J Algebr Comb (2011) 34:337–355
DOI 10.1007/s10801-011-0274-8

Kakeya-type sets in finite vector spaces

Swastik Kopparty · Vsevolod F. Lev · Shubhangi Saraf · Madhu Sudan

Received: 31 March 2010 / Accepted: 10 January 2011 / Published online: 29 January 2011

Abstract For a finite vector space V and a nonnegative integer $r \le \dim V$, we estimate the smallest possible size of a subset of V, containing a translate of every r-dimensional subspace. In particular, we show that if $K \subseteq V$ is the smallest subset with this property, n denotes the dimension of V, and q is the size of the underlying field, then for r bounded and $r < n \le rq^{r-1}$, we have $|V \setminus K| = \Theta(nq^{n-r+1})$; this improves the previously known bounds $|V \setminus K| = \Omega(q^{n-r+1})$ and $|V \setminus K| = O(n^2 q^{n-r+1})$.

Keywords Kakeya set · Kakeya problem · Polynomial method · Finite field

1 Introduction and summary of results

Given a finite vector space V and a nonnegative integer $r \le \dim V$, we say that a subset $K \subseteq V$ is a *Kakeya set of rank r* if it contains a translate of every r-dimensional

S. Kopparty · S. Saraf
Computer Science and Artificial Intelligence Laboratory, MIT, 32 Vassar Street, Cambridge, MA 02139, USA

S. Kopparty
e-mail: swastik@mit.edu

S. Saraf
e-mail: shibs@mit.edu

V.F. Lev (✉)
Department of Mathematics, The University of Haifa at Oranim, Tivon 36006, Israel
e-mail: seva@math.haifa.ac.il

M. Sudan
Microsoft Research, One Memorial Drive, Cambridge, MA 02142, USA
e-mail: madhu@mit.edu

subspace of V; that is, for every subspace $L \leq V$ with $\dim L = r$, there exists a vector $v \in V$ such that $v + L \subseteq K$. The goal of this paper is to estimate the smallest possible size of such a set as a function of the rank r, the dimension $\dim V$, and the size q of the underlying field.

For a prime power q, by $\mathbb{F}_q$ we denote the finite field of order q.

As shown by Ellenberg, Oberlin, and Tao [4, Proposition 4.16], if $n \geq 2$ is an integer, q a prime power, and $K \subseteq \mathbb{F}_q^n$ a Kakeya set of rank $r \in [1, n-1]$, then

$$|K| \geq \left(1 - q^{1-r}\right)^{\binom{n}{2}} q^n,$$

provided that q is sufficiently large as compared to n. Our lower bound presents an improvement of this estimate.

Theorem 1 *If $n \geq r \geq 1$ are integers, q a prime power, and $K \subseteq \mathbb{F}_q^n$ a Kakeya set of rank r, then*

$$|K| \geq \left(\frac{q^{r+1}}{q^r + q - 1}\right)^n = \left(1 + (q-1)q^{-r}\right)^{-n} q^n.$$

The proofs of Theorem 1 and most of other results, discussed in the introduction, are postponed to subsequent sections.

We notice that Theorem 1 extends [3, Theorem 11], and indeed, the latter result is a particular case of the former, obtained for $r = 1$. The proof of Theorem 1 uses the polynomial method in the spirit of [3, 8], the major novelty introduced being that in our present settings, we have to consider polynomials over the ring of rational functions.

Using the inequality

$$(1+x)^{-m} \geq 1 - mx, \quad x \geq 0,\ m \geq 1,$$

one readily derives

Corollary 2 *If $n \geq r \geq 1$ are integers, q a prime power, and $K \subseteq \mathbb{F}_q^n$ a Kakeya set of rank r, then*

$$|K| \geq \left(1 - n(q-1)q^{-r}\right) q^n.$$

We remark that in the particular case $r = n-1$ a better estimate is known: namely, [5, Theorem 5.1] shows that if $n \geq 3$ is fixed and $K \subseteq \mathbb{F}_q^n$ is a Kakeya set of rank $n-1$, then $|K| \geq q^n - q^2 + o(q^2)$ as $q \to \infty$.

To facilitate comparison between estimates, we introduce the following terminology. Given two bounds B_1 and B_2 for the smallest size of a Kakeya set in $\mathbb{F}_q^n$ (which are either both upper bounds or both lower bounds), we say that these bounds are *essentially equivalent* in some range of n and q if there is a constant C such that for all n and q in this range, we have

$$B_1 \leq C B_2, \qquad B_2 \leq C B_1,$$

and also

$$q^n - B_1 \le C\big(q^n - B_2\big), \qquad q^n - B_2 \le C\big(q^n - B_1\big).$$

We will also say that *the estimates*, corresponding to these bounds, are essentially equivalent.

With this convention, it is not difficult to verify that for every fixed $\varepsilon > 0$, the estimates of Theorem 1 and Corollary 2 are essentially equivalent whenever $n \le (1-\varepsilon)q^{r-1}$. If $n \ge (1 + \frac{1}{q-1})\, q^{r-1}$, then the estimate of Corollary 2 becomes trivial.

The second, considerably larger in volume part of the paper, deals with the upper bounds. We here give a number of different constructions. Some of them can be regarded as refined and adjusted versions of previously known ones; other, to our knowledge, did not appear in the literature, but have been "in the air" for a while.

We first present a Kakeya set construction geared toward large fields. It is based on the "quadratic residue construction" due to Mockenhaupt and Tao [6] (with a refinement by Dvir, see [8]), the "lifting technique" from [4], and the "tensor power trick." Our starting point is [8, Theorem 8], stating that if $n \ge 1$ is an integer and q a prime power, then there exists a rank 1 Kakeya set $K \subseteq \mathbb{F}_q^n$ such that

$$|K| \le 2^{-(n-1)} q^n + O\big(q^{n-1}\big), \tag{1}$$

with an absolute implicit constant. Indeed, the proof in [8] yields the explicit estimate

$$|K| \le \begin{cases} q(\frac{q+1}{2})^{n-1} + q^{n-1} & \text{if } q \text{ is odd,} \\ (q-1)(\frac{q}{2})^{n-1} + q^{n-1} & \text{if } q \text{ is even.} \end{cases} \tag{2}$$

This can be used to construct Kakeya sets of rank higher than 1 using an observation of Ellenberg, Oberlin, and Tao.

