This lecture started with a fairly detailed recap of the material covered in Lecture 16, in particular:

- Hasse derivative,
- Multiplicity,
- Proposition 3(3),
- Lemma 5.
- Corollary 7,

leading up to the statement of the multiplicities-aware Schwartz-Zippel lemma

LEMMA 8 (SCHWARTZ-ZIPPEL WITH MULTIPLICITIES)

Let $p(\vec{x}) \in \mathbb{F}[\vec{x}]$ be an n-variate nonzero polynomial of total degree $\deg(p) \le d$. Then for any finite $S \subseteq \mathbb{F}$ it holds that

$$\sum_{a \in S^n} \operatorname{mult}(p, \vec{a}) \le d \cdot |S|^{n-1}$$

Proof By induction over n.

Base case $n = 1$

First show that if $\operatorname{mult}(p, a) = m$, then $(x-a) \mid p(x)$ (as should be the case unless we got the definitions wrong).

By def of multiplicity, we have

$$p(a+z) = \sum_i p^{(i)}(a)\, z^i$$

and

$$\forall i < m \quad p^{(i)}(a) = 0$$

Hence

$$z^m \mid p(a+z)$$

and

$$(x-a)^m \mid p(a+(x-a)) = p(x)$$

Hence [or, if you want to vary your language, write "thus", "consequently," or "therefore"] the sum of multiplicities cannot exceed the degree of p, or

$$\sum_{a \in S} \text{mult}(p, a) \leq \deg(p)$$

Inductive step

Suppose $n > 1$. Write

$$p(\vec{x}) = \sum_{j=0}^{t} p_j(x_1, \ldots, x_{n-1})\, x_n^j \qquad (1)$$

where $\deg(p_j) \leq d-j$ and $t \leq d$ is chosen so that $p_t(x_1, \ldots, x_{n-1}) \neq 0$.

For any $(a_1, \ldots, a_{n-1}) \in S^{n-1}$, let

$$m_{a_1, \ldots, a_{n-1}} = \text{mult}(p_t, (a_1, \ldots, a_{n-1}))$$

We want to show that

$$\sum_{a_n \in S} \text{mult}(p, (a_1, \ldots, a_n)) \leq m_{a_1, \ldots, a_{n-1}} \cdot |S| + t \qquad (2)$$

If we can prove this, the lemma follows
Assuming (2), we get

$$\sum_{(a_1, \ldots, a_n) \in S^n} \text{mult}(p, (a_1, \ldots, a_n)) \leq$$

$$\sum_{(a_1, \ldots, a_{n-1}) \in S^{n-1}} \sum_{a_n \in S} \text{mult}(p, (a_1, \ldots, a_n)) \leq$$

$$\sum_{(a_1, \ldots, a_{n-1}) \in S^{n-1}} \left(m_{a_1, \ldots, a_{n-1}} |S| + t \right) \leq \quad [\text{using } (2)]$$

[using IH]

$\leq \quad \deg(p_t) \cdot |S|^{n-2} \cdot |S| \; + \; t \cdot |S|^{n-1}$

$\leq \quad (d - t \; + t)\; |S|^{n-1}$

and the induction step goes through.
So let us prove (2).

Fix $a_1, \ldots, a_{n-1} \in S$
Let $\vec{i} = (i_1, \ldots, i_{n-1})$ be such
that $wt(\vec{i}) = m_{a_1, \ldots, a_{n-1}}$ and

$$p_t^{(\vec{i})}(x_1, \ldots, x_{n-1}) \neq 0$$

Write $(\vec{i}, 0)$ to denote $(i_1, \ldots, i_{n-1}, 0)$
By using $(+)$ again, we observe that

$$p^{(\vec{i},0)}(x_1, \ldots, x_n) = \sum_{j=0}^{t} p_j^{(\vec{i})}(x_1, \ldots, x_{n-1})\, x_n^j \quad (3)$$

and hence, in particular, $p^{(\vec{i},0)}$ is
a nonzero polynomial

By Lemma 5 and Corollary 7 we have
that if we look at the line through
$\vec{c}_1 = (a_1, \ldots, a_{n-1}, 0)$ in direction $\vec{c}_2\,(0, \ldots, 0, a_n)$
it holds that

$$\mathrm{mult}\,(p(x_1, \ldots, x_n), (a_1, \ldots, a_n)) \leq \qquad [\text{Lem } 5]$$

$$\leq wt(\vec{i}, 0) + \mathrm{mult}(p^{(\vec{i},0)}(x_1, \ldots, x_n), (a_1, \ldots, a_n)) \leq$$

