

Testing Affine-Invariant Properties

Madhu Sudan
Microsoft

Surveys: works with/of Eli Ben-Sasson, Elena Grigorescu, Tali Kaufman, Shachar Lovett, Ghid Maatouk, Amir Shpilka.

Property Testing

- ... of functions from D to R :
 - Property $P \subseteq \{D \rightarrow R\}$
- Distance
 - $\delta(f,g) = \Pr_{x \in D} [f(x) \neq g(x)]$
 - $\delta(f,P) = \min_{g \in P} [\delta(f,g)]$
 - f is ϵ -close to g ($f \approx_{\epsilon} g$) iff $\delta(f,g) \leq \epsilon$.
- Local testability:
 - P is (k, ϵ, δ) -locally testable if $\exists$ k -query test T
 - $f \in P \Rightarrow T^f$ accepts w.p. $1-\epsilon$.
 - $\delta(f,P) > \delta \Rightarrow T^f$ accepts w.p. ϵ .
- Notes: want $k(\epsilon, \delta) = O(1)$ for $\epsilon, \delta = \Omega(1)$.

Classical Property Test: Linearity [BLR]

- Does $f(x+y) = f(x) + f(y)$, for all x, y ?
- Variation (Affineness):
 - Is $f(x+y) + f(0) = f(x) + f(y)$, for all x, y ?
 - (roughly $f(x) = a_0 + \sum_{i=1}^n a_i x_i$)
- Test: Pick random x, y and verify above.
- Obvious: f affine $\Rightarrow$ passes test w.p. 1.
- BLR Theorem: If f is δ -far from every affine function, then it fails test w.p. $\Omega(\delta)$.
- Ultimate goal of talk: To understand such testing results.

Affine-Invariant Properties

- Domain = $K = \text{GF}(q^n)$ (field with q^n elements)
- Range = $\text{GF}(q)$; $q = \text{power of prime } p$.
- P forms F -vector space.
- P invariant under affine transformations of domain.
 - Affine transforms? $x \mapsto a.x + b$, $a \in K^*$, $b \in K$.
 - Invariance? $f \in P \Rightarrow g_{a,b}(x) = f(ax+b) \in P$.
 - “affine permutation of domain leaves P unchanged”.
- Quest: What makes affine-invariant property testable?

(My) Goals

- Why?
 - BLR test has been very useful (in PCPs, LTCs).
 - Other derivatives equally so (low-degree test).
 - Proof magical! Why did 3 (4) queries suffice?
 - Can we find other useful properties?
- Program:
 - Understand the proof better (using invariance).
 - Get structural understanding of affine-invariant properties, visavis local testability.
 - Get better codes/proofs?