Lemma 3 ([4, Remark 4.19]) *Let $n \ge r \ge 1$ be integers, and $\mathbb{F}$ a field. Suppose that K_1 is a rank 1 Kakeya set in the vector space $\mathbb{F}^{n-(r-1)}$, considered as a subspace of $\mathbb{F}^n$, and let $K := K_1 \cup (\mathbb{F}^n \setminus \mathbb{F}^{n-(r-1)})$. Then K is a Kakeya set of rank r in $\mathbb{F}^n$.*

Combining (2) with $n = 2$ and Lemma 3 with $n = r + 1$, we conclude that for every $r \ge 1$, there exists a Kakeya set $K \subseteq \mathbb{F}_q^{r+1}$ of rank r such that

$$|K| \le \begin{cases} (1 - \frac{q-3}{2q^r})q^{r+1} & \text{if } q \text{ is odd,} \\ (1 - \frac{q-1}{2q^r})q^{r+1} & \text{if } q \text{ is even.} \end{cases} \tag{3}$$

For $q = 3$, this estimate is vacuous. However, replacing in this case (2) with the fact that the vector space $\mathbb{F}_3^2$ contains a seven-element rank 1 Kakeya set, we find a Kakeya set $K \subseteq \mathbb{F}_3^{r+1}$ of rank r with

$$|K| \le 3^{r+1} - 2 = \left(1 - \frac{3 - (5/3)}{2 \cdot 3^r}\right) 3^{r+1}. \tag{4}$$

Since the product of Kakeya sets of rank r is a Kakeya set of rank r in the product space, from (3) and (4) we derive

Theorem 4 *Let $n \geq r \geq 1$ be integers, and q a prime power, and write*

$$\delta_q := \begin{cases} 3 & \text{if } q \text{ is odd and } q \geq 5, \\ 1 & \text{if } q \text{ is even}, \\ \frac{5}{3} & \text{if } q = 3. \end{cases}$$

There exists a Kakeya set $K \subseteq \mathbb{F}_q^n$ of rank r such that

$$|K| \leq \left(1 - \frac{q - \delta_q}{2q^r}\right)^{\lfloor \frac{n}{r+1} \rfloor} q^n.$$

We notice that if n, r, q, and δ_q are as in Theorem 4 and $n > r$, then

$$\left(1 - \frac{q - \delta_q}{2q^r}\right)^{\lfloor \frac{n}{r+1} \rfloor} \leq 1 - \Omega\left(q^{-(r-1)}\right)$$

and that the inequality

$$(1 - x)^m \leq 1 - mx + (mx)^2, \quad 0 \leq x \leq 1,\ m \geq 1,$$

shows that if $r < n \leq rq^{r-1}$, then indeed

$$\left(1 - \frac{q - \delta_q}{2q^r}\right)^{\lfloor \frac{n}{r+1} \rfloor} \leq 1 - \Omega\left(\frac{n}{r} q^{-(r-1)}\right),$$

with absolute implicit constants. Therefore, we have

Corollary 5 *Let $n > r \geq 1$ be integers, and q a prime power. There exists a Kakeya set $K \subseteq \mathbb{F}_q^n$ of rank r such that*

$$|K| \leq q^n - \Omega\left(q^{n-(r-1)}\right);$$

moreover, if $n \leq rq^{r-1}$, then in fact

$$|K| \leq q^n - \Omega\left(\frac{n}{r} q^{n-(r-1)}\right)$$

(*with absolute implicit constants*).

We remark that Corollaries 2 and 5 give nearly matching bounds on the smallest possible size of a Kakeya set of rank r in $\mathbb{F}_q^n$ in the case where r is bounded, q grows, and the dimension n does not grow "too fast."

In contrast, for q bounded and n growing, neither (1) nor Theorem 4 give satisfactory upper bounds. Specifically, the O-term in (1) do not even allow for constructing Kakeya sets of size $o(q^n)$, whereas the estimate of Theorem 4 is nontrivial, but relatively weak. Addressing this situation first in the case $r = 1$, we develop further the idea behind the proof of [8, Theorem 8] to show that the O-term just mentioned can be well controlled, making the result nontrivial in the regime under consideration.

Theorem 6 *Let $n \geq 1$ be an integer, and q a prime power. There exists a rank 1 Kakeya set $K \subseteq \mathbb{F}_q^n$ with*

$$|K| < \begin{cases} 2(1+\frac{1}{q-1})(\frac{q+1}{2})^n & \text{if } q \text{ is odd,} \\ \frac{3}{2}(1+\frac{1}{q-1})(\frac{2q+1}{3})^n & \text{if } q \text{ is an even power of } 2, \\ \frac{3}{2}(\frac{2(q+\sqrt{q}+1)}{3})^n & \text{if } q \text{ is an odd power of } 2. \end{cases}$$

Theorem 6 is to be compared against the case $r = 1$ of Theorem 1 showing that if $K \subseteq \mathbb{F}_q^n$ is a rank 1 Kakeya set, then $|K| \geq (q^2/(2q-1))^n$.

For several small values of q, the estimate of Theorem 6 can be improved using a combination of the "missing digit construction" and the "random rotation trick" of which we learned from Terry Tao, who, in turn, refers to Imre Ruzsa (personal communication in both cases).

For a field $\mathbb{F}$, by $\mathbb{F}^\times$ we denote the set of nonzero elements of $\mathbb{F}$.

The missing digit construction by itself gives a very clean but rather weak estimate.

Theorem 7 *Let $n \geq 1$ be an integer, and q a prime power, and suppose that $\{e_1, \ldots, e_n\}$ is a linear basis of $\mathbb{F}_q^n$. Let*

$$A := \left\{\varepsilon_1 e_1 + \cdots + \varepsilon_n e_n \colon \varepsilon_1, \ldots, \varepsilon_n \in \mathbb{F}_q^\times\right\}$$

and

$$B := \left\{\varepsilon_1 e_1 + \cdots + \varepsilon_n e_n \colon \varepsilon_1, \ldots, \varepsilon_n \in \{0,1\}\right\}.$$

Then $K := A \cup B$ is a rank 1 Kakeya set in $\mathbb{F}_q^n$ with

$$|K| = (q-1)^n + 2^n - 1.$$

Using the random rotation trick, we boost Theorem 7 to

Theorem 8 *Let $n \geq 1$ be an integer, and $q \geq 3$ a prime power. There exists a rank 1 Kakeya set $K \subseteq \mathbb{F}_q^n$ such that*

$$|K| < \left(\frac{q}{2^{2/q}}\right)^{n+O(\sqrt{n \ln q/q})}$$

(*with an absolute implicit constant*).

To compare Theorems 6 and 8, we notice that $(q+1)/2 < 2^{-2/q}q$ for every integer $q \geq 4$, that $(2q+1)/3 < 2^{-2/q}q$ for every integer $q \geq 5$, and that $2(q+\sqrt{q}+1)/3 < 2^{-2/q}q$ for every integer $q \geq 14$. Thus, for q fixed and n growing, Theorem 6 supersedes Theorem 8 except if $q \in \{3, 4, 8\}$. Indeed, the remark following the proof of Proposition 19 (Sect. 3) shows that the value $q = 8$ can be removed from this list.

Finally, we return to constructions of Kakeya sets of rank $r \geq 2$, with the case where q is bounded and n grows in mind. As remarked above, for r large, the bound

of Theorem 4 (and consequently, that of Corollary 5) is rather weak. The best possible construction we can give in this regime does not take linearity into account and is just a *universal set* construction where, following [2], we say that a subset of a group is k-universal if it contains a translate of every k-element subset of the group. As shown in [2], every finite abelian group G possesses a k-universal subset of size at most $8^{k-1}k|G|^{1-1/k}$. In our present context the group under consideration is the additive group of the vector space $\mathbb{F}_q^n$, in which case we were able to give a particularly simple construction of universal sets and refine slightly the bound just mentioned.

