Error-Correcting Radius of Folded Reed–Solomon Code Designs

Joschi Brauchle – joschi.brauchle@tum.de

Motivation: Fractional Loss in Decoding Radius of FRS Codes

Folded Reed–Solomon (FRS) codes [1] of rate R can be decoded up to the Singleton bound asymptotically using linear-algebraic algorithms:

Asymptotic Decoding Radius (Singleton Bound)

$$\tau \leq 1 - R.$$

However, for finite code and decoding algorithm parameters, current decoders exhibit a fractional loss in radius:

Decoding Radius of linear-algebraic Algorithms with Finite Parameters

- Algorithm A: $\tau_A \sim (1 - aR)$ $\quad a > 1$
- Algorithm B: $\tau_B \sim b(1 - R)$ $\quad 0 < b < 1$

Notation and Definitions: Let...

- $\mathbb{F}_q$ denote a finite field of order q,
- $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$ be the multiplicative group with generator $\alpha \in \mathbb{F}_q^*$,
- $\mathbb{F}_q^m$ represent a vector space of dimension m over $\mathbb{F}_q$,
- $\mathbf{r} = (r_0, r_1, \ldots, r_{m-1}) \in \mathbb{F}_q^m$, $r_i \in \mathbb{F}_q$ an m-dimensional vector over $\mathbb{F}_q$,
- $\mathbf{R} = (\mathbf{r}_0, \mathbf{r}_1, \ldots)$ denote a vector over $\mathbb{F}_q^m$ or matrix over $\mathbb{F}_q$,
- $\mathbb{F}_q[x]$ be the ring of polynomials in indet. x and coefficients in $\mathbb{F}_q$,
- $\mathbb{F}_q[x]_{<k} := \{f(x) \in \mathbb{F}_q[x] \colon \deg f(x) < k\}$ be the vector space of polynomials in $\mathbb{F}_q[x]$ of degree less than k
- $\mathcal{E}(j, i, \ell) := \{\alpha^j, \alpha^{j+i}, \ldots, \alpha^{j+(\ell-1)i}\}$ denote an ordered set of ℓ distinct multiples of $\alpha^i \in \mathbb{F}_q$, starting at α^j,
- $\mathrm{ev}_{\mathcal{E}(j,i,\ell)}$ be an evaluation map defined as

$$\mathrm{ev}_{\mathcal{E}(j,i,\ell)} : \mathbb{F}_q[x]_{<k} \to \mathbb{F}_q^\ell$$
$$f \mapsto \left(f(\alpha^j), f(\alpha^{j+i}), \ldots, f(\alpha^{j+(\ell-1)i})\right),$$

- $[1, n] := \{1, 2, \ldots, n\}$ be the set of integers from 1 to n,
- $s \in [1, m]$ be an integer s. th. $(s+1)$ is the dimension of an interpolation point $(x, y_1, \ldots, y_s)$,
- $\mathcal{I}$ be the set of interpolation points used by the decoding algorithm,
- $Q(x, y_1, \ldots, y_s) = Q_0(x) + Q_1(x)y_1 + \cdots + Q_s(x)y_s \in \mathbb{F}_q[x, y_1, \ldots, y_s]$ be an $(s+1)$-variate interpolation polynomial with coefficients in $\mathbb{F}_q$,
- the $w = (1, k-1, \ldots, k-1)$-weighted degree of a monomial $x^{d_0} y_1^{d_1} \cdots y_s^{d_s}$ be defined as

$$\deg_w\left(x^{d_0} y_1^{d_1} \cdots y_s^{d_s}\right) := d_0 + (k-1)\left(\sum_{i=1}^{s} d_i\right), \quad (1)$$

- $D_Q = \deg_w(Q)$ be the w-weighted degree of its leading monomial under w-weighted lexicographic ordering.

Folded Reed–Solomon Codes [1]

Let m (*folding parameter*) be an integer satisfying $m \geq 1$ and $m|n$. Choose $N = n/m$ disjoint ordered sets of evaluation points

$$\mathcal{E}(jm, 1, m) = \left\{\alpha^{jm}, \alpha^{jm+1}, \ldots, \alpha^{jm+m-1}\right\}, \quad j \in [0, N-1]. \quad (2)$$

Definition (Folded Reed–Solomon Code)

An m-FRS code of dimension k, length N, rate $R = k/n$ has symbols

$$\mathbf{c}_j = \mathrm{ev}_{\mathcal{E}(jm,1,m)}(f) = \left[f(\alpha^{jm}), \ldots, f(\alpha^{jm+m-1})\right]^T \in \mathbb{F}_q^m \quad (3)$$

for $j \in [0, N-1]$ such that

$$\mathrm{FRS}[q, k, m] := \left\{(\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{N-1}) \in (\mathbb{F}_q^m)^N : \forall f \in \mathbb{F}_q[x]_{<k}\right\}. \quad (4)$$

In case of $m = 1$, an FRS code reduces to a Reed–Solomon (RS) code.

