Annales Fennici Mathematici
Volumen 50, 2025, 467–481

# Exceptional set estimates in finite fields

Paige Bright and Shengwen Gan

**Abstract.** We study the exceptional set estimate for projections in $\mathbb{F}_q^n$. For each $V \in G(k, \mathbb{F}_q^n)$, let

$$\pi_V : \mathbb{F}_q^n \to V$$

be the projection map. We prove the following result: If $A \subset \mathbb{F}_q^n$ with $\#A = q^a$ $(n-1 \le a \le n)$ and $0 < s < \frac{a+n-2}{2}$, then

$$\#\{V \in G(n-1, \mathbb{F}_q^n) : \#\pi_V(A) < q^s\} \lessapprox q^{n-2}.$$

This improves the previous range $0 < s < \frac{n-1}{n}a$. Also, our range of $s$ is sharp in the sense that if $s > \frac{a+n-2}{2}$, then the right hand side above should be at least $q^t$ for some $t > n-2$.

**Äärellisten kuntien poikkeusjoukkojen arvioita**

**Tiivistelmä.** Tässä tutkimuksessa arvioidaan avaruuden $\mathbb{F}_q^n$ projektioiden poikkeusjoukkoja. Merkitään kutakin aliavaruutta $V \in G(k, \mathbb{F}_q^n)$ vastaavaa projektiota

$$\pi_V : \mathbb{F}_q^n \to V.$$

Työssä todistetaan seuraava tulos: Jos joukko $A \subset \mathbb{F}_q^n$ sisältää $\#A = q^a$ alkiota $(n-1 \le a \le n)$ ja $0 < s < \frac{a+n-2}{2}$, niin

$$\#\{V \in G(n-1, \mathbb{F}_q^n) : \#\pi_V(A) < q^s\} \lessapprox q^{n-2}.$$

Tämä parantaa aiempaa arvoväliä $0 < s < \frac{n-1}{n}a$. Lisäksi uusi arvoväli on siinä mielessä tarkka, että jos $s > \frac{a+n-2}{2}$, niin edellisen kaavan oikean puolen täytyy olla vähintään $q^t$ jollakin $t > n-2$.

## 1. Introduction

Let $p$ be a prime number and $q = p^r$. The goal of this paper is to study exceptional set estimates over the finite field $\mathbb{F}_q^n$. For any subspace $V \subset \mathbb{F}_q^n$, we can define the orthogonal projection

$$\pi_V : \mathbb{F}_q^n \to V$$

in the natural way. (For precise statement, see Definition 2.3.)

**Definition 1.1.** (Exceptional set in finite field) For $A \subset \mathbb{F}_q^n$ and a number $s > 0$, we define the $s$-exceptional set of $A$ for projection onto $k$-planes to be

$$E_s(A) := \{V \in G(k, \mathbb{F}_q^n) : \#\pi_V(A) < q^s\}. \tag{1.1}$$

**Remark 1.2.** One should think of $E_s(A) = E_s^{n,k}(A)$ depends on another two parameters: the ambient dimension $n$, and the dimension of the planes where $A$ is projected onto, $k$. For simplicity, since $n, k$ will be clear from context, we drop the $n, k$ from our notation.

We record known results as follows: Let $A \subset \mathbb{F}_q^n$ be a set with $\#A = q^a$ $(0 < a < n)$. For $s \in (0, \min\{a, k\})$, we have the following estimates:

(i) $\#E_s(A) \lesssim q^{k(n-k)+s-k}$;

https://doi.org/10.54330/afm.163667
2020 Mathematics Subject Classification: Primary 28A75, 28A78.
Key words: Projection theory, exceptional set estimate.

(ii) $\#E_s(A) \lesssim q^{\max\{k(n-k)+s-a,0\}}$.
(iii) $\#E_s(A) \lesssim_{n,k,a,s,\epsilon} q^{\epsilon+k(n-k)-1}$ if $s < \frac{k}{n}a$.

**Remark 1.3.** The three estimates were first proved in the Euclidean setting. The first estimate is known as the Kaufman-type estimate [5]. The second estimate is known as the Falconer-type estimate [2]. The Falconer-type estimate was also proved by Peres and Schlag [10]. The third estimate is due to He [4].

In the finite field setting, the first two estimates are obtained by Chen [1, Theorem 1.2]. The third did not appear in any reference. However, we believe that it can be proved by adapting He's proof [4]. For the most recent results, see [6].

**1.1. Motivation.** We first consider a special case when $n = 3$, $k = 2$ and $A \subset \mathbb{F}_q^3$ with $\#A \sim q^2$. Both 1 and 1 imply that

$$\#E_s(A) \lesssim q^s. \tag{1.2}$$

This estimate is sharp when $s \to 1^+$. The example is when $A = \mathbb{F}_q^2 \times \{0\}$. For such $A$ and $1 < s < 2$, we see that $E_s(A) = \{V \in G(2, \mathbb{F}_q^3)\colon V \text{ parallel to } (0,0,1)\}$, which has cardinality $\sim q$. When $s$ is essentially bigger than 1, the example does not match the upper bound in (1.2), so we suspect (1.2) is not sharp when $s > 1$. In fact, 1 shows that

$$\#E_{\frac{4}{3}}(A) \lesssim_\epsilon q^{1+\epsilon}$$

for any $\epsilon > 0$.

We begin to think about the following question. Suppose we consider the case $n = 3, k = 2$. What is the largest $s$, so that for any $\#A = q^2$,

$$\#E_s(A) \lesssim_\epsilon q^{1+\epsilon}?$$

In this paper, we will show that this largest $s$ is $\frac{3}{2}$. We will prove a general theorem (Theorem 1.4) for all the dimensions. We will also discuss the obstruction to generalize the finite field version to $\mathbb{R}^n$ at the end of the paper.

**1.2. Main results.** Next, we state our main theorem.

**Theorem 1.4.** *Let $A \subset \mathbb{F}_q^n$ be a set with $\#A = q^a$ $(0 < a < n)$. Then for $0 < s < \frac{a+2k-n}{2}$, we have*

$$\#\{V \in G(k, \mathbb{F}_q^n)\colon \#\pi_V(A) < q^s\} \le C_{n,k,a,s} \cdot \log q \cdot q^{t(a,s)}, \tag{1.3}$$

*where $t(a,s) = \max\{k(n-k) + 2(s-a), (k-1)(n-k)\}$. Here, $C_{n,k,a,s}$ is a constant that may depend on $n, k, a, s$, but not depend on $q$.*

In the theorem, one particularly interesting case is when $k = n - 1$, $a \ge n - 1$ and $s > a - 1$. This range of parameters is our motivation to work on this project, so we would like to also state the theorem for this specific range of parameters.

**Theorem 1.5.** *Let $A \subset \mathbb{F}_q^n$ be a set with $\#A = q^a$ $(n - 1 \le a < n)$. Then for $0 < s < \frac{a+n-2}{2}$, we have*

$$\#\{V \in G(n-1, \mathbb{F}_q^n)\colon \#\pi_V(A) < q^s\} \lesssim C_{n,a,s} \cdot \log q \cdot q^{n-2}. \tag{1.4}$$

**Remark 1.6.** We will discuss how sharp our estimate (1.4) is. For fixed $n$ and $a \in [n-1, n)$, we would like to find pairs $(s, t)$ so that

$$\#\{V \in G(n-1, \mathbb{F}_q^n)\colon \#\pi_V(A) < q^s\} \lessapprox q^t$$

holds for any $\#A = q^a$. Here, $X \lessapprox Y$ means $X \lesssim_\epsilon q^\epsilon Y$ for any $\epsilon > 0$.

