DISCRETE ANALYSIS, 2021:22, 16 pp.
www.discreteanalysisjournal.com

Simple Proofs for Furstenberg Sets Over Finite Fields

Manik Dhar Zeev Dvir* Ben Lund†

Received 19 September 2019; Revised 12 June 2021; Published 14 October 2021

Abstract: A (k,m)-Furstenberg set $S \subset \mathbb{F}_q^n$ over a finite field is a set that has at least m points in common with a k-flat in every direction. The question of determining the smallest size of such sets is a natural generalization of the finite field Kakeya problem. The only previously known bound for these sets is due to Ellenberg-Erman [6] and requires sophisticated machinery from algebraic geometry. In this work we give new, completely elementary and simple proofs that significantly improve the known bounds. Our main result relies on an equivalent formulation of the problem using the notion of min-entropy, which could be of independent interest.

Key words and phrases: Kakeya, Furstenberg, finite fields, min-entropy, polynomial method

1 Introduction

For a prime power q, let $\mathbb{F}_q$ be the finite field of order q. Let $n > k \geq 1$ and $m \geq 1$ be integers. A subset $S \subseteq \mathbb{F}_q^n$ is a (k,m)-*Furstenberg* set if, for each rank k subspace W of $\mathbb{F}_q^n$, there is a translate of W that intersects S in at least m points.

For a prime power q and integers n,k, and m with $1 \leq k < n$ and $m \leq q^k$, let $K(q,n,k,m)$ be the least t such that there exists a (k,m)-Furstenberg set in $\mathbb{F}_q^n$ of cardinality t.

A $(1,q)$-Furstenberg set is called a Kakeya set. The question of determining $K(q,n,1,q)$ was originally posed by Wolff [13] as a toy version of the Euclidean Kakeya conjecture. For this case, the polynomial method [4, 11, 5] gives the bound

$$K(q,n,1,q) \geq 2^{-n} q^n, \tag{1}$$

*Supported by NSF grant DMS-1953807.
†Supported by NSF postdoctoral fellowship DMS-1802787 and Institute for Basic Science (IBS-R029-C1).

DOI: 10.19086/da.29067

which is tight up to a factor of 2. This was recently improved by Bukh and Chao [2], who proved a bound that is tight up to lower order terms. The same techniques also handle the more general case of arbitrary m, giving the bound

$$K(q,n,1,m) \geq 2^{-n} m^n. \tag{2}$$

The approach used to prove (1) was generalized to all k when $m = q^k$ by Kopparty, Lev, Saraf, and Sudan [9], who improved earlier work by Ellenberg, Oberlin, and Tao [7]. They show

$$K(q,n,k,q^k) \geq \left(\frac{q^{k+1}}{q^k+q-1}\right)^n = \left(1+\frac{q-1}{q^k}\right)^{-n} q^n. \tag{3}$$

For fixed $k \geq 2$, fixed n, and q large, (3) states that a (k,q^k)-Furstenberg set in $\mathbb{F}_q^n$ must contain nearly all of the points of $\mathbb{F}_q^n$. For fixed $k \geq 2$, fixed q, and n large, (3) states that a (k,q^k)-Furstenberg set in $\mathbb{F}_q^n$ must have size at least $C^{-n}q^n$, for some constant $C > 1$ depending on q and k.

Kopparty, Lev, Saraf, and Sudan also described several ways to construct small Furstenberg sets when $m = q^k$. We include only one of these here. Other constructions described in [9] give better bounds for large k, and for some explicit, small values of q.

$$K(q,n,k,q^k) \leq \left(1-\frac{q-3}{2q^k}\right)^{\lfloor n/(k+1)\rfloor} q^n. \tag{4}$$

Furstenberg sets with $k \geq 2$ and $m < q^k$ are not understood as well. The first progress on the general case was by Ellenberg and Erman [6], who used a sophisticated algebraic argument to prove

$$K(q,n,k,m) \geq C_{n,k} m^{n/k}. \tag{5}$$

Ellenberg and Erman did not explicitly specify the value of $C_{n,k}$ obtained, but a close inspection of the proof shows that it is $C_{n,k} = (1/n)^{\Omega(n\ln(n/k))}$. Recent work of the current authors [3] gives a slightly more streamlined version of the Ellenberg and Erman proof to obtain (5) with $C_{n,k} = \Omega((1/16)^{n\ln(n/k)})$.

The contribution of this paper is to improve (5) using much simpler and more elementary arguments. Our first main result deals with the case of general k and $m \leq q^k$:

Theorem 1. *Let q be a prime power, and let n,k, and m be positive integers such that $m \leq q^k$, then*

$$K(q,n,k,m) \geq \frac{1}{2^n} m^{n/k}.$$

Ellenberg and Erman's method can be used to prove Furstenberg-style bounds involving hypersurfaces that don't follow from the proof of Theorem 1. The proof of Theorem 1 relies on a new equivalent formulation of the problem using the notion of min-entropy. This new formulation, described in Section 3, allows us to derive the bound for general k using a recursive argument, starting with $k = 1$ as a base case (proved using the polynomial method).

A separate argument gives stronger bounds for large m. Let S be any set of mq^{n-k} points in $\mathbb{F}_q^n$. A simple pigeonholing argument shows that S is a (k,m)-Furstenberg set. When m is sufficiently large relative to q, it turns out that there are no Furstenberg sets much smaller than this trivial construction.

Theorem 2. *Let $\varepsilon > 0$, let q be a prime power, and let n,k, and m be integers with $2 \le k < n$ and $m \le q^k$. If $m \ge 2^{n+7-k} q\varepsilon^{-2}$, then*

$$K(q,n,k,m) \ge (1-\varepsilon) m q^{n-k}.$$

Note that, since $q^k \ge m$, Theorem 2 never applies if $q^{k-1} < 2^{n+7-k}$.

When $k > n/2$ and $m > q^{n-k}$, we can remove the assumption that the k-flats are in different directions and still prove a stronger bound than previously known. The number of rank k subspaces in $\mathbb{F}_q^n$ is given by the q-binomial coefficient $\binom{n}{k}_q$ (see Section 2.1 for details).

