Addendum to Folded-Reed-Solomon Codes + Decoding

1 The codes

$FRS_{n,k,m,\gamma}$:

Map : $P(x) \in \mathbb{F}_q^{<k}[X]$

to $\left\langle \left[P(\alpha_i)\ P(\gamma\alpha_i) \dots P(\gamma^{r-1}\alpha_i) \right] \right\rangle_{i=1}^{n}$

- Maps $\mathbb{F}_q^k \longrightarrow \left(\mathbb{F}_q^r\right)^n$
- Rate $= \dfrac{k}{r \cdot n} = R$
- Claim : can list decode from $1-R-\epsilon$ fraction errors !

~~Algorithm : Step 1 : find $A_0(X)$; $A_1(X) \dots A_r(X)$ s.t~~

Problem: Given:

$\alpha_1 \ldots\ldots \alpha_n$

$\beta^1_1 \ldots\ldots \beta^1_n$

$\vdots$

$\beta^r_1 \ldots\ldots \beta^r_n$

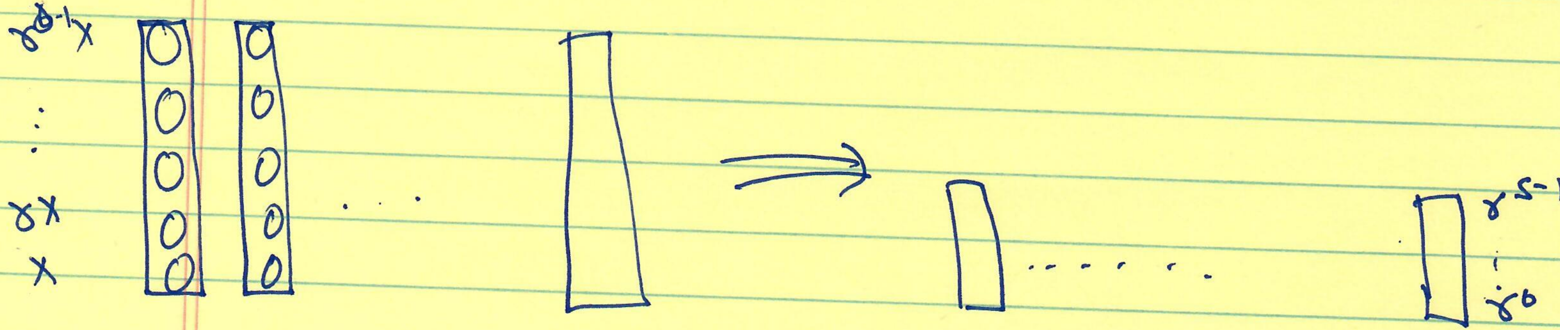
find all Poly $P \in \mathbb{F}_q^{<k}[x]$ s.t.

(*) $$\#\{i \mid \forall j \;\; P(\gamma^{j-1}\alpha_i) = \beta^j_i\} \geq \frac{n}{r+1} + \frac{r}{r+1}\cdot k$$

Does not get to $1-R-\epsilon$....!

~~Algorithm:~~

Aside: How to get to rate from here?



$\alpha_1 \ldots\ldots \alpha_n \qquad \alpha'_1 \ldots\ldots \alpha'_{n'}$

$k \longrightarrow k$

$n \longrightarrow n' = n(r-s)$

$r \longrightarrow s$

$$\frac{n'}{s+1} + \frac{s}{s+1}k \approx \frac{rn}{s+1} + \frac{s}{s+1}k$$

Algorithm: Step 1: find $(A_0 \dots A_r) \neq 0$

$\deg A_0 < D + k$

$\deg A_j \leq D$

$\forall\, i, j \quad A_0(\alpha_i) + \sum_j \beta_i^j \cdot A_j(\alpha_i) = 0$

Step 2: find all polynomials $P \in \mathbb{F}_q^{<}[x]$

s.t. $\Lambda_p(x) \triangleq A_0(x) + \sum_j P(x^{j-1} x) \cdot A_j(x) \equiv 0$

Efficiency: Step 1 : Linear Algebra !

Step 2 : Linear Algebra !

Analysis Questions: (1) is every P reported?

(2) How large is the set of all P?

Claim 0: Solution to Step 1 exists if $(r+1)D + k \geq n+2$

Claim 1: if P satisfies (*) (on page (2)) then

$\Lambda_p(x) = 0 \Rightarrow$ it is included in list of solutions

[Need $\alpha_1 \dots \alpha_n$ distinct]

Proof: Exercise

Why is # solutions bounded?

- (We'll show $O(q^{r})$.)
- key will look at linear system that solves for P given $(A_0, \ldots, A_r)$
- will be a "triangular system" naturally.

$$C_\ell = \text{function}\,(C_0 \ldots C_{\ell-1})$$

- Claim: C_ℓ unique unless $B(\lambda^\ell) = 0$ for some fixed polynomial $B(\,)$.

Details: Let $P(X) = \sum_{\ell=0}^{k-1} c_\ell X^\ell$

Let $A_j(X) = \sum_{i=0}^{\cdots} a_{ij} X^i$

then coeff of X^t in $\Lambda_P(X)$ is

$$a_{t0} + \sum_{j=1}^{r} \left(\sum_{s=0}^{t} c_s \cdot \lambda^{(j-1)s} \right) \cdot a_{(t-s)j}$$

$$\Rightarrow \quad c_t \cdot \sum_{j=1}^{r} a_{0j} \lambda^{(j-1)t} + \underbrace{f(c_0 \ldots c_{t-1})} = 0$$

Define $B(Y) = \sum_{j=1}^{r} a_{0j} \cdot Y^{j-1}$

1. $\deg B < r$
2. $B \neq 0$ [if not divide $A_1 \cdots A_r$ by x & also A_0]
(can arrange that)
3. Have $B(\lambda^t) \cdot C_t = \text{fun}(C_0 \cdots C_{t-1})$

$\Rightarrow$ if $B(\lambda^t) \neq 0$ C_t determined.

- But at most r choices of t s.t. $B(\lambda^t) = 0$
- in all other cases at most q choices of C_t.