February 26, 2019

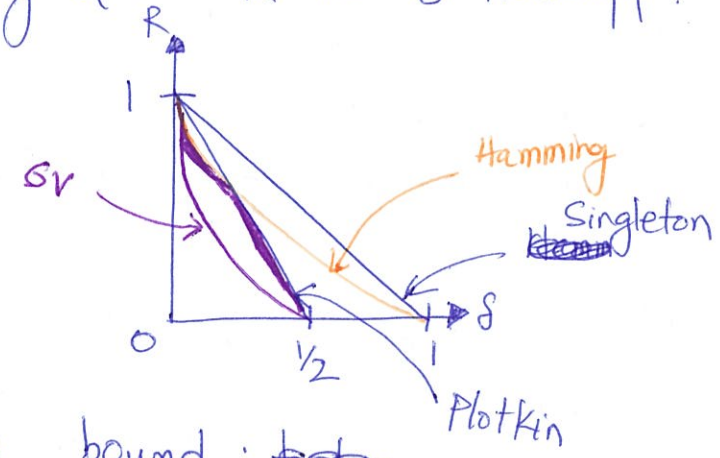
REMINDERS:

- (•) HW 1 due tonight 11:59pm
- (•) Group composition + video topic due Tue Mar 5 at 11:59pm
- (•) HW 2 out by tonight
- (•) 2nd proof reading schedule up

make sure you choose carefully since topic CANNOT be changed later.

RECAP: Big Q: R vs δ tradeoff?

→ $q=2$



→ $\mathbb{F}_p \equiv \mathbb{Z}_p$ (integers mod p, p: prime)

→ Singleton bound: For any $(n,k,d)_q$ code, $k \le n-d+1$.

TODAY (Proof reader: Alex)

(•) Reed Solomon codes: $[n, k, n-k+1]_q$ code (q → prime power, $q \ge n$)

⇒ MEETS Singleton bound

↳ Based on polynomials over $\mathbb{F}_{q^p}$ (p: prime)

↳ Side benefit: will see a representation of elements in $\mathbb{F}_{p^s}$ (p: prime, s ≥ 1 int)

Polynomials

$f(X) = \sum_{i=0}^{\infty} f_i X^i$ (f_i ← coefficient of X^i) $\quad f_i \in \mathbb{F}_q$

→ Only consider finite case: $\sum_{i=0}^{d} f_i X^i$ (represent this as vector $(f_0, f_1, \ldots, f_d) \in \mathbb{F}_q^{d+1}$) $\quad f_d \neq 0$

Ex: $4X^3+5X+6$ is a poly over $\mathbb{F}_7$ $\quad \deg(4X^3+5X+6) = 3$

→ Def (Degree) $f(X) = \sum_{i=0}^{d} f_i X^i$ $\quad f_d \neq 0 \Rightarrow \deg(f) = d$

Def: $\mathbb{F}_q[X]$ = set of all polynomials over $\mathbb{F}_q$

Operations over polys

Addition: $f(X) + g(X) = \sum_{i=0}^{\max(\deg(f),\deg(g))} (f_i + g_i) X^i$

Ex: Over $\mathbb{F}_2$: $1 + (1+X) = X$

Multiplication: $g(X) \cdot f(X)$

$$= \sum_{i=0}^{\deg(f)+\deg(g)} X^i \left(\sum_{j=0}^{\min(i,\deg(f))} g_j f_{i-j} \right)$$

Ex: For $\mathbb{F}_2$ $(1+X)^2 = (1+X)(1+X)$

$= 1 + X(1+1) + X^2 = 1 + X^2$

Evaluation: $f(X)$ evaluated at $\alpha \in \mathbb{F}_q$

$$f(\alpha) = \sum_{i=0}^{\deg(f)} f_i (\alpha)^i$$ over $\mathbb{F}_2$

Eg: $f_1(X) = (1+X)^2$: $f_1(1) = (1+1)^2 = 0^2 = 0$

$f_2(X) = 1 + X^2$: $f_2(1) = 1 + 1^2 = 0$

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

$\Rightarrow$ 1 is a root of $1 + X^2$.

