TWO GEOMETRIC COMBINATORIAL PROBLEMS IN VECTOR SPACES OVER FINITE FIELDS

EMMETT WYMAN

Abstract. First, we show that the number of ordered right triangles with vertices in a subset E of the vector space $\mathbb{F}_q^2$ over the finite field $\mathbb{F}_q$ is equal to the expected value $q^{-1}|E|^3$ up to an error term $O(q^{\frac{3}{2}}|E|^{\frac{3}{2}})$. Second, let $E \subset \mathbb{F}_q^d$. We give a lower bound for the maximum discrepancy between $|E \cap H|$ and the expected value $q^{-1}|E|$ taken over all hyperplanes H in $\mathbb{F}_q^d$. This result is easily extended to take H over all hyperplanes and spheres in $\mathbb{F}_q^d$.

Contents

1. Introduction 1
2. Fourier Analysis in $\mathbb{F}_q^d$ 2
3. Right Triangles 4
3.1. Statement of Results 4
3.2. Proof of Theorem 2 5
4. Discrepancies 8
4.1. Statement of Results 8
4.2. Proof of Theorem 3 9
References 14

1. Introduction

Geometric combinatorics in the Euclidean setting is a classical area of study. Recently, problems in the setting of vector spaces over finite fields have garnered much attention. Many of the results in the finite setting have continuous analogues. Consequentially, vector spaces over finite fields provide an excellent setting in which to study problems which may have similar results in Euclidean space [6]. In general, we are concerned with the asymptotic behavior of quantities dependent on a subset E of $\mathbb{F}_q^d$ as $q \to \infty$, e.g. the number of distinct distances between points in E, or the number of distinct areas of triangles with vertices in E (see [10] and [11]). The following notation will be useful in our treatment of such quantities. Let X and Y be quantities dependent on q. We write $X \lesssim Y$ if $X \leq CY$ for all large q, where C is some constant. $X \gtrsim Y$ means $Y \lesssim X$. We write $X \approx Y$ if $X \lesssim Y$ and $Y \lesssim X$. We write $X \ll Y$ if $X/Y \to 0$ as $q \to \infty$ and we write $X \gg Y$ if $Y \ll X$. In addition, we will use big O and little O notation: $Y = O(X)$ if there exists a constant C such that $|Y| < C|X|$ for all large q, and $X = o(Y)$ if $X/Y \to 0$ as $q \to \infty$.

Often, we will ask how large a subset E of $\mathbb{F}_q^d$ must be in order to ensure that it contains a certain kind of geometric structure, such as a simplex of particular volume or triangle with a particular angle. A k-simplex in $\mathbb{F}_q^d$ is a set of $k+1$ points such that any $n-1$-dimension subspace of $\mathbb{F}_q^d$ contains no more than n of them. In [9], D. Hart and A. Iosevich prove that any subset E of $\mathbb{F}_q^d$ such that $d > \binom{k+1}{2}$ and $|E| > Cq^{\frac{dk}{k+1}+\frac{k}{2}}$ where C is a universal constant, then E contains a copy of every k-simplex up to a rotation (a transformation by a matrix in the orthogonal group) and translation. In [4], the authors prove that if $|E| > Cq^{\frac{d+k}{2}}$, then E contains a positive proportion of non-congruent k-simplices.

In [20], L. A. Vinh gives the following result regarding triangles with vertices in a subset E of the plane $\mathbb{F}_q^2$: Let $s \in \mathbb{F}_q$ and suppose $|E| \gg q^{\frac{3}{2}}$, then the number $A(E,s) = |\{(x,y,z) \in E^3 : s = (x-y)\cdot(x-z)^{\perp}\}|$ of ordered triangles with vertices in E of area s is equal to $(1+o(1))q^{-1}|E|^3$. This result demonstrates that if E is large enough, then the number of triangles of area s determined by E converges to the expected value $q^{-1}|E|^3$. Vinh goes on to prove that $A(E,0) = (1+o(1))q^{-1}|E|^3$ if $|E| \gg q^{\frac{5}{3}}$. We will prove an analogous result for angles using a similar method.

Another result of interest is due to L. A. Vinh [19] regarding the proportion of right triangles determined by a subset E of the vector space $\mathbb{F}_q^d$ over the finite field $\mathbb{F}_q$ of q elements for $d \geq 2$, as follows.

Theorem 1. *Let $E \subset \mathbb{F}_q^d$ and let $D(E) = \{(x,y,z) \in E \times E \times E : (x-y)\cdot(x-z) = 0\}$ denote the set of ordered right triangles with vertices in E. Then $D(E)$ contains at least one element if $|E| > 2q^{\frac{2d+1}{3}}$.*

We will give a mild improvement on the constant for the case of $d = 2$.

In 1954, K. F. Roth published *On irregularities of distribution* in Mathematika, which proves the following result. Let E be a collection of points in the square $[0,1]\times[0,1]$. The maximum discrepancy between $|E \cap ([0,x]\times[0,y])|$ and the expected value $xy|E|$ is bounded below by $C\log|E|$ where C is a universal constant (see [14]). We will prove a result in a similar spirit in the finite field setting. Let $E \subset \mathbb{F}_q^d$ and consider the difference $\mathscr{D}_E(H) = |E \cap H| - q^{-1}|E|$ for each hyperplane H in $\mathbb{F}_q^d$. We will show that if E is a sufficiently small subset of $\mathbb{F}_q^d$, then there exists a hyperplane H such that $|\mathscr{D}_E(H)|$ is asymptotic to $q^{-\frac{1}{2}}|E|^{\frac{1}{2}}$.

