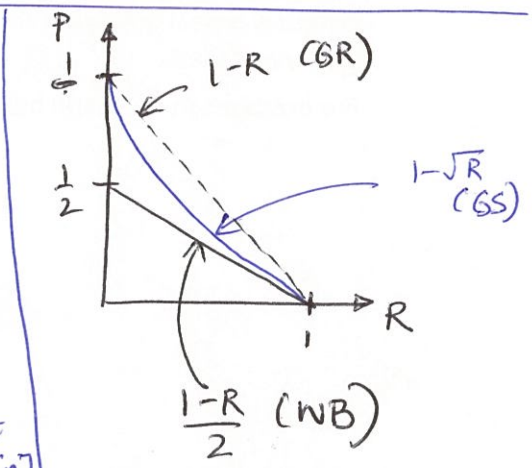
Apr 29

# REMINDERS

(•) Video due < 2 week (by 11:59 pm on Wed, May 11)

(•) All OH for the rest of the semester will be virtual

## RECAP




• Generic RS (list) decoder

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

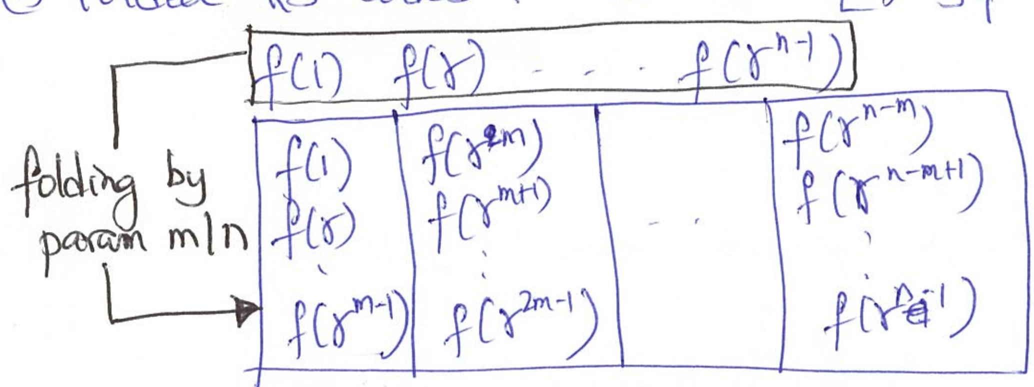
Step 2 (Root finding): Compute all factors $Y - P(X)$ of $Q(X,Y)$ s.t. (i) $\deg(P) < k$ (ii) $P(\alpha_i) = y_i$ for $\geq t$ values $i \in [n]$

• Welch-Berlekamp (WB) algo $\quad Q(X,Y) = Y\underbrace{E(X)}_{\text{monic } \deg = e} - \underbrace{N(X)}_{\deg \leq e+k-1}$

Guruswami-Sudan (GS) algo $\quad Q(X,Y)$ has $(1, k-1)$ wt deg $\leq \sqrt{nkr(r-1)}$ $\left(r = \frac{?}{2(k-1)n}\right)$

s.t. $Q(X,Y)$ has roots at $(\alpha_i, y_i)$ $\forall i \in [n]$ with multiplicity $r$

(•) Folded RS codes: $C$ be $[n,k]_q$ RS code over 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" & use GS

## TODAY

(•) Proof readers: Shweta, Atharva

(•) Parvaresh-Vardy codes

---

Claim: FRS with folding parameter $m$ has dist $\frac{n}{m} - \frac{k}{m} + 1$ (Pf: unfold & use the fact that RS has dist $n-k+1$)

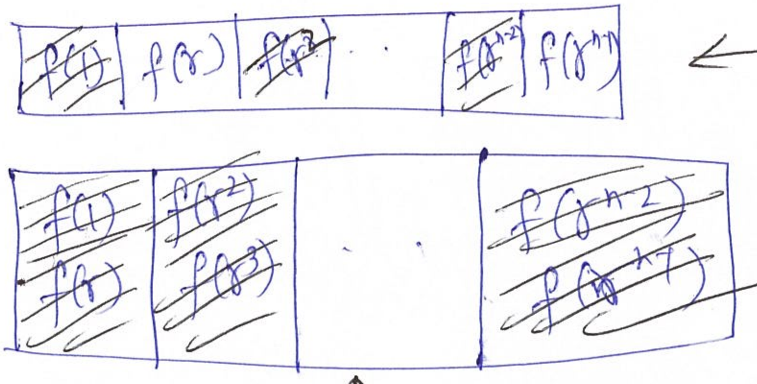
$\Rightarrow$ FRS is MDS

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

Ham dist over $\mathbb{F}_q$

$m=2$ $\Downarrow$

Ham dist over $\to$ $\mathbb{F}_{q^2}$




$\leftarrow \frac{1}{2}$ frac of errors

$\uparrow$

eg: If $1-\sqrt{R} > \frac{1}{2}$

$\Leftrightarrow R < \frac{1}{4}$

need to handle this error pattern in RS list decoder.

