The Kakeya Problem Over Finite Fields

Juraj Milcak
University of Toronto
MAT477
Instructor: Prof. Milman

November 16, 2011

Kakeya sets $K \subset \mathbb{F}^n$, $\mathbb{F}$-finite field, $|\mathbb{F}| = q$.

Def. K Kakeya if $\forall$ direction $x \in \mathbb{F}^n$ $\exists y \in \mathbb{F}^n$ s.th. the line

$$L_{y,x} = \{y + t \cdot x | t \in \mathbb{F}\} \subset K.$$

Thm. $|K| \geq C_n \cdot q^n$, $C_n := C(n)$ (does not depend on q !).

Def. K is (δ, γ)-Kakeya set if $\exists$ subset $\mathcal{L} \subset \mathbb{F}^n$ s.th. $|\mathcal{L}| \geq \delta \cdot q^n$

and $\forall$ direction $x \in \mathcal{L}$ $\exists$ y s.th. $|\{y + t \cdot x | t \in \mathbb{F}\} \cap K| \geq \gamma \cdot q$.

The size of $(\delta, \gamma) - K$ sets

Main Prop. K is (δ, γ)-Kakeya, $d := \lfloor q \cdot \min\{\delta, \gamma\} \rfloor - 2 \Longrightarrow$

$$|K| \geq \binom{d+n-1}{n-1} = \# of \text{ monomials} \in \mathbb{F}[x_1, \cdots, x_n] \text{ of degree } d.$$

Proof (next 4 pages). If otherwise:

$|K| < \binom{d+n-1}{n-1}$. $\overset{lin.alg.}{\Longrightarrow}$ $\exists$ homogenous $g \in \mathbb{F}[x_1, \ldots, x_n] \setminus \{0\}$,

$deg(g) = d$ and $\forall x \in K$, $g(x) = 0$.

$K' := \{c \cdot x | x \in K, c \in \mathbb{F}\} \subset \{g(x) = 0\}$, since $g(cx) = c^d g(x)$.

Claim 1: $\forall y \in \mathcal{L}, g(y) = 0 \Longleftarrow \mathcal{L}$ as on page 2, i.e.

$\forall y \in \mathcal{L}$, $\exists\ z \in \mathbb{F}^n$ s.th. $|\{z + t \cdot y | t \in \mathbb{F}\} \cap K| \geq \gamma \cdot q \geq d + 2$.

Proof: $\Longrightarrow \exists\ a_1, \cdots, a_{d+1} \in \mathbb{F} \setminus \{0\}$, s.th. $z + a_i \cdot y \in K$.

Put $w_i := a_i^{-1} \cdot z + y$ so that $w_i \in K' \implies g(w_i) = 0$.

Then if $z = 0 \Longrightarrow g(y) = 0$ and if $z \neq 0 \Longrightarrow w_i \neq w_j$ for $i \neq j$

$\Longrightarrow$ univariate $g_{y,z}(t) := g(y + t \cdot z)$ has $d + 1$ zeros (roots)

$\Longrightarrow g_{y,z} \equiv 0 \Longrightarrow g(y) = 0$.

The Beautiful Shwartz-Zippel Lemma:

$f \in \mathbb{F}[\ \overrightarrow{x}\ ]$, $deg(f) = d > 1 \implies |\{x \in \mathbb{F}^n | f(x) = 0\}| \leq d \cdot q^{n-1}$.

Pf. Say $n \geq 2, d < q$. Let $g + h := f$, g homogenous, $deg(g) = d$

and $deg(h) < d$; $p \in \mathbb{F}^n \setminus \{0\}$ s.th. $g(p) \neq 0$. Split $\mathbb{F}^n$ into q^{n-1}

parallel lines $\{x + t \cdot p | t \in \mathbb{F}\}$ and denote $f_{x,p} := f(x + t \cdot p)$

$\implies deg(f_{x,p}) \leq d$, $f_{x,p} \not\equiv 0$ (since coeff. of t^d is $g(p) \neq 0$).

$\implies |\{t \in \mathbb{F} | f_{x,p}(t) = 0\}| \leq d \implies |\{x \in \mathbb{F}^n | f(x) = 0\}| \leq d \cdot q^{n-1}$.

Claim 2: $\forall \epsilon > 0, |K| \geq C_{n,\epsilon} \cdot q^{n-\epsilon}$.

Claim 1: $\mathcal{L} \subset \{x \in \mathbb{F}^n | g(x) = 0\}$. Since $d = \lfloor q \cdot \min\{\delta, \gamma\} \rfloor - 2$

$\implies d/q < \delta$ plus $|\mathcal{L}| \geq \delta \cdot q^n \implies$?! with the Beautiful S-Z.

$\implies |K| \geq \binom{d+n-1}{n-1}$ as claimed. □

Corollary of Main Proposition for $\delta = \gamma = 1$:

$$|K| \geq \binom{q+n-1}{n-1} = \frac{1}{(n-1)!} q^{n-1} + O_n(q^{n-2}) \geq C_n \cdot q^{n-1}.$$

A product of Kakeya sets is also a Kakeya set $\implies |K|^r \geq C_{nr} q^{nr-1}$

$\implies |K| \geq C_{n/r} \cdot q^{n-1/r} \implies \forall \epsilon > 0, \ |K| \geq C_{n,\epsilon} \cdot q^{n-\epsilon}$.

Proof of: $|K| \geq C_n \cdot q^n$. If otherwise $\Longrightarrow$

$\exists\ K,\ |K| < \binom{q+n-1}{n} \overset{lin.alg.}{\Longrightarrow} \exists\ P \in \mathbb{F}[\ \overrightarrow{x}\ ] \setminus \{0\},\ deg(P) \leq q-1,$

s.th. $P|_K \equiv 0$. Set $P =: \sum_{i=0}^{q-1} P_i$, P_i is homogenous, $deg(P_i) = i$

$\Longrightarrow \forall y \in \mathbb{F}^n\ \exists\ b \in \mathbb{F}^n$ s.th. $P(b+ty) = 0,\ \forall\ t \in \mathbb{F}$.

$P(b+ty)$ is of $deg \leq q-1$ in $t \Longrightarrow P(b+ty) \equiv 0$ for all t

$\Longrightarrow$ coeff. of t^{q-1} is 0 $\Longrightarrow P_{q-1}(y) = 0$.

Proof that $|K| \geq C_n \cdot q^n$ continued:

$y \in \mathbb{F}^n$ was arbitrary $\Longrightarrow P_{q-1} \equiv 0$

$\Longrightarrow$ inductively, $P_{q-2}, \ldots, P_1 \equiv 0$.

$\Longrightarrow P = P_0 = 0$ i.e. $P \equiv 0$, contradiction.

Conclusion:

$$|K| \geq \binom{q+n-1}{n} = \frac{1}{n!} q^n + O_n(q^{n-1}) \geq C_n \cdot q^n. \quad \square$$