Linear-Algebraic Multivariate Interpolation Decoding

1. **Interpolation Problem:** Find an $(s+1)$-variate interpolation polynomial $Q \in \mathbb{F}_q[x, y_1, \ldots, y_s]$ of w-weighted degree D_Q, satisfying

$$Q(\alpha^i, r_i, \ldots, r_{i+s-1}) = 0, \quad \forall i \in \mathcal{I}. \quad (5)$$

Interpolation Problem

The homogeneous linear system (5) has a nonzero solution, if

$$D_Q \geq D(I, s) := \left\lceil \frac{I + s(k-1)}{s+1} \right\rceil \quad (6)$$

2. **Root-Finding Problem:** Recover a list of candidate message polynomials $f(x) \in \mathbb{F}_q[x]_{<k}$ from $Q \in \mathbb{F}_q[x, y_1, \ldots, y_s]$ via

$$Q(x, f(x), f(\alpha x), \ldots, f(\alpha^{s-1}x)) = 0. \quad (7)$$

Root-Finding Problem

According to the *Polynomial Factor Theorem*, $f(x)$ satisfies (7) if the number of correct interpolation points is larger than $D(I, s)$.

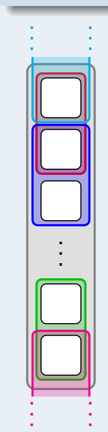
How FRS Symbol Errors affect Interpolation Points

Let $E := |\{j \in [0, N-1] : \mathbf{r}_j \neq \mathbf{c}_j\}|$ be the number of symbols errors in $\mathbf{R}$.

Lemma (Number of Interpolation Points Affected by Symbol Error)

The maximum number of interpolation points corrupted by a symbol error $\mathbf{r}_j \neq \mathbf{c}_j$, $j \in [0, N-1]$ is given by

$$A := \max_j \left|\{i \in \mathcal{I} : [i, i+s-1] \cap [jm, jm+m-1] \neq \emptyset\}\right|. \quad (8)$$



Sketch of Proof:

- White boxes represent elements in $\mathbb{F}_q$,
- Colored boxed are interpolation points from $\mathcal{I}$,
- Dotted borders depict partial interpolation points,
- Gray background box denotes received symbol $\mathbf{r}_j \in \mathbb{F}_q^m$.

Simple counting argument...

Achievable Decoding Radius τ

Lemma

An $(s+1)$-variate polynomial $Q \in \mathbb{F}_q[x, y_1, \ldots, y_s]$ satisfying (5) with w-weighted degree $D(I, s)$ as in (6) also satisfies (7) if the number of correct interpolation point is

$$I - EA > D(I, s). \quad (9)$$

Theorem (Achievable Decoding Radius)

In case (7) suffices to recover all candidate polynomials $f \in \mathbb{F}_q[x]_{<k}$, a decoding radius

$$\tau := \frac{E}{N} \leq \frac{s}{s+1}\left(\frac{I-k}{AN}\right) \quad (10)$$

is achievable.

In addition to N and k, the decoding radius τ is a function of the

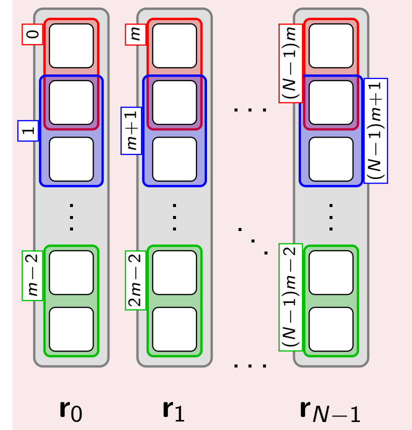
- Interpolation parameter $s \in [1, m]$,
- Number of interpolation points $I \in [1, n]$ used,
- Interpolation points affected by symbol error $A \in [I/N, m+s-1]$.

