Invariance in Property Testing

Madhu Sudan
Microsoft Research

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

Property Testing

- Sublinear time algorithms:
  - Algorithms running in time o(input), o(output).
    - Probabilistic.
    - Correct on (approximation) to input.
    - Input given by oracle, output implicit.
  - Crucial to modern context
    - (Massive data, no time).
- Property testing:
  - Restriction of sublinear time algorithms to decision problems (output = YES/NO).
- Amazing fact: Many non-trivial algorithms exist!

Example 1: Polling

- Is the majority of the population Red/Blue
  - Can find out by random sampling.
  - Sample size $\not\propto$ margin of error
    - Independent of size of population
- Other similar examples: (can estimate other moments …)

Example 2: Linearity

- Can test for homomorphisms:
  - Given: $f: G \rightarrow H$ (G,H finite groups), is f essentially a homomorphism?
  - Test:
    - Pick x,y in G uniformly, ind. at random;
    - Verify f(x) ¢f(y) = f(x ¢y)
  - Completeness: accepts homomorphisms w.p. 1
    - (Obvious)
  - Soundness: Rejects f w.p prob. Proportional to its "distance" (margin) from homomorphisms.
    - (Not obvious, [BlumLubyRubinfeld'90])

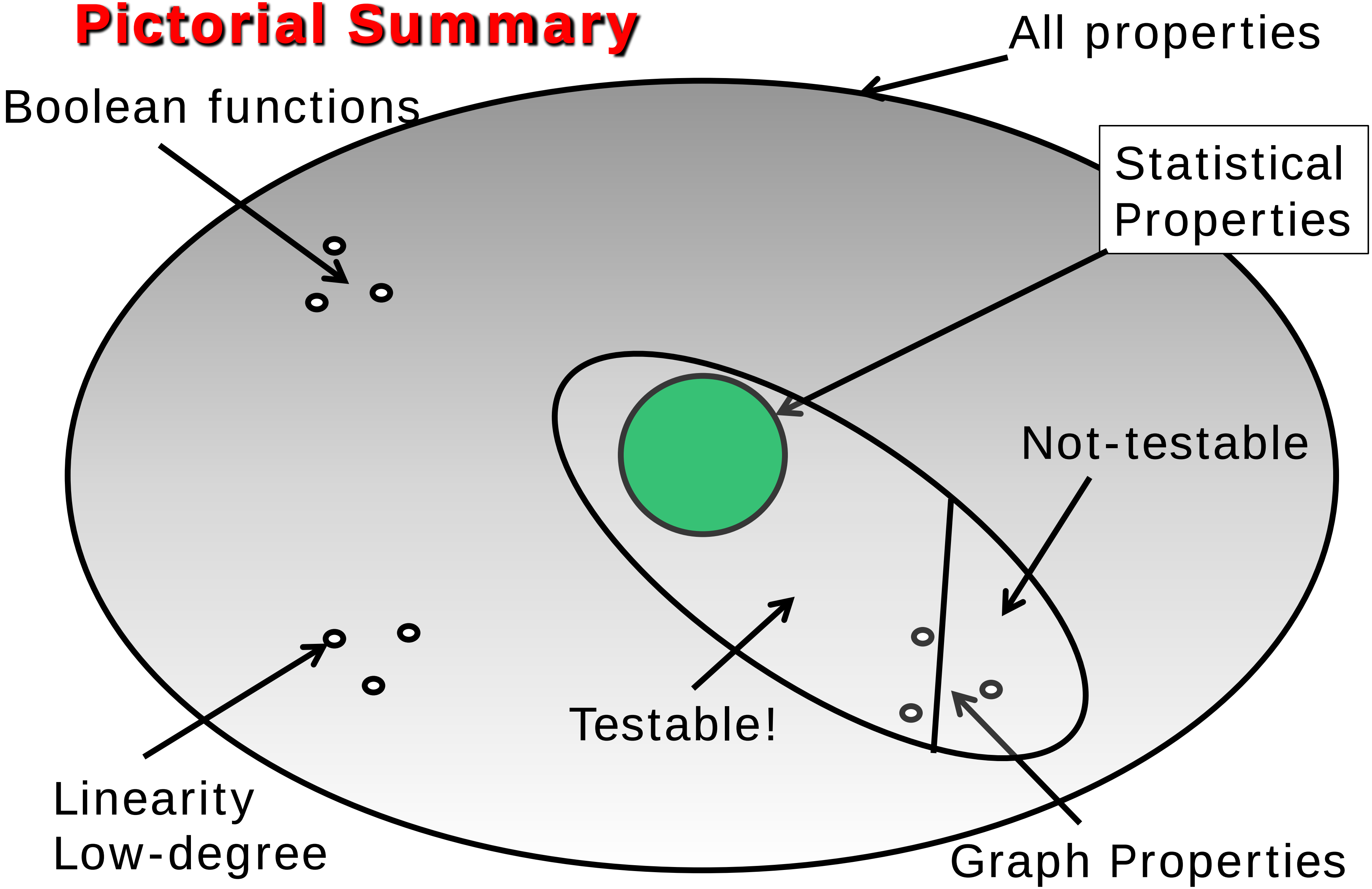
History (slightly abbreviated)