[by construction
of $\vec{i}$]

$\leq m_{a_1,\dots,a_{n-1}} + \text{mult}(p^{(\vec{i},0)}(x_1,\dots,x_n), (a_1,\dots,a_n))$ $\overset{\text{V}}{\leq}$

$\left[\text{setting } q(t) = p^{(\vec{i},0)}_{\vec{c}_1,\vec{c}_2}(t) = p^{(\vec{i},0)}(\vec{c}_1 + t\vec{c}_2)\right]$

$$\leq m_{a_1,\dots,a_{n-1}} + \text{mult}(q(t), a_n) \qquad (4)$$

But by (3), $q(t)$ is a degree-t univariate polynomial, so

$$\sum_{a_n \in S} \text{mult}(q(t), a_n) \leq t. \qquad (5)$$

Summing (4) over all $a_n \in S$ and using (5) we obtain

$\text{mult}(p, \vec{a}) \leq$

$$m_{a_1,\dots,a_{n-1}} \cdot |S| + t$$

which is exactly what we wanted to prove
The lemma follows by the induction principle $\boxed{\text{Q}}$

Setting $S = \mathbb{F}_q$, we can state the multiplicities Schwartz-Zippel lemma as follows.

COROLLARY 9

Let $p \in \mathbb{F}_q[x_1, \ldots, x_n]$ be a polynomial of total degree at most d. Then if

$$\sum_{\vec{a} \in \mathbb{F}_q^n} \text{mult}(p, \vec{a}) > d \cdot q^{n-1}$$

it holds that $p(\vec{x})$ is the identically zero polynomial.

Next time we will use Schwartz-Zippel with multiplicities to prove an almost optimal lower bound on the size of Kakeya sets.

Lower bound on Kakeya set size — the plan

1. Find a somewhat low-degree polynomial that vanishes on K with high multiplicity

2. Show that homogeneous part of this polynomial vanishes with fairly high multiplicity <u>everywhere on $\mathbb{F}_q^n$</u>

3. Use multiplicities Schwartz-Zippel to derive contradiction

<u>CLAIM A & B</u>

Given a set $K \subseteq \mathbb{F}_q^n$ and $m, d \in \mathbb{N}^+$ such that

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

there exists a nonzero polynomial $p \in \mathbb{F}_q[\vec{x}]$ of total degree $\leq d$ such that $\forall \vec{a} \in K$

$$\mathrm{mult}(p, \vec{a}) \geq m$$

Proof As before

$\#$ monomial of degree $\le d$ $\binom{d+n}{n}$

Condition $\mathrm{mult}(p, \vec{a}) \ge m$ imposes $\binom{m+n-1}{n}$ homogeneous linear constraints.

$\#$ constraints $<$ $\#$ unknowns (coefficients of monomials)

$\Downarrow$

$\exists$ nonormal solution p. $\boxed{}$

We are aiming to prove:

> THEOREM If $K \subseteq \mathbb{F}_q^n$ Kakeya set, then $|K| \ge \left(\frac{q}{2-1/q}\right)^n$

Let $\ell = Cq$ for some large constant $C \in \mathbb{N}^+$

Set

$$m = 2\ell - \ell/q \qquad (1)$$

$$d = \ell q - 1 \qquad (2)$$

Meaning of parameters

d : degree of polynomial p (upper bound)

m : multiplicities of zeros of p on K

ℓ : multiplicities of zeros of H_p

We have

$$d < \ell q \qquad (3)$$

$$(m-\ell)q > d-\ell \qquad (4)$$

~~From~~ (4) it follows (since $q \geq 1$) that

$$(m-w)q > d-w \quad \text{for } w \leq \ell \qquad (5)$$

We will show

$$|K| \geq \frac{\binom{d+n}{n}}{\binom{m+n-1}{n}} \geq \alpha^n$$

for $\alpha \to \dfrac{q}{2-1/q}$ as $\ell \to \infty$

Assume towards contradiction

$$|K| < \frac{\binom{d+n}{n}}{\binom{m+n-1}{n}} \qquad (6)$$

By Claim A&B $\exists\, d^*$, $0 < d^* \leq d$, and $p \in \mathbb{F}_q[\vec{x}]$, $\deg(p) = d^*$, such that $\forall \vec{x} \in K$ $\mathrm{mult}(p, \vec{x}) \geq m$

