PROJECTIONS IN VECTOR
SPACES OVER FINITE FIELDS

Changhao Chen

The University of New South Wales, School of Mathematics and Statistics
Sydney NSW 2052, Australia; changhao.chenm@gmail.com

Abstract. We study the projections in vector spaces over finite fields. We prove finite fields analogues of the bounds on the dimensions of the exceptional sets for Euclidean projection mapping. We provide examples which do not have exceptional projections via projections of random sets. In the end we study the projections of sets which have the (discrete) Fourier decay.

1. Introduction

A fundamental problem in fractal geometry is that how the projections affect dimension. Recall the classical Marstrand–Mattila projection theorem: Let $E \subset \mathbf{R}^n$, $n \geq 2$, be a Borel set with Hausdorff dimension s.

- If $s \leq m$, then the orthogonal projection of E onto almost all m-dimensional subspaces has Hausdorff dimension s.
- If $s > m$, then the orthogonal of E onto almost all m-dimensional subspaces has positive m-dimensional Lebesgue measure.

In 1954 Marstrand [14] proved this projection theorem in the plane. In 1975 Mattila [15] proved this for general dimension via 1968 Kaufman's [12] potential theoretic methods. Furthermore the bounds on the dimensions of the exceptional sets of projections was well studied. We put these results in the following form Theorem 1.1 which come from a recent survey paper of Falconer, Fraser and Jin [8], and Mattila [17, Corollary 5.12]. Theorem 1.1 (a) was proved by Kaufman [12] for $m = 1$, $n = 2$, and by Mattila [15] for general $1 \leq m < n$. The estimate (b) was proved by Falconer [7] and all known proofs depend on Fourier transform. The estimate (c) was proved by Peres and Schlag [24] under their generalized projections.

Theorem 1.1. (Bounds on the dimensions of the exceptional sets) *Let $E \subset \mathbf{R}^n$ be a Borel set and $s = \dim E$.*

(a) *If $s \leq m$ and $t \in (0, s]$, then*
$$\dim\{V \in G(n, m) \colon \dim \pi_V(E) < t\} \leq m(n - m) - (m - t).$$

(b) *If $s > m$, then*
$$\dim\{V \in G(n, m) \colon \mathcal{H}^m(\pi_V(E)) = 0\} \leq m(n - m) - (s - m).$$

(c) *If $s > 2m$, then*
$$\dim\{V \in G(n, m) \colon \pi_V(E) \text{ has empty interior }\} \leq m(n - m) - (s - 2m).$$

Here $G(n, m)$, called Grassmanian manifold, denotes the collection of all the m-dimensional linear subspaces of $\mathbf{R}^n$. The notation $\dim E$ denotes the Hausdorff dimension of the set E, and $\pi_V \colon \mathbf{R}^n \to V$ stands for the orthogonal projections onto

V. Recalling that the Grassmanian manifold $G(n, m)$ has dimension $m(n - m)$, this is why we compare with it in the above estimates. Note that the upper bound in (b) is sharp, while the knowledge for the upper bounds in (a) and (c) are not complete, see Mattila [17, Chapter 5] for more details.

Recently there has been a growing interest in studying finite field version of some classical problems arising from Euclidean spaces. For instance, there are finite field Kakeya sets (also called Besicovitch sets) [6], [9], [29], [30], there are finite field Erdős/ Falconer distance problem [11], [27], etc.

Motivated by the above works, we study the projections in vector spaces over finite fields. We show some notations first. Let $\mathbf{F}_p$ denote the finite field with p elements where p is prime, and $\mathbf{F}_p^n$ be the n-dimensional vector space over this field. The number of the m-dimensional linear subspaces of $\mathbf{F}_p^n$ is $\binom{n}{m}_p$ which is called Gaussian coefficient, see [3], [13] for more details. Note that to obtain a m-dimensional subspace, it is sufficient to choose m linear independent vectors. For the first vector we have $p^n - 1$ choices from $\mathbf{F}_p^n$ (except the zero vector); for the second vector we have $p^n - p$ choices to make that the second vector is independent to the first one; and so on. In the end we have $(p^n - 1)(p^n - p) \cdots (p^n - p^{m-1})$ amount of choices. Note that for each m-dimensional subspace, there are amount of $(p^m - 1)(p^n - p) \cdots (p^m - p^{m-1})$ choices which generate (or span) the same subspace. It follows that (see [3, Theorem 6.3], [13] for more details)

$$(1) \qquad \binom{n}{m}_p = \frac{(p^n - 1)(p^n - p) \cdots (p^n - p^{m-1})}{(p^m - 1)(p^m - p) \cdots (p^m - p^{m-1})}.$$

One interesting fact of Gaussian binomial coefficient is that

$$\binom{n}{m}_p = (1 + o(p))p^{m(n-m)}.$$

The notation $o(p)$ means that $o(p)$ goes to zero as p goes to infinity. However, the following estimate is enough for our purpose. Throughout the paper, we assume that the prime number p is large enough such that

$$(2) \qquad p^{m(n-m)} \leq \binom{n}{m}_p \leq 2p^{m(n-m)}.$$

Note that the exponent $m(n-m)$ is the dimension of the real Grassmanian manifold. For convenience, we use the same notation $G(n, m)$ to denote all the m-dimensional linear subspaces of $\mathbf{F}_p^n$.

