May 6

REMINDERS

(•) Video due by 11:59pm next WED!

(•) Survey due by 11:59pm next FRI!

RECAP

(•) Maximum Distance Separable (MDS).
$(n,k,d)_q$ - code is MDS if $d = n-k+1$

(•) RS is MDS

(•) Systematic code (HW 2) $c(\bar{m}) = (\bar{m}, \dots)$ ← parity check symbols

---

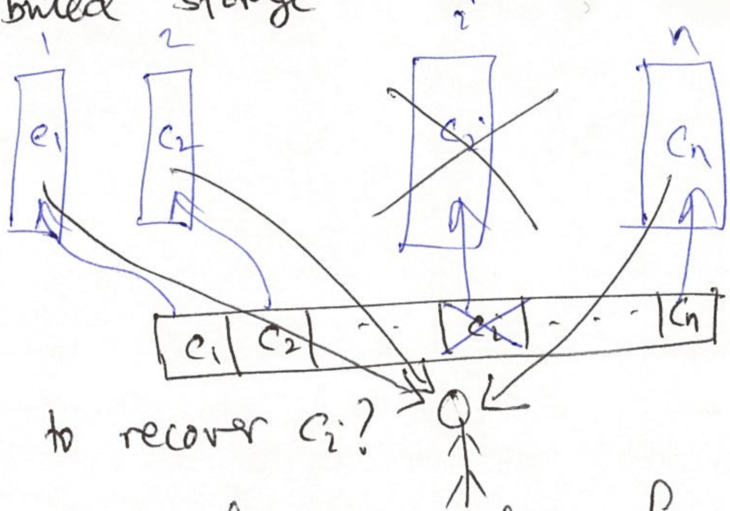
TODAY

(•) Proof readers: Aishwarya, Muskan

(•) Coding for the cloud!
↳ aka Locally recoverable codes (LRCs)

(•) Practical motivation: protect your data on the cloud
↳ Distributed storage

$\bar{c} = (c_1, \dots, c_n) \in \mathcal{C}$



1 erasure.

Q: Want to recover c_i?

A1: Use erasure decoding algo for HW 1!
BUT need $c_1, c_2, \dots, c_{i-1}, c_{i+1}, \dots, c_n$ from $n-1$ servers!

Q: How can we do better?

A2: For RS codes can do this with k symbols! ← Knowing eval of deg $\le k-1$ poly over k pts ⇒ recover the poly.
↳ Also true for MDS codes.

Algo: ~~Get~~ $c_{i_1}, \dots, c_{i_k}$.
(•) Do poly interpolation to figure out $P(X)$
(•) Computing $P(\alpha_i)$

Q: Can we ~~get~~ recover only erased symbol c_i using only r ~~constant~~ many codeword symbols? (Think of r as a constant!)

↳ Actually implemented in distributed storage → Azure (MS)
(MSR SVC)

Locally Recoverable codes (LRCs)

2 definitions → only recover message bits.
→ recover any codeword symbol

Def 1 C be an $[n,k]_q$ code that is systematic (so $C(\bar{m}) = (\bar{m}, \ldots)$)

C is a message symbol (r,d)-locally recoverable code or (r,d) mLRC if

(i) C has min dist d. $\quad c = (\underbrace{c_1, \ldots, c_k}_{\text{msg bits}}, c_{k+1}, \ldots, c_n)$

(ii) $\forall\ i \in \boxed{[k]}$, $\exists\ R_i \subseteq [n]\setminus\{i\}$ s.t $|R_i| \le r$ s.t i^{th} symbol in $\bar{c} = (c_1, \ldots, c_n)$ can be recovered from $\bar{c}_{R_i} = \{c_j\}_{j \in R_i}$

Def 2: (r,d) - LRC $\quad$ replace $[k] \leftarrow [n]$

Remarks: (Ex 19.2)

(i) No error recovery algo specified BUT $c_i = \langle \overset{\text{known/fixed for } c_i}{\bar{u}_i}, \bar{c}_{R_i} \rangle$

(ii) $r \le k$.

