May 2

REMINDERS

(•) Video due in ~ 1.5 weeks (by 11:59 pm on Wed, May 11)
→ Make sure to follow ALL instructions!

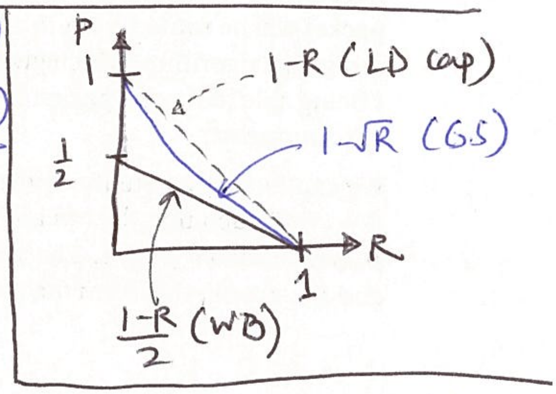
(•) All the rest of my OH will be virtual

(•) 11:59pm on Friday last week of class (May 13) is last deadline! (Survey submission)

$\boxed{\text{RECAP}}$

$\begin{pmatrix} f(1) & & f(\gamma^{n-m}) \\ \vdots & \cdots & \vdots \\ f(\gamma^{m-1}) & & f(\gamma^{n-1}) \end{pmatrix}$

List decoding problem for FRS



I/P: Agreement param $0 \le t < N \leftrightarrow N = \frac{n}{m}$ and received word

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

O/P: All poly $P(X)$ of deg $\le k-1$ s.t. for atleast t values $0 \le i < N$:

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

Algo (PV) $\boxed{\text{TBD}: D}$

1. Compute non-zero $Q(X, Y_1, \ldots, Y_m)$ where
$Q(X, Y_1, \ldots, Y_m) = A_0(X) + A_1(X)Y_1 + \cdots + A_m(X)Y_m$
s.t. $\deg(A_0) \le D+k-1$, $\deg(A_j) \le D \quad \forall j \in [m]$
where $\forall\ 0 \le i < N$:
$Q(\gamma^{mi}, y_{mi}, y_{mi+1}, \ldots, y_{m(i+1)-1}) = 0$

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

$\boxed{\text{TODAY}}$

(•) Proof readers: Deepak, Pratik

(•) Compute p vs R tradeoff $\left(\frac{m}{m+1}(1-\boxed{m}R) \le p\right)$ get rid of this factor

(•) Towards getting $1-R-\varepsilon$ frac of errors (2nd FRS LD algo)

Last time: Lemma 1 If $(m+1)(D+1)+k-1 > N \Rightarrow$ step 1 is correct

Lemma 2: If $t > D+k-1 \Rightarrow$ step 2 is correct

Param choice: $D = \left\lfloor \frac{N-k+1}{m+1} \right\rfloor$ $\qquad x+1 > \lfloor x \rfloor$

$$\Rightarrow (m+1)(D+1)+k-1 > (m+1)\left(\frac{N-k+1}{m+1}\right)+k-1 \qquad R = \frac{k/m}{n/m}$$

$$= N-k+1+k-1 = N$$

For Lemma 2 to be satisfied it is enough to sh

$$t > \frac{N-k+1}{m+1}+k-1 = \frac{N}{m+1} + \left(\frac{m}{m+1}\right)(k-1) \qquad \frac{k}{N} = m \cdot R$$

$$\Leftarrow t \geq \frac{N}{m+1} + \left(\frac{m}{m+1}\right)k = N\left(\frac{1}{m+1} + \frac{m}{m+1} \cdot mR\right) \qquad = \frac{k}{n/m} = m \cdot \frac{k}{n}$$

$$\Rightarrow \text{frac of errors} \le 1 - \frac{t}{N} = \frac{m}{m+1}(1-mR)$$

get rid of this

this beats $1-\sqrt{R}$ for $R \to 0$

TODO: show algo can be implemented in poly time.