Before we show the definition of projections in vector spaces over finite fields, let's recall the orthogonal projections in Euclidean spaces. Let $E \subset \mathbf{R}^n$ and V be a subspace of $\mathbf{R}^n$. Then the orthogonal projection of E onto V is defined as

$$\pi_V(E) = \{x \in V : (x + V^\perp) \cap E \neq \emptyset\}$$

where $V^\perp$ is the orthogonal complement of V. Note that the vector space $\mathbf{F}_p^n$ is not an inner product space (in general). For instance the Lagrange's (four square) theorem, every nature number is the sum of four squares, implies that $\mathbf{F}_p^n$ is never an inner product space for $n \geq 4$. Therefore, the word orthogonal make no sense in these spaces. Thus we need a new way to define 'projection' in $\mathbf{F}_p^n$. The following is one of these choices. Let E be a subset of $\mathbf{F}_p^n$ and W be a non-trivial subspace of $\mathbf{F}_p^n$. Let $\pi^W(E)$ denote the collection of cosets of W which intersect E, i.e.,

$$\pi^W(E) = \{x + W : E \cap (x + W) \neq \emptyset, x \in \mathbf{F}_p^n\}.$$

In this paper we are interested in the cardinality of $\pi^W(E)$. Let $|J|$ denote the cardinality of a set J. Observe that if $E \subset \mathbf{R}^n$ is a finite set (i.e., $|E| < \infty$), then

$$|\pi_{W^\perp}(E)| = |\pi^W(E)|.$$

Observe that for any set $E \subset \mathbf{F}_p^n$ and $W \in G(n, n-m)$ (Lagrange's group theorem),

$$|\pi^W(E)| \le \min\{|E|, p^m\}.$$

In analogy of Theorem 1.1, we have the following finite fields version.

Theorem 1.2. *Let $E \subset \mathbf{F}_p^n$. Then*

(a) *for any $N < \frac{1}{2}|E|$,*

$$|\{W \in G(n, n-m) \colon |\pi^W(E)| \le N\}| \le 4p^{(n-m)m-m}N;$$

(b) *for any $\delta \in (0,1)$,*

$$|\{W \in G(n, n-m) \colon |\pi^W(E)| \le \delta p^m\}| \le 2\left(\frac{\delta}{1-\delta}\right)p^{m(n-m)+m}|E|^{-1}.$$

We note that Theorem 1.2 (a) for $m = n-1$ follows from Orponen's pair argument [20, Estimate (2.1)]), and Theorem 1.2 (b) for $m = 1, n = 2$ follows from Murphy and Petridis [18, Corollary 1]. We immediately have the following corollary via the special choices of N and δ in Theorem 1.2.

Corollary 1.3. *Let $E \subset \mathbf{F}_p^n$ with $|E| = p^s$.*

(a) *If $s \le m$ and $t \in (0, s]$, then*

$$|\{W \in G(n, n-m) \colon |\pi^W(E)| \le p^t/10\} \le \frac{1}{2}p^{m(n-m)-(m-t)}.$$

(b) *If $s > m$, then*

$$|\{W \in G(n, n-m) \colon |\pi^W(E)| \le p^m/10\}| \le \frac{1}{2}p^{m(n-m)-(s-m)}.$$

(c) *If $s > 2m$, then*

$$|\{W \in G(n, n-m) : |\pi^W(E)| \ne p^m\}| \le 4p^{m(n-m)-(s-2m)}.$$

The Corollary 1.3 (c) follows by the choice of $\delta = \frac{p^m-1}{p^m}$, and an easy fact that if $|\pi^W(E)| > p^m - 1$ then $|\pi^W(E)| = p^m$ (i.e., E intersects each coset of W). Note that the exponents in Corollary 1.3 are the same as in Theorem 1.1, and $|\pi^W(E)| = p^m$ correspondence to the existence of interior in Theorem 1.1 (c).

I do not know whether these bounds are sharp. We formulate the following finite field version of one conjecture for the dimension bound of the exceptional set in the Euclidean plane. For more backgrounds, and partial improvements on the size of the exceptional set in Euclidean plane, see [17, Chapter 5], [19, Theorem 1.2], [20], [21, Proposition 1.11], [22], [23].

Conjecture 1.4. *For any $s/2 \le t \le s \le 1$ and $E \subset \mathbf{F}_p^2$ with $p^s/C \le |E| \le Cp^s$. Then*

$$|\{W \in G(2, 1) \colon |\pi^W(E)| \le p^t\}| \le C(s, t, C)p^{2t-s}.$$

In Euclidean space, there are various random fractal sets which do not have exceptional set in the projection theorem, see [25] for more details and reference therein. For the finite field case, we study the projections of random sets in $\mathbf{F}_p^n$ (percolation on $\mathbf{F}_p^n$). We have the following results.

Theorem 1.5. *For any $0 < s \leq m$, there is a positive number $p_0 = p_0(n, m, s)$ such that for any prime number $p \geq p_0$, there exists a subset $E \subset \mathbf{F}_p^n$ with $p^s/2 \leq |E| \leq 2p^s$ such that,*

$$|\pi^W(E)| \geq |E|/24 \;\; \text{for all } W \in G(n, n-m).$$

Theorem 1.6. *For any $m < s \leq n$, there is a positive number $p_0 = p_0(n, m, s)$ such that for any prime number $p \geq p_0$, there exists a subset $E \subset \mathbf{F}_p^n$ with $p^s/2 \leq |E| \leq 2p^s$ such that*

$$|\pi^W(E)| = p^m \;\; \text{for all } W \in G(n, n-m).$$

Fourier analysis plays an important role in many topics in fractal geometry. Furthermore there are some results which all known proofs depend on Fourier transforms, for example the statement (c) of Theorem 1.1. Note that the proof for Theorem 1.2 (b) also depends on the (discrete) Fourier transformation.

Proposition 1.7. *Let $E \subset \mathbf{F}_p^n$ with $|\widehat{E}(\xi)| \leq C|E|^\alpha$ for all $\xi \neq 0$ where $\alpha \in [1/2, 1)$ and C is a positive constant.*

(a) *If $|E| \leq C_1 p^{\frac{m}{2-2\alpha}}$, then*

$$|\pi^W(E)| \geq C_2|E|^{2-2\alpha} \;\; \text{for all } W \in G(n, n-m).$$

(b) *If $|E| > C_1 p^{\frac{m}{2-2\alpha}}$, then*

$$|\pi^W(E)| \geq p^m/2 \;\; \text{for all } W \in G(n, n-m).$$

(c) *If $|E| > C_3 p^{\frac{m}{1-\alpha}}$, then*

$$|\pi^W(E)| = p^m \;\; \text{for all } W \in G(n, n-m).$$

The constants C_1, C_2, C_3 only depend on the constant C and α.

