Today
- Locally Decodable Codes
  Efremenko's Matching
  Vector Construction.

CS5.318.1
Coding Theory
Lecture 19 (2022.11.9)
Instructor: Prahladh Harsha.

Locally Decodable Codes

$\ell \in \mathbb{Z}_{>0}$, $\varepsilon \in (0,1)$

$C: \Sigma^k \to \Sigma^n$ is (ℓ,ε)-locally decodable (or (ℓ,ε)-LDC) if

there exists a (randomized) decoder D s.t.

On input: $y: [n] \to \Sigma$ (oracle access)
w/ promise that $\exists\, m \in \Sigma^k$
$\Delta(y, C(m)) < \varepsilon n$

$i \in [k]$ (explicit input)

$D^y(\cdot)$ - queries y in at most ℓ locations
& outputs a symbol $\in \Sigma$.

$\forall i \in [k]$, $\Pr[D^y(i) = m_i] \geq 2/3$

Do (ℓ,ε)-LDCs exist for constant ℓ?

Hadamard code. $\{0,1\}^k \to \{0,1\}^{2^k}$

$x \mapsto (y \mapsto \langle x,y \rangle)$

Promise: $f:\{0,1\}^k \to \{0,1\}$ s.t. $\exists x, \Delta(f, Had(x)) \leq \delta 2^k$

$\forall i, \quad \Pr_{r}[f(r \oplus e_i) - f(r) = x_i] \geq 1-2\delta.$

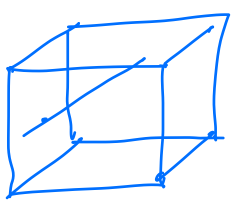
Had is $(2,\varepsilon)$-LDC for any $\varepsilon < 1/4$.

— $RM_q(m,r)$ - Reed Muller Codes

#vars $= m$; deg $= r$; $q > \frac{r}{1-2\varepsilon}$

Input: $z \in \mathbb{F}_q^m$

z



1. Pick a random line ℓ through z
2. Query f on all line pts
3. Perform univariate interpolation and o/p value at z.

(q,ε)-LDC. $\quad r = (1-2\varepsilon)q$

$n = q^m$

$k = \binom{m+r}{m} \geq \left(\frac{r}{m}\right)^m = \left(\frac{1-2\varepsilon}{m}\right)^m \cdot n$

locality $\ell = q = n^{1/m}$

1. $m = 1/\varepsilon$; $k/n \approx \varepsilon^{1/\varepsilon}$; $\ell = n^{\varepsilon}$
2. $m = \frac{\log n}{\log\log n}$; $n = \mathrm{poly}(k)$; $\ell = \mathrm{polylog}\, n$.

③ $q = O(1)$; $n = \exp(k^{1/(q-1)})$ $\ell = q = O(1)$

[deWolf-Kerenedis '04]: 2-query LDC must have inverse exponential rate.

Initial belief:

① Non-trivial locality → Rate → 0

② locality = $O(1)$ → Rate - inverse exponential.

Both beliefs were refuted

① multiplicity. (polylog n locality & Rate → 1)

② Yekhanin's code (3-query LDC w/ subexponential blowup)

Yekhanin '07 [assuming infinitely many Mersenne primes exist]

Raghavendra '07 [alternate description of [Yek]]

Efremenko '09 [unconditional construction using matching vectors]

Today: Sudan & Gopalan's description of Efremenko's construction.

Matching Vectors:

m - $\mathbb{Z}_{>0}$, $n \in \mathbb{Z}_{>0}$.

Ring - $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$.

Definition: $\mathcal{L} \subseteq \mathbb{Z}_m \setminus \{0\}$

$$\mathcal{U} = (u[1], u[2], \ldots u[k]) \qquad u[i], v[i] \in \mathbb{Z}_m^n$$

$$\mathcal{V} = (v[1], v[2], \ldots, v[k])$$

$(\mathcal{U}, \mathcal{V})$ is $\mathcal{L}$-matching vector if

$$\forall i \in [k] \quad u[i] \cdot v[i] = 0 \quad (\text{in } \mathbb{Z}_m)$$

$$\forall i \neq j \in [k] \quad u[i] \cdot v[j] \in \mathcal{L}. \quad (\text{in } \mathbb{Z}_m)$$

Thm [Grolmusz 00]. m - composite - t distinct prime factors.

