Invariance in Property Testing

Madhu Sudan
Microsoft/MIT

Modern challenge to Algorithm Design

- Data = Massive; Computers = Tiny
  - How can tiny computers analyze massive data?
  - Only option: Design sublinear time algorithms.
    - Algorithms that take less time to analyze data, than it takes to read/write all the data.
    - Can such algorithms exist?

Yes! Polling …

- Is the majority of the population Red/Blue
  - Can find out by random sampling.
  - Sample size $\propto$ margin of error
    - Independent of size of population
- Other similar examples: (can estimate other moments …)

Recent "novel" example

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

Brief History

- [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
- [Goldreich,Goldwasser,Ron]
  - Graph property testing
- Since then … many developments
  - Graph properties
  - Statistical properties
  - …
  - More algebraic properties

Property Testing

- Data = a function from D to R:
  - Property $P \subseteq \{D \to R\}$
- 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 $\delta(f,g) \leq \varepsilon$.
- Local testability:
  - P is (k, ε, δ)-locally testable if $\exists$ k-query test T
    - $f \in P \Rightarrow T^f$ accepts w.p. $1-\varepsilon$.
    - $\delta(f,P) > \delta \Rightarrow T^f$ accepts w.p. ε.
- Notes: want $k(\varepsilon, \delta) = O(1)$ for $\varepsilon,\delta = \Omega(1)$.

Why is BLR special?

Why is BLR special?

- Impressive collection of generalizations, alternate proofs, applications (all of PCP, LTC theory, e.g.)?
- Why is it more interesting than just polling?
- Why did the proof work? Was it a one-shot thing?
- Most previous attempts to extend "broadly" failed …

BLR Analysis

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

- Define $g(x)$ = 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.

Key Step: Step 1

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

    (Note: Prob over y,z for fixed x.)

- Proof:
    - $f(x+y) + f(z) = f(x+y+z)$ [w.h.p.]
      $= f(x+z) + f(y)$ [w.h.p. again]

- Proof from the Book.
    - (Indisputable! Inexplicable!)

Extensions

- [Rubinfeld + S. 92-96]: Low degree tests
- [Rubinfeld 94]: Functional equations
- [ALMSS, etc.]: PCP theory
- [AKKLR 02]: Reed-Muller tests
- [KaufmanRon, JPRZ]: Generalized RM tests.

    - … each time a new proof of key step.

Abstraction of BLR (in special case)

- Restrict to $G = F^n$ and $H = F$

  (F = finite field; with q elements)
- Property:
  - Linear: (sum of linear functions is linear)
  - Locally characterized: $\forall$ x,y f(x) + f(y) = f(x+y)
  - Linear-invariant: Linear function remains linear after linear transformation of domain.
  - Single-orbit: Constraints above given by one constraint and implication of linear-invariance.
- Our hope: Such abstractions explain, extend and unify algebraic property testing.

Invariances

- 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

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

- Can ask: Does invariance of P w.r.t. "nice" G leads to local testability?

Invariances are the key?

- "Polling" works well when (because) invariant group of property is the full symmetric group.
- Modern property tests work with much smaller group of invariances.
- Graph property ~ Invariant under vertex renaming.
- Algebraic Properties & Invariances?

Example motivating symmetry

- Conjecture (AKKLR '96):
  - Suppose property P is a vector space over F_2;
  - Suppose its "invariant group" is "2-transitive".
  - Suppose P satisfies a k-ary constraint
    - $\forall f \in P$, $f(\alpha_1) + \cdots + f(\alpha_k) = 0$.
  - Then P is $(q(k), \epsilon(k,\delta),\delta)$-locally testable.
- Inspired by "low-degree" test over F_2. Implied all previous algebraic tests (at least in weak forms).

Abstracting Algebraic Properties

- [Kaufman & S.]

- Range is a field F and P is F-linear.
- Domain is a vector space over F (or some field K extending F).

- Property is invariant under affine (sometimes only linear) transformations of domain.

- "Property characterized by single constraint, and its orbit under affine (or linear) transformations."