Here and in what follows, $\xi \neq 0$ means that ξ is a non-zero vector in $\mathbf{F}_p^n$. For $E \subset \mathbf{F}_p^n$, we simply write $E(x)$ for the characteristic function of E, and $\widehat{E}$ it's discrete Fourier transform.

Now we discuss the condition that $\alpha \in [1/2, 1)$. By the definition of Fourier transformation (see (5)), for any subset $E \subset \mathbf{F}_p^n$,

$$|\widehat{E}(\xi)| \leq |E| \;\; \text{for all } \xi \neq 0.$$

For the case $\alpha = 1/2$, Iosevich and Rudnev [11] called these sets Salem sets. To be formal, a subset $E \subset \mathbf{F}_p^n$ is called a (C, s) Salem set if $p^s/C \leq |E| \leq Cp^s$ and for any $\xi \neq 0$,

$$|\widehat{E}(\xi)| \leq C\sqrt{|E|}.$$

Iosevich and Rudnev [11] introduced the finite fields Salem sets for their study of Erdős/Falconer distance problem in vector spaces over finite fields. Note that this is a finite fields version of Salem sets in Euclidean spaces, see [17, Chapter 3] for more details on Salem sets in Euclidean spaces. Roughly speaking the Fourier coefficients of Salem sets have the 'best possible' upper bound. This follows by the Plancherel identity,

$$\sum_{\xi \in \mathbf{F}_p^n} |\widehat{E}(\xi)|^2 = p^n |E|.$$

To be precise, let $E \subset \mathbf{F}_p^n$ with $|E| \leq p^n/2$ and $|\widehat{E}(\xi)| \leq |E|^\alpha$ for any $\xi \neq 0$. Then

$$p^n|E| - |E|^2 = \sum_{\xi \neq 0} |\widehat{E}(\xi)|^2 \leq p^n|E|^{2\alpha}.$$

It follows that

$$1/2 \leq |E|^{2\alpha - 1}.$$

Thus $\alpha \geq 1/2$ provided E is large enough. See [2, Proposition 2.6], [11] for more details.

Observe that Proposition 1.7 implies that finite field Salem sets do not have exceptional directions in the Corollary 1.3. Furthermore, if there exists (C, s) Salem set where C does not depend on p, then by Proposition 1.7 we can obtain Theorems 1.5–1.6. However, it seems that the only known examples of Salem sets in $\mathbf{F}_p^n$ are the discrete paraboloid and the discrete sphere, and both the size of the discrete paraboloid and the discrete sphere in $\mathbf{F}_p^n$ are roughly p^{n-1}, see [11] for more details. It is natural to ask that does there exists (C, s) Salem set in $\mathbf{F}_p^n$ for any (large) prime number p. The above results and [16, Problem 20] suggest that there exists (C, s) Salem set only if s is an integer. If we loose the condition in the definition of Salem sets, the author [4], Hayes [10] showed the existence of (weak) Salem sets in any given size via the random subsets of $\mathbf{F}_p^n$. A set E is called (weak) Salem set if there is a constant C (does not depend on p) such that

$$|\widehat{E}(\xi)| \leq C\sqrt{|E| \log p} \quad \text{for all} \ \xi \neq 0.$$

See Chen [5] for a random construction of Salem set in Euclidean space (with a log factor also).

The structure of the paper is as follows. In Section 2, we set up notation and lemmas for later use. We prove Theorem 1.2, Theorems 1.5–1.6, and Proposition 1.7 in Section 3, Section 4 and Section 5 respectively. In the last section, we extend an identity of Murphy and Petridis [18]. We give another definition of projections in $\mathbf{F}_p^n$, and show that our results still holds under this definition.

2. Preliminaries

For $1 \leq m \leq n$, recall that $G(n, m)$ stands for all the m-dimensional linear subspaces of $\mathbf{F}_p^n$. Let $A(n, m)$ denote the family of all m-dimensional planes, i.e., the translation of some m-dimensional subspace. Let $W \in G(n, n-m)$, then observe by Lagrange's group theorem that there are p^m cosets of W. Let $x_{W,j} + W, 1 \leq j \leq p^m$ be the different cosets of W. Let $G \subset G(n, n-m)$, and define

$$G' = \{x_{W,j} + W : 1 \leq j \leq p^m, W \in G\}.$$

Outline of the method. The method is an adaptation of the counting pairs argument of Orponen [20, Estimate (2.1)] to our setting. Let $E \subset \mathbf{F}_p^n$ and $W \in G(n, n-m)$, then $|E| = \sum_{j=1}^{p^m} |E \cap (x_{W,j} + W)|$, and the Cauchy–Schwarz inequality implies

$$(3) \qquad |E|^2 \leq |\pi^W(E)| \sum_{j=1}^{p^m} |E \cap (x_{W,j} + W)|^2.$$

Note that $|E \cap (x_{W,j} + W)|^2$ is the amount of pairs of E inside $x_{W,j} + W$. Let $N \leq p^m$, define

$$\Theta = \{W \in G(n, n-m) : |\pi^W(E)| \leq N\}.$$

Summing two sides over $W \in \Theta$ in estimate (3), we obtain

$$(4) \qquad |\Theta||E|^2 \leq N \sum_{W \in \Theta} \sum_{j=1}^{p^m} |E \cap (x_{W,j} + W)|^2 := N\mathcal{E}(E, \Theta').$$

Therefore, the left problem is to estimate $\mathcal{E}(E, \Theta')$.

2.1. Counting pairs and energy arguments. Motivated by the above pairs argument of Orponen [20, Estimate (2.1)], an incidence identity of Murphy and Petridis [18, Lemma 1], and the additive energy in additive combinatorics [28, Chapter 2], we give the following definition which plays a key role for the proof of Theorem 1.2.