Theorem 3. *Let q be a prime power, and let n,k, and m be integers with $n/2 < k < n$ and $0 \le m \le q^k$. Let $S \subseteq \mathbb{F}_q^n$. Let L be a set of k-flats that each contain at least m points of S, with $|L| = \binom{n}{k}_q$. Then,*

$$|S| \ge \left(1 - q^{n-2k} - \sqrt{q^{n-k}m^{-1}}\right) m q^{n-k}.$$

In particular, the same lower bound holds for $K(q,n,k,m)$.

Note that, if $m < q^{n-k}$, then the right side of the inequality in Theorem 3 is negative. Hence Theorem 3 is interesting only for larger m.

The proof of Theorem 2 combines (1) with incidence estimates for large sets in finite fields. The proof of Theorem 3 relies only on incidence estimates for large sets in finite fields, and doesn't rely on the polynomial method.

Lastly, when n is divisible by k, a very simple proof shows that the following bound follows directly from (2).

Theorem 4. *Let q be a prime power, and let n,k and m be positive integers such that $m \le q^k$ and n is divisible by k, we have*

$$K(q,n,k,m) \ge \frac{1}{2^{n/k}} m^{n/k}.$$

Organization: We begin in Section 2 with some preliminaries on finite geometry and polynomials over finite fields. In Section 3 we discuss the equivalent entropic formulation to the problem of bounding the size of Furstenberg sets. In Section 4 we prove the one dimensional case of the entropic version using the polynomial method and in Section 5 we prove the general case (Theorem 1) using recursion. Theorem 4 is proved in Section 6 and Theorems 2 and 3 are proved in Section 7.

2 Preliminaries

2.1 Facts from finite geometry

In this section, we review a few basic facts from finite geometry, as well as the results we need from incidence geometry.

A *k-flat* is a translate of a rank k linear subspace. The span of a set $X \subseteq \mathbb{F}_q^n$ is the smallest flat that contains X, and is denoted $\overline{X}$. For flats Λ, Γ in $\mathbb{F}_q^n$, we denote by $\overline{\Lambda,\Gamma}$ the span of $\Lambda \cup \Gamma$. If Λ and Γ are subspaces (*i.e.* they each contain the origin), then

$$\dim(\overline{\Lambda,\Gamma}) = \dim(\Lambda) + \dim(\Gamma) - \dim(\Lambda \cap \Gamma). \tag{6}$$

For integers $1 \leq k < n$, the number of rank k subspaces of $\mathbb{F}_q^n$ is given by the q-binomial coefficient $\binom{n}{k}_q$. As with ordinary binomial coefficients, the q-binomial coefficients are centrally symmetric:

$$\binom{n}{k}_q = \binom{n}{n-k}_q. \tag{7}$$

The Pascal identities for q-binomial coefficients are

$$\binom{n}{k}_q = q^k \binom{n-1}{k}_q + \binom{n-1}{k-1}_q, \text{ and} \tag{8}$$

$$\binom{n}{k}_q = \binom{n-1}{k}_q + q^{n-k}\binom{n-1}{k-1}_q. \tag{9}$$

A direct expression is given by

$$\binom{n}{k}_q = \frac{(1-q^n)(1-q^{n-1})\dots(1-q^{n-k+1})}{(1-q)(1-q^2)\dots(1-q^k)}. \tag{10}$$

The number of k-flats in $\mathbb{F}_q^n$ is $q^{n-k}\binom{n}{k}_q$.

A point is *incident* to a flat if the point is contained in the flat. Given a set L of flats, and a set S of points, both in $\mathbb{F}_q^n$, we denote by

$$I(S,L) = |\{(p,\ell) \in S \times L : p \in \ell\}|$$

the number of incidences between S and L.

The following bound on the number of incidences between points and k-flats was first proved by Haemmers [8, Chapter 3]. The exact statement used here can also be recovered from the proof of Theorem 1 in [10].

Lemma 5. *If S is a set of points and L a set of k-flats, both in $\mathbb{F}_q^n$, then*

$$I(S,L) \leq q^{k-n}|S|\,|L| + \sqrt{q^k \binom{n-1}{k}_q |S|\,|L|\,(1-|S|q^{-n})\left(1-|L|q^{k-n}\binom{n}{k}_q^{-1}\right)}.$$

Given a set S of points, a flat is (S,t)-*rich* if it contains at least t points of S. A flat is (S,t)-*poor* if it contains fewer than t points of S. The following upper bound on the number of (S,t)-poor flats is a slight reformulation of [10, Corollary 5]. A slightly weaker bound was proved earlier by Alon [1].

Lemma 6. *Let $S \subset \mathbb{F}_q^k$ be a set of m points. Let $0 < \delta < 1$ and $1 \leq \ell \leq k-1$. The number of $(S, \delta m q^{\ell-k}+1)$-poor ℓ-flats is at most*

$$\left(1 + mq^{\ell-k}(1-\delta)^2\right)^{-1} q^{k-\ell}\binom{k}{\ell}_q.$$

2.2 Method of multiplicities

The results here are from a paper by Dvir, Kopparty, Saraf, and Sudan [5]. We state the theorems we need and the proofs can be found in the aforementioned paper.

Definition 7 (Hasse Derivatives)**.** *Given a polynomial $P \in \mathbb{F}[x_1,\ldots,x_n]$ and an $i \in \mathbb{Z}^n_{\geq 0}$, the ith* Hasse derivative *of P is the polynomial $P^{(i)}$ in the expansion $P(x+z) = \sum_{i\in\mathbb{Z}^n_{\geq 0}} P^{(i)}(x)z^i$ where $x = (x_1,...,x_n)$, $z = (z_1,...,z_n)$ and $z^i = \prod_{j=1}^n z_j^{i_j}$.*

Hasse derivatives satisfy some useful identities. We state the only one we will need.