2. Fourier Analysis in $\mathbb{F}_q^d$

Fourier analysis in $\mathbb{F}_q^d$ is a key technique applied to many problems in geometric combinatorics, and it will be an invaluable tool in the study of the problems presented herein. In the following section, we state and prove some of the tools of Fourier analysis in $\mathbb{F}_q^d$. Let $x = (x_1, \ldots, x_d)$ and $y = (y_1, \ldots, y_d) \in \mathbb{F}_q^d$. Then we define the dot product

$$x \cdot y := x_1y_1 + \cdots + x_dy_d.$$

We will also write

$$\|x\| := x \cdot x = x_1^2 + \cdots x_d^2.$$

Let $\chi : \mathbb{F}_q \to \mathbb{C}$ be a nontrivial additive character with the following properties.

1. $\chi(x+y) = \chi(x)\chi(y)$
2. For each $x \in \mathbb{F}_q$,

$$\sum_{m \in \mathbb{F}_q} \chi(mx) = \begin{cases} q & \text{if } x = 0, \\ 0 & \text{if } m \neq 0. \end{cases}$$

It follows from the above properties that $\chi(0) = 1$, $\overline{\chi(x)} = \chi(-x)$. Moreover, for any $x \in \mathbb{F}_q^d$

$$\sum_{m \in \mathbb{F}_q^d} \chi(x \cdot m) = \begin{cases} q^d & \text{if } x = 0, \\ 0 & \text{if } m \neq 0. \end{cases}$$

For more information regarding additive characters, see [6]. We now define the Fourier transform on $\mathbb{F}_q^d$ and prove some useful properties.

Definition 1. *Let $f : \mathbb{F}_q^d \to \mathbb{C}$. The Fourier transform $\hat{f}$ of f is defined to be*

$$\hat{f}(m) := q^{-d} \sum_{x \in \mathbb{F}_q^d} f(x)\chi(-x \cdot m).$$

Note that, in particular, the Fourier transform of f at 0 evaluates to

$$\hat{f}(0) = q^{-d} \sum_{x \in \mathbb{F}_q^d} f(x),$$

the average of f over $\mathbb{F}_q^d$.

Proposition 1. (Fourier Inversion Formula) *Let $f : \mathbb{F}_q^d \to \mathbb{C}$. Then*

$$f(x) = \sum_{m \in \mathbb{F}_q^d} \hat{f}(m)\chi(x \cdot m).$$

Proof.

$$\begin{aligned} \sum_{m \in \mathbb{F}_q^d} \hat{f}(m)\chi(x \cdot m) &= q^{-d} \sum_{m \in \mathbb{F}_q^d} \sum_{y \in \mathbb{F}_q^d} f(y)\chi(-m \cdot y)\chi(m \cdot x) \\ &= q^{-d} \sum_{y \in \mathbb{F}_q^d} f(y) \sum_{y \in \mathbb{F}_q^d} \chi(m \cdot (x-y)) \\ &= q^{-d} \sum_{y \in \mathbb{F}_q^d} \begin{cases} q^d & \text{if } x = y \\ 0 & \text{if } x \neq y \end{cases} \\ &= f(x). \end{aligned}$$

□

Proposition 2. (Plancherel's Formula) *Let $f, g : \mathbb{F}_q^d \to \mathbb{C}$. Then*

$$\sum_{m \in \mathbb{F}_q^d} \hat{f}(m)\overline{\hat{g}(m)} = q^{-d} \sum_{x \in \mathbb{F}_q^d} f(x)\overline{g(x)}.$$

Proof.

$$\begin{aligned}
\sum_{m \in \mathbb{F}_q^d} \hat{f}(m)\overline{\hat{g}(m)} &= q^{-2d} \sum_{m \in \mathbb{F}_q^d} \sum_{x \in \mathbb{F}_q^d} f(y)\chi(-x \cdot m) \sum_{y \in \mathbb{F}_q^d} \overline{g(y)}\chi(y \cdot m) \\
&= q^{-2d} \sum_{x,y \in \mathbb{F}_q^d} f(x)\overline{g(y)} \sum_{m \in \mathbb{F}_q^d} \chi((y-x) \cdot m) \\
&= q^{-2d} \sum_{x,y \in \mathbb{F}_q^d} f(x)\overline{g(y)} \begin{cases} q^d & \text{if } x = y \\ 0 & \text{if } x \neq y \end{cases} \\
&= q^{-d} \sum_{x \in \mathbb{F}_q^d} f(x)\overline{g(x)}.
\end{aligned}$$

□

We obtain Parseval's formula,

$$\sum_{m \in \mathbb{F}_q^d} |\hat{f}(m)|^2 = q^{-d} \sum_{x \in \mathbb{F}_q^d} |f(x)|^2,$$

a special case of Plancherel's formula, by setting $f = g$ in Plancherel's formula.

3. Right Triangles

3.1. **Statement of Results.** Here we state the main theorem for the distribution of right triangles in the plane.

