Apr 20

REMINDERS

(•) HW 6 due by 11:59pm tonight

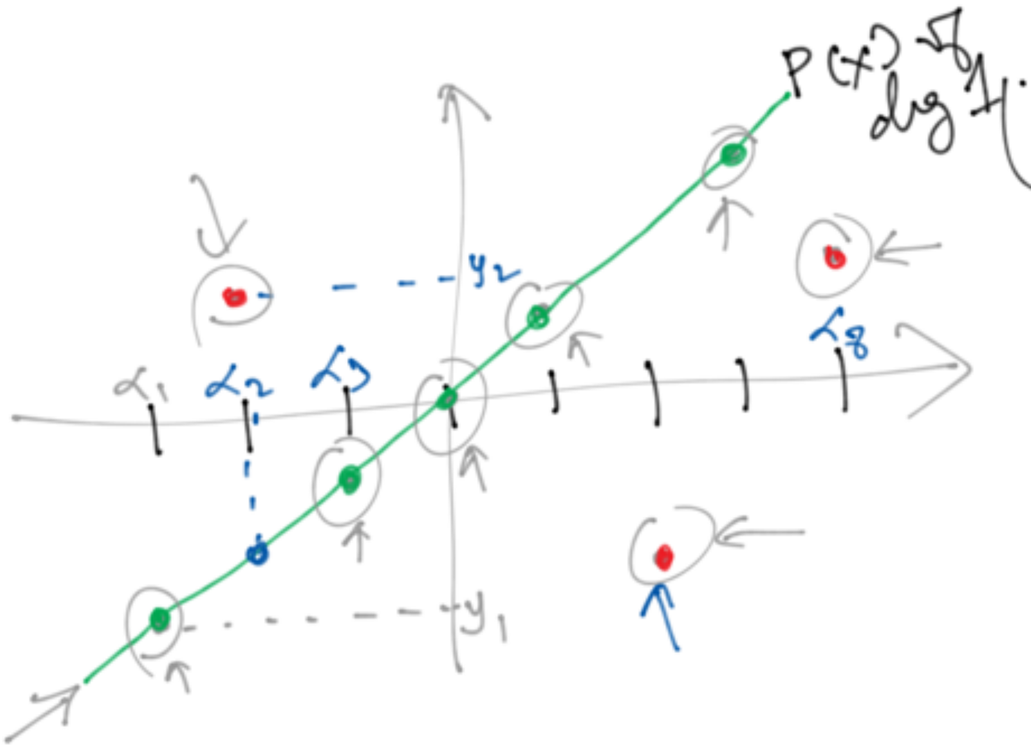
(•) Mini project video due in 3 weeks (May 11)

RECAP

(•) RS unique decoding ($\alpha_1, \dots, \alpha_n$ distinct)

Input: $(y_1,\alpha_1), (y_2,\alpha_2), \dots, (y_n,\alpha_n) \in \mathbb{F}_q \times \mathbb{F}_q$

Output: (Unique) $P(X)$ of degree $< k$ s.t. for at least $\boxed{t = n-e}$ locations $i \in [n]$ $P(\alpha_i) = y_i$ (where $e < (n-k+1)/2$) or $\boxed{t > \frac{n+k-1}{2}}$



$n = 8$

$k = 2$

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

$e = 3$

Q2 in HW 0

Welch-Berlekamp algo $\rightarrow O(n^3)$ ops

n linear equations $\leq n$ vars

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

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

1. Compute a monic $E(X)$ of deg e & $N(X)$ of deg $\leq k+e-1$ s.t. $\boxed{\forall i \in [n] \; N(\alpha_i) = y_i \cdot E(\alpha_i)}$
2. If no such E or N $\exists$, output FAIL
3. If $E(X)$ doesn't divide $N(X)$, output FAIL
4. $P(X) \leftarrow N(X)/E(X)$ — $O(n^3)$ ops "long" division
5. If $\deg(P) \geq k$ or $\Delta(\bar{y}, (P(\alpha_i))_{i=1}^n) > e$ output FAIL
6. Return $P(X)$

2, 3, 5, 6 in $O(n)$

TODAY

(•) Proof readers: Chitra, Daniel

(•) Prove correctness of WB algo (+runtime)

(•) List decoding algos for RS codes

Overall runtime: $O(n^3) + O(n^3) + O(n)$
$= O(n^3)$ [ops over $\mathbb{F}_q$]

Correctness:

① If $P(X)$ is output by WB algo $\Rightarrow$ it is a correct output.

THM: If $P(X)$ is close enough to $\bar{y}$, then WB algo outputs it.

Compute a monic $E(X)$ of deg e & $N(X)$ of deg $\le \boxed{k+e-1}$ s.t. $\forall i \in [n]$ $N(\alpha_i) = y_i \cdot E(\alpha_i)$ } ①

Claim 1: $\exists$ $E^*(X), N^*(X)$ s.t. it satisfies step 1 AND $P(X) = \dfrac{N^*(X)}{E^*(X)}$

$\boxed{\text{Claim 2:}}$ If $\exists$ $(N_1(X), E_1(X)) \neq (N_2(X), E_2(X))$ that both satisfy step 1 $\Rightarrow \dfrac{N_1(X)}{E_1(X)} = \dfrac{N_2(X)}{E_2(X)}$.