Lemma 8. *Given a polynomial $P \in \mathbb{F}[x_1,\ldots,x_n]$ and $i,j \in \mathbb{Z}^n_{\geq 0}$, we have*

$$(P^{(i)})^{(j)} = P^{(i+j)} \prod_{k=1}^{n} \binom{i_k + j_k}{i_k}$$

We make precise what it means for a polynomial to vanish on a point $a \in \mathbb{F}^n$ with multiplicity. First we recall for a point j in the non-negative lattice $\mathbb{Z}^n_{\geq 0}$, its weight is defined as $\mathrm{wt}(i) = \sum_{i=1}^n j_i$.

Definition 9 (Multiplicity)**.** *For a polynomial $P \in \mathbb{F}[x_1,\ldots,x_n]$ and a point $a \in \mathbb{F}^n$, we say P vanishes on a with* multiplicity *N, if N is the largest integer such that all Hasse derivatives of P of weight strictly less than N vanish on a. We use $mult(P,a)$ to refer to the multiplicity of P at a.*

Notice, $\mathrm{mult}(P,a) = 1$ just means $f(a) = 0$. We will use the following simple property concerning multiplicities of composition of polynomials.

Lemma 10. *Given a polynomial $P \in \mathbb{F}[x_1,\ldots,x_n]$ and a tuple $Q = (Q_1,\ldots,Q_n)$ of polynomials in $\mathbb{F}[y_1,\ldots,y_m]$, and $a \in \mathbb{F}^m$ we have,*

$$mult(P \circ Q, a) \geq mult(P, Q(a)).$$

The key lemma here is an extended Schwartz-Zippel bound [12][14] which leverages multiplicities.

Lemma 11 (Schwartz-Zippel with multiplicity)**.** *Let $f \in \mathbb{F}[x_1,..,x_n]$, with $\mathbb{F}$ an arbitrary field, be a nonzero polynomial of degree at most d. Then for any finite subset $U \subseteq \mathbb{F}$,*

$$\sum_{a\in U^n} mult(f,a) \leq d|U|^{n-1}.$$

We will also need the following lemma which lets us find polynomials which vanish on different points with differing multiplicities.

Lemma 12. *Given a non-negative integer d and a set of non-negative integers N_x indexed by elements $x \in \mathbb{F}_q^n$ which satisfy*

$$\sum_{x\in\mathbb{F}_q^n} \binom{N_x + n - 1}{n} < \binom{d+n}{n},$$

we can find a non-zero polynomial P of total degree at most d such that for all $x \in \mathbb{F}_q^n$, P vanishes on x with multiplicity at least N_x.

Proof. Note $\binom{d+n}{n}$ is the vector space dimension of the space of polynomials in n variables with total degree at most d. The condition of a polynomial vanishing on a point x with multiplicity N_x is defined by $\binom{N_x+n-1}{n}$ many linear equations in the coefficients of the polynomial. The condition of vanishing on x with multiplicity N_x for all x is then defined by at most $\sum_{x\in\mathbb{F}_q^n}\binom{N_x+n-1}{n}$ many linear equations. The condition in the statement of the lemma implies that we can find a non-zero polynomial which satisfies all these conditions. □

3 Entropy formulation for the Kakeya problem

Let R be a random variable (r.v.) taking values in $\mathbb{F}_q^n$. The q-ary *min entropy* of R (or just min-entropy if q is clear from the context) is defined as

$$\mathbf{H}_\infty^q(R) = -\log_q\left(\max_{w\in\mathbb{F}_q^n}\mathbf{Pr}[R=w]\right)$$

For example, if R is distributed uniformly on a set of size q^k then its min-entropy will be exactly k. In general, a r.v with min-entropy k must have support size at least q^k.

We first consider a class of statements which state Furstenberg bounds in the usual manner.

Definition 13. *(Furstenberg set bound, $A(n,k)$) Let $1\le k<n$ be integers. We say that the statement $A(n,k)$ holds with constant $C_{n,k}$ if the following is true:*

If $S\subset\mathbb{F}_q^n$ is (k,m)-Furstenberg then $|S|\ge C_{n,k}\cdot m^{n/k}$.

In other words $A(n,k)$ is the statement that $K(q,n,k,m)\ge C_{n,k}\cdot m^{n/k}$.

Note, as mentioned earlier, the proof of the Kakeya bound in [5] shows that for all n, $A(n,1)$ holds with $C_{n,1}=2^{-n}$.

We now define a seemingly different statement involving min-entropy of linear maps.

Definition 14. *(Linear maps with high min-entropy, $B(n,k)$) Let $1\le k<n$ be integers. We say that the statement $B(n,k)$ holds with constant $D_{n,k}$ if the following is true:*

For all $\delta\in[0,1]$, if $S\subset\mathbb{F}_q^n$ is of size $|S|=q^{\delta n}$ then there exists an onto linear map $\varphi:\mathbb{F}_q^n\mapsto\mathbb{F}_q^{n-k}$ such that $\mathbf{H}_\infty^q(\varphi(U_S))\ge\delta(n-k)-D_{n,k}$, where U_S is a random variable distributed uniformly over S, and $\varphi(U_S)$ is the pushforward of U_S.

In other words, $B(n,k)$ says that given the random variable U_S, which is uniform over a set S of size $q^{\delta n}$ and hence having min-entropy δn, one can find a linear map that keeps the same *relative* min-entropy (the ratio between min-entropy and dimension) up to some small loss $D_{n,k}$.

The two statements $A(n,k)$ and $B(n,k)$ are equivalent for $C_{n,k}\in(0,1]$ and $D_{n,k}\ge 0$, with a simple formula relating $C_{n,k}$ and $D_{n,k}$.