The value of τ is maximized for $s_{\max} := m$, $I_{\max} := n$ and $A_{\max} := I/N$:

Maximum Achievable Decoding Radius

$$\tau_{\max} = \frac{m}{m+1}(1 - R). \quad (11)$$

Decoding Radius of FRS Codes – Algorithm A [2, 3]



Strategy: Use only interpolation points strictly contained within received symbols.

Parameters:

$$N = n/m$$
$$\mathcal{I} = \bigcup_{j=0}^{N-1} [mj, mj+m-1]$$
$$I = N(m-s+1) < I_{\max}$$
$$A = m-s+1 = A_{\max}$$

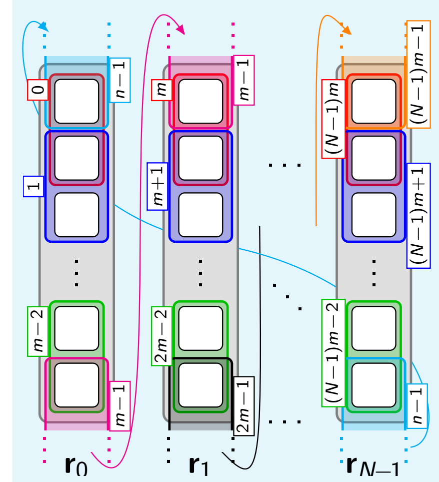
Drawback: Not all possible interpolation points are used.

Decoding Radius of Algorithm A

$$\tau_{\mathrm{FRS_A}} = \frac{s}{s+1}\left(1 - \left(\frac{m}{m-s+1}\right)R\right) \quad (12)$$

with a rate restriction of $0 \leq R \leq (m-s+1)/m$.

Decoding Radius of FRS Codes – Algorithm B [1, Sec. 3.2]



Strategy: Use all interpolation points.

Parameters:

$$N = n/m$$
$$\mathcal{I} = [0, n-1]$$
$$I = n = I_{\max}$$
$$A = m+s-1 > A_{\max}$$

Problem: Symbol errors cause extra erroneous interpolation points to affect possibly correct neighboring symbols.

Decoding Radius of Algorithm B

$$\tau_{\mathrm{FRS_B}} = \frac{s}{s+1}\left(\frac{m}{m+s-1}\right)(1 - R) \quad (13)$$

for $0 \leq R \leq 1$. Note that $\tau_{\mathrm{FRS_B}} > \tau_{\mathrm{FRS_A}}$ if $R > (m-s+1)/2m$.

Low-Order Folded Reed–Solomon Codes [4]

Objective:

- Achieve optimal parameters $I_{\max} = n$ and $A_{\max} = m$.
- Prevent erroneous interpolation points to affect correct neighboring symbols in case of a symbol error.

Solution:

1. Make transboundary interpolation points "wrap around" into the *same* code symbol instead of a neighboring one.
2. Recall that α^N is an element of low order $N = (q-1)/m$ over $\mathbb{F}_q$.
3. Choose $N = n/m$ disjoint ordered sets of evaluation points

$$\mathcal{E}(j, N, m) = \left\{\alpha^j, \alpha^{j+N}, \alpha^{j+2N}, \ldots, \alpha^{j+(m-1)N}\right\}, \quad j \in [0, N-1]. \quad (14)$$

Definition (LOFRS Code)

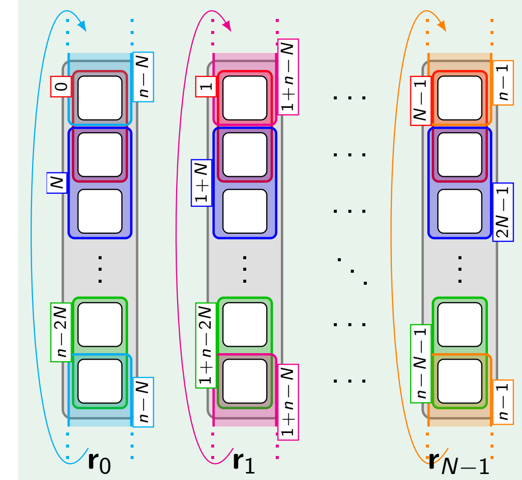
A m-LOFRS code of dimension k, length N, rate $R = k/n$ has symbols

$$\mathbf{c}_j = \mathrm{ev}_{\mathcal{E}(j,N,m)}(f) = \left[f(\alpha^j), f(\alpha^{j+N}), \ldots, f(\alpha^{j+(m-1)N})\right]^T \in \mathbb{F}_q^m \quad (15)$$

for $j \in [0, N-1]$ such that

$$\mathrm{LOFRS}[q, k, m] := \left\{(\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{N-1}) \in (\mathbb{F}_q^m)^N : \forall f \in \mathbb{F}_q[x]_{<k}\right\}. \quad (16)$$