- [Blum,Luby,Rubinfeld – S'90]
  - Linearity + application to program testing
- [Babai,Fortnow,Lund – F'90]
  - Multilinearity + application to PCPs (MIP).
- [Rubinfeld+S.]
  - Low-degree testing; Formal definition.
- [Goldreich,Goldwasser,Ron]
  - Graph property testing; Systematic study.
- Since then … many developments
  - More graph properties, statistical properties, matrix properties, properties of Boolean functions …
  - More algebraic properties

Aside: Story of graph property testing

- Initiated by [GoldreichGoldwasserRon] (dense graphs) and [GoldreichRon] (sparse graphs).
- Focus of intensive research.
- Near classification for dense graphs:
  - Works of Alon, Shapira and others (relate to Szemerdi's regularity lemma)
  - Works of Lovasz, B. Szegedy and others (theory of graph limits).
- Significant progress in sparse graph case also:
  - [Benjamini, Schramm, Shapira]
  - [Nguyen, Onak]

Pictorial Summary



Some (introspective) questions

- What is qualitatively novel about linearity testing relative to classical statistics?
- Why are the mathematical underpinnings of different themes so different?
- Why is there no analog of "graph property testing" (broad class of properties, totally classified wrt testability) in algebraic world?

Invariance?

- Property $P \subseteq \{f : D \to R\}$
- Property P invariant under permutation (function) $\pi : D \to D$, if

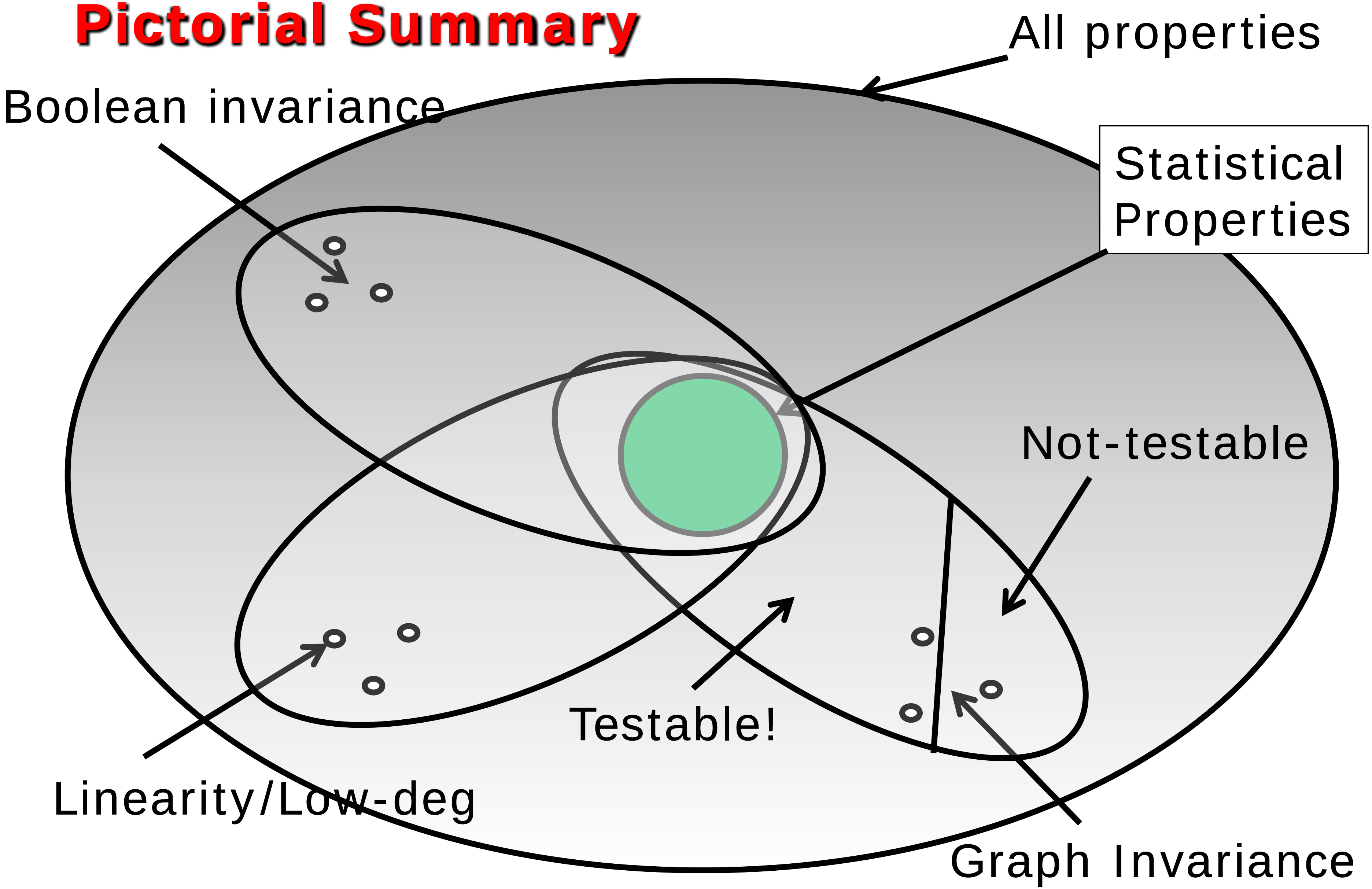
$$f \in P \Rightarrow f \circ \pi \in P$$

- Property P invariant under group G if

  $\forall \pi \in G$, P is invariant under π.

- Observation: Different property tests unified/separated by invariance class.

Pictorial Summary



Invariances (contd.)

