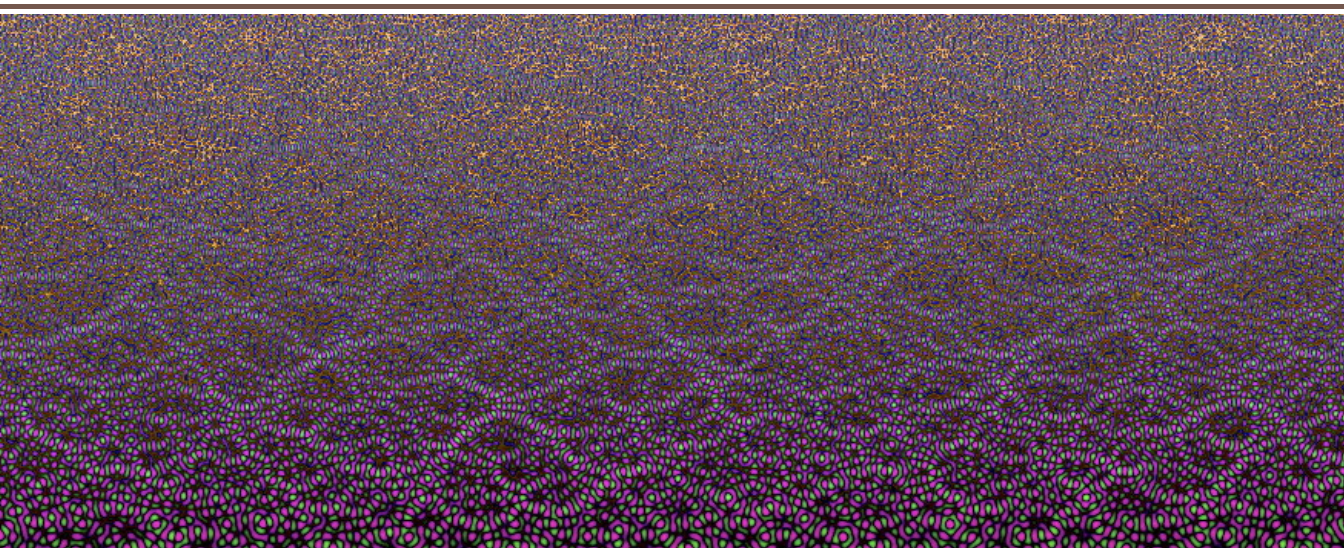
ANALYSIS & PDE

Volume 1 No. 3 2008

AN IMPROVED LOWER BOUND ON THE SIZE OF KAKEYA SETS OVER FINITE FIELDS

SHUBHANGI SARAF AND MADHU SUDAN



mathematical sciences publishers

ANALYSIS AND PDE
Vol. 1, No. 3, 2008

AN IMPROVED LOWER BOUND ON THE SIZE OF KAKEYA SETS OVER FINITE FIELDS

SHUBHANGI SARAF AND MADHU SUDAN

In a recent breakthrough, Dvir showed that every Kakeya set in $\mathbb{F}^n$ must have cardinality at least $c_n|\mathbb{F}|^n$, where $c_n \approx 1/n!$. We improve this lower bound to $\beta^n|\mathbb{F}|^n$ for a constant $\beta > 0$. This pins down the correct growth of the constant c_n as a function of n (up to the determination of β).

Let $\mathbb{F}$ be a finite field with q elements. A set $K \subseteq \mathbb{F}^n$ is said to be a *Kakeya set* in $\mathbb{F}^n$ if, for every $\boldsymbol{b} \in \mathbb{F}^n$, there exists a point $\boldsymbol{a} \in \mathbb{F}^n$ such that, for every $t \in \mathbb{F}$, the point $\boldsymbol{a} + t\,\boldsymbol{b}$ lies in K. In other words, K contains an affine line in every direction.