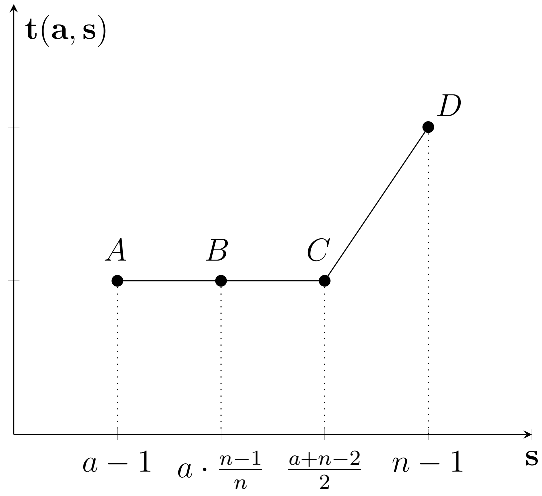


Figure 1. The range of $t$ when $k=n-1$, $a\geq n-1$ and $s>a-1$.

We draw those points $(s,t)$ in Figure 1: The three points $A,B,C$ have the same ordinate $n-2$ and the respective abscissas indicated in the figure; the point $D$ has the coordinate $(n-1,2(n-1)-a)$; the line segment $C-D$ is given by equation $t=t(a,s)=2s-a$. We will construct examples in Section 3 to show that the necessary condition for (1.3) to hold is when $(s,t(a,s))$ lies above the graph $A-B-C-D$. The estimate 1 above Remark 1.3 indicates that a sufficient condition for (1.3) to hold is when $(s,t(a,s))$ lies above $A-B$. Our Theorem 1.5 extends 1 by showing that (1.3) holds when $(s,t(a,s))$ lies above $A-B-C$. We see that our theorem finds the optimal range of $s$ for which $t(a,s)$ could be $n-2$.

We discuss the new ingredients in this paper. The first new ingredient is a refined Falconer-type estimate (see Lemma 4.8). This is a refined version of 1. See Remark 4.9. The second new ingredient is a slicing argument, which is discussed in Section 5.

We talk about the structure of the paper. In Section 3, we talk about some examples. In Section 4, we briefly review the Fourier transform in finite fields. In Section 5, we prove Theorem 1.4.

*Acknowledgement.* We would like to thank Prof. Larry Guth for numerous helpful discussions over the course of this project.

## 2. Definition of the orthogonal projections

Let $p$ be a prime number and $q=p^r$. The goal of this paper is to study the estimates of the exceptional set in a finite field $\mathbb{F}_q^n$. We first note that $\mathbb{F}_q^n$ is equipped with a natural nondegenerate bilinear form $\mathbb{F}_q^n\times\mathbb{F}_q^n\to\mathbb{F}_q$ given by

$$x\cdot y:=x_1y_1+\cdots+x_ny_n\quad\text{for } x,y\in\mathbb{F}_q^n.$$

We remark that this bilinear form is not necessarily an inner product. For example, if $n=p$ and $x=(1,\dots,1)\in\mathbb{F}_q^p$, then $x\cdot x=0$. However, we can still use this bilinear form to define "orthogonality", even though some nonzero vectors may be orthogonal to itself.

**Definition 2.1.** We say that two vectors $x,y\in\mathbb{F}_q^n$ are orthogonal, denoted by $x\perp y$, if $x\cdot y=0$. For $V\subset\mathbb{F}_q^n$ being a $k$-dimensional subspace whose directions are spanned by the vectors $v_1,\dots,v_k$, we say $x$ is orthogonal to $V$, denoted by $x\perp V$, if

$x \perp v_1, \dots, v_k$. We also define the orthogonal complement of $V$ to be

$$V^\perp := \{x \in \mathbb{F}_q^n \colon x \perp V\}.$$

**Remark 2.2.** By linear algebra, we see that $V^\perp$ is an $(n-k)$-dimensional subspace. Later we will see that $V^\perp$ is exactly the dual of $V$, see Definition 4.4.

Since in $\mathbb{F}_q^n$ some vector may be orthogonal to itself, we need a slightly trickier definition of the orthogonal projection. Recall that for $V \in G(k, \mathbb{R}^n)$, $\pi_V \colon \mathbb{R}^n \to V$ is the orthogonal projection on $V$. We can also identify $\pi_V$ as the map

$$\mathbb{R}^n \to A(n-k, \mathbb{R}^n), \tag{2.1}$$

so that $\pi_V(x)$ is the unique $(n-k)$-dimensional plane that is parallel to $V^\perp$ and passes through $x$. This motivates the definition of projection in finite fields.

**Definition 2.3.** Let $\mathbb{F}_q$ be a finite field. Denote the $k$-dimensional subspaces and the $k$-dimensional affine subspaces of $\mathbb{F}_q^n$ by $G(k, \mathbb{F}_q^n)$ and $A(k, \mathbb{F}_q^n)$, respectively. For $V \in G(k, \mathbb{F}_q^n)$, define

$$\pi_V \colon \mathbb{F}_q^n \to A(n-k, \mathbb{F}_q^n), \tag{2.2}$$

so that $\pi_V(x)$ is the unique element in $A(n-k, \mathbb{F}_q^n)$ that is parallel to $V^\perp$ and passes through $x$.

## 3. Examples of the exceptional sets in the prime field

We discuss some examples of exceptional sets. In $\mathbb{R}^2$, it is conjectured that (see Section 5.4 in [7]):

**Conjecture 3.1.** *Let $A \subset \mathbb{R}^2$ be with $\dim(A) = a$. For $\theta \in G(1, \mathbb{R}^2)$, let $\pi_\theta \colon \mathbb{R}^2 \to \theta$ be the orthogonal projection on the line $\theta$. For $0 < s < \max\{1, a\}$, define $E_s(A) := \{\theta : \dim(\pi_\theta(A)) < s\}$. Then*

$$\dim(E_s(A)) \le \max\{0, 2s - a\}.$$

Of course, we can also ask the question in $\mathbb{F}_p^2$:

**Conjecture 3.2.** *Let $A \subset \mathbb{F}_p^2$ be with $\#A = p^a$. For $0 < s < \max\{1, a\}$, define $E_s(A)$ as in (1.1) with $n = 2$, $k = 1$. Then*

$$\#E_s(A) \le C_{\epsilon,a,s} p^{\epsilon + \max\{0, 2s-a\}}. \tag{3.1}$$

**Remark 3.3.** Conjecture 3.1 was recently resolved by Orponen–Shmerkin [9] and Ren–Wang [11]. However, its finite field analogue (Conjecture 3.2) is still open. Another remarkable thing is that (3.1) is not true over $\mathbb{F}_q$ for prime powers $q$ due to the existence of the subfield (see the Introduction of [6]). The existence of the subfield causes the Szemerédi–Trotter theorem to fail in $\mathbb{F}_q^2$ (see the Introduction of [8]). However, it is reasonable to believe (3.1) is true over prime fields.

We show that the upper bound in (3.1) can be attained.