Terminology

- k-Constraint: Sequence of k elements of domain, and set of forbidden values for this sequence.

  e.g. $f(a) + f(b) = f(a+b)$
- k-characterization: Collection of k-constraints, satisfaction of which is necessary and sufficient criterion for satisfying property

  e.g. $f(a) + f(b) = f(a+b)$, $f(c) + f(d) = f(c+d)$ …
- k-single-orbit characterization: One k-constraint such that its translations under affine group yields k-characterization.

  $f(L(a)) + f(L(b)) = f(L(a+b))$; a,b fixed, all linear L.

Main Results

Some results

- If P is affine-invariant and has k-single orbit characterization then it is $(k, \delta/k^3, \delta)$-locally testable.
    - Unifies previous algebraic tests (in basic form) with single proof.

Analysis of Invariance-based test

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

BLR Analog

- $Rej(f) = Pr_{x,y} [f(x) + f(y) \neq f(x+y)] < \epsilon$
- Define $g(x) = \text{majority}_y \{Vote_x(y)\}$,
  where $Vote_x(y) = f(x+y) - f(y)$.
- Step 0: Show $\delta(f,g)$ small
- Step 1: $\forall$ x, $Pr_{y,z} [Vote_x(y) \neq Vote_x(z)]$ small.
- Step 2: Use above to show g is well-defined and a homomorphism.

Generalization

- $g(x) = \beta$ that maximizes, over A s.t. $A(\alpha_1) = x$,
  $\Pr_A [(\beta, f(A(\alpha_2)),\ldots,f(A(\alpha_k)))\in V]$
- Step 0: $\delta(f,g)$ small.
- $\mathrm{Vote}_x(A) = \beta$ s.t. $(\beta, f(A(\alpha_2))\ldots f(A(\alpha_k)))\in V$
  (if such β exists)
- Step 1 (key): $\forall\ x$, whp $\mathrm{Vote}_x(A) = \mathrm{Vote}_x(B)$.
- Step 2: Use above to show $g \in P$.