Theorem 2. *Let $E \subset \mathbb{F}_q^d$ and $D(E) = \{(x, y, z) \in E \times E \times E : (x-y) \cdot (x-z) = 0\}$. Then*

$$|D(E)| = q^{-1}|E|^3 + \theta q^{\frac{3}{2}}|E|^{\frac{3}{2}},$$

where $|\theta| < 2^{1/2}$, with the leading term dominating if $|E| > 2^{\frac{1}{3}} q^{\frac{5}{3}}$. If we assume $q \equiv 3 \pmod 4$, then $|\theta| < 1 + o(1)$ and the leading term will dominate when $|E| > (1 + o(1))q^{\frac{5}{3}}$.

A remark: The main term is the expected value of $|D(E)|$ in the following sense. If we define

$$D_r(E) = \{(x, y, z) \in E^3 : (x-y) \cdot (x-z) = r\},$$

then E^3 can be expressed as the disjoint union $\bigcup_{r \in \mathbb{F}_q} D_r(E)$. Hence

$$|E|^3 = \sum_{r \in \mathbb{F}_q} |D_r(E)|,$$

and so we expect to find $|E|^3/q$ elements in $D_0(E) = D(E)$.

3.2. **Proof of Theorem 2.** We will make use of the following counting lemmas.

Lemma 1. *Let q be a prime power such that $q \equiv 3 \pmod 4$. Then for each $r \in \mathbb{F}_q$,*

$$|\{(x,y) \in \mathbb{F}_q^2 : x^2 + y^2 = r\}| \leq q + 1.$$

Proof. We have that

$$q^2 = \sum_{r \in \mathbb{F}_q} |\{(x,y) \in \mathbb{F}_q^2 : x^2 + y^2 = r\}|.$$

Since $q \equiv 3 \pmod 4$, the only solution to $x^2 + y^2 = 0$ is the trivial solution $x = y = 0$. Moreover, if r_1 and r_2 are both nonzero quadratic residues in $\mathbb{F}_q$, there exists $\lambda \in \mathbb{F}_q$ such that $r_1 = \lambda^2 r_2$. Hence

$$\begin{aligned} |\{(x,y) \in \mathbb{F}_q^2 : x^2 + y^2 = r_1\}| &= |\{(\lambda x, \lambda y) \in \mathbb{F}_q^2 : (\lambda x)^2 + (\lambda y)^2 = r_1\}| \\ &= |\{\lambda(x,y) \in \mathbb{F}_q^2 : (\lambda x)^2 + (\lambda y)^2 = \lambda^2 r_2\}| \\ &= |\{(x,y) \in \mathbb{F}_q^2 : x^2 + y^2 = r_2\}|. \end{aligned}$$

This works similarly if r_1 and r_2 are quadratic nonresidues. Note that since -1 is a quadratic nonresidue, we have

$$\begin{aligned} q^2 - 1 &= \sum_{r \in \mathbb{F}_q \setminus \{0\}} |\{(x,y) \in \mathbb{F}_q^2 : x^2 + y^2 = r\}| \\ &= \frac{q-1}{2} |\{(x,y) \in \mathbb{F}_q^2 : x^2 + y^2 = 1\}| + \frac{q-1}{2} |\{(x,y) \in \mathbb{F}_q^2 : x^2 + y^2 = -1\}|, \end{aligned}$$

and so

$$2(q+1) = |\{(x,y) \in \mathbb{F}_q^2 : x^2 + y^2 = 1\}| + |\{(x,y) \in \mathbb{F}_q^2 : x^2 + y^2 = -1\}|.$$

Now the number of solutions to $x^2 + y^2 = 1$ where $y \neq 0$ is the same as the number of solutions to $b^2 - a^2 = 1$ where $b \neq 0$ (divide through by y^2 and let $a = x/y$ and $b = 1/y$), which is equal to the number of solutions to $b^2 - a^2 = 1$ if b is allowed to be 0. This, however, is equal to the number of solutions to $\alpha\beta = 1$ by letting $\alpha = b - a$ and $\beta = b + a$. This has $q - 1$ solutions, and so $x^2 + y^2 = 1$ has $q + 1$ solutions, the extra two solutions coming from $x = \pm 1$, $y = 0$. It follows from the above equation that $x^2 + y^2 = -1$ also has $q + 1$ solutions. The lemma follows. □

Lemma 2. *Let $E \subset \mathbb{F}_q^2$. Then*

$$\begin{aligned} &|\{(y,z,y',z') \in E^4 : y + z = y' + z' \text{ and } y \cdot z = y' \cdot z'\}| \\ &\qquad \leq \begin{cases} (q+2)|E|^2 & \text{if } q \equiv 3 \pmod 4 \\ (2q+1)|E|^2 & \text{otherwise.} \end{cases} \end{aligned}$$

Proof. First consider the case where $z = z'$. Then $y = y'$ and the equation $y \cdot z = y' \cdot z'$ is automatically satisfied. There are $|E|$ options for both z and y, and so this case contributes $|E|^2$ elements. Now consider the case where $z \neq z'$. We may choose y and z in $|E|$ different ways each. After we determine y', there is at most one value

for $z' \in E$. This yields at most $|E|^2$ combinations of values for y, z, and z'. Then we write $z' = y + z - y'$. Plugging into $y \cdot z = y' \cdot z'$ yields

$$(*) \qquad 0 = y \cdot z - y' \cdot (y + z) + \|y'\|.$$

Now write $y' = (y_1', y_2')$, $z = (z_1, z_2)$, and $y = (y_1, y_2)$. There are at most q values which we could fix for y_1', and then the above equation becomes the quadratic

$$0 = (y \cdot z + y_1'^2 - y_1'(y_1 + z_1)) - y_2'(y_1 + z_1) + y_2'^2$$

as a function of y_2'. Hence there are at most two values for which y_2' can take, yielding $2q|E|^2$ for this case. Hence, we have $(2q+1)|E|^2$ as an upper bound. Now suppose $q \equiv 3 \pmod 4$. First note that q cannot be a power of 2, and so at $(*)$ we complete the square to obtain

$$\frac{\|y+z\|}{4} - y \cdot z = \frac{\|y+z\|}{4} - y' \cdot (y+z) + \|y'\| = \left\| y' - \frac{y+z}{2} \right\|.$$