**Example 3.4.** Let $p$ be a large prime. We assume $\frac{a}{2} < s < \max\{1, a\}$, $a < 2$. Consider a set of lines $\mathcal{L} = \{l_{k,m} \colon |k| \le p^{2s-a}, |m| \le 10p^s\}$ in $\mathbb{F}_p^2$. Here, $k$ and $m$ are integers and $l_{k,m}$ is given by

$$l_{k.m} \colon y = kx + m.$$

We used the convention that if an integer $m$ satisfies $|m| < p/2$, then $m$ can be naturally viewed as an element in $\mathbb{F}_p$. Hence, the $l_{k,m}$ defined above is a line in $\mathbb{F}_p^2$.

We see that $\mathcal{L}$ consists of lines from $\sim p^{2s-a}$ many directions, and in each of these directions there are $\sim p^s$ many lines. We denote these directions by $E$, and for $\theta \in E$, let $\mathcal{L}_\theta$ be the lines in $\mathcal{L}$ that are in direction $\theta$.

Consider the set $A := \{(x,y) \in \mathbb{F}_p^2 \colon |x| \le p^{a-s}, |y| \le p^s\}$. For any $|k| \le p^{2s-a}$, we see that every $(x,y) \in A$ satisfies $|y - kx| \le 10p^s$. This means that for any direction $\theta \in E$, $A$ is covered by $\mathcal{L}_\theta$. Therefore we have for each $\theta \in E$,

$$\#\pi_\theta(A) \le \#\mathcal{L}_\theta \lesssim p^s.$$

We obtain the following estimate:

$$\#\{\theta \colon \#\pi_\theta(A) \lesssim p^s\} \ge \#E \sim p^{2s-a}.$$

Therefore, we showed that under the setting of Conjecture 3.2, there exists $A$ such that

$$\#E_s(A) \gtrsim p^{\max\{0,2s-a\}}.$$

From now on, we denote such sets $A$ and $E$ by $\mathbf{A}_{s,a}(\subset \mathbb{F}_p^2)$ and $\mathbf{E}_{s,a}(\subset G(1,\mathbb{F}_p^2))$. They serve as a tight example for (3.1). Later, we will use $\mathbf{A}_{s,a}$ and $\mathbf{E}_{s,a}$ as building blocks to build more examples in higher dimensions.

For simplicity, we define $t(a,s)$ to be the smallest number such that for any $A \subset \mathbb{F}_p^n$ with $\#A = p^a$,

$$\#E_s(A) \lesssim_{n,k,a,s,\epsilon} p^{\epsilon + t(a,s)},$$

for any $\epsilon > 0$. Equivalently,

$$t(a,s) = \overline{\lim_{p\to\infty}} \sup_{A \subset \mathbb{F}_p^n, \#A = p^a} \log_p(\#E_s(A)).$$

**3.1. Sharpness of Theorem 1.5.** In this subsection, we discuss how sharp our Theorem 1.5 is. Although the theorem is stated for $q$, the examples only work for prime fields. Therefore, in this subsection, we assume $q = p$.

Consider the case where $k = n-1, a \ge n-1$. Theorem 1.5 gives the bound:

$$t(a,s) \le n-2, \text{ when } s < \frac{a+n-2}{2}.$$

On the other hand, we can construct examples to show that

$$t(a,s) \ge n-2, \text{ when } a \ge n-1,\ a-1 < s < n-1.$$

In other words, we will construct $\#A \sim p^a$ so that $\#E_s(A) \gtrsim p^{n-2}$.

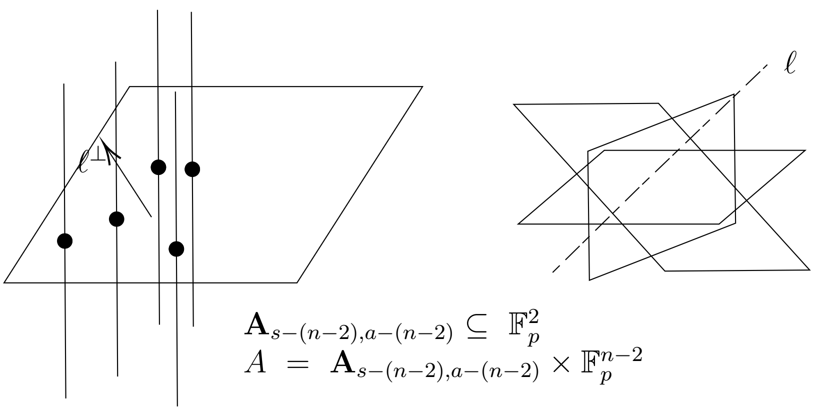


Figure 2. Projection to planes.

Let $A = \mathbb{F}_p^{n-1} \times I$ where $I \subset \mathbb{F}_p$ with $\#I = \lfloor p^{a-(n-1)} \rfloor$. We want to see what $E_s(A)$ is. For $V \in G(n-1, \mathbb{F}_p^n)$, if $(0,\ldots,0,1) \notin V$, then $\pi_V$ restricts to an isomorphism on $\mathbb{F}_p^{n-1} \times \{0\}$

$$\pi_V \colon \mathbb{F}_p^{n-1} \times \{0\} \xrightarrow{\sim} V.$$

Therefore, $\#\pi_V(A) = \#\mathbb{F}_p^{n-1} = p^{n-1} > p^s$, which implies $V \notin E_s(A)$. If $(0,\ldots,0,1) \in V$, then $\pi_V(A) = \mathbb{F}_p^{n-2} \times I$. Therefore, $\#\pi_V(A) = \#\mathbb{F}_p^{n-2} \#I \le p^{a-1} < p^s$, which implies $V \in E_s(A)$. We have $E_s(A) = \{V \in G(n-1, \mathbb{F}_p^n) \colon (0,\ldots,0,1) \in V\} \cong G(n-2, \mathbb{F}_p^{n-1})$, which implies

$$\#E_s(A) \sim p^{n-2}.$$

This shows that when $s \in (a-1, \frac{a+n-2}{2})$, in order for (1.3) to hold, $(s, t(a,s))$ must be above the graph $A-B-C$ in Figure 1.

In addition, our estimate is sharp in another sense: the range of $s$ is sharp. In fact, we show that if $s > \frac{a+n-2}{2}$, then

$$t(a,s) \ge 2s - a \ (> n-2).$$

In other words, when $s > \frac{a+n-2}{2}$, we will construct $\#A \sim p^a$ so that $\#E_s(A) \gtrsim p^{2s-a}$. This means that in order for (1.3) to hold, $(s, t(a,s))$ must be above the graph $C-D$ in Figure 1.

The proof of this part is trickier (it might be easier for the reader to first assume $n=3$). In addition, we need to use the examples in the two-dimensional case (Example 3.4). We remark that this part is the reason we need to work in a prime field.