Basic intuition for next algo $\qquad$ Let's say $m=3$

An agreement over $\mathbb{F}_{q^3}$

$$\boxed{\begin{matrix} P(\gamma^{3i}) \\ P(\gamma^{3i+1}) \end{matrix}} = \boxed{\begin{matrix} y_{3i} \\ y_{3i+1} \end{matrix}} \text{ AND } \boxed{\begin{matrix} P(\gamma^{3i+1}) \\ P(\gamma^{3i+2}) \end{matrix}} = \boxed{\begin{matrix} y_{3i+1} \\ y_{3i+2} \end{matrix}} \Leftarrow \begin{bmatrix} P(\gamma^{3i}) \\ P(\gamma^{3i+1}) \\ P(\gamma^{3i+2}) \end{bmatrix} = \begin{bmatrix} y_{3i} \\ y_{3i+1} \\ y_{3i+2} \end{bmatrix}$$

Instead of 1 ~~algo~~ roots we get 2 roots!

More generally:

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

If we "slide" a window of size s, one agreement over $\mathbb{F}_{q^m}$ $\Rightarrow$ $(m-s+1)$ agreements over $\mathbb{F}_{q^s}$

Algo (Gur R. 06, Gur 11)

$\boxed{\text{TBD} : D}$

$s = m \Rightarrow$ prev algo

1. Compute a non-zero $Q(X, Y_1, \ldots, Y_s)$ s.t.

$$Q(X, Y_1, \ldots, Y_s) = A_0(X) + A_1(X)Y_1 + \cdots + A_s(X)Y_s$$

w/ $\deg(A_0) \le D+k-1$, $\deg(A_\ell) \le D$ $\forall$ $\ell \in [s]$

s.t $\forall$ $0 \le i \le N$, $0 \le j \le m-s$ we have

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

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

Correctness

Lemma 3: If $D \ge \left\lfloor \dfrac{N(m-s+1)-k+1}{s+1} \right\rfloor \Rightarrow$ step 1 is correct

Pf: Goal: # coeff > # eqns.

coeff in Q $= D+k + s(D+1) = (s+1)(D+1)+k-1$

eqns $= N(m-s+1)$

we need # coeffs > # eqns

$$\Leftarrow (s+1)(D+1)+k-1 > N(m-s+1)$$

$$\Leftarrow (s+1)(D+1) > N(m-s+1)-k+1$$

$$\Leftarrow D+1 > \frac{N(m-s+1)-k+1}{s+1}$$

implies

We'll choose $D = \left\lfloor \dfrac{N(m-s+1)-k+1}{s+1} \right\rfloor$

Lemma 4: If $t > \dfrac{D+k-1}{m-s+1} \Rightarrow$ step 2 is correct

Let $P(X)$ satisfy $(*)$

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

Goal: show $R(X) = 0$ (same argument as last time)

$\deg(R) \le D+k-1$

New Goal: argue # roots > deg $\xrightarrow{\text{degree mantra}}$ $R(X) = 0$

Fix any $0 \le i < N$ s.t. ← there are t such i's.

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

s

$\Rightarrow \forall \quad 0 \le j \le m-s$

$$R(\gamma^{mi+j}) = Q(\gamma^{mi+j}, P(\gamma^{mi+j}), P(\gamma \cdot \gamma^{mi+j}), \dots, P(\gamma^{s-1} \cdot \gamma^{mi+j}))$$

$$= Q(\gamma^{mi+j}, P(\gamma^{mi+j}), P(\gamma^{mi+j+1}), \dots, P(\gamma^{mi+j+s-1}))$$

$$\xrightarrow{\text{agreement above}} = Q(\gamma^{mi+j}, y_{mi+j}, y_{mi+j+1}, \dots, y_{mi+j+s-1})$$

$$\xrightarrow{\text{step 1}} = 0$$

$\#$ roots $\ge t(m-s+1)$

need $\#$ roots $>$ deg $\Leftarrow t(m-s+1) > D+k-1$

$$\Leftrightarrow t > \frac{D+k-1}{m-s+1}.$$

$$\xrightarrow[\text{monotone}]{\text{deg}} R(X) = 0$$

Choice of params $D = \left\lceil \frac{N(m-s+1)-k+1}{s+1} \right\rceil$

need $t > \left\lfloor \frac{D+k-1}{s+1} \right\rfloor$

Algo can correct from $\underbrace{\frac{s}{s+1}}_{\sim 1-\varepsilon}\left(1 - \underbrace{\left(\frac{m}{m-s+1}\right)}_{\sim 1-\varepsilon} R\right)$ frac of errors

↳ note if $s = m \rightarrow \frac{m}{m+1}(1 - mR)$

↳ If $s \sim \frac{1}{\varepsilon}$, $m \sim \frac{1}{\varepsilon^2}$

$\Rightarrow$ frac of err $1 - R - \varepsilon$!