There are, by Lemma 1, at most $q+1$ possible values y' may take to satisfy this equation. Hence our upper bound becomes $(q+2)|E|^2$. □

With the above lemmas in hand, we proceed with the proof of Theorem 2.

Proof. We write

$$|\{(x,y,z) \in E^3 : (x-y) \cdot (x-z) = 0\}| = q^{-1} \sum_{s \in \mathbb{F}_q} \sum_{x,y,z \in E} \chi(s(x-y) \cdot (x-z))$$

and split the sum into two terms: one for $s = 0$ and one for $s \neq 0$, so that the above becomes

$$= q^{-1} \sum_{x,y,z \in E} \chi(0) + q^{-1} \sum_{s \neq 0} \sum_{x,y,z \in E} \chi(s(x-y) \cdot (x-z)).$$

The first term is evaluated to $q^{-1}|E|^3$, the main term. Now we estimate the second term. Applying the Cauchy-Schwarz inequality twice yields

$$\begin{aligned}
&\left| q^{-1} \sum_{s\neq 0} \sum_{x,y,z\in E} \chi(s(x-y)\cdot(x-z)) \right|^2 \\
&\leq q^{-2}(q-1) \sum_{s\neq 0} \left| \sum_{x,y,z\in E} \chi(s(x-y)\cdot(x-z)) \right|^2 \\
&\leq q^{-2}(q-1)|E| \sum_{s\neq 0} \sum_{x\in E} \left| \sum_{y,z\in E} \chi(s(x-y)\cdot(x-z)) \right|^2 \\
&\leq q^{-2}(q-1)|E| \sum_{s\neq 0} \sum_{x\in \mathbb{F}_q^2} \left| \sum_{y,z\in E} \chi(s(x-y)\cdot(x-z)) \right|^2 \\
&= q^{-2}(q-1)|E| \sum_{s\neq 0} \sum_{x\in \mathbb{F}_q^2} \sum_{y,z,y',z'\in E} \chi(s(x-y)\cdot(x-z) - s(x-y')\cdot(x-z')) \\
&= q^{-2}(q-1)|E| \sum_{s\neq 0} \sum_{x\in \mathbb{F}_q^2} \sum_{y,z,y',z'\in E} \chi(s(y\cdot z - y'\cdot z'))\chi(sx\cdot(-y-z+y'+z')).
\end{aligned}$$

Then by the properties of the character χ, we have

$$\begin{aligned}
&= (q-1)|E| \sum_{s\neq 0} \sum_{\substack{y,z,y',z'\in E \\ y+z=y'+z'}} \chi(s(y\cdot z - y'\cdot z')) \\
&\leq (q-1)|E| \sum_{s\in \mathbb{F}_q} \sum_{\substack{y,z,y',z'\in E \\ y+z=y'+z'}} \chi(s(y\cdot z - y'\cdot z')) \\
&= q(q-1)|E| \sum_{\substack{y,z,y',z'\in E \\ y+z=y'+z' \\ y\cdot z=y'\cdot z'}} 1.
\end{aligned}$$

Then by Lemma 2,

$$q(q-1)|E| \sum_{\substack{y,z,y',z'\in E \\ y+z=y'+z' \\ y\cdot z=y'\cdot z'}} 1 \leq q(q-1)|E|^3(2q+1) \leq 2q^3|E|^3.$$

Hence the second term is bounded above by $2^{\frac{1}{2}} q^{\frac{3}{2}} |E|^{\frac{3}{2}}$, and so we write

$$|D(E)| = q^{-1}|E|^3 + \theta q^{\frac{3}{2}} |E|^{\frac{3}{2}}.$$

where $|\theta| < 2^{1/2}$. It follows from direct computation that the first term exceeds the second if $|E| > 2^{\frac{1}{3}} q^{\frac{5}{3}}$. Now if $q \equiv 3 \pmod 4$, Lemma 2 instead yields

$$q(q-1)|E| \sum_{\substack{y,z,y',z' \in E \\ y+z=y'+z' \\ y \cdot z = y' \cdot z'}} 1 \leq q(q-1)|E|^3(q+2) = (q^3+q^2-2q)|E|^3.$$

