May 11

REMINDER

(o) Deadline extension!
- ↳ Both video + survey due by 11:59pm on Sunday, May 15
- ↳ I had to delete original survey so please re-vote if needed.

RECAP

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

not needed for LRC

(i) C has dist d

(ii) $\forall\, i \in [k]$, $\exists\, R_i \subseteq [n]\setminus\{i\}$ s.t. $|R_i| \le r$ &
($\forall\, i \in [n]$ resp.) for any codeword $(c_1, \ldots, c_n) \in C$, c_i can be recovered from $\bar{c}_{R_i}$

(o) Optimal tradeoff for (r,d)-mLRC:

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

(o) ~~Lower~~ Upper bound obviously holds for (r,d)-LRC but ~~upper~~ lower bound doesn't.

TODAY

(o) Proof readers: Sri Varsha, Mitali, Nick

(o) Construction of (r,d)-LRC with $d = n - k - \left\lceil \frac{k}{r} \right\rceil + 2$

Construction: sub-code of RS

↳ we'll only use polys (of low deg) but with specific structure.

don't really need them.

THM: ~~[illegible]~~ $n > k \ge r > 0$ with (i) $(r+1) \mid n$ (divides)

(ii) $q \ge n+1$ prime power s.t. $(r+1) \mid q-1$

$\Rightarrow \exists$ an explicit $[n,k]_q$ code (infact RS sub-code) that is (r,d)-LRC with $d \underset{(=)}{\ge} n - k - \left\lceil \frac{k}{r} \right\rceil + 2$

by mLRC upper bound

Pf: Pick $n = q-1$ $\quad ((i) \Leftrightarrow (ii))$

Fact $\quad$ (ii) $\Rightarrow$ $\mathbb{F}_q$ has $(r+1)^{th}$ root of unity, $\omega \neq 1$

(Ex 9.9+9.10) $\quad \Rightarrow \underbrace{\omega, \omega^2, \ldots, \omega^r}_{\text{also roots of unity}}$ ~~are~~ are distinct & $\omega^{r+1} = 1$

$\equiv \omega^{r+1} - 1 = 0$

Def: Let k' be the smallest int s.t

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

Fact: $\quad k' = k + \left\lceil \frac{k}{r} \right\rceil - 1$

Initial code $\quad C_0 = [\underset{q-1}{\overset{\shortparallel}{n}}, k']$ RS code w/ eval points $\mathbb{F}_q^*$

$$C_0 = \{ \langle f(\alpha) \rangle_{\alpha \in \mathbb{F}_q^*} \mid f(X) \in \mathbb{F}_q[X], \deg(f) < k' \}$$

Aside: locality $\geq k'$ $\quad$ b/c: fixing $k'-1$ values of a $\deg \leq k'$ poly doesn't fix poly.

Small detour: $\quad \mathcal{U} = \{1, \omega, \omega^2, \ldots, \omega^r\}$

Fun fact: $\quad \prod_{u \in \mathcal{U}} (X - u) = X^{r+1} - 1$ $\qquad f(X) \in \mathbb{F}_q[X]$, $\deg(f) < k'$

Claim 1: $\quad g(X) := f(X) \bmod X^{r+1} - 1 \quad \deg(g) \leq r$

(Ex. 9.13) $\quad \Rightarrow g(\alpha) = f(\alpha) \quad \forall \alpha \in \mathcal{U}$

Case 1: $\deg(g) < r$

Claim 2: $\quad S \subseteq \mathbb{F}_q$, $\deg(h) \leq |S| - 2 \Rightarrow \exists \lambda_\alpha \; \forall \alpha \in S$ s.t $\sum_{\alpha \in S} \lambda_\alpha g(\alpha) = 0$ s.t not all $\lambda_\alpha = 0$

(Ex 19.14) (RS codes w/ eval pt $|S|$ $\quad [|S|, |S|-1]_S$ RS code)

$\forall \alpha \in S$ $\quad$ pick $(\lambda_\alpha)_{\alpha \in S}$ to be non-zero codeword in dual RS code. $\Rightarrow$ infact pick a non-zero codeword of wt $= |S|$)

$$\lambda_\alpha \cdot g(\alpha) = - \sum_{\beta \in S \setminus \{\alpha\}} \lambda_\beta g(\beta) \Leftarrow$$

$\Rightarrow \forall\ i \in \mathcal{U}$, define $R_i = \mathcal{U} \setminus \{i\}$ & R_i is recovery set for i.

<u>Case 2:</u> $\deg(g) = r$

<u>Issue:</u> $\exists\ f$ s.t $\deg(g) = r$

<u>Q:</u> $X^a \bmod (X^{r+1} - 1) = X^{a \bmod (r+1)}$

$X^{r+1} \bmod (X^{r+1} - 1) = 1$ $\quad X^{r+2} \bmod (X^{r+1} - 1)$

$= (X\,(X^{r+1} \bmod (X^{r+1}-1)) \bmod (X^{r+1}-1)$

$f(X) = f_0 + f_1 X + f_2 X^2 + \cdots + f_r X^r + f_{r+1} X^{r+1} + \cdots + f_{k'-1} X^{k'-1}$

$g(X) = f(X) \bmod (X^{r+1} - 1)$

only $a_b X^b$ contributes to X^r monomial in $g(X)$ iff $b \equiv r \bmod (r+1)$

$\Rightarrow$ deg r term of $g(X) = (f_r + f_{2r+1} + f_{3r+2} \cdots) X^r$

$g(X) = \underbrace{(f_r + f_{2r+1} + f_{3r+2} + \cdots)}_{\text{set all to } 0!} X^r + (\deg \le r-1 \text{ poly})$

Final code: $C^* = \{ \langle f(\alpha) \rangle_{\alpha \in \mathbb{F}_q^*} \mid f(X) = \sum_{j=1}^{k'-1} f_j X^j$ s.t $f_j = 0$ if $j \equiv r \bmod (r+1)$

$\Rightarrow$ for this code can do LRC for any $i \in \mathcal{U}$.

<u>Claim:</u> $\dim(C^*) = k$

$\text{dist}(C^*) \ge n - k' + 1 = n - k - \lceil \frac{k}{r} \rceil + 2$

<u>Fun fact:</u> <u>coset</u> $\alpha\mathcal{U} = \{\alpha, \alpha\omega, \alpha\omega^2, \ldots, \alpha\omega^r\}$

$\mathbb{F}_q^* =$ disjoint union of $\frac{q-1}{r+1}$ cosets $\alpha \cdot \mathcal{U}$

$\forall$ ~~[illegible]~~ $\beta \in \mathbb{F}_q^*$, $\exists \alpha$ s.t. $\beta \in \alpha U$

More fun facts: $\prod_{j=1}^{r} (X - \alpha \omega^j) = X^{r+1} - \alpha^{r+1}$

$g^{(\alpha)}(x) = f(x) \bmod X^{r+1} - \alpha^{r+1}$