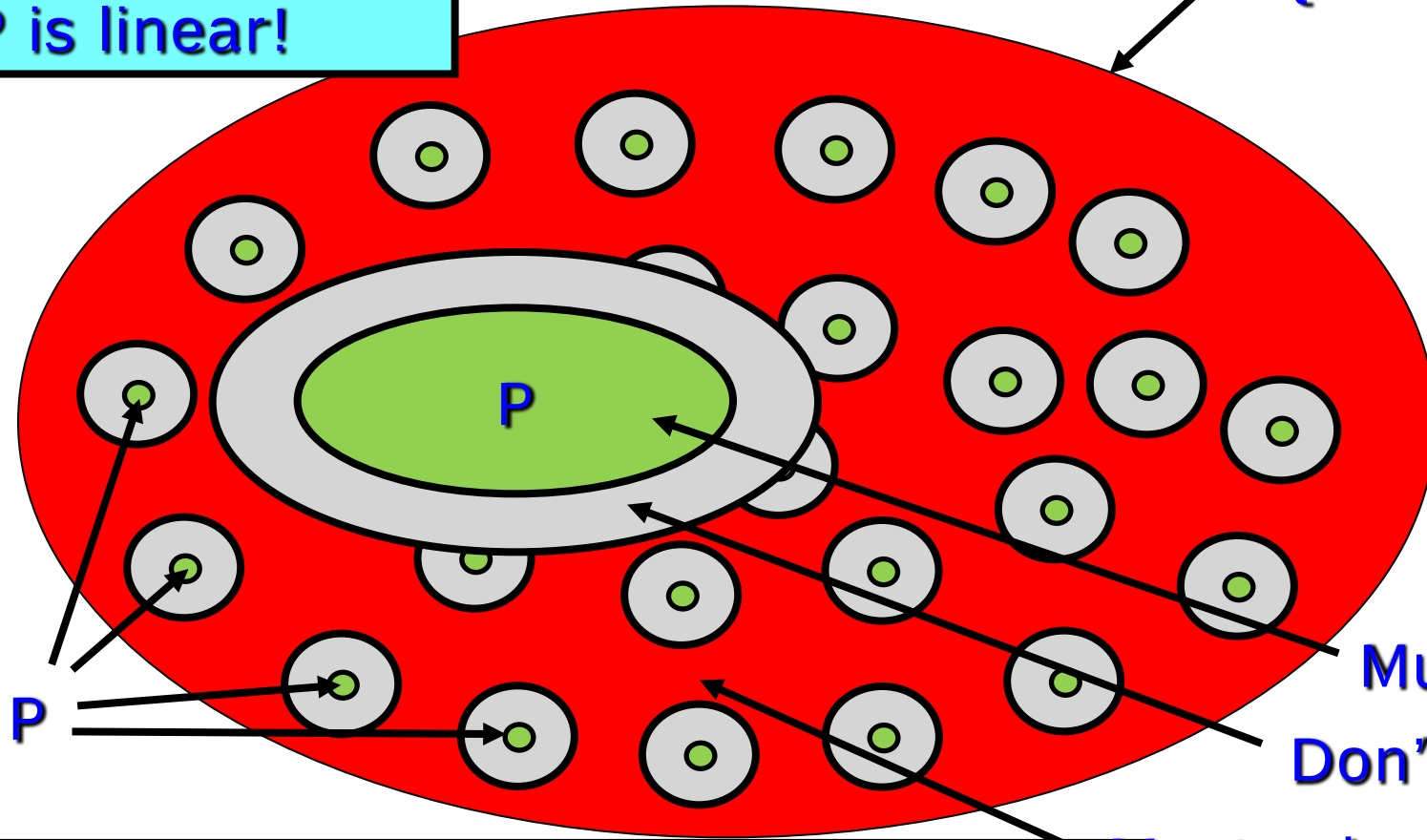
Why's?

- Why Invariance
 - Natural way to abstract/unify common themes (in property testing).
 - Graph properties, Boolean, Statistical etc.?
- Why affine-invariance:
 - Abstracts linearity (affine-ness) testing.
 - Low-degree testing
 - BCH testing ...
- Why F-vector space?
 - Easier to study (gives nice structure).
 - Common feature (in above + in codes).

Contrast w. Combinatorial P.T.

R is a field F;
P is linear!

Universe:
 $\{f: D \rightarrow R\}$



Must accept

Don't care

Must reject

Algebraic Property = Code! (usually)

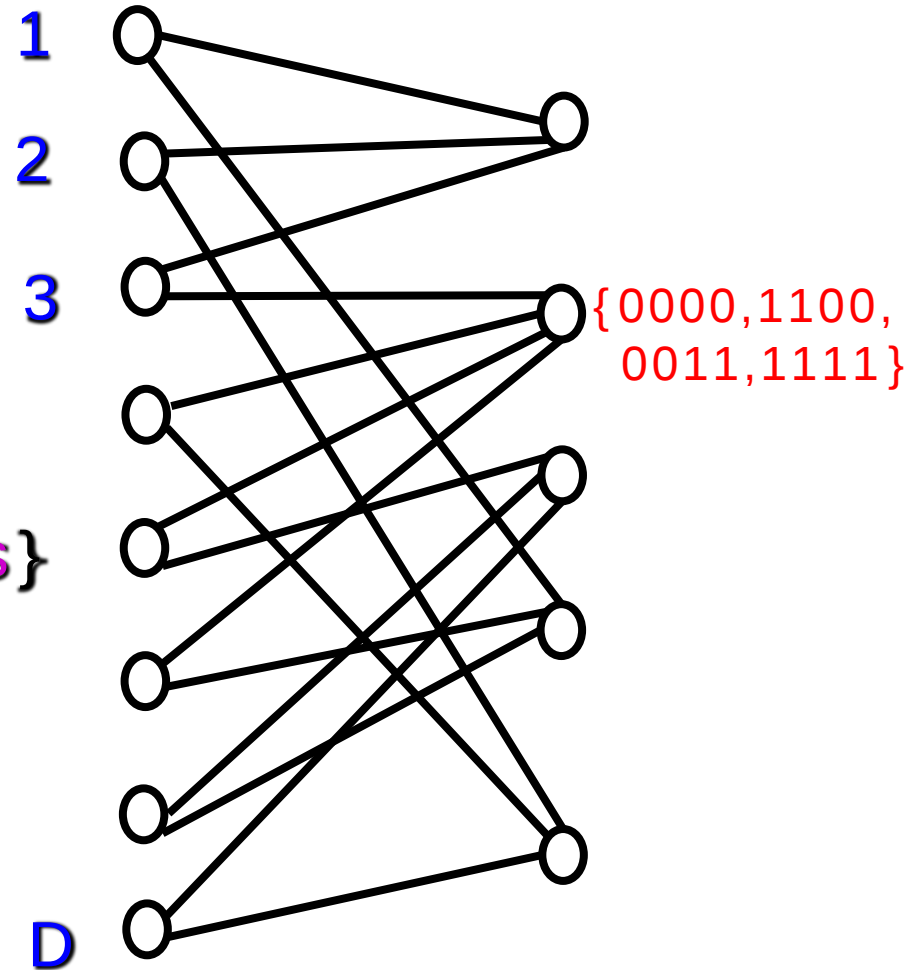
Bertinoro: Testing Affine-Invariant
Properties

