Property Testing and Affine Invariance

Part I

Madhu Sudan
Harvard University

Goals of these talks

- Part I
  - Introduce Property Testing (broadly interesting)
    - Philosophy behind "Invariance"
  - Introduce Algebraic Property Testing
    - Affine-Invariance
- Part II
  - Structural results about Affine-Invariance
  - Testing & Affine-Invariance

Property Testing

- Broadly: Test if massive data has some global property approximately, quickly.
  - E.g.: 16th/17th century astronomy: Do planetary positions have geometric structure?
- Formalization:
  - Data = Function $f : D \to R$ (D, R finite)
  - Property = $P \subseteq \{f : D \to R\}$
  - Approximately? $\delta(f, P)$ small, where
    $$\delta(f,P) = \min_{g \in P} \{ \delta(f,g) \stackrel{\text{def}}{=} \Pr_{x \leftarrow D}[f(x) \neq g(x)] \}$$
  - Quickly? With $\ell \ll |D|$ queries into f

Ancient Example: Majority

- Is Majority of Population (roughly) Blue/Red?
  - D = Population; R = {Blue, Red}
  - f = Current preferences
  - $P = \left\{g : \Pr_x[g(x) = Blue\,] \geq \frac{1}{2}\right\}$
- Test: Pick $x_1, \ldots, x_\ell \in D$ uniformly independently.
  - Accept if more than $\left(\frac{1}{2} - \frac{\epsilon}{2}\right)\ell$ vote Blue.
  - Theorem:
    - $f \in P \Rightarrow$ Accept w.p. $\geq 1 - \exp(-\epsilon^2 \ell)$
    - $\delta(f, P) \geq \epsilon \Rightarrow$ Accept w.p. $\leq \exp(-\epsilon^2 \ell)$
- Emphasis: ℓ independent of $|D|$; Error acceptable

Less Ancient Example: Linearity

- Is $f(x_1, \dots, x_m) \approx \sum_i a_i x_i$ for some $a_1, \dots, a_n$
- Abstraction: $D = G, R = H$; G, H finite groups
  $$P = \{\phi : G \to H \mid \forall x, y\ \phi(x+y) = \phi(x) + \phi(y)\}$$
- Test: Pick $x, y \in G$ uniformly & independently
  - Accept if $f(x+y) = f(x) + f(y)$
- Analysis [Blum,Luby,Rubinfeld '90]:
  - $f \in P \Rightarrow$ Accept w.p. 1 (by definition)
  - $\delta(f, P) \geq \delta \Rightarrow$ Reject w.p. $\geq \frac{2}{9}\delta$ (non-trivial)

Non-triviality?

- Example:
  - $n = 3^t$; $G = \mathbb{Z}_{3n}$; $H = \mathbb{Z}_n$; $P = \{x \mapsto ax \ (\mathrm{mod}\ n)\}$;
  - Consider $f(x) = \left\lfloor \frac{x}{3} \right\rfloor$
  - $\delta(f, P) = 1 - \frac{1}{n}$
  - $\Pr[Acceptance] = \frac{7}{9}$ (Reject iff $x\ mod\ 3 = y\ mod\ 3 \in \{+1, -1\}$)
- Reason for non-triviality:
  - Gap between
    - "f usually satisfies P" and
    - "f usually equals g which always satisfies P"
  - Gap invisible in "Polling"; gaping in "linearity"

Example 3: Low-degree testing

- Is $f(x_1,\ldots,x_m) \approx g(x_1,\ldots,x_m)$ with $\deg(g) \leq d$?
- $D = \mathbb{F}_q^m\,; R = \mathbb{F}_q$
- Test: Is $\deg(f|_{line}) \leq d$?
  - (More generally: Is $\deg(f|_A) \leq d$ for affine subspace A?)
  - Locality $\ell = q$ vs. $|D| = q^m$
- (Example) Analyses:

$$\exists \alpha > 0 \text{ s.t. } \forall\, m,q,d \leq \frac{q}{2},\ \Pr_{line}[Rejecting\ f] \geq \alpha \cdot \delta(f,P_d)$$

