Note Title 2/2/2012

Invariance in Property Testing

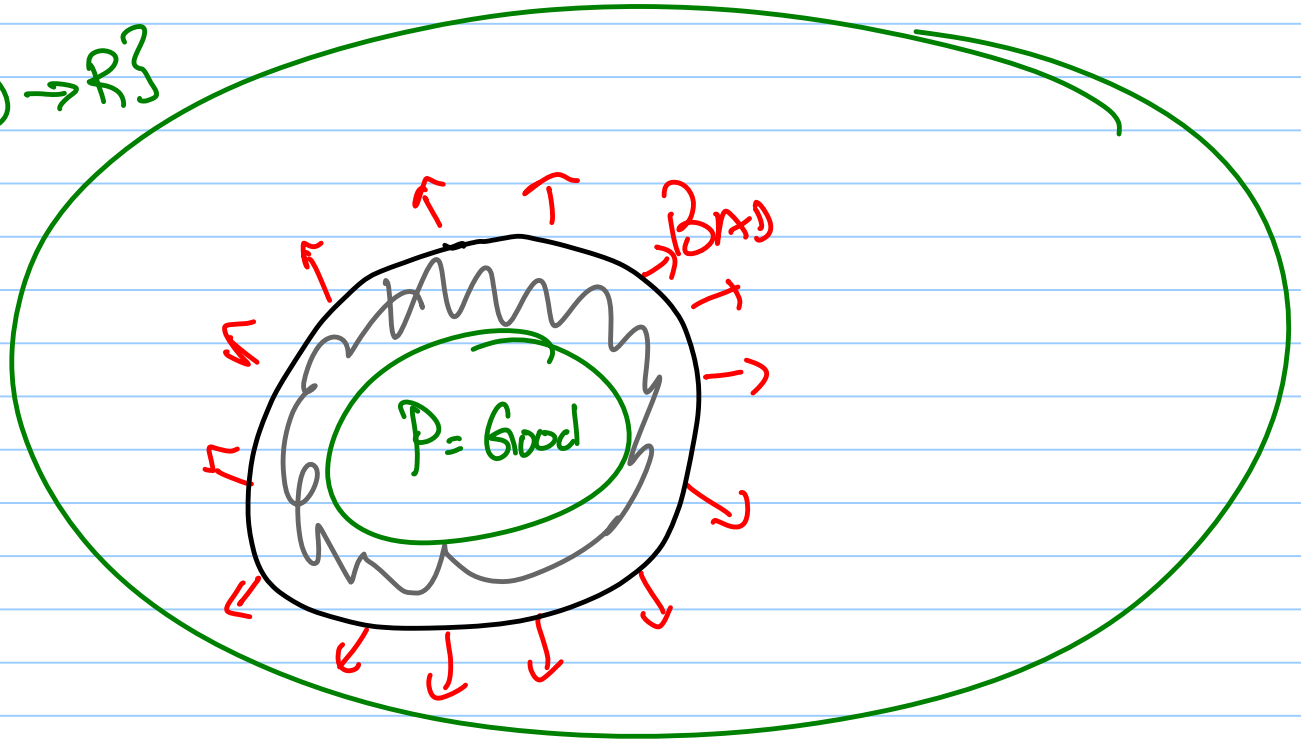
Madhu Sudan
(MSR)

Based on works of/with: Ben-Sasson, Grigorescu, Guo, Kaufman, Kopparty, Lovett, Matoušek, Shpilka.

Agenda

1. Property Testing?
2. Invariance?
3. Affine-Invariance
   - New Properties
   - Analysis of Tests.

Property testing



Given $f: D \to R$

is $f \in P$?

Or ϵ-far from P?

Goal: Answer with few queries to f.

Example 1: MAJORITY

$f : \{1, \ldots n\} \to \{0,1\}$; Binary votes

$P = \{ f \mid \sum_{i \in [n]} f(i) > \frac{n}{2} \}$; Majority = 1

"Chernoff bounds" $\Rightarrow$ Can be tested with $O(1/\epsilon^2)$ queries

Example 2: "Linearity" [BLR '90]

- $f : \mathbb{F}_2^n \to \mathbb{F}_2$ ($\mathbb{F}_2$ = binary field)
- $P = \{f \mid \forall x, y \quad f(x) + f(y) = f(x+y)\}$
- Test [Blum, Luby, Rubinfeld]: Test above for random independent x, y
- Analysis: Non-trivial!

