2-Transitivity Is Insufficient For Local Testability

Note Title 3/29/2008

Madhu Sudan (MIT)

Joint work with Elena Grigorescu (MIT)

Tali Kaufman (IAS & MIT)

Locally Testable Codes (LTC)

$C \subseteq \{0,1\}^n$ is an LTC if it is a

(1) Linear Code: (a) $\forall\ x, y \in C \quad x+y \in C$

& (b) $\delta(x,y) \triangleq \Pr_i[x_i \neq y_i] \geq \delta_0$.

(2) Locally Testable: $\exists$ prob. alg. T (tester) that makes q-queries into oracle for $r \in \{0,1\}^n$

and (a) Accepts $r \in C$ w.p. 1.

(b) Rejects r s.t. $\delta(r, C) \geq \frac{\delta_0}{2}$ w.p. ϵ

[δ_0, ϵ, q independent of n]

Some Known Examples

1. Hadamard Codes — 3-locally testable.
   (Evaluation of homogenous linear polynomials)
2. PCP-based constructions — 3-locally testable.
   ([Goldreich+S., BGHSV, Ben-Sasson+S., Dinur])
   (complex).
   Goldreich+S., BGHSV, Ben-Sasson+S.: poly-based; Dinur: other
3. Reed-Muller Codes — 2^d-locally testable
   (Evaluations of deg d poly. over $\mathbb{F}_2$)
4. Dual-BCH codes — t-locally testable.
   (Duals of t-BCH codes)

Any general sufficient conditions?

1. Every sparse, high-distance code is testable

   [Kaufman + Litsyn, Kaufman + S.]

   ... Alas - does not give any dense codes!

2. [AKKLR] Maybe suffices to have
   ① Small "dual distance".
   ② "2-transitivity".

   ?

Dual Distance?

- $C^{\perp} = \{ y \in \{0,1\}^n \mid \langle x, y \rangle = 0 \quad \forall x \in C \}$
- [Ben-Sasson, Harsha, Raskhodnikova]: Only test for membership in linear code C is to pick $y \in C^{\perp}$ and verify $\langle r, y \rangle = 0$

  Locality = $wt(y) = |\{i \mid y_i = 1\}|$

Dual Distance (continued)

- Dual Distance = $\min_{y \in C^{\perp} \setminus \{0\}} \{wt(y)\}$;

- Code has q-local tester $\Rightarrow$ $Dist(C^{\perp}) \leq q$
- [B-S, H, R]: $\exists$ codes with $Dist(C^{\perp}) \leq q$

  but not $o(n)$-locally testable

  (Not sufficient)

2. Transitivity

- Potential criticism of [BS, H, R] theorem: C has no "symmetries"
- [AKKLR]: Lets insist on C having some "symmetry".
- C invariant under permutation $\pi : [n] \to [n]$ if $\forall \; c = c_1 \dots c_n \in C$, $c_{\pi(1)} c_{\pi(2)} \dots c_{\pi(n)} \in C$.
- $Aut(C) = \{\pi \mid C \text{ invariant under } \pi\}$

2 Transitivity

C is 2-transitive if $\forall\ i_1 \neq i_2,\ j_1 \neq j_2 \in [n]$

$\exists\ \pi \in Aut(C)$ s.t. $\pi(i_1) = j_1$

and $\pi(i_2) = j_2$

[AKKLR] Conjecture: $\forall k, \exists q$ s.t. $\forall C \subseteq \{0,1\}^n$

$\left.\begin{array}{l} dist(C^\perp) \leq k \\ \& \ C \text{ is 2-transitive} \end{array}\right\} \Rightarrow C$ is q-locally testable.

Our Theorem $\exists\, k(\delta),\ \forall\, q,\ \exists\, C$ s.t.

$$\left\{\begin{array}{l} \text{dist}(C^{\perp}) \le k \\ C \text{ is 2transitive} \end{array}\right\} \text{ but } C \text{ is not } q\text{-locally testable}$$

$\Uparrow$ [BS, H, R]

Lemma $\forall\, q,\ \exists\, C \subsetneq D \subseteq \{0,1\}^n$

$$\left\{\begin{array}{l} \text{dist}(D^{\perp}) \le \delta \\ C \text{ is 2 transitive} \end{array}\right\} \text{ and } \quad y \in C^{\perp},\ \text{wt}(y) \le q \Rightarrow y \in D^{\perp}$$

The Counterexample

Given q, • Pick $s > 2q$, $n = 2^s$.

• Let $K = \mathbb{F}_n$

$$C_\ell = \left\{ \langle f(x) \rangle_{x \in K} \;\middle|\; \exists\, \gamma, \beta_0, \beta_1, \ldots \beta_\ell \text{ s.t. } f(x) = \text{Trace}\left(\gamma + \beta_0 x + \sum_{i=1}^{\ell} \beta_i x^{2^i+1}\right) \right\}$$

$$C = C_q \quad ; \quad D = C_s$$

$$\text{Trace}(z) = z + z^2 + z^4 + \cdots + z^{2^{s-1}}$$

Motivation - I : 2 Transitivity ?

- Only known + broad class of 2-transitive codes [Kaufman + S.]

$$\mathcal{F} \subseteq \{ f : K^m \to F \}, \quad K \supseteq F \text{ fields}$$

- $\mathcal{F}$ is F-linear : $\forall f, g \in \mathcal{F}$, $\alpha, \beta \in F$

$$\alpha f + \beta g \in \mathcal{F}$$

- $\mathcal{F}$ is affine-invariant : $\forall f \in \mathcal{F}$, affine $A : K^m \to K^m$

$$f \circ A \in \mathcal{F}.$$

Claim: $\mathcal{F}$ is affine-invariant $\Rightarrow$ $\mathcal{F}$ is 2-transitive.

