Note Title 8/12/2013

Absolutely Sound Testing Of Lifted Codes

Madhu Sudan (MSR)

Joint works with

1. Bhattacharyya, Kopparty, Schoenebeek, Zuckerman
2. Haramaty, Shpilka
3. Haramaty, Ron-Zewi

Testing Low-Degree Polynomials

Given: oracle access to $f : \mathbb{F}_q^m \to \mathbb{F}_q$; degree d

Test: if f close to degree $\leq d$ polynomial?

- $\deg(f) \leq d \Rightarrow$ accept w.p. 1
- $\delta_d(f) \geq \delta \Rightarrow$ reject w.p. $\epsilon(f) \geq \epsilon$.

$\delta(f,g) \triangleq \Pr_x[f(x) \neq g(x)]$; $\delta_d(f) \triangleq \min_{g : \deg(g) \leq d} \{\delta(f,g)\}$

Testing Low-Degree Polynomials

Given: oracle access to $f: \mathbb{F}_q^m \to \mathbb{F}_q$; degree d

Test: if f close to degree $\leq d$ polynomial ?

- $\deg(f) \leq d \Rightarrow$ accept w.p. 1
- $\delta_d(f) \geq \delta \Rightarrow$ reject w.p. $\epsilon(f) \geq \epsilon$.

Questions: - How many queries does tester make ?

- What is relationship between $\delta(f)$ & $\epsilon(f)$?

Natural Test : "Subspace Test"

- Basic Fact : $\deg(f) \leq d \implies \deg(f|_A) \leq d \quad \forall$ subspaces A
- Use this to test ? Query complexity = q^t if $\dim(A) = t$.
- What is minimum t that suffices?
  - Every function on t vars has $\deg \leq t(q-1)$

    $\implies t \geq \left\lceil \frac{d+1}{q-1} \right\rceil$

Testing Dimension

- $q =$ prime : $t = \left\lceil \frac{d+1}{q-1} \right\rceil$ suffices

  $\left(\deg(f) > d \Rightarrow \exists A,\ \deg(f|_A) > d,\ \dim(A) = t \right)$

- $q = p^s$; $p =$ prime : $t = \left\lceil \frac{d+1}{q - q/p} \right\rceil$ is the right answer.

- Best query complexity $\sim q^{d/q}$

- This Talk: Best $\epsilon(f)$ vs. $\delta(f)$ for "best" t-dim. test.

Known Results :

