Apr 26

1 min checkin

REMINDER

(•) Video due in ~ 2.5 weeks (11:59pm Sun, May 14)

~~REMINDERS~~

RECAP

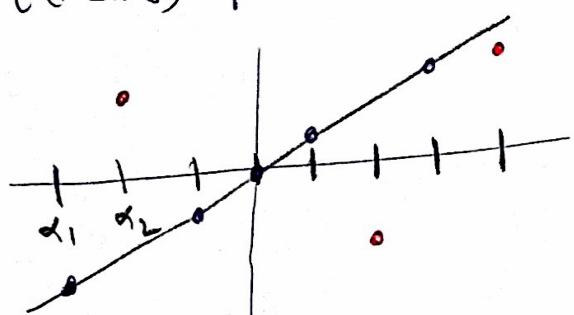
(•) RS Unique decoding ($\{\alpha_1, \dots, \alpha_n\}$ distinct)

Input: $(\alpha_1, y_1), (\alpha_2, y_2), \dots, (\alpha_n, y_n) \in \mathbb{F}_q^2$

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

$n = 8$, $k = 2$

$e = 3$



(•) Welch-Berlekamp algo

Input: $1 \le k \le n$, $0 < e < \frac{n-k+1}{2}$, n pairs $(\alpha_i, y_i) \in \mathbb{F}_q^2$ for all $i \in [n]$

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

n linear equations in $e+k+e \le n$ vars → GE in $O(n^3)$

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

② If no such $N(X)$ or $E(X)$ $\exists$ output FAIL

③ If $E(X)$ doesn't divide $N(X)$, output FAIL

④ $P(X) \leftarrow \frac{N(X)}{E(X)}$ ← "long form" division algo $O(n^3)$

⑤ If $\deg(P) \ge k$ or $\Delta(\bar{y}, (P(\alpha_i))_{i=1}^{n}) > e$, return FAIL

⑥ return $P(X)$

②, ⑤, ⑥ in $O(n)$ time

(•) Degree mantra

Any non-zero poly of deg t has $\le t$ roots

Plan for today (•) Correctness of W.B algo (•) Start with list decoding RS

Overall for WB = $O(n^3) + O(n) = O(n^3)$ ops over $\mathbb{F}_q$

Note: If WB outputs $P(X)$ then it is correct ✓

THM: If $\Delta(\bar{y}, (P(\alpha_i))_{i=1}^{n}) \le e \Rightarrow$ WB algo outputs $P(X)$.

$\exists P(X)$ of deg $\le k-1$

Recall: Step 1 compute monic $E(X)$ of deg e & $N(X)$ of deg $\le \underline{k+e-1}$ s.t. $\forall i \in [n]$ $N(\alpha_i) = y_i E(\alpha_i)$

$P \leftarrow \frac{N(X)}{E(X)}$

Claim 1: $\exists$ $N^*(X), E^*(X)$ s.t they satisfy Step 1 and $P(X) = \frac{N^*(X)}{E^*(X)}$

Claim 2: If $\exists$ $(N_1(X), E_1(X)) \neq (N_2(X), E_2(X))$ s.t both satisfy Step 1 $\Rightarrow$ $\frac{N_1(X)}{E_1(X)} = \frac{N_2(X)}{E_2(X)}$

Claims 1+2 $\Rightarrow$ THM

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

$\Rightarrow P(X) = \frac{N^*(X)}{E^*(X)}$, $\deg(N^*) \le \deg(P) + \deg(E^*)$

$\le k-1+e$

$= k+e-1$

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

Like last time we can show $\forall i$, $\underbrace{P(\alpha_i) \cdot E^*(\alpha_i)}_{N^*(\alpha_i)} = y_i E^*(\alpha_i)$

Pf of Claim 2: Assume $\exists$ $(N_1, E_1) \neq (N_2, E_2)$ s.t. they both satisfy Step 1

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

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

$\equiv E_2(X) N_1(X) \neq E_1(X) N_2(X) \equiv \underbrace{N_1(X) E_2(X) - N_2(X) E_1(X)}_{\overset{\text{def}}{=} R(X)} \neq 0$

Note: $R(X) \neq 0$

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

$= y_i E_1(\alpha_i) E_2(\alpha_i) - y_i E_2(\alpha_i) E_1(\alpha_i) = 0$

$\Rightarrow R$ has $\ge n$ roots

Otw $\deg(R) \le \deg(N) + \deg(E)$ $\qquad e < \frac{n-k+1}{2}$

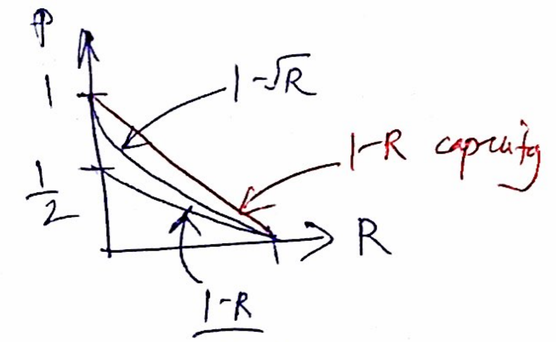
$\le k+e-1+e$

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

$\Rightarrow \deg(R) < n$. (but has $\ge n$ roots & is non-zero)

$\Rightarrow$ contradicts degree mantra ▮

List decoding of RS codes



Recall: Johnson bound $\Rightarrow$ RS code of rate R is $(1-\sqrt{R}, O(n^3))$-l-d $\quad q = O(n)$

Q: Can we efficiently list decode RS codes up to $1-\sqrt{R}$ fraction of errors?
(arithmetic mean $\ge$ geo mean)

A: Yes!

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

Algo 2: $1-\sqrt{2R}$ (Sudan '96) $\quad$ Algo 3: $1-\sqrt{R}$ (Guruswami-Sudan '98)

Input: $k, t, (\alpha_1, y_1), (\alpha_2, y_2), \ldots, (\alpha_n, y_n) \in \mathbb{F}_q^2$

Output: ALL polys $P(X)$ of deg $\le k-1$ s.t. $P(\alpha_i) = y_i$ for at least t positions $i \in [n]$

$\hookrightarrow$ Goal: make t as small as possible.

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

Want $1-\sqrt{R}$

$t = \sqrt{nk}$

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

$\Rightarrow$ frac of error $\approx 1-\sqrt{R}$.

Reformulation of WB:

Step 1: Compute $N(X)$ & $E(X)$ s.t. $\forall i \in [n]$ $N(\alpha_i) = y_i \cdot E(\alpha_i)$

Step 2: If $Y - P(X)$ divides $YE(X) - N(X)$ $\rightarrow$ bivariate poly

$E(X)\left(Y - \frac{N(X)}{E(X)}\right)$ $\rightarrow$ poly in Y coeff in $\mathbb{F}_q[X]$