- Robust version:

$$\exists\, \beta > 0 \text{ s.t. } \forall m,q,d \leq \frac{q}{2}, \mathbb{E}_{line}[\delta(f|_{line},P_d)] \geq \beta \cdot \delta(f,P_d)$$

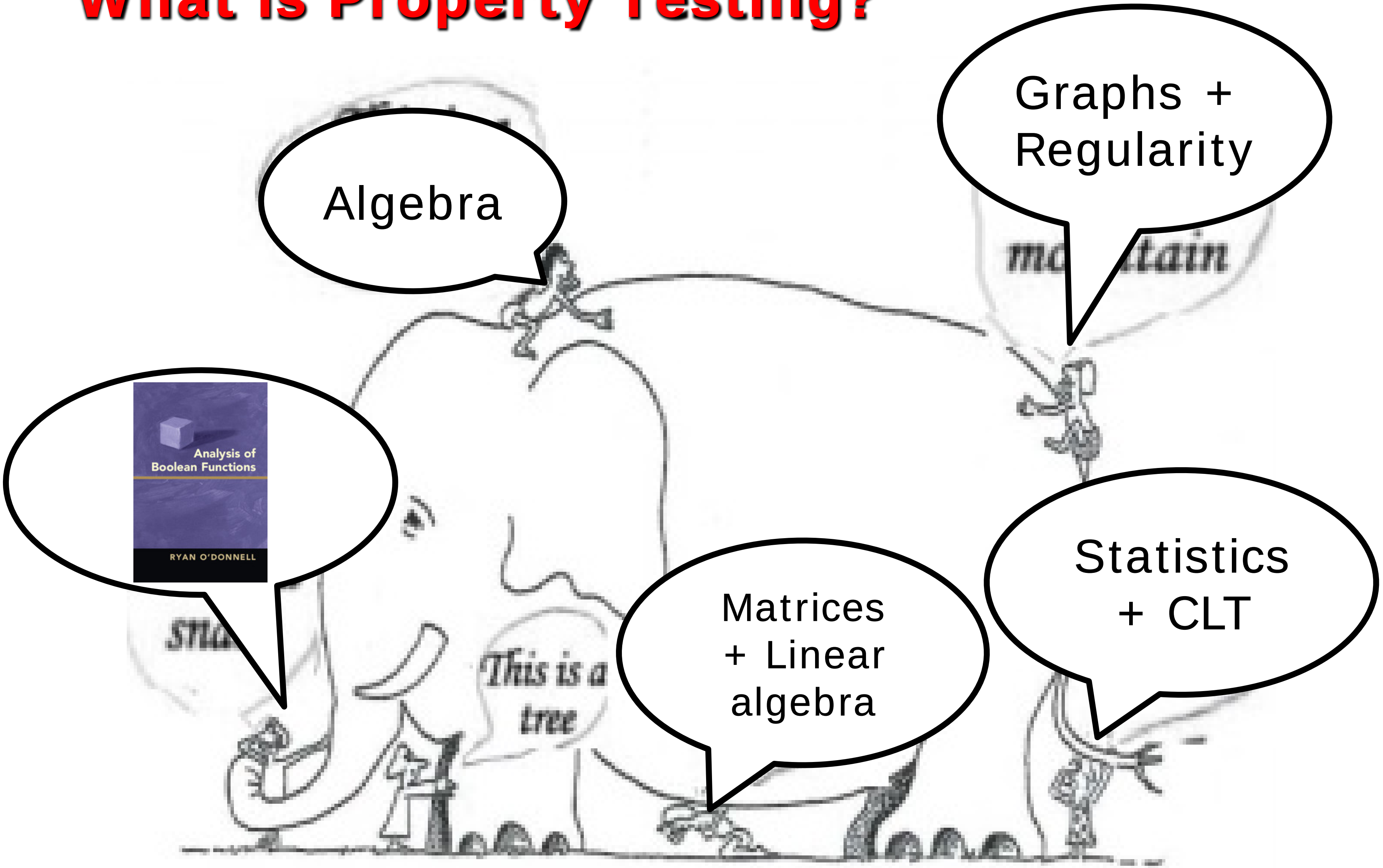
Aside: Importance of Low-degree Testing

- Central element in PCPs (Probabilistically Checkable Proofs).
  - Till [Dinur'06] – no proof without (robust) low-degree testing.
  - Since: Best proofs (smallest, tightest parameters etc.) rely on improvements to low-degree tests.
- Connected to Gowers Norms:
  - [Viola-Wigderson'07]: [AKKLR]⇒Hardness Amplification
- Yield Locally Testable Codes
  - Best in high-rate regime.