Basic Implications of Linearity [BHR]

- If P is linear, then:
 - Tester can be made non-adaptive.
 - Tester makes one-sided error
 - ($f \in P \Rightarrow$ tester always accepts).
- Motivates:
 - Constraints:
 - k -query test $\Rightarrow$ constraint of size k :
 - value of f at $\alpha_1, \dots, \alpha_k$ constrained to lie in subspace.
 - Characterizations:
 - If non-members of P rejected with positive probability, then P characterized by local constraints.
 - functions satisfying all constraints are members of P .

Pictorially

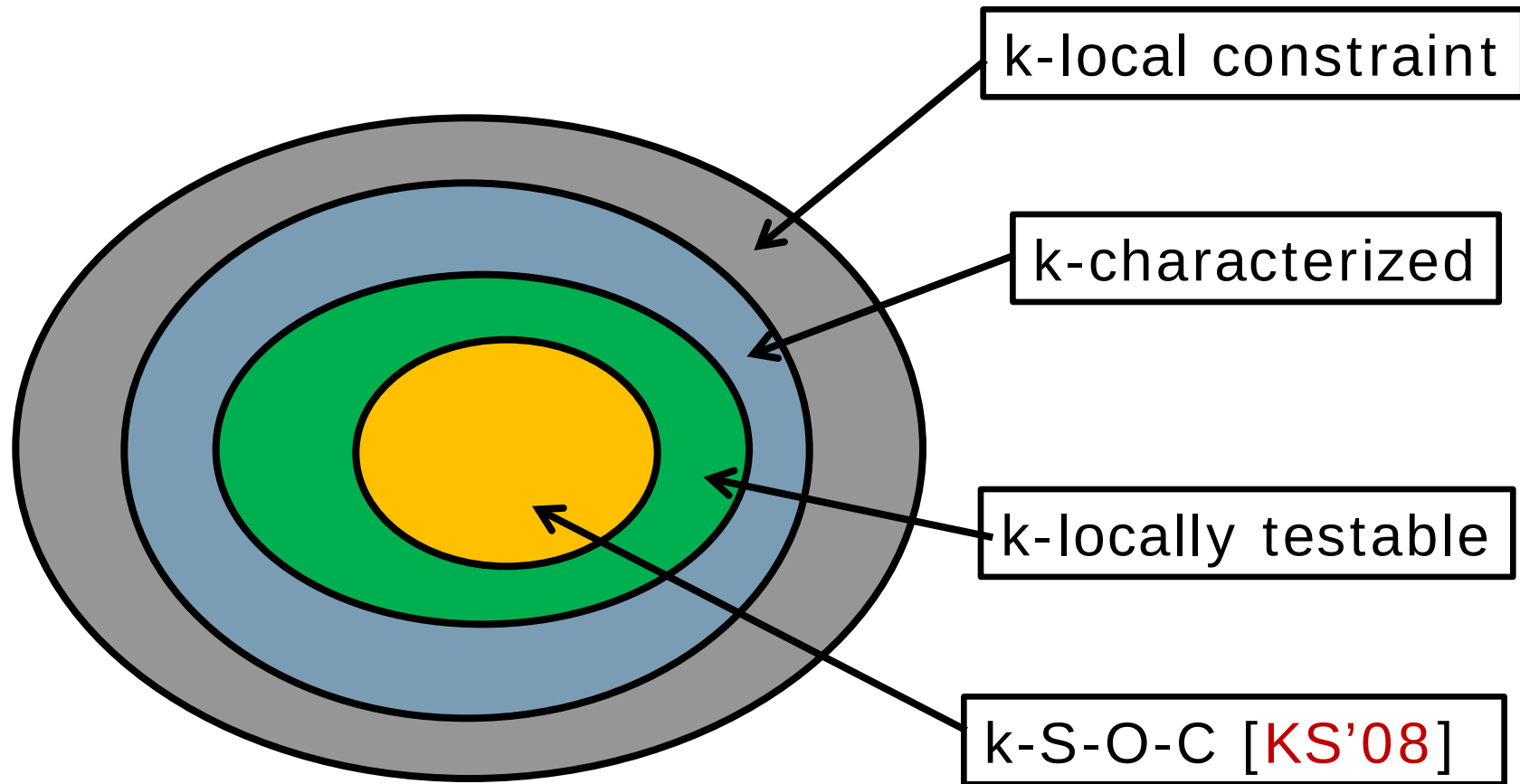
- f = assgm't to left
- Right = constraints
- Characterization of P :
 $P = \{f \text{ sat. all constraints}\}$



