DVIR'S WORK ON THE FINITE FIELD KAKEYA PROBLEM

PETE L. CLARK

1. The Dvir-Alon-Tao Theorem

Let $\mathbb{F}$ be a field and $n \in \mathbb{Z}^+$. A subset $S \subset \mathbb{F}^n$ is a **Kakeya set** if for every line $\mathbb{F}v$ in V, S contains some translate $\ell_{a,v} := a + \mathbb{F}v$. The general Kakeya problem is to show that Kakeya sets are in some sense(s) "large." Here we shall be concerned only with the case of $F = \mathbb{F}_q$ a finite field of cardinality q. We can then interpret large simply in terms of the cardinality $|S|$.[1] Perhaps because of the analogy to $F = \mathbb{R}$ as a "limit as $q \to \infty$", all known work has focused on bounds for fixed n and large q.

Let $K(n,q)$ denote the minimum cardinality of a Kakeya set in $\mathbb{F}_q^n$. Clearly $K(n,q) \leq |\mathbb{F}_q^n| = q^n$; but what about lower bounds? In 1999 T. Wolff showed [Wol99]

$$K(2,q) \geq \frac{(q+1)q}{2}$$

and for all $n \in \mathbb{Z}^+$,

$$K(n,q) \gg_n q^{n/2+1}.$$

Recently Z. Dvir showed [Dvi08] that for all $\epsilon > 0$, $|S| \gg_{n,\epsilon} q^{n-\epsilon}$. Remarkably, N. Alon and T. Tao were able to refine his argument to arrive at the following:

Theorem 1.1. *(Dvir-Alon-Tao, 2008) For all n and q we have*

$$K(n,q) \geq \binom{q+n-1}{n}.$$

Proof. Suppose there is a Kakeya set $S \subset \mathbb{F}_q^n$ with $|S| < \binom{q+n-1}{n}$.

Recall that the dimension of the $\mathbb{F}_q$-vector space of polynmials of degree at most d in n variables is $\binom{d+n}{n}$. On the other hand, the dimension of the space of all functions $f : S \to \mathbb{F}_q$ is $|S|$, so under our hypothesis on $\#S$, there is a a (not necessarily homogeneous) nonzero polynomial $g(\mathbf{t})$ of degree at most $q-1$ vanishing on S. Write $g(\mathbf{t}) = \sum_{i=0}^{q-1} g_i(\mathbf{t})$, where each g_i is homogenous of degree i. By the Kakeya property, for any $y \in \mathbb{F}_q^n$ there exists $a \in \mathbb{F}_q^n$ such that $P(a+ty)$ is a univariate polynomial of degree at most $q-1$ with at least q zeros, thus $P(a+ty) = 0 \in \mathbb{F}_q[t]$. In particular the coefficient of t^{q-1} (i.e., the leading coefficient) in

$$P(a+ty) = P_0(a+ty) + \ldots + P_{q-1}(a+ty)$$

must be zero, but the coefficient of t^{q-1} is precisely $P_{q-1}(y)$. Thus P_{q-1} vanishes on all of $\mathbb{F}_q^n$. Since its total degree $q-1$, it is a **reduced** polynomial in the sense of [ChWar] and therefore it must be the zero polynomial. Similarly we find that

[1] A Kakeya set over an infinite field must be infinite, so the problem is fundamentally more sophisticated. The most studied case is $F = \mathbb{R}$, where "large" refers to any of several different kinds of fractal dimension.

$P_{q-1}, \ldots, P_1$ are all identically zero, so P is constant. Since P vanishes at all points of the Kakeya set S, we conclude $P(\mathbf{t})$ is the zero polynomial, a contradiction! $\square$

Note that this precisely recovers Wolff's bound when $n = 2$. In general it gives $K(n,q) \asymp_n q^n$, which is remarkably tight. Still, one can always ask for more: for $n = 2$ and odd q, work of X. Faber [Fab07] and J. Cooper [Coo06] gives

$$\frac{(q+1)q}{2} + \frac{5q}{14} - \frac{1}{14} \leq K(2,q) \leq \frac{(q+1)q}{2} + \frac{q-1}{2}.$$

Apparently the upper bound is believed to be sharp.[2]

2. Travaux de Dvir

Zeev Dvir's original proof, while still very simple and elegant, is (obviously!) more complicated than the proof of Theorem 1.1 above. On the other hand, I find the original proof to be more interesting, especially because it is "more geometric." In this section we describe Dvir's proof.

2.1. **Preliminaries.**

First, Dvir considers a slightly more general problem: roughly he considers subsets of $\mathbb{F}_q^n$ which contain sufficiently many points on some translate of sufficiently many lines. More precisely: for $\delta, \gamma \in \mathbb{R}^+$, a subset $S \subset \mathbb{F}_q^n$ is a (δ,γ)-**Kakeya set** if there exists a subset $\mathcal{L} \subset V$ of size at least δq^n such that for $v \in \mathcal{L}$, there is a line ℓ in V in direction v such that $|\ell \cap S| \geq \gamma q$. Thus a Kakeya set is a $(1,1)$-Kakeya set.