$$\epsilon(f) \le \frac{1}{q^{2t}} \Rightarrow \delta(f) \le 2\epsilon(f)$$

AKKLR : $q = 2$

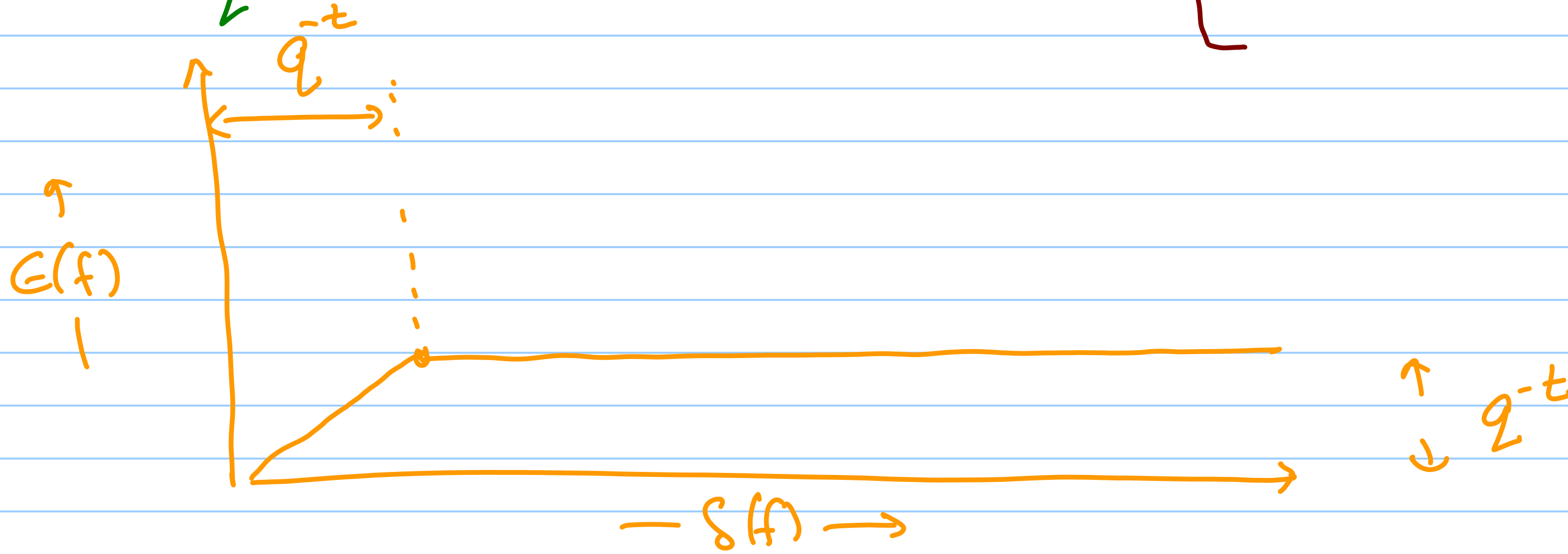
JPRZ, KR : arbit. q

KS : all aff. inv. prop.

Known Results:

$$\epsilon(f) \le \frac{1}{q^{2t}} \implies \delta(f) \le 2\epsilon(f)$$

AKKLR : $q = 2$
JPRZ, KR : arbit. q
KS : all aff. inv. prop.



Special Case of $q=2$

- for random function f: $\epsilon(f) \approx \delta(f) \approx \frac{1}{2}$
- Does every function with $\epsilon(f) \leq \frac{1}{2} - \alpha$

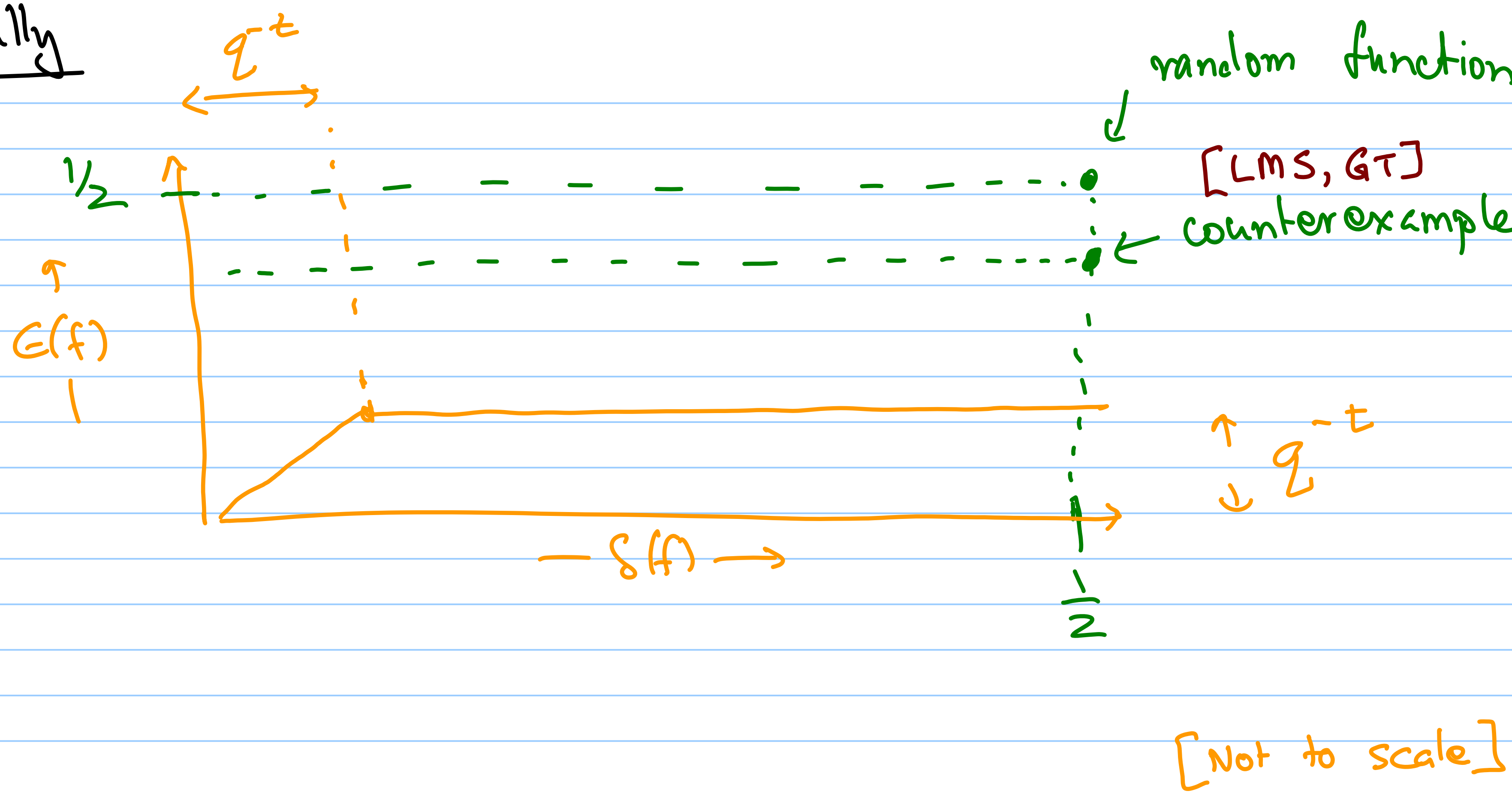
  have $\delta(f) \leq \frac{1}{2} - \beta(d, \alpha)$? $\Bigg\}$ $\alpha > 0 \Rightarrow \beta > 0$