then there exists an explicit construction of $\mathcal{L}$-matching vectors $(\mathcal{U}, \mathcal{V})$ for every n.

$$\text{w/ } \ell = |\mathcal{L}| \leq 2^t - 1$$

$$k \geq \exp\left(\frac{(\log n)^t}{(\log \log n)^{t-1}}\right)$$

$\mathbb{F}_q$ - field $\quad \gamma \in \mathbb{F}_q^* \quad \operatorname{ord}_{\mathbb{F}_q}(\gamma) = m \quad (m / q-1)$

Thm: $\mathbb{F}_q$ - field, $m / (q-1)$

Suppose $(\mathcal{U}, \mathcal{V})$ is a $\mathcal{L}$-matching vectors in $\mathbb{Z}_m^n$ of size k.

where $\ell = |L|$, $(L \neq 0)$,
then there exists a $\left(\ell+1, \frac{1}{3(\ell+1)}\right)$ - LDC.

$C_v : \mathbb{F}_q^k \to \mathbb{F}_q^N$ where
$N = (q-1)^n$

q - constant
m - constant

N - exponential.
K - superpolynomial
Rate - subexponential.

Code Construction: $C_v : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^N$

Message - Coefficients of some multivariate poly

Codeword: Evaluation of poly on all points in $(\mathbb{F}_q^*)^n$

Allowed monomials. $x_i(x_1 \ldots x_n)$; $i \in [k]$

$$x_i(x_1, \ldots, x_n) = \prod_{j=1}^{n} x_j^{v[i]_j}$$

(monomial obtained by using $v[i]$ as the exponent vector).

$$(a_1 \ldots a_k) \in \mathbb{F}_q^k \longrightarrow P_a(\bar{x}) = \sum_{i \in [k]} a_i x_i(\bar{x})$$

C_v - Eval of P_a on $(\mathbb{F}_q^*)^n$.

Decoding: Use u vectors to decode
In particular to decode coeff of x_i
use matching vector $u[i]$.

Notation: (i) $x, y \in (\mathbb{F}_q^*)^n$
$(x \odot y) \in (\mathbb{F}_q^*)^n$ s.t. $(x \odot y)_i = x_i y_i$

(ii) $x \in (\mathbb{F}_q^*)^n$; $h \in \mathbb{Z}_m$
$x^h = (x_1^h, x_2^h, \ldots \ x_n^h)$

(iii) $a \in \mathbb{F}_q^*$; $u \in \mathbb{Z}_m^n$
$a^u = (a^{u_1}, a^{u_2}, \ldots \ , a^{u_n})$

L - possible bilinear forms of matching vectors

$B = \{ \gamma^l \,/\, l \in L \}$ $\qquad l = |L|$
$|B| = L \qquad (\text{ord}(\gamma) = m)$
$1 \notin B$. (since $0 \notin L$)

Claim: There exist non-zero $c_0, c_1 \ldots \ c_l \in \mathbb{F}_q$
s.t.
(i) $\sum_{i=0}^{l} c_i = 1$

(ii) $\sum_{h=0}^{l} c_h \beta^h = 0 \quad \forall \beta \in B$.

Proof: Take poly $\prod_{\beta \in B} \frac{(x-\beta)}{1-\beta}$

"Multiplicative" Line $\quad x \in (\mathbb{F}_q^*)^n$ - point

$y \in (\mathbb{F}_q^*)^n$ - direction

$(\, y = \gamma^{u[i]} \,)$

$$\ell_{x,y} = \{ x \odot y^t \mid t \in \mathbb{Z}_m \}.$$

Claim: $\forall\, i,j \in [k]$, $x \in (\mathbb{F}_q^*)^n$, $h \in \mathbb{Z}_m$.

$$\chi_j\left(x \odot \gamma^{h u[i]}\right) = \begin{cases} \chi_j(x) & \text{if } i=j \\ \chi_j(x)\beta_y^h & \text{if } i \neq j \text{ for some } \beta_y \in B \end{cases}$$

Proof: $$\chi_j\left(x \odot \gamma^{h u[i]}\right) = \prod_{\ell=1}^{k} \left(x_\ell\, \gamma^{h u[i]_\ell}\right)^{v[j]_\ell}$$

$$= \chi_j(x)\, \gamma^{h(u[i]\cdot v[j])}$$

$$= \begin{cases} \chi_j(x) & \text{if } i=j \\ \chi_j(x)\beta_{y_j}^h & \text{where } \beta_y \in B \end{cases}$$