- Some examples:
  - Classical statistics: Invariant under all permutations.
  - Graph properties: Invariant under vertex renaming.
  - Boolean properties: Invariant under variable renaming.
  - Matrix properties: Invariant under mult. by invertible matrix.
  - Algebraic Properties = ?
- Goals:
  - Possibly generalize specific results.
  - Get characterizations within each class?
  - In algebraic case, get new (useful) codes?

Abstracting Linearity/Low-degree tests

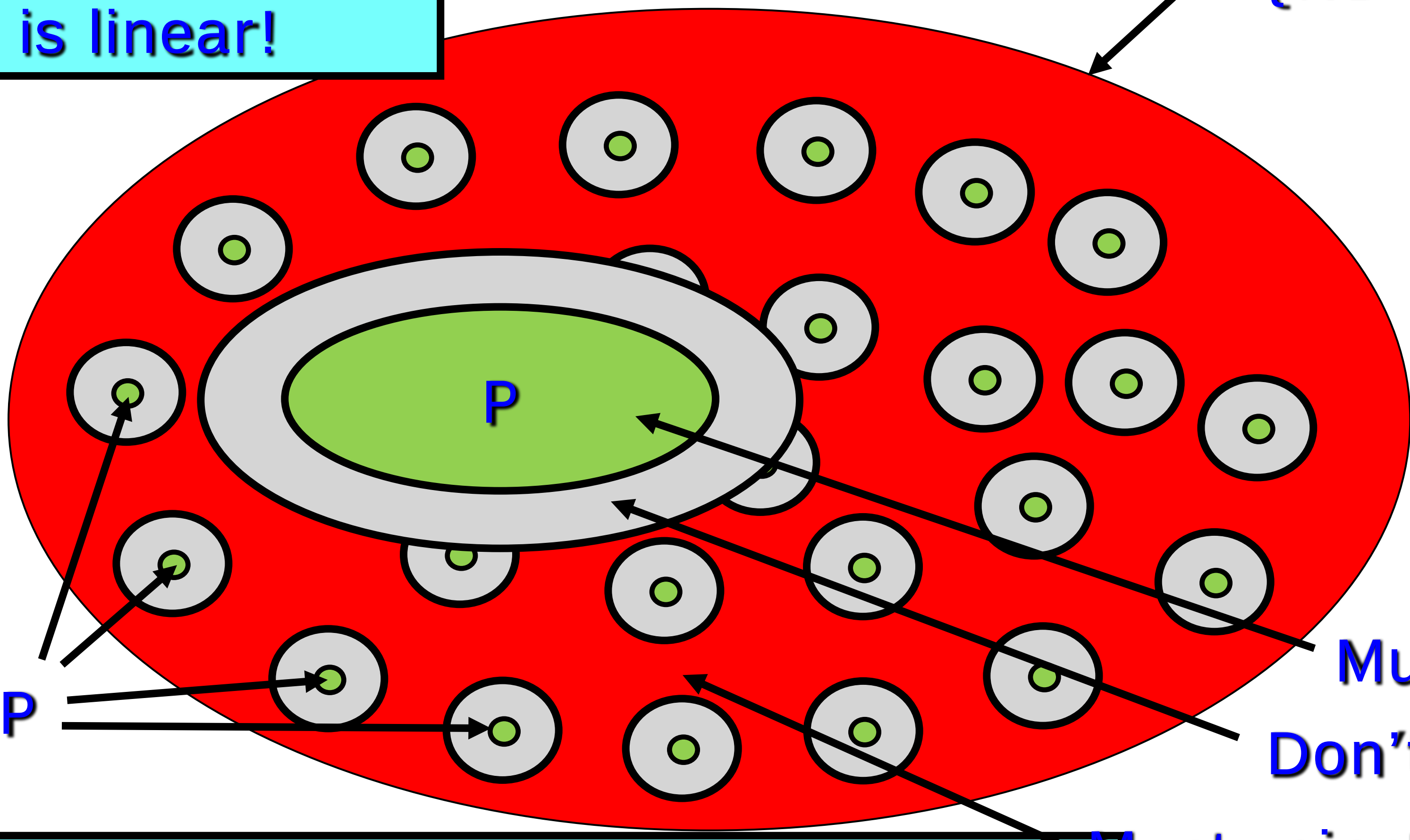
- Affine Invariance:
  - Domain = Big field ($GF(2^n)$)

    or vector space over small field ($GF(2)^n$).
  - Property invariant under affine transformations of domain ($x \mapsto A.x + b$)

- Linearity:
  - Range = small field ($GF(2)$)
  - Property = vector space over range.

Testing Linear Properties

R is a field F;
P is linear!



Algebraic Property = Code! (usually)

Why study affine-invariance?