  "Inverse Gowers Conjecture" [Bogdanov-Viola, others]

- No: [Lovett Meshulam-Samorodnitsky, Green-Tao]

$\exists \alpha > 0, \forall d, \exists f$ with $\epsilon(f) = \frac{1}{2} - \alpha, \ \delta(f) = \frac{1}{2} - o(1)$

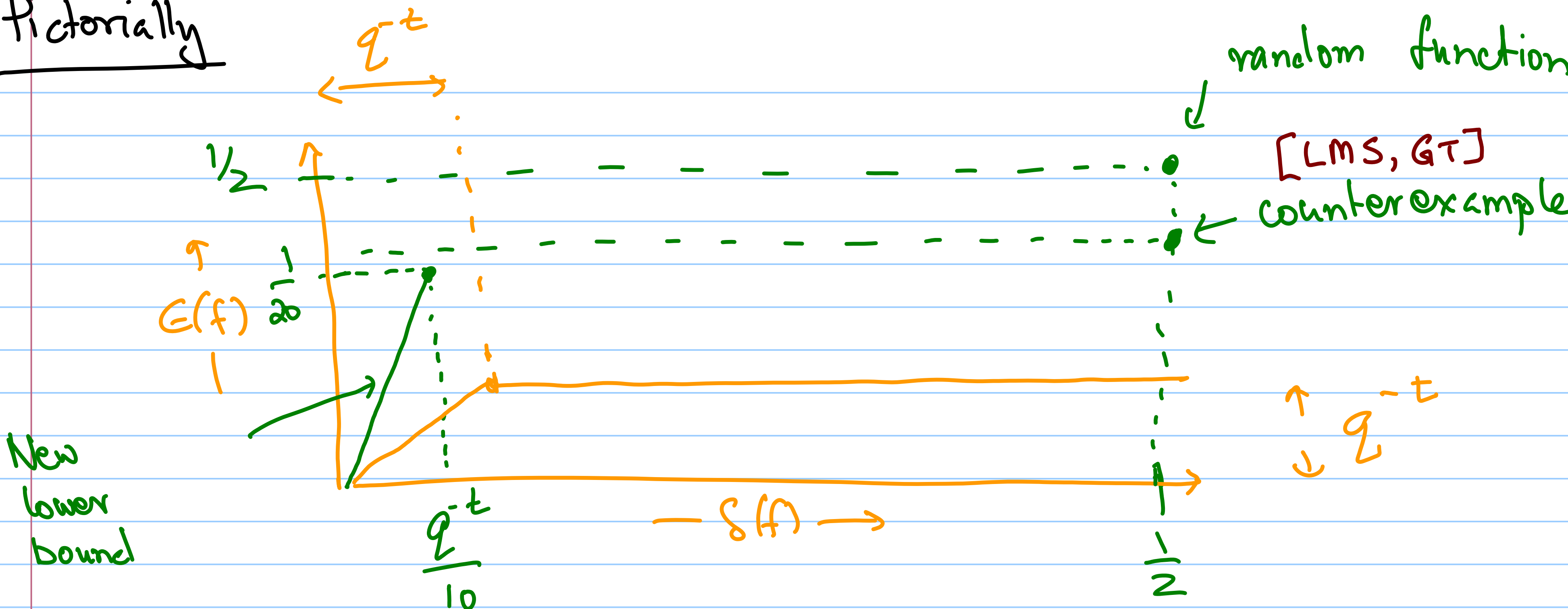
Pictorially



Better Initial Slope: $\delta(f) \le \frac{q^{-t}}{10}$: Let g be nearest deg. d poly.