Back to affine-invariance: More Notes

- Why $K \rightarrow F$?
 - Very few permutations ($|K|^2$) !!
 - Still “2-transitive”
 - Includes all properties from F^n to F that are affine-invariant over F^n .
 - (Hope: Maybe find a new range of parameters?)
- Contrast with “linear-invariance” [Bhattacharyya et al.]
 - Linear vs. Affine.
 - Arbitrary P vs. F -vector space P
 - Linear over F^n vs. Affine over $K = GF(q^n)$.

Affine-invariance & testability



Goal of this talk

- Definition: Single-orbit-characterization (S-O-C)
- Known testable affine-invariant properties
(all S-O-C!).
- Structure of Affine-invariant properties.
- Non testability results
- Open questions

Single-orbit-characterization (S-O-C)

- Many common properties are given by
 - (Affine-)invariance
 - Single constraint.
- Example: Affineness over $GF(2)^n$:
 - Affineness is affine-invariant.
 - $f(000000) - f(100000) \neq f(010000) - f(110000)$
- S-O-C: Abstracts this notion.
 - Suffices for testability [Kaufman+S'08]
 - Unifies all known testability results!!
 - Nice structural properties.

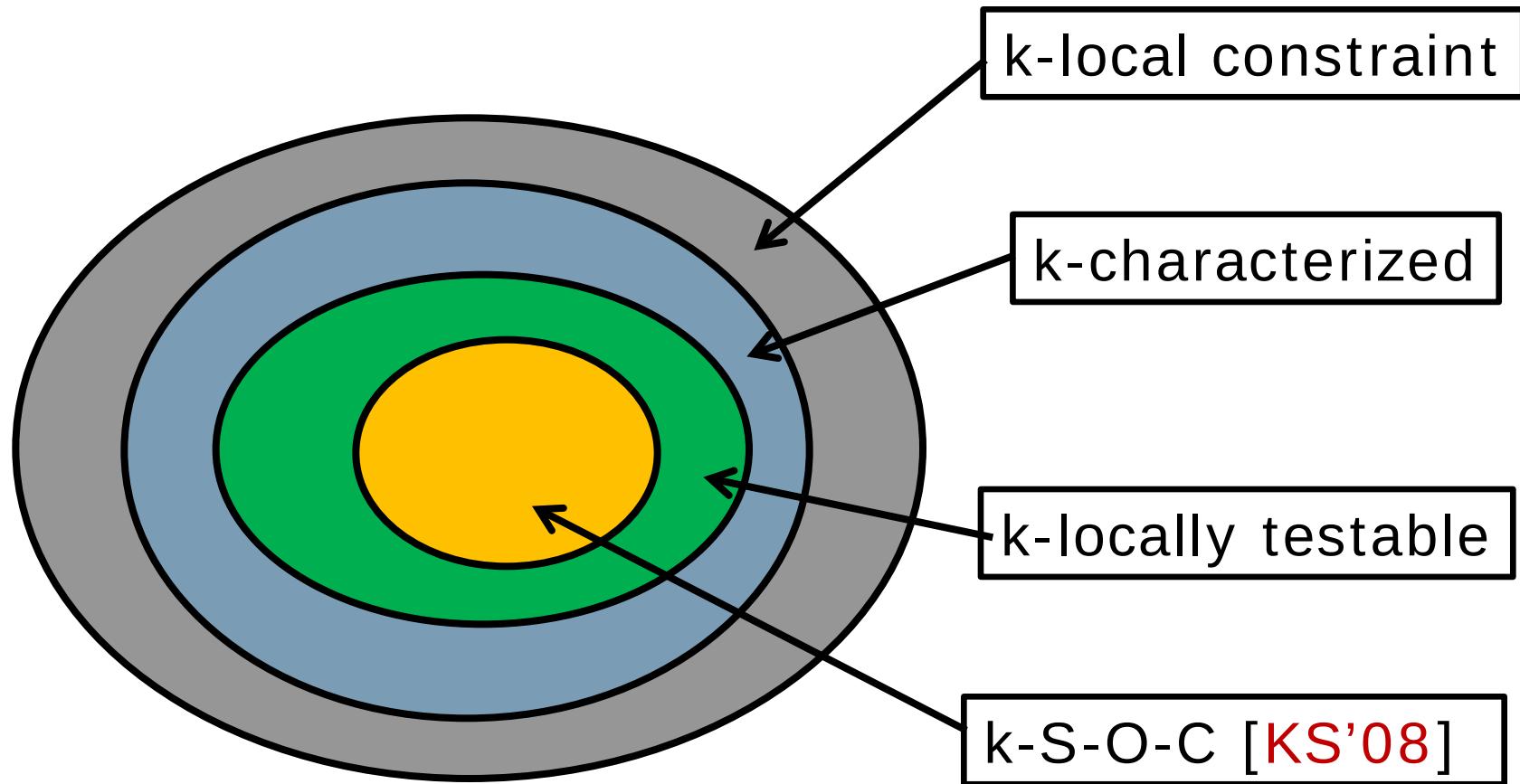
S-O-C: Formal Definition

- Constraint:
 - $C = (\alpha_1, \dots, \alpha_k; V \subseteq F^k); \alpha_i \in K$
 - C satisfied by f if
 - $(f(\alpha_1), \dots, f(\alpha_k)) \in V$.
- Orbit of constraint = $\{C \circ \pi\}_{\pi}, \pi$ affine.
 - $C \circ \pi = (\pi(\alpha_1), \dots, \pi(\alpha_k); V)$.
- P has k -S-O-C, if $\text{orbit}(C)$ characterizes P .

Known testable properties - 0

- Theorem [Kaufman-S.'08]:
 - If P has a k -S-O-C, then P is k -locally testable.

Affine-invariance & testability



Known testable properties - 0

- Theorem [Kaufman-S.'08]:
 - If P has a k -S-O-C, then P is k -locally testable.
- But who has k -S-O-C?
 - Affine functions:
 - over affine transforms of F^n
 - Degree d polynomials:
 - again, over affine transforms of F^n

Known testable properties - 1

- Reed-Muller Property:
 - View domain as F^n (n -variate functions)
 - Parameter d .
 - $RM(d) = n$ -var. polynomials of degree $\leq d$.
- Known to be $q^{O(d/q)}$ -locally testable:
 - Test: Test if f restricted to $O(d/q)$ -dimensional subspace is of degree d .
 - Analysis: [Kaufman-Ron] (see appendix 1).
- Single-Orbit?
 - Yes – naturally over affine transforms of F^n .
 - Yes – unnaturally over K (field of size F^n).

Known testable properties - 2

- Sparse properties:
 - Parameter t
 - $|P| \leq |K|^t$
- Testability:
 - Conditioned on “high-distance” [Kaufman-Litsyn, Kaufman-S.]. (no need for aff. inv.)
 - Unconditionally
 - [Grigorescu, Kaufman, S.], [Kaufman-Lovett] (for prime q).
 - Also S-O-C.

Known Testable Properties - 3

- Intersections:
 - $P_1 \cap P_2$ always locally testable, also S-O-C.
- Sums:
 - $P_1 + P_2 (= \{f_1 + f_2 \mid f_i \in P_i\})$
 - S-O-C iff P_1 and P_2 are S-O-C [BGMSS'11]
- Lifts [BMSS'11]
 - Suppose $F \subseteq L \subseteq K$.
 - $P \subseteq \{L \rightarrow F\}$ has k -S-O-C, with constraint C .
 - Then $\text{Lift}_{\{L \rightarrow K\}}(P) =$ property characterized by $K\text{-orbit}(C)$.
 - By Definition: $\text{Lift}(P)$ is k -S-O-C.

