Today
- Locally Recoverable Codes

CS5.318.1
Coding Theory
Lecture 20 (2022-11-11)
Instructor: Prahladh Harsha.

Locally Recoverable Codes:

- Requirement: weaker than LDC

  LDC: can locally decode if there is a constant fraction of errors.

  LRC: (1) can locally decode if there is a constant # of errors

  (2) if there is a constant fraction of errors, globally decode

  (1) - typical failure

  (2) - catastrophic failure

— Today: local recovery from 1 corruption.

r - locality parameter.

d - distance of code.

q - alphabet - large

C - $[n,k,d]_q$-code is (r,d)-message symbol locally recoverable (C (r,d)-mLRC)

$C : \Sigma^k \to \Sigma^n$ (C is systematic, ie first k symbols of codeword is message)

(r-local recovery): For every $i \in [k]$, there exist $R_i \subseteq [n] \setminus \{i\}$, such that $(R_i \Rightarrow i)$

C is (r,d)-locally recoverable ((r,d)-LRC)

(r-local recovery): For every $i \in [n]$, there exist $R_i \subseteq [n] \setminus \{i\}$, such that $(R_i \Rightarrow i)$

Remarks: (i) (r,d)-LRC $\Rightarrow$ (r,d)-mLRC

(ii) No computational restrictions.

RS: or any MDS code

$[n_0, k, d]_q$ - code where $n_0 = k+d-1$

r - locality parameter.

Generator matrix G

$$\begin{bmatrix} I \\ \hline \longleftarrow p^{(1)} \longrightarrow \\ \longleftarrow p^{(2)} \longrightarrow \\ \longleftarrow p^{(d-1)} \longrightarrow \end{bmatrix}$$

$p^{(i)} \in \Sigma^k$

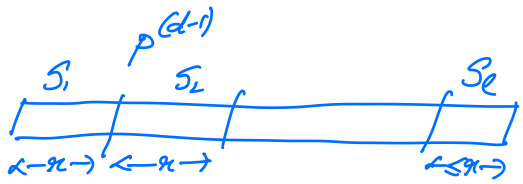
$G \in \Sigma^{n \times k}$

$$\begin{array}{ccc} x & \mapsto & Gx \\ \cap & & \cap \\ \Sigma^k & & \Sigma^n \end{array}$$

has this form if C is systematic

Obs: $\mathrm{Supp}(p^{(i)}) = [k]$, $\forall\, 1 \le i \le d-1$

Pf: Otherwise suppose $j \notin \mathrm{Supp}(p^{(i)})$
$[k] \setminus j \cup (k+i)$ - locations do not determine the message. ☒



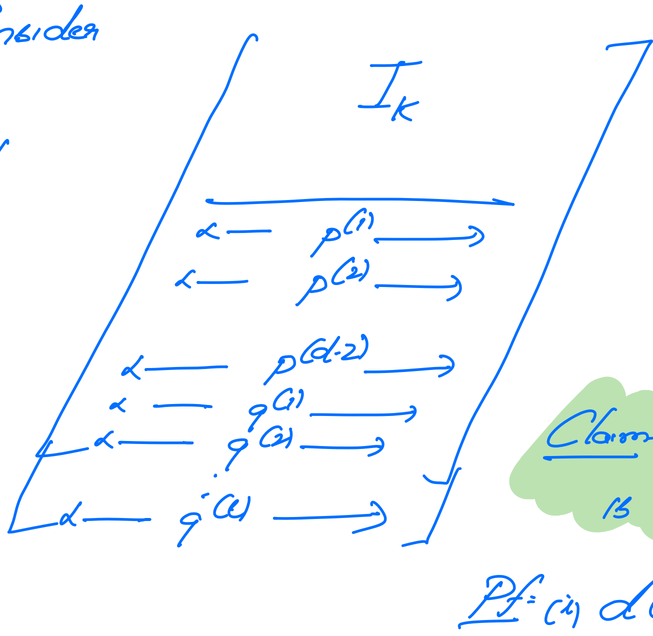
$\ell = \lceil \frac{k}{r} \rceil$; $|S_i| = \begin{cases} r & \text{if } i<\ell \\ \le r & \text{if } i=\ell \end{cases}$

$$p^{(d-1)} = q^{(1)} + q^{(2)} + \cdots + q^{(\ell)}$$

where $\mathrm{supp}(q^{(i)}) = S_i$

Consider

G'



; $G' \in \Sigma^{k \times n}$

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

Claim: $\mathcal{C}' = \{ G'x \mid x \in \Sigma^k \}$ is (r,d)-LRC

Pf: (i) $d(\mathcal{C}') \ge d(\mathcal{C}) = d$

(ii) $i \in [k]$, $j_i :=$ "$i \in S_{j_i}$"

$R_i := (S_{j_i} \setminus \{i\}) \cup \{k+d-2+j_i\}$

since $\mathrm{Supp}(q^{(j_i)}) = S_{j_i}$

Rate: MDS: $k \to n = k+d-1$

(r,d)-mLRC $k \to n = k+d+\lceil \frac{k}{r} \rceil - 2$

Singleton-like bound for (r,d)-mLRC

$C: \Sigma^k \to \Sigma^n$ be a (r,d)-mLRC then

$$n \geq k+d+\lceil \frac{k}{r} \rceil - 2.$$

Pf: Suppose we have 2 subsets of $[n]$ st S & T

(i) $S \cap T = \emptyset$

(ii) $|T| < k$

(iii) "$T \underset{C}{\Rightarrow} S$"

Singleton like proof

$\Rightarrow d(C) \leq n - |T \cup S|$

$n \geq d + |T \cup S|$

Construct S & T as follows:

$S, T \leftarrow \emptyset$

While $|S| < \lfloor \frac{k-1}{r} \rfloor$

Let $t \in [k]$ be the first index in $[k]$ outside $S \cup T$.