$\uparrow$ 100 % error!

we do not need to handle this error pattern for FRS! $\Leftarrow$

$\to$ We have to handle less error patterns for FRS over RS

$\to$ Absurdity ensues if $m=n$

In our case: $m$ is a constant.

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

i/p: Argreement parameter $0 \le t \le N$ and received word

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

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

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

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

<u>Algo idea</u> : Follow WB more closely

(m = 1 $\Rightarrow$ recover WB exactly)

<u>Recall</u>: $Q_{WB}(X,Y) = Y E(X) - N(X)$ $\{ \deg_Y(Q) = 1 \}$

| 1 | $\gamma^m$ | | $\gamma^{n-m}$ |
|---|---|---|---|
| $y_0$ | $y_m$ | | $y_{n-m}$ |
| $\vdots$ | $\vdots$ | $\cdots$ | $\vdots$ |
| $y_{m-1}$ | $y_{2m-1}$ | | $y_{n-1}$ |

<u>Want</u>: (Step 1) Interpolation

Compute a non-zero $Q(X, Y_1, \ldots, Y_m)$ s.t. $\deg_{Y_i}(Q) = 1$ $\forall i \in [m]$

$Q(\gamma^{mi}, y_{mi}, y_{mi+1}, \ldots, y_{m(i+1)-1}) = 0$ $\forall_{0 \le} i < N$

---

Algo (PV) param D: TBD

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

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

s.t $\deg(A_0) \le D+k-1$ & $\deg(A_j) \le D$ $\forall j \in [m]$

for m = 1 WB: $Y_1 \leftarrow Y$, $A_1 \leftarrow E$, $A_0 \leftarrow -N$

where $\forall$ $0 \le i < N$

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

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

s.t. $\deg(P) < k$ & for atleast $t$ values of $0 \le i < N$

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

m = 1 is EXACTLY WB!

# Correctness of PV algo

**Step 1:** If $\boxed{(m+1)(D+1)+k-1 > N} \Rightarrow \exists$ a non-zero $Q(X, Y_1, \ldots, Y_m)$ that satisfies step 1.

Pf: variables: coeff of $\underset{D+k}{\underset{\uparrow}{A_0(X)}}$ & $\underset{D+1}{\underset{\uparrow}{A_j(X)}}$ $\forall j \in [m]$

$$\# \text{var} = D+k+m(D+1) = (m+1)D + m + k$$
$$= (m+1)D + m+1 + k-1$$
$$= (m+1)(D+1)+k-1$$

$\#$ eqns $= N$

$\Rightarrow \#$ vars $> \#$ eqns $\Rightarrow$ non-zero $Q \exists$

**Step 2:** If $\boxed{t > D+k-1}$, then all poly $P(X)$ that agree with $y$ in atleast $t$ locations satisfy

$$Q(X, P(X), P(\gamma X), \ldots, P(\gamma^{m-1}X)) = 0.$$

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

Goal: $R(X) = 0$

Fix any $0 \le i < N$ that satisfies $(\cancel{*})$ ie $P(X)$ agrees with $y$

$P(\cancel{\alpha_i}) \cancel{= Q(\alpha_i, P(\alpha_i)}$

$$P(\gamma^{im}) = Q(\gamma^{mi}, P(\gamma^{mi}), P(\gamma \cdot \gamma^{mi}), \ldots, P(\gamma^{m-1}\gamma^{mi}))$$
$$= Q(\gamma^{mi}, P(\gamma^{mi}), P(\gamma^{mi+1}), \ldots, P(\gamma^{m(i+1)-1}))$$
$$\xrightarrow{\text{by agr w/ } y} = Q(\gamma^{mi}, y_{mi}, y_{mi+1}, \ldots, y_{m(i+1)-1})$$
$$\xrightarrow{\text{by step 1}} = 0$$

$\Rightarrow R$ has $\ge t$ roots.

OTOH, $\deg(R) \le D+k-1$ as $\deg(A_0) \le D+k-1$, $\deg(A_j(X) \cdot P(\gamma^j X)) \le D+k-1$

$\Rightarrow \#$ roots $> \deg \xrightarrow[\text{degree mantra}]{} R(X) = 0.$