Decoding Radius of LOFRS Codes



Parameters:

$$N = n/m$$
$$\mathcal{I} = [0, n-1]$$
$$I = n = I_{\max}$$
$$A = m = A_{\max}$$

Benefit: Uses all interpolation points **and** avoids neighboring symbol corruption.

Decoding Radius of LOFRS Codes

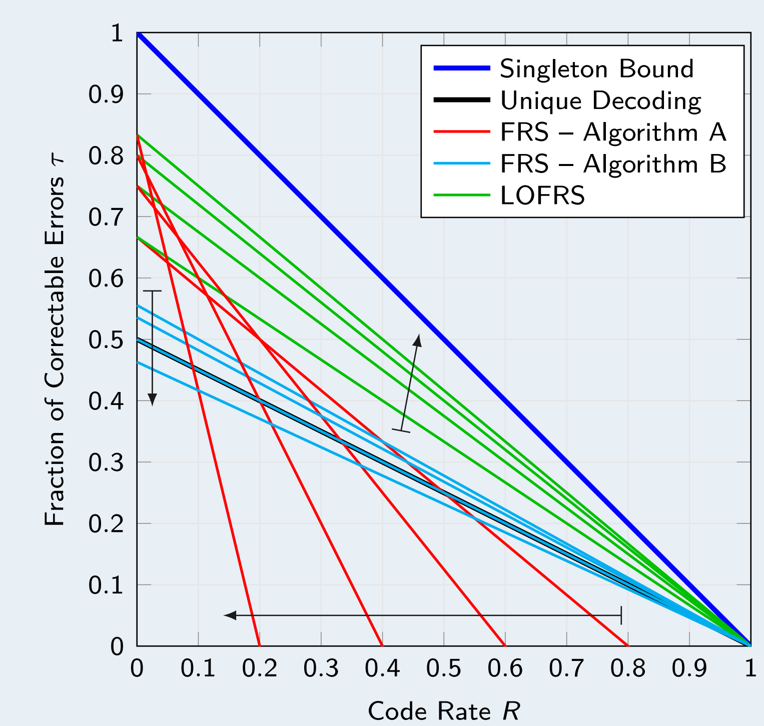
$$\tau_{\mathrm{LOFRS}} = \frac{m}{m+1}(1 - R). \quad (17)$$

Comparison of Decoding Radius

The following plot shows the decoding radius τ versus code rate R of a $m = 5$-FRS and $m = 5$-LOFRS codes for

- FRS – Algorithm A: $\tau_{\mathrm{FRS_A}} = \frac{s}{s+1}\left(1 - \left(\frac{m}{m-s+1}\right)R\right)$
- FRS – Algorithm B: $\tau_{\mathrm{FRS_B}} = \frac{s}{s+1}\left(\frac{m}{m+s-1}\right)(1 - R)$
- LOFRS: $\tau_{\mathrm{LOFRS}} = \frac{m}{m+1}(1 - R)$

and parameter $s \in [2, 5 = m]$ (in increasing order along black arrows).



Note: For any fixed value of the folding parameter $m > 1$ and interpolation parameter $s \in [1, m]$, we have

$$\tau_{\mathrm{LOFRS}} > \max\{\tau_{\mathrm{FRS_A}}, \tau_{\mathrm{FRS_B}}\}$$

for all rates $0 < R < 1$.

References

[1] V. Guruswami and A. Rudra, "Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 135–150, Jan. 2008.

[2] S. Vadhan, "Pseudorandomness," *Foundations and Trends in Theoretical Computer Science*, 2011.

[3] V. Guruswami and C. Wang, "Linear-algebraic list decoding for variants of Reed–Solomon codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 6, pp. 3257–3268, Jun. 2013.

[4] ——, "Explicit rank-metric codes list-decodable with optimal redundancy," *CoRR*, vol. abs/1311.7084, Nov. 2013.

Institute for Communications Engineering

Unterstützt von / Supported by Alexander von Humboldt Stiftung/Foundation

Technische Universität München