- Common abstraction of properties studied in [BLR], [RS], [ALMSS], [AKKLR], [KR], [KL], [JPRZ].
  - (Variations on low-degree polynomials)

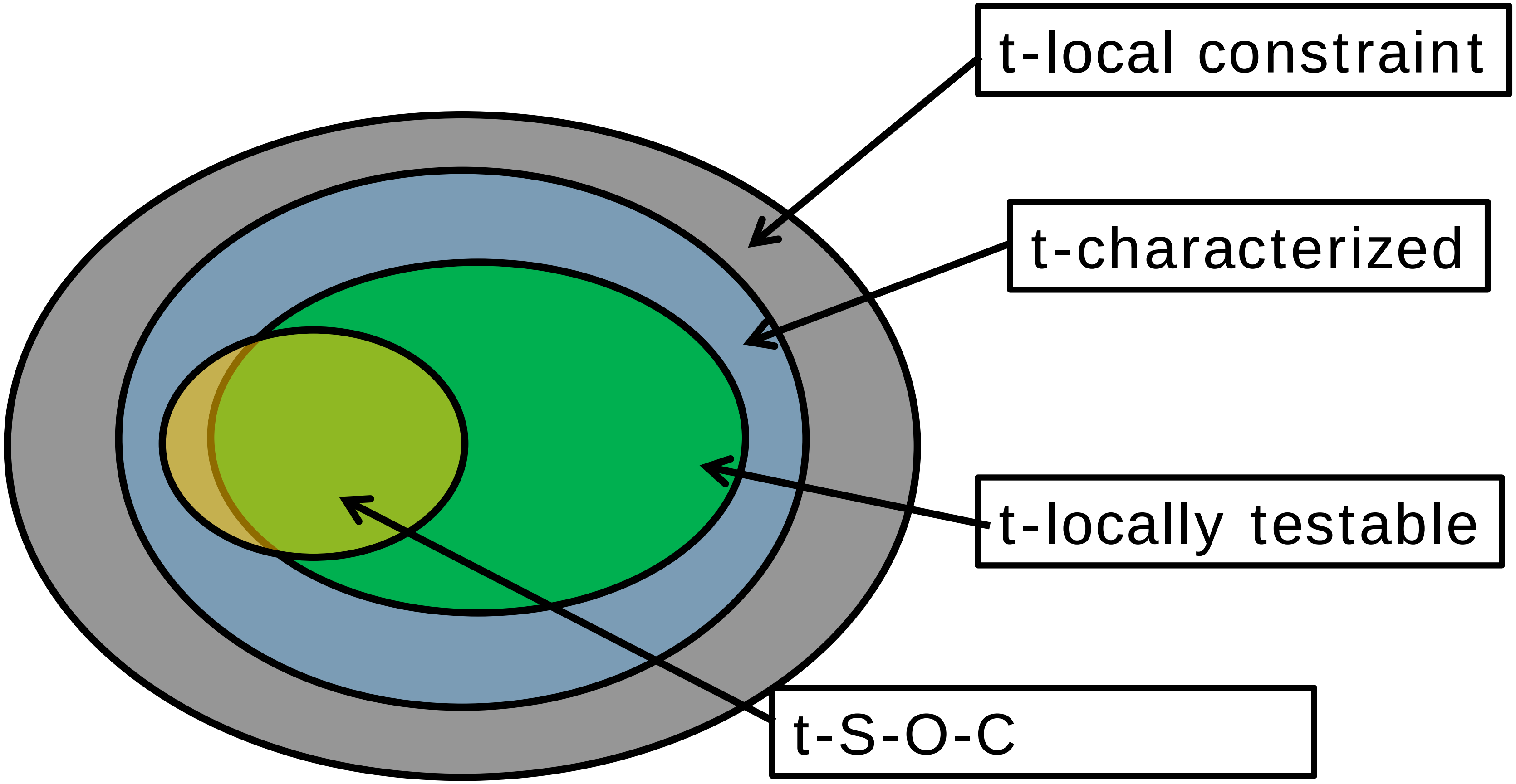
- Hopes
  - Unify existing proofs
  - Classify/characterize testability
  - Find new testable codes (w. novel parameters)

- Rest of the talk: Brief summary of findings

Basic terminology

- Local Constraint:
  - Example: $f(1) + f(2) = f(3)$.
  - Necessary for testing Linear Properties [BHR]
- Local Characterization:
  - Example: $\forall$ x, y, $f(x) + f(y) = f(x+y) \Leftrightarrow f \in P$
  - Aka: LDPC code, k-CNF property etc.
  - Necessary for affine-invariant linear properties.
- Single-orbit characterization:
  - One linear constraint + implications by affine-invariance.
  - Feature in all previous algebraic properties.