Choose $A = \mathbf{A}_{s-(n-2),a-(n-2)} \times \mathbb{F}_p^{n-2}$ (see Figure 2). We first look at those $(n-1)$-subspaces $V$ that contain $\{(0,0)\} \times \mathbb{F}_p^{n-2}$. This $V$ can be written as $\ell \times \mathbb{F}_p^{n-2}$, where $\ell \in G(1, \mathbb{F}_p^2)$. It is not hard to see that $\pi_V(A) = \pi_\ell(\mathbf{A}_{s-(n-2),a-(n-2)}) \times \mathbb{F}_p^{n-2}$ (where we view $\pi_\ell : \mathbb{F}_p^2 \to \ell$). Therefore, we obtain

$$\#\pi_V(A) = \#\mathbb{F}_p^{n-2} \cdot \#\pi_\ell(\mathbf{A}_{s-(n-2),a-(n-2)}).$$

If $\ell \in \mathbf{E}_{s-(n-2),a-(n-2)}$, then $\#\pi_\ell(\mathbf{A}_{s-(n-2),a-(n-2)}) < p^{s-(n-2)}$, and hence

$$\#\pi_V(A) < p^s.$$

To indicate the relationship between $V$ and $\ell$, we denote $V_\ell = \ell \times \mathbb{F}_p^{n-2}$. We have shown that if $\ell \in \mathbf{E}_{s-(n-2),a-(n-2)}$ then

$$V_\ell \in E_s(A).$$

Let $\ell^\perp \subset \mathbb{F}_p^2$ be the line orthogonal to $\ell$. By abuse of notation, we also use $\ell^\perp$ to denote the vector in $\mathbb{F}_p^2$. Consider another $(n-1)$-subspace $W$ whose normal direction is of form $\ell^\perp + y$ for $y \in \{(0,0)\} \times \mathbb{F}_p^{n-2}$ (see the right hand side of Figure 2 for such $W$'s). We note that $\ell^\perp$ is the normal direction of $V_\ell$. We claim $\#\pi_{V_\ell}(A) = \#\pi_W(A)$. Note that $\#\pi_{V_l}(A)$ is the number of lines parallel to $\ell^\perp$ that are needed to cover $A$. It is equal to the number of lines parallel to $\ell^\perp + y$ that are needed to cover $A$. Based on one $V_\ell$, we find another $\sim p^{n-2}$ many $W$'s that are in $E_s(A)$. Therefore,

$$\#E_s(A) \gtrsim \#\mathbf{E}_{s-(n-2),a-(n-2)} p^{n-2} \gtrsim p^{2\left(s-(n-2)\right)-\left(a-(n-2)\right)+n-2} = p^{2s-a}.$$

## 4. Fourier transform in finite field

**4.1. Definition of Fourier transform.** We briefly introduce the Fourier transform in $\mathbb{F}_q^n$. We first set up our notation. $\mathbb{F}_q^n$ is our physical space and we use $x, y$ to denote the points in $\mathbb{F}_q^n$. The frequency space is also $\mathbb{F}_q^n$, and we use $\xi, \eta$ to denote the points there. For $x \in \mathbb{F}_q^n$ or $\xi \in \mathbb{F}_q^n$, we also write $x = (x_1, \dots, x_n)$ or $\xi = (\xi_1, \dots, \xi_n)$ in coordinate, where each $x_i$ or $\xi_i$ belongs to $\mathbb{F}_q$.

Before giving the definition of the Fourier transform, we need to introduce some notation from number theory. Recall that $q = p^r$. Define the trace map

$$\mathrm{Tr}\colon \mathbb{F}_q \to \mathbb{F}_p, \quad x \mapsto \sum_{i=0}^{r-1} x^{p^i}.$$

First, we need to explain why $\mathrm{Tr}(x) \in \mathbb{F}_p$. Let

$$\sigma\colon \mathbb{F}_q \to \mathbb{F}_q, \quad x \mapsto x^p$$

be the Frobenius map. Then we can write $\mathrm{Tr} = \sum_{i=0}^{r-1} \sigma^i$. By a fundamental fact in number theory, we know that the Galois group $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ is generated by $\sigma$. Since $\sigma(\mathrm{Tr}(x)) = \mathrm{Tr}(x)$, we see that $\mathrm{Tr}(x)$ is invariant under the Galois group, and hence $\mathrm{Tr}(x) \in \mathbb{F}_p$. Another two important properties of Tr are that Tr is $\mathbb{F}_p$ linear, i.e., $\mathrm{Tr}(x + y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$ and $\mathrm{Tr}(\lambda x) = \lambda \mathrm{Tr}(x)$ for $\lambda \in \mathbb{F}_p$.

We are ready to define the Fourier transform in $\mathbb{F}_q^n$. For a function $f(x)$ on $\mathbb{F}_q^n$, the Fourier transform of $f$ is a function on the frequency space $\mathbb{F}_q^n$ given by

$$\widehat{f}(\xi) = \sum_{x \in \mathbb{F}_q^n} f(x) e_p(-\mathrm{Tr}(x \cdot \xi)).$$

Here, $e_p(x) = e^{\frac{2\pi i x}{p}}$, and we view $\mathrm{Tr}(x \cdot \xi)$ as an element in $\{1, 2, \dots, p\}$. For a function $g(\xi)$ on $\mathbb{F}_q^n$, the inverse Fourier transform of $g$ is a function on $\mathbb{F}_q^n$ given by

$$g^\vee(x) = \frac{1}{q^n} \sum_{\xi \in \mathbb{F}_q^n} g(\xi) e_p(\mathrm{Tr}(x \cdot \xi)).$$

We conclude this section by noting the following results on Fourier analysis over finite fields. The statements are foundational, so their proofs are in Appendix A.

**Lemma 4.1.** *For $x \in \mathbb{F}_q$, we have*

$$\sum_{\xi \in \mathbb{F}_q} e_p(\mathrm{Tr}(x\xi)) = q \cdot \mathbf{1}_{x=0}.$$

**Lemma 4.2.** (Fourier inversion) *Given $f\colon \mathbb{F}_q^n \to \mathbb{C}$, we have $(\widehat{f})^\vee = f$.*

**Lemma 4.3.** (Plancherel's identity) *Given $f\colon \mathbb{F}_q^n \to \mathbb{C}$, we have*

$$\sum_{x \in \mathbb{F}_q^n} |f(x)|^2 = \frac{1}{q^n} \sum_{\xi \in \mathbb{F}_q^n} |\widehat{f}(\xi)|^2.$$

**4.2. Dual space.**

**Definition 4.4.** (Dual space) For $V \in G(k, \mathbb{F}_q^n)$, we define $V^* = \mathrm{supp}\widehat{\mathbf{1}}_V$.

The intuition in $\mathbb{R}^n$ is that if $V \in G(k, \mathbb{R}^n)$, then $\mathrm{supp}\widehat{\mathbf{1}}_V = V^\perp$ (viewing $\mathbf{1}_V$ as a distribution). Therefore, the dual space of $V$ is $V^\perp \in G(n-k, \mathbb{R}^n)$. We will show that for a finite field, it is also true that $V^* = V^\perp$.

