Three announcements

1. 3 problem sets (not 4)
   Pset 2 was posted on Friday

2. You have to provide at least one solution on Piazza to pass a pset. This holds also for pset 1
   (Plus you need at least a C on the pset itself to pass, but local TCS students usually get an A)

3. Time to start thinking about a research paper to present

LAST TIME

Saw an application of the POLYNOMIAL METHOD

1. Given subset K satisfying some algebraic conditions, construct nonzero low-degree polynomial g that vanishes on all $x \in K$

2. Use algebraic conditions on K to show that in fact g (or some relative g^*) vanishes on a set K' such that $|K'| \gg |K|$

3. Conclude that g (or g^*) has to be identically zero. Contradiction. Hence properties of K "impossibly good"

Recall Kakeya set $K \subseteq \mathbb{F}_q^n$
"contains a line in every direction"

$\forall \vec{x} \in \mathbb{F}_q^n \ \exists \vec{y} \in \mathbb{F}_q^n$

$$L_{\vec{y},\vec{x}} = \{ y + ax \mid a \in \mathbb{F}_q \} \subseteq K$$

Also considered "somewhat" Kakeya sets or "statistical" Kakeya sets

$K \subseteq \mathbb{F}_q^n$ (δ, γ)-Kakeya set if

$\exists \mathcal{L} \subseteq \mathbb{F}_q^n$ (good directions), $|\mathcal{L}| \geq \delta \cdot q^n$

$\forall \vec{x} \in \mathcal{L} \ \exists \vec{y} \in \mathbb{F}_q^n$

$$| L_{\vec{y},\vec{x}} \cap K | \geq \gamma \cdot q$$

First proved lower bound

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

using statistical Kakeya set

(1) Construct low-degree homogeneous $g \in \mathbb{F}_q[\vec{x}]$ s.t. $g(\vec{x}) = 0 \quad \forall x \in K$

(2) By homogeneity $g(\vec{y}) = 0 \quad \forall \vec{y}$ on lines through 0 and $\vec{x} \in K$

(3) For direction $\vec{x} \in \mathcal{L}$, can find line $\ell = \{ \vec{a} + t\vec{b} \mid t \in \mathbb{F}_q \}$ such that

(a) $x \in \ell$
(b) $g \restriction \ell$ has many zeros (and is univariate polynomial in t).

(4) Hence $g(x) = 0 \quad \forall x \in \mathcal{L}$
But this set is too large!
Contradicts Schwartz-Zippel lemma $\Rightarrow$
g zero after all $\Rightarrow$
Contradicts that K can be small

Then proved lower bound

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

(1) Let K real Kakeya set (not statistical).
Construct low-degree poly g that vanishes on K.

(2) write $g = \bar{g} + g^*$

$\bar{g}$ homogeneous part of max degree d ($d \neq 0$)

(3) For any $\vec{x} \in \mathbb{F}_q^n$ $\exists \vec{y} \in \mathbb{F}_q^n$ s.t.
$\{\vec{y} + a\vec{x} \mid a \in \mathbb{F}_q\} \subseteq K$
Then $h(t) = g(\vec{y} + t\vec{x})$ has
many zeros and must be identically
zero $\Rightarrow h = \sum_{i=0}^{d} a_i t^i$ with all $a_i = 0$

(4) But coefficient a_d in $h(t)$ is
$a_d = \bar{g}(x)$, so $\bar{g}(x) = 0 \quad \forall x \in \mathbb{F}_q^n$
Contradicts Schwartz-Zippel, so
K cannot be this small.

OK, so now we know
$|K| \geq C_n \cdot q^n$
and question is settled, right?

Not quite ... What is C_n ?

$C_n \leq 1$ since $\mathbb{F}_q^n$ is a Kakeya set

In fact, Dvir showed there are Kakeya sets for

$$C_n \approx \frac{1}{2^{n-1}}$$

Lower bound from last lecture yields

$$C_n \geq 1/n!$$

[Saraf & Sudan]: $C_n \geq 1/(2.6)^n$

TODAY AND NEXT LECTURE
Show result from (Conference version earlier)

[Dvir, Kopparty, Saraf & Sudan '13]

that $C_n \geq 1/2^n$

Effectively closes the gap (except for factor 2)

Improves state-of-the-art randomness extractors (we won't have time to talk about this)

METHOD OF MULTIPLICITIES

① Given set K satisfying algebraic properties, construct nonzero low-degree $g \in \mathbb{F}[\vec{x}]$ that vanishes on K with high multiplicity

② Use algebraic conditions on K to show that g (or relative g^*) vanishes on larger set with high multiplicity

③ Conclude that g (or g^*) has to be identically zero, using beefed-up version of Schwartz-Zippel.
Contradicts "too good" properties of K

To warm up, look at univariate polynomials over, say, $\mathbb{R}$ or $\mathbb{Q}$.

