| May 8 |

1 min checkin

(REMINDER)

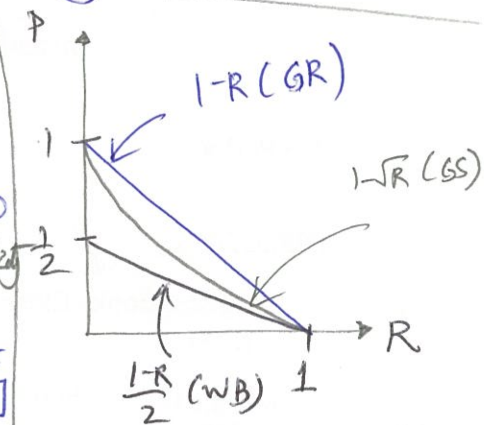
(•) Video and peer survey due by 11:59pm on Sunday
↳ Please check to make sure your team mates are showing up correctly in your peer-survey

RECAP

(•) <u>Generic RS (list) decoder</u>

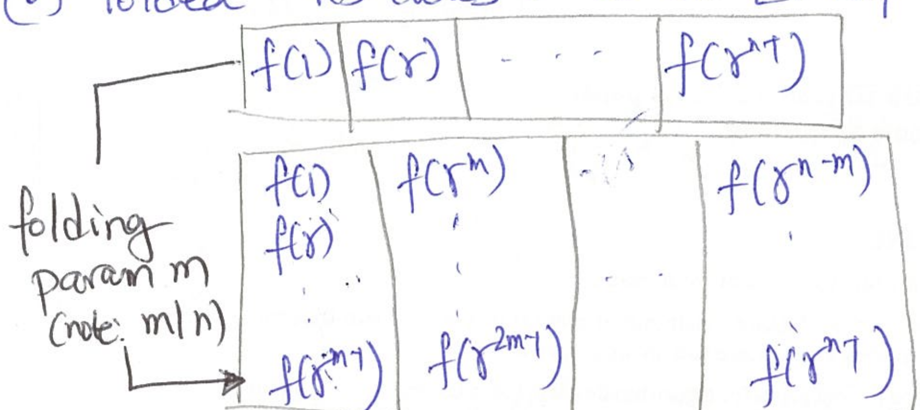
<u>Step 1 (Interpolation)</u> Compute non-zero $Q(X,Y)$ with "some properties" s.t. $\forall i \in [n]$ $Q(\alpha_i, y_i) = 0$ ← with multiplicity

<u>Step 2 (Root finding)</u>: Compute all factors $Y - P(X)$ of $Q(X,Y)$ s.t. (i) $\deg(P) < k$ (ii) $P(\alpha_i) = y_i$ for $\geq t$ values of $i \in [n]$



(•) <u>Welch-Berlekamp (WB) algo</u> $Q(X,Y) = YE(X) - N(X)$ — E: monic $\deg = e$; N: $\deg \leq e+k-1$

(•) Folded RS codes: C be $[n,k]_q$ RS code w/ eval pts $1, \gamma, \gamma^2, \ldots, \gamma^{n-1}$



FRS is $\left(\frac{n}{m}, \frac{k}{m}\right)_{q^m}$ code

(•) FRS can correct $1-\sqrt{R}$ frac of errors ⇒ "unfold" and use GS

Plan for today: (•) Intuition for list decoding FRS codes
(•) Parvaresh-Vardy l.d algo

Claim: FRS code with folding param m has dist $\geq \frac{n}{m} - \frac{k}{m} + 1$

⇒ matches Singleton bound
MDS

Pf: Unfold to get $[n,k]_q$ RS code & use the fact that the code has dist $\geq n-k+1$

Intuition for why FRS can correct > errors than RS
($m=2$)

Ham dist over $\mathbb{F}_q$ →

$\cancel{f(1)}$	$f(\gamma)$	$\cdots$	$\cancel{f(\gamma^{n-2})}$	$f(\gamma^{n-1})$

← $\frac{1}{2}$ frac of errors

for RS:

if $1-\sqrt{R} > \frac{1}{2}$

($\equiv R < \frac{1}{4}$)

then list decoding algo has to handle this error pattern.

$\Downarrow m=2$

Ham dist over $\mathbb{F}_{q^2}$ →

$\cancel{f(1)}$	$\cancel{f(\gamma)}$	$\cdots$	$\cancel{f(\gamma^{n-2})}$
$f(\gamma)$	$f(\gamma^2)$		$f(\gamma^{n-1})$

$\Rightarrow$ 100% of The symbols are in error

$\Rightarrow$ any FRS l-d-algo does NOT have to handle this error pattern.

Crux: We need to handle fewer error patterns in FRS vs RS.

$\Rightarrow$ $m=n$ leads to absurdity!

In our code: m is a constant.