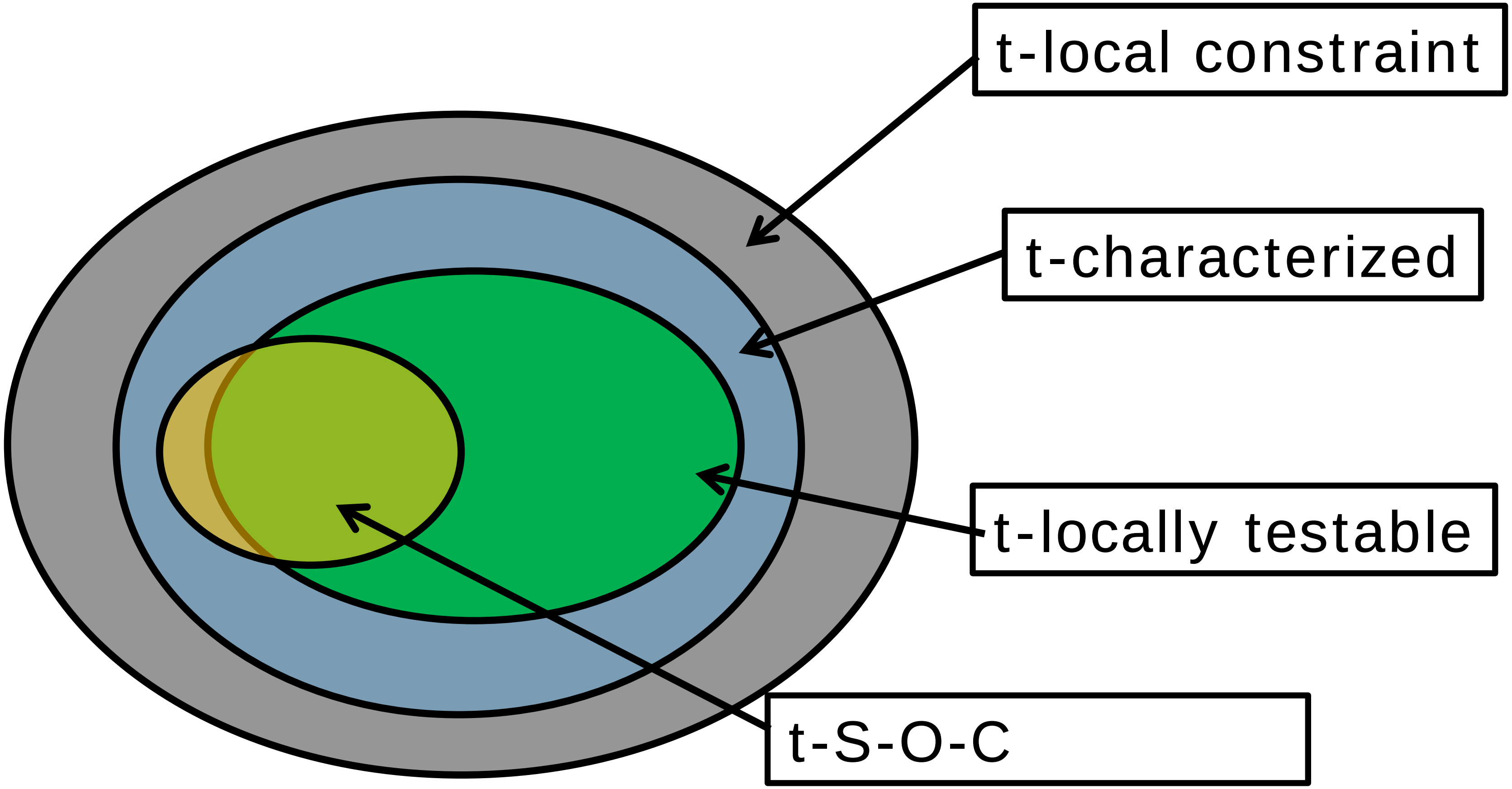
Affine-invariance & testability



State of the art in 2007

- [AKKLR]: t-constraint = t'-testable, for all linear affine-invariant properties?

Affine-invariance & testability



Some results

- [Kaufman+S.'07]: Single-orbit $\Rightarrow$ Testable.

- Next few slides: the Proof

Proof: t-S-O-C ⇒ t-testable

- Property P (t-S-O-C) given by $\alpha_1,\ldots,\alpha_t$; $V \in F^t$
- $P = \{f \mid f(A(\alpha_1)) \ldots f(A(\alpha_t)) \in V, \forall$ affine $A: K^n \to K^n\}$
- $\mathrm{Rej}(f) = \mathrm{Prob}_A$ [$f(A(\alpha_1)) \ldots f(A(\alpha_t))$ not in V]
- Wish to show: If $\mathrm{Rej}(f) < 1/t^3$,

  then $\delta(f,P) = O(\mathrm{Rej}(f))$.

Proof: BLR Analog

- $\mathrm{Rej}(f) = \Pr_{x,y} [\, f(x) + f(y) \neq f(x+y)] < \epsilon$

- Define $g(x) = \mathrm{majority}_y \{\mathrm{Vote}_x(y)\}$,
  where $\mathrm{Vote}_x(y) = f(x+y) - f(y)$.

- Step 0: Show $\delta(f,g)$ small

- Step 1: $\forall\, x$, $\Pr_{y,z} [\mathrm{Vote}_x(y) \neq \mathrm{Vote}_x(z)]$ small.

- Step 2: Use above to show g is well-defined and a homomorphism.

Proof: BLR Analysis of Step 1

- Why is $f(x+y) - f(y) = f(x+z) - f(z)$, usually?

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

Proof: Generalization

- $g(x) = \bar{\beta}$ that maximizes, over A s.t. $A(\alpha_1) = x$,
  $\Pr_A [\bar{\beta}, f(A(\alpha_2)), \ldots, f(A(\alpha_t)) \in V]$