Claim 1+2 $\Rightarrow$ Thm is fine.

Pf of Claim 1: $N^*(X) = P(X) \cdot E^*(X)$

$(\Rightarrow P(X) = \dfrac{N^*(X)}{E^*(X)}$ $\deg(N^*) \le k-1+e = k+e-1)$

$$E^*(X) = X^{e - \Delta(\bar{y}, (P(\alpha_i))_{i=1}^n)} \prod_{i:\, P(\alpha_i) \neq y_i} (X - \alpha_i) \Rightarrow \deg(E^*) = e$$

monic

Last time, $\forall i \in [n]$ $N^*(\alpha_i) = y_i \, E^*(\alpha_i)$ ∎

$\deg(E) = e > 0$

$\boxed{\text{claim 2:}}$ If $\exists$ $(N_1(X), E_1(X)) \neq (N_2(X), E_2(X))$ that both satisfy step 1 $\Rightarrow$ $\frac{N_1(X)}{E_1(X)} = \frac{N_2(X)}{E_2(X)}$.

Pf: Assume $(N_1(X), E_1(X)) \neq (N_2(X), E_2(X))$ s.t. $\forall$ $i \in [n]$ $N_1(\alpha_i) = y_i E_1(\alpha_i)$

and $N_2(\alpha_i) = y_i E_2(\alpha_i)$

BUT $\frac{N_1(X)}{E_1(X)} \neq \frac{N_2(X)}{E_2(X)}$. $\quad \cancel{E_1} E_2 \frac{N_1}{\cancel{E_1}} \neq E_1 \cancel{E_2} \frac{N_2}{\cancel{E_2}}$

$\Rightarrow E_2 N_1 - E_1 N_2 \neq 0$

Defn $R(X) = N_1(X) \cdot E_2(X) - N_2(X) E_1(X)$

Note that $R(X) \not\equiv 0$

$\forall$ $i \in [n]$ $R(\alpha_i) = N_1(\alpha_i) E_2(\alpha_i) - N_2(\alpha_i) E_1(\alpha_i)$

$< n$ $\quad = y_i E_1(\alpha_i) E_2(\alpha_i) - y_i E_2(\alpha_i) E_1(\alpha_i)$

$= 0$

$\Rightarrow$ R has at least n roots

contradicts

OTOH $\deg(R) \leq \deg(N) + \deg(E)$

$\leq k + e - 1 + e$

$= 2e + k - 1 \leq 2\left(\frac{n-k+1}{2}\right) + k - 1$

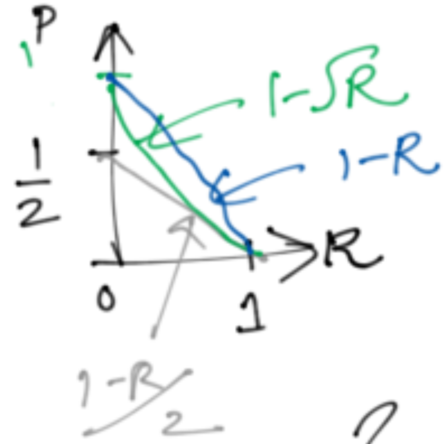
$= n$

Recall: deg mantra
any non-zero poly of
deg d has $\leq$ d roots $\Rightarrow R(X) \equiv 0$

Thm: For any $[n, k, d = n-k+1]_q$ RS codes, WB algo can correct $\le \frac{d-1}{2}$ errors ($\le \frac{1-R}{2}$ frac of errors) in $O(n^3)$ ops over $\mathbb{F}_q$.

List decoding of RS codes

Recall: Johnson bound $\Rightarrow$ RS is $(1-\sqrt{R}, O(n^3))$ list decodable (q is $O(n)$)



Q: Can we efficiently decode RS codes up to $1-\sqrt{R}$ fraction of errors?

A: Yes!

Plan: Algo 1: $1 - 2\sqrt{R}$

Algo 2: $1 - \sqrt{2R}$ (Sudan '96)

Algo 3: $1 - \sqrt{R}$ (Guruswami-Sudan '98)

Input: $(y_1, \alpha_1), \ldots, (y_n, \alpha_n) \in (\mathbb{F}_q)^2$

Output: ALL poly $P(X)$ of deg $\leq k-1$

s.t $P(\alpha_i) = y_i$ for at least t location $i \in [n]$

[in poly time]

WB: $t = \frac{n+k}{2}$

Goal: to make t as small as possible

$t = \sqrt{nk}$

$\equiv \frac{t}{n} = \frac{\sqrt{nk}}{n} = \sqrt{\frac{nk}{n^2}} = \sqrt{\frac{k}{n}} = \sqrt{R}$

Reformulation of WB:

Step 1: Compute $N(X), E(X)$

s.t $\forall i \in [n]$ $N(\alpha_i) = y_i E(\alpha_i)$

Step 2: If $\underline{Y - P(X)}$ divides $YE(X) - N(X) = \underline{Q(X,Y)}$

$\Rightarrow$ output $P(X)$

$\equiv P(X) = \frac{N(X)}{E(X)}$

$\underbrace{E(X)\left(Y - \frac{N(X)}{E(X)}\right)}$