Affine-Invariant Properties K? F?

$\mathcal{F} \subseteq \{K^m \to F\}$, affine-invariant

$\Leftrightarrow$

$\mathcal{F} \subseteq \{L \to F\}$ affine-invariant $(L = \mathbb{F}_{|K|^m})$

$\Rightarrow$ if counterexample exists, $m = 1$.

Might as well choose: $F = \mathbb{F}_2$, $K = \mathbb{F}_n$, $m = 1$.

Good for choice of code C

$\mathcal{F} \subseteq \{ \mathbb{F}^m \to \mathbb{F} \}$, linear + affine-invariant

$\Rightarrow$ AKKLR conjecture is true !! [Kaufman + S.]

Good for choice of code D

Idea: 1. Start with code $D \subseteq \{ F^s \to F \}$ testable

2. View $D \subseteq \{ K \to F \}$ $\left(K = \mathbb{F}_{2^s} \right)$

3. Pick C arbitrary / random / wierd subcode of D

(but affine-invariant)

Natural Choice for D

1. Try D = linear functions from $\mathbb{F}^s \to \mathbb{F}$

   ... doesn't work ☹

2. D = quadratic functions from $\mathbb{F}^s \to \mathbb{F}$ } RM(2)

   ... did work .... ☺

Functions from $K \to F$

Essentially generated by $b_d(x) \triangleq \text{Trace}(x^d)$

Properties of Trace

1. $\text{Trace}(x+y) = \text{Trace}(x) + \text{Trace}(y)$
2. $\text{Trace}(a \cdot x) = 0 \quad \forall x \in K \quad \Rightarrow \quad a = 0$

Reed-Muller (2)

1. $D = \{ \langle f(x_1 \cdots x_s) \rangle_{x_1 \cdots x_s \in \mathbb{F}_2} \mid f \text{ of degree } 2 \}$

$= \{ \langle \text{Trace}(p(x)) \rangle_{x \in K} \mid p \text{ univ. poly in } K[x]$ supported on $\{1, x, x^3, x^5, x^9, x^{17}, \ldots\}\}$

(x^{2^k+1})

2. $\forall w, x, y, z \in K$,

$f \in D \iff \sum_{v \in \text{SPAN}(x,y,z)} f(v+w) = 0$

The Code C

1. 1st Try: $C = \{ \text{Trace}(\gamma + \beta_0 x + \beta_1 x^3) \mid \gamma, \beta_0, \beta_1 \}$
   - Affine-Invariant !
   - Unfortunately C is locally-testable ! (morning 1 result).
2. Same problem with any other sparse collection of monomials.
3. $C = C_q = \{ \text{Trace}(\gamma + \beta_0 x + \sum_{i=1}^{q} \beta_i x^{2^i+1}) \mid \gamma, \beta_0, \dots \beta_q \}$

   Works !!

Proof of Lemma

- $C = C_q = \left\{ \text{Trace}\left(\gamma + \beta_0 x + \sum_{i=1}^{q} \beta_i x^{2^i+1} \right) \;\middle|\; \gamma, \beta_0, \cdots \beta_2 \right\}$
- D = Reed-Muller (2)

Claims to be checked

1. C, D linear ;
2. C affine-invariant
3. $D^\perp$ has weight 8 codeword
4. $C \subsetneq D$

5. Every weight $< q$ word in $C^\perp$ is also in $D^\perp$.

Proof of 5. Assume otherwise; $\exists\ \alpha_1 \dots \alpha_q \in K$, $g \in D$

s.t. $g(\alpha_1) + \cdots g(\alpha_q) \neq 0$

but $f(\alpha_1) + \cdots + f(\alpha_q) = 0$

$\forall f \in C.$

Step 1: $\exists\ b_1 \dots b_q \in K$ & $\{\lambda_{ij}\}_{0 \le i \le j \le q} \neq \bar{0}$ ($\lambda_{ij} \in \{0,1\}$)

(F-linearly independent)

s.t. $\forall\ f \in C$

$$\sum_{i,j} \lambda_{ij} f(b_i + b_j) = 0$$

Step 2: $\exists$ non-empty graph $G = ([q], E)$ (& $b_1 \dots b_q$ linearly ind.)

$$\sum_{(i,j) \in E} \left(b_i^{2^\ell} b_j + b_j^{2^\ell} b_i \right) = 0 \qquad \forall \ell \in [q]$$

Step 3: $\exists$ $b_1 \dots b_q$ linearly ind.; and $c_1 \dots c_q \in K$ (not all zero)

s.t. $$\sum_{i=1}^{q} c_i b_i^{2^\ell} = 0 \qquad \forall \ell$$

Step 4: $\exists$ contradiction ....

Conclusions

- Disproved the conjecture
- But only in letter not in spirit.
- **Possibility 1:** C linear, 2-transitive,

  and $\text{span}\left(C^{\perp} \cap \{ wt(y) \leq k \} \right) = C^{\perp}$

  $\Rightarrow C$ is q-locally testable.
- **Possibility 2:** Above when $C \subseteq \{K \to F\}$ is affine-invariant.
- **Possibility 3** = Possibility-2 and NOT (Possibility-2)