Definition 2.1. Let $E \subset \mathbf{F}_p^n$ and $\mathcal{A} \subset A(n,k)$. Define the (generalized) energy of E on $\mathcal{A}$ as

$$\mathcal{E}(E, \mathcal{A}) = \sum_{W \in \mathcal{A}} |E \cap W|^2.$$

Remark 2.2. Recalling the additive energy, if $A, B \subset \mathbf{F}_p$ then the additive energy $E(A, B)$ between A and B is defined as the quantity

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

Observe that by our notation

$$E(A, B) = \mathcal{E}(A \times B, \mathcal{L}),$$

where

$$\mathcal{L} = \{\ell_k\}_{k=0}^{p-1}, \text{ and } \ell_k = \{(x, y) \in \mathbf{F}_p^2 : x + y = k\}.$$

For more details on additive energy, see [28].

2.2. Discrete Fourier transformation. In the following we collect the basic facts about Fourier transformation which related to our setting. For more details on discrete Fourier analysis, see Green [9], Stein and Shakarchi [26]. Let $f \colon \mathbf{F}_p^n \longrightarrow \mathbf{C}$ be a complex value function. Then the Fourier transform of f at $\xi \in \mathbf{F}_p^n$ is defined as

$$(5) \qquad \widehat{f}(\xi) = \sum_{x \in \mathbf{F}_p^n} f(x) e(-x \cdot \xi),$$

where $e(-x \cdot \xi) = e^{-\frac{2\pi i x \cdot \xi}{p}}$ and the dot product

$$x \cdot \xi = x_1 \xi_1 + \cdots + x_n \xi_n \,(\mathrm{mod}\,p).$$

Recall the following Plancherel identity,

$$\sum_{\xi \in \mathbf{F}_p^n} |\widehat{f}(\xi)|^2 = p^n \sum_{x \in \mathbf{F}_p^n} |f(x)|^2.$$

Specially for the subset $E \subset \mathbf{F}_p^n$, we have

$$\sum_{\xi \in \mathbf{F}_p^n} |\widehat{E}(\xi)|^2 = p^n |E|.$$

In the following of this subsection we intend to establish the following ('Plancherel identity on subspaces') Lemma 2.3. To be formal we give some notation first. For $W \in G(n, n-m)$, we define the 'orthogonal complement' of W as

$$\mathrm{Per}(W) := \{x \in \mathbf{F}_p^n \colon x \cdot w = 0 \,(\mathrm{mod}\,p), w \in W\}.$$

Note that unlike in the Euclidean spaces, here $W \cap \mathrm{Per}(W)$ can be some non-trivial subspace. For example let $W = \mathrm{span}\{(1,1)\} \subset \mathbf{F}_2^2$ then $\mathrm{Per}(W) = W$. However, the rank-nullity theorem of linear algebra (or the solution of system of linear equations) implies that for any subspace $W \subset \mathbf{F}_p^n$,

$$(6) \qquad \dim W + \dim \mathrm{Per}(W) = n.$$

The following result shows the connection between $|E \cap (x_{W,j} + W)|, 1 \le j \le p^m$ and the Fourier transform of E, and the identity (7) plays an important role in the proof of Theorem 1.2 (b) and the proof of Proposition 1.7.

Lemma 2.3. *Use the above notation. We have*

$$(7) \qquad \sum_{j=1}^{p^m} |E \cap (x_{W,j} + W)|^2 = p^{-m} \sum_{\xi \in \mathrm{Per}(W)} |\widehat{E}(\xi)|^2.$$

Proof. Let $\xi \in \mathrm{Per}(W)$. Then

$$\widehat{E}(\xi) = \sum_{x \in \mathbf{F}_p^n} E(x)e(-x \cdot \xi) = \sum_{j=1}^{p^m} \sum_{w \in W} E(x_{W,j} + w)e(-(x_{W,j} + w) \cdot \xi)$$

$$= \sum_{j=1}^{p^m} |E \cap (x_{W,j} + W)|e(-x_{W,j} \cdot \xi).$$

It follows that

$$|\widehat{E}(\xi)|^2 = \sum_{j=1}^{p^m} |E \cap (x_{W,j} + W)|^2$$

$$+ \sum_{j \neq k} |E \cap (x_{W,j} + W)||E \cap (x_{W,k} + W)|e(-(x_{W,j} - x_{W,k}) \cdot \xi).$$

Note that $(x_{W,j} - x_{W,k}) \notin W$ for any $j \neq k$. Together with the following Lemma 2.4, we obtain

$$\sum_{\xi \in \mathrm{Per}(W)} e(-(x_{W,j} - x_{W,k}) \cdot \xi) = 0.$$

Thus we complete the proof. $\qquad \square$

Lemma 2.4. *Let $V \in G(n,k)$ and $x \notin V$. Then*

$$\sum_{y \in \mathrm{Per}(V)} e(-x \cdot y) = 0.$$

Proof. We claim that there exists $y_0 \in \mathrm{Per}(V)$ such that $y_0 \cdot x \neq 0$. Suppose that $x \cdot y = 0$ for any $y \in \mathrm{Per}(V)$. It follows that

$$\mathrm{Per}(V) \subset \mathrm{Per}(V \cup \{x\}).$$

Combing with the estimate (6) (rank-nullity theorem), we obtain that $n-k \le n-k-1$ which is impossible. Since $\mathrm{Per}(V)$ is a subspace and $e(-y_0 \cdot x) \neq 1$, we obtain

$$e(-y_0 \cdot x) \sum_{y \in \mathrm{Per}(V)} e(-x \cdot y) = \sum_{y \in \mathrm{Per}(V)} e(-x \cdot y),$$

and hence $\sum_{y \in \mathrm{Per}(V)} e(-x \cdot y) = 0$. $\qquad \square$

Remark 2.5. We do not know if the Lemma 2.4 also holds for vector spaces over general finite fields. For that case we will take nonprincipal character instead of $e^{\frac{2\pi i x}{p}}$. We note that the Lemma 2.4 is the only place in this paper where the prime field $\mathbf{F}_p$ is needed.

2.3. Counting subspaces of $\mathbf{F}_p^n$. In the following, we collect some basic identities for $\binom{n}{m}_p$ for our later use. For more details see [3, Chapter 6], [13].

Lemma 2.6. Let $1 \leq m \leq n$.

