Lecture 20

TODAY

- LOCAL DECODABILITY / CORRECTABILITY
  - Example: Hadamard Codes
    Reed Muller Codes
- LOCAL TESTABILITY
  - Hadamard Code
  - RM Codes
- PCPs & LDCs & LTCs.

Local Decodability

Defn: $C \subseteq \Sigma^n$ is (ℓ, ϵ)- locally correctible

if $\exists$ Decoder D s.t.

$\forall g \in \Sigma^n$ s.t. $\exists f \in C$ $\delta(f,g) < \epsilon$

$\forall x \in [n]$

randomized alg. $\rightarrow$ $D^g(x)$ makes ℓ- queries into g

& outputs $f(x)$ w.p. $> 1/2$

Example: Hadamard code $\mathcal{H}_n \subseteq \{f : \mathbb{F}_2^n \to \mathbb{F}_2\} \cong \mathbb{F}_2^{2^n}$

- $\mathcal{H}_n = \left\{ f : \mathbb{F}_2^n \to \mathbb{F}_2 \;\middle|\; \begin{array}{l} \exists \alpha_1 .. \alpha_n \in \mathbb{F}_2 \text{ s.t.} \\ \forall x_1 .. x_n \quad f(x) = \sum \alpha_i x_i \end{array} \right\}$

- Local Charaterization of $\mathcal{H}_n$

$$f \in \mathcal{H}_n \iff \forall x, y \in \mathbb{F}_2^n, \; f(x) + f(y) = f(x+y)$$

Local Decoding Problem

- Given ① oracle access to $g: \mathbb{F}_2^n \to \mathbb{F}_2$
  s.t. $\exists\, f \in H_n$ with $\delta(f, g) < \epsilon$

  ② $x \in \mathbb{F}_2^n$

Need to compute: $f(x)$

Local Decoder:

- $D^g(x)$: • Pick $y \in \mathbb{F}_2^n$ at random
  - • Output $g(x+y) - g(y)$ $\boxed{\ell = 2}$

Analysis:

Claim: $\Pr[D^g(x) \neq f(x)] < 2\epsilon$

Proof: $\Pr_y[g(y) \neq f(y)] < \epsilon$

$\forall x \quad \Pr_y[g(x+y) \neq f(x+y)] < \epsilon$

$\Pr_y[\underbrace{g(x+y) \neq f(x+y) \text{ OR } g(y) \neq f(y)}_{(*)}] < 2\epsilon$

$\neg(*) \Rightarrow g(x+y) - g(y) \underset{\text{logically}}{=} f(x+y) - f(y) \underset{f \in H_n}{=} f(x)$.

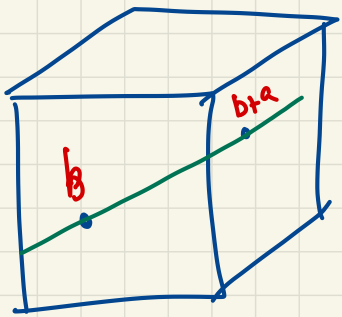
Thm: H_n is $(2, 1/4)$-locally correctible.

Reed-Muller Codes

$$RM(q,r,m) = \{ f : \mathbb{F}_q^m \to \mathbb{F}_q \mid \deg(f) \leq r \}$$

(Today: $r < q$)

Local Constraints / Characterizations:



line: $\ell_{a,b} = \{ a\cdot t + b \mid t \in \mathbb{F}_q \}$

$a, b \in \mathbb{F}_q^m$

$$f|_{\ell_{a,b}}(t) \triangleq f(a\cdot t + b)$$

Constraint: $f \in RM(q,r,m) \Rightarrow f|_{\ell_{a,b}} \in RM(q,r,1)$

m-variate $\Rightarrow$ univariate.

q-local

Characterization: $r < q/2$

$$f \in RM(q,r,m) \Longleftarrow \forall a,b \ f|_{\ell_{a,b}} \in RM(q,r,1)$$

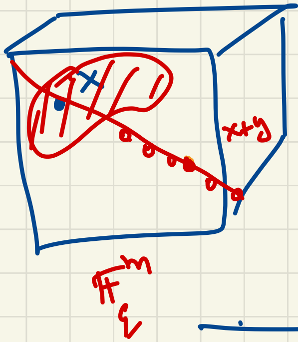
Exercise: By induction on m.

Local Decoder for RM Codes : [Beaver-Feigenbaum]

Thm: $\forall\, m, r < q$, $RM(q,r,m)$ is $\left(r+1, O\left(\frac{1}{r+1}\right)\right)$ - locally correctible

$r < q-1$!

Pr: Given g ϵ-close to f, $x \in \mathbb{F}_q^m$



- Pick random $y \in \mathbb{F}_q^m$
- Consider $g|_{\ell_{y,x}}(1) \ldots g|_{\ell_{y,x}}(r+1)$

interpolate & output $g|_{-}(0)$.

Thm: $r = o(q) \Rightarrow RM(q,r,m)$ is $\left(O(r), \frac{1}{4} - o(1)\right)$-LCC.

(Exercise / PS6).

$\Pr[f(x+iy) \neq g(x+iy)] < \epsilon$

$\Pr[\exists i \in [r+1]$ s.t. $\downarrow$ $] < (r+1)\epsilon$

Common generalization to H_n & $RM(q,r,m)$:

Restriction to low-dim subspaces preserves degree.

H_n : 2-d linear subspace

RM : 1-d affine subspace.