Property Testing : 1990-2013

- Algebraic Properties : Is $f: \mathbb{F}_2^n \to \mathbb{F}_2$ of degree $\leq d$?
- Graph Properties : Is G 2-colorable ?
- Statistical Property : Does $f: D \to R$ have entropy $\geq \frac{1}{2} \log |R|$?
- Matrix Property : Does $M: [n] \times [m] \to \mathbb{F}$ have rank $\leq R$?

Property Testing Techniques

- Each area brings its own techniques
- Little unification.
- Why?
- "Properties / Testing influenced by Invariance"

INVARIANCE ?

- $\pi : D \to D$ permutation.

P invariant under π if $\forall f \in P \quad f \circ \pi \in P$

Invariance class $(P) = \{ \pi \mid P$ invariant under $\pi \}$

- Examples: Invariance (Majority) $= S_n$

Invariance (Linearity) = Linear Transforms on $\mathbb{F}_2^n$

Why Invariance?

Constraint: Sequence of domain elements $\alpha_1 \dots \alpha_k \in D$

Set of legitimate value $S \subseteq R^k$

Tester: Roughly: a collection of Constraints ...

But we need many (covering all of D)

Invariance + 1 Constraint $\Rightarrow$ Many Constraints

$\alpha_1 \dots \alpha_k \Rightarrow \pi(\alpha_1), \dots \pi(\alpha_k)$

$S \Rightarrow S$

Invariance of familiar subareas

- Graph Property Testing: Invariant under vertex renaming
- Statistical properties: Invariant under all permutations
- Boolean properties: Domain $= \{0,1\}^n$
  Invariant under S_n
- Algebraic properties: Domain $= \mathbb{F}_q^n$;
  Invariant under affine transformations

Does Invariance Help?

- Obviously for "statistical" properties (Invariance = S_n)
- By defn. for "graph" properties
- Other classes? Till 2007 ... unknown ...

Theorem: [Kaufman + S. 2008]:

if $\mathcal{P} \subseteq \{\mathbb{F}_2^n \to \mathbb{F}_2\}$ is linear and k-single-orbit

then $\mathcal{P}$ is k-locally-testable

k-single-orbit: $\mathcal{P}$ defined by k-local-constraint + invariance.

$\mathcal{P}$ defined by $\alpha_1 \dots \alpha_k \in \mathbb{F}_2^n$; $S \subseteq \mathbb{F}_2^k$; S subspace

$$\mathcal{P} = \{ f \mid (f(\gamma\cdot\alpha_1 + \delta), f(\gamma\cdot\alpha_2 + \delta) \dots f(\gamma\cdot\alpha_k + \delta)) \in S, \ \forall \gamma, \delta \in \mathbb{F}_2^n \}$$

Main Lemma:

[Linearity]

$$\epsilon(f) \triangleq \Pr_{x,y}\left[f(x)+f(y) \neq f(x+y)\right]$$

$$\delta(f) \triangleq \min_{g \text{ linear}} \left\{ \Pr_{x}\left[f(x) \neq g(x)\right] \right\}$$

$$\epsilon(f) < \frac{2}{9} \Rightarrow \delta(f) \leq 2\epsilon(f)$$

Main Lemma:

[Linearity]

$$\epsilon(f) \triangleq \Pr_{x,y}\left[f(x)+f(y) \neq f(x+y)\right]$$

$$\delta(f) \triangleq \min_{g \text{ linear}} \left\{ \Pr_{x}\left[f(x) \neq g(x)\right] \right\}$$

$$\epsilon(f) < \frac{2}{9} \Rightarrow \delta(f) \leq 2\epsilon(f)$$

[Single-orbit]

$$\epsilon(f) \triangleq \Pr_{r,\delta}\left[(f(r\alpha_1+\delta), \ldots f(r\alpha_k+\delta)) \notin S\right]$$

$$\delta(f) \triangleq \min_{g \in P} \left\{ \Pr_{x}\left[f(x) \neq g(x)\right]\right\}$$

$$\epsilon(f) < O\left(\frac{1}{k^2}\right) \Rightarrow \delta(f) \leq 2\epsilon(f)$$