Known Testable Properties - ∞

- Finite combination of Lifts, Intersections, Sums of Sparse and Reed-Muller properties.
 - Known: They are testable (for prime q).
 - Open: Are they the only testable properties?
 - If so, Testability $\equiv$ Single-Orbit.
 - First target: $n = \text{prime}$:
 - no lifts/intersections; only need to show that every testable property is sum of sparse and Reed-Muller property.

Affine-Invariant Properties: Structure

Preliminaries

- Every function from $K \rightarrow K$, including $K \rightarrow F$, is a polynomial in $K[x]$
 - So every property $P = \{\text{set of polynomials}\}$.
 - Is set arbitrary? Any structure?
- Alternate representation:
 - $\text{Tr}(x) = x + x^q + x^{q^2} + \dots + x^{q^{n-1}}$
 - $\text{Tr}(x+y) = \text{Tr}(x) + \text{Tr}(y)$; $\text{Tr}(\alpha x) = \alpha \text{Tr}(x)$, $\alpha \in F$.
 - $\text{Tr}: K \rightarrow F$.
 - Every function from $K \rightarrow F$ is $\text{Tr}(f)$ for some polynomial $f \in K[x]$.
 - Any structure to these polynomials?

Example

- $F = \text{GF}(2)$, $K = \text{GF}(2^n)$.
- Suppose P contains $\text{Tr}(x^{11} + x^3 + 1)$.
- What other functions must P contain (to be affine-invariant)?
- Claims:
 - Let $D = \{0, 1, 3, 5, 9, 11\}$.
 - Then P contains every function of the form $\text{Tr}(f)$, where f is supported on monomials with degrees from D .
 - So $\text{Tr}(x^5), \text{Tr}(\alpha x^9 + \beta x^5), \text{Tr}(x^{11} + x^5 + x^3 + x) + 1 \in P$.
 - How? Why?

Structure - 1

- Definitions:

- $\text{Deg}(P) = \{d \mid \exists f \in P, \text{ with } x^d \in \text{supp}(f)\}$
- $\text{Fam}(D) = \{f: K \rightarrow F \mid \text{supp}(f) \subseteq D\}$

- Proposition: For affine-invariant property P
 $P = \text{Fam}(\text{Deg}(P)).$

Structure - 2

■ Definitions:

- $\text{Shift}(d) = \{d, q.d, q^2.d, \dots\} \bmod (q^n - 1)$.
- D is shift-closed if $\text{Shift}(D) = D$.
- $e \leq d : e = e_0 + e_1 p + \dots;$
 $d = d_0 + d_1 p + \dots;$
 $e \leq d$ if $e_i \leq d_i$ for all i .
- $\text{Shadow}(d) = \{e \leq d\};$
- $\text{Shadow}(D) = \bigcup_{d \in D} \text{Shadow}(d)$.
- D is shadow-closed if $\text{Shadow}(D) = D$.

Structure - 3

- Proposition: For every affine-invariant property P , $\text{Deg}(P)$ is p -shadow-closed and q -shift-closed.
(Shadowing comes from affine-transforms;
Shifts come from range being F).
- Proposition: For every p -shadow-closed, q -shift-closed family D , $\text{Fam}(D)$ is affine-invariant and
$$D = \text{Deg}(\text{Fam}(D))$$

Example revisited

- $\text{Tr}(x^{11} + x^3) \in P$
 - $\text{Deg}(P) \ni 11, 3$ (definition of Deg)
 - $\text{Deg}(P) \ni 11, 9, 5, 3, 1, 0$ (shadow-closure)
 - $\text{Deg}(P) \ni \text{Tr}(x^{11}), \text{Tr}(x^9)$ etc. (shift-closure).
 - $\text{Fam}(\text{Deg}(P)) \ni \text{Tr}(x^{11})$ etc. (definition of Fam).
 - $P \ni \text{Tr}(x^{11})$ ($P = \text{Fam}(\text{Deg}(P))$)

What kind of properties have k -S-O-C?