Lemma 9 *Let q be a prime power, and $n, k \geq 1$ integers satisfying $k \leq q^n$. There exists a set $U \subseteq \mathbb{F}_q^n$ with*

$$|U| = \left(1 - \left(1 - q^{-\lfloor n/k \rfloor}\right)^k\right) q^n$$

such that U contains a translate of every k-element subset of $\mathbb{F}_q^n$.

As an immediate consequence, we have

Theorem 10 *Let $n \geq r \geq 1$ be integers, and q a prime power. There exists a Kakeya set $K \subseteq \mathbb{F}_q^n$ of rank r such that*

$$|K| \leq \left(1 - \left(1 - q^{-\lfloor n/q^r \rfloor}\right)^{q^r}\right) q^n.$$

Using the estimates $\lfloor n/q^r \rfloor > n/q^r - 1$ and $(1-x)^m \geq 1 - mx$ (applied with $x = q^{-\lfloor n/q^r \rfloor}$ and $m = q^r$), we obtain

Corollary 11 *Let $n \geq r \geq 1$ be integers, and q a prime power. There exists a Kakeya set $K \subseteq \mathbb{F}_q^n$ of rank r such that*

$$|K| < q^{n(1-q^{-r})+r+1}.$$

It is not difficult to verify that Corollary 11 supersedes Corollary 5 for $n \geq (r+2)q^r$ and that for n growing, Theorem 10 supersedes Theorem 4 if r is sufficiently large as compared to q (roughly, $r > Cq/\log q$ with a suitable constant C).

A slightly more precise version of Corollary 11 is that there exists a Kakeya set $K \subseteq \mathbb{F}_q^n$ of rank r with

$$|K| \leq q^{n - \lfloor n/q^r \rfloor + r};$$

this is essentially equivalent to Theorem 10, provided that $n \geq (r+1)q^r$. (On the other hand, Theorem 10 becomes trivial if $n < q^r$.)

The remainder of the paper is mostly devoted to the proofs of Theorems 1, 6, 7, and 8, and Lemma 9. For the convenience of the reader and self-completeness, we also prove (a slightly generalized version of) Lemma 3 in the Appendix. Section 6 contains a short summary and concluding remarks.

2 Proof of Theorem 1

As a preparation for the proof of Theorem 1, we briefly review some basic notions and results related to the polynomial method; the reader is referred to [3] for an in-depth treatment and proofs.

For the rest of this section, we use multidimensional formal variables, which are to be understood just as n-tuples of "regular" formal variables with a suitable n. Thus, for instance, if n is a positive integer and $\mathbb{F}$ is a field, we can write $X = (X_1, \ldots, X_n)$ and $P \in \mathbb{F}[X]$, meaning that P is a polynomial in the n variables $X_1, \ldots, X_n$ over $\mathbb{F}$. By $\mathbb{N}_0$ we denote the set of nonnegative integers, and for X as above and an n-tuple $i = (i_1, \ldots, i_n) \in \mathbb{N}_0^n$, we let $\|i\| := i_1 + \cdots + i_n$ and $X^i := X_1^{i_1} \cdots X_n^{i_n}$.

Let $\mathbb{F}$ be a field, $n \geq 1$ an integer, and $X = (X_1, \ldots, X_n)$ and $Y = (Y_1, \ldots, Y_n)$ formal variables. To every polynomial P in n variables over $\mathbb{F}$ and every n-tuple $i \in \mathbb{N}_0^n$, there corresponds a uniquely defined polynomial $P^{(i)}$ over $\mathbb{F}$ in n variables such that

$$P(X+Y) = \sum_{i \in \mathbb{N}_0^n} P^{(i)}(Y) X^i.$$

The polynomial $P^{(i)}$ is called *the Hasse derivative of P of order i*. Notice that $P^{(0)} = P$ (which follows, for instance, by letting $X = (0, \ldots, 0)$), and if $\|i\| > \deg P$, then $P^{(i)} = 0$. Also, it is easy to check that if P_H denotes the homogeneous part of P (meaning that P_H is a homogeneous polynomial such that $\deg(P - P_H) < \deg P$) and if $(P^{(i)})_H$ denotes the homogeneous part of $P^{(i)}$, then

$$(P_H)^{(i)} = \begin{cases} (P^{(i)})_H & \text{if } \deg P^{(i)} = \deg P - \|i\|, \\ 0 & \text{if } \deg P^{(i)} < \deg P - \|i\|. \end{cases}$$

A polynomial P in n variables over a field $\mathbb{F}$ is said to *vanish at a point $a \in \mathbb{F}^n$* with multiplicity m if $P^{(i)}(a) = 0$ for each $i \in \mathbb{N}_0^n$ with $\|i\| < m$, whereas there exists $i \in \mathbb{N}_0^n$ with $\|i\| = m$ such that $P^{(i)}(a) \neq 0$. In this case, a is also said to be *a zero of P of multiplicity m*. We denote the multiplicity of zero of a nonzero polynomial P at a by $\mu(P, a)$. It is not difficult to see that the multiplicity $\mu(P, a)$ can be alternatively defined as the largest integer m with the property that

$$P(X + a) = \sum_{i \in \mathbb{N}_0^n :\ \|i\| \geq m} c(i, a) X^i; \quad c(i, a) \in \mathbb{F}.$$

Lemma 12 ([3, Lemma 5]) *Let $n \geq 1$ be an integer. If P is a nonzero polynomial in n variables over the field $\mathbb{F}$ and $a \in \mathbb{F}^n$, then for any $i \in \mathbb{N}_0^n$, we have*

$$\mu\big(P^{(i)}, a\big) \geq \mu(P, a) - \|i\|.$$

Lemma 13 ([3, Proposition 10]) *Let $n, m \geq 1$ and $k \geq 0$ be integers, and $\mathbb{F}$ a field. If a finite set $S \subseteq \mathbb{F}^n$ satisfies $\binom{m+n-1}{n} |S| < \binom{n+k}{n}$, then there is a nonzero polynomial over $\mathbb{F}$ in n variables of degree at most k, vanishing at every point of S with multiplicity at least m.*

Yet another lemma we need is a direct corollary of [3, Proposition 6].

Lemma 14 *Let $n, r \geq 1$ be integers, and P a nonzero polynomial in n variables over the field $\mathbb{F}$, and suppose that $b, d_1, \ldots, d_r \in \mathbb{F}^n$. Then for any $t_1, \ldots, t_r \in \mathbb{F}$, we have*

$$\mu\big(P(b + T_1 d_1 + \cdots + T_r d_r), (t_1, \ldots, t_r)\big) \geq \mu(P, b + t_1 d_1 + \cdots + t_r d_r),$$

where $P(b + T_1 d_1 + \cdots + T_r d_r)$ is a polynomial in the formal variables $T_1, \ldots, T_r$.

The multiplicity Schwartz–Zippel lemma is as follows.