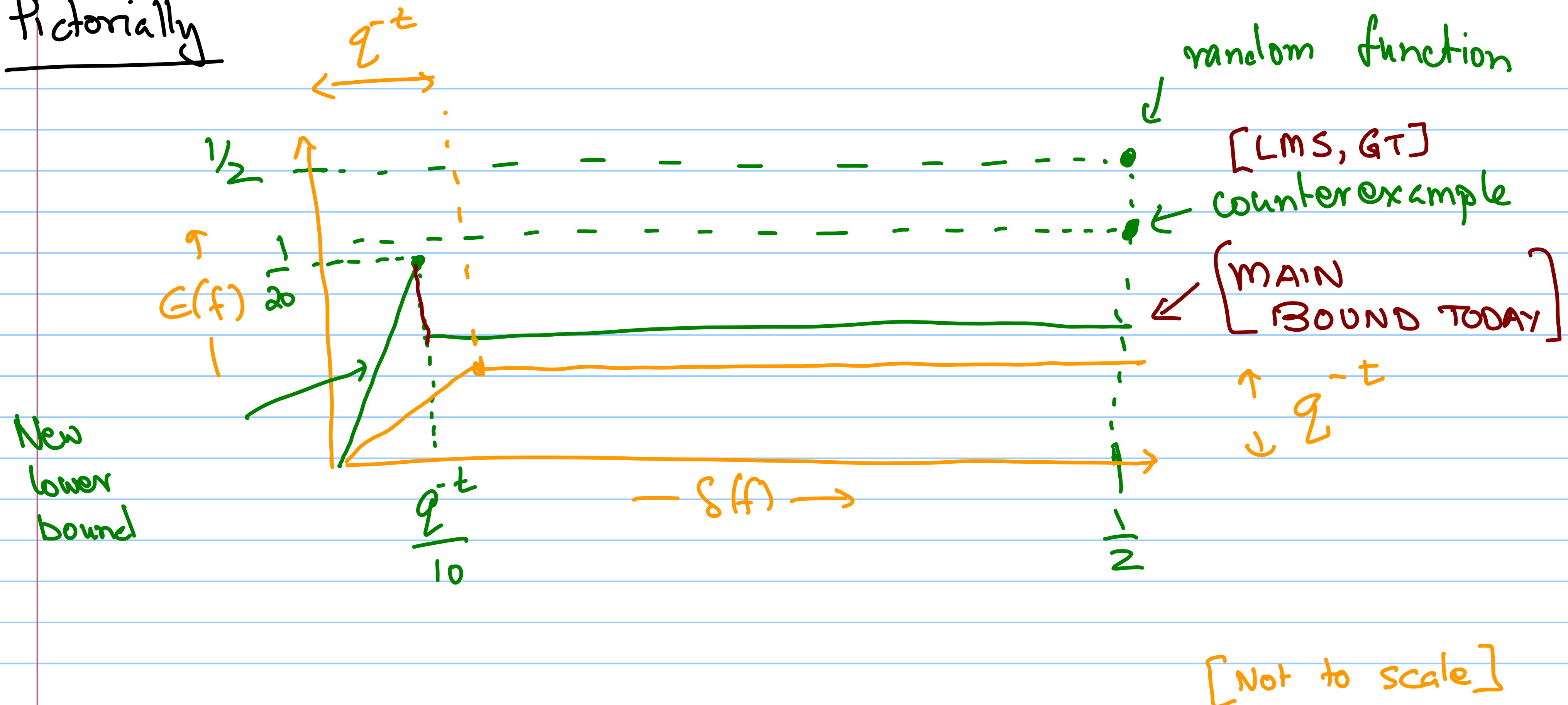
- Random t-dim subspace contains $q^t \cdot \delta$ pts s.t. $f(x) \neq g(x)$ in expectation.
- Chebychev $\Rightarrow$ $\Pr_A \left[\#\{\text{pts. in } A \text{ s.t. } f(x) \neq g(x)\} = 1 \right] \ge \frac{q^t \cdot \delta}{2}$

Pictorially



[Not to scale]

Pictorially



Theorem [BKSSZ, HSS, HRS]: $\forall q \; \exists \epsilon_q > 0$ s.t. $\forall t, \forall m$,

$\forall B \subseteq \{ \mathbb{F}_q^t \to \mathbb{F}_q \}$,

$\forall P = \text{Lift}_m(B)$

$$\epsilon(f) \geq \min \{ q^t \cdot \delta(f), \epsilon_q \}$$

[BKSSZ]: $q=2$; B = deg d poly

[HSS]: q arbit; ''

[HRS]: '' ; B arbit.

