DVIR, KOPPARTY, SARAF, AND SUDAN ON THE SIZE OF KAKEYA SETS IN FINITE FIELDS

AN EXPOSITION BY VSEVOLOD F. LEV

A Kakeya, or Besicovitch, set in a vector space is a set which contains a line in every direction. The finite field Kakeya problem is to estimate, for integer $r > 0$ and prime power q, the smallest possible size of a Kakeya set in $\mathbb{F}_q^r$. A conjecture, which was open for almost a decade and considered quite tough, says that this size is $\Omega_r(q^r)$; that is, for r fixed and q growing, every Kakeya set in $\mathbb{F}_q^r$ has positive density. This conjecture was recently solved by Dvir [D], who gave a strikingly simple proof, using the polynomial method, of the lower bound $\binom{q+r-1}{r} \geq q^r/r!$.

A significant further progress was made in a subsequent paper by Dvir, Kopparty, Saraf, and Sudan [DKSS], who use what they call *the method of multiplicities* to improve Dvir's bound to $\left(\frac{q}{2-1/q}\right)^r$.

Below we first present Dvir's original argument and then sketch the proof of the DKSS' estimate.

1. Dvir's Bound.

Theorem 1 (Dvir, 2008)**.** *If r is a positive integer, q is a prime power, and $K \subseteq \mathbb{F}_q^r$ is a Kakeya set, then $|K| \geq \binom{q+r-1}{r} \geq q^r/r!$.*

The proof is based on the following well-known lemma which shows that for every small set in a finite vector space there is low-degree polynomial, vanishing on this set.

Lemma 1. *Let $r \geq 1$ and $d \geq 0$ be integers and q a prime power. If $S \subseteq \mathbb{F}_q^r$ satisfies $|S| < \binom{r+d}{r}$, then there is a non-zero polynomial over $\mathbb{F}_q$ in r variables of degree at most d, vanishing on S.*

Proof. Consider the linear space $\mathcal{L}$ of all polynomials over $\mathbb{F}_q$ in r variables of degree at most d. The dimension of $\mathcal{L}$ does not exceed (in fact, is equal to) the number of monomials in $\mathcal{L}$, which is $\binom{r+d}{d}$. Consequently, the evaluation mapping $\mathcal{L} \to \mathbb{F}_q^{|S|}$, sending every polynomial to the $|S|$-tuple of its values on the elements of S, is degenerate. Every polynomial in the kernel of this mapping vanishes on S. $\square$

Proof of Theorem 1. Let $K \subseteq \mathbb{F}_q^r$ be a Kakeya set. We show that no polynomial of degree, smaller than q, vanishes on K; by Lemma 1, this implies that $|K| \geq \binom{r+q-1}{r}$, as claimed.

Suppose, for a contradiction, that there do exist non-zero polynomials of degree, smaller than q, vanishing on K. Let P be such a polynomial. Write $d := \deg P$ and $P = P_H + P_N$, where P_H is a homogeneous polynomial of degree d, and $\deg P_N < d$.

By the definition of a Kakeya set, for every $u \in \mathbb{F}_q^r \setminus \{0\}$ (the direction) there exists $v \in \mathbb{F}_q^r$ such that $P(v + \lambda u) = 0$ for each $\lambda \in \mathbb{F}_q$. We notice that $P(v + \lambda u) = P_H(v+\lambda u)+P_N(v+\lambda u)$ is a polynomial in λ of degree $d < q$, with leading coefficient $P_H(u)$. Since this polynomial vanishes for each $\lambda \in \mathbb{F}_q$, all its coefficients are equal to 0; in particular, $P_H(u) = 0$ for every $u \in \mathbb{F}_q^r \setminus \{0\}$. Since P_H is homogeneous, we also have $P_H(0) = 0$. Thus, P_H vanishes identically, whence $P = P_N$ and P_N is not identically zero (for P is not).

Thus, starting from the polynomial P we have found a non-zero polynomial of lower degree, which also vanishes on K. Continuing in this way we will eventually reach a zero-degree polynomial, vanishing on K, which is an absurdum. □

In contrast with [D], we have not used the *Schwartz-Zippel lemma* in the proof of Theorem 1. However, the multiplicity version of this lemma is an important ingredient of the argument of [DKSS] (presented in the next section). For this reason we believe that the classical version of the lemma, showing that a polynomial of low degree cannot have "too many" roots on a cartesian product, is also worth including here.

