Mar 7

REMINDERS

(i) Clarifications added on HW 2

(ii) Yunus' OH will change ~~(soon)~~ MTW 11-11:50am

(iii) Let me know if a group-mate has resigned the course

↳ Would be a good idea to check w/ your group mates

RECAP:

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

(∘) Poly of deg $\bar{d}$, $f(X) = \sum_{i=0}^{\bar{d}} f_i X^i$ $\quad f_i \in \mathbb{F}_q$, $f_{\bar{d}} \neq 0$

(∘) Poly evaluation: eval at $\alpha \in \mathbb{F}_q$, $f(\alpha) = \sum_{i=0}^{\bar{d}} \underbrace{f_i \alpha^i}_{\text{ops over } \mathbb{F}_q}$

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

(∘) $\mathbb{F}_{p^s} \cong \mathbb{F}_p[X]/E(X)$ irr over $\mathbb{F}_p$ of deg s. (Such a poly $\exists$ $\forall s \ge 1$, prime p)

PROOF READER for today: Gokul

PLAN for today: Reed-Solomon codes $[n,k,n-k+1]_q$ code for $q \ge n$

Reed-Solomon codes $[n,k]_q$ $\quad q \ge n \ge k$

Let $\alpha_1, \ldots, \alpha_n$ distinct elements from $\mathbb{F}_q$. $\Rightarrow q \ge n$

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

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

$RS(\bar{m}) = (P_{\bar{m}}(\alpha_1), P_{\bar{m}}(\alpha_2), \ldots, P_{\bar{m}}(\alpha_n))$

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

$P_{\bar{m}}(X)$:	0	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)	(2,1,0)

Special evaluation pts: $n = q \Rightarrow$ eval pts $\mathbb{F}_q$, $n = q-1 \xrightarrow{\text{common}} \mathbb{F}_q \setminus \{0\} \triangleq \mathbb{F}_q^*$

Claim: RS is a linear code.

Pf (sketch) $RS(\bar{m}_1) + RS(\bar{m}_2) = \text{eval}(P_{\bar{m}_1}(X)) + \text{eval}(P_{\bar{m}_2}(X))$ (at $\alpha_1, \ldots, \alpha_n$)

$= \text{eval}(P_{\bar{m}_1}(X) + P_{\bar{m}_2}(X))$

$= \text{eval}(P_{\bar{m}_1 + \bar{m}_2}(X))$

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

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

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

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

Vandermonde (full rank) generator matrix

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

Claim: RS is $[n, k, n-k+1]_q$

$\alpha_1, \ldots, \alpha_n$ by def

$\to d \geq 1$ (as $k \leq n$)

$\Rightarrow$ distinct messages get mapped to distinct codewords.

Pf: Argue $d \geq (n-k+1)$ { note: $d \leq n-k+1$ by Singleton bound!

Since RS is linear, enough to prove $\forall \bar{m} \in \mathbb{F}_q^k \setminus \{\bar{0}\}$,

$wt(RS(\bar{m})) \geq n-k+1$

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

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

But $P_{\bar{m}}(X)$ is a non-zero poly of deg $\leq k-1$

$\xRightarrow{\text{degree mantra}} P_{\bar{m}}(X)$ has $\leq k-1$ roots in $\mathbb{F}_q$

$\Rightarrow |\{i \mid P_{\bar{m}}(\alpha_i) = 0\}| \leq k-1$ ∎

Pf of degree mantra: By induction on t

Base case $t=0$ (non-zero const. poly $\Rightarrow 0$ roots) ✓

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

I.S. $f(X)$ has deg $t > 0$

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

Case 2: $\exists \alpha \in \mathbb{F}_q$, $f(\alpha)=0$

Claim: If $f(\alpha)=0 \Rightarrow (X-\alpha) \mid f(X)$ — divides

Claim $\Rightarrow$ $f(X) = (X-\alpha)\cdot g(X)$ (but $(X-\alpha)$ doesn't divide $g(X)$)

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

Also $g(X) \neq 0$

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

If $\exists \beta \neq \alpha$ s.t. $f(\beta)=0 \Rightarrow g(\beta)=0$

$$\Rightarrow 0 = f(\beta) = \underbrace{(\beta-\alpha)}_{\neq 0}\cdot \underbrace{g(\beta)}_{=0}$$

$$\Rightarrow \#\text{roots of } f = 1 + \underbrace{\#\text{roots } \beta \neq \alpha}_{\le t-1}$$ (roots of g)

$\le t$ ∎

Pf of claim: By fundamental rule of division

$$f(X) = (X-\alpha)\,g(X) + r(X) \qquad \deg(r) < \deg(X-\alpha) = 1$$

$\Rightarrow \deg(r) = 0 \Rightarrow r(X) = r \in \mathbb{F}_q$

$$\Rightarrow 0 = f(\alpha) = \underbrace{(\alpha-\alpha)\cdot g(\alpha)}_{0} + \underbrace{r(\alpha)}_{r} \Rightarrow r=0$$

$\Rightarrow f(X) = (X-\alpha)\cdot g(X)$.

Reading assignment: MDS