Efficient Decoding of Folded Linearized Reed–Solomon Codes in the Sum-Rank Metric

Felicitas Hörmann[0000−0003−2217−9753] and Hannes Bartz[0000−0001−7767−1513]

Institute of Communications and Navigation
German Aerospace Center (DLR), Germany
{felicitas.hoermann, hannes.bartz}@dlr.de

Abstract. Recently, codes in the sum-rank metric attracted attention due to several applications in e.g. multishot network coding, distributed storage and quantum-resistant cryptography. The sum-rank analogs of Reed–Solomon and Gabidulin codes are linearized Reed–Solomon codes. We show how to construct h-folded linearized Reed–Solomon (FLRS) codes and derive an interpolation-based decoding scheme that is capable of correcting sum-rank errors beyond the unique decoding radius. The presented decoder can be used for either list or probabilistic unique decoding and requires at most $\mathcal{O}(sn^2)$ operations in $\mathbb{F}_{q^m}$, where $s \leq h$ is an interpolation parameter and n denotes the length of the unfolded code. We derive a heuristic upper bound on the failure probability of the probabilistic unique decoder and verify the results via Monte Carlo simulations.

1 Introduction

The sum-rank metric was first encountered in the context of space-time coding [11, Sec. III] and can be seen as a hybrid between the Hamming and the rank metric. Codes in the sum-rank metric are of interest for error control in multishot network coding [16], for the construction of locally repairable codes [15] and in the context of quantum-resistant cryptography [17]. The family of linearized Reed–Solomon (LRS) codes was first described by Martínez-Peñas [13], independently studied in [6], and fulfills the Singleton-like bound in the sum-rank metric with equality. A Welch–Berlekamp-like decoder that can correct errors of sum-rank weight $t \leq \lfloor \frac{n-k}{2} \rfloor$, where n is the length and k the dimension of the code, was proposed in [14]. In [1], a speed-up was achieved by using approximant bases. Recently, it was shown in [2] and [3] that *interleaved* LRS codes allow to correct sum-rank errors beyond the unique decoding radius.

Our Contribution: We introduce a *folded* variant of LRS codes and provide an interpolation-based algorithm allowing to decode errors of sum-rank weight up to $t < \frac{s}{s+1}\left(\frac{N(h-s+1)-k+1}{h-s+1}\right)$, where h is the blockwise folding parameter, N the code length, k the dimension of the code, and $s \leq h$ a decoding parameter. Therefore, our approach allows to correct sum-rank errors beyond the unique decoding radius in quadratic complexity. Even though the worst-case list size

is exponential, we show that a unique solution is obtained with high probability which allows to use the scheme as a probabilistic unique decoder. We derive a heuristic upper bound on the decoding failure probability and verify the findings by Monte Carlo simulations. It is worth noting that the proposed decoding scheme generalizes known decoders for folded Reed–Solomon and folded Gabidulin codes in the Hamming and the rank metric, respectively.

2 Preliminaries

Let q be a prime power and $\mathbb{F}_q$ a finite field of order q. For any $m \in \mathbb{N}^*$, let $\mathbb{F}_{q^m} \supseteq \mathbb{F}_q$ denote an extension field with q^m elements. We call $\alpha \in \mathbb{F}_{q^m}$ *primitive* in $\mathbb{F}_{q^m}$ if it generates the multiplicative group $\mathbb{F}_{q^m}^* := \mathbb{F}_{q^m} \setminus \{0\}$.

In this paper, we mostly consider matrices whose N columns are divided into $\ell \in \mathbb{N}^*$ blocks of the same length $\Lambda := \frac{N}{\ell} \in \mathbb{N}^*$. Fix $h \in \mathbb{N}^*$ and let $\boldsymbol{X} = (\boldsymbol{X}^{(1)} \mid \cdots \mid \boldsymbol{X}^{(\ell)}) \in \mathbb{F}_{q^m}^{h \times N}$ be a matrix with $\boldsymbol{X}^{(i)} \in \mathbb{F}_{q^m}^{h \times \Lambda}$ for all $i \in \{1, \ldots, \ell\}$. Then, the *sum-rank weight* of $\boldsymbol{X}$ is defined as $\mathrm{wt}_{\Sigma R}(\boldsymbol{X}) := \sum_{i=1}^{\ell} \mathrm{rk}_q\left(\boldsymbol{X}^{(i)}\right)$, where $\mathrm{rk}_q\left(\boldsymbol{X}^{(i)}\right)$ is the maximum number of $\mathbb{F}_q$-linearly independent columns of $\boldsymbol{X}^{(i)}$. The *sum-rank distance* of two comparable elements is computed as the sum-rank weight of their difference and forms indeed a metric. We are concerned with *sum-rank codes* $\mathcal{C}$ being subsets of an $\mathbb{F}_{q^m}$-vector space equipped with the sum-rank metric. If $\mathcal{C}$ is an $\mathbb{F}_{q^m}$-linear subspace, the code is called *linear* and its *minimum (sum-rank) distance* is $d_{\Sigma R}(\mathcal{C}) = \min\{\mathrm{wt}_{\Sigma R}(\mathbf{c}) : \mathbf{c} \in \mathcal{C}, \mathbf{c} \neq 0\}$.