Lemma 15. *For integers $1\le k<n$. If $B(n,k)$ holds with constant $0\le D_{n,k}$, then $A(n,k)$ holds with constant*

$$C_{n,k}=q^{-\frac{n}{k}D_{n,k}}.$$

Proof. Let $S \subset \mathbb{F}_q^n$ be (k,m)-Furstenberg, and suppose that $B(n,k)$ holds. Let φ be an arbitrary linear map from $\mathbb{F}^n$ to $\mathbb{F}^{n-k}$. Since $\varphi^{-1}(x)$ is a k-flat for each $x \in \mathbb{F}^{n-k}$ and S is (k,m)-Furstenberg,

$$\max_{x \in \mathbb{F}_q^{n-k}} |\varphi^{-1}(x)| \geq m,$$

and hence

$$H_\infty^q(\varphi(U_S)) \leq -\log_q(m|S|^{-1}).$$

Taking δ such that $|S| = q^{\delta n}$, $B(n,k)$ implies that

$$\log_q(m|S|^{-1}) \leq D_{n,k} - \delta(n-k)$$

and hence

$$m \leq q^{D_{n,k}}|S|^{k/n}.$$

Since $A(n,k)$ is equivalent to $m \leq (|S|C_{n,k}^{-1})^{k/n}$, this implies that $A(n,k)$ holds for $C = q^{-(n/k)D_{n,k}}$, as claimed. □

We also show that $A(n,k)$ implies $B(n,k)$ for suitable choices of $C_{n,k}$ and $D_{n,k}$, although this direction is not needed in the proof of Theorem 1.

Lemma 16. *For integer $1 \leq k < n$. If $A(n,k)$ holds with constant $0 < C_{n,k} \leq 1$ then $B(n,k)$ holds with constant*

$$D_{n,k} = \frac{k}{n} \cdot \log_q\left(\frac{1}{C_{n,k}}\right).$$

Proof. Let $n > k$ and suppose in contradiction that $B(n,k)$ does not hold for the above $D_{n,k}$. This means that there exists a $\delta \in [0,1]$ and a set $S \subset \mathbb{F}_q^n$ of size $|S| = q^{\delta n}$ such that for any onto linear map $\varphi : \mathbb{F}_q^n \mapsto \mathbb{F}_q^{n-k}$ we have $\mathbf{H}_\infty^q(\varphi(U_S)) < \delta(n-k) - D_{n,k}$. By the definition of min-entropy this means that for all φ there must exist some $v = v_\varphi \in \mathbb{F}_q^{n-k}$ such that

$$\mathbf{Pr}\left[\varphi(U_S) = v_\varphi\right] = \frac{|\varphi^{-1}(v_\varphi) \cap S|}{|S|} > \frac{q^{D_{n,k}}}{q^{\delta(n-k)}}. \tag{11}$$

Let $K_\varphi \subset \mathbb{F}_q^n$ denote the k-dimensional kernel of φ. Then, (11) implies that there is a shift $w_\varphi \in \mathbb{F}_q^n$ so that

$$|(K_\varphi + w_\varphi) \cap S| > |S| \cdot \frac{q^{D_{n,k}}}{q^{\delta(n-k)}} \geq q^{\delta k + D_{n,k}} \tag{12}$$

Since K_φ can be any k-dimensional linear subspace, S is (k,m)-Furstenberg with $m > q^{\delta k + D_{n,k}}$. Since $A(n,k)$ holds with constant $C_{n,k}$ we get that

$$|S| > C_{n,k} \cdot \left(q^{\delta k + D_{n,k}}\right)^{n/k} = C_{n,k} \cdot q^{\frac{n}{k}D_{n,k}} \cdot |S|. \tag{13}$$

Cancelling $|S|$ from both sides and using the expression for $D_{n,k}$, we get a contradiction. □

The statement $B(n,k)$ is easily generalizable, with U_S replaced by a general random variable. The generalization of the statement $B(n,1)$ can be proven using a simple generalization of the proof in [5]. This generalized statement will allow us to perform induction to prove Furstenberg set bounds.

Theorem 17 (Entropic-Furstenberg bound)**.** *For any random variable R supported over $\mathbb{F}_q^n$ there exists an onto linear map $\phi : \mathbb{F}_q^n \to \mathbb{F}_q^{n-k}$ such that*

$$\mathbf{H}_\infty^q(\phi(R)) \geq \frac{n-k}{n}\mathbf{H}_\infty^q(R) - \log_q(2-q^{-1})k.$$

Theorem 1 follows easily from Theorem 17.

Proof of Theorem 1. Theorem 17 proves the statement $B(n,k)$ with constant $D_{n,k} = k\log_q(2)$. Lemma 15 then proves Theorem 1. □

We will prove Theorem 17 using the polynomial method for the case $k = 1$ and the general case will follow from an inductive argument by composing a sequence of onto maps. For that reason, we restate the $k = 1$ case separately.

Theorem 18 (Entropic bound for $k = 1$)**.** *For any random variable R supported over $\mathbb{F}_q^n$ there exists an onto linear map $\phi : \mathbb{F}_q^n \to \mathbb{F}_q^{n-1}$ such that*

$$\mathbf{H}_\infty^q(\phi(R)) \geq \frac{n-1}{n}\mathbf{H}_\infty^q(R) - \log_q(2-q^{-1}).$$

4 Proof of the entropic bound when $k = 1$

We will prove Theorem 18 by first proving an estimate for the ℓ^n norm of integer valued functions over $\mathbb{F}_q^n$ and reducing Theorem 18 to it.

Theorem 19. *Given $r \in \mathbb{Z}_{\geq 0}$ and a function $f : \mathbb{F}_q^n \to \mathbb{Z}$ such that for every direction γ there exists a line E_γ in that direction such that $\sum_{x\in E_\gamma} |f(x)| \geq r$ we have the following bound,*

$$\|f\|_{\ell^n}^n = \sum_{x\in\mathbb{F}_q^n} |f(x)|^n \geq \frac{r^n}{(2-q^{-1})^n}.$$

Note, if f is an indicator function for a subset of $\mathbb{F}_q^n$ and $r = q$ then the theorem above is simply the Kakeya bound in [5]. Also note that this theorem can easily be generalized to real valued functions and positive real r by taking ratios and limits.

