| Apr 24 |

1 min checkin

REMINDERS

(•) Project video due in (bit less than) 3 weeks (11:59pm Sun, May 14)
(•) Peer survey due the same time
↳ Will be out last week of class

RECAP

(•) Explicit codes that can be decoded upto $\frac{1}{2}$ (Zyablov bound) in poly time (*)
(•) Explicit BSCp capacity achieving codes + efficient decoding (*)
(*) Assuming $\exists$ poly time unique decoding algo for RS codes (up to $\frac{1-R}{2}$ frac of errors in $O(N^3)$ ops)

Plan for today: Unique decoder for RS codes [Welch-Berlekamp algo]

Last missing piece: Unique decoder for RS codes

Given $1 \le k \le n$ $\quad [n, k, d = n-k+1]_q$ code

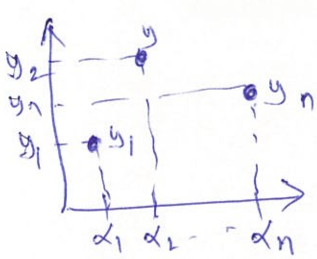
(•) Fix eval points $\underbrace{\alpha_1, \ldots, \alpha_n}_{\text{distinct}} \in \mathbb{F}_q \Rightarrow q \ge n$

Enc: $\bar{m} \in \mathbb{F}_q^k$
$\bar{m} \to P_{\bar{m}}(X) = \sum_{i=0}^{k-1} m_i X^i$
$RS(\bar{m}) = (P_{\bar{m}}(\alpha_1), \ldots, P_{\bar{m}}(\alpha_n))$

(•) Received word $\bar{y} = (y_1, y_i, y_n) \in \mathbb{F}_q^n$
$\alpha_1 \quad \alpha_i \quad \alpha_n$

Syntactic switch: $\underbrace{(\alpha_1, y_1), (\alpha_2, y_2) \ldots, (\alpha_n, y_n)}_{\text{a set! (this obs. used to design hashes for fingerprints)}} \in \mathbb{F}_q \times \mathbb{F}_q$

Input: $(\alpha_i, y_i) \in \mathbb{F}_q^n$ $i \in [n]$



output: poly $P(X)$ of deg $\le k-1$ s.t. for at least $n-e$ values of $i \in [n]$ $P(\alpha_i) = y_i$

$\equiv \le e$ values of $i \in [n]$, $P(\alpha_i) \ne y_i$

$\equiv \Delta\left(\bar{y}, (P(\alpha_i))_{i=1}^n\right) \le e$

$P(X)$ is unique $e < \frac{n-k+1}{2}$

$e < \frac{n-k+1}{2} \Rightarrow$ frac of errs $< \frac{1-R}{2} + \frac{1}{2n}$

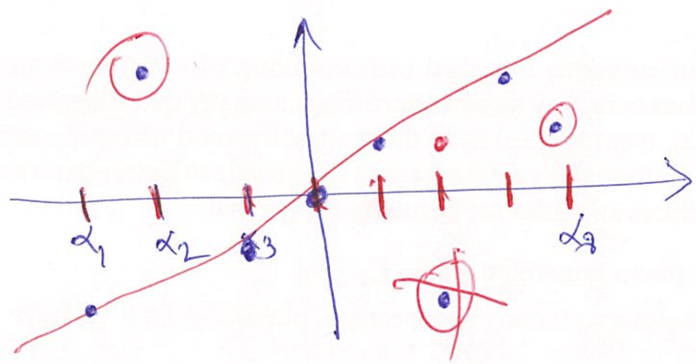
or $e \le \frac{1-R}{}$

Ex: $n = 8$, $k = 2$

$\uparrow$ deg 1 polynomials (pictorially: line)

$e < \frac{n-k+1}{2} = \frac{8-2+1}{2} = \frac{7}{2}$

$e = 3$ $n - e = 5$



Welch-Berlekamp Algo [Gemmell-Sudan]

