Locality in Coding Theory II: LTCs

Madhu Sudan
Harvard

Outline of this Part

- Three ideas in Testing:
  - Tensor Products
  - Composition/Recursion
  - Symmetry (esp. affine-invariance)

Part 0 - A Definition: Robust Testing

Recursive testing and Robustness

- Generic test for code $C \subseteq \{g: D \to \mathbb{F}_q\}$:
  - Given $f: D \to \mathbb{F}_q$, pick some set $S \subseteq D$, and verify $f|_S \in B$.
  - Test defined by distribution over S and B
  - Often, B itself an error-correcting code!
- Robust analysis (informally):
  - f far from $C \Rightarrow$ usually $f|_S$ far from B!

    (Stronger conclusion than just $\neg(f|_S \in B)$)

Recursive testing and Robustness-II

- Formally: C is α-robust w.r.t. B-test if

$$\mathbb{E}_S[\delta(f|_S, B)] \geq \alpha \cdot \delta(f, C)$$

  - α-robust $\Rightarrow$ α-sound
  - ϵ-sound $\Rightarrow$ $\frac{\epsilon}{\ell}$-robust
- Recursive testing:
  - If C is α-robust wrt B-test and B is (ϵ, ℓ)-LTC, then C is $(\alpha \cdot \epsilon, \ell)$-LTC
- Goal from now: Robust testing.

Part 1: Tensor Product Codes

Tensor Product Codes

- Given $B \subseteq \{f: S \to \mathbb{F}_q\}$ and $C \subseteq \{g: T \to \mathbb{F}_q\}$,
$B \otimes C \stackrel{\text{def}}{=} \{h: S \times T \to \mathbb{F}_q \mid \forall x, y, h(\cdot, y) \in B \ \& \ h(x, \cdot) \in C\}$
- Is $B \otimes C$ non-empty?
  - Miracle of linear algebra:
$$\dim(B \otimes C) = \dim(B) \cdot \dim(C)$$
  - (Not to be dismissed lightly! Fails miserably even for additive codes.)
- $B^{\otimes m} \stackrel{\text{def}}{=} B \otimes B \otimes \cdots \otimes B$

Tensor Product Codes - 2

- Locality from tensors: If $|S| = n$ and $N = n^m$ then
  - Block-length$\left(B^{\otimes m}\right) = N$;
  - Constraints of length $N^{\frac{1}{m}}$ (axis-parallel lines)
- Candidate test: "Lines test"
  - Pick $i \in [m]$ and $a_{-i} \in S^{m-1}$ uniformly. Verify $f|_{x_{-i}:=a_{-i}} \in F$.
  - Sound? Robust? Hope $\alpha = \alpha(m, \delta(B))$.
  - Question raised in [Ben-Sasson+S '04].
  - Answered negatively by [P. Valiant '05].

Testing Tensor Products

- Proposed by [Ben-Sasson+S'04]. Many strengthenings since, with final (?) word due to [Viderman '11]
- Test 1: Test B^m using $(m-1)$-dimensional projections!
- Lemma: [Viderman '11] $\forall m \geq 3, \delta, \exists \alpha > 0$ such that if $\delta(B) \geq \delta$ then B^m is α-robust wrt B^{m-1}-test.
- Test 2: Test B^m using 2-dimensional projections!
- Theorem: $\forall m, \delta, \exists \beta > 0$ s.t. if $\delta(B) \geq \delta$ then B^m is β-robust wrt B^2-test
- Proof: Let α_m be robustness of (m-1)-dimensional test from Lemma. Then $\beta = \alpha_m \cdot \alpha_{m-1} \cdots \alpha_2$. QED.

