May 4

REMINDERS

(•) Video due in 1 week! (by 11:59 pm on Wed, May 11)
(•) Survey due by 11:59 pm on Fri, May 13

List decoding algo for FRS

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

1. Compute non-zero $Q(X, Y_1, \ldots, Y_s)$ with
$Q(X, Y_1, \ldots, Y_s) = A_0(X) + A_1(X)Y_1 + \cdots + A_s(X)Y_s$
s.t. $\deg(A_0) \le D+k-1$, $\deg(A_\ell) \le D$ $\forall \ell \in [s]$
s.t. $\forall\ 0 \le i < N$, $0 \le j \le m-s$, 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. $\deg(P) < k$ where for at least $t \ge \left\lfloor \frac{D+k-1}{m-s+1} \right\rfloor$ values of $0 \le i < N$
$$\begin{bmatrix} P(\gamma^{mi}) \\ \vdots \\ P(\gamma^{m(i+1)-1}) \end{bmatrix} = \begin{bmatrix} y_{mi} \\ \vdots \\ y_{m(i+1)-1} \end{bmatrix}$$

Last time: Algo is correct.
<u>Params</u>: $s = \theta(\frac{1}{\varepsilon})$ & $m = \theta(\frac{1}{\varepsilon^2}) \Rightarrow$ Algo can list decode from $1-R-\varepsilon$ frac. of errors

---

TODAY

(•) <u>Proof readers</u>: Shantanu, Chaudhury
(•) Argue algo (Step 2) can be implemented in poly time.

<u>Goal</u>: Show that # $f(X)$ of deg $< k$ s.t.
$$Q(X, f(X), f(\gamma X), \ldots, f(\gamma^{s-1}X)) = 0 \quad \text{—— } (*)$$
is $\le q^{s-1}$. $\sim n^{O(1/\varepsilon)}$

Corollary of the proof $\Rightarrow$ Algo is poly time $— n^{O(1/\varepsilon)}$

(*) is same as # $f(X)$ s.t. known

$$A_0(X) + A_1(X)\,f(X) + A_2(X)\,f(\gamma X) + \cdots + A_s(X)\,f(\gamma^{s-1}X) = 0 \quad (\#)$$

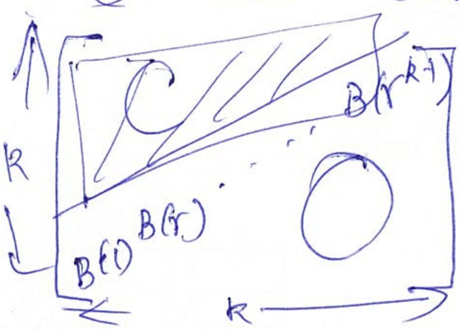
is $\le q^{s-1}$

unknowns: coefficients of

$$f(X) = f_0 + f_1 X + \cdots + f_{k-1}X^{k-1}$$

linear equations in $f_0, \ldots, f_{k-1}$

Overall argument: ~~(#) is same as~~ Any solution that satisfies (#) also satisfies

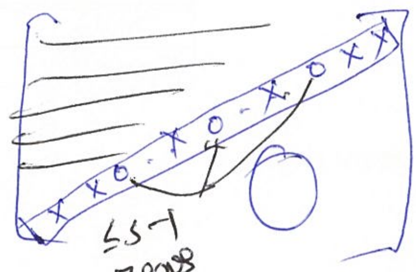


$$C\begin{bmatrix} f_0 \\ f_1 \\ \vdots \\ f_{k-2} \\ f_{k-1} \end{bmatrix} = \begin{bmatrix} -a_{0,k-1} \\ -a_{0,k-2} \\ \vdots \\ -a_{0,1} \\ -a_{0,0} \end{bmatrix}$$

variables ... fixed values

$\Rightarrow B(X)$ has $\le s-1$ roots

$\Rightarrow B(\gamma^i) = 0$ for $\le s-1$ values of $0 \le i \le k-1$



Fact: The rank of a upper Δ matrix $\ge$ # non-zeroes in the diagonal

$\Rightarrow$ C has rank $r \ge k-(s-1)$

Recall: Q2 on HW0 if $\mathrm{rank}(C) = r \Rightarrow$ system has $\le q^{k-r}$ solutions

$\Rightarrow \le q^{k-(k-(s-1))} = q^{s-1}$ ∎

Lemma: $\deg(A_0) \le D+k-1$, $\deg(A_\ell) \le D$. Then $\le q^{s-1}$ solutions to $f(X) = f_0 + f_1X + \cdots + f_{k-1}X^{k-1}$ to the eqns

$$A_0(X) + A_1(X)\,f(X) + A_2(X)\,f(\gamma X) + \cdots + A_s(X)\,f(\gamma^{s-1}X) = 0 \quad (e)$$

Pf: Define $a_{i,j}$ $\;0 \le i \le s$, $\;0 \le j \le D+k-1$

$$A_i(X) = \sum_{j=0}^{D+k-1} a_{ij}X^j \qquad \text{Note } a_{i,j} = 0 \text{ if } i>0,\ j>D$$

Assume X doesn't divide all of $A_0(X), A_1(X), \ldots, A_s(X)$

$\Rightarrow \exists\, i^* > 0$ s.t. $a_{i^*,0} \neq 0$

(if not i.e. $X \mid A_i(X)\ \forall i>0 \Rightarrow$ by (e) $X \mid A_0(X)$)

Define $B(X) = a_{1,0} + a_{2,0}X + a_{3,0}X^2 + \cdots + a_{s,0}X^{s-1}$

As $a_{i^*,i} \neq 0 \Rightarrow B(X) \neq 0$ & $\deg(B) \leq s-1$

~~degree~~ mantra $B(X)$ has $\leq s-1$ roots.

