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: $f: G \rightarrow H$ ($G, H$ 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)
Property Testing

- Informally:
  - Efficiently” test if ”data” satisfies some property”, in “essence”

- Formally:
  - Data: $f: D \rightarrow R$
  - Property: $P \subseteq \{g: D \rightarrow R\}$
  - Efficient: $f$ given as a
  - Tester should make few queries to $f$.

- Essentially:
  - Accept $f \in P$ w.p. 1;
  - Reject $f$ “far” from $P$ w.h.p.
Distance: Far/Close

- Distance = (normalized) Hamming distance
  - $\delta(f,g) = \text{Prob}_{x \in \mathcal{D}} \left[ f(x) \neq g(x) \right]$
  - $\delta(f,P) = \text{Min}_{g \in P} \left[ \delta(f,g) \right]$

- $(q, \epsilon, \delta)$-tester for $P$:
  - Makes $q$ queries to $f$.
  - Accepts w.p. probability $\approx 1$ if $f \in P$
  - Reject w.p. probability $\epsilon$ if $\delta(f,P) \geq \delta$

- Ideally: $q = O(1)$ and $\epsilon(\delta) > 0$, $\forall \delta > 0$. 
[BLR] Lemma

- Let \( \text{Rej}(f) = \text{Prob}_{x, y \in G} [f(x) \cdot f(y) \neq f(x \cdot y)] \)

- Lemma: If \( \text{Rej}(f) < 2/9 \)
  then \( \delta(f, \text{Hom}) = O(\text{Rej}(f)). \)

-Motivated by Program Checking:
  - E.g. to check if (complex) program multiplies matrices correctly:
    - Verify it is linear in each argument
    - Use this to check correctness.
Independently [Babai Fortnow Lund ‘90]

- Multilinearity testing: Is a function \( f: \mathbb{F}^m \rightarrow \mathbb{F} \) essentially a degree 1 polynomial in each of the \( m \) variables?
  - Let \( \text{Rej}(f) = \text{Prob}_\ell |f|_\ell \text{ is not affine} \)
    where \( \ell \) is a random axis parallel line.

- [BFL] Lemma:
  - If \( \text{Rej}(f) < 1/\text{poly}(m) \), then
    \( \delta(f, \text{MultiLin}) = O(\text{Rej}(f)) \).

- Implications to Complexity (precursor to “Probabilistically Checkable Proofs”)

December 2, 2009 IPAM: Invariance in Property Testing
Low-degree testing [Rubinfeld, S. ‘92-’96]

- Is a function $f: \mathbb{F}^m \rightarrow \mathbb{F}$ essentially a polynomial of degree $d$?
  - Let $\text{Rej}(f) = \Pr_{\ell} [f|_{\ell} \text{ is not of degree } d]$ where $\ell$ is a random line (not axis parallel).

- Lemma ([ALMSS]):
  - $\exists \epsilon > 0 \text{ s.t. } \forall d, m, \text{ sufficiently large } F$
    - if $\text{Rej}(f) < \epsilon$
      - then $\delta(f, \text{Degree}-d) = O(\text{Rej}(f))$
Low-degree testing & Derivatives

- Let $f_a(x) = f(x+a) - f(a)$.
- Let $f_{a,b} = (f_a)_b$

- Let $\text{Rej}'(f) = E_{a,x} \left[ I(f_{a,a,a,...}(x)) \right]$
  - where $I(a) = 1$ if $a = 0$ and 0 otherwise.