Let σ be an $\mathbb{F}_q$-linear automorphism on $\mathbb{F}_{q^m}$, that is $\sigma(a) = a^{q^s}$ for all $a \in \mathbb{F}_{q^m}$ and a particular $s \in \{0, \ldots, m-1\}$. Two elements $a, b \in \mathbb{F}_{q^m}$ are called *conjugate* if there is a $c \in \mathbb{F}_{q^m}^*$ such that $a^c := \sigma(c)ac^{-1} = b$. The set $\mathcal{C}(a) := \left\{a^c : c \in \mathbb{F}_{q^m}^*\right\}$ is called *conjugacy class* of a and $\mathbb{F}_{q^m}$ is partitioned into $q^{\gcd(s,m)}$ of these classes. If $s = 1$ and $\alpha \in \mathbb{F}_{q^m}^*$ is a primitive element, the set $\{1, \alpha, \ldots, \alpha^{q-2}\}$ contains representatives of all $q-1$ distinct nontrivial conjugacy classes.

The *skew polynomial ring* $\mathbb{F}_{q^m}[x, \sigma]$ (with zero derivation) is defined as the set of polynomials $\sum_i f_i x^i$ with finitely many nonzero coefficients $f_i \in \mathbb{F}_{q^m}$. It forms a non-commutative ring with respect to ordinary polynomial addition and multiplication determined by the rule $xf_i = \sigma(f_i)x$ for all $f_i \in \mathbb{F}_{q^m}$. We define the *degree* of a skew polynomial $f(x) = \sum_i f_i x^i$ as $\deg(f) := \max\{i : f_i \neq 0\}$ and write $\mathbb{F}_{q^m}[x, \sigma]_{<k} := \{f \in \mathbb{F}_{q^m}[x, \sigma] : \deg(f) < k\}$ for $k \geq 0$. We further introduce the operator $\mathcal{D}_a(b) := \sigma(b)a$ for any $a, b \in \mathbb{F}_{q^m}$ and its powers $\mathcal{D}_a^i(b) := \sigma^i(b)\sigma^{i-1}(a) \cdots \sigma(a)a$ for $i \in \mathbb{N}^*$. For a vector $\mathbf{x} = (\mathbf{x}^{(1)} \mid \cdots \mid \mathbf{x}^{(\ell)}) \in \mathbb{F}_{q^m}^K$ with ℓ blocks of length $\kappa := K/\ell \in \mathbb{N}^*$, a vector $\mathbf{a} = (a_1, \ldots, a_\ell) \in \mathbb{F}_{q^m}^\ell$, and a parameter $d \in \mathbb{N}^*$ the *generalized Moore matrix* is defined as

$$\mathfrak{M}_d(\mathbf{x})_{\mathbf{a}} := \left(\mathfrak{m}_d(\mathbf{x}^{(1)})_{a_1}\ \mathfrak{m}_d(\mathbf{x}^{(2)})_{a_2} \cdots \mathfrak{m}_d(\mathbf{x}^{(\ell)})_{a_\ell}\right) \in \mathbb{F}_{q^m}^{d \times K}, \tag{1}$$

$$\text{where} \quad \mathfrak{m}_d(\mathbf{x}^{(i)})_{a_i} := \begin{pmatrix} x_1^{(i)} & x_2^{(i)} & \cdots & x_\kappa^{(i)} \\ \mathcal{D}_{a_i}(x_1^{(i)}) & \mathcal{D}_{a_i}(x_2^{(i)}) & \cdots & \mathcal{D}_{a_i}(x_\kappa^{(i)}) \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{D}_{a_i}^{d-1}(x_1^{(i)}) & \mathcal{D}_{a_i}^{d-1}(x_2^{(i)}) & \cdots & \mathcal{D}_{a_i}^{d-1}(x_\kappa^{(i)}) \end{pmatrix} \quad \text{for } 1 \leq i \leq \ell.$$

If $\mathbf{a}$ contains representatives of pairwise distinct nontrivial conjugacy classes of $\mathbb{F}_{q^m}$ and $\mathrm{rk}_q(\mathbf{x}^{(i)}) = \kappa$ for all $1 \leq i \leq \ell$, we have by [13, Thm. 2] and [9, Thm 4.5] that $\mathrm{rk}_{q^m}(\mathfrak{M}_d(\mathbf{x})_\mathbf{a}) = \min(d, \ell\kappa)$.

The *generalized operator evaluation* of a skew polynomial $f \in \mathbb{F}_{q^m}[x,\sigma]$ at $b \in \mathbb{F}_{q^m}$ with respect to $a \in \mathbb{F}_{q^m}$ is defined as $f(b)_a = \sum_i f_i \mathcal{D}^i_a(b)$. Let $a_1, \ldots, a_\ell$ be representatives of distinct nontrivial conjugacy classes of $\mathbb{F}_{q^m}$ and consider n_i $\mathbb{F}_q$-linearly independent elements $\zeta^{(i)}_1, \ldots, \zeta^{(i)}_{n_i} \in \mathbb{F}_{q^m}$ for each $i = 1, \ldots, \ell$. Then any nonzero $f \in \mathbb{F}_{q^m}[x,\sigma]$ satisfying $f(\zeta^{(i)}_j)_{a_i} = 0$ for all $1 \leq j \leq n_i$ and all $1 \leq i \leq \ell$ has degree at least $\sum_{i=1}^{\ell} n_i$ (see e.g. [6]).

3 Interpolation-Based Decoding of Folded Linearized Reed–Solomon Codes

Motivated by the results for folded Reed–Solomon codes [8,19] and folded Gabidulin codes [4,12] we define folded linearized Reed–Solomon (FLRS) codes as follows. We start from a linearized Reed–Solomon code of length $n \in \mathbb{N}^*$ with $\ell \in \mathbb{N}^*$ same-sized blocks of length $\lambda := \frac{n}{\ell} \leq m$ over $\mathbb{F}_{q^m}$, and transform each block into an $(h \times \frac{\lambda}{h})$-matrix for a *folding parameter* $h \in \mathbb{N}^*$ dividing λ.