$p(a) = 0$ if $(x-a) \mid p(x)$

a multiple zero if $(x-a)^2 \mid p(x)$

$$p(x) = (x-a)^2 \, q(x)$$

$$p'(x) = 2(x-a)\, q(x) + (x-a)^2 \, q'(x)$$

so p and derivative p' share zero a.

$p(x) = x^3 - 3x^2 + 3x - 1$

$p(x) = (x-1)^3$

1 zero of multiplicity 3

$$\left.\begin{aligned} p'(x) &= 3(x-1)^2 \\ p''(x) &= 6(x-1) \end{aligned}\right\} \text{ also have 1 as zero}$$

Now look at $(x-1)^3$ over, say, $\mathbb{F}_3$

$p(x) = (x-1)^3 = x^3 - 1$

$p'(x) = 0$

Lost all info. Can't distinguish between, e.g.,

$(x-1)^3$ and identically zero polynomial.

Not nice.

Standard derivative not so helpful in positive characteristic.

Define instead HASSE DERIVATIVE

For $p(x) = \sum a_k x^k$, the ith Hasse derivative is

$$p^{(i)}(x) = \sum \binom{k}{i} a_k x^{k-i}$$

Need to generalize this to multivariate case.

From now on, write

$$\vec{i} = (i_1, \ldots, i_n)$$
$$\vec{x} = (x_1, \ldots, x_n)$$

etc (perhaps sometimes even without vector arrow)

$\vec{i}$ will denote vector of (non-negative) exponents

WEIGHT $wt(\vec{i}) = \sum_{j=1}^{n} i_j$

For compactness of notation

$$\vec{x}^{\vec{i}} = \prod_{j=1}^{n} x_j^{i_j}$$

Note that $\deg(\vec{x}^{\vec{i}}) = wt(\vec{i})$

Also use notation

$$\binom{\vec{i}}{\vec{j}} = \prod_{k=1}^{n} \binom{i_k}{j_k}$$

LEMMA 1 Let $\vec{z} = (z_1, \ldots, z_n)$ and $\vec{w} = (w_1, \ldots, w_n)$ and $r = (r_1, \ldots, r_n)$ and consider

$$(\vec{z} + \vec{w})^{\vec{r}} = (z_1 + w_1)^{r_1} \cdots (z_n + w_n)^{r_n} \qquad (*)$$

Then the coefficient of $\vec{z}^{\vec{i}} w^{\vec{r}-\vec{i}}$ in $(*)$ equals $\binom{\vec{r}}{\vec{i}}$

Proof Exercise.

DEF 2 For $p(\vec{x}) \in \mathbb{F}[\vec{x}]$ and $\vec{i} = (i_1, \ldots, i_n)$ non-negative, the $\vec{i}$ th HASSE DERIVATIVE of p, denoted $p^{(\vec{i})}(\vec{x})$ is the coefficient of $\vec{z}^{\,\vec{i}}$ in the polynomial

$$\hat{p}(\vec{x}, \vec{z}) := p(\vec{x} + \vec{z}) \in \mathbb{F}[\vec{x}, \vec{z}]$$

In particular

$$p(\vec{x} + \vec{z}) = \sum_{\vec{i}} p^{(\vec{i})}(\vec{x})\, \vec{z}^{\,\vec{i}} \qquad (\dagger)$$