Hence the second term is bounded by $q^{\frac{3}{2}}|E|^{\frac{3}{2}}(1+o(1))$. Hence the first term exceeds the second when $q^{-1}|E|^3 > q^{\frac{3}{2}}|E|^{\frac{3}{2}}(1+o(1))$, i.e. when

$$|E| > q^{\frac{5}{3}}(1+o(1)).$$

This concludes the proof of Theorem 2. □

4. Discrepancies

4.1. **Statement of Results.** A hyperplane in $\mathbb{F}_q^d$ is a set of the form $\{x \in \mathbb{F}_q^d : x \cdot m = t\}$ for some $t \in \mathbb{F}_q$ and some nonzero $m \in \mathbb{F}_q^d$. A sphere in $\mathbb{F}_q^d$ is a set in the form $\{x \in \mathbb{F}_q^d : \|x\| + x \cdot m = t\}$ for some $t \in \mathbb{F}_q$ and $m \in \mathbb{F}_q^d$. Let $\mathscr{H}(\mathbb{F}_q^d)$ denote the set of all hyperplanes in $\mathbb{F}_q^d$. We will write $\mathscr{H} = \mathscr{H}(\mathbb{F}_q^d)$ if it is clear that we are referring to the space $\mathbb{F}_q^d$. Similarly, we define $\mathscr{S} = \mathscr{S}(\mathbb{F}_q^d)$ to be the set of all spheres and hyperplanes in $\mathbb{F}_q^d$. We now state our primary result.

Theorem 3. *Let $E \subset \mathbb{F}_q^d$ and let $\mathscr{D}_E(H) = |E \cap H| - q^{-1}|E|$ for each $H \in \mathscr{H}$. Then*

$$\sup_{H \in \mathscr{H}} |\mathscr{D}_E(H)| \geq q^{-1/2}|E|^{1/2}(1-q^{-d}|E|)^{1/2}(1+O(q^{-\frac{1}{2}})).$$

It follows that if $|E| \ll q^d$, then the lower bound becomes $q^{-1/2}|E|^{1/2}(1+O(q^{-1/2}))$.

The above theorem tells us something about the distribution of points on each hyperplane. Suppose that we have $|\mathscr{H}|$ slots, and $|E||V(\mathbb{F}_q^d)|$ points to assign randomly to each slot, the same number we get when we sum up $|E \cap H|$ over the $H \in \mathscr{H}$. The "square root principle" tells us that each slot will have about $|E|/q$ points, plus or minus something akin to $q^{-1/2}|E|^{1/2}$. Theorem 3, however, tells us that there will always be a plane with - roughly - a higher deviation than $q^{-1/2}|E|^{1/2}$ from the mean. In fact, it tells us if $|E \cap H|$ is very close to $|E|/q$ for many planes, then there must be a plane with a high deviation from the mean.

If we let $\mathscr{D}_E(S) = |E \cap S| - q^{-1}|E|$ for each $S \in \mathscr{S}$, we have the following corollary.

Corollary 1. *Let $E \subset \mathbb{F}_q^d$. Then*

$$\sup_{S \in \mathscr{S}} |\mathscr{D}_E(S)| \geq q^{-1/2}|E|^{1/2}(1+o(1)).$$

The corollary follows trivially from Theorem 3 if $|E| \ll q^d$ since $\mathscr{H} \subset \mathscr{S}$. The corollary is nontrivial only if $|E| \gtrsim q^d$, in which case $\sup_{S\in\mathscr{S}} |\mathscr{D}_E(S)| \geq q^{-1/2}|E|^{1/2}(1+o(1))$ may be significantly larger than $\sup_{H\in\mathscr{H}} |\mathscr{D}_E(H)|$.

4.2. **Proof of Theorem 3.**

Definition 2. *We say that V is a* direction set *of a space $\mathbb{F}_q^d$ if for each nonzero vector $x \in \mathbb{F}_q^d$, there exists a unique $v \in V$ such that $\lambda v = x$ for some $\lambda \in \mathbb{F}_q$. For each q and d, we fix a direction set denoted by $V(\mathbb{F}_q^d)$.*

In the following proposition, we construct each $V(\mathbb{F}_q^d)$ inductively on d. In the process, we will determine the size of $V(\mathbb{F}_q^d)$.

Proposition 3. *There exists a direction set V of $\mathbb{F}_q^d$ for each q and d, and $|V| = (q^d-1)/(q-1)$.*

Proof. We prove the size of V first. Suppose that V is a direction set of $\mathbb{F}_q^d$. Then since each nonzero element in $\mathbb{F}_q^d$ is uniquely expressed as λv for some nonzero $\lambda \in \mathbb{F}_q$ and $v \in V$, we have $(q-1)|V| = |\mathbb{F}_q^d \setminus \{0\}| = q^d - 1$.

We prove that a direction set V exists for each $\mathbb{F}_q^d$ by induction on d. Clearly, $V = \{1\}$ is a direction set for $\mathbb{F}_q^1$. Assume now that V is a direction set for $\mathbb{F}_q^d$. Let

$$V' = (\mathbb{F}_q^d \times \{1\}) \cup (V \times \{0\}).$$

Suppose $(x, x_{d+1}) \in \mathbb{F}_q^d \times \mathbb{F}_q$ is nonzero. Suppose $x_{d+1} = 0$ and $x \neq 0$, in which case by the inductive hypothesis there exists a unique $v \in V$ and λ such that $x = \lambda v$, from which we obtain $\lambda(v, 0) = (x, x_{d+1})$, where $(v, 0) \in V'$. If $x_{d+1} \neq 0$, then $(x_{d+1}^{-1}x, 1) \in V'$ and $(x, x_{d+1}) = x_{d+1}(x_{d+1}^{-1}x, 1)$. Moreover, $(x_{d+1}^{-1}x, 1)$ is the only point in $\mathbb{F}_q^d \times \{1\}$ which can be scaled to (x, x_{d+1}). Hence, V' is a direction set for $\mathbb{F}_q^{d+1}$. □