Lemma 15 ([3, Lemma 8]) *Let $n \geq 1$ be an integer, P a nonzero polynomial in n variables over a field $\mathbb{F}$, and $S \subseteq \mathbb{F}$ a finite set. Then*

$$\sum_{z \in S^n} \mu(P, z) \leq \deg P \cdot |S|^{n-1}.$$

Corollary 16 *Let $n \geq 1$ be an integer, P a nonzero polynomial in n variables over a field $\mathbb{F}$, and $S \subseteq \mathbb{F}$ a finite set. If P vanishes at every point of S^n with multiplicity at least m, then $\deg P \geq m|S|$.*

We are now ready to prove Theorem 1.

Proof of Theorem 1 Assuming that m and k are positive integers with

$$k < q^r \left\lceil \frac{qm - k}{q - 1} \right\rceil \tag{5}$$

(no typo: k enters both sides!), we show first that

$$\binom{m + n - 1}{n} |K| \geq \binom{n + k}{n} \tag{6}$$

and then optimize by m and k.

Suppose for a contradiction that (6) fails; thus, by Lemma 13, there exists a nonzero polynomial P over $\mathbb{F}_q$ of degree at most k in n variables, vanishing at every point of K with multiplicity at least m.

Write $l := \lceil \frac{qm-k}{q-1} \rceil$ and fix $i = (i_1, \ldots, i_n) \in \mathbb{N}_0^n$ satisfying $w := \|i\| < l$. Let $Q := P^{(i)}$, the ith Hasse derivative of P.

Since K is a Kakeya set of rank r, for every $d_1, \ldots, d_r \in \mathbb{F}_q^n$, there exists $b \in \mathbb{F}_q^n$ such that $b + t_1 d_1 + \cdots + t_r d_r \in K$ for all $t_1, \ldots, t_k \in \mathbb{F}_q$; hence,

$$\mu(P, b + t_1 d_1 + \cdots + t_r d_r) \geq m,$$

and therefore, by Lemma 12,

$$\mu(Q, b + t_1 d_1 + \cdots + t_r d_r) \geq m - w$$

whenever $t_1, \ldots, t_r \in \mathbb{F}_q$. By Lemma 14, we have

$$\mu(Q, b + t_1 d_1 + \cdots + t_r d_r) \leq \mu\big(Q(b + T_1 d_1 + \cdots + T_r d_r), (t_1, \ldots, t_r)\big),$$

where $Q(b + T_1d_1 + \cdots + T_rd_r)$ is considered as a polynomial in the variables $T_1, \ldots, T_r$. Thus, for every $d_1, \ldots, d_r \in \mathbb{F}_q^n$, there exists $b \in \mathbb{F}_q^n$ such that $Q(b + T_1d_1 + \cdots + T_rd_r)$ vanishes with multiplicity at least $m - w$ at each point $(t_1, \ldots, t_r) \in \mathbb{F}_q^r$. Compared with

$$\deg Q(b + T_1d_1 + \cdots + T_rd_r) \le \deg Q \le k - w < q(m - w)$$

(as it follows from $w < l$), in view of Corollary 16, this shows that $Q(b + T_1d_1 + \cdots + T_rd_r)$ is the zero polynomial.

Let P_H and Q_H denote the homogeneous parts of the polynomials P and Q, respectively, so that $Q(b + T_1d_1 + \cdots + T_rd_r) = 0$ implies $Q_H(T_1d_1 + \cdots + T_rd_r) = 0$. Thus, $(P_H)^{(i)}(T_1d_1 + \cdots + T_rd_r) = 0$ for all $d_1, \ldots, d_r \in \mathbb{F}_q^n$. We interpret this saying that $(P_H)^{(i)}$, considered as a polynomial in n variables over the field of rational functions $\mathbb{F}_q(T_1, \ldots, T_r)$, vanishes at every point of the set

$$\{T_1d_1 + \cdots + T_rd_r : d_1, \ldots, d_r \in \mathbb{F}_q^n\} = S^n,$$

where

$$S := \{\alpha_1T_1 + \cdots + \alpha_rT_r : \alpha_1, \ldots, \alpha_r \in \mathbb{F}_q\}.$$

This shows that all Hasse derivatives of P_H of order, smaller than l, vanish on S^n; in other words, P_H vanishes with multiplicity at least l at every point of S^n. Since, on the other hand, by (5) we have

$$\deg P_H = \deg P \le k < q^r l = |S|l,$$

from Corollary 16 we conclude that P_H is the zero polynomial, which is wrong as the homogeneous part of a nonzero polynomial is nonzero.

Thus, (6) is established. Rewriting it as

$$|K| \ge \frac{(k+1)(k+2)\cdots(k+n)}{m(m+1)\cdots(m+n-1)},$$

to optimize we choose $k = Nq^{r+1} - 1$ and $m = (q^r + q - 1)N$, where N is a positive integer. With this choice, inequality (5) is satisfied for any values of N, and the assertion of Theorem 1 follows from the observation that the limit of the right-hand side as $N \to \infty$ is $(q^{r+1}/(q^r + q - 1))^n$. □

3 Proof of Theorem 6

For a field $\mathbb{F}$, a function $f : \mathbb{F} \to \mathbb{F}$, and an element $t \in \mathbb{F}$, we write

$$I_f(t) := \{f(x) + tx : x \in \mathbb{F}\}.$$

Our proof of Theorem 6 relies on the following lemma, a provisional form of which is implicitly contained in [8].

Lemma 17 *Let $n \geq 1$ be an integer, $\mathbb{F}$ a finite field, and $f : \mathbb{F} \to \mathbb{F}$ a nonlinear function. There exists a rank 1 Kakeya set $K \subseteq \mathbb{F}^n$ with*

$$|K| = \sum_{t \in \mathbb{F}} \frac{|I_f(t)|^n - 1}{|I_f(t)| - 1}.$$

Proof Let

$$K := \big\{(x_1, \ldots, x_j, t, 0, \ldots, 0) : 0 \leq j \leq n-1,\ t \in \mathbb{F},\ x_1, \ldots, x_j \in I_f(t)\big\}.$$

Since f is nonlinear, we have $|I_f(t)| > 1$ for each $t \in \mathbb{F}$, and it follows that

$$|K| = \sum_{j=0}^{n-1} \sum_{t \in \mathbb{F}} \big|I_f(t)\big|^j = \sum_{t \in \mathbb{F}} \frac{|I_f(t)|^n - 1}{|I_f(t)| - 1}.$$

To show that K is a rank 1 Kakeya set, we prove that it contains a line in every direction $d = (d_1, \ldots, d_n) \in \mathbb{F}^n \setminus \{0\}$. Without loss of generality we assume that, for some $j \in [1, n-1]$, we have $d_{j+1} = 1$ and $d_{j+2} = \cdots = d_n = 0$, and we let

$$b := \big(f(d_1), \ldots, f(d_j), 0, \ldots, 0\big).$$

For every $t \in \mathbb{F}$, we have then

$$b + td = \big(f(d_1) + td_1, \ldots, f(d_j) + td_j, t, 0, \ldots, 0\big) \in K,$$

completing the proof. □

The assertion of Theorem 6 for q odd follows immediately from Lemma 17 upon choosing $\mathbb{F} := \mathbb{F}_q$ and $f(x) := x^2$, and observing that then $|I_f(t)| = (q+1)/2$ for each $t \in \mathbb{F}$ in view of

$$x^2 + tx = (x + t/2)^2 - t^2/4.$$

In the case of q even, the assertion follows easily by combining Lemma 17 with the following two propositions.

