Property Testing and Affine Invariance

Part II

Madhu Sudan
Harvard University
Review of last lecture

- Property testing: Test global property with local inspection.
  - E.g., test if \( m \)-variate function over \( \mathbb{F}_q \) is deg. \( d \) poly.
    - \#coefficients = \( \exp(\min(m, d)) \)
    - query complexity (when \( d \leq \frac{q}{2} \)): \( \text{poly}(d) \)

- Affine-invariant Property: \( P \subseteq \{ f: \mathbb{F}_Q^m \to \mathbb{F}_q \}; \quad Q = q^n \)
  - \( P \) is \( \mathbb{F}_q \)-linear
  - \( P \) is invariant under affine maps \( \mathbb{F}_Q^m \to \mathbb{F}_Q^m \)
  - Generalize low-degree property; Testing results extend, strengthen; captures new properties.
Today

- Positive aspect of “New properties”
  - Lifted codes

- Testability of Lifted Codes
  - Result statements
  - Some proof ideas
(Recall) Lifted Codes

- Base Code \( B \subseteq \{ b : \mathbb{F}_Q^t \rightarrow \mathbb{F}_q \} \) affine-invariant
- \( m \)-dim Lift \( L_m(B) \equiv \{ f : \mathbb{F}_Q^m \rightarrow \mathbb{F}_q \} \)
- Last lecture: Used lifts to construct non-testable codes.
- Today: Use them to construct new, better, testable codes.
Coding Theoretic Objective

- Want codes of (Properties with)
  - High rate (many members)
  - High Distance (pairwise far)
  - Low Locality for Testing/Correcting
    (2-transitive and testable)
- Best known code (pre-2010) w. sublinear locality
  - Bivariate polynomials, w. deg. $k < q$.
  - $P \subseteq \{ f: \mathbb{F}_q^2 \to \mathbb{F}_q \}$;
  - “length”=dim. of ambient space = $q^2$
  - Rate $= \frac{\dim(P)}{\text{length}} = \frac{k^2}{2q^2} < \frac{1}{2}$; locality $\ell = q = \sqrt{\text{length}}$
Locality w. Rate $> \frac{1}{2}$?

- 2010 [Kopparty,Saraf,Yekhanin] “Multiplicity Codes”:
  - Locality = $(\text{length})^\varepsilon$; Rate $\to 1$
  - Not known to be testable!

- 2011 [Viderman] Tensor Product Codes:
  - Locality = $(\text{length})^\varepsilon$; Rate $\to 1$
  - Testable, but not symmetric 😞

- 2014 [Guo,Kopparty,S] Lifted Codes:
  - Locality = $(\text{length})^\varepsilon$; Rate $\to 1$
  - Testable + Symmetric!

- 2015 [Kopparty,Meir,RonZewi,Saraf]:
  - Locality = $(\text{length})^{o(1)}$; Rate $\to 1$
Lifted Reed-Solomon Codes

- **Base Code** \( B \subseteq \{ b : \mathbb{F}_q \to \mathbb{F}_q \mid \deg(b) \leq k = (1 - \delta)q \} \)
- **Lifted Code** \( L_m(B) \subseteq \{ f : \mathbb{F}_q^m \to \mathbb{F}_q \} \);
  - **Rate** = ?
  - **Distance** = ?
  - **Locality** = ? \( q \) (obvious)

- \( m \)-var. deg. \( k \) poly \( \subseteq L_m(B) \Rightarrow \text{Rate} \geq \frac{(1-m\delta)}{m!} ; \text{Dist} \leq \delta ; \)
- **Simple analysis:** \( \text{Dist} \geq \delta - \frac{1}{q} \)
- **Rate:** \( \forall \epsilon > 0, m, \ \exists \delta > 0 \text{ s.t. } \text{Rate} \geq 1 - \epsilon \)
Rate of bivariate Lifted RS codes

- \( B = \{ f \in \mathbb{F}_q[x] \mid \deg(f) \leq k = (1 - \delta)q \}; \ q = 2^s \)
  - Will set \( \delta = 2^{-c} \) and let \( c \to \infty \).
  - Note: \( m \leq k \iff \) one of its \( c \) MSBs is 0.
- \( L_2(B) = \{ f : \mathbb{F}_q[x,y] \mid f|_{y=ax+b} \in B, \forall a,b \} \)
  - When is \( x^i y^j \in C? \)
  - (Will need to look at binary rep’n of \( i, j \).)
Lucas’s theorem & Rate

- Recall: \( r \leq 2 \cdot j \), if \( r = \sum \eta_i 2^i \) and \( j = \sum j_i 2^i \) (\( \eta_i, j_i \in \{0,1\} \)) and \( \eta_i \leq j_i \) for all \( i \).