Our proof is a simple modification of the proof of the Kakeya theorem in [5]. A more general Kakeya estimate appears in [7], but with a larger constant in place of $(2-q^{-1})^n$.

Proof of Theorem 19. Fix m to be a positive multiple of r. Let $d = mq$ where and $N = m(2q-1)/r$. It suffices to prove the following for large enough values of m:

$$\sum_{x\in\mathbb{F}_q^n}\binom{N|f(x)|+n-1}{n}\geq\binom{d+n}{n}. \tag{14}$$

Indeed, dividing by $\binom{d+n}{n}$ on both sides and substituting for d and N gives us

$$\sum_{x\in\mathbb{F}_q^n}\frac{((2q-1)m|f(x)|/r+n-1)\dots((2q-1)m|f(x)|/r)}{(mq+n)\dots(mq+1)}\geq 1.$$

As m can be arbitrarily large, we let it grow towards infinity which gives us

$$\sum_{x\in\mathbb{F}_q^n}|f(x)|^n\geq\frac{r^n}{(2-q^{-1})^n},$$

which is exactly what we want to prove. Hence, we only need to prove (14) now.

Suppose that (14) is false. Using Lemma 12, we can find a non-zero polynomial P of total degree at most d such that it vanishes on each point x of $\mathbb{F}_q^n$ with multiplicity $N|f(x)|$.

Let P^H refer to the homogenous part of P of highest degree. We make the following claim.

Claim 20. *For all $b\in\mathbb{F}_q^n$,*

$$mult(P^H,b)\geq m.$$

Proof. It is easy to see the statement is true for $b=0$ because P^H is a homogenous polynomial of degree $d>m$.

Recall, for any $\alpha\in\mathbb{Z}_{\geq 0}^n$ its weight is defined as the sum of its coordinates. Fix any $\alpha\in\mathbb{Z}_{\geq 0}$ such that $\mathrm{wt}(\alpha)=m'<m$. Let us consider $Q=P^{(\alpha)}$, that is, the αth Hasse derivative of P. Q has degree at most $d-m'$ and vanishes on every x with multiplicity $\max(N|f(x)|-m',0)$. For any direction $b\in\mathbb{F}_q^n\setminus\{0\}$, we can find a point $a\in\mathbb{F}_q^n$ such that the line $L=\{x:x=a+bt,t\in\mathbb{F}_q^n\}$ satisfies

$$\sum_{x\in L}|f(x)|\geq r. \tag{15}$$

This implies

$$\sum_{x\in L}\mathrm{mult}(Q,x)\geq\sum_{x\in L}\max(N|f(x)|-m',0)\geq Nr-qm'. \tag{16}$$

Let $Q_{a,b}(t)=Q(a+bt)$. Then $Q_{a,b}$ is a univariate polynomial of degree at most $d-m'$. Lemma 10 and (16) implies

$$\sum_{t\in\mathbb{F}_q}\mathrm{mult}(Q_{a,b},t)\geq\sum_{x\in L}\mathrm{mult}(Q,x)\geq Nr-qm'. \tag{17}$$

If $Q_{a,b}$ is non-zero then Lemma 11 and (17) give us the bound $Nr-qm'\leq d-m'$, which implies $m(q-1)\leq m'(q-1)$. This leads to a contradiction, proving that $Q(a+bt)$ is identically zero. We note $(P^H)^{(\alpha)}$ is precisely the homogenous part of highest degree of Q. $Q(a+bt)$ being identically zero implies $(P^H)^{(\alpha)}$ vanishes on b. This proves the claim. □

Putting everything together we now know that P^H, which has total degree at most d, vanishes on all values in $\mathbb{F}_q^n$ with multiplicity at least m. Lemma 11 now implies that $mq \leq d$, leading to a contradiction. This finishes the proof of the Theorem. □

We are now ready to prove Theorem 18.

Proof of Theorem 18. We will prove this theorem for random variables R such that $\mathbf{Pr}(R=x)$ is a rational number for all $x \in \mathbb{F}_q^n$. After a simple limiting argument we will obtain the statement for all random variables R. As mentioned earlier, we will reduce to Theorem 19. We let $\mathbf{Pr}(R=w) = f(x)/S$ for some positive integer S and non-negative integer $f(x)$ for all $x \in \mathbb{F}_q^n$. It is clear that $S = \sum_{x\in\mathbb{F}_q^n} f(x)$.

We note $\mathbf{H}_\infty^q(R)$ is simply going to be $-\log_q(f(v)/S)$ where $v \in \mathbb{F}_q^n$ is the mode of R.

Given any onto linear map $\phi : \mathbb{F}_q^n \to \mathbb{F}_q^{n-1}$, its kernel is some line passing through the origin with direction γ. It is easy to check that, for every $x \in \mathbb{F}_q^{n-1}$, $\mathbf{Pr}(\phi(R)=x)$ is obtained by summing $\mathbf{Pr}(R=y)$ over all y in the line through x in direction γ.

Let $\mathbf{L}_\gamma$ be the set of lines in direction γ. This means we can write $\mathbf{H}_\infty^q(\phi(R))$ as

$$\mathbf{H}_\infty^q(\phi(R)) = -\log_q\left(\max_{\ell\in\mathbf{L}_\gamma}\sum_{x\in\ell}\mathbf{Pr}(R=x)\right).$$

We now pick the ϕ for which $\mathbf{H}_\infty^q(\phi(R))$ is the largest. This is basically done by picking the direction γ such that $\max_{\ell\in\mathbf{L}_\gamma}\sum_{x\in\ell}\mathbf{Pr}(R=x)$ is the smallest. Let γ_0 be that direction and $\max_{\ell\in\mathbf{L}_{\gamma_0}}\sum_{x\in\ell}\mathbf{Pr}(R=x)$ equals r/S where r is some non-negative integer. We can now re-write the statement of the Theorem as follows:

$$\begin{aligned}
&-\log_q\left(\frac{r}{S}\right) \geq -\frac{n-1}{n}\log_q\left(\frac{f(v)}{S}\right) - \log_q(2-q^{-1}) \\
\iff &\frac{S}{r} \geq \frac{1}{2-q^{-1}}\left(\frac{S}{f(v)}\right)^{1-1/n} \\
\iff &\left(\frac{S}{f(v)}\right)^{1/n} \geq \frac{1}{2-q^{-1}}\frac{r}{f(v)} \\
\iff &\sum_{x\in\mathbb{F}_q^n} f(x)f(v)^{n-1} \geq \frac{1}{(2-q^{-1})^n}r^n \qquad (18)
\end{aligned}$$

Noting that $f(v) \geq f(x) \geq 0$ for all x, (18) immediately follows from Theorem 19. □

5 Proving the general entropic bound

Let us first prove Theorem 17 which is obtained from Theorem 18 by a simple recursion.