Proposition 18 (cf. [9]) *Suppose that q is an even power of 2, and let $f(x) := x^3$ $(x \in \mathbb{F}_q)$. Then for every $t \in \mathbb{F}_q$, we have $|I_f(t)| \leq (2q+1)/3$.*

Proposition 19 *Suppose that q is an odd power of 2 and let $f(x) := x^{q-2} + x^2$ $(x \in \mathbb{F}_q)$. Then for every $t \in \mathbb{F}_q$, we have $|I_f(t)| \leq 2(q + \sqrt{q} + 1)/3$.*

To complete the proof of Theorem 6, it remains to prove Propositions 18 and 19. Indeed, Proposition 18 follows immediately from the main result of [9]; however, we include below a self-contained proof since it also serves as a simplified model of the more involved proof of Proposition 19.

We need the following well-known fact.

Lemma 20 *Suppose that q is a power of 2, and let* Tr *denote the trace function from the field $\mathbb{F}_q$ to its two-element subfield. For $\alpha, \beta, \gamma \in \mathbb{F}_q$ with $\alpha \neq 0$, the number of solutions of the equation $\alpha x^2 + \beta x + \gamma = 0$ in the variable $x \in \mathbb{F}_q$ is*

$$\begin{cases} 1 & \text{if } \beta = 0, \\ 0 & \text{if } \beta \neq 0 \text{ and } \mathrm{Tr}(\alpha\gamma/\beta^2) = 1, \\ 2 & \text{if } \beta \neq 0 \text{ and } \mathrm{Tr}(\alpha\gamma/\beta^2) = 0. \end{cases}$$

We can now prove Proposition 18.

Proof of Proposition 18 The assumption that q is an even power of 2 implies that $q-1$ is divisible by 3. Consequently, $\mathbb{F}_q$ contains $(q-1)/3+1 < (2q+1)/3$ cubes, and we assume below that $t \neq 0$.

For $x, y \in \mathbb{F}_q$, we write $x \sim y$ if $x^3 + tx = y^3 + ty$. Clearly, this defines an equivalence relation on $\mathbb{F}_q$, and $|I_f(t)|$ is just the number of equivalence classes. Since the equation $x^3 + tx = 0$ has exactly two solutions, which are 0 and $\sqrt{t}$, the set $\{0, \sqrt{t}\}$ is an equivalence class. Fix now $x \notin \{0, \sqrt{t}\}$ and consider the equivalence class of x. For $x \sim y$ to hold, it is necessary and sufficient that either $y^2 + xy + x^2 = t$ or $x = y$, and these two conditions cannot hold simultaneously in view of $x \neq \sqrt{t}$. Hence, with Tr defined as in Lemma 20, and using the assertion of the lemma, the number of elements in the equivalence class of x is

$$\begin{cases} 1 & \text{if } \mathrm{Tr}((x^2+t)/x^2) = 1, \\ 3 & \text{if } \mathrm{Tr}((x^2+t)/x^2) = 0. \end{cases}$$

As x runs over all elements of $\mathbb{F}_q \setminus \{0, \sqrt{t}\}$, the expression $(x^2+t)/x^2$ runs over all elements of $\mathbb{F}_q \setminus \{0, 1\}$. Since q is an even power of 2, we have $\mathrm{Tr}(1) = \mathrm{Tr}(0) = 0$; thus, there are $q/2-2$ values of $x \notin \{0, \sqrt{t}\}$ with $\mathrm{Tr}((x^2+t)/x^2) = 0$.

To summarize, $q/2-2$ elements of $\mathbb{F}_q$ are contained in three-element equivalence classes, the elements 0 and $\sqrt{t}$ form a two-element class, and the remaining $q/2$ elements lie in one-element classes. It follows that the number of classes is

$$\frac{q/2-2}{3} + 1 + q/2 = \frac{2q+1}{3}. \qquad \square$$

We now turn to the proof of Proposition 19.

Proof of Proposition 19 We define the equivalence relation $\sim$ and the trace function Tr on $\mathbb{F}_q$ as in the proof of Proposition 18. Notice that the assumption that q is an odd power of 2 implies that $q-1$ is not divisible by 3, whence the cube function $x \mapsto x^3$ is a bijection of $\mathbb{F}_q$ onto itself. Furthermore, we have $x^{q-2} = x^{-1}$ for $x \in \mathbb{F}_q^\times$, implying

$$I_f(t) = \left\{x^{-1} + x^2 + tx : x \in \mathbb{F}_q^\times\right\} \cup \{0\}.$$

Suppose first that $t = 0$, in which case

$$I_f(0) = \left\{x^{-1} + x^2 : x \in \mathbb{F}_q^\times\right\}$$

in view of $1^{-1}+1^2=0$. A simple computation shows that $x\sim y$ with $x,y\in\mathbb{F}_q^\times$, $x\neq y$, holds if and only if $1/(xy)=x+y$; that is, $xy^2+x^2y+1=0$. For $x\in\mathbb{F}_q^\times$ fixed, this equation in y has, by Lemma 20, two (nonzero) solutions if $\mathrm{Tr}(1/x^3)=0$, and no solutions if $\mathrm{Tr}(1/x^3)=1$. It follows that each $x\in\mathbb{F}_q^\times$ contains either three or one nonzero element in its equivalence class, according to whether $\mathrm{Tr}(1/x^3)=0$ or $\mathrm{Tr}(1/x^3)=1$. By a remark at the beginning of the proof, as x runs over all elements of $\mathbb{F}_q^\times$, so does $1/x^3$. Hence, there are exactly $q/2-1$ of those $x\in\mathbb{F}_q^\times$ with $\mathrm{Tr}(1/x^3)=0$, and $q/2$ of those $x\in\mathbb{F}_q^\times$ with $\mathrm{Tr}(1/x^3)=1$. Consequently, $|I_f(0)|$, which is the number of equivalence classes, is equal to

$$\frac{q/2-1}{3}+q/2=\frac{2q-1}{3}.$$

For the rest of the proof, we assume that $t\neq 0$.