**Lemma 4.5.** *If $V \in G(k, \mathbb{F}_q^n)$, then $V^* = V^\perp$. Moreover, $\widehat{\mathbf{1}}_V = q^k \mathbf{1}_{V^*}$.*

*Proof.* Suppose the $k$-dimensional space $V$ is spanned by the following $k$ vectors:

$$\mathbf{v}_1 = (v_{11}, \cdots, v_{1n}),\ \mathbf{v}_2 = (v_{21}, \cdots, v_{2n}), \cdots,\ \mathbf{v}_k = (v_{k1}, \cdots, v_{kn}).$$

We use $\mathcal{V}$ to denote the $k \times n$ matrix

$$\mathcal{V} = \begin{pmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \\ \vdots \\ \mathbf{v}_k \end{pmatrix}.$$

Therefore $V$ can be written as

$$V = \{(y_1, \dots, y_k)\mathcal{V} \colon y_1, \dots, y_k \in \mathbb{F}_q\}.$$

We will calculate $\widehat{\mathbf{1}}_V$. By definition

$$\widehat{\mathbf{1}}_V = \sum_{x \in V} e_p(-\mathrm{Tr}(x \cdot \xi)) = \sum_{y_1, \dots, y_k \in \mathbb{F}_q} e_p \left( -\mathrm{Tr} \left( (y_1, \dots, y_k)\mathcal{V} \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix} \right) \right). \tag{4.1}$$

To calculate the right hand side, we first choose $\mathbf{v}_{k+1}, \dots, \mathbf{v}_n$, so that $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ forms a basis of $\mathbb{F}_q^n$. Define

$$\mathcal{W} = \begin{pmatrix} \mathcal{V} \\ \mathbf{v}_{k+1} \\ \vdots \\ \mathbf{v}_n \end{pmatrix} = \begin{pmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_n \end{pmatrix},$$

which is invertible. We can write the right hand side of (4.1) as

$$\sum_{y_1, \dots, y_k \in \mathbb{F}_q} e_p \left( -\mathrm{Tr} \left( (y_1, \dots, y_k, 0, \dots, 0)\mathcal{W} \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix} \right) \right). \tag{4.2}$$

By Lemma 4.1, we see that this sum $= q^k$, if $\mathcal{W} \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix} \in \{0\}^k \times \mathbb{F}_q^{n-k}$; and $= 0$ otherwise. Therefore,

$$V^* = \mathcal{W}^{-1}(\{0\}^k \times \mathbb{F}_q^{n-k})$$

is an $(n-k)$-dimensional subspace, and

$$\widehat{\mathbf{1}}_V = q^k \cdot \mathbf{1}_{V^*}.$$

To show $V^* = V^\perp$, we just need to check any vector $\mathcal{W}^{-1}(0, \dots, 0, a_1, \dots, a_{n-k})^T \in \mathcal{W}^{-1}(\{0\}^k \times \mathbb{F}_q^{n-k})$ is orthogonal to any $\mathbf{v}_i$ $(1 \le i \le k)$. In other words,

$$\mathbf{v}_i \mathcal{W}^{-1} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ a_1 \\ \vdots \\ a_{n-k} \end{pmatrix} = 0.$$

This is true since $\mathbf{v}_i \mathcal{W}^{-1} = (0, \dots, 0, 1, 0 \dots, 0)$ where the $i$-th entry is 1. $\square$

It is also not hard to see the following results, for which we omit the proof.

**Lemma 4.6.** *If $V \in G(k, \mathbb{F}_q^n)$, then $(V^*)^* = V$. Therefore, $(\cdot)^* \colon G(k, \mathbb{F}_q^n) \to G(n-k, \mathbb{F}_q^n)$ is a bijection.*

**Lemma 4.7.** *For two subspaces $V, W$ in $\mathbb{F}_q^n$, we have $V \subset W \Leftrightarrow W^* \subset V^*$.*

We also need a key lemma about the Falconer-type exceptional estimate.

**Lemma 4.8.** *Let $A \subset \mathbb{F}_q^n$ be a set with $\#A = q^a$ $(0 < a < n)$. For $s \in (0, a)$, recall*

$$\begin{aligned} E_s(A) &= \{V \in G(k, \mathbb{F}_q^n) \colon \#\pi_V(A) < q^s\} \\ &= \{V^* \in G(n-k, \mathbb{F}_q^n) \colon \#\{\text{translated copies of } V^* \text{ to cover } A\} < q^s\}. \end{aligned}$$

*Let $M$ be the overlapping number of $\{V \setminus \{0\} \colon V \in E_s(A)\}$, i.e.,*

$$M := \sup_{\xi \in \mathbb{F}_q^n \setminus \{0\}} \sum_{V \in E_s(A)} \mathbf{1}_V(\xi).$$

*Then*

$$\#E_s(A) \lesssim M q^{n-k+s-a}. \tag{4.3}$$

**Remark 4.9.** Noting that for $\xi \in \mathbb{F}_q^n \setminus \{0\}$, we have

$$\sum_{V \in E_s(A)} \mathbf{1}_V(\xi) \le \sum_{V \in G(k, \mathbb{F}_q^n)} \mathbf{1}_V(\xi) = \#\{V \in G(k, \mathbb{F}_q^n) \colon 0, \xi \in V\}.$$

Denote the line passing through $0, \xi$ by $\ell_\xi$. Noting that $\ell_\xi \subset V \Leftrightarrow V^* \subset \ell_\xi^*$ (by Lemma 4.7), we see that the right hand side of the inequality above is equal to

$$\#\{W \in G(n-k, \mathbb{F}_q^n) \colon W \subset \ell_\xi^*\} = \#G(n-k, \ell_\xi^*) \sim q^{(k-1)(n-k)}.$$

We obtain that $M \lesssim q^{(k-1)(n-k)}$. Plugging into (4.3), we obtain that

$$\#E_s(A) \lesssim q^{k(n-k)+s-a}, \tag{4.4}$$

which is the Falconer-type estimate 1.

*Proof of Lemma 4.8.* By definition, for each $V \in E_s(A)$, there exists a set of $(n-k)$-planes $\mathcal{L}_V (= \pi_V(A))$ parallel to $V^*$ such that $A \subset \bigcup_{W \in \mathcal{L}_V} W$. Furthermore, we have $\#\mathcal{L}_V < q^s$.

Let

$$f = \sum_{V \in E_s(A)} \sum_{W \in \mathcal{L}_V} \mathbf{1}_W.$$

We will apply the high-low method to $f$ using the Fourier transform on $\mathbb{F}_q^n$. Denote $\#E_s(A) = q^t$ for simplicity. Then, notice that for every $a \in A$ and for every $V \in E_s(A)$, there exists a $W \in \mathcal{L}_V$ containing $a$. Therefore, we have that

$$q^a q^{2t} = \#A(\#E_s(A))^2 \le \int_A f^2 = \int_A \left( \sum_{V \in E_s(A)} \sum_{W \in \mathcal{L}_V} \mathbf{1}_W \right)^2. \tag{4.5}$$

We now seek to find an upperbound for the right hand side, for which we use the high-low method. The idea of the high-low method originates from [12, 3], and has recently been applied to solve many problems. We briefly explain the idea of high-low method in the finite field setting. For a function $f$ on $\mathbb{F}_q^n$, we want to decompose it into high part and low part:

$$f = f_h + f_l.$$

The "high part" $f_h$ satisfies $0 \notin \mathrm{supp}\widehat{f_h}$; the "low part" $f_l$ satisfies $\mathrm{supp}\widehat{f_l} \subset \{0\}$. By the requirement of the high part and low part, we can see that

$$f_l(x) = \left(\frac{1}{q^n}\int_{\mathbb{F}_q^n} f(x)\,dx\right)\mathbf{1}_{\mathbb{F}_q^n}(x), \quad f_h(x) = f(x) - \left(\frac{1}{q^n}\int_{\mathbb{F}_q^n} f(x)\,dx\right)\mathbf{1}_{\mathbb{F}_q^n}(x).$$

The Fourier support condition on $f_h$ will give us more orthogonality, and hence more gains when we use $L^2$ estimate.