Definition 1 (Folded Linearized Reed–Solomon Codes). *Consider a primitive element α of $\mathbb{F}_{q^m}$ and let $\mathbf{a} = (a_1, \ldots, a_\ell) \in \mathbb{F}^\ell_{q^m}$ contain representatives of pairwise distinct nontrivial conjugacy classes of $\mathbb{F}_{q^m}$. An h-folded linearized Reed–Solomon code of length $N := \frac{n}{h}$ and dimension $k \leq n$ is defined as*

$$\mathrm{FLRS}[\mathbf{a}, \alpha, \ell, h; N, k] := \left\{ \left(\mathbf{C}^{(1)}(f) \mid \cdots \mid \mathbf{C}^{(\ell)}(f) \right) : f \in \mathbb{F}_{q^m}[x,\sigma]_{<k} \right\} \tag{2}$$

$$\text{with } \mathbf{C}^{(i)}(f) := \begin{pmatrix} f(1)_{a_i} & f(\alpha^h)_{a_i} & \cdots & f(\alpha^{\lambda-h})_{a_i} \\ f(\alpha)_{a_i} & f(\alpha^{h+1})_{a_i} & \cdots & f(\alpha^{\lambda-h+1})_{a_i} \\ \vdots & \vdots & \ddots & \vdots \\ f(\alpha^{h-1})_{a_i} & f(\alpha^{2h-1})_{a_i} & \cdots & f(\alpha^{\lambda-1})_{a_i} \end{pmatrix} \in \mathbb{F}^{h \times \Lambda}_{q^m} \tag{3}$$

for all $i \in \{1, \ldots, \ell\}$. We denote the length of a folded block by $\Lambda := \frac{\lambda}{h} = \frac{n}{h\ell}$.

Note that this definition can easily be generalized to different block lengths and more general $\mathbb{F}_q$-linearly independent code locators. FLRS codes are naturally embedded in $\mathbb{F}_{q^{mh}}$ but linearity is only guaranteed over the subfield $\mathbb{F}_{q^m}$.

Lemma 1 (Minimum Distance). *The code $\mathrm{FLRS}[\mathbf{a}, \alpha, \ell, h; N, k]$ has minimum distance $d_{\Sigma R}(\mathrm{FLRS}[\mathbf{a}, \alpha, \ell, h; N, k]) = N - \lceil \frac{k}{h} \rceil + 1$. It is a maximum sum-rank distance (MSRD) code if and only if h divides k.*

Proof. For every nonzero codeword $\mathbf{C} \in \mathrm{FLRS}[\mathbf{a}, \alpha, \ell, h; N, k]$ with message polynomial $f \in \mathbb{F}_{q^m}[x,\sigma]_{<k}$, there are $z, z_1, \ldots, z_\ell \geq 0$ with $z = \sum_{i=1}^{\ell} z_i$ such that $\mathrm{wt}_{\Sigma R}(\mathbf{C}) = N - z$ and $\mathrm{rk}_q(\mathbf{C}^{(i)}) = \Lambda - z_i$ for $i = 1, \ldots, \ell$. The column-reduced echelon form of $\mathbf{C}^{(i)}$, whose entries can still be expressed as evaluations of f

at evaluation parameter a_i, has exactly z_i zero columns. In the blockwise reduced matrix are hence z zero columns in total. Since the number of $\mathbb{F}_q$-linearly independent roots of f is bounded by its degree, we get $zh \leq k-1$ and equivalently $z \leq \left\lfloor \frac{k-1}{h} \right\rfloor = \left\lceil \frac{k}{h} \right\rceil - 1$. It follows $d_{\Sigma R}(\mathrm{FLRS}[\mathbf{a}, \alpha, \ell, h; N, k]) \geq \mathrm{wt}_{\Sigma R}(\mathbf{C}) \geq N - \left\lceil \frac{k}{h} \right\rceil + 1$. On the other hand, the Singleton-like bound [13, Prop. 34] yields $d_{\Sigma R}(\mathrm{FLRS}[\mathbf{a}, \alpha, \ell, h; N, k]) \leq N - \frac{k}{h} + 1$ and the claim follows. □

As channel model we consider a sum-rank channel with fixed error weight $t \in \mathbb{N}$ where the input $\mathbf{C} \in \mathrm{FLRS}[\mathbf{a}, \alpha, \ell, h; N, k]$ is related to the output $\mathbf{R}$ by $\mathbf{R} = \mathbf{C} + \mathbf{E} \in \mathbb{F}_{q^m}^{h \times N}$. The error matrix $\mathbf{E} \in \mathbb{F}_{q^m}^{h \times N}$ is chosen uniformly at random from the set of all matrices in $\mathbb{F}_{q^m}^{h \times N}$ having sum-rank weight t. In the following we write

$$\mathbf{R} = \left(\mathbf{R}^{(1)} \mid \cdots \mid \mathbf{R}^{(\ell)} \right) \quad \text{and} \quad \mathbf{R}^{(i)} = \begin{pmatrix} r_1^{(i)} & r_{h+1}^{(i)} & \cdots & r_{\lambda-h+1}^{(i)} \\ \vdots & \vdots & \ddots & \vdots \\ r_h^{(i)} & r_{2h}^{(i)} & \cdots & r_{\lambda}^{(i)} \end{pmatrix} \in \mathbb{F}_{q^m}^{h \times \Lambda} \tag{4}$$

for $i \in \{1, \ldots, \ell\}$ and proceed to our interpolation-based decoder.