(1) $\binom{n}{0}_p := \binom{n}{n}_p = 1, \quad \binom{n}{m}_p = \binom{n}{n-m}_p$.

(2) $\binom{n}{m}_p = \binom{n-1}{m}_p + p^{n-m}\binom{n-1}{m-1}$.

(3) $\binom{n}{m}_p = \binom{n-1}{m-1}_p + p^m\binom{n-1}{m}$.

Lemma 2.7. Let ξ be a non-zero vector of $\mathbf{F}_p^n$.

(1) $|\{V \in G(n,m) \colon \xi \in V\}| = \binom{n-1}{m-1}_p$.

(2) $|\{V \in G(n,m) \colon \xi \in \mathrm{Per}(V)\}| = \binom{n-1}{m}_p$.

Proof. First note that if $m = 1$ then (1) holds. For the case $2 \leq m < n$, note that to obtain a m-dimensional subspace which contains the given vector ξ, it is sufficient to choose another $m-1$ vectors such that these $m-1$ vectors and the vector ξ span a m-dimensional subspace. For the choice of the first vector, we have $p^n - p$ choices from $\mathbf{F}_p^n$ (except the vectors from the subspace of $\mathbf{F}_p^n$ which spanned by ξ). For the choice of the second vector, we have $p^n - p^2$ choices to make sure that the second vector, the first vector, and the vector ξ span a 3-dimensional subspace. We continue to do this until we choose $m - 1$ vectors. In the end we have $(p^n - p)(p^n - p^2) \cdots (p^n - p^{m-1})$ amount of choices. Note that for each m-dimensional subspace which contains vector ξ, there are amount of $(p^m - p)(p^n - p^2) \cdots (p^m - p^{m-1})$ choices which generate (or span) the same subspace. It follows that (see (1) for the definition of $\binom{n}{m}_p$) the amount of m-dimensional plane which contain ξ is

$$\frac{(p^n - p)(p^n - p^2) \cdots (p^n - p^{m-1})}{(p^m - p)(p^m - p^2) \cdots (p^m - p^{m-1})} = \binom{n-1}{m-1}_p.$$

To establish (2), first note that $\dim \mathrm{Per}(\xi) = n - 1$. Observe that

$$\{V \in G(n,m) \colon \xi \in \mathrm{Per}(V)\}$$

is the collection of all the m-dimensional subspace of $\mathrm{Per}(\xi)$, which the conclusion follows. $\qquad\square$

3. Proof of Theorem 1.2

Let $\Theta \subset G(n, n-m)$. Recall that

$$\Theta' = \{x_{W,j} + W \colon 1 \leq j \leq p^m, W \in \Theta\}.$$

Lemma 3.1. Let $E \subset \mathbf{F}_p^n$, $\Theta \subset G(n, n-m)$. Then

(8) $\quad \mathcal{E}(E, \Theta') \leq \min\left\{ |E||\Theta| + 2|E|^2 p^{(n-m-1)m}, 2|E|p^{(n-m)m} + |E|^2|\Theta|p^{-m} \right\}.$

Proof. We first show the estimate

$$\mathcal{E}(E, \Theta') \leq |E||\Theta| + 2|E|^2 p^{(n-m-1)m}.$$

Let $x \in \mathbf{F}_p^n$. Since for any $W \in \Theta$ there is only one coset of W which contains x, we obtain

$$\sum_{V \in \Theta'} V(x) = |\Theta|.$$

By Lemma 2.7, there are $\binom{n-1}{n-m-1}_p$ amount of $(n-m)$-dimensional subspaces containing the given non-zero vector of $\mathbf{F}_p^n$. Then

$$\mathcal{E}(E, \Theta') = \sum_{V \in \Theta'} \left(\sum_{x \in E} V(x) \right)^2 = \sum_{V \in \Theta'} \left(\sum_{x \in E} V(x) + \sum_{x \neq y \in E} V(x)V(y) \right)$$

$$\leq |E||\Theta| + |E|(|E|-1)\binom{n-1}{n-m-1}_p \leq |E||\Theta| + 2|E|^2 p^{(n-m-1)m}.$$

Now we turn to the other estimate. Applying Lemma 2.7 we have

$$\sum_{W \in \Theta} \sum_{\xi \in \mathrm{Per}(W)} |\widehat{E}(\xi)|^2 - |\Theta||E|^2 \leq \binom{n-1}{m-1}_p \sum_{\xi \in \mathbf{F}_p^n \setminus \{0\}} |\widehat{E}(\xi)|^2 \leq \binom{n-1}{m-1}_p p^n |E|.$$

Together with Lemma 2.3, we obtain

$$\mathcal{E}(E, \Theta') = \sum_{W \in \Theta} \sum_{j=1}^{p^m} |E \cap (x_{W,j} + W)|^2 = p^{-m} \sum_{W \in \Theta} \sum_{\xi \in \mathrm{Per}(W)} |\widehat{E}(\xi)|^2$$

$$= p^{-m} \left(\sum_{V \in \Theta} \sum_{\xi \in V} |\widehat{E}(\xi)|^2 - |\Theta||E|^2 + |\Theta||E|^2 \right)$$

$$\leq p^{-m} p^n |E| \binom{n-1}{m-1}_p + |E|^2 |\Theta| p^{-m} \leq 2p^{(n-m)m} |E| + |E|^2 |\Theta| p^{-m}.$$

Thus we complete the proof. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Remark 3.2. Let $|E| \leq p^m$ and $\Theta \subset G(n, n-m)$. Then by the estimate (2) and Lemma 2.6 (1)

$$|\Theta| \leq \binom{n}{n-m}_p \leq 2p^{m(n-m)}.$$

Thus

$$|E||\Theta| + 2|E|^2 p^{(n-m-1)m} \leq 2|E|p^{(n-m)m} + |E|^2 |\Theta| p^{-m}.$$

Therefore, in the proof of Theorem 1.2, if $|E| \leq p^m$, then we use the estimate

