On the size of Kakeya sets in finite vector spaces

Gohar Kyureghyan *

Institute of Algebra and Geometry
Otto-von-Guericke University Magdeburg
39106 Magdeburg, Germany

gohar.kyureghyan@ovgu.de

Peter Müller

Institute for Mathematics
University of Würzburg
Campus Hubland Nord, 97074 Würzburg, Germany

peter.mueller@mathematik.uni-wuerzburg.de

Qi Wang

Institute of Algebra and Geometry
Otto-von-Guericke University Magdeburg
39106 Magdeburg, Germany

qi.wang@ovgu.de

Submitted: Mar 7, 2013; Accepted: Aug 29, 2013; Published: Sep 6, 2013
Mathematics Subject Classifications: 11T30, 11T06

Abstract

For a finite field $\mathbb{F}_q$, a Kakeya set K is a subset of $\mathbb{F}_q^n$ that contains a line in every direction. This paper derives new upper bounds on the minimum size of Kakeya sets when q is even.

Keywords: Kakeya set; finite vector space; Gold power function

1 Introduction

Let $\mathbb{F}_q$ be a finite field with q elements. A *Kakeya set* $K \subset \mathbb{F}_q^n$ is a set containing a line in every direction. More formally, $K \subset \mathbb{F}_q^n$ is a Kakeya set if and only if for every $\mathbf{x} \in \mathbb{F}_q^n$,

*The first and third authors thank Vsevolod Lev for bringing their attention to [7]. The third author is supported by the Alexander von Humboldt (AvH) Stiftung/Foundation.

there exists $\mathbf{y} \in \mathbb{F}_q^n$ such that $\{\mathbf{y} + t\mathbf{x} : t \in \mathbb{F}_q\} \subset K$. Wolff in [11] asked whether a lower bound of the form $|K| \geqslant C_n \cdot q^n$ holds for all Kakeya sets K, where C_n is a constant depending only on n. Dvir [2] first gave such a lower bound with $|K| \geqslant (1/n!)q^n$. Later Dvir, Kopparty, Saraf and Sudan improved the lower bound to $|K| \geqslant (1/2^n)q^n$ in [4] (see also [10]). It was shown in [4] that for any $n \geqslant 1$ there exists a Kakeya set $K \subset \mathbb{F}_q^n$ with

$$|K| \leqslant 2^{-(n-1)}q^n + O(q^{n-1}). \tag{1}$$

For more information on Kakeya sets, we refer to a recent survey [3].

When q is bounded and n grows, bound (1) is weak, and some recent papers improved the O-term in it to give better upper bounds for this case. The best currently known bound was obtained by Kopparty, Lev, Saraf and Sudan in [5], following the ideas from [10, 4] (see also [9]):

Theorem 1. *[5, Theorem 6] Let $n \geqslant 1$ be an integer and q a prime power. There exists a Kakeya set $K \subset \mathbb{F}_q^n$ with*

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

Theorem 1 was proved by constructing a Kakeya set $K \subset \mathbb{F}_q^n$ from a suitable function $f : \mathbb{F}_q \to \mathbb{F}_q$ as follows: For a given $t \in \mathbb{F}_q$, set

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

Further, define

$$K := \{(x_1, \dots, x_j, t, 0, \dots, 0) \mid 0 \leqslant j \leqslant n-1, t \in \mathbb{F}_q, x_1, \dots, x_j \in I_f(t)\}.$$

If f is a non-linear function, then K is a Kakeya set [5] of size

$$|K| = \sum_{j=0}^{n-1} \sum_{t \in \mathbb{F}_q} |I_f(t)|^j = \sum_{t \in \mathbb{F}_q} \frac{|I_f(t)|^n - 1}{|I_f(t)| - 1}. \tag{2}$$

Clearly, to construct a small Kakeya set, we need to find a function $f : \mathbb{F}_q \to \mathbb{F}_q$ for which the sets $I_f(t)$ are small. However, for a generic function $f : \mathbb{F}_q \to \mathbb{F}_q$, it is difficult to have a good estimation for the values $|I_f(t)|$, where $t \in \mathbb{F}_q$. Theorem 1 was proved by taking

- $f(x) = x^2$ for q odd, since then $|I_f(t)| \leqslant (q+1)/2$ holds for all $t \in \mathbb{F}_q$;

- $f(x) = x^3$ for q an even power of 2, since then $|I_f(t)| \leqslant (2q+1)/3$ holds for all $t \in \mathbb{F}_q$;

- $f(x) = x^{q-2} + x^2$ for q an odd power of 2, since then $|I_f(t)| \leqslant 2(q+\sqrt{q}+1)/3$ holds for all $t \in \mathbb{F}_q$.