  - [BarakGopalanHåstadMekaRaghavendraSteurer'12]:
    [BKSSZ'11] ⇒ Small-set expanders.

History of Property Testing (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 + 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

What is Property Testing?



Invariance?

- Property $P \subseteq \{f: D \to R\}$
- Property P invariant under 1-1 $\pi: D \to D$, if

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

- Property P invariant under group G if

$$\forall \pi \in G \Rightarrow P \text{ is invariant under } \pi.$$

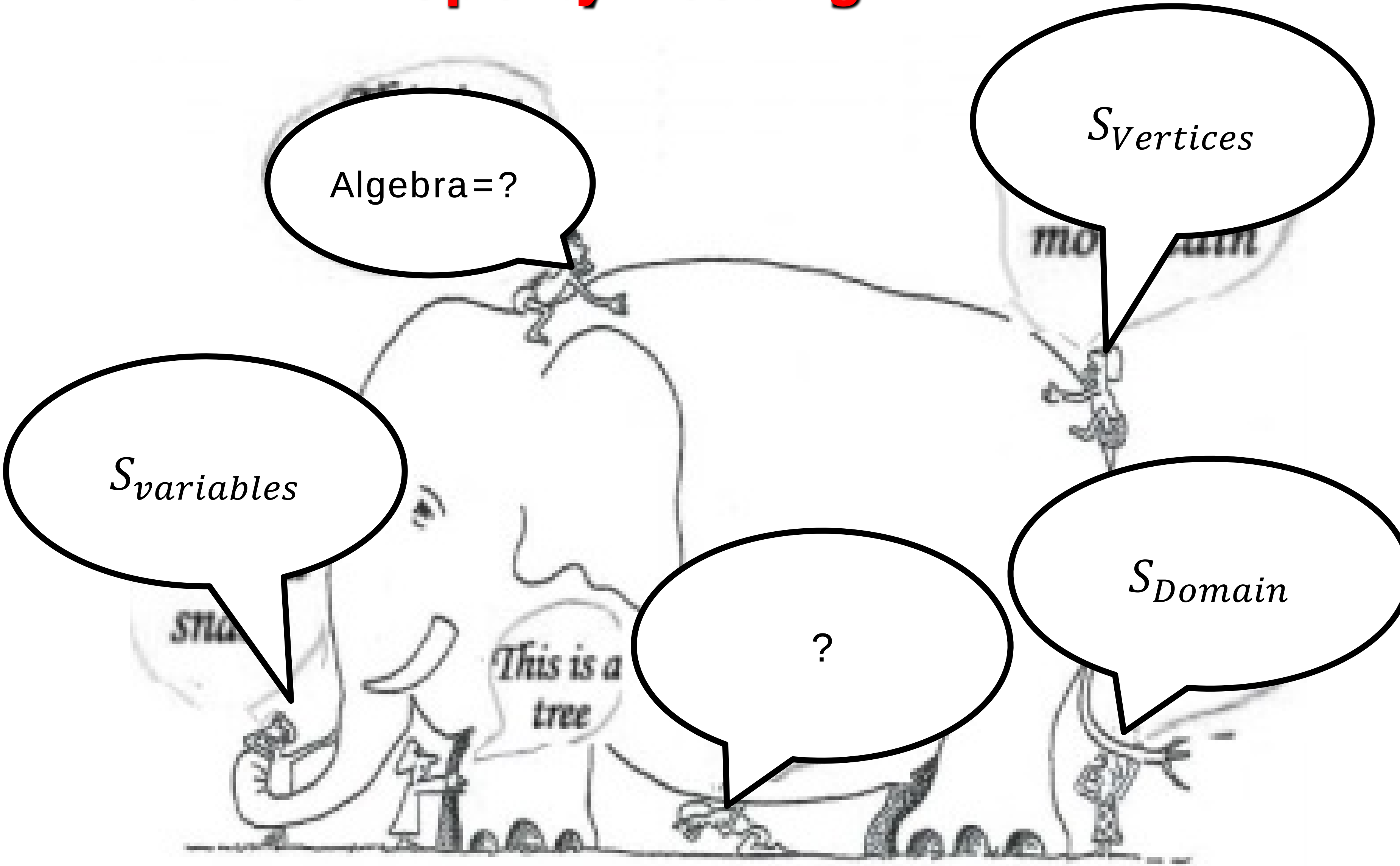
  - G is invariance class of P.