Lemma 2 (Schwartz-Zippel)**.** *If P is a non-zero polynomial of degree at most d in r variables over the finite field $\mathbb{F}$, and $S \subseteq \mathbb{F}$, then P has at most $|S|^{r-1}d$ roots on the cartesian product $S^r := S \times \cdots \times S$.*

Proof. Induction by r. Write

$$P(x_1, \dots, x_r) = P_k(x_1, \dots, x_{r-1})x_r^k + \cdots + P_0(x_1, \dots, x_{r-1}),$$

where $\deg P_k \leq d - k$ and P_k is a non-zero polynomial. By the induction hypothesis, the number of $(r-1)$-tuples $(x_1, \dots, x_{r-1}) \in S^{r-1}$, on which P_k vanishes, is at most $|S|^{r-2}(d-k)$, and to every such $(r-1)$-tuple there correspond at most $|S|$ roots of P on S^r. On the other hand, to every $(r-1)$-tuple $(x_1, \dots, x_{r-1}) \in S^{r-1}$ on which P_k does *not* vanish there correspond at most k roots of P on S^r. Consequently, the total number of roots of P on S^r does not exceed

$$|S|^{r-1}(d-k) + |S|^{r-1}k = |S|^{r-1}d.$$

□

2. The DKSS Bound.

The major innovation introduced in [DKSS] is that instead of a polynomial, vanishing on a Kakeya set "with multiplicity 1", a polynomial vanishing with higher multiplicity is considered. We refer the reader to [DKSS] for the historical account and the systematic development of the background notions, confining here to a very brief overview of Hasse derivatives and multiplicities.

Let $\mathbb{N}_0$ denote the semigroup of non-negative integers, and let $r \geq 1$ be an integer. For a vector $i = (i_1, \dots, i_r) \in \mathbb{N}_0^r$ write $w(i) := i_1 + \dots + i_r$. Given yet another vector $X = (X_1, \dots, X_r)$ with the entries X_i in an arbitrary ring, let $X^i := X_1^{i_1} \cdots X_r^{i_r}$.

For a polynomial P in r variables and a vector $i \in \mathbb{N}_0^r$, the *Hasse derivative* of P of order i is the polynomial $P^{(i)}$, defined by

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

Notice that, letting $X = 0$, we get $P^{(0)}(Y) = P(Y)$. 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 $(P^{(i)})_H$ denotes the homogeneous part of $P^{(i)}$, then $(P^{(i)})_H = (P_H)^{(i)}$.

A polynomial P in r variables over a field $\mathbb{F}$ is said to vanish at a point $a \in \mathbb{F}^r$ with multiplicity $m \geq 0$ if $P^{(i)}(a) = 0$ for each $i \in \mathbb{N}_0^r$ with $w(i) < m$, whereas there exists $i \in \mathbb{N}_0^r$ with $w(i) = m$ 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 P at a by $\mu(P, a)$; thus, $\mu(P, a)$ is the largest integer m with the property that

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

It is not difficult to see that for any $i \in \mathbb{N}_0^r$ and any $a \in \mathbb{F}^r$ we have

$$\mu(P^{(i)}, a) \geq \mu(P, a) - w(i);$$

this is [DKSS, Lemma 5].

We need the following multiplicity version of Lemma 1.

Lemma 3 ([DKSS, Proposition 10])**.** *Let $r, m \geq 1$ and $d \geq 0$ be integers, and q a prime power. If $S \subseteq \mathbb{F}_q^r$ satisfies $\binom{m+r-1}{r} |S| < \binom{r+d}{r}$, then there is a non-zero polynomial over $\mathbb{F}_q$ in r variables of degree at most d, vanishing at every point of S with multiplicity at least m.*

Proof. The proof is a rather straightforward modification of that of Lemma 1. Let $\mathcal{L}$ be the linear space of all polynomials over $\mathbb{F}_q$ in r variables of degree at most d; thus, the dimension of $\mathcal{L}$ is $\binom{r+d}{d}$. Consider the evaluation mapping on $\mathcal{L}$, sending every polynomial to the vector of all its $\binom{m+r-1}{r}|S|$ Hasse derivatives of order at most $m-1$ on the elements of S. (Notice that the number of Hasse derivatives of order at most $m-1$ of a given polynomial is the number of r-tuples $i=(i_1,\dots,i_r)$ with non-negative integer $i_1,\dots,i_r$, satisfying $i_1+\dots+i_r\le m-1$, which is $\binom{m+r-1}{r}$.) Under the assumptions of the lemma, this mapping is degenerate. Every polynomial in its kernel has all its Hasse derivatives of order at most $m-1$ vanishing on each element of S; that is, each element of S is a zero of this polynomial of multiplicity at least m. □

Another ingredient is the following multiplicity version of the Schwartz-Zippel lemma.