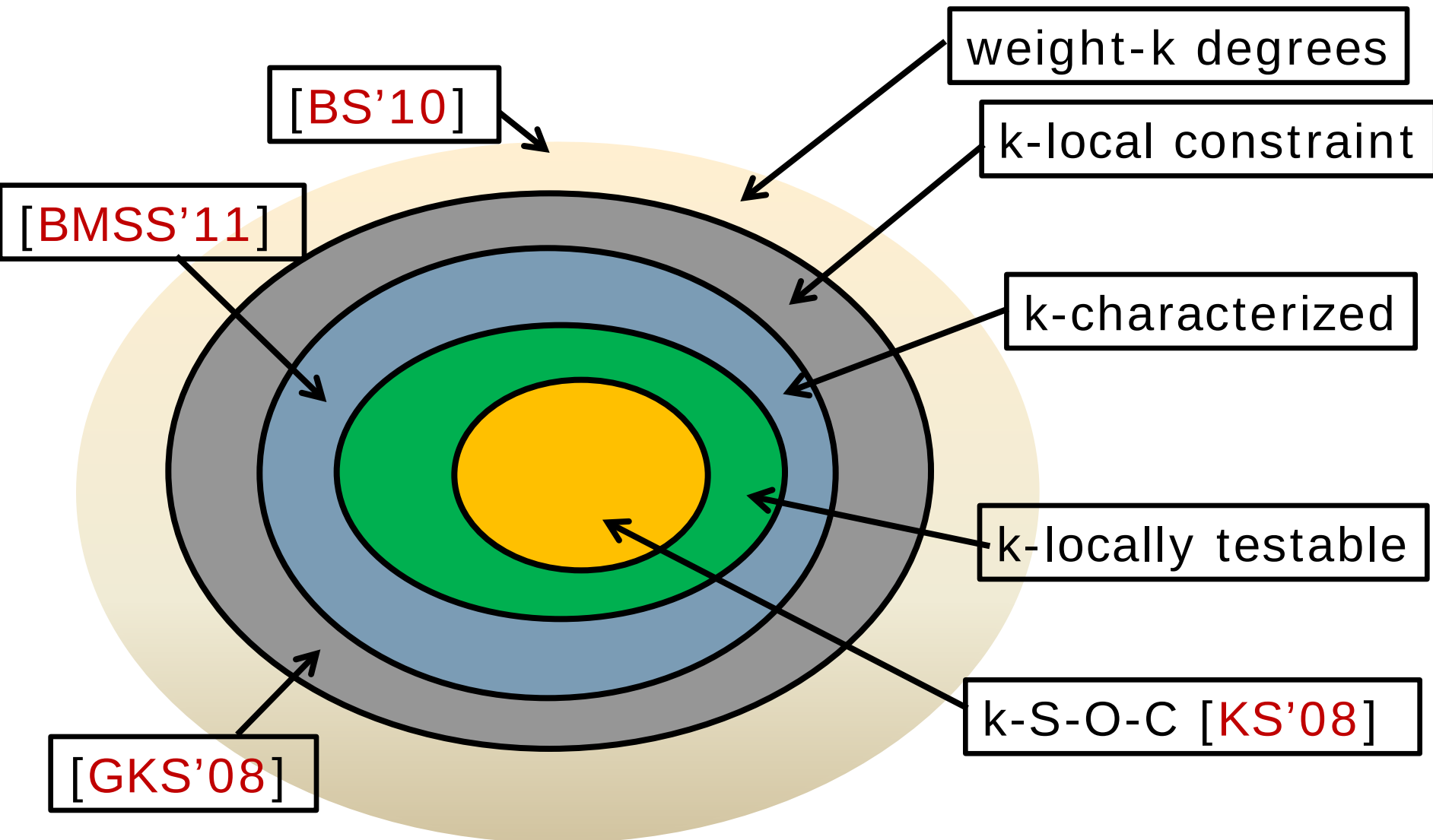
(Positive results interpreted structurally)

- If property has all degrees of q -weight at most k then it is RM and has (q^k) -S-O-C:
 - $q\text{-weight}(d) = \sum_i d_i,$
where $d = d_0 + d_1 q + \dots$
- Also, if $P = \text{Fam}(D)$ & $D = \text{Shift}(S)$ for small shadow-closed S , then P is $k(|S|)$ -S-O-C.
 - (Alternate definition of sparsity.)
- Other examples from Intersection, Sum, Lift.

What affine-invariant properties are not locally testable.