Local Testability

Defn. $C \subseteq \Sigma^n$ is (ℓ, α)-locally-testable if $\exists$ tester T s.t.

- T^g accepts w.p. 1 if $g \in C$
- $\forall g$ T^g rejects w.p. $\geq \alpha \cdot \delta(g, C)$

  where $\delta(g, C) \triangleq \min_{f \in C} \{ \delta(f, g) \}$.
- T^g makes ℓ queries to g.

Thm: $\mathcal{H}_n$ is $(3, \Omega(1))$-LTC

$RM(q, r, m)$ is $\left(r+2, \frac{1}{r^2}\right)$-LTC

In both cases test: Pick x at random

Accept if $g(x) = D^g(x)$

$\underbrace{\text{1-query} + \ell\text{-queries}}$

$\Rightarrow (\ell+1)$-query.

$\mathcal{H}_n$ analysis [BLR]

$g(x) \stackrel{?}{=} g(x+y) - g(y)$

- Fix $g : \mathbb{F}_2^n \to \mathbb{F}_2$; let $\epsilon(g) \triangleq \Pr_{x,y}\left[g(x)+g(y) \neq g(x+y)\right]$
- $f(x) \triangleq$ " $D^g(x)$ " ; $D^g(x;r) = g(x+r) - g(r)$

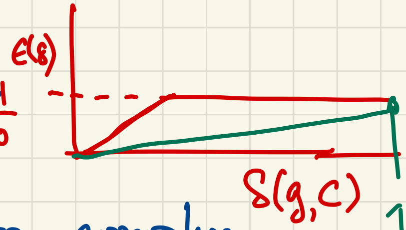
  $f(x) \triangleq \text{plurality}_r \{ D^g(x;r)$
- $\underline{\text{Lemma } 0}$: $\delta(f,g) \leq 2\epsilon(g)$ ⇐ if $f(x) \neq g(x)$

  $\Rightarrow \Pr_y\left[g(x) \neq g(x+y) - g(y)\right] \geq \frac{1}{2}$
- $\underline{\text{Lemma } 1}$: $\forall x$

  $$\Pr_{r_1, r_2}\left[D^g(x;r_1) \neq D^g(x;r_2)\right] \leq 2\epsilon(g)$$
- Cor. $\forall x \quad \Pr_r\left[f(x) \neq D(x;r)\right] \leq 2\epsilon(g)$
- $\underline{\text{Lemma } 2}$: $\quad \epsilon(g) < \frac{1}{10}$

$\Rightarrow \forall x,y \quad f(x) + f(y) = f(x+y) \quad \Rightarrow \quad f \in H_n$.

$\underline{\text{Thm}}$: $\mathcal{H}_n$ is $(3, \underset{=}{\frac{1}{10}})$-LCC



Rm analysis similar but more complex.

$$\epsilon(g) \geq \frac{1}{10}\,\delta(g,C)$$

RM LTCs + LDC $\Rightarrow$ PCP

PCP: Prob. checkable Proof.

Example: for Graph 3-Coloring

3-Col $\in$ PCP$(\ell, \ )$ if $\exists$ polytime verifier V

accessing $\pi \in \{0,1\}^*$ s.t.

$\forall G$

- if G is 3-Col $\Rightarrow \exists \pi \in \{0,1\}^{poly(|G|)}$
  s.t. $V^{\pi}(G) = 1$ w.p. 1
- G not 3-Col $\Rightarrow \forall \pi$
  $$\Pr\left[V^{\pi}(G) = 1\right] \leq \frac{1}{2}$$
- V makes ℓ queries to π.

Intermediate step: PCP for Reed-Solomon Code (RS-Prox.)

- $g : \mathbb{F}_q \to \mathbb{F}_q$ oracle access to + Proof π
- $\exists \pi \; \Pr[V^{g,\pi}(k) = 1] = 1$ if $\deg(g) \le k$
- $\forall \pi \; \Pr[V^{g,\pi}(k) = 1] \le \frac{1}{2}$ if $\delta(f,g) \geq .1$ $\forall f$ s.t. $\deg(f) \le 2k$
- $\ell = \mathrm{polylog}(|H|)$. (counts g-queries & π-queries)

Probably a PS6 question

3Col $\le$ RS-Prox:

G: given by $E : V \times V \to \mathbb{F}_q$ $\quad V \subseteq \mathbb{F}_q$

$\Downarrow$ ss

G 3col if $\exists$ $\chi : V \to \mathbb{F}_q$

- $\mathrm{Im}(\chi) \subseteq \{-1, 0, 1\}$
- $\forall u, v \in V \quad E(u,v) \cdot \prod_{i \in \{-2,-1,1,2\}} (\chi(u) - \chi(v) - i) = 0$

So proof:

$$\pi = (A, B, C, D, E)$$

$C, A : \mathbb{F}_q \to \mathbb{F}_q$; $B, D, E : \mathbb{F}_q \times \mathbb{F}_q \to \mathbb{F}_q$

s.t.

1. $\deg(A) \leq |V|$

2. $C \triangleq \dfrac{A(x) \cdot (A(x)-1) \cdot (A(x)+1)}{Z_V(x)}$; $\deg(C) \leq |V|$

3. $B(x,y) = E(x,y) \cdot \prod_{i \in \{-2,-1,1,2\}} (A(x) - A(y) - i)$

4. $B(x,y) = D \cdot Z_V(x) + E \cdot Z_V(y)$