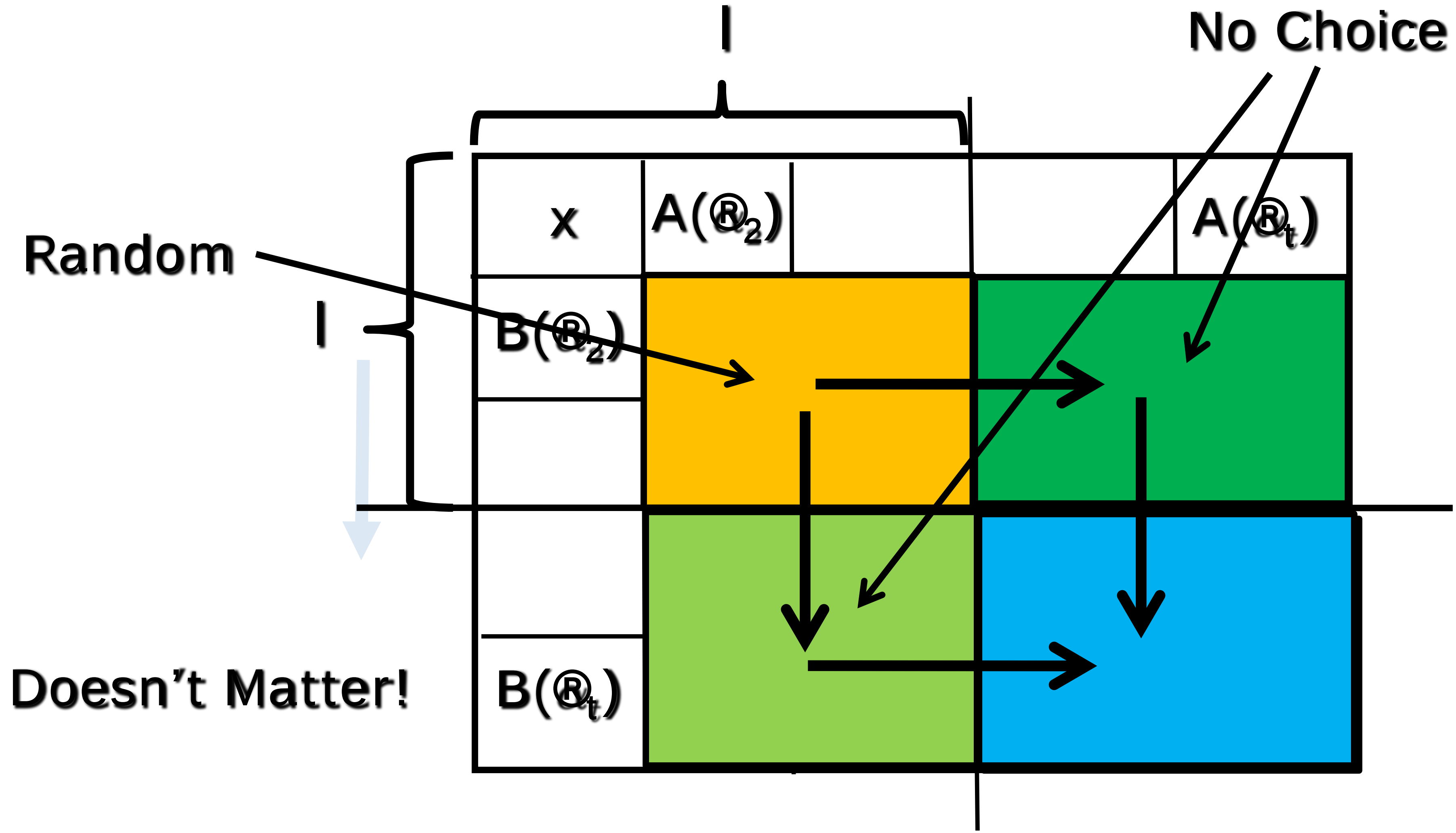
- Step 0: $\delta(f,g)$ small.

- $\mathrm{Vote}_x(A) = \bar{\beta}$ s.t. $\bar{\beta}, f(A(\alpha_2)) \ldots f(A(\alpha_t)) \in V$
  (if such $\bar{\beta}$ exists)

- Step 1 (key): $\forall\, x$, whp $\mathrm{Vote}_x(A) = \mathrm{Vote}_x(B)$.
- Step 2: Use above to show $g \in P$.

Proof: Matrix Magic?