We come back to the proof. Notice that

$$\int_A \left(\sum_{V\in E_s(A)}\sum_{W\in\mathcal{L}_V}\mathbf{1}_W\right)^2 \lesssim \int_A \left(\sum_{V\in E_s(A)}\sum_{W\in\mathcal{L}_V}\mathbf{1}_W - \frac{1}{q^k}\right)^2 + \int_A \left(\sum_{V\in E_s(A)}\sum_{W\in\mathcal{L}_V}\frac{1}{q^k}\right)^2.$$

We now show that the first term on the right hand side dominates. To see this, notice that

$$\int_A \left(\sum_{V\in E_s(A)}\sum_{W\in\mathcal{L}_V}\frac{1}{q^k}\right)^2 = \int_A \left(\#E_s(A)\cdot\#\mathcal{L}_V\cdot\frac{1}{q^k}\right)^2 \le q^a\cdot q^{2(s+t-k)}.$$

Notice that this is much less than the left hand side of (4.5) since $s<k$ and we may assume $q$ is large enough (since for small $q$, (1.3) naturally holds by choosing large enough constant $C_{n,k,a,s}$). Therefore, we have that

$$q^{a+2t} \lesssim \int_A \left(\sum_{V\in E_s(A)}\sum_{W\in\mathcal{L}_V}\mathbf{1}_W - \frac{1}{q^k}\right)^2 \le \int_{\mathbb{F}_q^n} \left(\sum_{V\in E_s(A)}\sum_{W\in\mathcal{L}_V}\mathbf{1}_W - \frac{1}{q^k}\right)^2.$$

We now apply the Fourier transform to the last integrand.

Since any $W\in\mathcal{L}_V$ is a translation of $V^*$, we can write $W = x_W + V^*$ for some $x_W\in\mathbb{F}_q^n$. By Lemma 4.5, we have that

$$\widehat{\mathbf{1}}_W(\xi) = e_p(-\mathrm{Tr}(x_W\cdot\xi))\widehat{1}_{V^*} = q^{n-k}e_p(-\mathrm{Tr}(x_W\cdot\xi))\mathbf{1}_V.$$

We also simply note that $\widehat{\mathbf{1}}_{\mathbb{F}_q^n} = q^n\mathbf{1}_{\{0\}}$. We have

$$\left(\mathbf{1}_W - \frac{1}{q^k}\right)^\wedge(\xi) = q^{n-k}e_p(-x_W\cdot\xi)\mathbf{1}_V(\xi) - q^{n-k}\cdot\mathbf{1}_{\{0\}}(\xi).$$

Therefore, we see that $\mathrm{supp}\left(\sum_{W\in\mathcal{L}_V}(\mathbf{1}_W - \frac{1}{q^k})\right)^\wedge \subset V\setminus\{0\}$. Applying Plancherel and noting the definition of $M$, we have

$$\begin{aligned} q^{a+2t} &\lesssim \frac{1}{q^n}\int_{\mathbb{F}_q^n}\left|\sum_{V\in E_s(A)}\sum_{W\in\mathcal{L}_V}(\mathbf{1}_W - \frac{1}{q^k})^\wedge\right|^2 \\ &\lesssim \frac{1}{q^n}M\sum_{V\in E_s(A)}\int_{\mathbb{F}_q^n}\left|\sum_{W\in\mathcal{L}_V}(\mathbf{1}_W - \frac{1}{q^k})^\wedge\right|^2 \\ &= M\sum_{V\in E_s(A)}\int_{\mathbb{F}_q^n}\left|\sum_{W\in\mathcal{L}_V}\mathbf{1}_W - \frac{1}{q^k}\right|^2 \\ &\lesssim M\sum_{V\in E_s(A)}\int_{\mathbb{F}_q^n}(\sum_{W\in\mathcal{L}_V}\mathbf{1}_W)^2 + \int_{\mathbb{F}_q^n}(\#\mathcal{L}_V)^2\frac{1}{q^{2k}}. \end{aligned}$$

Noting that $(\sum_{W\in\mathcal{L}_V}\mathbf{1}_W)^2=\sum_{W\in\mathcal{L}_V}\mathbf{1}_W$ (as $\{\mathbf{1}_W\}_{W\in\mathcal{L}_V}$ are disjoint), $\#\mathcal{L}_V<q^s$, and $\#E_s(A)=q^t$, we see that the inequality above is

$$\lesssim Mq^t(q^{s+n-k}+q^{2s+n-2k})\lesssim Mp^{t+s+n-k}.$$

Combining with the lower bound $q^{a+2t}$, we obtain

$$q^t\lesssim Mp^{n-k+s-a}. \qquad \square$$

## 5. Proof of Theorem 1.4

The goal of this section is to prove Theorem 1.4 which we restate here:

**Theorem 5.1.** *Let $A\subset\mathbb{F}_q^n$ be a set with $\#A=q^a$ $(0<a<n)$. For $s\in(0,a)$, define*

$$E_s(A):=\{V\in G(k,\mathbb{F}_q^n)\colon \#\pi_V(A)<q^s\}.$$

*Then for $s<\frac{a+2k-n}{2}$, we have*

$$\#E_s(A)\le C_{n,k,a,s}\cdot\log q\cdot q^t, \tag{5.1}$$

*where $t=\max\{k(n-k)+2(s-a),(k-1)(n-k)\}$. Here, $C_{n,k,a,s}$ is a constant that may depend on $n,k,a,s$, but not depend on $q$.*

**5.1. Proof of Theorem 1.4.** Let $A\subset\mathbb{F}_q^n$ with $\#A=q^a$. We consider two cases.

*Case 1*: There exists a hyperplane, $H\in A(n-1,\mathbb{F}_q^n)$, such that

$$\#(A\cap H)\ge q^{s+n-k-1}.$$

Let $H_0\in G(n-1,\mathbb{F}_q^n)$ be such that $H$ is parallel to $H_0$. Then, we claim that every $V\in E_s(A)$ must satisfy $V^*\subset H_0$.

To see this, notice that if $V^*\in G(n-k,\mathbb{F}_q^n)$ is not contained in $H_0$, then $H\cap V^*$ is a $(n-k-1)$-dimensional plane, which means that $\#(H\cap V^*)=q^{n-k-1}$. Recalling the definition of $\pi_V$ in (2.2), we have

$$\#\pi_V(A)\ge\#\pi_V(A\cap H)\ge\frac{\#(H\cap A)}{\#(H\cap V^*)}\ge q^s.$$

So, $\{V^*:V\in E_s(A)\}\subset G(n-k,H_0)$. It follows that

$$\#E_s(A)\le\#G(n-k,H_0)\sim q^{(k-1)(n-k)}.$$

*Case 2*: Suppose for every hyperplane $H\in A(n-1,\mathbb{F}_q^n)$, we have that

$$\#(A\cap H)\le q^{s+n-k-1}.$$

First, we define

$$M:=\sup_{\xi\in\mathbb{F}_q^n\setminus\{0\}}\sum_{V\in E_s(A)}\mathbf{1}_V(\xi).$$

We denote $\#E_s(A)=q^t$. By Lemma 4.8, we have

$$q^t\le Mq^{n-k+s-a}.$$

To complete the proof, it remains to prove the following lemma.