Def (Irreducible poly): $f(X) \in \mathbb{F}_q[X]$ is an irreducible poly (non-constant)

s.t $\nexists\, g_1(X), g_2(X) \in \mathbb{F}_q[X]$ s.t $f(X) = g_1(X) g_2(X)$

$\Rightarrow$ either $g_1(X)$ or $g_2(X)$ has deg 0.

→ Analogous to primes

→ Ex: $1 + X^2$ is not irr over $\mathbb{F}_2$

Only irr of deg 2 over $\mathbb{F}_2$ = $1 + X + X^2$

NOTE: Can have poly with no roots in $\mathbb{F}_q$ that are not irreducible! E.g. $(1 + X + X^2)^2$

Thm: Let $E(X)$ be an irr. poly of deg $s \geq 2$ over $\mathbb{F}_p$ (p: prime)
Then the set of all polynomials mod $E(X)$ is a field
$\mathbb{F}_q[X]/E(X)$ { any $f(X) \in \mathbb{F}_q[X]$, $\exists$ unique poly $q(X)$ & $r(X)$ with $\deg(r) < \deg(E)$

$f(X) = q(X) \cdot E(X) + r(X)$.
$\equiv f(X) \bmod E(X) = r(X)$

Pf: Ex.

$p = 2$ $E(X) = 1 + X + X^2$
$s = 2$ elements of $\mathbb{F}_q[X]/(1+X+X^2)$
$= \{1, X, 1+X, 0\}$

$X \cdot (1+X) \bmod E(X) = X^2 + X \pmod{X^2+X+1} = 1$ ($X^2+X = (1)(X^2+X+1) + 1$)

Trick: $E(X) = X^s + \bar{E}(X)$ $\quad X^s \bmod E(X) = -\bar{E}(X)$

Thm: $\forall s \geq 2$, prime p $\exists$ an irr poly $E(X) \in \mathbb{F}_p[X]$ of deg s. (Asymptotically: $\Theta\left(\frac{p^{s+1}}{s}\right)$)

(Recall: Unique field $\mathbb{F}_{q^s}$ $s \geq 1$
$\Rightarrow \mathbb{F}_{p^s} \cong \mathbb{F}_p[X]/E(X)$ ← irr of deg s.

Reed-Solomon Codes: $[n,k]_q$ $\quad q \geq n \geq k$

Let $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ distinct. (evaluation pts)
$RS: \mathbb{F}_q^k \to \mathbb{F}_q^n$

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

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

Special cases: (i) $n = q$ eval pts $= \mathbb{F}_q$ (ii) $n = q-1$ eval pts $= \mathbb{F}_q \setminus \{0\} \triangleq \mathbb{F}_q^*$

Ex: $[3,2]_3$ RS

(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)
0	1	2	X	X+1	X+2	2X	2X+1	2X+2

Claim: RS is a linear code

Pf (sketch) $RS(\bar{m}_1) + RS(\bar{m}_2) = eval(f_{\bar{m}_1}(x)) + eval(f_{\bar{m}_2}(x))$

$= eval\left(f_{\bar{m}_1}(x) + f_{\bar{m}_2}(x)\right)$

$= eval\left(f_{\bar{m}_1+\bar{m}_2}(x)\right)$

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

$a \cdot RS(\bar{m}_1) = RS(a \cdot \bar{m}_1)$

Alt proof: $RS(\bar{m}) = (m_0\ m_1\ \ldots\ m_{k-1})$ $\begin{pmatrix} 1 & \cdots & 1 & \cdots & 1 \\ \alpha_1 & & \alpha_i & & \alpha_n \\ \vdots & & \vdots & & \vdots \\ \alpha_1^{k-1} & & \alpha_i^{k-1} & & \alpha_n^{k-1} \end{pmatrix}$ ← Vandermonde matrix

---

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

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

$d = n-k+1 \ge 1 \Rightarrow \dim(RS) = k.$

Argue: $d \ge n-k+1$ ($d \le n-k+1$ from Singleton bound)

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

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

$\Leftrightarrow wt(f_{\bar{m}}(\alpha_1), \ldots, f_{\bar{m}}(\alpha_n)) \ge n-k+1$

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

But $f_{\bar{m}}(x)$ has deg $k-1$ & is non-zero $\Rightarrow$ has $\le k-1$ roots

$\Rightarrow |\{i \mid f_{\bar{m}}(\alpha_i) = 0\}| \le k-1$ ✓