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

Invariances (contd.)

- Some examples:
  - Classical statistics: Invariant under all permutations S_D.
  - Graph properties: Invariant under vertex renaming.
  - Boolean properties: Invariant under variable renaming.
  - Matrix properties: Invariant under mult. by invertible matrix.
  - Algebraic Properties = ?
- Some introspection:
  - Classical statistics only dealt with S_D
  - Different invariances $\Leftrightarrow$ different techniques.
  - Invariance for algebra?

What is Property Testing?



Algebraic Property Testing

- Property = "algebraic"
  - Linearity Property (esp. $G = \mathbb{F}_q^m; H = \mathbb{F}_q$)
  - Low-degree Property.
  - Is there anything else? What is the abstraction?

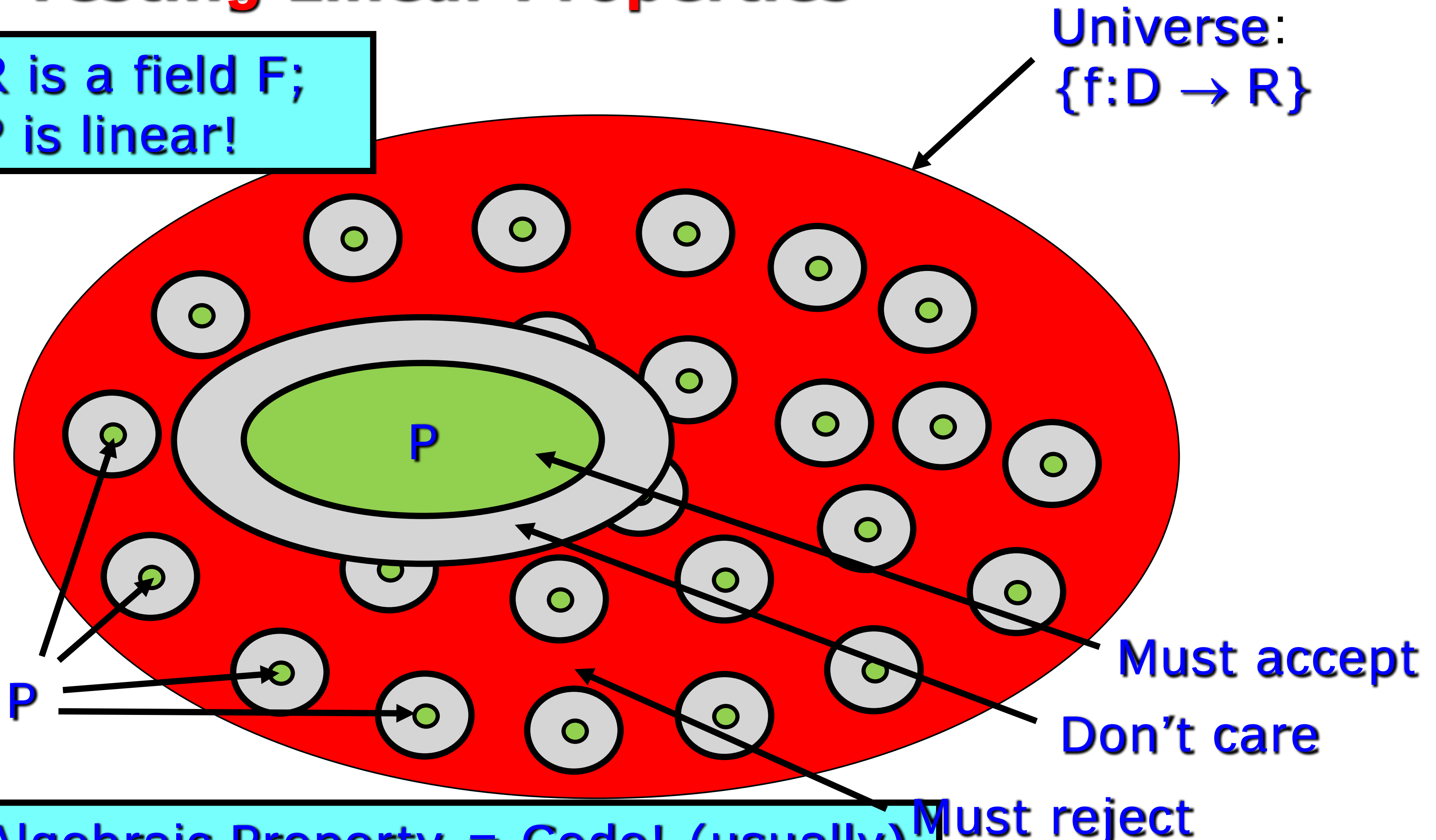
Abstracting algebraic properties

- [Kaufman+S.'08]
- Affine Invariance:
  - Range = Small Field $\mathbb{F}_q$
  - Domain = Vector space over extension field $\mathbb{F}_{q^n}^m$
  - Property invariant under affine transformations of domain ($x \mapsto A \cdot x + b$)

- Additional feature: Linearity of Properties:
  - Property = vector space over range.
  - Critical in use in Coding Theory/PCP.

Testing Linear Properties

R is a field F;
P is linear!



Algebraic Property = Code! (usually)

Connection to Coding Theory

- Algebraic properties lead to error-correcting codes