Linearity Analysis

- $\text{Vote}_y(x) \triangleq f(x+y) - f(y)$
- $g(x) \triangleq \underset{\beta}{\text{argmax}} \left\{ \Pr_y \left[\text{Vote}_y(x) = \beta \right] \right\}$
- **Step 1:** $\Pr_x \left[f(x) \neq g(x) \right] \leq 2\epsilon(f)$
- **Step 2:** $\forall x \quad \Pr_{y,z} \left[\text{Vote}_y(x) \neq \text{Vote}_z(x) \right] \leq 2\epsilon$
- **Step 3:** $\forall x, y$ (assuming $\epsilon < 1/6$)

  $g(x) + g(y) = g(x+y)$

Affine-Inv. Analysis

Linearity Analysis

- $\text{Vote}_y(x) \triangleq f(x+y) - f(y)$
- $g(x) \triangleq \underset{\beta}{\text{argmax}} \left\{ \Pr_y \left[\text{Vote}_y(x) = \beta \right] \right\}$
- **Step 1:** $\Pr_x \left[f(x) \neq g(x) \right] \leq 2\epsilon(f)$
- **Step 2:** $\forall x \quad \Pr_{y,z} \left[\text{Vote}_y(x) \neq \text{Vote}_z(x) \right] \leq 2\epsilon$
- **Step 3:** $\forall x, y$ (assuming $\epsilon < 1/6$)

  $g(x) + g(y) = g(x+y)$

Affine-Inv. Analysis

Vote ?

Fix affine A s.t. $A(\alpha_1) = x$

$\text{Vote}_A(x) \triangleq \beta$ s.t.

$\left(\beta, f(A(\alpha_2)), \ldots f(A(\alpha_k)) \right) \in S$

(if such β exists)

Linearity Analysis

- $\text{Vote}_y(x) \triangleq f(x+y) - f(y)$
- $g(x) \triangleq \underset{\beta}{\text{argmax}} \{\Pr_y[\text{Vote}_y(x) = \beta]\}$
- **Step 1:** $\Pr_x[f(x) \neq g(x)] \leq 2\epsilon(f)$
- **Step 2:** $\forall x \ \Pr_{y,z}[\text{Vote}_y(x) \neq \text{Vote}_z(x)] \leq 2\epsilon$
- **Step 3:** $\forall x, y$ (assuming $\epsilon < 1/6$)

  $g(x) + g(y) = g(x+y)$

Affine-Inv. Analysis

- Definition extends naturally
- Same
- Same averaging
- ? Key step !!
- Similar to Step 2.

Step 2 Magic (Linearity)

?	$f(y)$	$-f(x+y)$
$f(z)$		
$-f(x+z)$		

Want ? s.t. first row & first column sum to zero.

Step 2 Magic (Linearity)

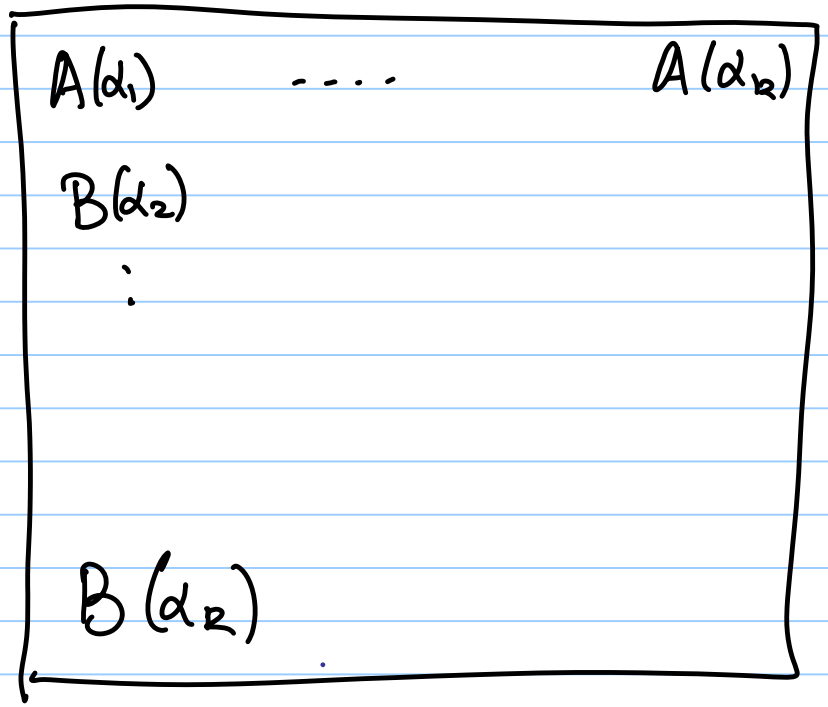
?	$f(y)$	$-f(x+y)$
$f(z)$	0	$-f(z)$
$-f(x+z)$	$-f(y)$	$f(x+y+z)$