- Variant of low-degree test implies that if the $(d+1)$st derivative in random direction usually vanishes, then $f$ is close to a degree $d$ polynomial.
Low-degree testing (Strong form)

- Is a function $f: F^m \to F$ essentially a polynomial of degree $d$?
  - Let $\rho(f) = \text{Exp}_l [ \delta(f|_l, \text{Univ-Deg}(d))]$
    where $l$ is a random line.
  - Note: $\text{Rej}(f)/F \leq \rho(f) \leq \text{Rej}(f)$

- Lemma ([ALMSS]):
  - $\exists \epsilon > 0$ s.t. $\forall d, m$, sufficiently large $F$
    \[ \text{if } \rho(f) < \epsilon \]
    \[ \text{then } \delta(f, \text{Degree}-d) = O(\rho(f)) \]
Low-degree testing (Stronger form)

- Is a function $f: \mathbb{F}^m \to \mathbb{F}$ essentially a polynomial of degree $d$?
  - Let $\rho(f) = \text{Exp}_\ell [ \delta(f|_\ell, \text{Univ-Deg}(d))]$
    where $\ell$ is a random line.
  - Note: $\text{Rej}(f)/F \leq \rho(f) \leq \text{Rej}(f)$

- Lemma (Arora + S. ‘97, Raz+Safra ‘97)
  - $\forall d,m, \epsilon > 0$, sufficiently large $F$
    if $\rho(f) < 1 - \epsilon$
      then $\delta(f, \text{Degree-d}) = 1 - O(\epsilon)$
Motivations:

- [BLR] Linearity test: Program checking

- [BFL], [ALMSS]: Probabilistically checkable proofs
  - There exists a format for writing proofs that can be checked for correctness with constant queries and constant error probability
    - Uses low-degree testing & linearity testing.

- [GGR]: Should be studied for algorithm design.
1996-today

- **Graph property testing** [GGR, ..., Alon, Shapira, Newman, Szegedy, Fisher]
  - Almost total understanding of graphical property testing ... Regularity lemma.
  - Graph limits approach ... (Borgs, Chayes, Lovasz, Sos, Szegedy, Vesztergombi)

- **Algebraic Property Testing:**
  - Many stronger results
  - Fewer new properties
    - Low-degree testing over small fields ($F_2$)
Low-degree testing over GF(2)

- [AKKLR] = Alon-Kaufman-Krivelevich-Litsyn-Ron
- Let $F = F_2$
- Is a function $f: F^m \to F$ essentially a polynomial of degree $d$?
  - Let $\text{Rej}(f) = \text{Prob}_A [f|_A \text{ is a degree } d \text{ poly}]$
    - $A$ is a random $(d+1)$-dim. affine subspace.
  - $U_{d+1}(f) = (\frac{1}{2} - \text{Rej}(f))^{2^{-d}}$
- Lemma [AKKLR]
  - $\exists \epsilon > 0 \text{ s.t. If } \text{Rej}(f) < \epsilon \cdot 2^{-d}$
    - then $\delta(f, \text{Degree-}d) = O(\text{Rej}(f))$
      (Very weak “inverse Gowers” theorem)
1996-today

- **Graph property testing** [GGR, ..., Alon, Shapira, Newman, Szegedy, Fisher]
  - Almost total understanding of graphical property testing ... Regularity lemma.
  - Graph limits approach ... (Borgs, Chayes, Lovasz, Sos, Szegedy, Vesztergombi)

- **Algebraic Property Testing:**
  - Many stronger results
  - Fewer new properties
    - Low-degree testing over small fields \( (F_2) \)
My concerns ...

- Why is the understanding of Algebraic Property Testing so far behind?
  - Why can’t we get “rich” class of properties that are all testable?
  - Why are proofs so specific to property being tested.
- What made Graph Property Testing so well-understood?
- What is “novel” about Property Testing, when compared to “polling”?
Example

- 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
    - $\forall f \in P, f(\alpha_1) + \ldots + f(\alpha_k) = 0$.
  - Then $f$ is $(q(k), \epsilon(k,\delta),\delta(k))$-locally testable.

