhai, 'Areas of triangles and Beck's theorem in planes over finite fields', *arXiv:1205.0107*, (2012).

[9] T. G. F. Jones, 'Further improvements to incidence and Beck-type bounds over prime finite fields', *arXiv:1206.4517*, (2012).

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

[11] N. D. Phoung, P. V. Thang and L. A. Vinh, 'On the number of incidences between points and spheres in vector space over finite fields and related problems', *Forthcoming*.

[12] L. A. Vinh, 'The Szemerédi-Trotter type theorem and the sum-product estimate in finite fields', *European J. Combin.* **32** (2011), no. 8, 1177-1181.

J. Cilleruelo: Instituto de Ciencias Matemáticas (CSIC-UAM-UC3M-UCM) and Departamento de Matemáticas, Universidad Autónoma de Madrid, 28049 Madrid, Spain

E-mail address: franciscojavier.cilleruelo@uam.es

A. Iosevich: Department of Mathematics, University of Rochester, Rochester, NY

E-mail address: iosevich@gmail.com

B. Lund: Department of Computer Science, Rutgers, The State University of New Jersey, NJ

E-mail address: lund.ben@gmail.coms

O. Roche-Newton: Johann Radon Institute for Computational and Applied Mathematics (RICAM), Austrian Academy of Sciences, 4040 Linz, Austria

E-mail address: o.rochenewton@gmail.com

M. Rudnev: School of Mathematics, University Walk, Bristol, BS8 1TW

E-mail address: M.Rudnev@bristol.ac.uk