Step 2 Magic (Linearity)

?	$f(y)$	$-f(x+y)$
$f(z)$	0	$-f(z)$
$-f(x+z)$	$-f(y)$	$f(x+y+z)$

- 2^{nd} row & column always sum to zero.
- 3^{rd} row & column "usually" sum to zero

Abstracting: Given affine A & B s.t. $A(\alpha_1) = B(\alpha_1) = X$



Want $A_1 \dots A_k$; $A_1 = A$

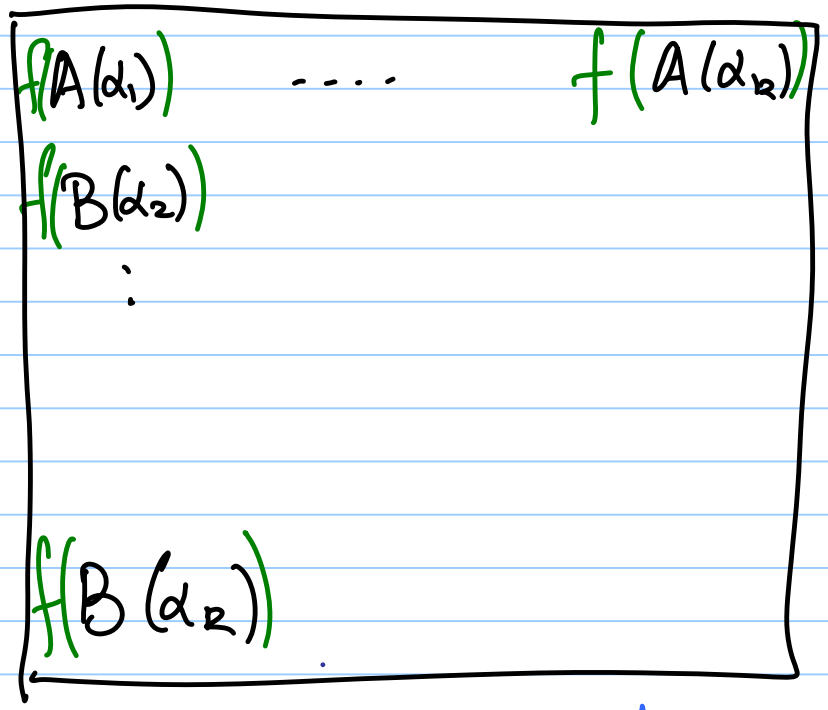
$B_1 \dots B_k$; $B_1 = B$

s.t. $\forall i, j$

$$A_i(\alpha_j) = B_j(\alpha_i)$$

Idea: Pick $A_2(\alpha_2)$ randomly: $\exists!$ way to fill rest of matrix (linear algebra!)

Abstracting: Given affine A & B s.t. $A(\alpha_1) = B(\alpha_1) = X$



$\exists$ $A_1 \dots A_k$; $A_1 = A$

$B_1 \dots B_k$; $B_1 = B$

s.t. $\forall i, j$

$$A_i(\alpha_j) = B_j(\alpha_i)$$

- whp. f-(matrix) s.t. all rows / columns except first $\in S$
- S subspace $\Rightarrow$ first row can be filled consistently.