The question of establishing lower bounds on the size of Kakeya sets was posed in [Wolff 1999]. Till recently, the best known lower bound on the size of Kakeya sets was of the form $q^{\alpha n}$ for some $\alpha < 1$. In a recent breakthrough Dvir [2008] showed that every Kakeya set must have cardinality at least $c_n q^n$ for $c_n = (n!)^{-1}$. (Dvir originally achieved a weaker lower bound of $c_n q^{n-1}$, but the paper cited includes the stronger bound of $c_n q^n$, the improvements being attributed to Alon and Tao.) We show:

Theorem 1. *There exist constants $c_0, c_1 > 0$ such that for all n, if K is a Kakeya set in $\mathbb{F}^n$ then $|K| \geq c_0 (c_1 q)^n$.*

Remark. Our proofs give some tradeoffs on the constants c_0, c_1 that are achievable. We comment on the constants at the end of the paper.

Our improvement shows that c_n remains bounded from below by β^n for some fixed $\beta > 0$. While this improvement in the lower bound on the size of Kakeya sets is quantitatively small (say, compared to the improvement of Alon and Tao over Dvir's original bound), it is qualitatively significant in that it does determine the growth of the leading constant c_n, up to the determination of the right constant β. In particular, it compares well with known upper bounds. Previously, it was known there exists a constant $\beta < 1$ such that there are Kakeya sets of cardinality at most $\beta^n q^n$, for every odd q. A bound of $\beta \leq 1/\sqrt{2}$ follows from [Mockenhaupt and Tao 2004] and the fact that products of Kakeya sets are Kakeya sets (in higher dimension). The best known constant has $\beta \to \frac{1}{2}$ due to Dvir (personal communication, 2008). We include his proof here (see Section 3), complementing it with a similar construction and bound for the case of even q as well (so now the upper bounds work for all large fields).

Our proof follows the one in [Dvir 2008]. Given a Kakeya set K in $\mathbb{F}^n$, we show that there exists an n-variate polynomial, whose degree is bounded from above by some function of $|K|$, that vanishes at all of K. Looking at restrictions of this polynomial to lines yields that this polynomial has too many zeroes, which in turn yields a lower bound on the size of K. Our main difference is that we look for polynomials that vanish with high multiplicity at each point in K. The requirement of high multiplicity forces the

MSC2000: primary 52C17; secondary 05B25.
Keywords: Kakeya set, finite fields, polynomial method.

degree of the n-variate polynomial to go up slightly, but yields more zeroes when this polynomial is restricted to lines. The resulting tradeoff turns out to yield an improved bound. (We note that this is similar to the techniques used for the improved method of list decoding of Reed-Solomon codes created by Guruswami and Sudan [1999].)

In the next section we give the preliminaries that will be needed for the proof of Theorem 1. The actual proof of the theorem appears in Section 2. In Section 3, we give Dvir's proof for the upper bound for the size of Kakeya sets.

1. Preliminaries

For $\boldsymbol{x} = \langle x_1, \ldots, x_n \rangle$, let $\mathbb{F}[\boldsymbol{x}]$ denote the ring of polynomials in $x_1, \ldots, x_n$ with coefficients in $\mathbb{F}$. We recall the following basic fact on polynomials.

Fact 2. *Let $P \in \mathbb{F}[\boldsymbol{x}]$ be a polynomial of degree at most $q-1$ in each variable. If $P(\boldsymbol{a}) = 0$ for all $\boldsymbol{a} \in \mathbb{F}^n$, then $P \equiv 0$.*

For integer $m \geq 0$, let $N_q(n, m)$ denote the number of monomials in n variables of total degree less than mq and of individual degree at most $q-1$ in each variable.

We say that a polynomial $g \in \mathbb{F}[\boldsymbol{x}]$ has a zero of *multiplicity* m at a point $\boldsymbol{a} \in \mathbb{F}^n$ if the polynomial $g_{\boldsymbol{a}}(\boldsymbol{x}) = g(\boldsymbol{x} + \boldsymbol{a})$ has no support on monomials of degree strictly less than m. Note that the coefficients of $g_{\boldsymbol{a}}$ are (homogeneous) linear forms in the coefficients of g and thus the constraint g has a zero of multiplicity m at $\boldsymbol{a}$ yields $\binom{m+n-1}{n}$ homogeneous linear constraints on the coefficients of g. As a result we conclude:

Proposition 3. *Given a set $S \subseteq \mathbb{F}^n$ satisfying $\binom{m+n-1}{n} |S| < N_q(n, m)$, there exists a nonzero polynomial $g \in \mathbb{F}[\boldsymbol{x}]$ of total degree less than mq and degree at most $q-1$ in each variable such that g has a zero of multiplicity m at every point $\boldsymbol{a} \in S$.*

Proof. The number of possible coefficients for g is $N_q(n, m)$ and the number of (homogeneous) linear constraints is $\binom{m+n-1}{n} |S| < N_q(n, m)$. Since the number of constraints is strictly smaller than the number of unknowns, there is a nontrivial solution. □

For $g \in \mathbb{F}[\boldsymbol{x}]$ we let $g_{\boldsymbol{a},\boldsymbol{b}}(t) = g(\boldsymbol{a} + t\,\boldsymbol{b})$ denote its restriction to the line $\{\boldsymbol{a} + t\,\boldsymbol{b} \mid t \in \mathbb{F}\}$. We note the following facts on the restrictions of polynomials to lines.

Proposition 4. *If $g \in \mathbb{F}[\boldsymbol{x}]$ has a root of multiplicity m at some point $\boldsymbol{a} + t_0\boldsymbol{b}$ then $g_{\boldsymbol{a},\boldsymbol{b}}$ has a root of multiplicity m at t_0.*

Proof. By definition, the fact that g has a zero of multiplicity m at $\boldsymbol{a} + t_0\boldsymbol{b}$ implies that the polynomial $g(\boldsymbol{x} + (\boldsymbol{a} + t_0\boldsymbol{b}))$ has no support on monomials of degree less than m. Thus, under the homogeneous substitution $\boldsymbol{x} \leftarrow t\,\boldsymbol{b}$, we get no monomials of degree less than m either, and thus we have t^m divides $g(t\boldsymbol{b} + (\boldsymbol{a} + t_0\boldsymbol{b})) = g(\boldsymbol{a} + (t + t_0)\boldsymbol{b}) = g_{\boldsymbol{a},\boldsymbol{b}}(t + t_0)$. The final form implies that $g_{\boldsymbol{a},\boldsymbol{b}}$ has a zero of multiplicity m at t_0. □

Proposition 5 [Dvir 2008]. *Let $g \in \mathbb{F}[\boldsymbol{x}]$ be a nonzero polynomial of total degree d and let g_0 be the (unique, nonzero) homogeneous polynomial of degree d such that $g = g_0 + g_1$ for some polynomial g_1 of degree strictly less than d. Then $g_{\boldsymbol{a},\boldsymbol{b}}(t) = g_0(\boldsymbol{b})t^d + h(t)$ where h is a polynomial of degree strictly less than d.*

2. Proof of Theorem 1

Lemma 6. *If K is a Kakeya set in $\mathbb{F}^n$, then for every integer $m \geq 0$, $|K| \geq \binom{m+n-1}{n}^{-1} N_q(n, m)$.*

Proof. Assume for a contradiction that $|K| < \binom{m+n-1}{n}^{-1} N_q(n, m)$. Let $g \in \mathbb{F}[\boldsymbol{x}]$ be a nonzero polynomial of total degree less than mq and degree at most $q-1$ in each variable that has a zero of multiplicity m for each $x \in K$. (Such a polynomial exists by Proposition 3.) Let $d < mq$ denote the total degree of g and let $g = g_0 + g_1$ where g_0 is homogeneous of degree d and g_1 has degree less than d. Note that g_0 is also nonzero and has degree at most $q-1$ in every variable.

Now fix a direction $\boldsymbol{b} \in \mathbb{F}^n$. Since K is a Kakeya set, there exists $\boldsymbol{a} \in \mathbb{F}^n$ such that $\boldsymbol{a} + t\boldsymbol{b} \in K$ for every $t \in \mathbb{F}$. Now consider the restriction $g_{\boldsymbol{a},\boldsymbol{b}}$ of g to the line through $\boldsymbol{a}$ in direction $\boldsymbol{b}$; it is a univariate polynomial of degree at most $d < mq$. At every point $t_0 \in \mathbb{F}$ we have that $g_{\boldsymbol{a},\boldsymbol{b}}$ has a zero of multiplicity m (Proposition 4). Thus counting up the zeroes of $g_{\boldsymbol{a},\boldsymbol{b}}$ we find it has mq zeroes (m at every $t_0 \in \mathbb{F}$) which is more than its degree. Thus $g_{\boldsymbol{a},\boldsymbol{b}}$ must be identically zero. In particular its leading coefficient must be zero. By Proposition 5 this leading coefficient is $g_0(\boldsymbol{b})$ and so we conclude $g_0(\boldsymbol{b}) = 0$.