Lemma 21 in [5] shows that for any q and any function $f : \mathbb{F}_q \to \mathbb{F}_q$, there is an element $t \in \mathbb{F}_q$ such that $|I_f(t)| > q/2$. Hence for q odd the function $f(x) = x^2$ yields the best upper bound for the minimum size of Kakeya sets produced by the construction presented above. For an even q, the authors of [5] ask whether and to which extent the bounds of Theorem 1 can be improved by choosing a better function f. In this paper, we investigate this question further and derive indeed better upper bounds on the size of Kakeya sets $K \subset \mathbb{F}_q^n$, when q is even. Our main result is

$$|K| < \begin{cases} \frac{2q}{q+\sqrt{q}-2}\left(\frac{q+\sqrt{q}}{2}\right)^n & \text{if } q \text{ is an even power of 2,} \\ \frac{8q}{5q+2\sqrt{q}-3}\left(\frac{5q+2\sqrt{q}+5}{8}\right)^n & \text{if } q \text{ is an odd power of 2.} \end{cases} \tag{3}$$

When q is an even power of 2, say $q = 2^m$, we prove (3) by determining explicitly the values $|I_f(t)|$ for $f(x) = x^{2^{m/2}+1}$ and $t \in \mathbb{F}_q$. In the case q is an odd power of 2, the result follows with $f(x) = x^4 + x^3$. Presently, it is not clear to us, whether the bounds in (3) can be improved.

The following result by Bluher [1] is used later in the paper:

Theorem 2. *[1, Theorem 5.6] Let $q = 2^m$ and $0 \leqslant i < m$ with $d = \gcd(i, m)$. Let N_0 denote the number of $b \in \mathbb{F}_q^*$ such that $x^{2^i+1} + bx + b$ has no root in $\mathbb{F}_q$.*

(i) If m/d is even, then $N_0 = \dfrac{2^d(q-1)}{2(2^d+1)}$.

(ii) If m/d is odd, then $N_0 = \dfrac{2^d(q+1)}{2(2^d+1)}$.

2 On Kakeya sets constructed using Gold power functions

In this section, we use the Gold power functions $f(x) = x^{2^i+1}$ to derive upper bounds on the minimum size of Kakeya sets $K \subset \mathbb{F}_q^n$ with q even. Theorem 2 allows us to determine explicitly the size of the image set $I_f(t) := \{f(x) + tx : x \in \mathbb{F}_q\}$ with $f(x) = x^{2^i+1}$ and $t \in \mathbb{F}_q$.

Proposition 3. *Let $q = 2^m$, $f(x) = x^{2^i+1} \in \mathbb{F}_q[x]$ with $0 \leqslant i < m$, and $d = \gcd(i, m)$. Set $I_f(t) := \{f(x) + tx : x \in \mathbb{F}_q\}$ for $t \in \mathbb{F}_q$. We have:*

(i) if m/d is even, then $|I_f(0)| = 1 + \dfrac{q-1}{2^d+1}$, *and* $|I_f(t)| = \dfrac{q+1}{2} + \dfrac{q-1}{2(2^d+1)}$ *for all $t \in \mathbb{F}_q^*$;*

(ii) if m/d is odd, then $|I_f(0)| = q$, and $|I_f(t)| = \dfrac{q-1}{2} + \dfrac{q+1}{2(2^d+1)}$ for all $t \in \mathbb{F}_q^*$.

Proof. For $t = 0$, we have

$$|I_f(0)| = 1 + \frac{2^m - 1}{\gcd(2^m - 1, 2^i + 1)}.$$

From the well-known fact (e.g. [8, Lemma 11.1]) that

$$\gcd(2^m - 1, 2^i + 1) = \begin{cases} 1 & \text{if } m/d \text{ is odd,} \\ 2^d + 1 & \text{if } m/d \text{ is even,} \end{cases}$$

the assertion on $|I_f(0)|$ follows.