Proposition 4. *Each hyperplane $H \in \mathscr{H}(\mathbb{F}_q^d)$ is uniquely expressible as $H_{v,t} \equiv \{x \in \mathbb{F}_q^d : x \cdot v = 1\}$ where $v \in V(\mathbb{F}_q^d)$ and $t \in \mathbb{F}_q$. It follows that $|\mathscr{H}(\mathbb{F}_q^d)| = q|V(\mathbb{F}_q^d)|$.*

Proof. We will show that the map

$$\begin{aligned} \mathbb{F}_q \times V(\mathbb{F}_q) &\to \mathscr{H} \\ (v, t) &\mapsto H_{v,t} \end{aligned}$$

is a bijection. To show that the map is one-to-one, let $v_1, v_2 \in V(\mathbb{F}_q^d)$ and $t_1, t_2 \in \mathbb{F}_q$ such that $H_{v_1,t_1} = H_{v_2,t_2}$. Then by definition of the hyperplane, $x \cdot v_1 = t_1$ and $x \cdot v_2 = t_2$ have the same solution set. Now pick any x_0 in H_{v_1,t_1}, then $H_{v_1,t_1} - x_0 = H_{v_1,0}$ and $H_{v_2,t_2} - x_0 = H_{v_2,0}$. Then $x \cdot v_1 = 0$ and $x \cdot v_2 = 0$ have the same solution set, and so $v_1 = \lambda v_2$. But then $v_1 = v_2$. Now $t_1 = x_0 \cdot v_1 = x_0 \cdot v_2 = t_2$. Hence the map is one-to-one.

To show that the map is onto, we recall that every $H \in \mathscr{H}$ can be written as $\{x \in \mathbb{F}_q^d : x \cdot m = s\}$ for some $s \in \mathbb{F}_q$ and nonzero m in $\mathbb{F}_q^d$. Then there exist unique $v \in V(\mathbb{F}_q^d)$ and $\lambda \in \mathbb{F}_q \setminus \{0\}$ such that $m = \lambda v$. Then we write

$$\begin{aligned}\{x \in \mathbb{F}_q^d : x \cdot m = s\} &= \{x \in \mathbb{F}_q^d : x \cdot \lambda v = s\} \\ &= \{x \in \mathbb{F}_q^d : x \cdot v = \lambda^{-1} s\} \\ &= H_{v,\lambda^{-1}s}.\end{aligned}$$

□

The thrust of the proof of Theorem 3 comes from the following lemma, which is interesting in its own right. It states that the l^2 norm of the size of the intersection $|E \cap H|$ over $H \in \mathscr{H}$ only depends on the size of E, as opposed to its structure. Hence, it is a very useful tool for when trying to find a lower bound on the maximum discrepancy $\sup_{H \in \mathscr{H}} |\mathscr{D}_E(H)|$ of E when nothing about the structure of E is assumed.

Lemma 3. *Let $E \subset \mathbb{F}_q^d$. Then*

$$\sum_{H \in \mathscr{H}} |E \cap H|^2 = q^{d-1}|E| + q^{-1}(|V(\mathbb{F}_q^d)| - 1)|E|^2.$$

We conclude that

$$\sum_{H \in \mathscr{H}} |\mathscr{D}_E(H)|^2 = q^{-1}|E|(q^d - |E|).$$

Proof. We have by the above proposition,

$$\begin{aligned}
\sum_{H\in\mathscr{H}} |E\cap H|^2 &= \sum_{\substack{v\in V(\mathbb{F}_q^d)\\ t\in\mathbb{F}_q}} |E\cap H_{v,t}|^2 \\
&= \sum_{\substack{v\in V(\mathbb{F}_q^d)\\ t\in\mathbb{F}_q}} \left| q^{-1}\sum_{x\in\mathbb{F}_q^d} E(x)\sum_{s\in\mathbb{F}_q}\chi(s(t-x\cdot v))\right|^2 \\
&= q^{-2}\sum_{\substack{v\in V(\mathbb{F}_q^d)\\ t\in\mathbb{F}_q}}\sum_{\substack{x,x'\in\mathbb{F}_q^d\\ s,s'\in\mathbb{F}_q}} E(x)E(x')\chi((s-s')t)\chi((-sx+s'x')\cdot v) \\
&= q^{-1}\sum_{v\in V(\mathbb{F}_q^d)}\sum_{\substack{x,x'\in\mathbb{F}_q^d\\ s\in\mathbb{F}_q}} E(x)E(x')\chi(s(-x+x')\cdot v) \\
&= q^{2d-1}\sum_{\substack{v\in V(\mathbb{F}_q^d)\\ s\in\mathbb{F}_q}} \left| q^{-d}\sum_{x\in\mathbb{F}_q^d} E(x)\chi(-sx\cdot v)\right|^2 \\
&= q^{2d-1}\sum_{\substack{v\in V(\mathbb{F}_q^d)\\ s\in\mathbb{F}_q}} |\hat{E}(sv)|^2 \\
&= q^{2d-1}\sum_{\substack{v\in V(\mathbb{F}_q^d)\\ s\in\mathbb{F}_q^*}} |\hat{E}(sv)|^2 + q^{2d-1}\sum_{v\in V(\mathbb{F}_q^d)} |\hat{E}(0)|^2.
\end{aligned}$$

