Improved lower bound on the size of Kakeya sets over finite fields

Shubhangi Saraf* Madhu Sudan†

August 18, 2008

Abstract

In a recent breakthrough, Dvir showed that every Kakeya set in $\mathbb{F}^n$ must be of 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 growth of the leading constant to the right form as a function of n.

Let $\mathbb{F}$ be a finite field of q elements.

Definition 1 (Kakeya Set) *A set $K \subseteq \mathbb{F}^n$ is said to be a* Kakeya set *in $\mathbb{F}^n$, if for every $\mathbf{b} \in \mathbb{F}^n$, there exists a point $\mathbf{a} \in \mathbb{F}^n$ such that for every $t \in \mathbb{F}$, the point $\mathbf{a} + t \cdot \mathbf{b} \in K$.*

We show:

Theorem 2 *There exist constants $c_0, c_1 > 0$ such that for all n, if K is a Kakeya set in $\mathbb{F}^n$ then $|K| \geq c_0 \cdot (c_1 \cdot q)^n$.*

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.

The question of establishing lower bounds on the size of Kakeya sets was posed in Wolff [7]. 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 [1] showed that every Kakeya set must have cardinality at least $c_n q^n$ for $c_n = (n!)^{-1}$. (Dvir's original bound achieved a weaker lower bound of $c_n \cdot q^{n-1}$, but [1] includes the stronger bound of $c_n \cdot q^n$, with the improvements being attributed to Alon and Tao.) The growth, as a function of q for fixed n is obviously tight since every set in $\mathbb{F}^n$ has cardinality at most q^n. Furthermore, it is known that there exists a constant $\beta < 1$ such that there are Kakeya sets of cardinality at most $\beta^n q^n$ (for odd q). The best known constant has $\beta \to \frac{1}{2}$ due to Dvir [2] (see Appendix A), and the best published bound of $\beta \leq \frac{1}{\sqrt{2}}$ follows from Mockenhaupt and Tao [6] and the fact that products of Kakeya sets are Kakeya sets (in higher dimension). Thus, while our improvement is quite small (say compared to the improvement of Alon and Tao over Dvir's original bound), our bound does determine the form of the leading constant, up to the determination of the right constant β.

Our proof follows that of Dvir [1]. 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 on 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 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 "improved list-decoding of Reed-Solomon codes" by Guruswami and Sudan [4].) We now give a formal proof of Theorem 2.

*MIT CSAIL. shibs@mit.edu.
†MIT CSAIL. madhu@mit.edu.

1 Preliminaries

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

Fact 3 *Let $P \in \mathbb{F}[\mathbf{x}]$ be a polynomial of degree at most $q-1$ in each variable. If $P(\mathbf{a}) = 0$ for all $\mathbf{a} \in \mathbb{F}^n$, then $P \equiv 0$.*

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

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

Proposition 4 *Given a set $S \subseteq \mathbb{F}^n$ satisfying $\binom{m+n-1}{n} \cdot |S| < N_q(n, m)$, there exists a non-zero polynomial $g \in \mathbb{F}[\mathbf{x}]$ 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 $\mathbf{a} \in S$.*

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

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

Proposition 5 *If $g \in \mathbb{F}[\mathbf{x}]$ has a root of multiplicity m at some point $\mathbf{a} + t_0\mathbf{b}$ then $g_{\mathbf{a},\mathbf{b}}$ has a root of multiplicity m at t_0.*

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

Proposition 6 ([1]) *Let $g \in \mathbb{F}[\mathbf{x}]$ be a non-zero polynomial of total degree d and let g_0 be the (unique, non-zero) homogenous polynomial of degree d such that $g = g_0 + g_1$ for some polynomial g_1 of degree strictly less than d. Then $g_{\mathbf{a},\mathbf{b}}(t) = g_0(\mathbf{b})t^d + h(t)$ where h is a polynomial of degree strictly less than d.*

2 Proof of Theorem 2

Lemma 7 *If K is a Kakeya set in $\mathbb{F}^n$, then for every integer $m \geq 0$, $|K| \geq \frac{1}{\binom{m+n-1}{n}} \cdot N_q(n, m)$.*

Proof Assume for contradiction that $|K| < \frac{1}{\binom{m+n-1}{n}} \cdot N_q(n, m)$. Let $g \in \mathbb{F}[\mathbf{x}]$ be a non-zero 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 4.) Let $d < mq$ denote the total degree of g and let $g = g_0 + g_1$ where g_0 is homogenous of degree d and g_1 has degree less than d. Note that g_0 is also non-zero and has degree at most $q-1$ in every variable.

Now fix a "direction" $\mathbf{b} \in \mathbb{F}^n$. Since K is a Kakeya set, there exists $\mathbf{a} \in \mathbb{F}^n$ such that $\mathbf{a} + t\mathbf{b} \in K$ for every $t \in \mathbb{F}$. Now consider the restriction $g_{\mathbf{a},\mathbf{b}}$ of g to the line through $\mathbf{a}$ in direction $\mathbf{b}$. $g_{\mathbf{a},\mathbf{b}}$ is a univariate polynomial of degree at most $d < mq$. At every point $t_0 \in \mathbb{F}$ we have that $g_{\mathbf{a},\mathbf{b}}$ has a zero of multiplicity m (Proposition 5). Thus counting up the zeroes of $g_{\mathbf{a},\mathbf{b}}$ we find it has mq zeroes (m at every $t_0 \in \mathbb{F}$) which is

more than its degree. Thus $g_{\mathbf{a},\mathbf{b}}$ must be identically zero. In particular its leading coefficient must be zero. By Proposition 6 this leading coefficient is $g_0(\mathbf{b})$ and so we conclude $g_0(\mathbf{b}) = 0$.