3.1 Interpolation Step

We perform $(s+1)$-variate skew polynomial interpolation with respect to a chosen interpolation parameter $s \in \mathbb{N}^*$ with $s \leq h$. The set $\mathcal{P}$ of interpolation points is defined by means of a blockwise sliding window approach, whose eligible starting positions are collected in the index set $\mathcal{W}$. Namely, we consider

$$\begin{aligned} \mathcal{W} &:= \{(j-1)h + l : j \in \{1, \ldots, \Lambda\}, l \in \{1, \ldots, h-s+1\}\} \\ \text{and} \quad \mathcal{P} &:= \left\{ \left(\alpha^{w-1}, r_w^{(i)}, r_{w+1}^{(i)}, \ldots, r_{w+s-1}^{(i)} \right) : w \in \mathcal{W}, i \in \{1, \ldots, \ell\} \right\}. \end{aligned} \tag{5}$$

We wish to find a multivariate skew interpolation polynomial of the form

$$Q(x, y_1, \ldots, y_s) = Q_0(x) + Q_1(x)y_1 + \cdots + Q_s(x)y_s, \tag{6}$$

where $Q_r(x) \in \mathbb{F}_{q^m}[x, \sigma]$ for all $r \in \{0, \ldots, s\}$, that satisfies certain interpolation constraints. The *generalized operator evaluation* of such a polynomial $Q \in \mathbb{F}_{q^m}[x, y_1, \ldots, y_s, \sigma]$ at a given interpolation point (w, i) is defined as

$$\mathscr{E}_Q(w, i) := Q_0(\alpha^{w-1})_{a_i} + Q_1(r_w^{(i)})_{a_i} + \cdots + Q_s(r_{w+s-1}^{(i)})_{a_i} \tag{7}$$

where $w \in \mathcal{W}$ and $1 \leq i \leq \ell$ as in (5).

Problem 1 (Interpolation Problem). For a chosen parameter $D \in \mathbb{N}^*$ find a nonzero $(s+1)$-variate skew polynomial Q of the form (6) satisfying

1. $\mathscr{E}_Q(w, i) = 0$ for all $w \in \mathcal{W}$ and $i \in \{1, \ldots, \ell\}$ as well as
2. $\deg(Q_0) < D$ and $\deg(Q_r) < D - k + 1$ for all $r \in \{1, \ldots, s\}$.

The second condition of the interpolation problem allows us to write

$$Q_0(x) = \sum_{j=0}^{D-1} q_{0,j} x^j \quad \text{and} \quad Q_r(x) = \sum_{j=0}^{D-k} q_{r,j} x^j \quad \text{for} \quad r \in \{1, \ldots, s\} \tag{8}$$

with all coefficients from $\mathbb{F}_{q^m}$. For each block index $1 \leq i \leq \ell$, we collect all $\Lambda(h-s+1)$ interpolation points originating from $\mathbf{R}^{(i)}$ as rows in a matrix $\mathbf{P}_i \in \mathbb{F}_{q^m}^{\Lambda(h-s+1)\times(s+1)}$ and denote its columns by $\mathbf{p}_{i,0}, \ldots, \mathbf{p}_{i,s}$. Define further $\mathbf{p}_r = (\mathbf{p}_{1,r}^\top \mid \cdots \mid \mathbf{p}_{l,r}^\top)$ for $0 \leq r \leq s$. Then, Problem 1 can be written as

$$\mathbf{S}\mathbf{q}_I^\top = \mathbf{0} \tag{9}$$

$$\text{with} \quad \mathbf{S} = \Big((\mathfrak{M}_D(\mathbf{p}_0)_\mathbf{a})^\top \Big| (\mathfrak{M}_{D-k+1}(\mathbf{p}_1)_\mathbf{a})^\top \Big| \cdots \Big| (\mathfrak{M}_{D-k+1}(\mathbf{p}_s)_\mathbf{a})^\top \Big)$$

$$\text{and} \quad \mathbf{q}_I = (q_{0,0} \cdots q_{0,D-1} \mid q_{1,0} \cdots q_{1,D-k} \mid \cdots \mid q_{s,0} \cdots q_{s,D-k}) .$$

The interpolation system (9) can be solved using skew Kötter interpolation from [10] (similar as in [5, Sec. V]) requiring at most $\mathcal{O}(sn^2)$ operations in $\mathbb{F}_{q^m}$.

Lemma 2 (Existence). *A nonzero solution to Problem 1 exists if*

$$D = \left\lceil \frac{N(h-s+1) + s(k-1) + 1}{s+1} \right\rceil . \tag{10}$$

Proof. A nontrivial solution of (9) exists if less equations than unknowns are involved. That is, if $N(h-s+1) < D(s+1) - s(k-1)$. □

Lemma 3 (Roots of Polynomial). *Define the univariate skew polynomial*

$$\begin{aligned} P(x) &:= Q_0(x) + Q_1(x)f(x) + Q_2(x)f(x)\alpha + \cdots + Q_s(x)f(x)\alpha^{s-1} \\ &= Q(x, f(x), f(x)\alpha, \ldots, f(x)\alpha^{s-1}) \in \mathbb{F}_{q^m}[x, \sigma] \end{aligned} \tag{11}$$

and write $t_i := \mathrm{rk}_q(\boldsymbol{E}^{(i)})$ for $1 \leq i \leq \ell$. Then there exist $\mathbb{F}_q$-linearly independent elements $\zeta_1^{(i)}, \ldots, \zeta_{(\Lambda-t_i)(h-s+1)}^{(i)} \in \mathbb{F}_{q^m}$ for each $i \in \{1, \ldots, \ell\}$ such that $P(\zeta_j^{(i)})_{a_i} = 0$ for all $1 \leq i \leq \ell$ and all $1 \leq j \leq (\Lambda - t_i)(h-s+1)$.