We have
$$d^* \geq m$$
since p nonzero and vanishes to multiplicity $\geq m$ at some point and
$$m \geq \ell$$
by our choice (1), and so
$$d^* \geq \ell \qquad (7)$$

Let $H_p(\vec{x})$ homogeneous part of p of degree d^*. Note $H_p(\vec{x}) \neq 0$.

CLAIM C
$\forall \vec{b} \in \mathbb{F}_q^n \quad \text{mult}(H_p, \vec{b}) \geq \ell$

<u>Proof</u> Fix $\vec{i}$, $wt(\vec{i}) = w \leq \ell - 1$ (so we can apply (5)).

Let $q(\vec{x}) = p^{\vec{i}}(\vec{x})$

Let $d' := \deg(q(\vec{x})) \leq d^* - w$.

Fix $\vec{a} = \vec{a}(\vec{b})$ s.t. $\{\vec{a} + t\vec{b} \mid t \in \mathbb{F}_q\} \subseteq K$.

By Lem 5 $\text{mult}(q, \vec{a} + t\vec{b}) \geq m - w$

Applying (5) we have
$$(m-w)q > d^* - w \geq d'$$

Let $q_{\vec{a},\vec{b}}(t) = q(\vec{a} + t\vec{b})$

$q_{\vec{a},\vec{b}}$ univariate of degree $\leq d'$

By Cor 7

$q_{\vec{a},\vec{b}}$ vanishes at each point of F_q with multiplicity $m - w$

Since

$$(m-w)\, q > d^* - w \geq \deg(q_{\vec{a},\vec{b}}(t))$$

we have $q_{\vec{a},\vec{b}}(t)$ is identically zero

$$q = \sum_{i=1}^{d'} c_i t^i$$

$\forall_i\ c_i = 0$. In particular, $c_{d'} = 0$.

Let $H_q(\vec{x})$ be homogeneous part of q of highest degree. Then (as before) $c_{d'} = q(\vec{b})$

Hence $q(\vec{b}) = 0$

Now if $(H_p)^{(\vec{i})}(\vec{x}) = 0$ then clearly in particular $(H_p)^{(\vec{i})}(\vec{b}) = 0$. Otherwise by Prop 3 (3)

$$(H_p)^{(\vec{i})}(\vec{b}) = (H_q)(\vec{b}) = 0$$

Since this is true for all
$\vec{i}$ of weight $wt(\vec{i}) \leq \ell - 1$,
it follows that

$$\forall \vec{b} \in \mathbb{F}_q^n \quad mult(H_p, \vec{b}) \geq \ell$$

as claimed $\boxed{\text{Z}}$

It follows that (6) cannot hold,
and so

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

By the way we set the parameters (in (1) & (2))

$$\frac{\binom{d+n}{n}}{\binom{m+n-1}{n}} = \frac{\binom{\ell q - 1 + n}{n}}{\binom{2\ell - \ell/q + n - 1}{n}} = \frac{\prod_{i=1}^{n} (\ell q - 1 + i)}{\prod_{i=1}^{n} (2\ell - \ell/q - 1 + i)}$$

But this is true for all $\ell = Cq$
for arbitrarily large C (and ℓ)

Hence

$$|K| \geq \lim_{\ell\to\infty} \frac{\prod_{i=1}^{n} \ell(q - 1/\ell - i/\ell)}{\prod_{i=1}^{n} \ell(2 - 1/q - 1/\ell + i/\ell)}$$

$$= \lim_{\ell\to\infty} \frac{\prod_{i=1}^{n} (q - 1/\ell - i/\ell)}{\prod_{i=1}^{n} (2 - 1/q - 1/\ell + i/\ell)}$$

$$= \left(\frac{q}{2 - 1/q} \right)^{n}$$

which is what we wanted to prove. The theorem follows (Yay!).