  - Low-degree polynomials can't intersect often.
  - True for other classes of algebraic functions.
    - BCH codes, Dual BCH codes (same symmetries)
    - AG/Goppa codes (fewer symmetries)

- Coding theoretic metrics – want Property with:
  - Large pairwise "distance" ← Classical
  - Many members ("high rate") ← Classical
  - Small locality of tests. ← New!

Why Study Affine-Invariance

- Unify known testability results?
  - [Kaufman+S'08]: Unified [BLR'90], [RS '92], [AKKLR '03], [JPRZ '04], [KR '04].
  - [Haramaty+RonZewi+S'13]: extends [BKSSZ 10], [HSS '11]
  - [Guo+Haramaty+S'14]: strengthens robust low-degree tests [ALMSS'92,Raz-Safra'96]
- What leads to testability?
  - Negative results: Counterexamples to AKKLR conjecture
  - Positive results: Restrictions within Affine-invariance.
- New Codes and Implications:
  - Lifted codes

Rest of talk (including tomorrow)

- AKKLR Conjecture
  - Motivation, Counterexample, Lessons
- Lifted Codes
  - Intriguing generalization of polynomials!
- Ideas behind analyses of local tests
  - Role of the tensor product

AKKLR Conjecture

- [Alon,Kaufman,Krivelevich,Litsyn,Ron '03]
  - Extended low-degree testing to case of $d \geq q$.
  - Proof extended that of BLR.
  - Conjectured that testing should apply to symmetric codes with local constraints.
    - Symmetric = ? 2-transitive invariance class
      - 2-transitivity supports local "decoding"
    - Constraints = ?