**Lemma 5.2.**

$$M\lesssim\log q\cdot q^{(n-k)(k-1)+s-a}.$$

*Proof.* Let $\xi_0$ be the point in $\mathbb{F}_q^n - \{0\}$ such that

$$M = \#\{V \in E_s(A) \colon \xi_0 \in V\}. \tag{5.2}$$

We know that such a $\xi_0$ exists since there are only finitely many $\xi$. Let $\ell$ be the line passing through 0 and $\xi_0$, and let $H = \ell^*$ which is a hyperplane. We should view $\ell$ as a line in the frequency space, and view $H$ as a hyperplane in the physical space. Define the set

$$\Theta := \{V \in E_s(A) \colon \ell \subset V\} = \{V \in E_s(A) \colon V^* \subset H\}.$$

By (5.2), $\#\Theta = M$.

Now, we decompose $\mathbb{F}_q^n$ into $(n-1)$-dimensional planes that are parallel to $H$:

$$\mathbb{F}_q^n = \bigsqcup_{i=1}^{q} H_i.$$

Let $A_i = H_i \cap A$, which is the intersection of $A$ with each slice.

**Lemma 5.3.** *For each $i$, we have that*

$$\sum_{V\in\Theta} \#\pi_V(A_i) \gtrsim \#\Theta \min\{q^{k-1}, \#A_i q^{-(n-k)(k-1)}\#\Theta\}.$$

*Proof of Lemma 5.3.* If $\#A_i \cdot p^{-(n-k)(k-1)}\#\Theta \le C$ for some large constant $C$, then the estimate trivially holds since $\#\pi_V(A_i) \ge 1$. Therefore, we assume

$$\#A_i \cdot p^{-(n-k)(k-1)}\#\Theta > C.$$

The proof follows by applying (4.4) to the set $A_i$ in the $(n-1)$-dimensional space $H_i(\cong \mathbb{F}_q^{n-1})$. This is actually an exceptional set estimate for projection to $(k-1)$-planes in $\mathbb{F}_q^{n-1}$.

Let

$$\begin{aligned} E &:= \{V^* \in G(n-k, H) \colon \#\pi_V(A_i) < q^{s'}\} \\ &= \{V^* \in G(n-k, H) \colon \#\{\text{translated copies of } V^* \text{ to cover } A_i\} < q^{s'}\}, \end{aligned}$$

where $s'$ is to be determined. (4.4) yields that

$$\#E \lesssim q^{(k-1)(n-k)+s'}(\#A_i)^{-1}.$$

We choose $s'$ to be such that

$$q^{s'} = C^{-1}\min\{q^{k-1}, \#A_i q^{-(n-k)(k-1)}\#\Theta\},$$

where $C$ is a large constant. Plugging into the upper bound of $\#E$, we see that

$$\#E \le \frac{1}{2}\#\Theta.$$

Therefore,

$$\sum_{V\in\Theta} \#\pi_V(A_i) \ge \sum_{V\in\Theta\setminus E} \#\pi_V(A_i) \ge \frac{1}{2}\#\Theta q^{s'} \gtrsim \#\Theta \min\{q^{k-1}, \#A_i q^{-(n-k)(k-1)}\#\Theta\}. \quad \square$$

We continue the proof of Lemma 5.2. By a Fubini-type argument, we have

$$\#\Theta \cdot q^s \ge \sum_{V\in\Theta} \#\pi_V(A) = \sum_{V\in\Theta}\sum_{i=1}^{q} \#\pi_V(A_i) = \sum_{i=1}^{q}\sum_{V\in\Theta} \#\pi_V(A_i).$$

Applying Lemma 5.3, we have that

$$\#\Theta \cdot q^s \gtrsim \sum_{i=1}^{q} \#\Theta \min\{q^{k-1}, \#A_i q^{-(n-k)(k-1)}\#\Theta\}.$$

By dyadic pigeonholing, we choose $I$ which is a subset of these $i$, such that there exists $\beta > 0$ with $\#A_i \sim q^\beta$ for $i \in I$, and $\#I \cdot q^\beta \gtrsim (\log q)^{-1}\#A$. Thus,

$$\#\Theta \cdot q^s \gtrsim \sum_{i\in I} \#\Theta \min\{q^{k-1}, q^{\beta-(n-k)(k-1)}\#\Theta\}.$$

Also, recall the assumption at the beginning of Case 2:

$$q^\beta \le q^{s+n-k-1}. \tag{5.3}$$

We now have two cases depending on where the minimum is achieved. Firstly, if $q^{k-1} \ge q^{\beta-(n-k)(k-1)}\#\Theta$, we have that

$$\#\Theta \cdot q^s \gtrsim \#I \cdot q^\beta \cdot q^{-(n-k)(k-1)}(\#\Theta)^2 \gtrsim (\log q)^{-1} q^{a-(n-k)(k-1)}(\#\Theta)^2.$$

Therefore, $M = \#\Theta \le \log q \cdot q^{(n-k)(k-1)+s-a}$, which proves Lemma 5.2.

The second scenario is $q^{k-1} \le q^{\beta-(n-k)(k-1)}\#\Theta$. We will show that this will not happen. If it happens, we have

$$\#\Theta \cdot q^s \gtrsim \#I \cdot \#\Theta \cdot q^{k-1}.$$

Multiplying $q^\beta$ on both sides gives

$$q^\beta \#I \cdot q^{k-1} \lesssim q^\beta q^s.$$

This together with (5.3) implies that

$$q^{a+(k-1)}(\log q)^{-1} \lesssim q^{s+\beta} \le q^{2s+n-k-1}.$$

When $q$ is big enough, this is a contradiction, as we assumed that $s < \frac{a+2k-n}{2}$. Thus, Lemma 5.2 is proved. □

**Remark 5.4.** The main obstacle to generalizing the results of this paper to $\mathbb{R}^n$ is as follows. Let $A \subset \mathbb{R}^n$ with $\dim(A) = a$. Let $\{V_t\}_{t\in\mathbb{R}}$ be the one-parameter family of $(n-1)$-planes, where each $V_t$ is orthogonal to $(0,\dots,0,1)$ and intersects with the $x_n$-axis at $(0,\dots,0,t)$. Set $A_t = A \cap V_t$. If everything is finite, then $\#A = \sum_t \#A_t$, which implies that there exists $1 \le M \le \#A$ such that

$$\#A \lesssim \log(\#A) \cdot M \cdot \#\{t\colon \#A_t \le M\}.$$

In the continuous setting, we hope there exists $\beta \in (0,a]$ such that

$$\dim(A) \le \beta + \dim(\{t\colon \dim(A_t) \ge \beta\}).$$

This roughly says that if $A$ is big, then we can find many big slices $\{A_t\}$ of $A$. If we replace "$\le$" by "$\ge$" in the inequality above, then it is always true. However, it may fail in the reverse direction. Actually, there exists a set $A$ with $\dim(A) = n$ but $\dim(A_t) = 0$ for all $t$. This failure of Fubini-type argument is the main obstacle to generalize our theorem to $\mathbb{R}^n$.

