| Mar 13 | 1 min checkin

REMINDERS

(•) HW 3 due by 11:59pm this Wed

(•) Mini project report due by 11:59pm ~~in~~ on Wed Mar 29

↳ Make sure y'all follow all the requirements

(•) No in-person lecture on Friday

↳ See piazza post @56 for more details

RECAP

(•) Singleton bound: Any $(n,k,d)_q$ code satisfies $d \le n-k+1$

(•) Polynomial of degree $\bar{d}$, $f(X) = \sum_{i=0}^{\bar{d}} f_i \cdot X^i$ $f_i \in \mathbb{F}_q$, $f_{\bar{d}} \neq 0$

(•) Evaluation of $f(X)$ at $\alpha \in \mathbb{F}_q$, defined as $f(\alpha) = \sum_{i=0}^{\bar{d}} f_i \alpha^i \in \mathbb{F}_q$

α is a root of $f(x)$ if $f(\alpha) = 0$

(•) Poly $E(X) \in \mathbb{F}_q[X]$ of deg s is irreducible if it has no factor of degree >0 and $<s$

(•) $\mathbb{F}_{p^s} \cong \mathbb{F}_p[X]/E(X)$

irr poly of deg s over $\mathbb{F}_p$ (~~*~~ such a poly $\exists$ $\forall$ prime p & int $s \geq 1$)

| Plan for today | Reed Solomon Codes $[n,k,n-k+1]_q$ code for $q \geq n$

Reed-Solomon (RS) codes $[n,k]_q$ code $q \geq n \geq k$

Let $\alpha_1, \dots, \alpha_n$ be distinct elements from $\mathbb{F}_q \Rightarrow q \geq n$

evaluation points

RS: $\mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$

$(m_0, \dots, m_{k-1}) = \bar{m} \in \mathbb{F}_q^k \longmapsto P_{\bar{m}}(X) = \sum_{i=0}^{k-1} m_i X^i$

$P(\alpha_j) = \sum_{i=0}^{k-1} m_i (\alpha_j)^i$

m_0	m_1	·	m_i	...	m_{k-1}
			X^i		

$RS(\bar{m}) = (P_{\bar{m}}(\alpha_1), P_{\bar{m}}(\alpha_2), \dots, P_{\bar{m}}(\alpha_n)) \in \mathbb{F}_q^n$

Ex! $[3,2]_3$ RS $\bar{m} \in \mathbb{F}_3^2$, eval pts: $\mathbb{F}_3$

$\bar{m}$	00	10	20	01	11	21	02	12	22
$P_{\bar{m}}(X)$	$0+0\cdot X$	1	2	X	$X+1$	$X+2$	$2X$	$2X+1$	$2X+2$
$RS(\bar{m})$	(0,0,0)	(1,1,1)	(2,2,2)	(0,1,2)	(1,2,0)	(2,0,1)	(0,2,1)	(1,0,2)	(2,[illegible]

(evaluated at 0 1 2)

Special set of eval pts: $n = q \Rightarrow$ eval pts $= \mathbb{F}_q$

$n = q-1 \xrightarrow[\text{instance}]{\text{common}}$ eval pts $= \mathbb{F}_q \setminus \{0\} \stackrel{\text{def}}{=} \mathbb{F}_q^*$

Claim: RS is a linear code

Pf (sketch) eval pts $\alpha_1, \dots, \alpha_n$

$$RS(\bar{m}_1) + RS(\bar{m}_2) = (P_{\bar{m}_1}(\alpha_1), \dots P_{\bar{m}_1}(\alpha_n)) + (P_{\bar{m}_2}(\alpha_1), \dots, P_{\bar{m}_2}(\alpha_n))$$

$$= (P_{\bar{m}_1}(\alpha_1) + P_{\bar{m}_2}(\alpha_1), \dots, P_{\bar{m}_1}(\alpha_n) + P_{\bar{m}_2}(\alpha_n))$$

$$= (P_{\bar{m}_1+\bar{m}_2}(\alpha_1), \dots, P_{\bar{m}_1+\bar{m}_2}(\alpha_n))$$

$$= RS(\bar{m}_1 + \bar{m}_2)$$

$$P_{\bar{m}_1}(\alpha_1) + P_{m_2}(\alpha_1) = \sum_{i=0}^{k-1} m^1_i (\alpha_1)^i + \sum_{i=0}^{k-1} m^2_i (\alpha_1)^i = \sum_{i=0}^{k-1} (m^1_i + m^2_i)(\alpha_1)^i$$