Since $V(\mathbb{F}_q^d)$ is a direction set, we have

$$\begin{aligned}
&= q^{2d-1}\sum_{m\in\mathbb{F}_q^d\setminus\{0\}} |\hat{E}(m)|^2 + q^{-1}|V(\mathbb{F}_q^d)||E|^2 \\
&= q^{2d-1}\sum_{m\in\mathbb{F}_q^d} |\hat{E}(m)|^2 - q^{2d-1}|\hat{E}(0)|^2 + q^{-1}|V(\mathbb{F}_q^d)||E|^2.
\end{aligned}$$

Then by Parseval's formula,

$$\begin{aligned}
&= q^{d-1}\sum_{x\in\mathbb{F}_q^d} |E(x)|^2 - q^{-1}|E|^2 + q^{-1}|V(\mathbb{F}_q^d)||E|^2 \\
&= q^{d-1}|E| + q^{-1}(|V(\mathbb{F}_q^d)|-1)|E|^2.
\end{aligned}$$

Hence $\sum_{H\in\mathscr{H}}|E\cap H|^2 = q^{d-1}|E| + q^{-1}(|V(\mathbb{F}_q^d)|-1)|E|^2$. Applying this formula to $\sum_{H\in\mathscr{H}}|\mathscr{D}_E(H)|^2$ yields

$$\begin{aligned}\sum_{H\in\mathscr{H}}|\mathscr{D}_E(H)|^2 &= \sum_{\substack{v\in D(\mathbb{F}_q^d)\\ t\in\mathbb{F}_q}}(|E\cap H_{v,t}| - q^{-1}|E|)^2\\ &= \sum_{\substack{v\in D(\mathbb{F}_q^d)\\ t\in\mathbb{F}_q}}(|E\cap H_{v,t}|^2 - 2q^{-1}|E||E\cap H_{v,t}| + q^{-2}|E|^2)\\ &= q^{d-1}|E| + q^{-1}(|D(\mathbb{F}_q^d)|-1)|E|^2 - 2q^{-1}|D(\mathbb{F}_q^d)||E|^2 + q^{-1}|D(\mathbb{F}_q^d)||E|^2\\ &= q^{d-1}|E| - q^{-1}|E|^2\\ &= q^{-1}|E|(q^d - |E|),\end{aligned}$$

as desired. □

We now proceed with the proof of Theorem 3 below.

Proof. Suppose $M \geq |\mathscr{D}_E(H)|$ for each $H\in\mathscr{H}$. Then by Proposition 4 and Lemma 3,

$$q^{-1}|E|(q^d-|E|) = \sum_{H\in\mathscr{H}}|\mathscr{D}_E(H)|^2 \leq M^2|\mathscr{H}| = M^2q(q^d-1)(q-1)^{-1}.$$

Hence

$$M^2 \geq q^{-1}|E|(1-q^{-d}|E|)\frac{1-q^{-1}}{1-q^{-d}}.$$

Now

$$\left|1-\frac{1-q^{-1}}{1-q^{-d}}\right| = \left|\frac{-q^{-d}+q^{-1}}{1-q^{-d}}\right| \leq q^{-1},$$

so we have

$$M \geq q^{-\frac{1}{2}}|E|^{\frac{1}{2}}(1-q^{-d}|E|)^{\frac{1}{2}}(1+O(q^{-1}))^{\frac{1}{2}} = q^{-\frac{1}{2}}|E|^{\frac{1}{2}}(1-q^{-d}|E|)^{\frac{1}{2}}(1+O(q^{-\frac{1}{2}})).$$

Hence

$$\sup_{H\in\mathscr{H}}|\mathscr{D}_E(H)| \geq q^{-\frac{1}{2}}|E|^{\frac{1}{2}}(1-q^{-d}|E|)^{\frac{1}{2}}(1+O(q^{-\frac{1}{2}}))$$

as desired. □

We now prepare to prove the corollary to Theorem 3. Let $P(\mathbb{F}_q^{d+1})$ denote the paraboloid $\{(x,\|x\|)\in\mathbb{F}_q^d\times\mathbb{F}_q : x\in\mathbb{F}_q^d\}$. As for hyperplanes and spheres, we may suppress the dependence on $\mathbb{F}_q^{d+1}$ in the notation if it is clear from context.

Proposition 5. *Let $\pi : \mathbb{F}_q^{d+1} \to \mathbb{F}_q^d$ be the projection given by $\pi(x_1, \ldots, x_{d+1}) = (x_1, \ldots, x_d)$ for each $(x_1, \ldots, x_{d+1}) \in \mathbb{F}_q^{d+1}$. π gives a natural bijective correspondence between $\mathscr{H}(\mathbb{F}_q^{d+1})$ and $\mathscr{S}(\mathbb{F}_q^d)$ given by*

$$\bar{\pi} : \{H \cap P(\mathbb{F}_q^{d+1}) : H \in \mathscr{H}(\mathbb{F}_q^{d+1})\} \to \mathscr{S}(\mathbb{F}_q^d)$$
$$\{(x, \|x\|) \in \mathbb{F}_q^{d+1} : (x, \|x\|) \cdot (v, v_{d+1}) = t\} \mapsto \{x \in \mathbb{F}_q^d : v_{d+1}\|x\| + v \cdot x = t\}.$$