<u>Claim</u>: for every $0 \leq j \leq k-1$ — for $j=0 \Rightarrow f_0$ is fixed.

(•) If $B(\gamma^j) \neq 0 \Rightarrow f_j$ is uniquely determined by $f_{j-1}, f_{j-2}, \ldots, f_0$.

(•) If $B(\gamma^j) = 0 \Rightarrow f_j$ can take any value in $\mathbb{F}_q$.

Assume Claim is correct.

$1, \gamma, \ldots, \gamma^{k-1}$ are distinct $\Rightarrow$ for $\leq s-1$ values of j $B(\gamma^j) = 0$

$\Rightarrow \leq q^{s-1}$ solutions to $(f_0, \ldots, f_{k-1})$

TODO: Get rid of assumption that $X \mid A_0(X), \ldots, A_s(X)$

If not let X^l for some $l \geq 1$ be the largest power of X that divides all of $A_i(X)$

$A_i(X) = X^l \cdot A'_i(X)$

$$X^l \boxed{\left(A'_0(X) + A'_1(X)f(X) + A'_2(X)f(\gamma X) + \cdots + A'_s(X)f(\gamma^{s-1}X)\right) = 0}$$

$\Rightarrow$ redo argument by replacing $A_i(X)$ with $A'_i(X)$. — work with this.

<u>Pf of Claim</u> — Assume $X \nmid$ all of A_i

$$C(X) \stackrel{def}{=} A_0(X) + A_1(X)f(X) + \underline{A_2(X)f(\gamma X)} + \cdots + A_s(X)f(\gamma^{s-1}X)$$

$$= \underline{a_{0,0}} + a_{0,1}X + a_{0,2}X^2 + \cdots + a_{0,D+k-1}X^{D+k-1}$$

$$+ (\underline{a_{1,0}} + a_{1,1}X + a_{1,2}X^2 + \cdots + a_{1,D}X^D)(\underline{f_0} + f_1X + f_2X^2 + \cdots + f_{k-1}X^{k})$$

$$+ (a_{2,0} + a_{2,1}X + a_{2,2}X^2 + \cdots + a_{2,D}X^D)(f_0 + f_1\gamma X + f_2\gamma^2X^2 + \cdots + f_{k-1}\gamma^{k-1}X^{k-1})$$

$\vdots$

$$+ \left(a_{s,0} + a_{s,1}X + a_{s,2}X^2 + \cdots + a_{s,D}X^D\right)\left(f_0 + f_1\gamma^{s-1}X + f_2\gamma^{2(s-1)}X^2 + \cdots + f_{k-1}\gamma^{(k-1)(s-1)}X^{k-1}\right)$$

$$= c_0 + c_1X + c_2X^2 + \cdots + c_{D+k-1}X^{D+k-1}$$

Note $c_0 = c_1 = \cdots = c_{D+k-1} = 0$

↳ we'll only use $c_0 = c_1 = \cdots = c_{k-1} = 0$

Consider Claim for $j=0$ $\quad c_0 = 0$

$$0 = c_0 = a_{0,0} + a_{1,0}f_0 + a_{2,0}f_0 + \cdots + a_{s,0}f_0$$

$$\Rightarrow a_{0,0} + f_0\left(a_{1,0} + a_{2,0} + \cdots + a_{s,0}\right) = 0$$

$$\Rightarrow \underbrace{a_{0,0}}_{\text{known}} + f_0\underbrace{B(1)}_{\text{known}} = 0$$

Case 1: $B(1) \neq 0 \Rightarrow f_0 = \dfrac{-a_{0,0}}{B(1)}$

$\Rightarrow f_0$ is fixed.

Case 2: $B(1) = 0 \Rightarrow$ no constraint on f_0

Consider $j=1 \Rightarrow c_1 = 0$

$$0 = c_1 = a_{0,1} + a_{1,0}\cdot f_1 + a_{1,1}f_0 + a_{2,0}f_1\gamma + a_{2,1}\cdot f_0 + \cdots + a_{s,0}f_1\gamma^{s-1} + a_{s,1}f_0$$

$$\Rightarrow a_{0,1} + f_1\left(a_{1,0} + a_{2,0}\cdot\gamma + a_{3,0}\gamma^2 + \cdots + a_{s,0}\gamma^{s-1}\right) + f_0\left(\sum_{j=1}^{s} a_{j,0}\right) = 0$$

$$\Rightarrow a_{0,1} + f_1 B(\gamma) + f_0\cdot b_0^{(1)} = 0$$