Proof of Lemma ($m = 3$)

- Reinterpretation of robustness:
  - Pick random point $x \in S^3$
  - Pick random plane $p \ni x$
  - Accept if $f(x)$ agrees with best C^2 codeword on p
- Analysis:
  - x BAD if three planes disagree.
  - Line/plane BAD if contain many BAD points
  - Pr[test rejects | x BAD] $\geq \frac{1}{3} \Rightarrow$ Pr[x BAD] small
  - x BAD $\Rightarrow$ some line containing x BAD $\Rightarrow$ some plane containing x BAD
  - Throw away BAD planes; Rest of S^3 is clean $\Rightarrow$ consistent with some codeword of C^3

Testing via Tensor Products

- Starting with base code of rate R,
  - get Code of rate $R^{\frac{1}{\epsilon}}$, distance $(1-R)^{\frac{1}{\epsilon}}$ of length N, testable with locality $\ell(N) = N^{\epsilon}$
- But central ingredient in much better constructions!
  - E.g., Apply [KMR-ZS'16a] and get code of Rate R, distance $1 - R - \epsilon$, length N, locality $\ell(N) = N^{o(1)}$
- Also central ingredient in analyses of non-tensor codes!

Part 2: Testing & Composition

Zig-Zag Approach

- Pioneered by [Reingold-Vadhan-Wigderson]
  - Identify two parameters (a, b): (say we want to increase both).
  - Identify two operations:
    - Zig: $(a, b) \to (A, \beta)$ [$\alpha \leq a \leq A$; $\beta \leq b \leq B$]
    - Zag: $(a, b) \to (\alpha, B)$
  - If we are lucky:
    - Zig $\circ$ Zag: $(a, b) \to (A', B')$
- Remarkably successful approach!
  - Expanders – [RVW, CRVW]
  - Logspace connectivity – [Reingold]
  - PCP – [Dinur]

Zig-Zag LTC Construction [KMR-ZS'16b]

- Zig-Operation: Tensoring
  - Length Squares ✓
  - Robustness Reduces by O(1) factor ✓
  - Distance Squares ✗
- Zag-Operation: Alon-Luby Transform
  - Distance Increases ✓
  - Robustness decreases ✗
  - Length no worse ✓
- Combination:
  - Length Squares ✓
  - Distance Maintained! ✓
  - Robustness smaller by constant factor ✓

Zig-Zag LTC Theorem

- [KMR-ZS'16] Theorem: For every $R > 0$, for infinitely many n there exists codes of length n of rate R, distance $1 - R - o(1)$ that are $\left(\log^{\log n} n, \frac{1}{2}\right)$-LTCs

Part 3: Testing by Symmetries

Motivation

- If you wish to test natural codes (linearity, low-degree, …) how to do it?
- What if you want code to be LTC + LDC?

Testing via Symmetries

- Idea/Hope:
  - If code designed to be “symmetric” and has local constraints, then it must be locally testable.
- Actuality:
  - Not true completely generally
  - But with some mild restrictions.
  - Weakly true for “single-orbit properties”
  - Strongly true for “lifted codes”
  - Corollaries: Linearity testing, Low-degree testing …

Lifting Results

- Lifting:
  - Base Code $B \subseteq \left\{b: \mathbb{F}_q^t \to \mathbb{F}_q\right\}$
  - m-dim. Lift
    $L_m(B) = \left\{f: \mathbb{F}_q^m \to \mathbb{F}_q \middle| f|_A \in B \ \forall t - \text{dim affine } A\right\}$
- Theorems:
  - $\forall q \ \exists \epsilon \ \forall B, t, m \ L_m(B)$ is (q^t, ϵ)-LTC
  - $\forall \delta \ \exists \alpha \ \forall q, t, m, B$, if $\delta(B) \geq \delta$ then $L_m(B)$ is α-robust wrt B^{2t}-test.

Single-Orbit Codes

- ℓ-Constraint:

$$K = (S, V);\ S \subseteq \mathbb{F}_q^m, V \subseteq \left\{b: S \to \mathbb{F}_q\right\}, |S| = \ell$$

  - $f: \mathbb{F}_q^m \to \mathbb{F}_q$ satisfies K if $f|_S \in V$
- ℓ-single orbit: $C \subseteq \left\{g: \mathbb{F}_q^m \to \mathbb{F}_q\right\}$ is ℓ-single orbit if there exists an ℓ-constraint K s.t.

$$f \in P \Leftrightarrow \forall \text{ affine } A: \mathbb{F}_q^m \to \mathbb{F}_q^m, \qquad f \circ A \text{ satisfies } K$$

