|Mar 10| 1 min - check-in

REMINDERS

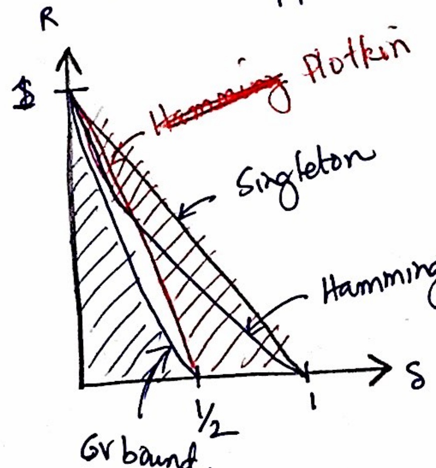
(•) HW 3 due by 11:59pm on Wed

(•) Project report due by 11:59pm on Mar 29 (Wed after Spring break)

RECAP

(•) Big Q : R vs. δ tradeoff

(•) $q = 2$



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

(•) $\mathbb{F}_q \to$ finite field for any $q = p^s$; $p \to$ prime $s \geq 1$ int

(•) Singleton bound: For any $(n, k, d)_q$ code $k \leq n-d+1$
$\equiv d \leq n-k+1$

Next up: Reed - Solomon codes $[n, k, n-k+1]_q$ code $q \geq n$
$\Rightarrow$ meets Singleton bound!

Plan for today: Polynomials!

$f(X) = 4X^3 + 5X + 6$ (Univariate) Polynomials

variable   over $\mathbb{F}_7$

$f(X) = \sum_{i=0}^{\infty} f_i X^i$ s.t $f_i \in \mathbb{F}_q$

monomial

coefficient of X^i

We'll only consider the finite case $f(X) = \sum_{i=0}^{\bar{d}} f_i X^i$ s.t $f_{\bar{d}} \neq 0$ & $\bar{d} < \infty$

$\Rightarrow$ Def (degree) $\to \deg(f) = \bar{d}$

$\deg(4X^3 + 5X + 7) = 3$

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

$f(X) = \sum_{i=0}^{\deg(f)} f_i X^i$ $g(X) = \sum_{i=0}^{\deg(g)} g_i X^i$

Addition: $f(x)+g(x) = \sum_{i=0}^{\max(\deg(f),\deg(g))} \underbrace{(f_i+g_i)}_{\text{over } \mathbb{F}_q} x^i$

Ex: Over $\mathbb{F}_2$ $f(x) = 1\cdot 1 + 0\cdot x$, $g(x) = 1+x$

$$f(x)+g(x) = (1+1)\cdot 1 + (0+1)\cdot x$$
$$= 2+x$$
$$= x$$

Multiplication

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

x^j x^{i-j}

Ex: Over $\mathbb{F}_2$, $f(x) = 1+x = g(x)$

$$f(x)\cdot g(x) = (1+x)(1+x)$$
$$= 1\cdot 1 + 1\cdot x + x\cdot 1 + x\cdot x$$
$$= 1 + x + x + x^2$$
$$= 1 + 2\cdot x + x^2$$
$$\text{over } \mathbb{F}_2 = 1+x^2$$

Note over $\mathbb{F}_2$

$$1+x^2 = (1+x)\cdot(1+x)$$

Division: $\dfrac{g(x)}{f(x)}$ $\deg(g) \geq \deg(f)$

Unique factorization axiom

$\exists\ q(x), r(x)$ s.t. $\deg(r) < \deg(f)$

$$g(x) = q(x)\cdot f(x) + r(x)$$
$$\Rightarrow g(x) \bmod f(x) = r(x)$$

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

$$1+x = \underbrace{1}_{q(x)}\cdot x + \underbrace{1}_{r(x)}$$

Evaluation of a poly $\quad f(X) = \sum_{i=0}^{\deg(f)} f_i X^i \qquad \alpha \in \mathbb{F}_q$

$$f(\alpha) = \sum_{i=0}^{\deg(f)} \underbrace{f_i (\alpha)^i}_{\text{all ops over } \mathbb{F}_q} \in \mathbb{F}_q$$

Ex: (1) $f_1(X) = (1+X)^2 = 1 + X^2$, $f_1(1) = 1 + 1^2 = 1+1 = 2 = 0$
over $\mathbb{F}_2$

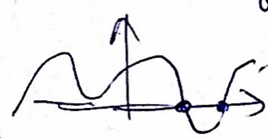
(2) $f_2(X) = 1 + X$, $f_2(4) = 1+4 = 5 \bmod 5 = 0$
over $\mathbb{F}_5$

(3) $f_3(X) = 1 + 2X + X^3$, $f(2) = 1 + 2\cdot 2 + 2^3 = 1+4+8 = 13 \bmod 3 = 1$
over $\mathbb{F}_3$

Def (root) $\alpha \in \mathbb{F}_q$ is a root of $f(X)$ if $f(\alpha) = 0$

Ex: $f_1(X)$ has a root at 1
$f_2(X)$ ——— 4
~~$f_3(X)$~~ 2 is not a root of $f_3(X)$ ← Ex: $f_3(X)$ has no roots in $\mathbb{F}_3$

over $\mathbb{R}$



Def: $E(X) \in \mathbb{F}_q[X]$ of deg $s \geq 1$ is an irreducible poly
if $\forall g_1(X), g_2(X)$ s.t. $E(X) = g_1(X) \cdot g_2(X)$
$\Rightarrow \deg(g_1) = 0$ or $\deg(g_2) = 0$ i.e. either $g_1(X)$ or $g_2(X)$ is a constant poly.

$$\frac{1 + 2X + X^3}{2} = 2 \cdot (1 + 2X + X^3) = 2 + X + 2X^3$$

> Analogous to primes

Ex: (for $\mathbb{F}_2$) $1 + X^2 = (1+X)^2$ is not irr.
Only irr poly over $\mathbb{F}_2$ of deg 2 $\quad 1 + X + X^2$.

~~integer~~ prime $\Leftrightarrow$ irreducible poly

$\mathbb{F}_q$ = integer mod p $\Longleftrightarrow$ polynomials mod irreducible polys
?? $\mathbb{F}_q \to p^s$

Let $E(X)$ be an irreducible poly of deg s over $\mathbb{F}_p$

Look at poly polys over $\mathbb{F}_q[X]$ modulo $E(X)$)

$$P(X) \in \mathbb{F}_q[X] \mapsto P(X) \bmod E(X)$$

Cycle through all polys $\rightarrow$ $\quad \underset{\deg(R(X)) < s}{\overset{\shortparallel}{}}$

cycle through all polys of deg $< s$

$$\left| \mathbb{F}_q[X] / E(X) \right| = p^s \qquad \sum_{i=0}^{s-1} r_i X^i \quad r_i \in \mathbb{F}_p$$

This is a (finite) field. $\equiv \mathbb{F}_{q=p^s}$

$+ \rightarrow$ poly addition

$\times \rightarrow$ poly mult mod $E(X)$

$\exists$ a finite for all p^s $\forall$ prime p : $s \geq 1$

THM: $\forall$ prime p, int $s \geq 1$, $\exists$ an irreducible poly $E(X)$ of deg s over $\mathbb{F}_p$. $\Theta\left(\frac{p^s}{s}\right)$

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

irr poly of deg s over $\mathbb{F}_p$