| May 9 | | 1 min checkin |

REMINDER

(•) Video + peer survey due by 11:59 pm this Sunday

RECAP

$f(1)$		$f(\gamma^{n-m})$
$\vdots$	....	$\vdots$
$f(\gamma^{m-1})$		$f(\gamma^{n-1})$

(•) List Decoding problem for FRS

I/p: Agreement parameter $0 \le t < N \Leftrightarrow N = n/m$ and received word

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

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

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

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

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

Lem1: $(m+1)(D+1) + k - 1 > N \Rightarrow$ step 1 is correct

Lem2: $t > D + k - 1 \Rightarrow$ step 2 is correct

for large enough m as $R \to 0$ $\quad > 1 - \sqrt{R}$

Plan for today | (•) Compute p vs R tradeoff in PV $\quad \boxed{\frac{m}{m+1}(1 - mR) \le p}$

(•) Towards getting $p = 1 - R - \varepsilon$ fraction of errors (another FRS LD algo)

useless if $R > \frac{1}{m}$

Param choice: $D = \left\lfloor \frac{N-k+1}{m+1} \right\rfloor$ $\quad$ (Note: $1 + \lfloor X \rfloor > X$)

$\quad$ $\lfloor X \rfloor$ + frac. part

$\Rightarrow (m+1)(D+1) + k - 1 > \cancel{(m+1)} \frac{(N-k+1)}{\cancel{m+1}} + k - 1 = N \cancel{-k+1+k-1}$

$= N \Rightarrow$ Lem 1 condition holds $\Rightarrow$ step 1 is correct.

For step 2 to be correct, by Lem 2 it is enough if

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

$R = \frac{k}{n} = \frac{k}{Nm} \Rightarrow \frac{k}{N} = Rm$

$$\Leftrightarrow t > \frac{N}{m+1} - \frac{(k-1)}{m+1} + k - 1 \Leftrightarrow$$

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

$$\Leftarrow t \geq \frac{N}{m+1} + \frac{k \cdot m}{m+1} = \frac{N}{\cancel{m+1}}\left(\frac{1}{m+1} + \frac{m}{m+1} \cdot \frac{k}{N}\right)$$

$$= \frac{N}{\cancel{m+1}}\left(\frac{1}{m+1} + \frac{m}{m+1} \cdot Rm\right)$$

frac of errors $p \le 1 - \frac{t}{N} = 1 - \frac{1}{\cancel{m+1}}\left(\frac{1}{m+1} + \frac{m\,Rm}{m+1}\right)$

$$= \frac{m}{m+1} - \frac{m}{m+1} \cdot Rm = \frac{m}{m+1}\left(1 - R\boxed{m}\right)$$

beats $1 - \sqrt{R}$ as $R \to 0$ but get rid of this

Next up: Get $1 - R - \varepsilon$ frac of errors.

Intuition   Say $m = 3$ agreement at $0 \le i < \frac{N}{3}$

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

2 agreements over $\mathbb{F}_{q^2}$ $\Longleftarrow$ Currently 1 agreement over $\mathbb{F}_{q^3}$

For general m:

If we "slide" a window of size $s \le m$

1 agreement over $\mathbb{F}_{q^m}$ $\Rightarrow (m-s+1)$ agreement over $\mathbb{F}_{q^s}$.

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

Algo (Guruswami, R '06, Guruswami '11) D: TBD

1. Compute non-zero $Q(X, Y_1, \ldots, Y_s) = \underline{A_0}(X) + Y_1 A_1(X) + \cdots + Y_s A_s(X)$
with $\deg(A_0) \leq D+k-1$, $\deg(A_j) \leq D$ $\forall j \in [s]$
s.t $\forall 0 \leq i < N$, $0 \leq j \leq m-s$
$$Q(\gamma^{mi+j}, y_{mi+j}, y_{mi+j+1}, \ldots, y_{mi+j+s-1}) = 0$$
2. Output all poly. $P(X)$ s.t $\deg(P) \leq k-1$
& $Q(X, P(X), P(\gamma X), \ldots, P(\gamma^{s-1} X)) = 0$

Correctness:

Lem 3: If $D \geq \left\lfloor \frac{N(m-s+1) - k+1}{s+1} \right\rfloor \Rightarrow$ Step 1 is correct.

Pf: Goal: # vars > # equats.

Same calculations from Mon

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

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

vars > # eqns $\Leftrightarrow (s+1)(D+1) + k-1 > N(m-s+1)$

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

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

Pick $D = \left\lfloor \frac{N(m-s+1) - k+1}{s+1} \right\rfloor$

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

Pf: Let $P(X)$ satisfy (*) $R(X) = Q(X, P(X), P(\gamma X), \ldots, P(\gamma^{s-1} X))$
Want $R(X) = 0$
$\deg(R) \leq D+k-1$ (same argument as in Mon)

Goal: # roots $> D+k-1$ $(\geq \deg(R)) \xrightarrow[\text{mantra}]{\text{by degree}} R(X) = 0)$

Fix $0 \le i < N$ s.t

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

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

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

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

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

by step 1 $\rightarrow\ = 0 \Rightarrow \gamma^{mi+j}$ is a root of R

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

We get Goal' if $t(m-s+1) > D+k-1$

$\iff t > \dfrac{D+k-1}{m-s+1}$

$$D = \left\lfloor \frac{N(m-s+1)-k+1}{s+1} \right\rfloor$$

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

$\vdots$

Algo can correct $\dfrac{s}{s+1}\left(1 - \left(\dfrac{m}{m-s+1}\right)R\right)$

$s \sim \dfrac{1}{\varepsilon}$ $\quad m \sim \dfrac{1}{\varepsilon^2}$ $\quad \rightarrow\ \ge 1-R-\varepsilon$!