$S \leftarrow S \cup \{t\}$

$T \leftarrow T \cup (R_t \setminus S)$

Output S & T.

For any R_i $\quad |R_i \cap [k]| \le r-1$

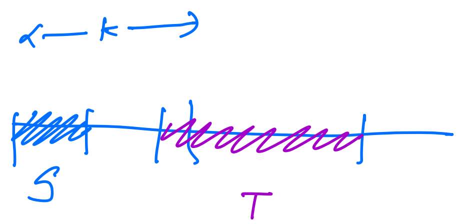
While $|S| < \lfloor \frac{k-1}{r} \rfloor$, $\quad |S \cup (T \cap [k])| \le r|S| \le k-1$

At the end of loop;

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

(ii) $|T| \le r|S| \le k-1$

(iii) $T \supseteq S$



Add $k-1-|T|$ elts from $[n] \setminus (S \cup T)$ to T

st (ii) is replaced by $|T| = k-1$

By Singleton-bound like argument (from before)

$$n \ge d + |T \cup S|$$
$$= d + k - 1 + \left\lfloor \frac{k-1}{r} \right\rfloor$$
$$= d + k + \left\lceil \frac{k}{r} \right\rceil - 2$$

(Since $\lfloor \frac{k-1}{r} \rfloor = \lceil \frac{k}{r} \rceil - 1$

What about (r,d)-LRC?

Construction of (r,d)-LRC (matching the Singleton Bound)

Thm: Let $n > k \ge r$; q-prime power
$(r+1)$ divides both n & $q-1$, then
explicit construction of a $[n,k]_q$-code which

is (r, d) - LRC w/ $d = n - k - \lceil \frac{k}{r} \rceil + 2$

Pf: $n = q-1$

$(r+1) \mid (q-1)$, there exists an element $\omega \in \mathbb{F}_q^*$ whose order is $r+1$.

ie, $1, \omega, \omega^2, \ldots, \omega^r$ - distinct

& $\omega^{r+1} = 1$

Let k' be the smallest integer such that

$$k = \left\lceil \frac{k'r}{r+1} \right\rceil$$

If above is true $k = \frac{k'r + a}{r+1}$ for $0 < a \leq r$

$$k' = \frac{(r+1)k - a}{r} = k + \frac{k-a}{r} = k + \left\lceil \frac{k}{r} \right\rceil - 1$$

C - $[n, k']$ - RS code.

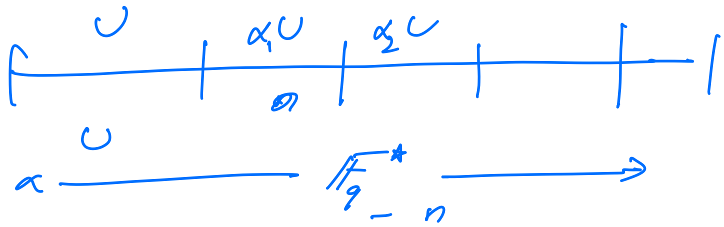
$$d = n - k' + 1 = n - k - \left\lceil \frac{k}{r} \right\rceil + 2$$

C - has distance d

but is not r- locally recoverable.

$U = \{1, \omega, \ldots \omega^r\}$

Claim: $\prod_{u \in U} (X - u) = X^{r+1} - 1$



$p(x)$ - restricted to U

$$p_U(x) \equiv p(x) \pmod{x^{r+1}-1}$$

$$C^* = \Big\{ \langle p(\alpha)\rangle_{\alpha\in \mathbb{F}_q^*} \;\Big|\; \deg(p) < k',\ p(x) = \sum_{i<k'} p_i x^i,\ p_i = 0 \text{ whenever } i \equiv r \pmod{r+1} \Big\}$$

(i) $C^* \subseteq C$: distance inherited from C.

(ii) $\mathbb{F}_q^*$ - partitioned by U's n/s cosets

For each such coset αU; $\prod_{u\in\alpha U}(X-u) = X^{r+1} - \alpha^{r+1}$

Within coset αU

$$p_{\alpha U}(x) \equiv p(x) \pmod{x^{r+1}-\alpha^{r+1}}$$

By construction, $\deg(p_{\alpha U}) < r$ (due to missing coefficients)

Hence, there is a non-zero linear combination involving the codeword locations in αU.

Furthermore, this linear comb involves <u>all</u> the codeword locations