Motivations

Originally [BKSSZ]:

- Clean question with broad interest
- Tight analysis would give first affine-inv. property with "perfect" understanding of testing complexity

Now [Barak Gopalan Håstad Meka Raghavendra Steurer]

- new constructions of small set expanders.
  Uses [BKSSZ]; other examples from [HRS].

Main Ingredient: Explore f restricted to "hyperplanes" - H
[codim 1 subspaces]

By defn: $$\epsilon(f) = \mathbb{E}_{H}\left[\epsilon(f|_H)\right]$$

Main Question: Is $\delta(f) \overset{?}{\approx} \mathbb{E}_{H}\left[\delta(f|_H)\right]$?

Our Answer: $\sim$ YES.

Lemma: Let $\mathcal{H}_\delta \triangleq \{H \mid \delta(f|_H) \le \delta\}$; Then if $|\mathcal{H}_\delta| \geq \Omega(q^t)$
then $\delta(f) \le O(\delta + q^{-t})$

Lemma $\Rightarrow$ Theorem?

- Proof by induction on n
- Either $\exists$ many hyperplanes on which $\delta(f|_H)$ small
  in which case Lemma does the job.
- Else on most hyperplanes $\delta(f|_H) \approx \delta(f)$ in which
  case on most hyperplanes $\epsilon(f|_H) \approx \epsilon_2$.

Important: most is highly overwhelming....

Restrictions to Hyperplanes :

5 $\mathcal{H}_\delta \triangleq \{H \mid \delta(f|_H) \leq \delta\}$: $|\mathcal{H}| \geq \Omega(q^t) \Rightarrow \delta(f) \leq 9\delta + O(q^{-t})$.

Restrictions to Hyperplanes:

1. $\delta(f) > 0 \Rightarrow \exists H$ s.t. $\delta(f|_H) > 0$

"characterization"

Proved by showing $\exists$ affine $\times$ form A s.t. $f \circ A$ has monomial of deg $> d$ supported on first $t+1$ variables.

5. $\mathcal{H}_\delta \triangleq \{H \mid \delta(f|_H) \leq \delta\}: |\mathcal{H}| \geq \Omega(q^t) \Rightarrow \delta(f) \leq q\delta + O(q^{-t})$.

Restrictions to Hyperplanes:

1. $\delta(f)>0 \implies \exists H$ s.t. $\delta(f|_H)>0$

2. $\delta(f)>0 \implies \Pr_H\left[\delta(f|_H)>0\right] \geq \frac{1}{q}$

3. $\mathcal{H}_\delta \triangleq \{H \mid \delta(f|_H) \leq \delta\} : |\mathcal{H}| \geq \Omega(q^t) \Rightarrow \delta(f) \leq q\delta + O(q^{-t})$.

Restrictions to Hyperplanes :

1. $\delta(f)>0 \implies \exists H$ s.t. $\delta(f|_H) > 0$

2. $\delta(f)>0 \implies \Pr_H\left[\delta(f|_H)>0\right] \geq \frac{1}{q}$

3. $\deg(f) = d+1$ $\left(\Rightarrow \delta(f) \geq q^{-t}\right) \implies \#\{H \mid \deg(f|_H) \leq d\} \leq O(q^{t})$

5. $\mathcal{H}_\delta \triangleq \{H \mid \delta(f|_H) \leq \delta\}$: $|\mathcal{H}| \geq \Omega(q^t) \Rightarrow \delta(f) \leq q\delta + O(q^{-t})$.