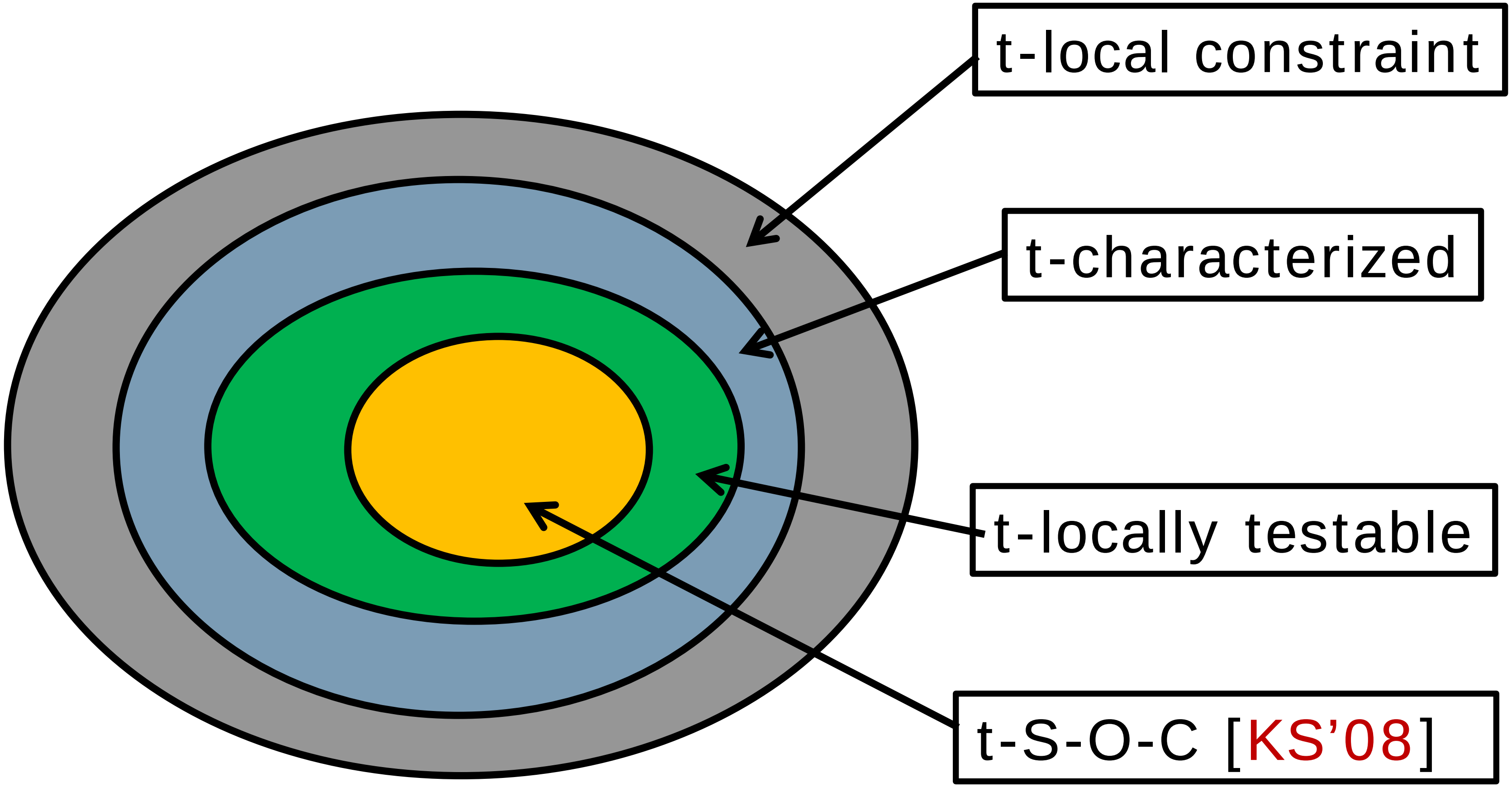
Say A(®$_1$) … A(®$_l$) independent;
rest dependent



Some results

- [Kaufman+S.'07]: Single-orbit $\not\Rightarrow$ Testable.