List decoding problem for FRS codes $\quad N=\frac{n}{m}$

i/p: Agreement parameter $0 \le t \le N$ & receiveword

$$\bar{y} = \begin{pmatrix} y_0 & y_m & & y_{n-m} \\ \vdots & \vdots & \cdots & \vdots \\ y_{m-1} & y_{2m-1} & & y_{n-1} \end{pmatrix} \in \mathbb{F}_q^{m\times n} \equiv \left(\mathbb{F}_{q^m}\right)^N$$

o/p: ALL poly $P(X)$ w/ $\deg(P) \le k-1$ s.t. for atleast t values of $i \in [N]$

$$\begin{bmatrix} P(\gamma^{mi}) \\ \vdots \\ P(\gamma^{mi+m-1}) \end{bmatrix} = \begin{bmatrix} y_{mi} \\ \vdots \\ y_{mi+m-1} \end{bmatrix}$$

$m=1 \Rightarrow$ gives RS

Parvaresh - Vardy '05 (not quite, Vadhan; Guruswami '11)

Algo idea: Follow to WB more closely.

Recall: $Q_{WB}(X, Y) = Y E(X) - N(X)$

y_0	y_m		y_{mi}	y_{n-m}
$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$
y_{m-1}	y_{2m-1}	$\cdots$	y_{mi+m-1}	y_{n-1}
1	γ^m		γ^{mi}	γ^{n-m}

Step 1: Compute a non-zero $Q(X, Y_1, \ldots, Y_m)$

$\forall i \in [m]$ $\deg_{Y_i}(Q) = 1$

s.t. $\forall i$

$Q(\gamma^{mi}, y_{mi}, \ldots, y_{im+m-1}) = 0$

$D \to PBD$

Algo (PV)

1. Compute non-zero $Q(X, Y_1, \ldots, Y_m)$ where

$$Q(X, Y_1, \ldots, Y_m) = A_0(X) + Y_1 A_1(X) + Y_2 A_2(X) + \cdots + Y_m A_m(X)$$

$\deg(A_0) \le D + k - 1$, $\deg(A_j) \le D$ $\forall j \in [m]$

s.t. $\forall i$ $Q(\gamma^{mi}, y_{mi}, y_{mi+1}, \ldots, y_{mi+m-1}) = 0$.

(note: $m = 1$ $Q(X, Y) = \underset{-N(X)}{A_0(X)} + Y \underset{E(X)}{A_1(X)}$ $\Rightarrow$ WB)

2. Output all $P(X)$ s.t. $Q(X, P(X), P(\gamma X), P(\gamma^2 X), \ldots P(\gamma^{m-1} X)) = 0$

with $\deg(P) < k$ & for at least t values of $i \in [m]$:

$$\begin{bmatrix} P(\gamma^{mi}) \\ P(\gamma^{mi+1}) \\ \vdots \\ P(\gamma^{mi+m-1}) \end{bmatrix} = \begin{bmatrix} y_{mi} \\ y_{mi+1} \\ \vdots \\ y_{mi+m-1} \end{bmatrix} \quad (*)$$

for $m = 1$

$Q(X, P(X)) = 0$

$\equiv Y - P(X) \mid Q(X, Y)$

$\Rightarrow$ WB

$m = 1 \Rightarrow PV = WB!$

Correctness of PV algo

(Step 1) Claim If $\boxed{(m+1)(D+1)+k-1 > N}$ $\Rightarrow \exists$ a non-zero Q that satisfies Step 1.

Pf: $\cancel{\#\text{eqns}} = \underline{N}$

vars : coeffs $A_0(X)$ $A_j(X)$ $\forall j \in [m]$

$\cancel{\#\text{vars}}$ coeffs $=$ $D+k$ $D+1$

total #vars $= (D+k)+(D+1)m = D(m+1)+k+m$

$= D(m+1)+m+1+k-1 = (m+1)(D+1)+k-1$

$\Rightarrow$ #vars $> N$ $\Rightarrow$ a non-zero Q $\exists$!

Step 2: If $t > D+k-1$, then all polys $P(X)$ that agree with y $\geq t$ locations satisfies $Q(X, P(X), P(\gamma X), \ldots, P(\gamma^{m-1}X)) = 0$

Pf: $R(X) = Q(X, P(X), P(\gamma X), \ldots, P(\gamma^{m-1}X))$

Goal: $R(X) = 0$

$R(\gamma^{mi}) = Q(\gamma^{mi}, P(\gamma^{mi}), P(\gamma \cdot \gamma^{mi}), \ldots, P(\gamma^{m-1} \cdot \gamma^{mi}))$

$= Q(\gamma^{mi}, P(\gamma^{mi}), P(\gamma^{mi+1}), \ldots, P(\gamma^{mi+m-1}))$

If (*) is true for i $\rightarrow$ $= Q(\gamma^{mi}, y_{mi}, y_{mi+1}, \ldots, y_{mi+m-1})$

step 1 $\rightarrow$ $= 0$

$\Rightarrow R(X)$ has $\geq t$ roots

Otoh $\deg(A_0) \leq D+k-1$ $\deg(P(\gamma^{j-1}X) \cdot A_j(X)) \leq D+k-1$

$\Rightarrow \deg(R) \leq D+k-1$

$\Rightarrow$ #roots $>$ deg $\Rightarrow$ $R(X) = 0$ ☺

degree mantra