Linearity Analysis

- $\text{Vote}_y(x) \triangleq f(x+y) - f(y)$
- $g(x) \triangleq \underset{\beta}{\text{argmax}} \left\{ \Pr_y \left[\text{Vote}_y(x) = \beta \right] \right\}$
- **Step 1:** $\Pr_x \left[f(x) \neq g(x) \right] \leq 2\epsilon(f)$
- **Step 2:** $\forall x \quad \Pr_{y,z} \left[\text{Vote}_y(x) \neq \text{Vote}_z(x) \right] \leq 2\epsilon$
- **Step 3:** $\forall x, y$ (assuming $\epsilon < 1/6$)

  $g(x) + g(y) = g(x+y)$

Affine-Inv. Analysis

→ Definition extends naturally

→ Same

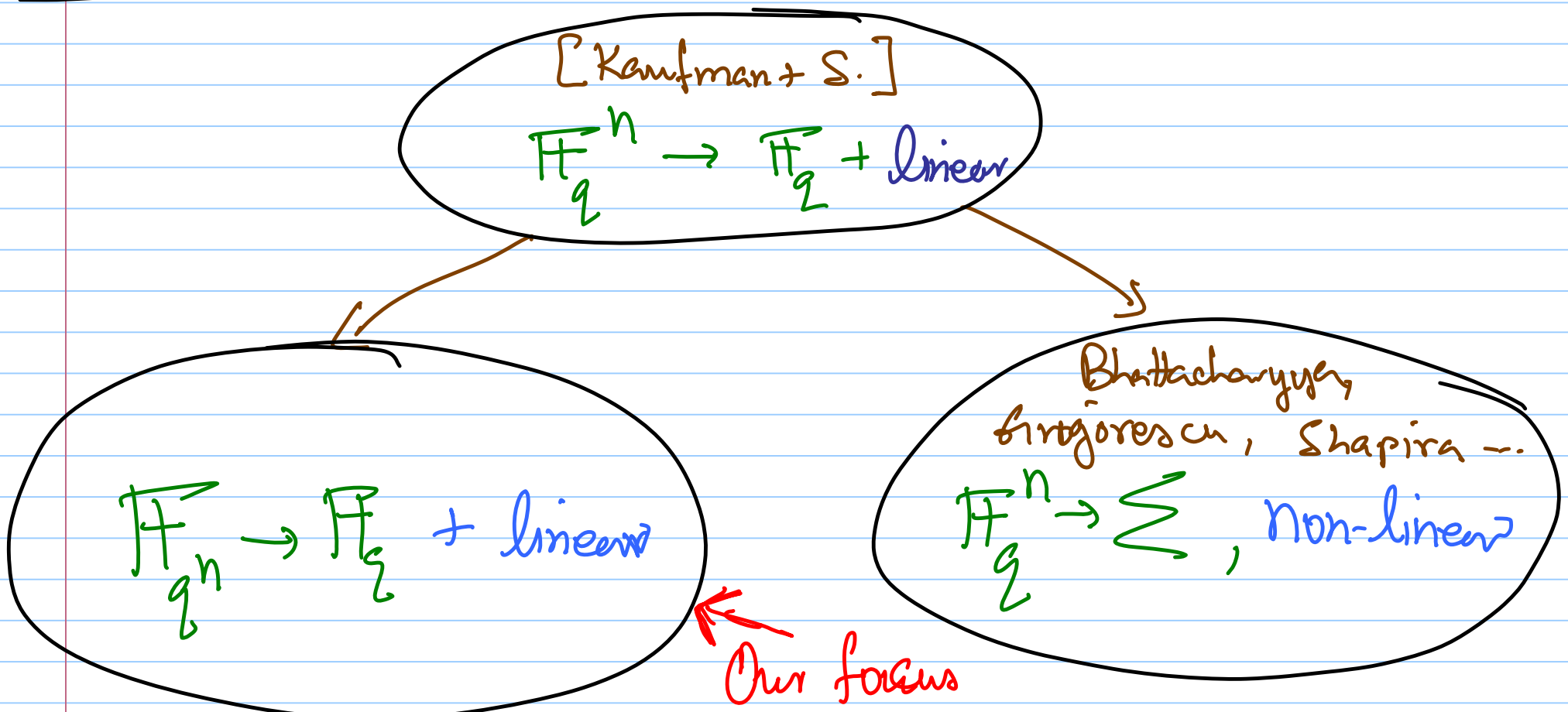
→ Same averaging

→ ? Key step !! ☑

→ Similar to Step 2.