Constraints, Characterization, Testing…

- Testing ⇒ Constraints
  - Example: Can not test degree d polynomials with locality $\ell \leq d+1$
    - No local constraints!
    - $\forall S \subseteq \mathbb{F}_q$, $|S| \leq d+1$, $\{p_S\}_p \equiv \{f_S\}_f$, where $p =$ random deg. d poly, $f =$ random function.
- Constraint$=(S,V)$: $S \subseteq D, |S| \leq \ell; V \subseteq \{h: S \to R\}$.

$$\text{Is } f\Big|_S \in V?$$

- Testing ⇒ Characterizations
  - Characterization$=\{C_1, \ldots, C_M\}$; C_j=constraint.

$$f \in P \quad \Leftrightarrow \quad \forall j, f \text{ satisfies } C_j$$

Constraints/Characterizations suffice?

- [Ben-Sasson,Harsha,Raskhodnikova '04]: No! even characterizations don't.
- AKKLR: Perhaps symmetry suffices?
  - Strong form: Constraint + 2-transitivity suffices
    - Does above imply characterization?
  - Weak form: Characterization + 2-transitivity …
- Both forms false:
  - [Grigorescu,Kaufman,S'08]: Constraint + 2-transitivity $\nRightarrow$ Characterization
  - [Ben-Sasson,Maatouk,Shpilka,S'11]: Characterization + 2-transitivity $\nRightarrow$ Testing

Structure of Affine-Invariant Properties

- $P \subseteq \{g: \mathbb{F}_Q^m \to \mathbb{F}_q\}; Q = q^n;$ P linear, affine-invariant.
- $Tr(x) \stackrel{\text{def}}{=} x + x^q + \cdots + x^{q^{n-1}}$.
- $\exists\, D = \mathrm{Deg}(P) \subseteq \mathrm{Monomials}(x_1, \ldots, x_m)$

  s.t. $P = \{Tr(\sum_{M \in D} c_M M)\}$
- Closure properties of the degree set $\mathrm{Deg}(P)$:
  - $x_1^i x_2^j M \in \mathrm{Deg}(P) \Rightarrow x_1^{i+j} M \pmod{x_1^Q - x_1} \in \mathrm{Deg}(P)$;
  - $x_1^i M \in \mathrm{Deg}(P) \Rightarrow x_1^{qi} M \left(\mathrm{mod}\, x_1^Q - x_1\right) \in \mathrm{Deg}(P)$
  - $x_1^i M \in \mathrm{Deg}(P)\ \&\ j \leq_p i \Rightarrow x_1^j M, x_1^j x_2^{i-j} M \in \mathrm{Deg}(P)$
    - $j \leq_p i \Leftrightarrow j_t \leq i_t\ \forall t,\ j = \sum j_t p^t\, ; i = \sum_t i_t p^t\, ; q = p^s$
- Any set closed wrt all three above is a degree set

Known Testable Properties

- Focus on univariate properties $P \subseteq \{f : \mathbb{F}_{q^n} \to \mathbb{F}_q\}$
- Basic locally testable univ. properties
  - Reed-Muller $\mathrm{Deg}(RM_w) = \{x^d \mid d = \sum_t d_t p^t ; \sum_t d_t \leq w\}$ (locality $\ell \leq 2^{w+1}$)
  - Sparse: $|\mathrm{Deg}(P)| \leq t$; locality $\ell \leq \ell\left(\frac{t}{n}, q\right)$

    [KaufmanLitsyn,GrigorescuKS,KLovett,BenSassonRonZewiS]
- Operations: Let P_1 be ℓ_1-locally testable and P_2 be ℓ_2-locally testable; $\exists \ell = \ell(\ell_1, \ell_2, q)$ s.t.
  - $P_1 \cap P_2$, and $P_1 + P_2$ are ℓ-locally testable. [BGMatoukShpilkaS,GuoS]
  - … and one more operation (to come later)