We conclude that g_0 is zero on all of $\mathbb{F}^n$ which contradicts the fact (Fact 2) that it is a nonzero polynomial of degree at most $q-1$ in each of its variables. □

Proof of Theorem 1. The theorem now follows by choosing m appropriately. Using for instance $m = n$, we obtain $|K| \geq \binom{2n-1}{n}^{-1} N_q(n, n)$. It easily follows by the definition of $N_q(n, m)$ that $N_q(n, n) = q^n$, since there are q choices for the individual degree of every variable in an n variate monomial, and this already forces total degree to be at most nq. Hence $|K| \geq \binom{2n-1}{n}^{-1} q^n \geq (q/4)^n$, establishing the theorem for $c_0 = 1$ and $c_1 = \frac{1}{4}$.

A better choice is with $m = \lceil n/2 \rceil \leq (n+1)/2$. In this case $N_q(n, m) \geq \frac{1}{2} q^n$ (since at least half the monomials of individual degree at most $q-1$ have degree at most $nq/2$). This leads to a bound of $|K| \geq \frac{1}{2}\binom{3n/2}{n}^{-1} q^n \geq \frac{1}{2}(q/2.6)^n$, yielding the theorem for $c_0 = 1/2$ and $c_1 = 1/2.6$. □

To improve the constant c_1 further, one could study the asymptotics of $N_q(n, m)$ closer. Let τ_α denote the quantity $\liminf_{n\to\infty}\{\liminf_{q\to\infty}(1/q)N_q(n, \alpha n)^{1/n}\}$. That is, for sufficiently large n and sufficiently larger q, $N_q(n, \alpha n) \to \tau_\alpha^n q^n$. Lemma 6 can be reinterpreted in these terms as saying that for every $\alpha \in [0, 1]$, every Kakeya set has size at least $c_0(c_\alpha q)^n - o(q^n)$ for some $c_0 > 0$, where $c_\alpha \to \tau_\alpha / 2^{(1+\alpha)H(1/(1+\alpha))}$ (where $H(x) = -x \log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function). The best estimate on τ_α we were able to obtain does not have a simple closed form expression. As $q \to \infty$, τ_α^n equals the volume of the following region in $\mathbb{R}^n$: $\{(x_1, x_2, \ldots x_n) \in [0, 1]^n \mid \sum_{i=1}^n x_i \leq \alpha n\}$. This volume can be expressed in terms of Eulerian numbers (See [Marichal and Mossinghoff 2008], §4.3). [Giladi and Keller 1994, §6] gives some asymptotics for Eulerian numbers and using their estimates $\alpha = 0.398$, it seems one can reduce c_α to something like $\frac{1}{2.46}$. This still remains bounded away from the best known upper bound which has $c_1 \to 1/2$.

Remark. While the main theorem only gives the limiting behavior of Kakeya sets for large n and q, Lemma 6 can still be applied to specific choices and get improvements over [Dvir 2008]. For example, for $n = 3$, using $m = 2$ we get a lower bound of $\frac{5}{24} q^3$ as opposed to the bound of $\frac{1}{6} q^3$ obtainable from [Dvir 2008].

3. An upper bound on Kakeya sets

We include here Dvir's proof (personal communication, 2008) giving a nontrivial upper bound on the size of Kakeya sets in fields of odd characteristic. The proof is based on the construction of Mockenhaupt and Tao [2004]. For the case of even characteristic we complement their results by using a variation (obtained with Swastik Kopparty) of their construction.

