May 9

REMINDERS

(•) Video due by 11:59 pm WED!

(•) Survey due by 11:59 pm FRI! Please chk the survey tool to make sure the correct group shows up for you

---

RECAP

(•) Coding for distributed storage

(•) [Def] Let C be an $[n,k]_q$ code that is systematic. C is an (r,d) mLRC (or (r,d)-LRC) if:

(i) C has dist d ← {handle catastrophic errors}

(ii) $\forall i \in [k]$ ($\forall i \in [n]$ resp.), $\exists R_i \subseteq [n]\setminus\{i\}$ s.t. $|R_i| \le r$ & (handle one server failure/ repair) for any codeword $(c_1, \dots, c_n) \in C$, c_i can be recovered from c_{R_i}

(•) THM1: $n > k \ge r > 0$, $q \ge n$, $\exists$ an explicit $[n,k]_q$ code C that is an (r,d) mLRC with $d = n-k-\lceil \frac{k}{r} \rceil + 2$ ($r=k \Rightarrow C$ is MDS)

(•) Saw last time: Let C_0 be an $[n_0,k]_q$ MDS code

$$\Rightarrow G_0 = \left(I_k \;\middle|\; \bar{p}^{(1)} \;\; \bar{p}^{(2)} \;\cdots\; \bar{p}^{(d-1)} \right)$$

{Recall since C_0 is MDS, $d-1 = n_0-k$}

Claim: $\bar{p}^{(\ell)}$ $\forall \ell \in [d-1]$ has full support (ie $wt(\bar{p}^{(\ell)}) = k$)

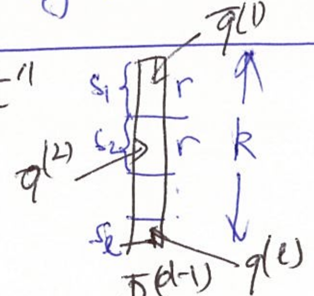
TODAY

(•) Proof readers: James, Jaswanth, Patrick

(•) finish proof of Thm

(•) Argue a tight lower bound.

Idea: "split"



$\ell = \lceil \frac{k}{r} \rceil$ $\quad |S_j| = r \;\; \forall\; 1 \le i < \ell$

$|S_\ell| \le r$

$S_j = \{(j-1)r+1, \dots, jr\}$

$S_\ell = \{(\ell-1)r+1, \dots, k\}$

$$G = \left(I_k \;\middle|\; \bar{p}^{(1)} \;\cdots\; \bar{p}^{d-2} \;\; \underbrace{\begin{pmatrix} \bar{q}^{(1)} \\ 0 \end{pmatrix}}_{\bar{s}^{(1)}} \;\; \underbrace{\begin{pmatrix} 0 \\ q^{(2)} \\ 0 \end{pmatrix}}_{\bar{s}^{(2)}} \;\cdots\; \begin{pmatrix} 0 \\ \bar{q}^{\ell} \end{pmatrix} \right)$$

$\Rightarrow C$ is linear & systematic

$$\bar{x} \mapsto \big(\bar{x}, \langle p^{(1)}, \bar{x}\rangle, \dots, \langle \bar{p}^{(d-2)}, x\rangle, \langle \bar{Q}^{(1)}, x\rangle, \dots, \langle \bar{Q}^{(\ell)}, x\rangle\big)$$
$$= (c_1, c_2, \dots, c_n)$$

$$n = k + (d-2) + \ell = k + d - 2 + \left\lceil \frac{k}{r} \right\rceil$$

Q: What is the distance of C? $\geq d$. Claim: $\langle \bar{p}^{(d-1)}, \bar{x}\rangle \neq 0$