Proof. Since $\mathrm{rk}_q(\boldsymbol{E}^{(i)}) = t_i$, there exists a nonsingular matrix $\boldsymbol{T}_i \in \mathbb{F}_q^{\Lambda\times\Lambda}$ such that $\boldsymbol{E}^{(i)}\boldsymbol{T}_i$ has only t_i nonzero columns for every $i \in \{1, \ldots, \ell\}$. Without loss of generality assume that these columns are the last ones of $\boldsymbol{E}^{(i)}\boldsymbol{T}_i$ and define $\boldsymbol{\zeta}^{(i)} = \mathbf{L} \cdot \boldsymbol{T}_i$ with $\mathbf{L} \in \mathbb{F}_{q^m}^{h\times\Lambda}$ containing the code locators $1, \ldots, \alpha^{\lambda-1}$ (cp. (3)). Note that the first $\Lambda - t_i$ columns of $\mathbf{R}^{(i)}\boldsymbol{T}_i = \mathbf{C}^{(i)}\boldsymbol{T}_i + \mathbf{E}^{(i)}\boldsymbol{T}_i$ are noncorrupted leading to $(\Lambda - t_i)(h-s+1)$ noncorrupted interpolation points according to (5). Now, for each $1 \leq i \leq \ell$, the first entries of the $(\Lambda - t_i)(h-s+1)$ noncorrupted interpolation points (i.e. the top left submatrix of size $(\Lambda - t_i) \times (h-s+1)$ of $\zeta^{(i)}$) are by construction both $\mathbb{F}_q$-linearly independent and roots of $P(x)$. □

Theorem 1 (Decoding Radius). *Let $Q(x, y_1, \ldots, y_s)$ be a nonzero solution of Problem 1. If $t = \mathrm{wt}_{\Sigma R}(\boldsymbol{E})$ satisfies*

$$t < \frac{s}{s+1} \left(\frac{N(h-s+1) - k + 1}{h-s+1} \right) , \tag{12}$$

then $P \in \mathbb{F}_{q^m}[x,\sigma]$ is the zero polynomial, that is for all $x \in \mathbb{F}_{q^m}$

$$P(x) = Q_0(x) + Q_1(x)f(x) + \cdots + Q_s(x)f(x)\alpha^{s-1} = 0. \tag{13}$$

Proof. By Lemma 3, there exist elements $\zeta_1^{(i)}, \ldots, \zeta_{(\Lambda-t_i)(h-s+1)}^{(i)}$ in $\mathbb{F}_{q^m}$ that are $\mathbb{F}_q$-linearly independent for each $i \in \{1, \ldots, \ell\}$ such that $P(\zeta_j^{(i)})_{a_i} = 0$ for $1 \leq i \leq \ell$ and $1 \leq j \leq (\Lambda - t_i)(h-s+1)$. By choosing $D \leq (N-t)(h-s+1)$, $P(x)$ exceeds the degree bound from [6, Prop. 1.3.7] which is possible only if $P(x) = 0$. Combining the above inequality with $N(h-s+1) < D(s+1) - s(k-1)$ from the proof of Lemma 2 yields the stated decoding radius. □

3.2 Root-Finding Step

By Theorem 1, the message polynomial $f \in \mathbb{F}_{q^m}[x,\sigma]_{<k}$ satisfies (13) if t satisfies (12). Therefore, we consider the following root-finding problem.

Problem 2 (Root-Finding Problem). Let $Q \in \mathbb{F}_{q^m}[x, y_1, \ldots, y_s, \sigma]$ be a nonzero solution of Problem 1 and let t satisfy constraint (12). Find all skew polynomials $f \in \mathbb{F}_{q^m}[x,\sigma]_{<k}$ that satisfy (13).

Problem 2 is equivalent to an $\mathbb{F}_{q^m}$-linear system of equations in the unknown

$$\mathbf{f} := (f_0, \sigma^{-1}(f_1), \ldots, \sigma^{-k+1}(f_{k-1}))^\top. \tag{14}$$

As e.g. in [4, 20], we use a basis of the interpolation problem's solution space instead of choosing only one solution Q of system (9). This improvement is justified by the following result.

Lemma 4 (Number of Interpolation Solutions). *For $d_I := \dim_{q^m}(\ker(\mathbf{S}))$ with $\mathbf{S}$ defined in (9), it holds $d_I \geq s(D-k+1) - t(h-s+1)$.*

Proof. The first D columns of $\mathbf{S}$ are given as $(\mathfrak{M}_D(\mathbf{p}_0)_\mathbf{a})^\top$. Since the ℓ blocks of $\mathbf{p}_0$ consist of pairwise distinct powers of α, the elements of a single block are $\mathbb{F}_q$-linearly independent. Hence $\mathrm{rk}_{q^m}(\mathfrak{M}_D(\mathbf{p}_0)_\mathbf{a}) = \min(D, N(h-s+1)) = D$. With the absence of an error, the remaining columns consist of linear combinations of the first D ones and do not increase the rank. If the error $\mathbf{E}$ with $\mathrm{wt}_{\Sigma R}(\mathbf{E}) = t$ is introduced, at most $t(h-s+1)$ interpolation points are corrupted according to Lemma 3. As a consequence, these columns can increase the rank of $\mathbf{S}$ by at most $t(h-s+1)$. Thus, $\mathrm{rk}_{q^m}(\mathbf{S}) \leq D + t(h-s+1)$ and the rank-nullity theorem directly yields $d_I = D(s+1) - s(k-1) - \mathrm{rk}_{q^m}(\mathbf{S}) \geq s(D-k+1) - t(h-s+1)$. □