(9) $$\mathcal{E}(E, \Theta') \leq |E||\Theta| + 2|E|^2 p^{(n-m-1)m}.$$

For the case $|E| > p^m$, we use the estimate

(10) $$\mathcal{E}(E, \Theta') \leq 2|E|p^{(n-m)m} + |E|^2 |\Theta| p^{-m}.$$

Proof of Theorem 1.2. First we prove (a). Let

$$\Theta = \{W \in G(n, n-m) \colon |\pi^W(E)| \leq N\}.$$

Applying the estimates (4) (outline of the method), (9), we obtain

$$|\Theta||E|^2 \leq \mathcal{E}(E, \Theta')N \leq (|E||\Theta| + 2|E|^2 p^{(n-m-1)m})N.$$

It follows that (recall that $N \leq |E|/2$)

$$|\Theta| \leq 4p^{(n-m)m-m}N.$$

Now we prove (b). For $\delta \in (0, 1)$, let

$$\Theta = \{W \in G(n, n-m)\colon |\pi^W(E)| \le \delta p^m\}.$$

Applying the estimates (4), (10), we obtain

$$|\Theta||E|^2 \le \mathcal{E}(E, \Theta')\delta p^m \le (2|E|p^{(n-m)m} + |E|^2|\Theta|p^{-m})\delta p^m,$$

and

$$|\Theta||E|(1-\delta) \le 2\delta p^{(n-m)m+m}.$$

Then

$$|\Theta| \le 2\left(\frac{\delta}{1-\delta}\right)p^{(n-m)m+m}|E|^{-1}.$$

Thus we complete the proof. $\square$

4. Proofs of Theorems 1.5 and 1.6

4.1.   Percolation on $\mathbf{F}_p^d$.   The random model we used here is related to many other well known models, for example: Erdős–Rényi–Gilbert model in random graphs, percolation theory on the graphs, and Mandelbrot percolation in fractal geometry. We show this model on $\mathbf{F}_p^n$ in the following. For an application of this model to find sets with small Fourier coefficient, see [2, Theorem 5.2], [4].

Let $0 < \delta < 1$. We choose each point of $\mathbf{F}_p^n$ with probability δ and remove it with probability $1 - \delta$, all choices being independent of each other. Let $E = E^\omega$ be the collection of these chosen points. Let $\Omega = \Omega(\mathbf{F}_p^n, \delta)$ be our probability space which consists of all the possible sets E^ω.

We prove Theorems 1.5 and 1.6 by choose $\delta = p^{s-n}$ in the above model, and show that the random set E has the desired properties with high probability when p is large enough. For convenience, we formulate a special large deviations estimate in the following. For more background and details on large deviations estimate, see Alon and Spencer [1, Appendix A].

Lemma 4.1.   (Chernoff bound) *Let $\{X_j\}_{j=1}^N$ be a sequence independent Bernoulli random variables with success probability δ'. Let $\mu = N\delta'$. Then*

$$\mathbf{P}\left(\sum_{j=1}^N X_j < \mu/2\right) \le e^{-\mu/16}.$$

4.2. Projections of random sets.

Proof of Theorem 1.5.   Let $\delta = p^{s-n}$. We consider the random model $\Omega(\mathbf{F}_p^n, \delta)$. Let $W \in G(n, n-m)$. Observe that $|\pi^W(E)|$ is a binomial distribution with parameters p^m and δ' where

$$\delta' = 1 - (1-\delta)^{p^{n-m}}.$$

Let $\mu = p^m\delta'$. Since $1 + x \le e^x$ holds for all x, $e^x \le 1 + x + 5x^2/6$ holds for $|x| \le 1$, and $s \le m$, we obtain

$$(11) \quad \begin{aligned} \mu = p^m\delta' &\ge p^m(1 - e^{-\delta p^{n-m}}) = p^m(1 - e^{-p^{s-m}}) \ge p^m(p^{s-m} - 5p^{2(s-m)}/6) \\ &\ge p^s/6. \end{aligned}$$

Applying Lemma 4.1 to $|\pi^W(E)|$ we have

$$\mathbf{P}\left(|\pi^W(E)| < \mu/2\right) \le e^{-\mu/16}.$$

Since there are $\binom{n}{m}_p$ elements of $G(n, n-m)$, we have

$$\mathbf{P}(\text{exists } W \in G(n, n-m) \text{ such that } |\pi^W(E)| \le \mu/2)$$

(12)
$$\le \binom{n}{m}_p e^{-\mu/16} \le 2p^{m(n-m)} e^{-p^s/96} \to 0 \quad \text{as} \quad p \to \infty.$$

Note that $p^s/2 \le |E| \le 2p^s$ with high probability ($> 1/2$). This follows by applying Chebyshev's inequality, which says that

$$\mathbf{P}(||E| - p^n \delta| > \frac{1}{2}p^n \delta) \le \frac{4p^n \delta(1-\delta)}{(p^n \delta)^2} \le \frac{4}{p^s} \to 0 \quad \text{as} \quad p \to \infty.$$

Together with the estimates (12) and (11), we conclude that there exists $E \in \Omega(\mathbf{F}_p^n, \delta)$ with

$$p^s/2 \le |E| \le 2p^s \quad \text{and} \quad |\pi^W(E)| > \mu/2 \ge p^s/12 \quad \text{for all} \quad W \in G(n, n-m)$$

when p is large enough. Thus we complete the proof. $\square$

Remark 4.2. Let $s \le m$ and $\delta = p^{s-n}$. Then the above proof implies that for "almost every" $E \in \Omega(\mathbf{F}_p^n, \delta)$ we have

$$p^s/2 \le |E| \le 2p^s \quad \text{and} \quad |\pi^W(E)| \ge |E|/24 \quad \text{for all} \quad W \in G(n, n-m).$$

Roughly speaking, there is no exceptional projections for almost every $E \in \Omega(\mathbf{F}_p^n, \delta)$.