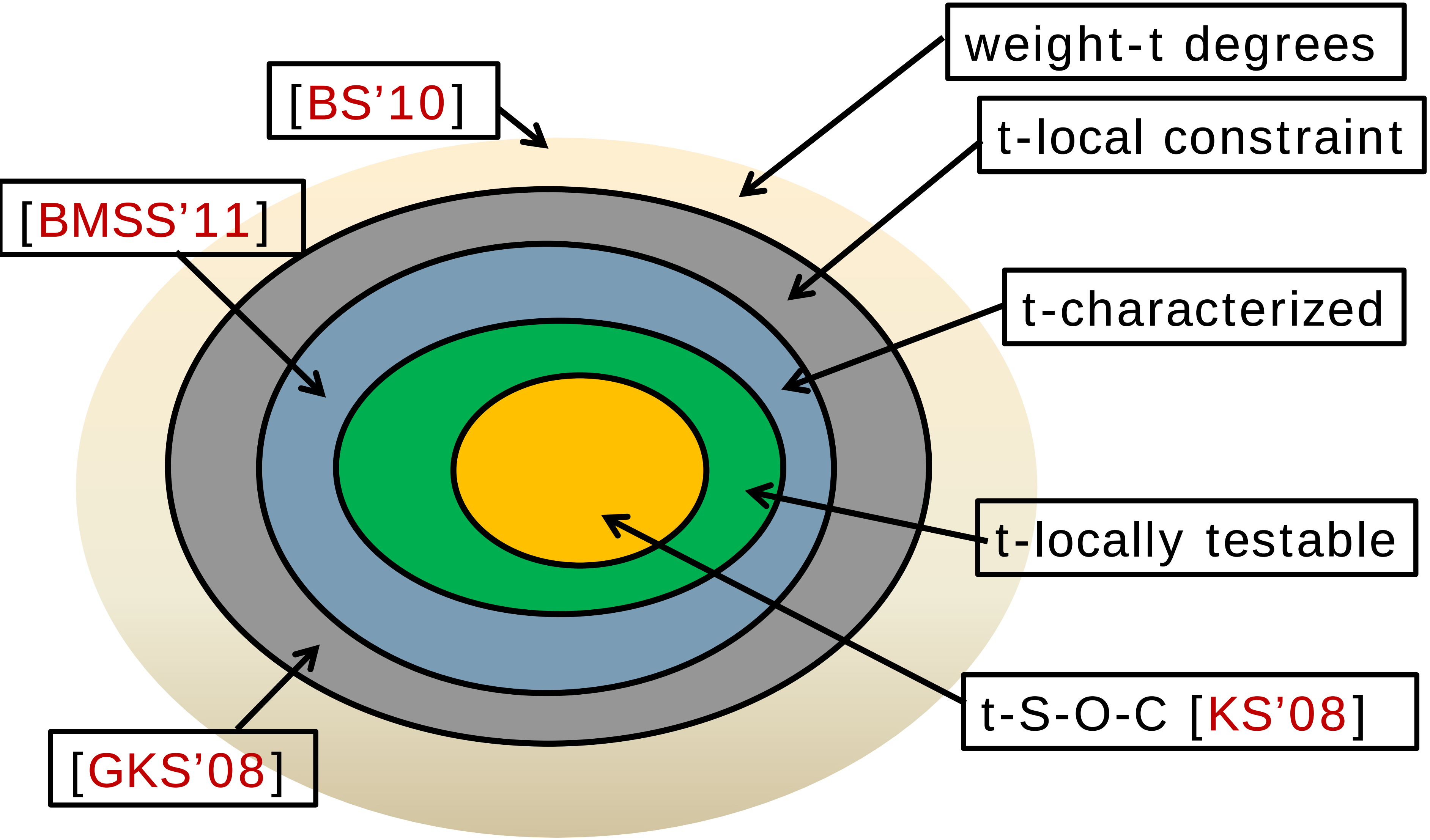
Affine-invariance & testability



Some results

- [Kaufman+S.'07]: Single-orbit $\Rightarrow$ Testable.
  - Unifies known algebraic testing results.
  - Converts testability to purely algebraic terms.
  - Yields "Constraints = Char. = Testability" for vector spaces over small fields.
  - Left open: Domain = Big field.
  - $\exists$ Many "non-polynomial" testable properties
- [GKS'08]: Over big fields, Constraint ≠ Char.
- [BMSS'11]: Over big fields, Char ≠ Testability.
- [BGMSS'11]: Many questions/conjectures outlining a possible characterization of affine-invariant properties.

Affine-invariance & testability



State of knowledge over big fields

- All known testable properties are S-O-C.

- If $|K| = |F^n|$, then the class of degree d n-variate polynomials is $(|F|^{d+1})$- S-O-C over K.

- [Kaufman-Lovett] If $P \subseteq \{K \rightarrow F_p\}$ has only $|K|^c$ members, then P is t(c,p)-S-O-C.

- Sums, Intersections, and "Lifts" of S-O-C properties are S-O-C.

Quest in lower bound

- Proposition: For every affine-invariant property P, there exists a set of degrees D s.t.

  P = {polynomials supported on monomials in D}

- Quest: Given degree set D (shadow-closed, shift-closed) prove it has no S-O-C.

- Equivalently: Prove there are no

  $\lambda_1 \ldots \lambda_t \in F$, $\circledR_1 \ldots \circledR_t \in K$ such that

  - $\sum_{i=1}^{t} \lambda_i \circledR_i^d = 0$ for every $d \in D$.
  - $\sum_{i=1}^{t} \lambda_i \circledR_i^d \neq 0$ for every minimal $d \notin D$.

Pictorially

$$M(D) = \left(\text{®}_1^{d} \quad \text{®}_2^{d} \quad \cdots \quad \text{®}_t^{d} \right)$$

Is there a vector $(\text{¸}_1, \ldots, \text{¸}_t)$ 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.

Structure of Degree sets

- Let D = degree set (P).
- D Shift closed: Range = F_q and $d \in D \Rightarrow q.d \in D$.
- D Shadow closed: Let p = char(q) and d in D. Then every e in p-shadow of d is also in D.
  - e in p-shadow of d if every digit in base p expansion is smaller.

Non-testable Property - 1

- AKKLR (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.
  - Range = $GF(2)$; Domain = $GF(2^n)$
  - $P = \mathrm{Fam}(\mathrm{Shift}(\{0,1\} \cup \{1+2, 1+2^2, \ldots, 1+2^k\}))$.

Proof (based on [BMSS'11])

- $F = GF(2)$; $K = GF(2^n)$;
- $P_k = Fam(Shift(\{0,1\} \cup \{1 + 2^i \mid i \in \{1,\ldots,k\}\}))$
- Let $M_i =$

$$\begin{pmatrix} \text{®}_1^{\,2} & \text{®}_2^{\,2} & \cdots & \text{®}_k^{\,2} \\ & & & \\ \text{®}_1^{\,2^i} & \text{®}_2^{\,2^i} & \cdots & \text{®}_k^{\,2^i} \end{pmatrix}$$

- If $Ker(M_i) = Ker(M_{i+1})$, then $Ker(M_{i+2}) = Ker(M_i)$
- $Ker(M_{k+1})$ = would accept all functions in P_{k+1}
- So $Ker(M_i)$ must go down at each step, implying $Rank(M_{i+1}) > Rank(M_i)$.

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. $Q = \cap_i Q_i$

Example: Sums of S-O-C properties

- Suppose $D_1 = \mathrm{Deg}(P_1)$ and $D_2 = \mathrm{Deg}(P_2)$
- Then $\mathrm{Deg}(P_1 + P_2) = D_1 \cup D_2$.
- Suppose S-O-C of P_1 is C_1: $f(a_1) + \ldots + f(a_k) = 0$; and S-O-C of P_2 is C_2: $f(b_1) + \ldots + f(b_k) = 0$.
- 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 orbit(C_1), orbit(C_2) does!
  - Proof uses $\mathrm{wt}(\mathrm{Deg}(P_1)) \leq k$.

Hopes

- Get a complete characterization of locally testable affine-invariant properties.
- Use codes of (polynomially large?) locality to build better LTCs/PCPs?
  - In particular move from "domain = vector space" to "domain = field".
- Codes invariant under other groups?
  - [KaufmanWigderson], [KaufmanLubotzky]
  - Yield symmetric LDPC codes, but not yet LTCs.
- More broadly: Apply lens of invariance more broadly to property testing.

Thank You!