- Lucas’s Theorem: \( x^r \in \text{supp}\left((ax + b)^j\right) \) iff \( r \leq 2 \cdot j \).

\[
\Rightarrow \text{supp}(x^i(ax + b)^j) \ni x^{i+r} \text{ iff } r \leq 2 \cdot j
\]

- So given \( i, j \); \( \exists r \leq 2 \cdot j \) s. t. \( i + r \pmod q > k \)?

<table>
<thead>
<tr>
<th>i</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>j</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

\[
\Pr_{i,j}[^*] \leq \left(\frac{15}{16}\right)^{\frac{c}{2}}
\]
Aside: Nikodym Sets

- \( N \subseteq \mathbb{F}_q^m \) is a Nikodym set if it almost contains a line through every point:
  - \( \forall a \in \mathbb{F}_q^m, \exists b \in \mathbb{F}_q^m \text{ s.t. } \{a + tb \mid t \in \mathbb{F}_q\} \subseteq N \cup \{a\} \)

- Similar to Kakeya Set (which contain line in every direction):
  - \( \forall b \in \mathbb{F}_q^m, \exists a \in \mathbb{F}_q^m \text{ s.t. } \{a + tb \mid t \in \mathbb{F}_q\} \subseteq K \)

- [Dvir], [DKSS]: \( |K|, |N| \geq \left(\frac{q}{2}\right)^m \)
Proof (“Polynomial Method”)

- Find low-degree poly \( F \neq 0 \) s.t. \( F(b) = 0, \forall b \in N \).
- \( \text{deg}(F) < q - 1 \) provided \( |N| < \binom{m+q-2}{m} \).
- But now \( F|_{L_a} = 0, \forall \) Nikodym lines \( L_a \Rightarrow F(a) = 0 \forall a \), contradicting \( F \neq 0 \).

Conclude \( |N| \geq \binom{m+q-2}{m} \approx \frac{q^m}{m!} \).

- Multiplicities, more work, yields \( |N| \geq \left( \frac{q}{2} \right)^m \).
- But what do we really need from \( F \)?
  - \( F \) comes from a large dimensional vector space.
  - \( F|_L \) is low-degree!
  - Using \( F \) from lifted code yields \( |N| \geq (1 - o(1))q^m \)
    (provided \( q \) of small characteristic).
Testing
Parameters of interest

- Property being tested: $P \subseteq \{ f : F_Q^m \rightarrow F_q \}$
- Locality of test $\ell$
- Rejection ratio: $\epsilon \equiv \min_f \frac{\Pr[\text{Rejecting } f]}{\delta(f,P)}$
- Robustness: $\alpha \equiv \min_f \frac{\delta(f|_{\text{local}}, P|_{\text{local}})}{\delta(f,P)}$
- Ideally should compare $\frac{\ell}{\epsilon}$ (or $\frac{\ell}{\alpha}$)
Important Definition

- **ℓ-single orbit Property**: \( P \subseteq \{g : F^m_Q \rightarrow F_q\} \) is ℓ-single orbit if there exists an ℓ-local constraint \( C \) s.t.
  \[
  f \in P \iff \forall \text{ affine } A : F^m_Q \rightarrow F^m_Q, \quad f \circ A \text{ satisfies } C
  \]

- (Single constraint + its orbit characterize \( P \))

- Lifted Property is \( Q^t \)-single orbit.

- Most known algebraic properties had single orbit tests.
  - Exceptions, pre-2008: Sparse Properties
  - Post-2008: Sparse properties are single-orbit.
Testing Theorems

- **Thm 1 [KS08]:** $\ell$-single orbit property is $\ell$-locally testable with $\epsilon \approx \frac{1}{\ell^2}$

- **Thm 2 [HRS’13]:** $\forall Q \exists \epsilon$ s.t. $\forall t, \forall B \subseteq \{b: F^t_Q \rightarrow F_q\}$, $\forall m L_m(B)$ is $Q^t$-locally testable with soundness $\epsilon$ (Works for lifted codes. Soundness independent of $t$. But depends on $Q$)

- **Thm 3 [GHS’15]:** $\forall \delta \exists \alpha$ s.t. if $B \subseteq \{b: F^t_Q \rightarrow F_q\}$ is a code of distance $\delta$ then $L_m(B)$ is $Q^{2t}$-locally testable with robustness $\alpha$ (Generalizes low-degree testing. Stronger. Works even when $d \rightarrow q$)
\( \ell \text{-single-orbit} \implies \ell \text{-locally testable} \)

- \( P \subseteq \{ F_q^m \to F_q \} \) given by \((\alpha_1, \ldots, \alpha_\ell; V \leq F_q^\ell)\)
  - \( P = \{ f \mid \forall A, \langle f(A(\alpha_1)), \ldots, f(A(\alpha_\ell)) \rangle \in V \} \)

- "Auto-correction" based-proof:
  - Fix \( f \) s.t. \( \rho \equiv \Pr[\text{Rejecting } f] \) small
  - Define \( g \) from \( f \) locally
  - Prove \( g \) close to \( f \)
  - Prove \( g \) satisfies constraint \( \forall A \)

- Only possible
  \[ g(x) = \arg\max_\beta \left\{ \Pr_{A : A(\alpha_1) = x} [\langle \beta, f(A(\alpha_2)), \ldots, f(A(\alpha_\ell)) \rangle \in V] \right\} \]
Analysis (contd.)