Constraint + 2-transitivity $\not\Rightarrow$ Characterization

- Counterexample univariate wlog.
- Idea: Remove basis elements from RM_2 so resulting property is not Reed-Muller or sparse, but satisfies closure.
- Specifically $\mathrm{Deg}(P) = \left\{x^{2^i+2^j} \mid i - j \leq \frac{n}{3}\right\} \cup \left\{x^{2^i} \mid i\right\} \cup \{x^0\}$
- Thm: For P as above, $\ell = \Omega(n)$
- Key Lemma: $\alpha_1, \dots, \alpha_k \in \mathbb{F}_{2^n}$ lin. ind. over $\mathbb{F}_2$,

$$\Rightarrow \begin{bmatrix} \alpha_1^{2^1} & \cdots & \alpha_k^{2^1} \\ \vdots & \ddots & \vdots \\ \alpha_1^{2^k} & \cdots & \alpha_k^{2^k} \end{bmatrix}$$ is non-singular

Towards Counterexample to weak form

- Idea: Start with $P_1, \ldots, P_k$: ℓ-locally testable properties and let $P = \cap_i P_i$
- By construction P is ℓ-locally characterized
- Hope: locality of testing $\to \infty$ as $k \to \infty$
- Unfortunately:
  - Sparse ∩ Anything = Sparse
  - RM ∩ RM = RM
  - (RM+Sparse) ∩ (RM+Sparse) = RM+Sparse
- Need non "RM+Sparse" locally testable property.
- Idea "lift" sparse properties to non-sparse ones!

Lifting

- Base Code $B \subseteq \{b: \mathbb{F}_Q \to \mathbb{F}_q\}$ affine-invariant
- Lifted Code $L_m(B) = \{f: \mathbb{F}_Q^m \to \mathbb{F}_q \mid \forall line\ f|_{line} \in B\}$;
- $L_m(B) \subseteq \{g: \mathbb{F}_Q^m \to \mathbb{F}_q\} \hookrightarrow \{g: \mathbb{F}_{Q^m} \to \mathbb{F}_q\}$
- Lift of Sparse ≠ Sparse ; Lift of RM ≠ RM
- [BMSS] Use lifts and intersections to show Characterization + 2-transitivity ⇏ Testing

Characterizations + 2-transitivity $\not\Rightarrow$ Testable

- $P \subseteq \{f: \mathbb{F}_{2^n} \to \mathbb{F}_2\}$; $n = n_1 \cdots n_k$; n_i distinct primes
- $B_i \subseteq \{b: \mathbb{F}_{2^{n_i}} \to \mathbb{F}_2\}$; $\mathrm{Deg}(B_i) = \left\{x^{2^j + 2^{j+1}} \mid j\right\} \cup \{1, x, x^2, x^4 \ldots\}$
- $P_i = L_{\frac{n}{n_i}}(B_i) \subseteq \{f: \mathbb{F}_{2^n} \to \mathbb{F}_2\}$; $P = \cap_i P_i$
- Lemma: Test-locality$(P) \to \infty$ as $k \to \infty$
  - Proof Steps:
    - Let $P_i' = \cap_{j \leq i} P_j$; Understand $\mathrm{Deg}(P_i')$
    - Find $Y_i \subseteq \mathrm{Deg}(P_i')$ with nice recursive structure.
    - Extract Matrices M_i such that constraint lies in its kernel.
    - Prove $\ker(M_i) \subsetneq \ker(M_{i-1})$

Characterizing testability

- Conjecture: To be $O(1)$ locally testable, code must be obtained from $\{RM, Sparse\}$ by finite #composition steps using $\{L_m, +, \cap\}$
- Conjecture implies:

$\forall t\ \exists k\ \forall$ prime n, $\forall S \subseteq \{1, \dots, n\}, \forall \alpha_1, \alpha_2, \dots, \alpha_k \in \mathbb{F}_{2^n}$ lin. ind. the matrix $M = \left[\alpha_i^{2^s}\right]_{i \in [k], s \in S}$ has rank $\geq t$

- Implication Open!
- In general, few techniques to lower bound rank of matrix over finite fields

Next Lecture

- Nice Lifted Properties
  - Surprising implications in incidence geometry
- Testability of Affine-invariant codes
  - Some ideas

Thank You