Proof of Theorem 1.6. Let $\delta = p^{s-n}$. We again consider the random model $\Omega(\mathbf{F}_p^n, \delta)$. Let $V \in A(n, n-m)$. Note that $|E \cap V|$ is a binomial distribution with parameters p^{n-m} and δ. Thus

$$\mathbf{P}(E \cap V = \emptyset) = (1-\delta)^{p^{n-m}} \le e^{-\delta p^{n-m}} = e^{-p^{s-m}}.$$

Observe that

$$|A(n, n-m)| = p^m \binom{n}{n-m}_p \le 2p^{m(n-m+1)}.$$

Now we have (recalling $s > m$)

$$\mathbf{P}(\text{exists } V \in A(n, n-m) \text{ such that } E \cap V = \emptyset)$$

$$\le 2p^{m(n-m+1)} e^{-p^{s-m}} \to 0 \quad \text{as} \quad p \to \infty.$$

It follows that

$$\mathbf{P}(\text{exists } W \in G(n, n-m) \text{ such that } |\pi^W(E)| < p^m) \to 0 \quad \text{as} \quad p \to \infty.$$

Again by Chebyshev's inequality, we have $p^s/2 \le |E| \le 2p^s$ with high probability ($> 1/2$) provided p is large enough. Thus we complete the proof. $\square$

Remark 4.3. Let $s > m$ and $\delta = p^{s-n}$. Then the above proof implies that for "almost every" $E \in \Omega(\mathbf{F}_p^n, \delta)$ we have

$$p^s/2 \le |E| \le 2p^s \quad \text{and} \quad |\pi^W(E)| = p^m \quad \text{for all} \quad W \in G(n, n-m).$$

Roughly speaking, there is no exceptional projections for almost every $E \in \Omega(\mathbf{F}_p^n, \delta)$.

5. Proof of proposition 1.7

Proof of Proposition 1.7. First we use the same argument as in the outline of the method. Let $W \in G(n, n-m)$ and $x_{W,j} + W$, $1 \leq j \leq p^m$, be the different cosets of W. Then the Cauchy–Schwarz inequality implies

$$|E|^2 \leq |\pi^W(E)| \sum_{j=1}^{p^m} |E \cap (x_{W,j} + W)|^2.$$

Applying Lemma 2.3 and the Fourier decay of E, we obtain

$$\sum_{j=1}^{p^m} |E \cap (x_{W,j} + W)|^2 = p^{-m} \sum_{\xi \in \mathrm{Per}(W)} |\widehat{E}(\xi)|^2 \leq p^{-m}(|E|^2 + p^m C^2 |E|^{2\alpha}).$$

Then

$$|E|^2 \leq |\pi^W(E)|(p^{-m}|E|^2 + C^2|E|^{2\alpha}).$$

It follows that if $p^{-m}|E|^2 \leq C^2|E|^{2\alpha}$, then

$$|\pi^W(E)| \geq |E|^{2-2\alpha}/2C^2.$$

On the other hand, if $p^{-m}|E|^2 > C^2 p^m |E|^{2\alpha}$, then

$$|\pi^W(E)| \geq p^m/2.$$

Then (a) and (b) hold. Now we turn to (c). Note that if $|\pi^W(E)| > p^m - 1$, then $|\pi^m(E)| = p^m$. Thus it is sufficient to show that

(13)
$$\frac{|E|^2}{p^{-m}|E|^2 + C^2|E|^{2\alpha}} > p^m - 1.$$

By calculation if

$$|E| > p^{\frac{m}{1-\alpha}}(2C^2)^{\frac{1}{2-2\alpha}},$$

then the estimate (13) holds. Thus we complete the proof. $\qquad \square$

6. Further results

In the following, we extend an identity of Murphy and Petridis [18] for general $1 \leq m \leq n$. They proved the special case $m = n - 1$ for the following identity (14). We prove it in two different ways. The first proof essentialy comes from [18]. The second proof depends on the discrete Fourier transformation.

Proposition 6.1. *Let $E \subset \mathbf{F}_p^n$. Then*

(14)
$$\mathcal{E}(E, A(n,m)) = |E|p^m \binom{n-1}{m}_p + |E|^2 \binom{n-1}{m-1}_p.$$

Proof. First proof. Recall that we denote by $F(x)$ the characteristic function of the subset $F \subset \mathbf{F}_p^n$. Applying the identities in Lemma 2.6 (Gaussian coefficient) and

Lemma 2.7, we have

$$
\begin{aligned}
\mathcal{E}(E, A(n,m)) &= \sum_{W \in A(n,m)} |E \cap W|^2 = \sum_{W \in A(n,m)} \left(\sum_{x \in E} W(x) \right)^2 \\
&= \sum_{W \in A(n,m)} \left(\sum_{x \in E} W(x) + \sum_{x \neq y \in E} W(x)W(y) \right) \\
&= |E| \binom{n}{m}_p + |E|(|E|-1) \binom{n-1}{m-1}_p \\
&= |E| p^m \binom{n-1}{m}_p + |E|^2 \binom{n-1}{m-1}_p .
\end{aligned}
$$

Now we use a Fourier approach to give a different proof. Applying Lemma 2.3, Lemmas 2.6–2.7, and Plancherel identity for subset $E \subset \mathbf{F}_p^n$, we obtain

$$
\begin{aligned}
\mathcal{E}(E, A(n,m)) &= \sum_{W \in G(n,m)} \sum_{j=1}^{p^m} |E \cap (x_{W,j} + W)|^2 = p^{m-n} \sum_{W \in G(n,m)} \sum_{\xi \in \mathrm{Per}(W)} |\widehat{E}(\xi)|^2 \\
&= p^{m-n} \left(\binom{n-1}{m}_p \sum_{\xi \neq 0} |\widehat{E}(\xi)|^2 + \binom{n}{m}_p |\widehat{E}(0)|^2 \right) \\
&= |E| p^m \binom{n-1}{m}_p + |E|^2 \binom{n-1}{m-1}_p .
\end{aligned}
$$

Thus we complete the proof. $\qquad\square$

I thank the anonymous referee for suggesting the following definition of projections in $\mathbf{F}_p^n$. Let $E \subset \mathbf{F}_p^n$ and $V \in G(n,m)$. Then the projection of E to V is defined as

$$
P_V(E) := \{x + \mathrm{Per}(V) : E \cap (x + \mathrm{Per}(V)) \neq \emptyset, \ x \in \mathbf{F}_p^n\}.
$$

We intend to show that our results also holds under this definition.