Decoder (D)

Input: $g : (\mathbb{F}_q^*)^n \to \mathbb{F}_q$ (oracle) $\quad$ (promise: $\exists\, a \in \mathbb{F}_q^k$ s.t. $\Delta(g, \mathcal{C}_V(a)) < \frac{N}{3(\ell+1)}$)

$i \in [k]$ explicit

Algorithm: (1) Pick $x \in_R (\mathbb{F}_q^*)^n$

(2) Query g on $x,\ x\odot\gamma^{u[i]},\ x\odot\gamma^{2u[i]},$

$\cdots \quad x \odot \gamma^{\ell u[i]},$

③ Output $\displaystyle\sum_{h=0}^{\ell} c_h\, y(x \odot \gamma^{hu[i]}) \cdot \chi_i(x)^{-1}$

If $y(x \odot \gamma^{hu[i]}) = p_a(x \odot \gamma^{hu[i]})$ for $h = 0, \ldots \ell$

(happens w/ probability $1 - (\ell+1)\varepsilon$
$\geq 1 - \frac{1}{3} = \frac{2}{3}$)

But $\left(\displaystyle\sum_{h=0}^{\ell} c_h p_a (x \odot \gamma^{hu[i]})\right)$

$$= \sum_{h=0}^{\ell} c_h \left(\sum_{j=1}^{k} \chi_j (x \odot \gamma^{hu[i]}) \right)$$

$$= \chi_i(x).$$

$\boxtimes$

Prop. $\forall i \in [k]$, $\Pr_D [D^y(i) = a_i] \geq 2/3$

Existence of Matching Vectors:

Thm [Grolmusz 00]. m - composite - t distinct prime factors.
then there exists an explicit construction of L-matching vectors $(\mathcal{U}, \mathcal{V})$ for every n.

w/ $\ell = |L| \leq 2^t - 1$

$$k \geq \exp\left(\frac{(\log n)^t}{(\log\log n)^{t-1}}\right)$$

Sudan's construction of matching vectors using OR representation.

$OR: \{0,1\}^n \to \{0,1\}$

$$x_1 \dots x_n \mapsto \begin{cases} 0 & \text{if } \bar{x} = 0 \\ 1 & \text{otherwise.} \end{cases}$$

$p \in \mathbb{Z}_m[x_1 \dots x_n]$ represents OR if.

$$\bar{x} = 0 \Rightarrow p(\bar{x}) = 0$$
$$\bar{x} \neq 0 \Rightarrow p(\bar{x}) \neq 0.$$

What is the smallest degree of any poly p that represents OR.

[Razborov, Smolensky] $\deg = \Omega(n)$ if m-prime.

[Bregel-Barrington-Rudich] m-composite w/ t distinct prime factors, then there exists an OR-representation over $\mathbb{Z}_m$ w/ degree $O(n^{1/t})$ & furthermore $|\{p(\bar{x}) \mid \bar{x} \in \{0,1\}^n \setminus \bar{0}\}| \leq 2^t - 1$

Construction of matching vectors using BBR
OR-representation construction.

BBR gives us $p \in \mathbb{Z}_m[x_1, .. x_n]$

$$p(x) = \begin{cases} 0 & \text{if } x = \bar{0} \\ \in L & \text{if } x \in \{0,1\}^n \setminus \bar{0} \end{cases}$$

where $0 \notin L$ & $|L| \le 2^{\epsilon} - 1$.

For each $y \in \{0,1\}^n$:

$$p^y(x) = \begin{cases} 0 & \text{if } x = y \\ \in L & \text{if } x \in \{0,1\}^n \setminus y \end{cases}$$

$p^y(x) = \sum p^y_\alpha \cdot \alpha(x)$ in the monomial basis.

$\binom{n}{\le d}$ where $d = O(n^{1/\epsilon})$

Construct $\mathcal{U}, \mathcal{V}$ as follows
where $K = 2^n$

$\mathcal{U} = (u[x])_{x \in \{0,1\}^n}$ $\qquad u(x) = \alpha(x)$

$\mathcal{V} = (v[x])_{x \in \{0,1\}^n}$ $\qquad v(y) = p^y_\alpha$

$\boxtimes$