- \( \text{Vote}_A(x) = \beta \) s.t. \( \langle \beta, f(A(\alpha_2)), \ldots, f(A(\alpha_\ell)) \rangle \in V \)
- \( g(x) = \text{majority}_{A:A(\alpha_1)=x} \{\text{Vote}_A(x)\} \)
- Key Lemma:
  \[ \forall x, \Pr_{A,B:A(\alpha_1)=B(\alpha_1)=x} [\text{Vote}_A(x) = \text{Vote}_B(x)] \geq 1 - 2\ell\rho \]
- \([\text{BLR, GLR, RS, AKLLR, KR, JPRZ}]\) Proofs: Build a miracle \( \ell \times \ell \) matrix \( M \):
  - Rows indexed by \( A_1 = A, A_2, \ldots, A_\ell \)
  - Columns by \( B_1 = B, B_2, \ldots, B_\ell \)
  - \( M_{ij} = A_i(\alpha_j) = B_j(\alpha_i) \ \forall i,j \)
  - Typical row/column random

Why does such a matrix exist?
Matrix Magic explained

- Wlog $C(\alpha_1), \ldots, C(\alpha_t)$ independent; rest determined when $C$ random (affine).

\[
\begin{array}{|c|c|c|}
\hline
x & A(\alpha_2) \ldots A(\alpha_t) & \ldots & A(\alpha_\ell) \\
\hline
\vdots & \vdots & \ddots & \vdots \\
B(\alpha_2) & \vdots & & \vdots \\
B(\alpha_t) & & & \vdots \\
B(\alpha_\ell) & & & \vdots \\
\hline
\end{array}
\]

Random

Determined

Overdetermined?

No! Linear algebra!
Theorem 2: Context & Ideas

- Thm 2 [HRS’13]: \( \forall Q \exists \varepsilon \text{ s.t. } \forall t, \forall B \subseteq \{ b: F_Q^t \to F_q \}, \forall m L_m(B) \) is \( Q^t \)-locally testable with soundness \( \varepsilon \)

- Test: Obvious one:
  - Pick random \( t \)-dim subspace \( A \).
  - Accept iff \( f|_A \in B \)
  - Claim: \( \Pr_{A}[f|_A \notin B ] \geq \varepsilon \cdot \delta(f, L_m(B)) \)

- [BKSSZ] Special case: \( Q = 2, B = \{ b| \sum_a b(a) = 0 \} \);
  - \( L_m(B) = m \text{-var deg } t - 1 \text{ poly} \)
Theorem 2 ($Q = q = 2$, contd.)

- Alternative view of test:
  - $f_a(x) \triangleq f(x + a) - f(a)$ “discrete derivative”
  - $\deg(f) < t \Rightarrow \deg(f_a) < t - 1$
  - $\ldots \Rightarrow \deg(f_{a_1, \ldots, a_t}) < 0 \Rightarrow f_{a_1, \ldots, a_t} = 0$
  - Rejection Prob. $\triangleq \rho(f) = \Pr_{a_1 \ldots a_t} [f_{a_1 \ldots a_t}] \neq 0$
  - $(1 - 2\rho(f))^{\frac{1}{2d}}$ special case of “Gowers norm”
- Strong “Inverse Conjecture” $\Rightarrow \rho(f) \rightarrow \frac{1}{2}$ as $\delta(f, L_m(B)) \rightarrow \frac{1}{2}$.
- Falsified by [LovettMeshulamSamorodnitsky],[GreenTao]:
  - $f = Sym_t(x_1 \ldots x_n); t = 2^s$;
  - $\delta(f, L_m(B)) = \frac{1}{2} - o_n(1); \rho(f) \leq \frac{1}{2} - 2^{-7}$
Theorem 2 (contd.)