For $t \in \mathbb{F}_q^*$, by definition, we have

$$\begin{aligned} |I_f(t)| &= |\{f(x) + tx : x \in \mathbb{F}_q\}| \\ &= |\mathbb{F}_q| - |\{c \in \mathbb{F}_q^* : f(x) + tx + c \text{ has no root in } \mathbb{F}_q\}| \\ &= q - N_0'. \end{aligned}$$

To make use of Theorem 2, we transform $f(x) + tx + c$ following the steps in [1]. Since $t \neq 0$ and $c \neq 0$, let $x = \dfrac{c}{t} z$, then

$$\begin{aligned} & f(x) + tx + c \\ &= x^{2^i+1} + tx + c \\ &= \frac{c^{2^i+1}}{t^{2^i+1}} \left(z^{2^i+1} + \frac{t^{2^i+1}}{c^{2^i}} z + \frac{t^{2^i+1}}{c^{2^i}} \right). \end{aligned}$$

Since

$$\left\{ \frac{t^{2^i+1}}{c^{2^i}} : c \in \mathbb{F}_q^* \right\} = \mathbb{F}_q^*,$$

we have $N_0' = N_0$, where N_0 denotes the number of $b \in \mathbb{F}_q^*$ such that $x^{2^i+1} + bx + b$ has no root in $\mathbb{F}_q$. The conclusion then follows from Theorem 2. □

Proposition 3 shows that the smallest Kakeya sets constructed using Gold power functions are achieved with $i = m/2$ for an even m, and $i = 0$ for an odd m. The discussion below shows that the choice $i = m/2$ implies a better upper bound on Kakeya sets compared with the one given in Theorem 1. The idea to use $f(x) = x^{2^{m/2}+1}$ to improve the bound in Theorem 1 appears in [6], and was independently suggested by David Speyer in [7]. Observe that $f(x) = x^3$ chosen in [5] to prove the bound for m even is the Gold power function with $i = 1$ and $d = 1$.

When m/d is odd, $|I_f(0)| = q$, and therefore the bound obtained by the Gold power functions cannot be good for large n. However, for small values of n, it is better than the one of Theorem 1 [6].

Next consider the function $f(x) = x^{2^{m/2}+1}$. In particular, we show that this function yields a better upper bound on the minimum size of Kakeya sets in $\mathbb{F}_q^n$ when q is an even power of 2. First we present a direct proof for the size of the sets $\{x^{2^{m/2}+1} + tx : x \in \mathbb{F}_q\}, t \in \mathbb{F}_q$.

Theorem 4. *Let m be an even integer. Then*

$$|I(0)| := |\{x^{2^{m/2}+1} : x \in \mathbb{F}_q\}| = 2^{m/2},$$

and

$$|I(t)| := |\{x^{2^{m/2}+1} + tx : x \in \mathbb{F}_q\}| = \frac{2^m + 2^{m/2}}{2}$$

for all $t \in \mathbb{F}_q^*$.

Proof. The identity on $I(0)$ is clear, since the image set of the function $x \mapsto x^{2^{m/2}+1}$ is $\mathbb{F}_{2^{m/2}}$. Let $t \in \mathbb{F}_q^*$. Note that $|I(t)| = |I(1)|$. Indeed, there is $s \in \mathbb{F}_q$, such that $t = s^{2^{m/2}}$ and then

$$x^{2^{m/2}+1} + tx = s^{2^{m/2}+1} \cdot \left((x/s)^{2^{m/2}+1} + (x/s)\right).$$

Hence it is enough to compute $I(1)$. Let $Tr(x) = x^{2^{m/2}} + x$ be the trace map from $\mathbb{F}_q$ onto its subfield $\mathbb{F}_{2^{m/2}}$. Recall that Tr is a $\mathbb{F}_{2^{m/2}}$-linear surjective map.