- Inspired by “low-degree” test over $F_2$. Implied all previous algebraic tests (at least in weak forms).
Invariances

- Property $P$ invariant under permutation (function) $\pi: D \rightarrow D$, if
  $$f \in P \Rightarrow f \circ \pi \in P$$

- Property $P$ invariant under group $G$ if for all $\pi \in G$, $P$ is invariant under $\pi$. 
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 $\sim$ Invariant under vertex renaming.

- Algebraic Properties & Invariances?
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.”
Example: Degree $d$ polynomials

- **Constraint:** When restricted to a small dimensional affine subspace, function is polynomial of degree $d$ (or less).
  - $\#\text{dimensions} \leq d/(K - 1)$

- **Characterization:** If a function satisfies above for every small dim. subspace, then it is a degree $d$ polynomial.

- **Single orbit:** Take constraint on any one subspace of dimension $d/(K-1)$; and rotate over all affine transformations.
Some results

- If $P$ is affine-invariant and has $k$-single orbit feature (characterized by orbit of single $k$-local constraint); then it is $(k, \frac{\delta}{k^3}, \delta)$-locally testable.
- Unifies previous algebraic tests (in weak form) with single proof.
Analysis of Invariance-based test

- Property $P$ given by $\alpha_1, \ldots, \alpha_k; \ V \in F^k$

- $P = \{f \mid f(A(\alpha_1)) \ldots f(A(\alpha_k)) \in V, \ \forall \text{ affine } A: K^n \to K^n\}$

- $\text{Rej}(f) = \text{Prob}_A [ f(A(\alpha_1)) \ldots f(A(\alpha_k)) \text{ not in } V ]$

- Wish to show: If $\text{Rej}(f) < 1/k^3,$
  then $\delta(f, P) = O(\text{Rej}(f)).$
BLR Analog

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

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

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

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

- **Step 2: Use above to show \( g \) is well-defined and a homomorphism.**
BLR Analysis of Step 1

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

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

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

- $\text{Vote}_x(A) = \beta$ s.t. $\beta, f(A(\alpha_2))...f(A(\alpha_k)) \in V$ (if such $\beta$ exists)

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

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

Random

$\times$

$A(\alpha_2)$

$A(\alpha_k)$

$B(\alpha_2)$

$B(\alpha_k)$

No Choice

Doesn’t Matter!

December 2, 2009

IPAM: Invariance in Property Testing
Some results

- If $P$ is affine-invariant and has $k$-single orbit feature (characterized by orbit of single $k$-local constraint); then it is $(k, \delta/k^3, \delta)$-locally testable.
  - Unifies previous algebraic tests with single proof.

- If $P$ is affine-invariant over $K$ and has a single $k$-local constraint, then it has a $q$-single orbit feature (for some $q = q(K,k)$)
  - (explains the AKKLR optimism)
Some results

- 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)

- Unfortunately, $q$ depends inherently on $K$, not just $F$ ... giving counterexample to AKKLR conjecture [joint with Grigorescu & Kaufman]

- Linear invariance when $P$ is not $F$-linear:
  - Abstraction of some aspects of Green’s regularity lemma ... [Bhattacharyyya, Chen, S., Xie]
  - Nice results due to [Shapira]
More results

- Invariance of some standard codes (BCH etc.):
  - Have $k$-single orbit property! So duals are testable. [Grigorescu, Kaufman, S.]

- Side effect: New (essentially tight) relationships between $\text{Rej}_{\text{AKKL}}(f) (= \frac{1}{2} + \text{Gowers norm}^{2d})$ and $\delta(f, \text{Degree}-d)$. [with Bhattacharyya, Kopparty, Schoenebeck, Zuckerman]

- One hope: Could lead to “simple, good locally testable code”?
  - (Sadly, not with affine-inv. [Ben-Sasson, S.])

- Still ... other groups could be used? [Kaufman+Wigderson]
Conclusions

- Invariance seems to be a very nice perspective on "property testing" ...

- (Needs Harmonic Analysis 😊)

- Hope: Can lead to interesting, new results?
Thanks