- So $\rho(f) \to \frac{1}{2}$ as $\delta(f) \to \frac{1}{2}$; but is $\rho(f) > 0$?
- Prior to [BKSSZ]: $\rho(f) > 4^{-t} \cdot \delta(f)$
- [BKSSZ] Lemma: $\rho(f) \geq \min\{\epsilon, 2^t \cdot \delta(f)\}$
- Key ingredient in proof:
  - Suppose $\delta(f) > 2^{-t}$
  - On how many “hyperplanes” $H$ can $\deg(f|_H) < t$?
Hyperplanes

\[ \delta(f) > 2^{-t} \Rightarrow \# \left\{ H \text{ s.t. } \deg(f|_H) < t \right\} \leq ? \]

1. \( \exists H \text{ s.t. } \deg(f|_H) \geq t \): defn of lifting.
2. \( \Pr_{H}[\deg(f|_H) \geq t] \geq \frac{1}{q} \iff \deg_{x_i}(f) < q - 1. \)
3. … What we needed: \( \# \left\{ H \text{ s.t. } \deg(f|_H) < t \right\} \leq O(2^t) \)
General Lifted Properties

- Lemma: \( \forall Q \exists c \text{ s.t. if } \delta(f) \geq Q^{-t} \text{ then } \#\{H \text{ s.t. } f|_H \in L_{m-1}(B)\} \leq c \cdot Q^t \)

- Ingredients in proof:
  - \( q = 2 \): Simple symmetry of subspaces, linear algebra.
  - \( q = 3 \): Roth’s theorem ...
  - General \( q \): Density Hales-Jewett theorem
Theorem 3: Context

- Thm 3 [GHS’15]: \( \forall \delta \exists \alpha \text{ s.t. if } B \subseteq \{b: F_Q^t \to F_q\} \text{ is a code of distance } \delta \text{ then } L_m(B) \text{ is } Q^{2t}\text{-locally testable with robustness } \alpha \)

- Test – not most natural one!
  - Most natural: Inspect \( f|_A \) for \( t\)-dim \( A \)
  - Our test: Inspect \( f|_A \) for \( 2t\)-dim \( A \)
  - Based on [Raz-Safra], [BenSassonS], ..., [Viderman]

- Need to show: \( \forall f \mathbb E_A[\delta(f|_A, B)] \geq \delta(f, L_m(B)) \)
- Not previously known even when \( t = 1 \) and \( B = \{b \mid \deg(b) \leq d\} \) with \( d = (1 - \epsilon)q \)
Robust Testing of Lifted Codes

- For simplicity $B \subseteq \{b: \mathbb{F}_q \to \mathbb{F}_q\}$ $(t = 1)$.
- General geometry + symmetry $\Rightarrow$ Robust analysis with $m = 4 \Rightarrow$ All $m$

- How to analyze robustness of the test for constant $m$?
Tensors: Key to understanding Lifts

- Given \( F \subseteq \{ f : S \rightarrow F_q \} \) and \( G \subseteq \{ g : T \rightarrow F_q \} \),
  \[
  F \otimes G = \{ h : S \times T \rightarrow F_q \mid \forall x, y, h(\cdot, y) \in F \& h(x, \cdot) \in G \}
  \]

- \( F \otimes^m = F \otimes F \otimes \cdots \otimes F \)

- \( L_m(B) \subseteq B \otimes^m \); \( L_m(B) = \bigcap_T T(B \otimes^m) \) (affine map \( T \))

- \((m - 1)\)-dim test for \( B \otimes^m \): Fix coordinate at random and test if \( f(\cdots, x_i, \cdots) \in B \otimes^{m-1} \)

- [Viderman’13]: Test is \( \alpha_{\delta(B), m} \)-robust.

- Hope: Use \( L_m(B) = \bigcap_T T(B \otimes^m) \) to show that testing for random \( T(B \otimes^m) \) suffices;
  - \( \delta_A(f), \delta_B(f) \) small \( \neq \delta_{A \cap B}(f) \) small \( \otimes \)
Actual Analysis

- Say testing $L_4(B)$ by querying 2-d subspace.
- Let $P_a = \{f \mid f|_{\text{line}} \in B \text{ for all coordinate parallel lines, and lines in direction } a\}$
- $L_4(B) = \cap_a P_a$;
- $P_a$ not a tensor code, but modification of tensor analysis works!
- $\cup_a P_a \subseteq B^\otimes 4$ is still an error-correcting code.
- So $\delta_{P_a}(f), \delta_{P_b}(f)$ small $\Rightarrow \delta_{P_a \cap P_b}(f)$ small!
- Putting things together $\Rightarrow$ Theorem 3.
Wrapping up

Affine-Invariance

- Fruitful abstraction of low-degree property
- Many open questions
  - Characterize $O(1)$-locally testable properties.
  - Rich properties beyond lifting?
  - Beat polynomials for $\ell = \text{polylog}(\text{length})$

Invariance in Property Testing

- Pursue in other contexts?
- Other unifying generalizations?
Thank You