Set $g(x) = x^{2^{m/2}+1} + x$. If $y, z \in \mathbb{F}_q$ are such that

$$g(z) = z^{2^{m/2}+1} + z = y^{2^{m/2}+1} + y = g(y),$$

then $z = y + u$ for some $u \in \mathbb{F}_{2^{m/2}}$, since the image set of the function $x \mapsto x^{2^{m/2}+1}$ is $\mathbb{F}_{2^{m/2}}$. Further, for any $u \in \mathbb{F}_{2^{m/2}}$

$$g(y+u) = (y+u)^{2^{m/2}+1} + y + u = y^{2^{m/2}+1} + y + u(y^{2^{m/2}} + y) + u^2 + u.$$

Hence, $g(y) = g(y+u)$ if and only if

$$u(y^{2^{m/2}} + y) + u^2 + u = u(Tr(y) + u + 1) = 0.$$

Consequently, two distinct elements y and z share the same image under the function g if and only $Tr(y) \neq 1$ and $z = y + Tr(y) + 1$. This shows that g is injective on the set $\mathcal{O}$ of elements from $\mathbb{F}_q$ having trace 1, and 2-to-1 on $\mathbb{F}_q \setminus \mathcal{O}$, completing the proof. $\square$

Theorem 5. *Let $q = 2^m$ with m even and $n \geqslant 1$. There is a Kakeya set $K \subset \mathbb{F}_q^n$ such that*

$$|K| < \frac{2q}{q + \sqrt{q} - 2}\left(\frac{q + \sqrt{q}}{2}\right)^n.$$

Proof. The statement follows from (2) and Theorem 4. $\square$

3 On Kakeya sets constructed using the function $x \mapsto x^4 + x^3$

In this section we obtain an upper bound on the minimum size of Kakeya sets constructed using the function $x \mapsto x^4 + x^3$ on $\mathbb{F}_q$. For every $t \in \mathbb{F}_q$, let $g_t : \mathbb{F}_q \to \mathbb{F}_q$ be defined by

$$g_t(x) := x^4 + x^3 + tx.$$

Next we study the image sets of functions $g_t(x)$. Given $y \in \mathbb{F}_q$, let $g_t^{-1}(y)$ be the set of preimages of y, that is

$$g_t^{-1}(y) := \{x \in \mathbb{F}_q \mid g_t(x) = y\}.$$

Further, for any integer $k \geqslant 0$ put $\omega_t(k)$ to denote the number of elements in $\mathbb{F}_q$ having exactly k preimages under $g_t(x)$, that is

$$\omega_t(k) := |\{y \in \mathbb{F}_q \ : \ |g_t^{-1}(y)| = k\}|.$$

Note that $\omega_t(k) = 0$ for all $k \geqslant 5$, since the degree of $g_t(x)$ is 4. The next lemma establishes the value of $\omega_t(1)$:

Lemma 6. *Let $q = 2^m$ and $t \in \mathbb{F}_q^*$. Then*

- *if m is odd*
$$\omega_t(1) = \begin{cases} \frac{q+1}{3} & \text{if } Tr(t) = 0 \\ \frac{q+4}{3} & \text{if } Tr(t) = 1 \end{cases}$$
- *if m is even*
$$\omega_t(1) = \begin{cases} \frac{q-1}{3} & \text{if } Tr(t) = 0 \\ \frac{q+2}{3} & \text{if } Tr(t) = 1. \end{cases}$$

Proof. Let $y \in \mathbb{F}_q$ and $y \neq t^2$. Then $t^{2^{m-1}}$ is not a solution of the following equation

$$h_{t,y}(x) := g_t(x) + y = x^4 + x^3 + tx + y = 0.$$

Observe that the number of the solutions for the above equation is equal to the one of

$$(t^2 + y)x^4 + t^{2^{m-1}}x^2 + x + 1 = x^4 \cdot h_{t,y}\left(\frac{1}{x} + t^{2^{m-1}}\right) = 0.$$

Hence either $\omega_t(1)$ or $\omega_t(1) - 1$ is equal to the number of elements $y \in \mathbb{F}_q$ such that the affine polynomial

$$(t^2 + y)x^4 + t^{2^{m-1}}x^2 + x + 1 \tag{4}$$

has exactly one zero in $\mathbb{F}_q$, depending on the number of preimages of $g_t(x)$ for t^2. Equation (4) has exactly 1 solution if and only if the linearized polynomial

$$(t^2 + y)x^4 + t^{2^{m-1}}x^2 + x$$

has no non-trivial zeros, or equivalently

$$u(x) := (t^2 + y)x^3 + t^{2^{m-1}} x + 1 \tag{5}$$

has no zeroes.