☒

Affine Invariance



Main Findings

(1) Symmetries + local constraints / characterizations insufficient
- violates conjecture of [Alon, Kaufman, Krivelevich, Litsyn, Ron]
[Grigorescu, Kaufman, S.], [Ben-Sasson, Maatouk, Shpilka, S.]

(2) Structure of affine-invariant properties (mostly known / rediscovered)
- spanned by Traces of Monomials.

(3) Basic Testable Properties
- "low weight Polynomials"
- Sparse families

Main Findings - 2

(4) Composition: P_1, P_2 locally listable

$\Rightarrow$ $P_1 \cap P_2$ locally testable,

$P_1 + P_2$ locally testable,

"Lift (P_1)" locally testable.

(5) New (Better) Codes via "Lifts"

(6) Nicer (?) Testing of "Lifted" Codes.

Lifting Codes

- Let $\mathbb{F}_Q$ extend $\mathbb{F}_q$
- Let $B \subseteq \{\mathbb{F}_Q^t \to \mathbb{F}_q\}$
- m-dimensional lift $P \subseteq \{\mathbb{F}_Q^m \to \mathbb{F}_q\}$

$$P = Lift_m(B) \triangleq \{f \mid f|_A \in B \ \forall\ t\text{-dim affine subspace } A\}$$

- Natural concept; natural way to think about low-degree polynomials; leads to most tests.

Lifting Characterization of low-degree polynomials

Lemma: p-prime $\Rightarrow$ $f: \mathbb{F}_p^m \to \mathbb{F}_p$ has degree $\leq d$

$\Leftrightarrow$ $\deg(f|_A) \leq d$ $\forall \left\lceil \frac{d+1}{p-1} \right\rceil$-dim. A

Lemma': q of characteristic p $\Rightarrow$ $f: \mathbb{F}_q^m \to \mathbb{F}_q$ has deg. $\leq d$

$\Leftrightarrow$ $\deg(f|_A) \leq d$ $\forall t$-dim A for $t = \left\lceil \frac{d+1}{q - \frac{q}{p}} \right\rceil$

low-deg testing harder for non-prime fields

Lifting Characterization of low-degree polynomials

Lemma: p-prime $\Rightarrow$ $f: \mathbb{F}_p^m \to \mathbb{F}_p$ has degree $\leq d$

$\Leftrightarrow$ $\deg(f|_A) \leq d$ $\forall \left\lceil \frac{d+1}{p-1} \right\rceil$-dim. A

Lemma': q of characteristic p $\Rightarrow$ $f: \mathbb{F}_q^m \to \mathbb{F}_q$ has deg. $\leq d$

$\Leftrightarrow$ $\deg(f|_A) \leq d$ $\forall t$-dim A for $t = \left\lceil \frac{d+1}{q - \frac{q}{p}} \right\rceil$

low-deg testing harder for non-prime fields

"lifted" codes better on non-prime fields.

New Codes from Lifting [Guo, Kopparty, S.]

Theorem: $\forall\, \alpha, \beta > 0$ $\exists\, \delta > 0$ s.t. $\forall N$ $\exists$ codes of length N, distance $(1-\delta)N$, dimension $(1-\alpha)N$, that are N^{β}-testable/dec...

Idea: Use $Q = q = N^{\beta}$; $t = 1$; $m = \frac{1}{\beta}$; Lift (deg $(1-\delta)q$ poly)

- leads to first LTCs of rate $\to 1$;
- leads to new lower bounds for "Nikodym" sets.
- Violates conjecture of [Gruth].

Conclusions

- Affine Inv. codes have nice "locality" properties
- Dominate low-deg. multiv. polynomials, with no loss in performance
- Deserve full understanding.

Questions

- Characterize $\Theta_q(1)$-testable $P \subseteq \{F_{q^n} \to F_q\}$.
- Beat low-deg. poly in polylog N-query range. (for codes of length N).

Thank You!