EXAMPLE A Let $p(\vec{x}) = 2x_1^3 + x_2 x_3^2$

$$p(\vec{x} + \vec{z}) = 2(x_1 + z_1)^3 + (x_2 + z_2)(x_3 + z_3)^2$$

$$= 2x_1^3 + 6x_1^2 z_1 + 6x_1 z_1^2 + 2z_1^3$$

$$+ x_2 x_3^2 + 2x_2 x_3 z_3 + x_2 z_3^2$$

$$+ x_3^2 z_2 + 2x_3 z_2 z_3 + z_2 z_3^2$$

$$= (2x_1^3 + x_2 x_3^2) \cdot \vec{z}^{(0,0,0)} \qquad p^{(0,0,0)} = 2x_1^3 + x_2 x_3^2$$

$$+ (6x_1^2) \cdot \vec{z}^{(1,0,0)} \qquad p^{(1,0,0)} = 6x_1^2$$

$$+ (6x_1) \cdot \vec{z}^{(2,0,0)} \qquad p^{(2,0,0)} = 6x_1$$

$$+ (2) \cdot \vec{z}^{(3,0,0)} \qquad p^{(3,0,0)} = 2$$

$$+ (x_3^2)\, \vec{z}^{(0,1,0)} \qquad p^{(0,1,0)} = x_3^2$$

$$+ (2x_2 x_3)\, \vec{z}^{(0,0,1)} \qquad p^{(0,0,1)} = 2x_2 x_3$$

$$+ (2x_3)\, \vec{z}^{(0,1,1)} \qquad p^{(0,1,1)} = 2x_3$$

$$+ (x_2)\, \vec{z}^{(0,0,2)} \qquad p^{(0,0,2)} = x_2$$

$$+ (1)\, \vec{z}^{(0,1,2)} \qquad p^{(0,1,2)} = 1$$

PROPOSITION 3 (Basic properties of Hasse derivatives)

1. $p^{(\vec{i})}(\vec{x}) + q^{(\vec{i})}(\vec{x}) = (p+q)^{(\vec{i})}(\vec{x})$

2. If $p(\vec{x})$ is homogeneous of degree d, then either $p^{(\vec{i})}(\vec{x})$ is homogeneous of degree $d - wt(\vec{i})$ or $p^{(\vec{i})}(\vec{x}) = 0$

3. Let $H_Q(\vec{x})$ denote the homogeneous part of Q of highest total degree. Then either $(H_p)^{(\vec{i})}(\vec{x}) = H_{p^{(\vec{i})}}(\vec{x})$ or $(H_p)^{(\vec{i})}(\vec{x}) = 0$

4. $(p^{(\vec{i})})^{(\vec{j})}(\vec{x}) = \binom{\vec{i}+\vec{j}}{\vec{i}} p^{(\vec{i}+\vec{j})}(\vec{x})$

Note that (1)-(3) are the same as for standard derivatives but (4) is not!

However (4) says that if $(\vec{i}+\vec{j})$th derivative is zero, then $\vec{j}$th derivative of $\vec{i}$th derivative is also zero, which will be critical

<u>Proof of Prop 3</u> Exercise.

DEF 4 (MULTIPLICITY)

For $p(\vec{x}) \in \mathbb{F}[\vec{x}]$ and $\vec{a} \in \mathbb{F}^n$, the MULTIPLICITY OF p AT $\vec{a}$, denoted $\mathrm{mult}(p, \vec{a})$, is the largest integer M such that for every nonnegative $\vec{i}$ with $\mathrm{wt}(\vec{i}) < M$ it holds that $p^{(\vec{i})}(\vec{a}) = 0$

If M can be taken arbitrarily large, we set $\mathrm{mult}(p, \vec{a}) = \infty$

Note that:

1. $\mathrm{mult}(p, \vec{a}) \geq 0$ for every $\vec{a}$ (vacuously)

2. $p(\vec{a}) = 0$ if and only if $\mathrm{mult}(p, \vec{a}) \geq 1$ (since $p^{(\vec{0})}(\vec{x}) = p(\vec{x})$)

3. Condition $p^{(\vec{i})}(\vec{a}) = 0$ imposes homogeneous linear constraint on coefficients of p

Suppose weight limit M

$$\# \vec{i} \text{ s.t. } \mathrm{wt}(\vec{i}) < M$$
$$= \# \vec{i} \text{ s.t. } i_j \geq 0, \ \sum_{j=1}^{n} i_j \leq M-1$$
$$= \binom{M+n-1}{n}$$

So $\mathrm{mult}(p, \vec{a}) \geq M$ imposes at most $\binom{M+n-1}{n}$ homogeneous linear constraints of coefficients of $p(\vec{x})$