Proof of Theorem 17. We induct over k. Theorem 18 is precisely the case $k = 1$. Now, let it be true for some fixed k. This means given any random variable R supported over $\mathbb{F}_q^n$ we can find an onto random variable $\phi : \mathbb{F}_q^n \to \mathbb{F}_q^{n-k}$ such that,

$$\mathbf{H}_\infty^q(\phi(R)) \geq \frac{n-k}{n}\mathbf{H}_\infty^q(R) - \log_q(2-q^{-1})k. \tag{19}$$

Applying Theorem 18 on $\phi(R)$ we can find another onto function $\psi : \mathbb{F}_q^{n-k} \to \mathbb{F}_q^{n-k-1}$ such that,

$$\mathbf{H}_\infty^q(\psi(\phi(R))) \geq \frac{n-k-1}{n-k}\mathbf{H}_\infty^q(\phi(R)) - \log_q(2-q^{-1}). \tag{20}$$

Substituting (19) in (20) proves the required statement. □

6 Better bounds when n is divisible by k

In this section we will prove Theorem 4 which gives us much better bounds in the case when n is divisible by k.

Proof of Theorem 4. As k is a factor of n we can find a positive integer r such that $n = rk$. Note there exists an $\mathbb{F}_q$-linear isomorphism between $\mathbb{F}_q^n$ and $\mathbb{F}_{q^k}^r$. This quickly follows from the fact $\mathbb{F}_{q^k}$ is by definition $\mathbb{F}_q[x]/I$ where I is a principal ideal generated by a degree k irreducible polynomial in $\mathbb{F}_q[x]$. This allows us to treat a point set S in $\mathbb{F}_q^n$ as a point set in $\mathbb{F}_{q^k}^r$. It is easy to see that any line in $\mathbb{F}_{q^k}^r$ is a k-dimensional subspace in $\mathbb{F}_q^n$. This means S is a Kakeya set in $\mathbb{F}_{q^k}^r$. Using the Kakeya bound (2) we have,

$$|S| \geq \frac{1}{2^{n/k}} m^{n/k},$$

which is precisely what we wanted. □

One could use a similar argument to prove bounds in the style of Theorem 17 with better constants. In fact, when $n-k$ has a factor smaller than k we can combine the recursive argument of Theorem 17 and argument presented in this section to obtain slightly better constants for Furstenberg set bounds.

7 Proof of Theorems 2 and 3

We start by proving three lemmas. The proof of Theorem 3 depends only on Lemma 23. The other two lemmas are only needed in the proof of Theorem 2.

The first lemma shows that a set of flats witnessing a Furstenberg set contains many flats of lower dimension.

Lemma 21. *Let F be a set of k-flats in $\mathbb{F}_q^n$, one parallel to each rank k subspace, with $2 \leq k < n$. Let $1 \leq \ell < k$. The number of ℓ-flats contained in the flats of F is at least $\binom{n}{\ell}_q K(q, n-\ell, k-\ell, q^{k-\ell})$.*

Proof. The basic observation behind this lemma is that the ℓ-flats that are contained in flats of F and are parallel to a fixed rank ℓ subspace correspond to the points of a $(k-\ell, q^{k-\ell})$-Furstenberg set in $\mathbb{F}_q^{n-\ell}$. The bound in the conclusion of the lemma comes from summing over all rank ℓ subspaces of $\mathbb{F}_q^n$.

For each rank ℓ subspace Λ, choose a rank $n-\ell$ subspace P_Λ so that $\Lambda \cap P_\Lambda$ is the origin. Since $\dim(\Lambda \cap P_\Lambda) = 0$, equation (6) implies that $\overline{\Lambda, P_\Lambda} = \mathbb{F}_q^n$. Let $F_\Lambda \subset F$ be the set of flats of F that contain a translate of Λ. We will show that $K_\Lambda = \bigcup_{\Gamma \in F_\Lambda} (\Gamma \cap P_\Lambda)$ is a $(k-\ell, q^{k-\ell})$-Furstenberg set in P_Λ.

Let g be the map from k-dimensional subspaces of $\mathbb{F}_q^n$ that contain Λ to $(k-\ell)$-dimensional subspaces of P_Λ defined by $g(\Gamma) = P_\Lambda \cap \Gamma$. Since $\overline{\Gamma, P_\Lambda} = \mathbb{F}_q^n$ for any subspace Γ that contains Λ, (6) implies that g is well-defined. In addition, any rank $k-\ell$ subspace H contained in P_Λ intersects Λ only at the origin, so $\dim(\overline{\Lambda, H}) = k$. Consequently, g is bijective.

Let $v \in \mathbb{F}_q^n$ be arbitrary. Let v_Λ and v_{P_Λ} so that $v = v_\Lambda + v_{P_\Lambda}$, where $v_\Lambda \in \Lambda$ and $v_{P_\Lambda} \in P_\Lambda$. Since $\overline{\Lambda, P_\Lambda} = \mathbb{F}_q^n$, this is always possible. Let Γ be a rank k subspace that contains Λ. Then,

$$(\Gamma + v) \cap P_\Lambda = (\Gamma + v_{P_\Lambda}) \cap P_\lambda = (\Gamma + v_{P_\Lambda}) \cap (P_\Lambda + v_{P_\Lambda}) = \Gamma \cap P_\Lambda + v_{P_\Lambda}.$$

We are now ready to show that K_Λ is a $(k-\ell, q^{k-\ell})$-Furstenberg set. Let H be a $(k-\ell)$-dimensional subspace contained in P_Λ. By the hypothesis on F, there is $v \in \mathbb{F}_q^n$ such that $g^{-1}(H) + v \in F_\Lambda$. Hence, $H + v_{P_\Lambda} \subseteq K_\Lambda$.