The equation $x^{-1}+x^2+tx=t^{-1}$ is easily seen to have the solution set $\{t,1/\sqrt{t}\}$, which, therefore, is an equivalence class consisting of two elements if $t\neq 1$ or just one element if $t=1$. Fix $x\in\mathbb{F}_q^\times\setminus\{t,1/\sqrt{t}\}$. For $y\in\mathbb{F}_q^\times$, $y\neq x$, we have $x\sim y$ if and only if $1/(xy)=x+y+t$; equivalently, $xy^2+x(x+t)y+1=0$. This equation has two solutions (distinct from x and 0) if $\mathrm{Tr}(1/x(x+t)^2)=0$ and no solutions if $\mathrm{Tr}(1/x(x+t)^2)=1$. In the former case the equivalence class of x contains three nonzero elements, and, consequently, if we let

$$N:=\#\bigl\{x\in\mathbb{F}_q^\times\setminus\bigl\{t,1/\sqrt{t}\,\bigr\}\colon\ \mathrm{Tr}\bigl(1/\bigl(x(x+t)^2\bigr)\bigr)=0\bigr\},$$

then

$$\bigl|I_f(t)\bigr|\leq\begin{cases}q-\frac{2}{3}N & \text{if } t=1,\\ q-\frac{2}{3}N-1 & \text{if } t\neq 1.\end{cases}\tag{7}$$

To estimate N, we notice that

$$\frac{1}{x(x+t)^2}=\frac{1}{t^2x}+\frac{1}{t^2(x+t)}+\frac{1}{t(x+t)^2}$$

and that

$$\mathrm{Tr}\biggl(\frac{1}{t(x+t)^2}\biggr)=\mathrm{Tr}\biggl(\frac{1}{\sqrt{t}(x+t)}\biggr),$$

implying

$$\begin{aligned}\mathrm{Tr}\biggl(\frac{1}{x(x+t)^2}\biggr)&=\mathrm{Tr}\biggl(\frac{1}{t^2x}+\biggl(\frac{1}{t^2}+\frac{1}{\sqrt{t}}\biggr)\frac{1}{x+t}\biggr)\\&=\mathrm{Tr}\biggl(\frac{x/\sqrt{t}+1/t}{x(x+t)}\biggr).\end{aligned}$$

Thus, if $t=1$, then

$$\mathrm{Tr}\biggl(\frac{1}{x(x+t)^2}\biggr)=\mathrm{Tr}\biggl(\frac{1}{x}\biggr),$$

showing that

$$N = \#\big\{x \in \mathbb{F}_q \setminus \{0,1\}\colon\ \mathrm{Tr}(1/x) = 0\big\} = q/2 - 1$$

(as the assumption that q is an odd power of 2 implies $\mathrm{Tr}(1) = 1$), and hence

$$\big|I_f(1)\big| \le q - \frac{2}{3}(q/2 - 1) = \frac{2q+2}{3}$$

by (7).

Finally, suppose that $t \notin \{0,1\}$. For brevity, we write

$$R(x) := \frac{x/\sqrt{t} + 1/t}{x(x+t)},$$

and let ψ denote the additive character of the field $\mathbb{F}_q$, defined by

$$\psi(x) = (-1)^{\mathrm{Tr}(x)}, \quad x \in \mathbb{F}_q.$$

Since $R(1/\sqrt{t}) = 0$, we have

$$\begin{aligned} N &= \frac{1}{2} \sum_{x \in \mathbb{F}_q \setminus \{0,t,1/\sqrt{t}\}} \big(1 + \psi\big(R(x)\big)\big) \\ &= \frac{1}{2} \sum_{x \in \mathbb{F}_q \setminus \{0,t\}} \psi\big(R(x)\big) + \frac{q}{2} - 2. \end{aligned}$$

Using Weil's bound (as laid out, for instance, in [7, Theorem 2]), we get

$$N \ge \frac{q}{2} - 2 - \frac{1}{2}\big(2\sqrt{q} + 1\big) = \frac{q}{2} - \sqrt{q} - \frac{5}{2}.$$

Now (7) gives

$$\big|I_f(t)\big| \le q - \frac{2}{3}\big((q/2) - \sqrt{q} - (5/2)\big) - 1 = \frac{2(q + \sqrt{q} + 1)}{3},$$

which completes the proof. □

We remark that for any particular prime power q, the estimates of Propositions 18 and 19 can (potentially) be improved by computing the exact values of the quantities $|I_f(t)|$. Say, a direct inspection shows that for $q = 8$ and $f(x) := x^6 + x^2$, one has $|I_f(t)| \le 6$ for each $t \in \mathbb{F}_8$; consequently, for every integer $n \ge 1$, the vector space $\mathbb{F}_8^n$ possesses a rank 1 Kakeya set of size smaller than $\frac{8}{5} \cdot 6^n$.

A natural question arising in connection with our proof of Theorem 6 is whether and to which extent the result can be improved by choosing "better" functions f in Propositions 18 and 19 and in the application of Lemma 20 in the case of q odd. We conclude this section showing that we have almost reached the limits of the method.

Lemma 21 *For every prime power q and function $f\colon \mathbb{F}_q \to \mathbb{F}_q$, there exists an element $t \in \mathbb{F}_q$ with*

$$\bigl|I_f(t)\bigr| > q/2.$$

Proof For $x, y, t \in \mathbb{F}_q$, we write $x \overset{t}{\sim} y$ if $f(x) + tx = f(y) + ty$; equivalently, if either $x = y$, or $x \neq y$ and $(f(x) - f(y))/(x - y) = -t$. It follows from the first form of this definition that $\overset{t}{\sim}$ is an equivalence relation on $\mathbb{F}_q$ and $|I_f(t)|$ is the number of equivalence classes, and from the second form that for every pair (x, y) with $x \neq y$, there exists a unique $t \in \mathbb{F}_q$ with $x \overset{t}{\sim} y$.

For each $t \in \mathbb{F}_q$, consider the graph Γ_t on the vertex set $\mathbb{F}_q$ in which two vertices $x \neq y$ are adjacent if and only if $x \overset{t}{\sim} y$. By the remark just made, every edge of the complete graph on the vertex set $\mathbb{F}_q$ belongs to exactly one graph Γ_t. Consequently, there exists $t \in \mathbb{F}_q$ such that the number of edges of Γ_t, which we denote by $e(\Gamma_t)$, does not exceed $q^{-1}\binom{q}{2} = (q-1)/2$. By the construction, the graph Γ_t is a disjoint union of cliques; let k denote the number, and $m_1, \dots, m_k$ the sizes of these cliques. Thus, we have

$$m_1 + \cdots + m_k = q \quad \text{and} \quad \bigl|I_f(t)\bigr| = k,$$

and it remains to show that $k > q/2$. We distinguish two cases.

If q is even, then, using convexity, we get

$$\frac{q}{2} - 1 \geq e(\Gamma_t) = \binom{m_1}{2} + \cdots + \binom{m_k}{2} \geq k\binom{q/k}{2} = \frac{1}{2}\,q\left(\frac{q}{k} - 1\right),$$

whence

$$q - 1 > \frac{q^2}{2k},$$

leading to the desired bound.

