Addendum to Folded-Reed-Solomon Codes + Decoding

0. The codes

\[ \text{FACTORS} n, k, m, s \]

map: \( P(x) \in \mathbb{F}_q[x] \leq k \)

\( \rightarrow \left\langle \left[ P(x_1), P(x_2), \ldots, P(x^m) \right] \right\rangle \)

- Maps \( \mathbb{F}_q^k \rightarrow (\mathbb{F}_q^n)^m \)

- Rate = \( \frac{k}{n} = R \)

- Claim: can \textit{list} decode from \( 1 - R - \varepsilon \) fraction wrong!

\textbf{Algorithm: Step 1} : find \( A_0(x), A_1(x), \ldots, A_n(x) \) s+
Problem: Given: \( a_1, \ldots, a_n \)
\[ B'_1, \ldots, B'_n \]
\[ \vdots \]
\[ B'_r, \ldots, B'_n \]

Find all \( P \in \mathbb{F}_2^k \) such that \( P(x_i) = B_i \).

\[ \# \{ i | \forall j \in \mathbb{F}_2^k \} \geq \frac{n + \Theta \cdot k}{n + 1} \]

\( \text{Does not get to } 1 - R - \varepsilon \ldots \)

Aside: How to get to rate from here?

\[ \frac{v'}{s+1} + \frac{s}{s+1} k = \frac{vn + \frac{s}{s+1} k}{s+1} \]
Algorithm: Step 1: Find $\prod(A_0 \ldots A_r) = 0$

$\deg A_0 \leq D + k$
$\deg A_i \leq D$

$\forall i,j \quad A_0(x_i) + \sum_j B_i \cdot A_j(x_i) = 0$

Step 2: find all polynomials $P \in \mathbb{F}_2^r[x]

s.t. \quad \Lambda_P(x) \equiv 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 $P$ repeated?
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 $\otimes$ (on page 2) then

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

Proof: Exercise
Why is \# solutions Bounded?

- (We'll show \(O(n^r)\).)

- Key: will look at linear system that solves for \(P\) given \((A_0, \ldots, A_r)\).

- Will be a "triangular system" naturally.

  \[ C_L = \text{function } (C_0, \ldots, C_{r-1}) \]

- Claim: \(C_L\) unique unless \(B(x^L) = 0\) for some fixed polynomial \(B(x)\).

\[ \times \]

\text{det}: \quad \text{det } P(x) = \prod_{l=0}^{k-1} C_L x^l

\text{det } A_j(x) = \prod_{i=0}^{L} a_{i,j} x^i

\text{then value of } x^L \text{ in } \Lambda_p(x) \text{ is}

\[ a_{L,0} + \sum_{j=0}^{r} \left( \sum_{s=0}^{L} C_s x^{(j-1)s} \right) a_{(L-s),j} \]

\[ = \sum_{j=1}^{r} a_{0,j} x^{(j-1)L} + (C_0, \ldots, C_{r-1}) = 0 \]
Define \( B(y) = \sum_{j=1}^{r} a_{0,j} y^{j-1} \)

1. \( \deg B < r \)
2. \( B(x) = 0 \quad [\text{if not divide } A_1 \ldots A_r \text{ by } x \text{ (can arrange otherwise)}] \)
3. \( B(x^t) \cdot C_t = \text{fun}(C_0 \ldots C_{t-1}) \)
   \[ \Rightarrow \quad \text{if } B(x^t) = 0 \quad C_t \text{ determined.} \]
   - But at most \( t \) choices of \( C_t \) s.t. \( B(x^t) = 0 \)
   - in all other cases at most \( 2 \) choices of \( C_t \).