Let now $Q^{(1)}, \ldots, Q^{(d_I)} \in \mathbb{F}_{q^m}[x, y_1, \ldots, y_s, \sigma]$ form a basis of the solution space of Problem 1 and denote the coefficients of $Q^{(u)}$ by $q_{i,j}^{(u)}$ for all $1 \leq u \leq d_I$ (cp. (8)). Define further the ordinary polynomials

$$B_j^{(u)}(x) = q_{1,j}^{(u)} + q_{2,j}^{(u)} x + \cdots + q_{s,j}^{(u)} x^{s-1} \in \mathbb{F}_{q^m}[x] \tag{15}$$

for $j \in \{0, \ldots, D-k\}$ and $u \in \{1, \ldots, d_I\}$ and the additional notations

$$\mathbf{b}_{j,a} = \left(\sigma^{-a}\left(B_j^{(1)}(\sigma^a(\alpha))\right), \ldots, \sigma^{-a}\left(B_j^{(d_I)}(\sigma^a(\alpha))\right)\right)^\top$$

$$\text{and} \qquad \mathbf{q}_a = \left(\sigma^{-a}\left(q_{0,a}^{(1)}\right), \ldots, \sigma^{-a}\left(q_{0,a}^{(d_I)}\right)\right)^\top$$

for $0 \leq j \leq D-k$ and $0 \leq a \leq D-1$. Then the root-finding system is given as

$$\mathbf{B} \cdot \mathbf{f} = -\mathbf{q} \tag{16}$$

$$\text{with} \quad \mathbf{B} := \begin{pmatrix} \mathbf{b}_{0,0} & & & & \\ \mathbf{b}_{1,1} & \mathbf{b}_{0,1} & & & \\ \vdots & \mathbf{b}_{1,2} & \ddots & & \\ \mathbf{b}_{D-k,D-k} & \vdots & & \mathbf{b}_{0,k-1} & \\ & \mathbf{b}_{D-k,D-k+1} & & \mathbf{b}_{1,k} & \\ & & \ddots & \vdots & \\ & & & \mathbf{b}_{D-k,D-1} & \end{pmatrix} \quad \text{and} \quad \mathbf{q} := \begin{pmatrix} \mathbf{q}_0 \\ \vdots \\ \mathbf{q}_{D-1} \end{pmatrix}.$$

The root-finding system (16) can be solved by back substitution in at most $\mathcal{O}(k^2)$ operations in $\mathbb{F}_{q^m}$ since we can focus on (at most) k nontrivial equations from different blocks of d_I rows. Note also that the transmitted message polynomial $f(x)$ is always a solution of (16) as long as t satisfies the decoding radius in (12).

3.3 Interpolation-Based List and Probabilistic Unique Decoding

The interpolation-based scheme from above can be used for list decoding or as a probabilistic unique decoder. The list decoder returns all solutions of (16).

Lemma 5 (Worst-Case List Size). *The list size is upper bounded by* $q^{m(s-1)}$.

Proof. With $d_{RF} := \dim_{q^m}(\ker(\mathbf{B}))$, the list size equals $q^{m \cdot d_{RF}}$ and $d_{RF} = k - \mathrm{rk}_{q^m}(\mathbf{B})$ due to the rank-nullity theorem. Let $\mathbf{B}_\triangle$ denote the lower triangular matrix consisting of the first $d_I k$ rows of $\mathbf{B}$. Then, $\mathrm{rk}_{q^m}(\mathbf{B}) \geq \mathrm{rk}_{q^m}(\mathbf{B}_\triangle)$ and the latter is lower bounded by the number of nonzero vectors on its diagonal. These vectors are $\mathbf{b}_{0,0}, \ldots, \mathbf{b}_{0,k-1}$ and we focus on their first components while neglecting application of σ. Each of them is given as the evaluation of $B_0^{(1)}$ at another conjugate of α. Since $B_0^{(1)}$ can have at most $s-1$ roots, it follows that at most $s-1$ of the vectors on the diagonal can be zero. Thus, $\mathrm{rk}_{q^m}(\mathbf{B}) \geq k-s+1$ and, as a consequence, $d_{RF} \leq s-1$. □

Note that, despite the exponential worst-case list size, an $\mathbb{F}_{q^m}$-basis of the list can be found in polynomial time. Theorem 2 summarizes the results for list decoding of FLRS codes and Figure 1 illustrates the achievable decoding region. In particular, the significant improvement of the normalized decoding radius $\tau := t/N$ of FLRS codes upon LRS codes is shown.

Theorem 2 (List Decoding). *Consider a folded linearized Reed–Solomon code* $\mathrm{FLRS}[\mathbf{a}, \alpha, \ell, h; N, k]$ *and a codeword* $\mathbf{C}$ *that is transmitted over a sum-rank channel with fixed error weight*

$$t < \frac{s}{s+1}\left(\frac{N(h-s+1)-k+1}{h-s+1}\right)$$

for an interpolation parameter $1 \leq s \leq h$. *Then, list decoding with a list size of at most* $q^{m(s-1)}$ *can be achieved in at most* $\mathcal{O}(sn^2)$ *operations in* $\mathbb{F}_{q^m}$.

