On the Size of Kakeya sets in finite fields

Zeev Dvir

Presented by Martin Tancer

Let $\mathbb{F}$ be a finite field (with q elements). A *Kakeya* set in $\mathbb{F}^n$ is a set $K \subseteq F^n$ containing line in every direction.

Theorem 1. *Let $K \subseteq \mathbb{F}^n$ be a Kakeya set. Then*

$$|K| \geq C_n \cdot q^{n-1}$$

where C_n depends only on n.

A set $K \subseteq \mathbb{F}^n$ is a (δ, γ)-Kakeya set if there exists a set $L \subseteq \mathbb{F}^n$ of size at least δq^n such that for every $x \in L$ there is a line in direction x that intersects K in at least γq points.

Remark. A Kakeya set is (1,1)-Kakeya set.

Theorem 2. *Let $K \subseteq \mathbb{F}^n$ be a (δ, γ)-Kakeya set. Then*

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

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

Theorem 3. *Let $K \subseteq \mathbb{F}^n$ be a Kakeya set. Then*

$$|K| \geq C_n q^n$$

where C_n depends only on n.

Lemma 4 (Schwartz-Zippel)**.** *Let $f \in \mathbb{F}[x_1, \ldots, x_n]$ be a nonzero polynomial with* $\deg(f) \leq d$. *Then*

$$|\{x \in \mathbb{F}^n | f(x) = 0\}| \leq dq^{n-1}.$$

Let $\mathbf{i} = (i_1, \ldots, i_n)$ be a vector of nonnegative integers. The *weight* of $\mathbf{i}$ is defined as $\mathrm{wt}(\mathbf{i}) := \sum_{k=1}^{n} i_k$. For an abstract variable $\mathbf{X} = (X_1, \ldots, X_n)$ we denote

$$\mathbf{X}^{\mathbf{i}} := \prod_{k=1}^{n} X_k^{i_k}.$$

For a polynomial $P(\mathbf{X})$, $H_P(\mathbf{X})$ denotes the homogeneous part of $P(\mathbf{X})$ of the highest total degree. We also denote

$$\binom{\mathbf{i}}{\mathbf{j}} := \prod_{k=1}^{n} \binom{i_k}{j_k}.$$

Remark (Binomial theorem). $(\mathbf{Z}+\mathbf{W})^{\mathbf{r}} = \sum_{\mathbf{i}\leq\mathbf{r}} \binom{\mathbf{r}}{\mathbf{i}} \mathbf{Z}^{\mathbf{i}}\mathbf{W}^{\mathbf{r}-\mathbf{i}}$.

Definition ((Hasse) Derivative)**.** For $P(\mathbf{X}) \in \mathbb{F}[\mathbf{X}]$ and non-negative vector $\mathbf{i}$, the ith (Hasse) derivative of P, denoted $P^{(\mathbf{i})}$, is the coefficient of $Z^{(i)}$ in the polynomial $\tilde{P}(\mathbf{X},\mathbf{Z}) = P(\mathbf{X}+\mathbf{Z}) \in \mathbb{F}[\mathbf{X},\mathbf{Z}]$. Thus,

$$P(\mathbf{X}+\mathbf{Z}) = \sum_{\mathbf{i}} P^{(\mathbf{i})}(\mathbf{X})\mathbf{Z}^{\mathbf{i}}.$$

Example. Let $P(\mathbf{X}) = P(X_1, X_2) = X_1^3 + X_1X_2 + 7 \in \mathbb{F}_{11}[X_1, X_2]$. Then

$$P(\mathbf{X}+\mathbf{Z}) = X_1^3 + X_1X_2 + 7 + (3X_1^2 + X_2)Z_1 + 3X_1Z_1^2 + Z_1^3 + X_1Z_2 + Z_1Z_2.$$

Thus, for example,

$$\begin{aligned} P^{((0,0))}(\mathbf{X}) &= X_1^3 + X_1X_2 + 7, \\ P^{((1,0))}(\mathbf{X}) &= 3X_1^2 + X_2, \\ P^{((3,0))}(\mathbf{X}) &= P^{((1,1))} = 1, \\ P^{((4,0))}\mathbf{X} &= P^{((1,2))} = 0. \end{aligned}$$

Definition (Multiplicity)**.** For $P(\mathbf{X}) \in \mathbb{F}[\mathbf{X}]$ and $\mathbf{a} \in \mathbb{F}^n$, the *multiplicity* of P at $\mathbf{a}$, denoted $\mathrm{mult}(P,\mathbf{a})$, is the largest integer M such that for every non-negative vector $\mathbf{i}$ with $\mathrm{wt}(\mathbf{i}) < M$ we have $P^{(\mathbf{i})}(\mathbf{a}) = 0$ (we set $\mathrm{mult}(P,\mathbf{a}) = \infty$ if there is no such largest M).

Lemma 5 (Basic properties of multiplicities)**.** *If $P(\mathbf{X}) \in F[\mathbf{X}]$ and $\mathbf{a} \in F^n$ are such that $\mathrm{mult}(P,\mathbf{a}) = m$, then $\mathrm{mult}(P^{(\mathbf{i})},\mathbf{a}) \geq m - \mathrm{wt}(\mathbf{i})$.*

Proposition 6. *Let $P(\mathbf{X}) \in \mathbb{F}[\mathbf{X}]$ where $\mathbf{X} = (X_1,\ldots,X_n)$. Let $\mathbf{a},\mathbf{b} \in \mathbb{F}^n$. Let $P_{\mathbf{a},\mathbf{b}}$ be the polynomial $P(\mathbf{a}+T\mathbf{b}) \in \mathbb{F}[T]$. Then for any $t \in \mathbb{F}$ we have*

$$\mathrm{mult}(P_{\mathbf{a},\mathbf{b}}, t) \geq \mathrm{mult}(P, \mathbf{a}+t\mathbf{b}).$$

Proposition 7 (Strengthening of the Schwartz-Zippel lemma)**.** *Let $P \in \mathbb{F}[\mathbf{X}]$ be a nonzero polynomial of total degree d. Then for any finite $S \subseteq \mathbb{F}$,*

$$\sum_{\mathbf{a}\in S^n} \mathrm{mult}(P,a) \leq d|S|^{n-1}.$$

Theorem 8. *If $K \subseteq F^n$ is a Kakeya set, then $|K| \geq \left(\frac{q}{2-1/q}\right)^n$.*

Proposition 9. *Given a set $K \subseteq \mathbb{F}^n$ and nonnegative integers m, d such that*

$$|K| < \binom{d+n}{n} \Big/ \binom{m+n-1}{n},$$

then there exists a nonzero polynomial $P = P_{m,K} \in \mathbb{F}[\mathbf{X}]$ of total degree at most d such that $\mathrm{mult}(P,a) \geq m$ for every $\mathbf{a} \in K$.