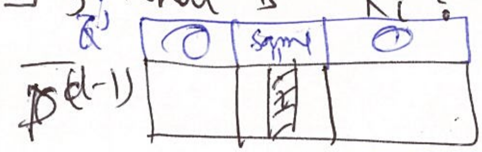
$$\langle \bar{p}^{(d-1)}, \bar{x}\rangle = \langle \bar{Q}^{(1)}, x\rangle + \langle \bar{Q}^{(2)}, \bar{x}\rangle + \dots + \langle \bar{Q}^{(\ell)}, \bar{x}\rangle$$

$\Rightarrow$ at least on of $\langle Q^{(j)}, \bar{x}\rangle \neq 0$

$$\Rightarrow \text{dist} = d = n - \left(k - 2 + \left\lceil \frac{k}{r} \right\rceil\right)$$
$$= n - k - \left\lceil \frac{k}{r} \right\rceil + 2$$

Q: Fix $i \in [k]$, what is R_i?

Say $i \in S_j$

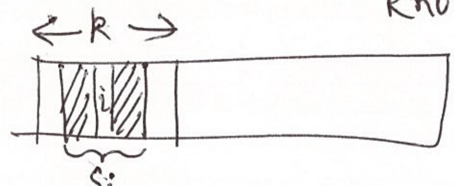


$$\langle \bar{Q}^{(j)}, x\rangle = \sum_{a \in S_j \setminus \{i\}} q_a^{(j)} \cdot x_a + \underbrace{q_i^{(j)} \cdot x_i}_{\text{unknown}}$$

$$\Rightarrow x_i = \frac{1}{q_i^{(j)}} \Big(\underbrace{\langle \bar{Q}^{(j)}, x\rangle}_{\text{know}} - \underbrace{\sum_{a \in S_j \setminus \{i\}} q_a \cdot x_a}_{\text{know}} \Big)$$

$R_i = S_j \setminus \{i\} \cup \{k+d-2+j\} \Longleftarrow$

$c_{k+d-2+j} = \langle \bar{Q}^{(j)}, \bar{x}\rangle$



$|R_i| = |S_j| - 1 + 1$
$= |S_j| \leq r$

A Singleton type bound

~~lower~~ Upper bound that shows dist in THM1 is tight

THM2: Any $(n,k)_q$-code C is an (r,d)-mLRC must satisfy $d \le n-k-\lceil \frac{k}{r} \rceil + 2$

Note: THM2 also holds for non-linear codes

Pf: C is systematic: $C_{[k]} = \mathbb{F}_q^k$

Claim1: $\exists$ subsets T' & S s.t.

(i) $|T'| = k-1$

(ii) $|S| = \lfloor \frac{k-1}{r} \rfloor$

(iii) $T' \cap S = \phi$

(iv) $\forall\, \bar{c}$, $\bar{c}_{T'}$ determines $\bar{c}_S$

(you cannot have $\bar{c} \ne \bar{c}'$ s.t. $\bar{c}_{T'} = \bar{c}'_{T'}$ but $\bar{c}_S \ne \bar{c}'_S$)

$|T'| = k-1 \Rightarrow |C_{T'}| \le q^{k-1} \underset{\text{pigeon-hole principle}}{\Rightarrow} \exists\ \bar{c} \ne \bar{c}' \in C$ s.t. $\bar{c}_{T'} = \bar{c}'_{T'}$

$\xrightarrow[\text{by (iv)}]{} \bar{c}_S = \bar{c}'_S$

$\Rightarrow \bar{c}$ & $\bar{c}'$ agree on S & T'

~~$\Rightarrow$ dist of code~~ $\Rightarrow \Delta(\bar{c}, \bar{c}') \le \overbrace{n - |S| - |T'|}^{\text{frm (iii)}}$

$\Rightarrow d \le n - |S| - |T'|$

by (i) + (ii) $= n - \lfloor \frac{k-1}{r} \rfloor - (k-1)$

$= n - k - \lfloor \frac{k-1}{r} \rfloor + 1$

$= n - k - \lceil \frac{k}{r} \rceil + 2$

EX: $\lfloor \frac{k-1}{r} \rfloor = \lceil \frac{k}{r} \rceil - 1$