If q is odd, we let

$$s := \#\bigl\{i \in [1,k]\colon m_i = 1\bigr\} \quad \text{and} \quad l := \#\bigl\{i \in [1,k]\colon m_i \geq 2\bigr\},$$

so that $s + l = k$ and

$$s + 2l \leq q. \tag{8}$$

Then

$$\begin{aligned}\frac{q-1}{2} \geq e(\Gamma_t) &= \sum_{i \in [1,k]\colon m_i \geq 2} \binom{m_i}{2} \geq l\binom{(q-s)/l}{2} \\ &= \frac{1}{2}\,(q-s)\left(\frac{q-s}{l} - 1\right) = \frac{1}{2l}\,(q-s)(q-k).\end{aligned}$$

If we had $k \leq q/2$, this would yield

$$\frac{q}{2} > \frac{q-1}{2} \geq \frac{1}{2l}\,(q-s)\cdot\frac{q}{2},$$

contradicting (8). □

4 Proof of Theorems 7 and 8

Proof of Theorem 7 Given a vector $d = \varepsilon_1 e_1 + \cdots + \varepsilon_n e_n$ with $\varepsilon_1, \ldots, \varepsilon_n \in \mathbb{F}_q$, let

$$b := \sum_{i \in [1,n]:\ \varepsilon_i = 0} e_i .$$

Thus, $b \in B$, and it is readily verified that for $t \in \mathbb{F}_q^\times$, we have $b + td \in A$. Therefore, the line through b in the direction d is entirely contained in K.

The assertion on the size of K follows from $A \cap B = \{e_1 + \cdots + e_n\}$. □

Proof of Theorem 8 We notice that the assertion is trivial if $n = O(q(\ln q)^3)$, as in this case for a sufficiently large constant C, we have

$$\left(\frac{q}{2^{2/q}}\right)^{n + C\sqrt{n \ln q / q}} > q^n;$$

consequently, we assume

$$n > 32q(\ln q)^3 \tag{9}$$

for the rest of the proof.

Fix a linear basis $\{e_1, \ldots, e_n\} \subseteq \mathbb{F}_q^n$ and, as in Theorem 7, let

$$A := \left\{\varepsilon_1 e_1 + \cdots + \varepsilon_n e_n : \varepsilon_1, \ldots, \varepsilon_n \in \mathbb{F}_q^\times\right\}$$

and

$$B := \left\{\varepsilon_1 e_1 + \cdots + \varepsilon_n e_n : \varepsilon_1, \ldots, \varepsilon_n \in \{0, 1\}\right\}.$$

Given a vector $v = \varepsilon_1 e_1 + \cdots + \varepsilon_n e_n$ with $\varepsilon_1, \ldots, \varepsilon_n \in \mathbb{F}_q$ and a scalar $\varepsilon \in \mathbb{F}_q$, let $\nu_\varepsilon(v)$ denote the number of those indices $i \in [1, n]$ with $\varepsilon_i = \varepsilon$. Set $\delta := 2\sqrt{\ln q}$ and define

$$D_0 := \left\{d \in \mathbb{F}_q^n : \nu_\varepsilon(d) > n/q - \delta(n/q)^{1/2} \text{ for all } \varepsilon \in \mathbb{F}_q\right\}$$

and

$$A_0 := \left\{a \in A : \nu_1(a) > 2n/q - 2\delta(n/q)^{1/2}\right\}.$$

Suppose that a vector $v \in \mathbb{F}_q^r$ is chosen at random, with equal probability for each vector to be chosen. For each fixed $\varepsilon \in \mathbb{F}_q$, the quantity $\nu_\varepsilon(v)$ is then a random variable, distributed binomially with the parameters n and $1/q$. As a result, using standard estimates for the binomial tail (as, for instance, [1, Theorem A.1.13]), we get

$$\mathsf{P}\left(\nu_\varepsilon(v) \le n/q - \delta(nq)^{1/2}\right) \le e^{-\delta^2(n/q)/(2n/q)} = \frac{1}{q^2}.$$

Consequently, the probability of a vector, randomly drawn from $\mathbb{F}_q^n$, not to belong to D_0, is at most $1/q$, for which reason we call the elements of D_0 *popular directions*.

If $d = \varepsilon_1 e_1 + \cdots + \varepsilon_n e_n \in D_0$, then, letting $b := \sum_{i\in[1,n]:\ \varepsilon_i=0} e_i$, for each $t \in \mathbb{F}_q^\times$, we have

$$\nu_1(b + td) = \nu_0(d) + \nu_{t^{-1}}(d) > 2n/q - 2\delta(n/q)^{1/2},$$

whence $b + td \in A_0$. Thus, the set $K_0 := B \cup A_0$ contains a line in every popular direction.

To estimate the size of K_0, we notice that, letting $N := \lfloor 2n/q - 2\delta(n/q)^{1/2} \rfloor + 1$, we have

$$|A_0| = \sum_{j=N}^{n} \binom{n}{j} (q-2)^{n-j}.$$

Assumption (9) implies that the summands in the right-hand side decay as j grows, whence

$$|A_0| \le n \binom{n}{N} (q-2)^{n-N}.$$

Consequently, writing

$$H(x) := x \ln(1/x) + (1-x)\ln\bigl(1/(1-x)\bigr), \quad x \in (0,1),$$

and using a well-known estimate for the binomial coefficients, we get

$$|A_0| < n \exp\bigl(nH(N/n) + (n-N)\ln(q-2)\bigr).$$

Now, in view of (9), we have

$$\frac{1}{q} \le \frac{N}{n} \le \frac{2}{q} \le 1 - \frac{1}{q},$$

and therefore, since $H(x)$ is concave and symmetric around the point $x = 1/2$, using (9) once again, from the mean value theorem we derive

$$\begin{aligned} H(N/n) - H(2/q) &= O\bigl((N/n - 2/q)\, H'(1/q)\bigr) \\ &= O\bigl((\ln q/(nq))^{1/2}\, H'(1/q)\bigr) \\ &= O\bigl((\ln q)^{3/2}/(nq)^{1/2}\bigr). \end{aligned}$$

Hence,

$$\begin{aligned} &nH(N/n) + (n-N)\ln(q-2) \\ &\quad = nH(2/q) + n(1-2/q)\ln(q-2) + O\bigl((n/q)^{1/2}(\ln q)^{3/2}\bigr) \\ &\quad = n\left(\ln q - \frac{2}{q}\ln 2\right) + O\bigl((n/q)^{1/2}(\ln q)^{3/2}\bigr), \end{aligned}$$

implying

$$|A_0| < \left(\frac{q}{2^{2/q}}\right)^n \exp\bigl(O\bigl((n/q)^{1/2}(\ln q)^{3/2}\bigr)\bigr).$$

Since $q/2^{2/q} > 2$ for $q \geq 3$, we conclude that

$$|K_0| \leq |A_0| + |B| < \left(\frac{q}{2^{2/q}}\right)^n \exp\bigl(O\bigl((n/q)^{1/2}(\ln q)^{3/2}\bigr)\bigr) = \left(\frac{q}{2^{2/q}}\right)^{n+O(\sqrt{n\ln q/q})}.$$

We now use the random rotation trick to replace K_0 with a slightly larger set K containing lines in *all* (not only *popular*) directions. To this end, we choose at random linear automorphisms $T_1, \ldots, T_n$ of the vector space $\mathbb{F}_q^n$ and set

$$K := T_1(K_0) \cup \cdots \cup T_n(K_0).$$

Thus, K contains a line in every direction from the set

$$D := T_1(D_0) \cup \cdots \cup T_n(D_0).$$

Choosing a vector $d \in \mathbb{F}_q^n \setminus \{0\}$ at random, for each fixed $j \in [1, n]$, the probability that $d \notin T_j(D_0)$ is at most $1/q$, whence the probability that $d \notin D$ is at most q^{-n}. Hence, the probability that $D \neq \mathbb{F}_q^n \setminus \{0\}$ is smaller than 1, showing that $T_1, \ldots, T_n$ can be instantiated so that K is a rank 1 Kakeya set. It remains to notice that $|K| \leq n|K_0|$. □