Theorem 7 (Dvir). *For every $n \geq 2$, and field $\mathbb{F}$, there exists a Kakeya set in $\mathbb{F}^n$ of cardinality at most $2^{-(n-1)}\, q^n + O(q^{n-1})$.*

Proof. We consider two cases depending on whether $\mathbb{F}$ is of odd or even characteristic.
Odd characteristic: Let

$$D_n = \{\langle \alpha_1, \ldots, \alpha_{n-1}, \beta\rangle | \alpha_i, \beta \in \mathbb{F}, \alpha_i + \beta^2 \text{is a square}\}.$$

Now let $K_n = D_n \cup (\mathbb{F}^{n-1} \times \{0\})$ where $\mathbb{F}^{n-1} \times \{0\}$ denotes the set $\{\langle \boldsymbol{a}, 0\rangle | \boldsymbol{a} \in \mathbb{F}^{n-1}\}$. We claim that K_n is a Kakeya set of the appropriate size.

Consider a direction $\boldsymbol{b} = \langle b_1, \ldots, b_n\rangle$. If $b_n = 0$, for $\boldsymbol{a} = \langle 0, \ldots, 0\rangle$ we have that $\boldsymbol{a} + t\boldsymbol{b} \in \mathbb{F}^{n-1} \times \{0\} \subseteq K_n$. The more interesting case is when $b_n \neq 0$. In this case let

$$\boldsymbol{a} = \langle (b_1/(2b_n))^2, \ldots, (b_{n-1}/(2b_n))^2, 0\rangle.$$

The point $\boldsymbol{a} + t\boldsymbol{b}$ has coordinates $\langle \alpha_1, \ldots, \alpha_{n-1}, \beta\rangle$ where $\alpha_i = (b_i/(2b_n))^2 + tb_i$ and $\beta = tb_n$. We have

$$\alpha_i + \beta^2 = (b_i/(2b_n) + tb_n)^2$$

which is a square for every i and so $\boldsymbol{a} + t\boldsymbol{b} \in D_n \subseteq K_n$. This proves that K_n is indeed a Kakeya set.

Finally we verify that the size of K_n is as claimed. First note that the size of D_n is exactly

$$|D_n| = q\,((q+1)/2)^{n-1} = 2^{-(n-1)} q^n + O(q^{n-1})$$

(q choices for β and $(q+1)/2$ choices for each $\alpha_i + \beta^2$).

Hence, as claimed, the size of K_n is at most

$$|K_n| = |D_n| + q^{n-1} = 2^{-(n-1)} q^n + O(q^{n-1}).$$

Even characteristic: This case is handled similarly with minor variations in the definition of K_n. Specifically, we let

$$K_n = E_n = \{\langle \alpha_1, \ldots, \alpha_{n-1}, \beta\rangle | \alpha_i, \beta \in \mathbb{F}, \exists \gamma_i \in \mathbb{F} \text{ such that } \alpha_i = \gamma_i^2 + \gamma_i \beta\}.$$

(As we see below E_n contains $\mathbb{F}^{n-1} \times \{0\}$ and so there is no need to set $K_n = E_n \cup \mathbb{F}^{n-1} \times \{0\}$.)

Now consider direction $\boldsymbol{b} = \langle b_1, \ldots, b_n\rangle$. If $b_n = 0$, then let $\boldsymbol{a} = 0$. We note that

$$\boldsymbol{a} + t\boldsymbol{b} = \langle tb_1, \ldots, tb_{n-1}, 0\rangle = \langle \gamma_1^2 + \beta\gamma_1, \ldots \gamma_{n-1}^2 + \beta\gamma_{n-1}, \beta\rangle$$

for $\beta = 0$ and $\gamma_i = \sqrt{tb_i} = (tb_i)^{q/2}$. We conclude that $\boldsymbol{a} + t\boldsymbol{b} \in E_n$ for every $t \in \mathbb{F}$ in this case.

Now consider the case where $b_n \neq 0$. Let

$$\boldsymbol{a} = \langle (b_1/b_n)^2, \ldots, (b_{n-1}/b_n)^2, 0\rangle.$$

The point $\boldsymbol{a} + t\boldsymbol{b}$ has coordinates $\langle \alpha_1, \ldots, \alpha_{n-1}, \beta \rangle$ where $\alpha_i = (b_i/b_n)^2 + tb_i$ and $\beta = tb_n$.

For $\gamma_i = (b_i/b_n)$,

$$\gamma_i^2 + \gamma_i \beta = (b_1/b_n)^2 + tb_i = \alpha_i.$$

Hence $\boldsymbol{a} + t\boldsymbol{b} \in E_n = K_n$.