- Lifted Property is q^t-single orbit;
- Single-orbit with S=subspace is "Lifted".
- $\exists$ natural properties that are single-orbit, but not Lifted: e.g. deg ≤ 1:

$$(S = \{0, e_1, e_2, e_1 + e_2\}, V = (f: f(e_1) - f(0) = f(e_1 + e_2) - f(e_2))$$

Testing Single-Orbit Codes

- Theorem: $C \subseteq \{f: \mathbb{F}_q^m \to \mathbb{F}_q\}$ is ℓ-single-orbit $\Rightarrow C$ is $\left(\ell, O\left(\ell^{-2}\right)\right)$ –LTC

- Extremely clean and general statement
- Unifies many of the "first" tests of properties. [BLR, GLRSW, RS, AKKLR, KR, JPRZ].
- Clean simple proof.

ℓ-single-orbit $\Rightarrow$ ℓ-locally testable

- $C \subseteq \{\mathbb{F}_q^m \to \mathbb{F}_q\}$ given by $(S = \{\alpha_1, \ldots, \alpha_\ell\}, V)$:
$$P = \{f \mid \forall A, (f \circ A)|_S \in V\}$$
- "Self-correction" based-proof:
  - Fix f s.t $\rho \stackrel{\text{def}}{=} \Pr[\text{Rejecting } f]$ small
  - Define g from f locally
  - Prove g close to f
  - Prove g satisfies constraint $\forall A$
- Only possible

$$g(x) = \text{argmax}_\beta \left\{ \Pr_{A:A(\alpha_1)=x} [\langle \beta, f(A(\alpha_2)), \ldots, f(A(\alpha_\ell)) \rangle \in V] \right\}$$

Analysis (contd.)

- $\mathrm{Vote}_A(x) = \beta \; s.t. \langle \beta, f\big(A(\alpha_2)\big), \ldots, f(A(\alpha_\ell))\rangle \in V$
- $g(x) = \mathrm{majority}_{A:A(\alpha_1)=x}\{\mathrm{Vote}_A(x)\}$
- Key Lemma:

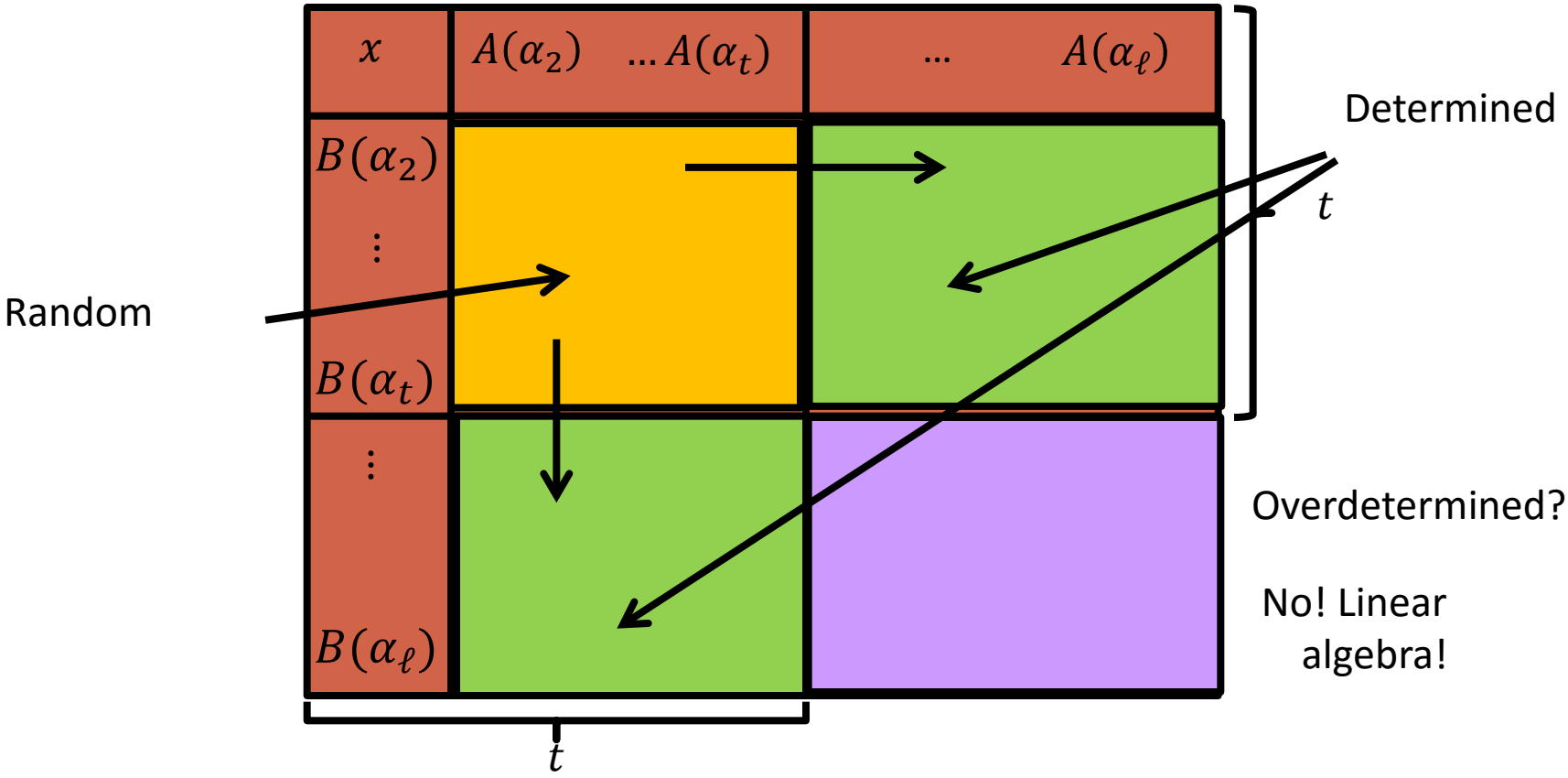
$$\forall x, \Pr_{A,B:A(\alpha_1)=B(\alpha_1)=x}[\mathrm{Vote}_A(x) = \mathrm{Vote}_B(x)] \geq 1 - 2\ell\rho$$

- [BLR,GLRSW,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 $L(\alpha_1), \ldots, C(\alpha_t)$ independent; rest determined when C random (affine).



Robust testing of Lifted Codes

- Thm [GHS'15]: $\forall \delta\ \exists \alpha$ s.t. if $B \subseteq \left\{b: \mathbb{F}_q^t \to \mathbb{F}_q\right\}$ is a code of distance δ then $L_m(B)$ is α-robust wrt B^2-test.
- 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 ⇒

  Robust analysis with $m = 4 \Rightarrow$ All m

- How to analyze robustness of the test for constant m?

Tensors: Key to understanding Lifts

- Insight: $L_m(B) = \cap_T T\left(B^{\otimes m}\right)$
- Wishful Approach:
  - Test verifies $\delta\left(f, T\left(B^{\otimes m}\right)\right)$ small for random T
  - Maybe can combine this?
- Approach Fails
  - $\delta_A(f), \delta_B(f)$ small $\not\equiv$ $\delta_{A\cap B}(f)$ small ☹

Actual Analysis

- Say testing $L_4(B)$ by querying 2-d subspace.
- Let $P_a = \{f \mid f|_{\text{line}} \in B$ 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 ⇒ Theorem.

Wrapping up

- Covered:
  - LTCs and LDCs in high-rate regime.
  - Many new developments: Simple, but surprising!
- Not Covered:
  - LTCs and LDCs in low-query regime:
    - [Yekhanin,Efremenko,Dvir-Gopi]: 3-query $\mathbb{F}_2$, 2-query $\mathbb{F}_2^t$
    - [Dinur, Meir, Viderman]: 3-query LTCs, Rate = 1/polylog n
- Open:
  - LTCs + LDCs with $\ell(n) = \text{polylog}\, n$: Can you beat multivariate polynomials?

Thank You