In a further twist, we will need to extend this definition to tuples of polynomials

$$\vec{p} = (p_1, \dots, p_m) \in \mathbb{F}[\vec{x}]^m$$

Define

$$\vec{p}^{(\vec{i})} = (p_1^{(\vec{i})}, \dots, p_m^{(\vec{i})})$$

then

$$\mathrm{mult}(\vec{p}, \vec{a}) = \min_{j \in [m]} \left(\mathrm{mult}(p_j, \vec{a}) \right)$$

We need to translate some of the properties of Hasse derivatives into properties of multiplicities

<u>LEMMA</u> 5 If $\mathrm{mult}(p, \vec{a}) = s$, then $\mathrm{mult}(p^{(\vec{i})}, \vec{a}) \geq s - wt(\vec{i})$

<u>Proof</u> By assumption, for any $\vec{k}$ with $wt(\vec{k}) < s$ we have $p^{(\vec{k})}(\vec{a}) = 0$.
Take any $\vec{j}$ s.t. $wt(\vec{j}) < s - wt(\vec{i})$.

We have $(p^{(\vec{i})})^{(\vec{j})}(\vec{a}) = \binom{\vec{i}+\vec{j}}{\vec{i}} p^{(\vec{i}+\vec{j})}(\vec{a})$

Since $wt(\vec{i}+\vec{j}) = wt(\vec{i}) + wt(\vec{j}) < s$
$p^{(\vec{i}+\vec{j})}(\vec{a}) = 0$ and hence $(p^{(\vec{i})})^{(\vec{j})}(a) = 0$.

Thus $\mathrm{mult}(p^{(\vec{i})}, \vec{a}) \geq s - wt(\vec{i})$.

Now let us see what happens with multiplicities when we compose polynomial tuples

Let $\vec{x} = (x_1, \ldots, x_n)$

$\vec{y} = (y_1, \ldots, y_\ell)$

$$\vec{p} = (p_1(\vec{x}), \ldots, p_m(\vec{x})) \in \mathbb{F}[\vec{x}]^m$$

$$\vec{q} = (q_1(\vec{y}), \ldots, q_n(\vec{y})) \in \mathbb{F}[\vec{y}]^n$$

Define the polynomial tuple

$$\vec{p} \circ \vec{q}\,(\vec{y}) \in \mathbb{F}[\vec{y}]^m$$

by

$$\vec{p} \circ \vec{q}\,(\vec{y}) =$$

$$\left(p_1(q_1(\vec{y}), \ldots, q_n(\vec{y})), \ldots, p_m(q_1(\vec{y}), \ldots, q_n(\vec{y}))\right)$$

PROPOSITION 6

For any $\vec{a} \in \mathbb{F}^\ell$ it holds that

$$\mathrm{mult}(\vec{p} \circ \vec{q}, \vec{a}) \geq \mathrm{mult}(\vec{p}, \vec{q}(\vec{a})) \cdot \mathrm{mult}(\vec{q} - \vec{q}(\vec{a}), \vec{a})$$

In particular, since $\mathrm{mult}(\vec{q} - \vec{q}(\vec{a})) \geq 1$, we have

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

Proof

Let $m_1 = \text{mult}\,(\vec{p}, \vec{q}(\vec{a}))$

$m_2 = \text{mult}\,(\vec{q} - \vec{q}(\vec{a}), \vec{a}) > 0$

If $m_1 = 0$ there is nothing to prove

Assume $m_1 > 0$ (so that $\vec{p}(\vec{q}(\vec{a})) = \vec{0}$.)

By liberal use of (†) we get

$$\vec{p}\,(\vec{q}\,(\vec{a} + \vec{z})) =$$

$$= \vec{p}\left(\vec{q}(\vec{a}) + \sum_{\vec{i} \neq 0} q^{(\vec{i})}(a)\,\vec{z}^{\,\vec{i}}\right) \qquad [\text{by } (\dagger)]$$

$$= \vec{p}\left(\vec{q}(\vec{a}) + \sum_{wt(\vec{i}) \geq m_2} \vec{q}^{(\vec{i})}(a)\,\vec{z}^{\,\vec{i}}\right)$$