We conclude that g_0 is zero on all of $\mathbb{F}^n$ which contradicts the fact (Fact 3) that it is a non-zero polynomial of degree at most $q-1$ in each of its variables. ■

Proof of Theorem 2: Theorem 2 now follows by choosing m appropriately. Using for instance $m = n$, we obtain that $|K| \geq \frac{1}{\binom{2n-1}{n}} \cdot q^n \geq (q/4)^n$, establishing the theorem for $c_0 = 1$ and $c_1 = 1/4$.

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 $|K| \geq \frac{1}{2\binom{(3/2)n}{n}} q^n \geq \frac{1}{2}(q/2.6)^n$, 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 $\liminf_{n\to\infty}\{\liminf_{q\to\infty} \frac{1}{q} \cdot N_q(n, \alpha \cdot n)^{1/n}\}$. I.e., for sufficiently large n and sufficiently larger q, $N_q(n,\alpha n) \to \tau_\alpha^n \cdot q^n$. Lemma 7 can be reinterpreted in these terms as saying that for every $\alpha \in [0,1]$, every Kakeya set has size at least $c_0(c_\alpha \cdot q)^n - o(q^n)$ 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 $\mathbb{R}^n$: $\{(x_1, x_2, \ldots x_n) \in [0,1]^n | \sum_{i=1}^n x_i \leq \alpha \cdot n\}$. This volume can be expressed in terms of Eulerian numbers (See [5], §4.3). [3, §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, q, Lemma 7 can still be applied to specific choices and get improvements over [1]. 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 [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 Appendix A). Thanks also to Chris Umans for valuable discussions.

References

[1] Zeev Dvir. On the size of Kakeya sets in finite fields. *Journal of the American Mathematical Society*, (to appear), 2008. Article electronically published on June 23, 2008.

[2] Zeev Dvir. Personal communication, August 2008.

[3] Eldar Giladi and Joseph B. Keller. Eulerian number asymptotics. *Proceedings of the Royal Society of London, Series A*, 445(1924):291–303, 1994.

[4] Venkatesan Guruswami and Madhu Sudan. Improved decoding of Reed-Solomon and algebraic-geometric codes. *IEEE Transactions on Information Theory*, 45:1757–1767, 1999.

[5] Jean-Luc Marichal and Michael J. Mossinghoff. Slices, slabs, and sections of the unit hypercube. *Online Journal of Analytic Combinatorics*, 3, 2008. 11 pages. Earlier version appears as eprint math/0607715 (2006).

[6] Gerd Mockenhaupt and Terence Tao. Restriction and Kakeya phenomena for finite fields. *Duke Mathematics Journal*, 121(1):35–74, 2004.

[7] T. Wolff. Recent work connected with the Kakeya problem. In *Prospects in Mathematics*, pages 129–162. Princeton, NJ, 1999.

A An upper bound on Kakeya sets

We include here Dvir's proof [2] giving a non-trivial upper bound on the size of Kakeya sets in fields of odd characteristic. The proof is based on the construction of Mockenhaupt and Tao [6].

Theorem 8 ([2]) *For every n, and field $\mathbb{F}$ of odd cardinality q, there exists a Kakeya set in $\mathbb{F}^n$ of cardinality at most $2^{-(n-1)} \cdot q^n + O(q^{n-1})$.*

Proof We construct a set K_n for every n by induction. We set $K_1 = \mathbb{F}$. For $n \geq 2$, 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 $K_n = D_n \cup (K_{n-1} \times \{0\})$ where $K_{n-1} \times \{0\}$ denotes the set $\{\langle \mathbf{a}, 0 \rangle | \mathbf{a} \in K_{n-1}\}$. We claim that K_n is a Kakeya set of the appropriate size.

Consider a direction $\mathbf{b} = \langle b_1, \ldots, b_n \rangle$. If $b_n = 0$, then let $\mathbf{b}' = \langle b_1, \ldots, b_{n-1} \rangle$. Let $\mathbf{a}' = \langle a_1, \ldots, a_{n-1} \rangle \in K_{n-1}$ be such that the line $\mathbf{a}' + t \cdot \mathbf{b}'$ is contained in K_{n-1}. Let $\mathbf{a} = \langle \mathbf{a}, 0 \rangle$. It follows that $\mathbf{a} + t\mathbf{b} \in K_{n-1} \times \{0\} \subseteq K_n$. The more interesting case is when $b_n \neq 0$. In this case let $\mathbf{a} = \langle (b_1/(2b_n))^2, \ldots, (b_{n-1}/(2b_n))^2, 0 \rangle$. The point $\mathbf{a} + t\mathbf{b}$ has coodinates $\langle \alpha_1, \ldots, \alpha_{n-1}, \beta \rangle$ 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 $\mathbf{a} + t\mathbf{b} \in D_n \subseteq K_n$.

For $n \geq 2$, the size of D_n is exactly $q \cdot ((q+1)/2)^{n-1}$ (q choices for β and $(q+1)/2$ choices for each $\alpha_i + \beta^2$). Thus for $n \geq 2$, the cardinalilty of K_n is upper bounded by $q + \left(q \cdot \sum_{i=1}^{n-1} ((q+1)/2)^i \right) = 2^{-(n-1)} q^n + O(q^{n-1})$. ■