It remains to compute the size of E_n. The number of points of the form $\langle \alpha_1, \ldots, \alpha_{n-1}, 0 \} \in E_n$ is exactly q^{n-1}. We now determine the size of $\langle \alpha_1, \ldots, \alpha_{n-1}, \beta \} \in E_n$ for fixed $\beta \neq 0$. We first claim that the set $\{\gamma^2 + \beta\gamma | \gamma \in \mathbb{F}\}$ has size exactly $q/2$. This is so since for every $\gamma \in \mathbb{F}$, we have $\gamma^2 + \beta\gamma = \tau^2 + \beta\tau$ for $\tau = \gamma + \beta \neq \gamma$, and so the map $\gamma \mapsto \gamma^2 + \beta\gamma$ is a 2-to-1 map on its image. Thus, for $\beta \neq 0$, the number of points of the form $\langle \alpha_1, \ldots, \alpha_{n-1}, \beta \}$ in E_n is exactly $(q/2)^{n-1}$. We conclude that E_n has cardinality

$$|E_n| = (q-1)(q/2)^{n-1} + q^{n-1} = 2^{-(n-1)} q^n + O(q^{n-1}). \qquad \square$$

We remark that for the case of odd characteristic, one can also use a recursive construction, replacing the set $\mathbb{F}^{n-1} \times \{0\}$ by $K_{n-1} \times \{0\}$. This would reduce the constant in the $O(q^{n-1})$ term, but not alter the leading term. Also we note that the construction used in the even case essentially also works in the odd characteristic case. Specifically the set $E_n \cup \mathbb{F}^{n-1} \times \{0\}$ is a Kakeya set also for odd characteristic. Its size can also be argued to be $2^{-(n-1)} q^n + O(q^{n-1})$.

Acknowledgments

Thanks to Zeev Dvir for explaining the Kakeya problem and his solution to us, for detailed answers to many queries, and for his permission to include his upper bound on the size of Kakeya sets here (see Section 3). Thanks also to Swastik Kopparty for helping us extend Dvir's proof to even characteristic. Thanks to Chris Umans and Terry Tao for valuable discussions.

References

[Dvir 2008] Z. Dvir, "On the size of Kakeya sets in finite fields", *J. Amer. Math. Soc.* (2008). To appear. arXiv 0803.2336

[Giladi and Keller 1994] E. Giladi and J. B. Keller, "Eulerian number asymptotics", *Proc. Roy. Soc. London Ser. A* **445**:1924 (1994), 291–303. MR 95c:05012 Zbl 0837.05012

[Guruswami and Sudan 1999] V. Guruswami and M. Sudan, "Improved decoding of Reed-Solomon and algebraic-geometry codes", *IEEE Trans. Inform. Theory* **45**:6 (1999), 1757–1767. MR 2000j:94033 Zbl 0958.94036

[Marichal and Mossinghoff 2008] J.-L. Marichal and M. J. Mossinghoff, "Slices, slabs, and sections of the unit hypercube", *Online J. Anal. Comb.* 3 (2008), Art. 1. MR 2008m:52017

[Mockenhaupt and Tao 2004] G. Mockenhaupt and T. Tao, "Restriction and Kakeya phenomena for finite fields", *Duke Math. J.* **121**:1 (2004), 35–74. MR 2004m:11200 Zbl 1072.42007

[Wolff 1999] T. Wolff, "Recent work connected with the Kakeya problem", pp. 129–162 in *Prospects in mathematics* (Princeton, 1996), edited by H. Rossi, Amer. Math. Soc., Providence, RI, 1999. MR 2000d:42010 Zbl 0934.42014

Received 22 Aug 2008. Revised 23 Sep 2008. Accepted 22 Oct 2008.

SHUBHANGI SARAF: shibs@mit.edu
Massachusetts Institute of Technology, Computer Science and Artificial Intelligence Laboratory, 32 Vassar Street, Cambridge, MA 02139, United States

MADHU SUDAN: madhu@mit.edu
Massachusetts Institute of Technology, Computer Science and Artificial Intelligence Laboratory, 32 Vassar Street, Cambridge, MA 02139, United States