[smaller derivatives of $\vec{q} = 0$ since $\text{mult}\,(\vec{q} - \vec{q}(\vec{a}), \vec{a}) = m_2$]

$$= \vec{p}\,(\vec{q}(\vec{a}) + \vec{h}(\vec{z}))$$

$$\left[\vec{h}(\vec{z}) = \sum_{wt(\vec{i}) \geq m_2} \vec{q}^{(\vec{i})}(\vec{a})\,\vec{z}^{\,\vec{i}}\right]$$

$$= \vec{p}\,(\vec{q}(\vec{a})) + \sum_{\vec{j} \neq 0} \vec{p}^{(\vec{j})}(\vec{q}(\vec{a}))\,\vec{h}(\vec{z})^{\vec{j}}$$

[by (†)]

$$= \sum_{wt(\vec{j}) \geq m_1} \vec{p}^{(\vec{j})}(\vec{q}(\vec{a}))\ \vec{h}(\vec{z}) \qquad (*)$$

[since $\mathrm{mult}(\vec{p}, \vec{q}(\vec{a})) = m_1 > 0$]

Now:

- Each monomial $\vec{z}^{\,\vec{i}}$ in $\vec{h}$ has $wt(\vec{i}) \geq m_2$.
- Also, each occurrence of $\vec{h}(\vec{z})$ is raised to $\vec{j}$ with $wt(\vec{j}) \geq m_1$

It follows that $(*)$ can be written on the form

$$\sum_{wt(\vec{k}) \geq m_1 \cdot m_2} c_{\vec{k}}\, \vec{z}^{\,\vec{k}}$$

By using $(\dagger)$ again, it follows that $(\vec{p} \circ \vec{q})^{\vec{k}}(\vec{a}) = 0$ for $wt(\vec{k}) < m_1 \cdot m_2$ and the proposition follows. $\boxtimes$

COROLLARY 7

Let $p(\vec{x}) \in \mathbb{F}[\vec{x}] = \mathbb{F}[x_1, \ldots x_n]$

Let $\vec{a}, \vec{b} \in \mathbb{F}^n$

Let

$$p_{\vec{a},\vec{b}}(t) := p(\vec{a} + t \cdot \vec{b}) \in \mathbb{F}[t]^*$$

Then for any $t \in \mathbb{F}$ it holds that

$$\text{mult}(p_{\vec{a},\vec{b}}, t) \geq \text{mult}(p, \vec{a} + t \cdot \vec{b}).$$

Proof Let $\vec{q}(t) = \vec{a} + t\vec{b} \in \mathbb{F}[t]^n$

Apply previous proposition to p, $\vec{q}$, and $p \circ \vec{q} = p_{\vec{a},\vec{b}}$. $\boxed{}$

Our previous lower bounds on Kakeya sets boiled down to applications of Schwartz-Zippel. We want to extend Schwartz-Zippel to take multiplicities of zeros into account

Standard form of Schwartz-Zippel says that for $p(\vec{x}) \in \mathbb{F}[\vec{x}]$ of degree d and $S \subseteq \mathbb{F}$, probability that $p(\vec{a}) = 0$ when a drawn uniformly at random from S^n is $\leq d / |S|$

---

*) Apologies for not warning sensitive viewers, but yes, this is suddenly a <u>univariate</u>, standard, non-vector polynomial

Note that

$$\min(1, \mathrm{mult}(p, \vec{a})) = \begin{cases} 1 & \text{if } p(\vec{a}) = 0 \\ 0 & \text{otherwise.} \end{cases}$$

Then we can write Schwartz-Zippel as follows

Schwartz-Zippel lemma, standard version

Let $p(\vec{x}) \in \mathbb{F}[\vec{x}]$, $\deg(p) \leq d$, $p \neq 0$, and let $S \subseteq \mathbb{F}$. Then

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

But what if p vanishes with higher multiplicity ~~of~~ on some $\vec{a}$?

Look at univariate case

Suppose $\mathrm{mult}(p, a) \geq 2$

Then $p(x) = (x-a)^2 \cdot p^*(x)$

for $\deg(p^*) = d - 2$

So p can only have $d-2$ other zeroes, since it "wasted" multiplicity 2 on a.

The key insight (or one of them) in [Dvir, Kopparty, Saraf, Sudan '13] is that this holds also in general.

XVII

LEMMA 8 (SCHWARTZ - ZIPPEL WITH MULTIPLICITIES)

Let $p \in \mathbb{F}[x_1, \dots, x_n]$ non-zero polynomial of total degree $\deg(p) \leq d$. Then for any finite $S \subseteq \mathbb{F}$ it holds that

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