1. Assume you know $P(X)$
2. Derive certain polynomial identities involving $P(X)$ and $\bar{y}$
3. ———— linear equations s.t $P(X)$ is a valid solution ("forget" ~~to~~ we know $P(X)$)
4. Solve this (Gaussian Elimination; Q2 on HW 0)
5. Argue $P(X)$ is the ONLY solution

Let $P(X)$ be of deg $\leq k-1$ & $P(\alpha_i) \neq y_i$ for $\leq e$ position $i \in [n]$

Def (Error locator poly) $E(X)$ be a poly s.t for all i where $P(\alpha_i) \neq y_i$, $E(\alpha_i) = 0$ $\equiv$ roots of $E(X)$ are the locations of errors

$\Rightarrow E(X) = \prod_{i: P(\alpha_i) \neq y_i} (X - \alpha_i)$ $\rightarrow$ so $E(\alpha_j) = 0 \Leftrightarrow j \in \{i \mid P(\alpha_i) \neq y_i\}$

$\deg(E) \leq e$ $\uparrow$ monic poly $\therefore X^e + \cdots$

Claim: $\forall i \in [n]$ $y_i \cdot E(\alpha_i) = P(\alpha_i) \cdot E(\alpha_i)$

Case 1: $y_i = P(\alpha_i) \Rightarrow$ ~~y~~ LHS = RHS = $y_i E(\alpha_i)$ ✓

Case 2: $y_i \neq P(\alpha_i) \Rightarrow$ LHS = RHS = 0 ✓ ∎

$P(X) = \sum_{j=0}^{k-1} P_j \cdot X^j$, $P(\alpha_i) = \underbrace{\sum_{j=0}^{k-1} P_j \cdot (\alpha_i)^j}_{\text{linear function in } P_0, \ldots, P_{k-1}}$ fixed for fixed α_i

Equations: $\forall i \in [n]$ $\quad y_i \underbrace{E(\alpha_i)}_{\text{linear}} = \underbrace{P(\alpha_i) E(\alpha_i)}_{\text{quadratic}}$

vars: coefficients of $\underset{k}{P(X)}$ & $E(X)$ — E monic of deg $\le e$ $\Rightarrow e$ coefficients.

Overall n quadratic equations in $k+e$ variables

$$k+e < k + \frac{n-k+1}{2} = \frac{n+k+1}{2} \le \frac{2n+1}{2} = n + \frac{1}{2}$$

$$\Rightarrow k+e \le n$$

$\#$vars $\le$ $\#$equations.

Trick (linearization)

$$E(X) \cdot P(X) = N(X)$$
$$\deg(N) \le e+k-1 \Rightarrow e+k \text{ coefficients}$$

$\rightarrow$ $\forall i \in [N]$ $\quad y_i \underbrace{E(\alpha_i)}_{e \text{ vars}} = \underbrace{N(\alpha_i)}_{e+k \text{ vars}}$

vars : coefs of E & N

$$\Rightarrow \# \text{vars} = e+e+k = 2e+k < \frac{(n-k+1)}{2} 2 + k = n-k+1+k$$
$$= n+1$$

or $\#$vars $\le n$ = $\#$ linear equations

$\rightarrow$ Solve the n linear eqns & get $E(X)$ & $N(X)$

from this (hopefully!) $\quad P(X) \leftarrow \frac{N(X)}{E(X)}$

WB algo

i/p: $1 \le k \le n$, $\; 0 < e < \frac{n-k+1}{2}$, n pairs $(\alpha_i, y_i) \in \mathbb{F}_q^2$

o/p: a poly $P(X)$ of deg $\le k-1$ or FAIL

1. Compute a monic $E(X)$ of deg e & $N(X)$ of deg $\le e+k-1$ s.t. $\forall i \in [n]$ $\quad y_i E(\alpha_i) = N(\alpha_i)$
2. If no such $E(X)$ or $N(X)$ $\exists$ output fail.
3. If $E(X)$ doesn't divide $N(X)$ output FAIL
4. $P(X) \leftarrow \frac{N(X)}{E(X)}$
5. If $\deg(P) \ge k$ OR $\Delta(\bar{y}, (P(\alpha_i))_{i=1}^n) > e$ output FAIL
6. return $P(X)$