Since $t^2 + y \neq 0$, the number of zeroes of $u(x)$ is equal to the one of

$$\frac{1}{t^2+y} \cdot u\left(\frac{1}{t^{2^{m-1}}} z\right) = \frac{1}{t^{2^{m-1}+1}} \left(z^3 + \frac{t^{2^{m-1}+1}}{t^2+y} z + \frac{t^{2^{m-1}+1}}{t^2+y} \right).$$

Note that

$$\left\{ \frac{t^{2^{m-1}+1}}{t^2+y} : y \in \mathbb{F}_q, y \neq t^2 \right\} = \mathbb{F}_q^*.$$

Hence by Theorem 2 with $i = 1$, the number of elements $y \in \mathbb{F}_q, y \neq t^2$, such that (5) has no zeros is

$$\begin{cases} \frac{q+1}{3} & \text{if } m \text{ is odd} \\ \frac{q-1}{3} & \text{if } m \text{ is even.} \end{cases}$$

To complete the proof, it remains to consider $y = t^2$. In this case

$$g_t(x) + y = x^4 + x^3 + tx + t^2 = (x^2 + t)(x^2 + x + t),$$

and therefore $g_t(x) + t^2$ has exactly one solution if $Tr(t) = 1$ and exactly 3 solutions if $Tr(t) = 0$.

□

Lemma 7. *Let $q = 2^m$ and $t \in \mathbb{F}_q^*$. Then*

$$\omega_t(3) = \begin{cases} 1 & \text{if } Tr(t) = 0 \\ 0 & \text{if } Tr(t) = 1. \end{cases}$$

Proof. The proof of Lemma 6 shows that for any $y \neq t^2$, the number of solutions for $h_{t,y}(x) = 0$ is a power of 2. Hence only t^2 may have 3 preimages under $g_t(x)$, which is the case if and only if $Tr(t) = 0$. □

The next lemma describes the behavior of the function $x^4 + x^3$:

Lemma 8. *Let $q = 2^m$ and $k \geqslant 1$ an integer. Then*

- *if m is odd*

$$\omega_0(k) = \begin{cases} q/2 & \text{if } k = 2 \\ 0 & \text{otherwise,} \end{cases}$$

in particular, the cardinality of $I(0) := \{x^4 + x^3 : x \in \mathbb{F}_q\}$ is $q/2$.

- *if m is even*

$$\omega_0(k) = \begin{cases} 1 & \text{if } k = 2 \\ \frac{2(q-1)}{3} & \text{if } k = 1 \\ \frac{(q-4)}{12} & \text{if } k = 4 \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Note that $x^4 + x^3 = 0$ has 2 solutions. Let $y \in \mathbb{F}_q^*$. Then the steps of the proof for Lemma 6 show that the number of solutions of

$$x^4 + x^3 + y = 0$$

is equal to the one of the affine polynomial

$$a_y(x) := yx^4 + x + 1.$$

If the set of zeros of $a_y(x)$ is not empty, then the number of zeros of $a_y(x)$ is equal to the one of the linearized polynomial

$$l_y(x) := yx^4 + x.$$

If m is odd, then $l_y(x)$ has exactly 2 zeroes for every $y \neq 0$, implying the statement for m odd. If m is even, then $l_y(x)$ has only the trivial zero if y is a non-cube in $\mathbb{F}_q$, and otherwise it has 4 zeroes. To complete the proof, it remains to recall that the number of non-cubes in $\mathbb{F}_q$ is $2(q-1)/3$. $\square$

Lemmas 6–8 yield the following upper bound for the size of the image sets of the considered functions:

Theorem 9. *Let $q = 2^m$ with m odd. For $t \in \mathbb{F}_q$ set $I(t) := \{x^4 + x^3 + tx : x \in \mathbb{F}_q\}$. Let v be the number of pairs $x, z \in \mathbb{F}_q$ with $x^2 + zx = z^3 + z^2 + t$. Then for $t \neq 0$*

$$|I(t)| = \frac{5}{8}q + \frac{q+1-v}{8} + \frac{\delta}{2} < \frac{5}{8}q + \frac{2\sqrt{q}+5}{8},$$

where $\delta = 0$ or 1 if $Tr(t) = 0$ or 1, respectively.