Theorem 2.1. *(Dvir, 2008) Let $S \subset \mathbb{F}_q^n$ be a (δ,γ)-Kakeya set. Then*

$$|K| \geq \binom{d+n-1}{n-1},$$

where

$$d = \lfloor q \min\{\delta, \gamma\} \rfloor - 2.$$

From this he deduces

Corollary 2.2. *(Dvir) For $n \in \mathbb{Z}^+$ and $\epsilon > 0$, there exists $C_{n,\epsilon} \in \mathbb{R}^+$ such that*

$$K(n,q) \geq C_{n,\epsilon} q^{n-\epsilon}.$$

At first glance, the deduction of Corollary 2.2 from Theorem 2.1 is surprising, since the most obvious application of Theorem 2.1 – i.e., taking $(\delta,\gamma) = (1,1)$ – gives (only) $K(n,q) \gg_n q^{n-1}$. But Dvir cleverly takes advantage of the following "multiplicative" property of Kakeya sets over any field:

Lemma 2.3. *Let V be a finite dimensional vector space over any field $\mathbb{F}$ and let $S \subset V$ be a Kakeya set. For any $r \in \mathbb{Z}^+$, the Cartesian product $S^r = \{(s_1, \ldots, s_r) \mid s_i \in S\}$ is a Kakeya set in V^r.*

Proof. Any line in V^r is of the form $\mathbb{F}(v_1, \ldots, v_r)$. By assumption, there exist $a_1, \ldots, a_r \in V$ such that $a_i + \mathbb{F}v_i \in S$. Then $(a_1, \ldots, a_r) + \mathbb{F}(v_1, \ldots, v_r) \in K^r$. $\square$

Thus, knowing only $K(n,q) \geq C_n q^{n-1}$, we may deduce Corollary 2.2: by Lemma 2.3, $K^r \subset V^r$ is a Kakeya set and thus $|K^r| \geq C_{rn} q^{rn-1}$, so $|K| \geq C_{rn}^{\frac{1}{r}} q^{n-\frac{1}{r}}$.

---

[2] I am not aware of any more precise information, established or conjectural, on $K(n,q)$ for $n > 2$ (but what do I know?).

2.2. **The Schwartz-Zippel Theorem.**

The following treatment is taken from `http://en.wikipedia.org/wiki/Schwartz-Zippel_Lemma`.

Theorem 2.4. *Let F be any field, and let $0 \neq f \in F[t_1, \dots, t_n]$ be a nonzero polynomial of degree d. Let S be a finite subset of F. Then the probability that for randomly chosen elements $x_1, \dots, x_n \in S$ we have $f(x_1, \dots, x_n) = 0$ is at most $\frac{d}{|S|}$. More precisely, put $Z_S(f) := \{(x_1, \dots, x_n) \in S^n \mid f(x_1, \dots, x_n) = 0\}$. Then*

$$|Z_S(f)| \leq d|S|^{n-1}.$$

Proof. By induction on n. For $n = 1$, it simply says that a nonzero degree d univariate polynomial over a field cannot have more than d roots. Assume true for $n - 1$ variables and write

$$f(t_1, \dots, t_n) = \sum_{i=0}^{d} f_i(t_2, \dots, t_n) t_1^i.$$

Since f is nonzero, so is some f_i; choose the largest such index i. We have $\deg(f_i) \leq d-i$. By our induction hypothesis, the probability that $P_i(x_1, \dots, x_n) = 0$ is at most $\frac{d-i}{|S|}$. Now, if $P_i(x_2, \dots, x_n) \neq 0$, then $P(t_1, x_2, \dots, x_n)$ is univariate of degree i. The conditional probability that $P(x_1, \dots, x_n) = 0$ given that $P_i(x_2, \dots, x_n)$ is not zero is therefore at most $\frac{i}{|S|}$. Let us denote by A the event that $P(x_1, \dots, x_n) = 0$ and by B the event that $P_i(x_2, \dots, x_n) = 0$. We therefore have

$$\Pr A = \Pr(A \cap B) + \Pr(A \cap B^c)$$
$$= \Pr(A)\Pr(B|A) + \Pr(B^c)\Pr(A|B^c)$$
$$\leq \Pr(B) + \Pr(A|B^c) \leq \frac{d-i}{|S|} + \frac{i}{|S|} = \frac{d}{|S|}.$$