Also $a \cdot RS(\bar{m}) = RS(a \cdot \bar{m})$

Alt pf $RS(\bar{m})$

$$= \boxed{(m_0 \ m_1 \ \dots \ m_{k-1})} \begin{pmatrix} 1 & & 1 & & 1 \\ \alpha_1 & & \alpha_i & & \alpha_n \\ \alpha_1^2 & & \alpha_i^2 & & \alpha_n^2 \\ \vdots & & \vdots & & \vdots \\ \alpha_1^{k-1} & & \alpha_i^{k-1} & & \alpha_n^{k-1} \end{pmatrix} = (P_{\bar{m}}(\alpha_1), \dots P_{\bar{m}}(\alpha_n))$$

Vandermonde matrix

(full rank iff $\alpha_1, \dots, \alpha_n$ are distinct)

generator matrix for RS code.

$\downarrow$ ith

$m_0 \cdot 1 + m_1\alpha_i + m_2\alpha_i^2 + \dots m_{k-1}\alpha_i^{k-1} = P_{\bar{m}}(\alpha_i)$

"Degree mantra" Any non-zero poly $f(x)$ of deg t has $\le t$ roots.

(assume correct for now)

Claim 2: RS is an $[n, k, \underbrace{n-k+1}]_q$ code

$\alpha_1, \dots, \alpha_n$

by defn

$\Rightarrow d \ge 1 \Rightarrow$ all q^k messages get mapped to distinct codewords

as $k \le n$ $\Rightarrow \dim = k$

Pf: Argue $d \ge n-k+1$ (note by ~~Singlet~~ Singleton bound $d \le n-k+1$)

As RS is linear $\equiv \forall\, \bar{m} \in \mathbb{F}_q^k \setminus \{\bar{0}\}$, $wt(RS(\bar{m})) \ge n-k+1$

$\Leftrightarrow \forall\, \bar{m}$ $\quad wt(P_{\bar{m}}(\alpha_1), \dots, P_{\bar{m}}(\alpha_n)) \ge n-k+1$

$\Leftrightarrow$ $\quad |\{i \mid P_{\bar{m}}(\alpha_i) = 0\}| \le n - (n-k+1) = n-n+k-1 = k-1$

But note $P_{\bar{m}}(X)$ is non-zero, it is of deg $\le k-1 \xRightarrow{\text{degree mantra}} P_{\bar{m}}(X)$ has $\le k-1$ roots

$\Rightarrow |\{i \mid P_{\bar{m}}(\alpha_i) = 0\}| \le$ roots of $P_{\bar{m}}(X) \le k-1$ ■

Pf of degree mantra : By induction on t

Base case: $t = 0$ (as poly is non-zero $\Rightarrow f(X) = cX^0$ $\Rightarrow$ has 0 roots) ✓

I.H. Any non-zero poly of deg $d \le t-1$ has $\le d$ roots

I.S. Want to show any non-zero $f(X)$ of deg t has $\le t$ roots.

Case 1: $f(X)$ has no roots $\Rightarrow$ ✓

Case 2: $\exists$ a root α i.e. $f(\alpha) = 0$

Claim 3: $f(\alpha) = 0 \Leftrightarrow (X-\alpha)$ divides $f(X)$
$f(X) = (X-\alpha) \cdot g(X)$

Claim 3 $\Rightarrow f(X) = (X-\alpha)\cdot g(X)$ note $g(X) \ne 0$ (since $f(X) \ne 0$)

Also $\deg(g) = \deg(f) - 1$

Claim 4: $g(\beta) = 0 \Rightarrow f(\beta) = 0$

Pf: $f(\beta) = (\beta - \alpha)\cdot g(\beta) = 0$

By I.H. g has $\le \deg(f) - 1$ roots $\le t-1$ roots

$\Rightarrow$ # root of $f \le \underset{\alpha}{1}$ + roots of $g \le 1 + t - 1 = t$ ∎