Restrictions to Hyperplanes :

1. $\delta(f) > 0 \implies \exists H$ s.t. $\delta(f|_H) > 0$

2. $\delta(f) > 0 \implies \Pr_H\left[\delta(f|_H) > 0\right] \geq \frac{1}{q}$

3. $\deg(f) = d+1 \quad \left(\implies \delta(f) \geq q^{-t}\right) \implies \#\{H \mid \deg(f|_H) \leq d\} \leq O(q^t)$

4. $\mathcal{H} \triangleq \{H \mid \deg(f|_H) \leq d\}$: $|\mathcal{H}| \geq \Omega(q^t) \implies \exists\, g$, $\deg(g) \leq d$
   & $\forall H \in \mathcal{H} \quad f|_H = g|_H$

5. $\mathcal{H}_\delta \triangleq \{H \mid \delta(f|_H) \leq \delta\}$: $|\mathcal{H}| \geq \Omega(q^t) \implies \delta(f) \leq q\delta + O(q^{-t})$.

(1) $\delta(f)>0 \implies \exists H$ s.t. $\delta(f|_H)>0$

$\Downarrow$

(2) $\delta(f)>0 \implies \Pr_H\left[\delta(f|_H)>0\right] \geq \frac{1}{q}$

Proof: a.w.l.o.g. $H = \{X_1 = \sum_{i>1} \alpha_i X_i\}$

let $g(\alpha_2 \ldots \alpha_n, X_2 \ldots X_n) = f(\sum \alpha_i X_i, X_2 \ldots X_n)$;

(1) $\Rightarrow$ $\exists$ monomial of deg $> d$ in $X_2 \ldots X_n$ in g whose coeff. is non-zero

But this coeff. is a poly of deg $q-1$ in $\alpha_2 \ldots \alpha_n$

$\boxtimes$

☆ 3 $\deg(f) = d+1$ $\left(\Rightarrow \delta(f) \geq q^{-t}\right) \Rightarrow \#\{H \mid \deg(f|_H) \leq d\} \leq O(q^t)$

$q=2$: Say $|\mathcal{H}| \geq 2^{d+2}$

- w.l.o.g. $\mathcal{H}$ contains $d+2$ linearly ind. hyperplanes.
- w.l.o.g. they are $X_1 = 0$, $X_2 = 0$, $\ldots$ $X_{d+2} = 0$
- Write $f = \ell + h$ $\deg(\ell) \leq d$; every monomial in h of deg $d+1$
- $\deg(f|_{x_i=0}) \leq d \Rightarrow x_i \mid h \Rightarrow \prod_{i=1}^{d+2} x_i \mid h$ $\boxtimes$

Proof of 3 : General q

Main Ideas: • Reduce "degree reduction" problem to "polynomial vanishing" problem

• Work with "monomials" in $1, X, X^2, \ldots X^{q-2}, X^{q-1} - 1$ non-standard.

• Simple but useful lemma:

deg d non-zero poly vanishes on at most $q^{d/q-1}$ hyperplanes.

Proof of 4 :

4 $\mathcal{H} \doteq \{H \mid \deg(f|_H) \le d\}$: $|\mathcal{H}| \ge \Omega(q^t) \Rightarrow \exists\, g$, $\deg(g) \le d$

& $\forall\, H \in \mathcal{H}$ $\quad f|_H = g|_H$

$q=2$

- As in proof of 3 , assume $X_1=0,\ X_2=0 \ldots X_{d+2}=0 \in \mathcal{H}$.
- What does nearby poly g look like?

$g|_{X_i=0} \equiv f|_{X_i=0}$; so every monomial visible in some restriction . . .

. . . $\boxtimes$

General q

- Quite hairy ...
- More induction using 2 for inductive step
- Base case uses "density Hales Jewett theorem"
  (dense set of pts has line in it)
- $\epsilon_q = \frac{1}{\text{ackerman}(q)}$ 

☆ 4 $\mathcal{H} \triangleq \{H \mid \deg(f|_H) \leq d\}$: $|\mathcal{H}| \geq \Omega(q^t) \Rightarrow \exists\, g$, $\deg(g) \leq d$

& $\forall\, H \in \mathcal{H}$ $\quad f|_H = g|_H$

$\Downarrow$

5 $\mathcal{H}_\delta \triangleq \{H \mid \delta(f|_H) \leq \delta\}$: $|\mathcal{H}| \geq \Omega(q^t) \Rightarrow \delta(f) \leq 9\delta + O(q^{-t})$.

$\xrightarrow{\quad\quad\quad} \!\!\!\!\!\not\quad \longrightarrow$

Straightforward counting with Chebychev.

Conclusions

- Even most basic "testing" problem not well understood
- What should ϵ_q really look like
- Independent of q? inverse-poly(q)? exponential?
- Can we test any single-orbit property this fast?

THANK YOU!