□

Theorem 2.5. *(J.T. Schwartz* [Sch90], *R. Zippel* [Zip89]*) Let $0 \neq f \in \mathbb{F}_q[t_1, \dots, t_n]$ be a polynomial of degree at most d. Then the number of zeros of f is at most dq^{n-1}.*

Proof. In Theorem 2.4 take $F = \mathbb{F}_q$, $S = F$. □

2.3. **Proof of Theorem 2.1.**

We suppose for a contradiction that $S \subset \mathbb{F}_q^n =: V$ is a (δ, γ)-Kakeya set with

$$|S| < \binom{d+n-1}{n-1}.$$

Then the number of monomials in $\mathbb{F}_q[x_1, \dots, x_n]$ of degree d is larger than $|S|$, so the total number of homogeneous polynomials of degree d is larger than the total number of functions from $S^n \to \mathbb{F}_q$. Therefore there exist distinct polynomials inducing the same function, and, taking their difference, a nonzero degree d homogeneous polynomial $g \in \mathbb{F}_q[t_1, \dots, t_n]$ vanishing identically on S. We wish to show that such a g must have too many zeros to satisfy the Schwartz-Zippel theorem.

Let $\tilde{S} \subset C$ be the union of all lines passing through the origin which meet S

in at least one point. In more geometric terms, if $c : V \setminus 0 \to \mathbb{P}V$ is the usual projectivization map, then

$$\tilde{S} = c^{-1}(c(S)).$$

Since g is homogeneous, we must also have that g vanishes at every point of $\tilde{S}$.

Let $\mathcal{L} \subset V$ be as in the definition of (δ, γ)-Kakeya set. Here is the key:

CLAIM g vanishes identically on $\mathcal{L}$.

SUFFICIENCY OF CLAIM Assuming the claim, g vanishes on at least δq^n points. This violates the Schwartz-Zippel bound if $\delta q^n > dq^{n-1}$, hence if $d < \delta q$, which is indeed the case for the value $d := \lfloor q \min\{\delta, \gamma\} \rfloor = 2$ appearing in the statement of the theorem. So it suffices to prove the claim.

PROOF OF CLAIM Let $0 \neq v \in \mathcal{L}$, so there exists $a \in V$ such that $\ell_{a,v} = a + \mathbb{F}v$ meets S in at least γq points. Thus, since $d + 2 \leq \gamma \cdot q$, there exist $d + 2$ elements of x of $\mathbb{F}$ such that $a + xv \in S$. Obviously at most one of these is zero, so there exist $x_1, \ldots, x_{d+1} \in \mathbb{F}^\times$ such that for all i, $a + x_i v \in S$. Therefore

$$w_i := v + \frac{1}{a_i} a \in \tilde{S},$$

so $g(w_i) = 0$ for all $1 \leq i \leq d+1$. Thus the degree d polynomial g has more than d zeros on the line $\ell_{v,a}$ and therefore is identically 0. In particular it vanishes on the point $v + 0a = v$, establishing the claim and completing the proof of Theorem 2.1.

Comments: The most clever feature of this argument is the use of projectivization to switch from the line $\ell_{a,v}$ to the "dual" line $\ell_{v,a}$. Comparing with the proof of Theorem 1.1 one sees this elegant use of homogeneous polynomials is exactly where the estimates become worse: that some nonzero homogeneous polynomial of degree at most d vanishes on S is a more stringent condition than without homogeneity. But the latter argument seems to give information about a **projective Nullstellensatz** for low degree hypersurfaces over finite fields.

References

[ChWar] P.L. Clark, *The Chevalley-Warning theorem*, available at `http://math.uga.edu/~pete/4400ChevalleyWarning.pdf`

[Coo06] J. Cooper, *Collinear triple graphs and the Finite Plane Kakeya Problem*, `http://arxiv.org/abs/math/0607734`

[Dvi08] Z. Dvir, *On the size of Kakeya sets in finite fields*, J. of the Amer. Math. Soc., to appear.

[Fab07] X.W.C. Faber, *On the finite field Kakeya problem in two dimensions*, J. Number Theory 124 (2007), no. 1, 248–257

[Sch90] J.T. Schwartz, *Fast probabilistic algorithms for verification of polynomial identities.* J. Assoc. Comput. Mach. 27 (1980), no. 4, 701–717.

[Wol99] T. Wolff, *Recent work connected with the Kakeya problem.* Prospects in mathematics (Princeton, NJ, 1996). pages 129162, 1999.

[Zip89] R. Zippel, *An explicit separation of relativised random polynomial time and relativised deterministic polynomial time.* Inform. Process. Lett. 33 (1989), no. 4, 207–212. *Probabilistic algorithms for sparse polynomials.* Symbolic and algebraic computation (EUROSAM '79, Internat. Sympos., Marseille, 1979), pp. 216–226, Lecture Notes in Comput. Sci., 72, Springer, Berlin-New York, 1979.