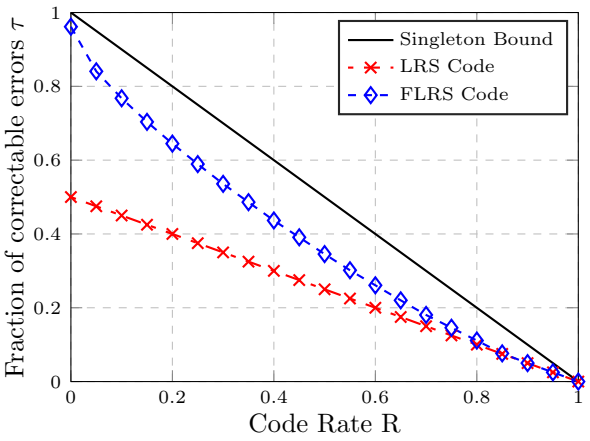

Fig. 1. Normalized decoding radius $\tau := \frac{t}{N}$ vs. code rate $R := \frac{k}{N}$ for an FLRS code with $h = 25$ and optimal decoding parameter $s \leq h$ for each code rate.

A different concept is probabilistic unique decoding where the decoder either returns a unique solution or declares a failure. In our setting, a failure occurs exactly when the root-finding matrix $\mathbf{B}$ is rank-deficient. Similar to [4] we now derive a heuristic upper bound on this probability $\mathbb{P}\left(\mathrm{rk}_{q^m}(\mathbf{B}) < k\right)$.

Lemma 6 (Decoding Failure Probability). *Assume that the coefficients of the polynomials $B_0^{(u)}(x) \in \mathbb{F}_{q^m}[x]$ from (15) for $u \in \{1, \ldots, d_I\}$ are independent and have a uniform distribution among $\mathbb{F}_{q^m}$. Then it holds that*

$$\mathbb{P}\left(\mathrm{rk}_{q^m}(\mathbf{B}) < k\right) \lesssim k \cdot \left(\frac{k}{q^m}\right)^{d_I}, \tag{17}$$

where $\lesssim$ indicates that the bound is a heuristic approximation.

Proof. Define $\mathbf{B}_\triangle$ as in the proof of Lemma 5 and note that $\mathbb{P}\left(\mathrm{rk}_{q^m}(\mathbf{B}) < k\right) \leq \mathbb{P}\left(\mathrm{rk}_{q^m}(\mathbf{B}_\triangle) < k\right)$ allows to focus on the latter. $\mathrm{rk}_{q^m}(\mathbf{B}_\triangle) = k$ is equivalent to all vectors $\mathbf{b}_{0,0}, \ldots, \mathbf{b}_{0,k-1}$ being nonzero. Because application of σ can be neglected, these vectors can be interpreted as codewords of a Reed–Solomon code. The proof of [4, Lemma 8] deals with this setting and yields the result. □

We introduce a threshold parameter $\mu \in \mathbb{N}^*$ and enforce $d_I \geq \mu$ which yields a degree constraint $D = \left\lceil \frac{N(h-s+1)+s(k-1)+\mu}{s+1} \right\rceil$. Theorem 3 provides a summary for probabilistic unique decoding of FLRS codes incorporating this threshold.

Theorem 3 (Probabilistic Unique Decoding). *Consider the FLRS code* $\mathrm{FLRS}[\mathbf{a}, \alpha, \ell, h; N, k]$ *and assume that the coefficients of the polynomials $B_0^{(u)}(x)$ for $u \in \{1, \ldots, \mu\}$ are independent and uniformly distributed among $\mathbb{F}_{q^m}$. For an interpolation parameter $1 \leq s \leq h$ and a dimension threshold $\mu \in \mathbb{N}^*$, transmit a codeword $\mathbf{C}$ over a sum-rank channel with fixed error weight*

$$t \leq \frac{s}{s+1}\left(\frac{N(h-s+1)-k+1}{h-s+1}\right) - \frac{\mu}{(s+1)(h-s+1)}. \tag{18}$$

Then, $\mathbf{C}$ *can be uniquely recovered with complexity* $\mathcal{O}(sn^2)$ *in* $\mathbb{F}_{q^m}$ *and with an approximate probability of at least*

$$1 - k \cdot \left(\frac{k}{q^m}\right)^{\mu}. \tag{19}$$

4 Simulation Results

We ran simulations in SageMath [18] to empirically verify the heuristic upper bound for probabilistic unique decoding from Theorem 3. We chose a 3-folded FLRS code of length $N = 4$ and dimension $k = 2$ over $\mathbb{F}_{3^6}$ with $\ell = 2$ blocks. Its minimum distance 4 implies a unique decoding radius of 1.5, whereas our probabilistic unique decoder allows to correct errors of weight $t = 2$ for $s = 2$ and $\mu \in \{1, 2\}$ ($t \leq 2.17$ and $t \leq 2$, respectively). We investigated the case $\mu = 1$ and collected 100 decoding failures within about $2.27 \cdot 10^7$ randomly chosen error patterns. The observed failure probability is hence about $4.40 \cdot 10^{-6}$, while the heuristic yields an upper bound of $5.49 \cdot 10^{-3}$. Note that the parameter set is explicitly designed to obtain an experimentally observable failure probability.