Lemma 4 ([DKSS, Lemma 8]). *If P is a non-zero polynomial of degree at most d in r variables over the finite field $\mathbb{F}$, and $S\subseteq\mathbb{F}$, then*

$$\sum_{z\in S^r}\mu(P,z)\le d|S|^{r-1}.$$

We omit the proof.

In fact, we need only the following corollary.

Corollary 1. *Let P be a non-zero polynomial of degree at most d in r variables over a finite field $\mathbb{F}$, and let m be a positive integer. If P vanishes at every point of $\mathbb{F}^r$ with multiplicity at least m, then $d\ge m|\mathbb{F}|$.*

Eventually, we are ready to prove the theorem of Dvir, Kopparty, Saraf, and Sudan on the size of a Kakeya set.

Theorem 2 ([DKSS, Theorem 11]). *If r is a positive integer, q is a prime power, and $K\subseteq\mathbb{F}_q^r$ is a Kakeya set, then $|K|\ge\left(\frac{q}{2-1/q}\right)^r$.*

Proof. Assuming that m and d are positive integers with

$$d<q\left\lceil\frac{qm-d}{q-1}\right\rceil, \tag{1}$$

(no typo: d enters both sides!) we show that

$$\binom{m+r-1}{r}|K|\ge\binom{r+d}{r}; \tag{2}$$

the rest follows by optimization which we suppress here.

Suppose for a contradiction that (2) fails whence, by Lemma 3, there exists a non-zero polynomial P over $\mathbb{F}_q$ of degree at most d in r variables, vanishing at every point of K with multiplicity at least m.

Write $l := \left\lceil \frac{qm-d}{q-1} \right\rceil$ and fix $i = (i_1, \dots, i_r)$ with integer $i_1, \dots, i_r \geq 0$ of weight $w := i_1 + \dots + i_r < l$. Let $Q := P^{(i)}$, the ith Hasse derivative of P.

Since K is a Kakeya set, for every $v \in \mathbb{F}_q^r$ there exists $u \in \mathbb{F}_q^r$ with

$$\mu(P, u + tv) \geq m \quad (t \in \mathbb{F}_q);$$

hence, with

$$\mu(Q, u + tv) \geq m - w \quad (t \in \mathbb{F}_q).$$

It is easily seen, however, that $\mu(Q, u + tv) \leq \mu(Q(u + Tv), t)$, where $Q(u + Tv)$ is considered as a polynomial in the variable T. Thus, for every $v \in \mathbb{F}_q^r$ there exists $u \in \mathbb{F}_q^r$ such that

$$\mu(Q(u + Tv), t) \geq m - w \quad (t \in \mathbb{F}_q).$$

Compared with

$$\deg Q(u + Tv) \leq \deg Q \leq d - w < q(m - w)$$

(as it follows from $w < l$), in view of Corollary 1 this shows that $Q(u + Tv)$ is the zero polynomial.

Let P_H and Q_H denote the homogeneous parts of the polynomials P and Q, respectively. As the leading coefficient of $Q(u + Tv)$ is $Q_H(v)$, we conclude that $P_H^{(i)} = Q_H$ vanishes identically on $\mathbb{F}_q^r$. This shows that all Hasse derivatives of P_H of order, smaller than l, vanish on $\mathbb{F}_q^r$; in other words, P_H vanishes with multiplicity at least l at every point of $\mathbb{F}_q^r$. Since, on the other hand, by (1) we have

$$\deg P_H = \deg P \leq d < ql,$$

from Corollary 1 we conclude that P_H is the zero polynomial, which is wrong as the homogeneous part of a non-zero polynomial is non-zero. This contradiction concludes the proof. □

References

[D] Z. Dvir, On the size of Kakeya sets in finite fields, *J. of the AMS*, to appear.

[DKSS] Z.Dvir, S. Kopparty, S. Saraf, and M. Sudan, Extensions to the method of multiplicities, with applications to Kakeya sets and mergers, *Submitted*.