- Very little known.
- Specific examples:
 - **GKS08**: Exists a-i property with k -local constraint which is not k -locally characterized.
 - **BMSS11**: Exists k -locally characterized a-i property that is not testable.
- **BSS'10**: If $\text{wt}(d) \geq k$ for some d in $\text{Deg}(P)$, then P does not have a k -local constraint.

Affine-invariance & testability



Quest in lower bound

- Given degree set D (shadow-closed, shift-closed) prove it has no S-O-C.
- Equivalently: Prove there are no $\lambda_1 \dots \lambda_k \in F, \alpha_1 \dots \alpha_k \in K$ such that
 - $\sum_{i=1}^k \lambda_i \alpha_i^d = 0$ for every $d \in D$.
 - $\sum_{i=1}^k \lambda_i \alpha_i^d \neq 0$ for every minimal $d \notin D$.

Pictorially

$$M(D) = \begin{pmatrix} \alpha_1^d & \alpha_2^d & \dots & \alpha_k^d \end{pmatrix}$$

Is there a vector $(\lambda_1, \dots, \lambda_k)$ in its right kernel?

Can try to prove “NO” by proving matrix has full rank.

Unfortunately, few techniques to prove non-square matrix has high rank.

Non-testable Property - 1

- AKCLR (Alon, Kaufman, Krivelevich, Litsyn, Ron) Conjecture:
 - If a linear property is 2-transitive and has a k -local constraint then it is testable.
 - [GKS'08]: For every k , there exists affine-invariant property with 8-local constraint that is not k -locally testable.
 - $P = \text{Fam}(\text{Shift}(\{0,1\} \cup \{1+2, 1+2^2, \dots, 1+2^k\})).$

Proof (based on [BMSS'11])

- $F = GF(2)$; $K = GF(2^n)$;
- $P_k = \text{Fam}(\text{Shift}(\{0,1\} \cup \{1 + 2^i \mid i \in \{1,\dots,k\}\}))$
- Let $M_i = \begin{pmatrix} \alpha_1^2 & \alpha_2^2 & \dots & \alpha_k^2 \\ \alpha_1^{2^i} & \alpha_2^{2^i} & \dots & \alpha_k^{2^i} \end{pmatrix}$
- If $\text{Ker}(M_i) = \text{Ker}(M_{i+1})$, then $\text{Ker}(M_{i+2}) = \text{Ker}(M_i)$
- $\text{Ker}(M_{k+1}) =$ would accept all functions in P_{k+1}
- So $\text{Ker}(M_i)$ must go down at each step, implying $\text{Rank}(M_{i+1}) > \text{Rank}(M_i)$.

Stronger Counterexample

- GKS counterexample:
 - Takes AKKLR question too literally;
 - Of course, a non-locally-characterizable property can not be locally tested.
- Weaker conjecture:
 - Every k -locally characterized affine-invariant (2 -transitive) property is locally testable.
 - Alas, not true: [BMSS]

[BMSS] CounterExample

- Recall:

- Every known locally characterized property was locally testable
- Every known locally testable property is S-O-C.
- Need a locally characterized property which is (provably) not S-O-C.

- Idea:

- Start with sparse family P_i .
- Lift it to get Q_i (still S-O-C).
- Take intersection of superconstantly many such properties. $Q = \bigcap_i Q_i$

Example: Sums of S-O-C properties

- Suppose $D_1 = \text{Deg}(P_1)$ and $D_2 = \text{Deg}(P_2)$
- Then $\text{Deg}(P_1 + P_2) = D_1 \cup D_2$.
- Suppose S-O-C of P_1 is $C_1: f(a_1) + \dots + f(a_k) = 0$;
and S-O-C of P_2 is $C_2: f(b_1) + \dots + f(b_k) = 0$.
- Then every $g \in P_1 + P_2$ satisfies:
$$\sum_{i,j} g(a_i b_j) = 0$$
- Doesn't yield S-O-C, but applied to random constraints in $\text{orbit}(C_1)$, $\text{orbit}(C_2)$ does!
 - Proof uses $\text{wt}(\text{Deg}(P_1)) \leq k$.

Concluding

- Affine-invariance gives nice umbrella to capture algebraic property testing:
 - Important (historically) for PCPs, LTCs, LDCs.
 - Incorporates symmetry.
- Would be nice to have a complete characterization of testability of affine-invariant properties.
 - Understanding (severely) lacking.
- Know:
 - Can't be much better than Reed-Muller.
 - Can they be slightly better? YES!

Thank You!