5 Proof of Lemma 9

If $k > n$, then the assertion of the lemma is trivial; suppose, therefore, that $k \leq n$, and let then $m := \lfloor n/k \rfloor$. Fix a decomposition $\mathbb{F}_q^n = V_0 \oplus V_1 \oplus \cdots \oplus V_k$, where $V_0, V_1, \ldots, V_k \leq \mathbb{F}_q^n$ are subspaces with $\dim V_i = m$ for $i = 1, \ldots, k$, and for each $i \in [0, k]$, let π_i denote the projection of $\mathbb{F}_q^n$ onto V_i along the remainder of the direct sum; thus, $v = \pi_0(v) + \pi_1(v) + \cdots + \pi_k(v)$ for every vector $v \in \mathbb{F}_q^n$. Finally, let

$$U := \bigl\{u \in \mathbb{F}_q^n \colon \pi_i(u) = 0 \text{ for at least one index } 1 \leq i \leq k\bigr\}.$$

A simple computation confirms that the size of U is as claimed. To see why U contains a translate of every k-element subset of $\mathbb{F}_q^n$, given such a subset $\{a_1, \ldots, a_k\}$, we let $b := -\pi_1(a_1) - \cdots - \pi_k(a_k)$ and observe that, for each $i \in [1, k]$,

$$\pi_i(b + a_i) = \pi_i(b) + \pi_i(a_i) = 0,$$

whence $b + a_i \in U$. □

6 Conclusion

For a vector space V and nonnegative integer $r \leq \dim V$, we defined *Kakeya sets of rank r in V* as those subsets of V, containing a translate of every r-dimensional subspace. In the case where V is finite, we established a lower bound and a number of upper bounds for the smallest possible size of such sets. Our bounds are close to best possible in the case where r is bounded and the dimension $\dim V$ does not grow "too fast." They are reasonably tight if $r = 1$ and $\dim V$ grows, particularly if q is odd and not "too small." In the case where $\dim V$ grows and $r \geq 2$, there is no reason to believe our bounds to be sharp; indeed, for $r \gtrsim q/\log q$, our best upper bound results from a universal set construction which completely ignores linearity.

Of possible improvements and research directions, the following two seem of particular interest to us. First, it would be nice to beat the universal set construction in the regime just mentioned ($\dim V$ grows and $r \geq 2$) or to show that it produces an essentially best possible bound. Even the case $q = r = 2$ seems nontrivial: we do not know any construction of Kakeya sets of rank 2 in $\mathbb{F}_2^n$ of size smaller than $O(2^{3n/4})$, the bound supplied by 4-universal sets. The second direction stems from the fact that the product of Kakeya sets of rank r is a Kakeya set of rank r in the product space. It is not difficult to derive that, with $\kappa_q^{(n)}(r)$ denoting the smallest possible size of a Kakeya set of rank r in $\mathbb{F}_q^n$, the limit $\lim_{n\to\infty} \frac{1}{n} \ln \kappa_q^{(n)}(r)$ exists for any fixed q and r. It would be very interesting to find this limit explicitly, even for just one particular pair $(q, r) \neq (2, 1)$. Arguably, most intriguing is the first nontrivial case $q = 3,\ r = 1$, due to the fact that lines in $\mathbb{F}_3^r$ are three-term arithmetic progressions.

Appendix: Proof of the lifting lemma

We prove here the following lemma, which is a slight extension of Lemma 3.

Lemma 22 *Let $n \geq r \geq r_1 \geq 1$ be integers, and $\mathbb{F}$ a field. Suppose that K_1 is a Kakeya set of rank r_1 in $\mathbb{F}^{n-(r-r_1)}$, considered as a subspace of $\mathbb{F}^n$, and let $K := K_1 \cup (\mathbb{F}^n \setminus \mathbb{F}^{n-(r-r_1)})$. Then K is a Kakeya set of rank r in $\mathbb{F}^n$.*

Proof Suppose that $L \leq \mathbb{F}^n$ is a subspace with $\dim L = r$. From

$$\dim L + \dim \mathbb{F}^{n-(r-r_1)} = \dim\bigl(L + \mathbb{F}^{n-(r-r_1)}\bigr) + \dim\bigl(L \cap \mathbb{F}^{n-(r-r_1)}\bigr)$$

it follows that either $L + \mathbb{F}^{n-(r-r_1)}$ is a proper subspace of $\mathbb{F}^n$, or $\dim(L \cap \mathbb{F}^{n-(r-r_1)}) = r_1$. Observing that if $v \notin L + \mathbb{F}^{n-(r-r_1)}$, then $v + L$ is disjoint with $\mathbb{F}^{n-(r-r_1)}$, we conclude that, in either case, there is a translate of L, intersecting $\mathbb{F}^{n-(r-r_1)}$ by a subset of an r_1-dimensional subspace. Hence, there is also a translate of L, the intersection of which with $\mathbb{F}^{n-(r-r_1)}$ is contained in K_1. By the construction, this translate of L is contained in K. □

References

1. Alon, N., Spencer, J.H.: The Probabilistic Method, 3rd edn. Wiley-Interscience Series in Discrete Mathematics and Optimization. Wiley, Hoboken (2008). xviii+352 pp.
2. Alon, N., Bukh, B., Sudakov, B.: Discrete Kakeya-type problems and small bases. Isr. J. Math. **174**, 285–301 (2009)
3. Dvir, Z., Kopparty, S., Saraf, S., Sudan, M.: Extensions to the method of multiplicities, with applications to Kakeya sets and mergers. Electron. Colloq. Comput. Complex. **16** (2009)
4. Ellenberg, J., Oberlin, R., Tao, T.: The Kakeya set and maximal conjectures for algebraic varieties over finite fields. Mathematika **56**(1), 1–25 (2009)
5. Feng, C., Li, L., Shen, J.: Some inequalities in functional analysis, combinatorics, and probability theory. Electron. J. Comb. **17**(1), #R58 (2010)
6. Mockenhaupt, G., Tao, T.: Restriction and Kakeya phenomena for finite fields. Duke Math. J. **121**(1), 35–74 (2004)
7. Moreno, C.J., Moreno, O.: Exponential sums and Goppa codes. I. Proc. Am. Math. Soc. **111**(2), 523–531 (1991)
8. Saraf, S., Sudan, M.: An improved lower bound on the size of Kakeya sets over finite fields. Anal. PDE **1**(3), 375–379 (2008)
9. Wan, D.Q.: A p-adic lifting lemma and its applications to permutation polynomials. In: Finite Fields, Coding Theory, and Advances in Communications and Computing (Las Vegas, 1991). Lecture Notes in Pure and Appl. Math., vol. 141, pp. 209–216. Dekker, New York (1993)