Proof. Note that

$$|I(t)| = \omega_t(1) + \omega_t(2) + \omega_t(3) + \omega_t(4)$$

and

$$q = \omega_t(1) + 2 \cdot \omega_t(2) + 3 \cdot \omega_t(3) + 4 \cdot \omega_t(4).$$

Let v' be the number of distinct elements $x, y \in \mathbb{F}_q$ with $x^4 + x^3 + tx = y^4 + y^3 + ty$. Clearly

$$v' = 2\omega_t(2) + 6\omega_t(3) + 12\omega_t(4),$$

hence

$$|I(t)| = \frac{5q - v' + 3\omega_t(1) - \omega_t(3)}{8}.$$

Setting $y = x + z$, we see that $x^4 + x^3 + tx = y^4 + y^3 + ty$ for $x \neq y$ is equivalent to $x^2 + zx = z^3 + z^2 + t$ for $z \neq 0$. However, for $z = 0$ this latter equation has a unique solution, so $v = v' + 1$.

Together with Lemmas 6–8 we see that the size of $I(t)$ is as claimed. The inequality follows from the Hasse bound for points on elliptic curves, which in our case says that $|v - q| \leqslant 2\sqrt{q}$. (Note that the projective completion of the curve $X^2 + ZX = X^3 + X^2 + t$ has a unique point at infinity.) $\square$

The bound obtained in Theorem 9 can be stated also as follows

$$|I(t)| \leqslant \left\lfloor \frac{5}{8}q + \frac{2\sqrt{q}+5}{8} \right\rfloor, \tag{6}$$

since $|I(t)|$ is an integer. Our numerical calculations show that for odd $1 \leqslant m \leqslant 13$ bound (6) is sharp, that is for these m there are elements $t \in \mathbb{F}_{2^m}$ for which equality holds in (6).

Theorem 10. *Let $q = 2^m$ with m odd and $n \geqslant 1$. There is a Kakeya set $K \subset \mathbb{F}_q^n$ such that*

$$|K| < \frac{8q}{5q + 2\sqrt{q} - 3}\left(\frac{5q + 2\sqrt{q} + 5}{8}\right)^n.$$

Proof. The statement follows from (2) and Theorem 9. $\square$

References

[1] A. W. Bluher. On $x^{q+1} + ax + b$. *Finite Fields Appl.*, 10(3):285–305, 2004.

[2] Z. Dvir. On the size of Kakeya sets in finite fields. *J. Amer. Math. Soc.*, 22(4):1093–1097, 2009.

[3] Z. Dvir. Incidence theorems and their applications. *arXiv preprint arXiv:1208.5073*, 2012.

[4] Z. Dvir, S. Kopparty, S. Saraf, and M. Sudan. Extensions to the method of multiplicities, with applications to Kakeya sets and mergers. In *2009 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2009)*, pages 181–190. IEEE Computer Soc., Los Alamitos, CA, 2009.

[5] S. Kopparty, V. F. Lev, S. Saraf, and M. Sudan. Kakeya-type sets in finite vector spaces. *J. Algebraic Combin.*, 34(3):337–355, 2011.

[6] G. Kyureghyan and Q. Wang. An upper bound on the size of kakeya sets in finite vector spaces. *to appear in proceedings of WCC 2013*.

[7] V. F. Lev. A mixing property for finite fields of characteristic 2, 2012. http://mathoverflow.net/questions/102751/a-mixing-property-for-finite-fields-of-characteristic-2.

[8] R. J. McEliece. *Finite fields for computer scientists and engineers*. The Kluwer International Series in Engineering and Computer Science, 23. Kluwer Academic Publishers, Boston, MA, 1987.

[9] G. Mockenhaupt and T. Tao. Restriction and Kakeya phenomena for finite fields. *Duke Math. J.*, 121(1):35–74, 2004.

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

[11] T. Wolff. Recent work connected with the Kakeya problem. In *Prospects in mathematics (Princeton, NJ, 1996)*, pages 129–162. Amer. Math. Soc., Providence, RI, 1999.