By definition, $|K_\Lambda| \geq K(q, n-\ell, k-\ell, q^{k-\ell})$. Each point in K_Λ is the intersection of P_Λ with an ℓ-flat parallel to Λ that is contained in some flat of F. So, the set L_Λ of ℓ-flats parallel to Λ and contained in k-flats of F is in 1-1 correspondence with the set K_Λ. Hence,

$$\sum_\Lambda |L_\Lambda| = \sum_\Lambda |K_\Lambda| \geq \binom{n}{\ell}_q K(q, n-\ell, k-\ell, q^{k-\ell}),$$

where Λ ranges over all rank ℓ subspaces of $\mathbb{F}_q^n$. □

For the proof of Theorem 2, we only need the case $\ell = k-1$ of Lemma 21. The application of (1) to obtain an explicit bound on $K(q, n, 1, q)$ for use with Lemma 21 is the only application in this section of any result proved using the polynomial method.

Lemma 22. *Let $2 \leq k < n$. Let S be a (k,m)-Furstenberg set in $\mathbb{F}_q^n$. Let $\delta < 1$. Let G_r be the set of $(k-1)$-flats that are each incident to at least $r = \delta m q^{-1} + 1$ points of S. If $m \geq 2^{n+3-k} q (1-\delta)^{-2}$, then $|G_r| > 2^{k-2-n} q^{n-k+1} \binom{n}{k-1}_q$.*

Proof. Let F be a set of k-flats that each intersect S in at least m points, such that, for each rank k subspace, there exists a flat of F parallel to it.

By Lemma 21 and the Kakeya bound (1), there is a set G of $(k-1)$-flats contained in the flats of F with

$$|G| \geq K(q, n-k+1, 1, q) \binom{n}{k-1}_q \geq 2^{k-1-n} q^{n-k+1} \binom{n}{k-1}_q.$$

Let $G_p \subseteq G$ be those flats of G that are (S,r)-poor. We will show that $|G_p| < 2^{-1}|G|$, which implies the conclusion of the lemma.

Applying Lemma 6, the number of (S,r)-poor $(k-1)$-flats contained in any given k-flat is at most $(1+mq^{-1}(1-\delta)^2)^{-1}q(1-q^k)(1-q)^{-1}$. Since $m \geq 2^{n+3-k}q(1-\delta)^{-2}$, we have

$$(1+mq^{-1}(1-\delta)^2)^{-1} < 2^{k-3-n}.$$

Summing over the flats of F and using the exact expression (10) for q-binomial coefficients,

$$\begin{aligned}
|G_p| &\leq |F|(1+mq^{-1}(1-\delta)^2)^{-1}\frac{1-q^k}{1-q}q \\
&< 2^{k-3-n}|F|\frac{1-q^k}{1-q}q \\
&= 2^{k-3-n}\binom{n}{k}_q \frac{1-q^k}{1-q}q \\
&= 2^{k-3-n}\binom{n}{k-1}_q \frac{1-q^{n-k+1}}{1-q}q \\
&< 2^{k-2-n}\binom{n}{k-1}_q q^{n-k+1} \\
&\leq 2^{-1}|G|,
\end{aligned}$$

as claimed. □

The next lemma is essentially a reformulation of Lemma 5.

Lemma 23. *Let $P \subseteq \mathbb{F}_q^n$ be a set of points. Let $\delta,\gamma > 0$, and let L be a set of ℓ-flats that each contain at least δq^ℓ points of P, and suppose that $|L| = \gamma q^{n-\ell}\binom{n}{\ell}_q$. Let $\kappa = \gamma q^\ell$. Then,*

$$|P| \geq \left(\delta\kappa(\kappa+1)^{-1} - \sqrt{\delta(1-\delta)\kappa^{-1}}\right)q^n.$$

Proof. Let $\varepsilon = |P|q^{-n}$. If $\delta \leq \varepsilon$, then $|P| \geq \delta q^n$, which is stronger than the conclusion of the lemma. Hence, we may assume that $\varepsilon < \delta$.

Since each flat of L contains at least δq^ℓ points of P, it follows that $I(P,L) \geq \delta q^\ell |L|$. By Lemma 5,

$$\delta q^\ell |L| \leq \varepsilon q^\ell |L| + \sqrt{q^\ell \binom{n-1}{\ell}_q |P|\,|L|\,(1-q^{-n}|P|)}.$$

Rearranging,

$$(\delta-\varepsilon)^2 q^\ell |L| \leq \varepsilon q^n (1-\varepsilon)\binom{n-1}{\ell}_q.$$

Since $\binom{n}{\ell}_q > q^\ell\binom{n-1}{\ell}_q$, applying the hypothesis on $|L|$ gives

$$(\delta-\varepsilon)^2 q^\ell \gamma - \varepsilon(1-\varepsilon) < 0. \tag{21}$$

Since the coefficient of ε^2 in (21) is positive, ε must be greater than the smaller root of (21). Hence,

$$\begin{aligned}\varepsilon &> \frac{1+2\delta\kappa-\sqrt{(2\delta\kappa+1)^2-4(\kappa+1)\delta^2\kappa}}{2(\kappa+1)}\\ &= \frac{1+2\delta\kappa-\sqrt{1+4\delta\kappa(1-\delta)}}{2(\kappa+1)}\\ &> \frac{\delta\kappa-\sqrt{\delta\kappa(1-\delta)}}{\kappa+1}\\ &> \delta\kappa(\kappa+1)^{-1}-\sqrt{\delta(1-\delta)\kappa^{-1}}.\end{aligned}$$

□

We are now ready to prove Theorems 2 and 3.

