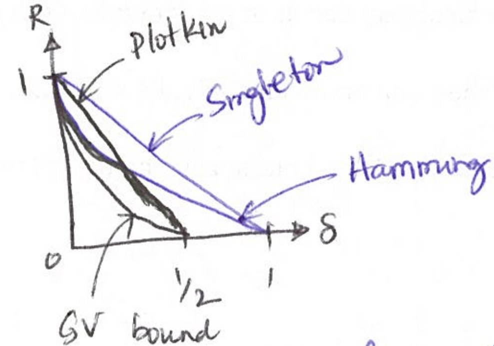
Mar 4 REMINDERS

(1) Video topics have been confirmed

(2) HW 2 submission up on Autolab: apologies for the delay!

RECAP: Big Q: R vs. δ tradeoff?

→ $(q=2)$



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

→ $\mathbb{F}_q$ → finite field for any $q = p^s$; p prime $s \geq 1$ int.

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

Proof reader for today? Felipe

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

Plan for today: Polynomials!!

(Univariate) Polynomials

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

variable

coefficient (of X^i)

Eg. $f(X) = 4X^3+5X+6$

→ Only consider finite case $\sum_{i=0}^{\bar{d}} f_i X^i$ $f_{\bar{d}} \neq 0$

→ $4X^3+5X+6$ is over $\mathbb{F}_7$

→ Def (degree) $f(X) = \sum_{i=0}^{\bar{d}} f_i X^i$, $f_{\bar{d}} \neq 0 \Rightarrow \deg(f) = \bar{d}$

$\deg(4X^3+5X+6) = 3$

→ Def $\mathbb{F}_q[X]$ → denote all polys over $\mathbb{F}_q$

Operations over polys

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

Addition: $f(X) + g(X)$

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

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

$f(X) + g(X)$
$= (1+1)\cdot 1 + (0+1)\cdot X$
$= 2 \cdot 1 + X$
$\xrightarrow{\text{over } \mathbb{F}_2} = X$

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

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

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

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

$$f(\alpha) = \sum_{i=0}^{\deg(f)} f_i \alpha^i \quad \leftarrow \text{ops over } \mathbb{F}_q$$

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

(2) $f_2(X) = 1 + X$ over $\mathbb{F}_5$; $f_2(4) = 1 + 4 = 0$ $\leftarrow$ over $\mathbb{F}_5$

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

Ex: (1) 1 is a root of f_1 (2) 4 is a root of f_2

Def: $E(X) \in \mathbb{F}_q[X]$ of $\deg \geq 1$ is an <u>irreducible</u> poly if

$\forall\, g_1(X), g_2(X) \in \mathbb{F}_q(X)$ s.t. $g_1(X) g_2(X) = E(X)$
$\Rightarrow \deg(g_1) = 0$ or $\deg(g_2) = 0$

$\rightarrow$ Analogous to primes

Ex: (over $\mathbb{F}_2$) $1 + X^2$ is NOT irr over $\mathbb{F}_2$

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

NOTE! $(1+X+X^2)^2$ has no roots over $\mathbb{F}_2$ but is not irreducible.

THM: Let $E(X)$ be an irr. poly of deg $s \geq 2$ over $\mathbb{F}_p$. Then the set of all polys over $\mathbb{F}_p$ mod $E(X)$ is a field.

$\mathbb{F}_p[X]/E(X)$

$\{$ for any $f(X) \in \mathbb{F}_q[X]$, $\exists$ unique polys $q(X)$ & $r(X)$
$\deg(r) < \deg(E)$

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

$\equiv f(X) \bmod E(X) = r(X) \}$

$p=2$ $\quad E(X) = 1+X+X^2$
$s=2$ $\quad \mathbb{F}_2[X]/E(X)$
$= \{1, X, 1+X, 0\}$

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

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

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

THM: $\forall\, s \geq 2$, prime p $\exists$ an irr poly of deg s over $\mathbb{F}_p$.

(Asymptotically $\Theta\left(\frac{p^{s+1}}{s}\right)$ number of irr. poly)

Recall: Unique field $\mathbb{F}_{p^s}$ $\leftarrow$ for any irr poly of deg s

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