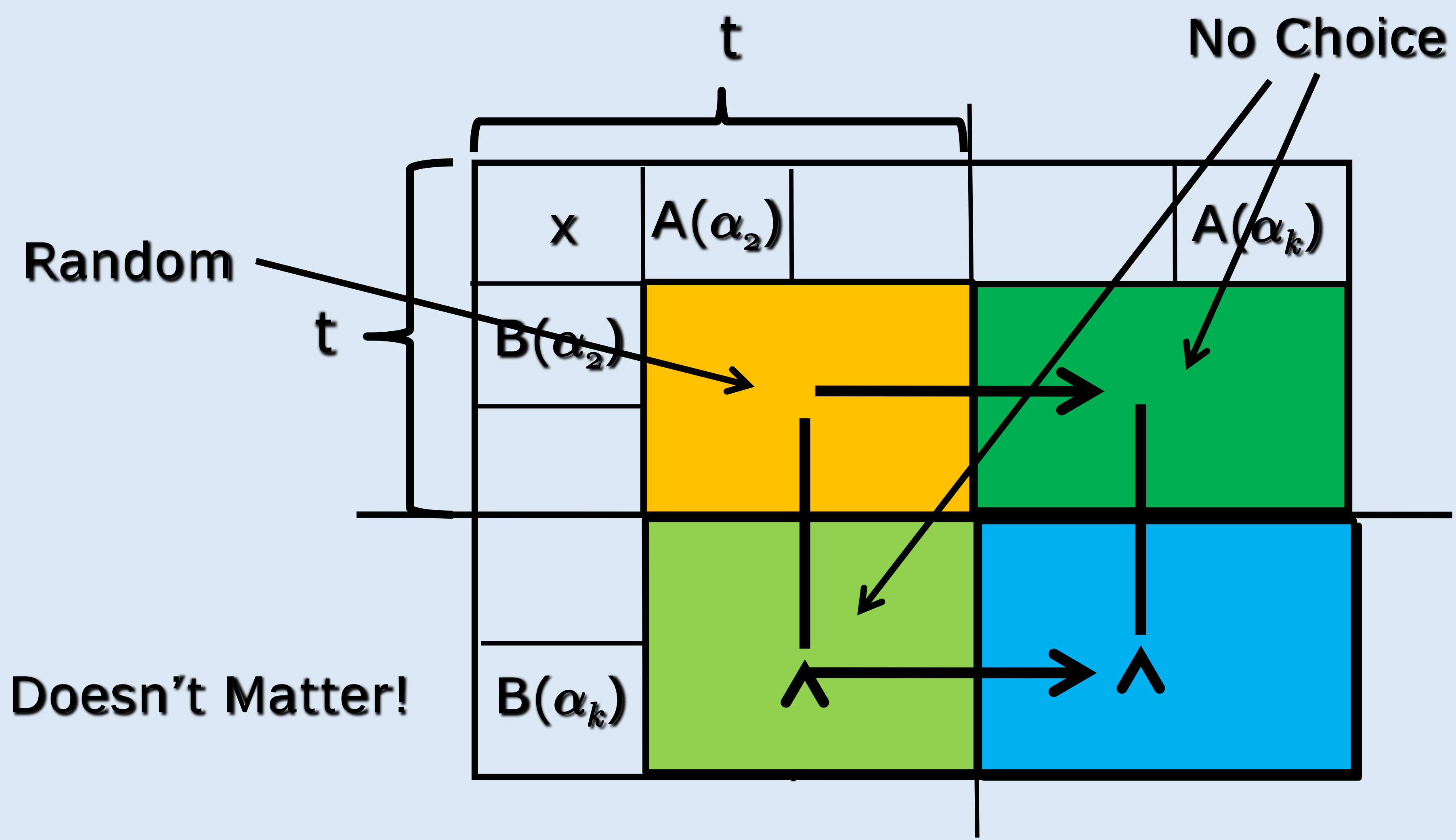
BLR Analysis of Step 1

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

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

Matrix Magic?

Say $A(\alpha_1)$ … $A(\alpha_t)$ independent; rest dependent



Results (contd.)

- Thm 2: If P is affine-invariant over K and has a single k-local constraint, then it is has a q-single orbit feature (for some $q = q(K,k)$)
- Proof ingredients:
  - Analysis of all affine invariant properties.
  - Characterization of all affine invariant properties in terms of degrees of monomials in support of polynomials in family
  - Rough characterization of locality of constraints, in terms of degrees.
- Infinitely many (new) properties …

Results from [KS '08]

- Thm 1: If P is affine-invariant and has k-single orbit feature then it is $(k, \delta/k^3, \delta)$-locally testable.
    - Unifies previous algebraic tests with single proof.
- Thm 2: If P is affine-invariant over K and has a single k-local constraint, then it is has a q-single orbit feature (for some $q = q(K,k)$)
    - (explains the AKKLR optimism)
- Completely characterizes local testability of affine-invariant properties over vector spaces over small fields.

Vector spaces over big fields?

- Most general case:
  - $f : K \to F^m$
  - Most interesting cases

    K = huge field; F, m small.

- Reasons to study:
  - Broader class: Potential counterexamples to intuitive beliefs.

  - Include starting point for all LTCs (so far).

Subsequent results

- [GrigorescuKaufmanS'08]: Counterexample to AKKLR Conjecture.
- [GrigorescuKaufmanS.'09]: Single orbit characterization of some BCH (and other) codes.
- [Ben-SassonS.]: Limitations on rate of (O(1)-locally testable) affine-invariant codes.

- [KaufmanWigderson]: LDPC codes with invariance (not affine-invariant)
- [BhattacharyyaChenS.Xie,Shapira]: Affine-invariant non-linear properties.

Technical nature of questions

- Given: k points $\alpha_1, \ldots, \alpha_k$ from K;
  and set of positive integers D,

  When is the $k \times |D|$ matrix with
  columns indexed by $[k]$ and rows by D, with
  (i,d)th entry being α_i^d, of full column rank?

- Nice connections to symmetric polynomials, and we have new results (we think).

Broad directions to consider

- Is every locally characterized affine-invariant property testable? (likely have a counterexample by now).
- What groups of invariances lead to testability?
- Is there a subclass of affine-invariant codes that will lead to linear-rate LTCs? ($n^{o(1)}$-locally testable with linear rate?)
- In general … seek invariances

Thanks