We also tracked the distribution χ of the coefficients of the polynomials $B_0^{(u)}(x) \in \mathbb{F}_{729}[x]$ from (15) for $1 \leq u \leq \mu$ for multiple transmissions and computed the Kullback–Leibler divergence D_{KL} with respect to the uniform distribution $\mathrm{unif}_{\mathbb{F}_{729}}$, which gives the number of additional bits needed to represent the approximated instead of the actual distribution (see e.g. [7, Sec. 2.3]). After 10^6 transmissions using the above code with $\mu = 1$, the result $D_{KL}(\chi \,||\, \mathrm{unif}_{\mathbb{F}_{729}}) \approx 3.19 \cdot 10^{-4}$ bits shows that the measured distribution χ is remarkably close to $\mathrm{unif}_{\mathbb{F}_{729}}$. This justifies the assumption in Theorem 3.

5 Conclusion

We considered the construction of folded linearized Reed–Solomon codes and proposed an efficient interpolation-based decoding scheme that is capable of correcting errors beyond the unique decoding radius in the sum-rank metric. The proposed algorithm can either be used as a (not necessarily polynomial-time) list decoder or as a probabilistic unique decoder that returns a unique solution with high probability. We analyzed the interpolation-based decoding scheme and derived both an upper bound on the worst-case list size and a heuristic upper bound on the decoding failure probability. The derivation of an upper bound on the failure probability that incorporates the distribution of the error matrices, a Justesen-like scheme for improved decoding of high-rate codes, and a comparison with decoding schemes for *interleaved* LRS codes are subject to future work.

The results in this paper can be extended to obtain more general code constructions over skew polynomial rings with derivations and/or codes with different block sizes. In particular, *lifted* FLRS codes and their properties in the sum-subspace metric can be used for error control in random linear multishot network coding. The construction of folded *skew* Reed–Solomon codes and the transfer of the presented decoder to the skew metric are other open problems.

References

1. Bartz, H., Jerkovits, T., Puchinger, S., Rosenkilde, J.: Fast Decoding of Codes in the Rank, Subspace, and Sum-Rank Metric. IEEE Trans. Inf. Theory **67**(8), 5026–5050 (2021)
2. Bartz, H., Puchinger, S.: Decoding of Interleaved Linearized Reed–Solomon Codes with Applications to Network Coding. In: IEEE Int. Symp. Inf. Theory. pp. 160–165 (2021)
3. Bartz, H., Puchinger, S.: Fast Decoding of Interleaved Linearized Reed—Solomon Codes and Variants. submitted to: IEEE Trans. Inf. Theory (2022), available at https://arxiv.org/abs/2201.01339
4. Bartz, H., Sidorenko, V.: Algebraic Decoding of Folded Gabidulin Codes. Des. Codes Cryptogr. **82**(1), 449–467 (2017)
5. Bartz, H., Wachter-Zeh, A.: Efficient Interpolation-Based Decoding of Interleaved Subspace and Gabidulin Codes. In: 52nd Annu. Allerton Conf. Commun., Control, Comput. pp. 1349–1356 (2014)
6. Caruso, X.: Residues of Skew Rational Functions and Linearized Goppa Codes. arXiv preprint (2019), available at https://arxiv.org/abs/1908.08430v1
7. Cover, T.M., Thomas, J.A.: Elements of Information Theory. Wiley-Interscience, USA (2006)
8. Guruswami, V., Rudra, A.: Explicit Codes Achieving List Decoding Capacity: Error-Correction With Optimal Redundancy. IEEE Trans. Inf. Theory **54**(1), 135–150 (2008)
9. Lam, T.Y., Leroy, A.: Vandermonde and Wronskian Matrices over Division Rings. J. Algebra **119**(2), 308–336 (1988)
10. Liu, S., Manganiello, F., Kschischang, F.R.: Kötter Interpolation in Skew Polynomial Rings. Des. Codes Cryptogr. **72**(3), 593–608 (2014)
11. Lu, H.f., Kumar, P.V.: A Unified Construction of Space-Time Codes with Optimal Rate-Diversity Tradeoff. IEEE Trans. Inf. Theory **51**(5), 1709–1730 (2005)
12. Mahdavifar, H., Vardy, A.: List-Decoding of Subspace Codes and Rank-Metric Codes up to Singleton Bound. In: IEEE Int. Symp. Inf. Theory. pp. 1488–1492 (2012)
13. Martínez-Peñas, U.: Skew and Linearized Reed–Solomon Codes and Maximum Sum Rank Distance Codes over any Division Ring. J. Algebra **504**, 587–612 (2018)
14. Martínez-Peñas, U., Kschischang, F.R.: Reliable and Secure Multishot Network Coding using Linearized Reed–Solomon Codes. IEEE Trans. Inf. Theory **65**(8), 4785–4803 (2019)
15. Martínez-Peñas, U., Kschischang, F.R.: Universal and Dynamic Locally Repairable Codes with Maximal Recoverability via Sum-Rank Codes. IEEE Trans. Inf. Theory pp. 792–799 (2019)
16. Nóbrega, R.W., Uchôa-Filho, B.F.: Multishot Codes for Network Coding using Rank-Metric Codes. In: 2010 3rd IEEE Int. Workshop Wirel. Netw. Coding. pp. 1–6 (2010)
17. Puchinger, S., Renner, J., Rosenkilde, J.: Generic Decoding in the Sum-Rank Metric. In: 2020 IEEE Int. Symp. Inf. Theory. pp. 54–59 (2020)
18. Stein, W.A., et al.: Sage Mathematics Software (Version 9.3). The Sage Development Team (2021), http://www.sagemath.org
19. Vadhan, S.P.: Pseudorandomness. In: Found. Trends Theor. Comput. Sci. (2011)
20. Wachter-Zeh, A.: Decoding of Block and Convolutional Codes in Rank Metric. Ph.D. thesis, Ulm University and University of Rennes 1 (2013)