By using our notation we obtain

$$
P_V(E) = \pi^{\mathrm{Per}(V)}(E).
$$

Note that the rank-nullity theorem clams $\dim V + \dim \mathrm{Per}(V) = n$. Now we show that for $W \in G(n, n-m)$ and $E \subset \mathbf{F}_p^n$

$$
P_{\mathrm{Per}(W)}(E) = \pi^W(E).
$$

This follows from the fact that $\mathrm{Per}(\mathrm{Per}(W)) = W$ for any subspace $W \subset \mathbf{F}_p^n$. First note that the definition of $\mathrm{Per}(W)$ implies $W \subset \mathrm{Per}(\mathrm{Per}(W))$. By applying rank-nullity theorem, we obtain

$$
\dim \mathrm{Per}(\mathrm{Per}(W)) = n - \dim \mathrm{Per}(W) = \dim W,
$$

and hence $\mathrm{Per}(\mathrm{Per}(W)) = W$. Therefore, for $E \subset \mathbf{F}_p^n$ and $N < p^m$, we obtain

$$
|\{V \in G(n,m) : |P_V(E)| \leq N\}| = |\{W \in G(n, n-m) : |\pi^W(E)| \leq N\}|.
$$

Thus we conclude that our results holds under the above definition.

the quality of this article. I am grateful for being supported by the Vilho, Yrjö, and Kalle Väisälä foundation.

References

[1] ALON, N., and J. SPENCER: The probabilistic method. - Wiley Interscience, New York, 2000.

[2] BABAI, L.: Fourier transforms and equations over finite Abelian groups. An introduction to the method of trigonometric sums. - http://people.cs.uchicago.edu/∼laci/reu02/fourier.pdf.

[3] CAMERON, P.: The art of counting. - cameroncounts.files.wordpress.com/2016/04/acnotes1.pdf.

[4] CHEN, C.: Salem sets in vector spaces over finite fields. - Ark. Mat. (to appear).

[5] CHEN, X.: Sets of Salem type and sharpness of the L^2 Fourier restriction theorem. - Trans. Amer. Math. Soc. (to appear).

[6] DVIR, Z.: On the size of Kakeya sets in finite fields. - J. Amer. Math. Soc. 22:4, 2009, 1093–1097.

[7] FALCONER, K. J.: Hausdorff dimension and the exceptional set of projections. - Mathematika 29, 1982, 109–115.

[8] FALCONER, K., J. FRASER, and X. JIN: Sixty years of fractal projections. - In: Fractal geometry and stochastics V, Progr. Probab. 70, 2015, 3–25.

[9] GREEN, B.: Restriction and Kakeya phonomena. - Lecture notes, 2003.

[10] HAYES, T.: A large-deviation inequality for vector-valued martingales. - https://www.cs.unm.edu/hayes/papers/VectorAzuma/VectorAzuma20050726.pdf.

[11] IOSEVICH, A., and M. RUDNEV: Erdős distance problem in vector spaces over finite fields. - Trans. Amer. Math. Soc. 359, 2007, 6127–6142.

[12] KAUFMAN, R.: On Hausdorff dimension of projections. - Mathematika 15, 1968, 153–155.

[13] KONVALINA, J.: A unified interpretation of the binomial coefficients, the Stirling numbers, and the Gaussian coefficients. - Amer. Math. Monthly 107:10, 2000, 901–910.

[14] MARSTRAND, J. M.: Some fundamental geometrical properties of plane sets of fractional dimensions. - Proc. London Math. Soc. (3) 4, 1954, 257–302.

[15] MATTILA, P.: Hausdorff dimension, orthogonal projections and intersections with planes. - Ann. Acad. Sci. Fenn. Ser. A I Math. 1:2, 1975, 227–244.

[16] MATTILA, P.: Hausdorff dimension, projections, and the Fourier transform. - Publ. Mat. 48, 2004, 3–48.

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

[18] MURPHY, B., and G. PETRIDIS: A point-line incidence identity in finite fields, and applications. - Preprint, arxiv.org/abs/1601.03981, 2016.

[19] OBERLIN, D.: Restricted Radon transforms and projections of planar set. - Canad. Math. Bull. 55, 2012, 815–820.

[20] ORPONEN, T.: A discretised projection theorem in the plane. - Preprint, arxiv.org/pdf/1407.6543.pdf, 2014.

[21] ORPONEN, T.: On the packing dimension and category of exceptional sets of orthogonal projections. - Ann. Mat. Pura Appl. 194:3, 2015, 843–880.

[22] ORPONEN, T.: Projections of planar sets in well-separated directions. - Adv. Math. 144:8, 2016, 3419–3430.

[23] ORPONEN, T.: Improving Kaufman's exceptional set estimate for packing dimension. - Preprint, arXiv:1610.06745, 2016.

[24] PERES, Y., and B. SCHLAG: Smoothness of projections, Bernoulli convolutions, and the dimension of exceptions. - Duke Math. J. 102, 2000, 193–251.

[25] SHMERKIN, P., and V. SUOMALA: Spatially independent martingales, intersections, and applications. - Mem. Amer. Math. Soc. (to appear).

[26] STEIN, E., and R. SHAKARCHI: Fourier analysis: An introduction. - Princeton Lectures in Analysis, Princeton Univ. Press, 2003.

[27] TAO, T.: Finite field analogues of Erdős, Falconer, and Furstenberg problems. - Preprint.

[28] TAO, T., and V. VU: Additive combinatorics. - Cambridge Stud. Adv. Math. 105, Cambridge Univ. Press, Cambridge, 2006.

[29] WOLFF, T.: Recent work connected with the Kakeya problem. - In: Prospects in mathematics (Princeton, NJ, 1996), 1999, 129–162.

[30] ZHANG, R.: On configurations where the Loomis–Whitney inequality is nearly sharp and applications to the Furstenberg set problem. - Mathematika 61:1, 2015, 145–161.