THM: $n > k \ge r > 0$ be ints, $q \ge n$, $\exists$ an explicit $[n,k]_q$ code that is an (r,d) - mLRC with

$$d = n - k - \left\lceil \frac{k}{r} \right\rceil + 2 \qquad \left\{ \text{if } r = k \Rightarrow d = n - k + 1 \right\}$$

(Pf)

Idea: (i) Convert any linear MDS code C_0 into C that is (r,d) - mLRC.

(ii) Define the generator matrix C (G) in terms of ________ of C_0 (G_0)

Let C_0 be $[n_0, k, d]_q$ - MDS code.

$$\bar{X} = (X_1, \ldots, X_k) \qquad C_0(\bar{X}) = \left(\underset{X_1}{\underset{\|}{c_1}}, \underset{X_2}{\underset{\|}{c_2}}, \ldots, \underset{X_k}{\underset{\|}{c_k}}, c_{k+1}, \ldots, \overset{c_{k+d-1}}{\overset{\|}{c_{n_0}}} \right)$$

$$\bar{x} \to \left(\bar{x}, \langle \bar{p}^{(1)}, \bar{x}\rangle, \langle \bar{p}^{(2)}, x\rangle, \ldots, \langle \bar{p}^{(d-1)}, x\rangle\right)$$

$c_{k+j} = \langle \bar{p}^{(j)}, \bar{x}\rangle$

$1 \le j \le n-k$
$= d-1$

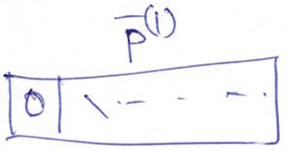
$$G_0 = (x_1 \ldots, x) \left(\underbrace{\begin{matrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{matrix}}_{k} \middle| \begin{matrix} \uparrow & \uparrow & & \uparrow \\ \bar{p}^{(1)} & \bar{p}^{(2)} & \cdots & \bar{p}^{(d-1)} \\ \downarrow & \downarrow & & \downarrow \end{matrix} \right)$$

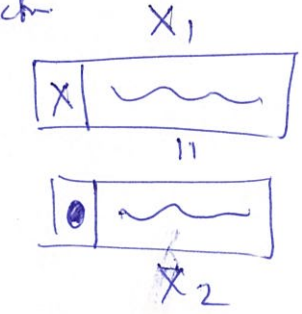
<u>Claim:</u> Each $\bar{p}^{(j)} \in \mathbb{F}_q^k$ $1 \le j \le d-1$ has full support.

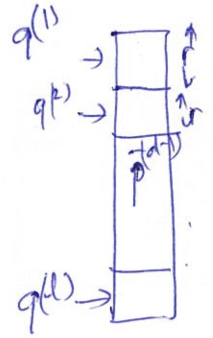
Q: Why? (EX)

Hint: Prove by contradiction

Assm

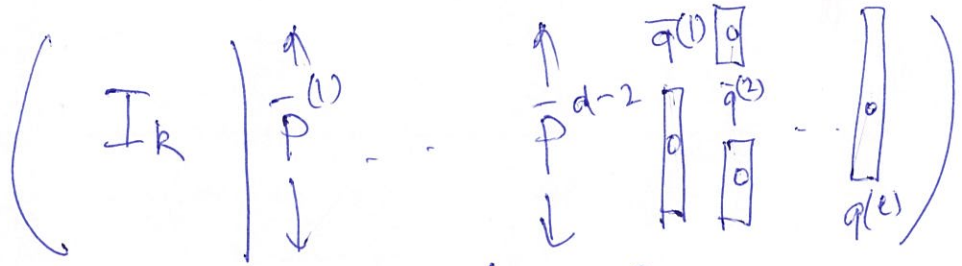






$\ell = \left\lceil \frac{\cancel{6}k}{r} \right\rceil$

$S =$



<u>Prove next time:</u> The C generated by S is (r,d) - mLRC

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