## Appendix A.

**Lemma A.1.** *For $x \in \mathbb{F}_q$, we have*

$$\sum_{\xi \in \mathbb{F}_q} e_p(\mathrm{Tr}(x\xi)) = q \cdot \mathbf{1}_{x=0}.$$

*Proof.* When $x = 0$, it is clear that the left hand side equals $q$ as desired. When $x \neq 0$, by the change of variables $\xi \mapsto x^{-1}\xi$, the left hand side equals

$$\sum_{\xi \in \mathbb{F}_q} e_p(\mathrm{Tr}(\xi)).$$

We just need to show that for any $y \in \mathbb{F}_p$, the number of $\xi \in \mathbb{F}_q$ such that $\mathrm{Tr}(\xi) = y$ are all the same. Then we have

$$\sum_{\xi \in \mathbb{F}_q} e_p(\mathrm{Tr}(\xi)) = \frac{q}{p} \sum_{y \in \mathbb{F}_p} e_p(y) = 0.$$

To calculate $\#\{\xi \in \mathbb{F}_q \colon \mathrm{Tr}(\xi) = y\}$, we first find a $\xi_0 \in \mathbb{F}_q$ such that $\mathrm{Tr}(\xi_0) = 1$. Note that

$$\mathrm{Tr}(\xi) = \sum_{i=0}^{r-1} \xi^{p^i}$$

is a polynomial of degree $p^{r-1}$. Therefore, there exists $\xi_1 \in \mathbb{F}_q$ such that $\mathrm{Tr}(\xi_1) \neq 0$. Choosing $\xi_0 = \mathrm{Tr}(\xi_1)^{-1}\xi_1$ and noting $\mathrm{Tr}(\xi_1)^{p^i} = \mathrm{Tr}(\xi_1)$ as $\mathrm{Tr}(\xi_1) \in \mathbb{F}_p$, we have

$$\mathrm{Tr}(\xi_0) = \sum_{i=0}^{r-1} (\mathrm{Tr}(\xi_1)^{-1}\xi_1)^{p^i} = \mathrm{Tr}(\xi_1)^{-1} \sum_{i=0}^{r-1} \xi_1^{p^i} = 1.$$

Now we can see that for any $y, y' \in \mathbb{F}_p$, if $\mathrm{Tr}(\xi) = y$, then by the $\mathbb{F}_p$-linearity of Tr, $\mathrm{Tr}(\xi + (y - y')\xi_0) = y'$. This shows that $\#\{\xi \in \mathbb{F}_q : \mathrm{Tr}(\xi) = y\}$ are the same for all $y \in \mathbb{F}_p$. □

**Lemma A.2.** (Fourier inversion) *Given $f \colon \mathbb{F}_q^n \to \mathbb{C}$, we have $(\widehat{f})^\vee = f$.*

*Proof.* By definition,

$$\begin{aligned}
(\widehat{f})^\vee(x) &= \frac{1}{q^n} \sum_{\xi \in \mathbb{F}_q^n} \sum_{y \in \mathbb{F}_q^n} f(y) e_p(-\mathrm{Tr}(y \cdot \xi)) e_p(\mathrm{Tr}(x \cdot \xi)) \\
&= \frac{1}{q^n} \sum_{y \in \mathbb{F}_q^n} \sum_{\xi \in \mathbb{F}_q^n} f(y) e_p\Big(\mathrm{Tr}\Big((x - y) \cdot \xi\Big)\Big) \\
&= \frac{1}{q^n} \sum_{y \in \mathbb{F}_q^n} \sum_{\xi \in \mathbb{F}_q^n} f(y) \prod_{j=0}^{n} e_p\Big(\mathrm{Tr}\Big((x_j - y_j)\xi_j\Big)\Big)
\end{aligned}$$

By Lemma A.1, the right hand side gives

$$= \frac{1}{q^n} \sum_{y \in \mathbb{F}_q^n} f(y) \prod_{j=0}^{n} q \cdot \mathbf{1}_{y_j = x_j} = f(x).$$ □

**Lemma A.3.** (Plancherel's identity) *Given $f \colon \mathbb{F}_q^n \to \mathbb{C}$, we have*

$$\sum_{x \in \mathbb{F}_q^n} |f(x)|^2 = \frac{1}{q^n} \sum_{\xi \in \mathbb{F}_q^n} |\widehat{f}(\xi)|^2.$$

*Proof.* By definition,

$$
\begin{aligned}
\frac{1}{q^n}\sum_{\xi\in\mathbb{F}_q^n}|\widehat{f}(\xi)|^2 &= \frac{1}{q^n}\sum_{\xi\in\mathbb{F}_q^n}\left|\sum_{x\in\mathbb{F}_q^n} f(x)e_p(-\mathrm{Tr}(x\cdot\xi))\right|^2 \\
&= \frac{1}{q^n}\sum_{\xi\in\mathbb{F}_q^n}\sum_{x\in\mathbb{F}_q^n}\sum_{x'\in\mathbb{F}_q^n} f(x)\overline{f(x')}e_p(\mathrm{Tr}((x'-x)\cdot\xi)) \\
&= \frac{1}{q^n}\sum_{x\in\mathbb{F}_q^n}\sum_{x'\in\mathbb{F}_q^n} f(x)\overline{f(x')}\sum_{\xi\in\mathbb{F}_q^n} e_p(\mathrm{Tr}((x'-x)\cdot\xi)) \\
&= \sum_{x\in\mathbb{F}_q^n}|f(x)|^2. \qquad \square
\end{aligned}
$$

## References


[1] Chen, C.: Projections in vector spaces over finite fields. - Ann. Acad. Sci. Fenn. Math. 43:1, 2018, 171–185.

[2] Falconer, K.: Hausdorff dimension and the exceptional set of projections. - Mathematika 29:1, 1982, 109–115.

[3] Guth, L., N. Solomon, and H. Wang: Incidence estimates for well spaced tubes. - Geom. Funct. Anal. 29:6, 2019, 1844–1863.

[4] He, W.: Orthogonal projections of discretized sets. - J. Fractal Geom. 7:3, 2020, 271–317.

[5] Kaufman, R.: On Hausdorff dimension of projections. - Mathematika 15:2, 1968, 153–155.

[6] Lund, B., T. Pham, and L. A. Vinh: Orthogonal projections in the plane over prime order fields. - arXiv:2311.05148 [math.CO], 2023.

[7] Mattila, P.: Fourier analysis and Hausdorff dimension. - Cambridge Stud. Adv. Math. 150, Cambridge Univ. Press, 2015.

[8] Mohammadi, A.: Szemerédi–Trotter type results in arbitrary finite fields. - arXiv:1808.05543 [math.CO], 2018.

[9] Orponen, T., and P. Shmerkin: Projections, Furstenberg sets, and the *ABC* sum-product problem. - arXiv:2301.10199 [math.CA], 2023.

[10] Peres, Y., and W. Schlag: Smoothness of projections, Bernoulli convolutions, and the dimension of exceptions. - Duke Math. J. 102:2, 2000, 193–251.

[11] Ren, K., and H. Wang: Furstenberg sets estimate in the plane. - arXiv:2308.08819 [math.CA], 2023.

[12] Vinh, L. A.: The Szemerédi–Trotter type theorem and the sum-product estimate in finite fields. - European J. Combin. 32:8, 2011, 1177–1181.


Received 21 December 2023 • Revision received 5 August 2025 • Accepted 5 August 2025
Published online 12 August 2025

Paige Bright
Massachusetts Institute of Technology
Department of Mathematics
Cambridge, MA 02142-4307, USA
paigeb@mit.edu

Shengwen Gan
University of Wisconsin-Madison
Department of Mathematics
Madison, WI 53706, USA
sgan7@wisc.edu