Proof. Since the restriction $\pi|_{P(\mathbb{F}_q^{d+1})} : P(\mathbb{F}_q^{d+1}) \to \mathbb{F}_q^d$ is a bijection, the map $\bar{\pi}$ is injective. It remains to show that $\bar{\pi}$ is surjective. Note that for each $H_{m,s} \in \mathscr{S}(\mathbb{F}_q^d)$, we have $\bar{\pi}(H_{(m,0),s} \cap P(\mathbb{F}_q^{d+1})) = H_{m,s}$. Now if we have a sphere

$$\{x \in \mathbb{F}_q^d : \|x\| + m \cdot x = s\} \in \mathscr{S}(\mathbb{F}_q^d),$$

Then

$$\begin{aligned}\bar{\pi}\{H_{(m,1),s} \cap P(\mathbb{F}_q^{d+1})\} &= \bar{\pi}\{(x, \|x\|) \in \mathbb{F}_q^{d+1} : (x, \|x\|) \cdot (m, 1) = s\} \\ &= \{\pi(x, \|x\|) : \|x\| + m \cdot x = s\} \\ &= \{x \in \mathbb{F}_q^d : \|x\| + m \cdot x = s\} \\ &= H_{m,s}.\end{aligned}$$

□

We now prove Corollary 1.

Proof. Let $E \subset \mathbb{F}_q^d$. Then consider the set $E' \subset \mathbb{F}_q^{d+1}$ given by $E' = (\pi|_{P(\mathbb{F}_q^{d+1})})^{-1}(E)$. Then since $|E'| \leq q^d \ll q^{d+1}$, by Theorem 3,

$$\begin{aligned}\sup_{H \in \mathscr{H}(\mathbb{F}_q^{d+1})} |\mathscr{D}_{E'}(H)| &\geq (1 + o(1))q^{-1/2}|E'|^{1/2} \\ &= (1 + o(1))q^{-1/2}|E|^{1/2}.\end{aligned}$$

Now if $H \in \mathscr{H}(\mathbb{F}_q^{d+1})$, let $S = \bar{\pi}(H \cap P(\mathbb{F}_q^{d+1}))$. Then

$$\pi(E' \cap H) = E \cap S.$$

Then since $\pi|_{P(\mathbb{F}_q^{d+1})}$ is bijective,

$$|E' \cap H| = |E \cap S|,$$

and so

$$|\mathscr{D}_{E'}(H)| = ||E' \cap H| - q^{-1}|E|| = ||E \cap S| - q^{-1}|E|| = |\mathscr{D}_E(S)|.$$

Then by Proposition 5,

$$\sup_{S \in \mathscr{S}} |\mathscr{D}_E(S)| = \sup_{H \in \mathscr{H}} |\mathscr{D}_{E'}(H)| \geq (1 + o(1))q^{-1/2}|E|^{1/2}.$$

□

References

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

[2] J. Pach, and P. Agarwal *Combinatorial geometry* Wiley-Interscience Series in Discrete Mathematics and Optimization. A Wiley-Interscience Publication. John Wiley and Sons, Inc., New York (1995).

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

[4] J. Chapman, M. Burak Erdoğan, D. Hart, A. Iosevich, D. Koh. *Pinned distance sets, k-simplices, Wolff's exponent in finite fields and sum-product estimates.* arXiv:0903.4218v2 [math.CO] 26 Mar 2009.

[5] D. Covert, D. Hart, A. Iosevich, D. Koh and M. Rudnev, *Generalized incidence theorems, homogeneous forms and sum-product estimates in finite fields*, European J. of Combinatorics 31, 2010, 306-319.

[6] D. Hart *Explorations of geometric combinatorics in vector spaces over finite fields.*

[7] D. Hart and A. Iosevich *Sums and products in finite fields: an integral geometric viewpoint*, Radon transforms, geometry, and wavelets, 129?135, Contemp. Math., **464**, Amer. Math. Soc., Providence, RI, (2008).

[8] 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), no. 6, 3255-3275.

[9] D. Hart, A. Iosevich. *Ubiquity of simplices in subsets of vector spaces over finite fields.* arXiv:math/0703504v2 [math.CA] 11 Oct 2007.

[10] A. Iosevich and M. Rudnev. *Erdös distance problem in vector spaces over finite fields.*

[11] A. Iosevich, M. Rudnev, Y. Zhai. *Areas of triangles and Beck's theorem in planes over finite fields.* arXiv:1205.0107v1 [math.CO] 1 May 2012.

[12] N. Katz and T. Tao, *Bounds on arithmetic projections, and applications to the Kakeya conjecture*, Math. Res. Lett. **6** (1999), no. 5-6, 625?630.

[13] J. Matousek *Lectures on Discrete Geometry* Graduate Texts in Mathematics, Springer **202** (2002).

[14] K. F. Roth, *On irregularities of distribution*, Mathematika 1 (1954), 73-79.

[15] E. Szemerédi, W. T. Trotter. *Extremal problems in discrete geometry.* Combinatorica 3, (1983) 381–392.

[16] T. Tao and V. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics, **105**. Cambridge University Press, Cambridge, (2010).

[17] P. Ungar. $2N$ *noncollinear points determine at least* $2N$ *directions.* J. Combin. Theory Ser. A **33** (1982), no. 3, 343-?347.

[18] 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.

[19] L. A. Vinh, *Right triangles in point sets over finite fields.*

[20] L. A. Vinh, *Distinct triangle areas in a planar point set over finite fields.*