Proof of Theorem 3. Applying Lemma 23 with $\delta = mq^{-k}$ and $\gamma = q^{k-n}$ yields

$$\begin{aligned}|S| &\geq mq^{n-k}\left(1-(q^{2k-n}+1)^{-1}-\sqrt{(1-mq^{-k})q^{n-k}m^{-1}}\right)\\ &\geq mq^{n-k}\left(1-q^{n-2k}-q^{2n-4k}-\sqrt{q^{n-k}m^{-1}}+\sqrt{q^{n-2k}}\right).\end{aligned}$$

The assumption that $k > n/2$ implies that $q^{(n-2k)/2} > q^{2(n-2k)}$, hence

$$|S| \geq mq^{n-k}\left(1-q^{n-2k}-\sqrt{q^{n-k}m^{-1}}\right).$$

□

Proof of Theorem 2. Let S be a (k,m)-Furstenberg set in $\mathbb{F}_q^n$ with $2 \leq k < m$ and $2^{n+7-k}q\varepsilon^{-2}m \leq q^k$. We show that $|S| \geq (1-\varepsilon)mq^{n-k}$.

Apply Lemma 22 to S with $\delta = 1-\varepsilon/4$. This gives a set G_r of $(k-1)$-flats, each incident to more than $(1-\varepsilon/4)mq^{-1}$ points of S, with $|G_r| > 2^{k-2-n}q^{n-k+1}\binom{n}{k-1}_q$.

Next apply Lemma 23 to G_r with $\delta = (1-\varepsilon/4)mq^{-k}$, $\ell = k-1$, and $\gamma = 2^{k-2-n}$. As in Lemma 23, let $\kappa = \gamma q^{k-1}$. Note that $q^k \geq m \geq 2^{n+7-k}q\varepsilon^{-2}$, and hence

$$\begin{aligned}\kappa(1+\kappa)^{-1} &\geq 1-\varepsilon^2 2^{-5} > 1-\varepsilon/4, \text{ and}\\ \kappa^{-1} &\leq 2^{-5}\varepsilon^2.\end{aligned}$$

Thus we have

$$\begin{aligned}|S|q^{-n} &\geq \delta\kappa(\kappa+1)^{-1}-\sqrt{\delta(1-\delta)\kappa^{-1}}\\ &> \delta(1-\varepsilon/4)-\sqrt{\delta}(\varepsilon/4)\\ &> \delta(1-\varepsilon/2)\\ &= (1-\varepsilon/4)(1-\varepsilon/2)mq^{-k}\\ &> (1-\varepsilon)mq^{-k}.\end{aligned}$$

□

Acknowledgments

The authors are grateful to the anonymous reviewer for numerous helpful comments.

References

[1] Noga Alon. Eigenvalues, geometric expanders, sorting in rounds, and Ramsey theory. *Combinatorica*, 6(3):207–219, 1986. 4

[2] Boris Bukh and Ting-Wei Chao. Sharp density bounds on the finite field Kakeya. *preprint arXiv:2108.00074*. 2

[3] Manik Dhar, Zeev Dvir, and Ben Lund. Furstenberg sets in finite fields: Explaining and improving the Ellenberg-Erman proof. *preprint arXiv:1909.02431*. 2

[4] Zeev Dvir. On the size of Kakeya sets in finite fields. *Journal of the American Mathematical Society*, 22(4):1093–1097, 2009. 1

[5] Zeev Dvir, Swastik Kopparty, Shubhangi Saraf, and Madhu Sudan. Extensions to the method of multiplicities, with applications to Kakeya sets and mergers. *SIAM Journal on Computing*, 42(6):2305–2328, 2013. 1, 5, 6, 8

[6] Jordan Ellenberg and Daniel Erman. Furstenberg sets and Furstenberg schemes over finite fields. *Algebra & Number Theory*, 10(7):1415–1436, 2016. 1, 2

[7] Jordan S. Ellenberg, Richard Oberlin, and Terence Tao. The Kakeya set and maximal conjectures for algebraic varieties over finite fields. *Mathematika*, 56(1):1–25, 2010. 2, 8

[8] Wilhelmus Hubertus Haemers et al. *Eigenvalue techniques in design and graph theory*. Number 121. Mathematisch centrum Amsterdam, 1980. 4

[9] Swastik Kopparty, Vsevolod F Lev, Shubhangi Saraf, and Madhu Sudan. Kakeya-type sets in finite vector spaces. *Journal of Algebraic Combinatorics*, 34(3):337–355, 2011. 2

[10] Ben Lund and Shubhangi Saraf. Incidence bounds for block designs. *SIAM Journal on Discrete Mathematics*, 30(4):1997–2010, 2016. 4

[11] Shubhangi Saraf and Madhu Sudan. An improved lower bound on the size of Kakeya sets over finite fields. *Anal. PDE*, 1(3):375–379, 2008. 1

[12] Jacob T Schwartz. Probabilistic algorithms for verification of polynomial identities. In *International Symposium on Symbolic and Algebraic Manipulation*, pages 200–215. Springer, 1979. 5

[13] Thomas Wolff. Recent work connected with the Kakeya problem. *Prospects in mathematics (Princeton,NJ, 1996)*, pages 29–162, 1999. 1

[14] Richard Zippel. Probabilistic algorithms for sparse polynomials. In Edward W. Ng, editor, *Symbolic and Algebraic Computation*, pages 216–226, Berlin, Heidelberg, 1979. Springer Berlin Heidelberg. 5

AUTHORS

Manik Dhar
Department of Computer Science
Princeton University
Princeton, New Jersey, USA
manikd@princeton.edu

Zeev Dvir
Department of Computer Science and Department of Mathematics
Princeton University
Princeton, New Jersey, USA
zeev.dvir@gmail.com

Ben Lund
Discrete Mathematics Group
Institute for Basic Science
Daejeon, South Korea
lund.ben@gmail.com