Speeding up Error-Erasure Decoding of Linearized Reed–Solomon Codes in the Sum-Rank Metric

Felicitas Hörmann¹, Hannes Bartz¹, and Sven Puchinger²
{felicitas.hoermann, hannes.bartz}@dlr.de, sven.puchinger@tum.de

¹ Institute of Communications and Navigation
German Aerospace Center (DLR), Germany

² Hensoldt Sensors GmbH, Germany
Outline

1. Skew Polynomials and Their Basic Properties
2. Error-Erasure Decoding of Linearized Reed–Solomon Codes
3. Root Finding Using the Skew Skachek–Roth Algorithm
4. Conclusion
Skew Polynomials

Consider an $\mathbb{F}_q$-linear automorphism $\theta$ of $\mathbb{F}_{q^m}$.

**Definition [Ore, 1933]**

The **skew polynomial ring** $\mathbb{F}_{q^m}[x; \theta]$ is defined as the ordinary polynomial ring $\mathbb{F}_{q^m}[x]$ but with multiplication defined by $xa := \theta(a)x$ for all $a \in \mathbb{F}_{q^m}$.

For $a, b \in \mathbb{F}_{q^m}[x; \theta]$ with $\deg(b) \leq \deg(a)$, there are unique representations

$$a = b \cdot q_L + r_L$$

and

$$a = q_R \cdot b + r_R$$

for $q_L, q_R, r_L, r_R \in \mathbb{F}_{q^m}[x; \theta]$ with $\deg(r_L) \leq \deg(b)$ and $\deg(r_R) \leq \deg(b)$.

**Definition**

If $r_L = 0$, we call $b$ a **left divisor** of $a$ and if $r_R = 0$, $b$ is a **right divisor** of $a$. 
Minimal Polynomials

Definition

The minimal (skew) polynomial that vanishes on the set \( \{ b_1^{(i)}, \ldots, b_{n_i}^{(i)} \} \subseteq \mathbb{F}_{q^m} \) with respect to generalized operator evaluation with parameter \( a_i \in \mathbb{F}_{q^m} \) for all \( i = 1, \ldots, \ell \) is defined as the monic polynomial satisfying

\[
\text{mpol}_{\{ a_i \}_{i=1}^{\ell}} \left\{ b_1^{(i)}, \ldots, b_{n_i}^{(i)} \right\}_{\kappa=1}^{n_i} (b_\kappa^{(i)}) a_i = 0 \quad \text{for all} \quad 1 \leq \kappa \leq n_i \quad 1 \leq i \leq \ell .
\]
Generalized Operator Evaluation

Consider the operator $D_a(b) := \theta(b)a$ for all $a, b \in \mathbb{F}_{q^m}$.

**Definition**

The **generalized operator evaluation** of a skew polynomial $f = \sum_i f_i x^i \in \mathbb{F}_{q^m}[x; \theta]$ at an element $b \in \mathbb{F}_{q^m}$ with respect to $a \in \mathbb{F}_{q^m}$ is defined as

$$f(b)_a = \sum_i f_i D_a^i(b).$$

We obtain $D_a^i(b) = \theta^i(b)\mathcal{N}_i(a)$ for all $a, b \in \mathbb{F}_{q^m}$ and $i \geq 0$ if we write

$$\mathcal{N}_i(a) = \prod_{j=0}^{i-1} \theta^j(a) = \theta^{i-1}(a) \cdots \theta(a) \cdot a.$$
Root Space of Skew Polynomials

Lemma
For a fixed evaluation parameter \( a \in \mathbb{F}_{q^m} \) the generalized operator evaluation is an \( \mathbb{F}_q \)-linear map.

\[ \Rightarrow \] The zeros of a polynomial with respect to generalized operator evaluation with fixed parameter \( a \in \mathbb{F}_{q^m} \) form an \( \mathbb{F}_q \)-linear vector subspace of \( \mathbb{F}_{q^m} \).

Definition
The conjugacy class of \( a \in \mathbb{F}_{q^m} \) is \( \mathcal{C}(a) := \{ \theta(c)ac^{-1} : c \in \mathbb{F}_{q^m}^* \} \).
Root Space of Skew Polynomials

Lemma [Caruso, 2019]
Consider $a_1, \ldots, a_\ell \in F_{q^m}^*$ from distinct conjugacy classes of $F_{q^m}$. Choose for each $i = 1, \ldots, \ell$ a basis $B_i \subseteq F_{q^m}$ of the $F_q$-linear root space of $p \in F_{q^m}[x; \theta]$ with respect to generalized operator evaluation with parameter $a_i$. Then

$$
\sum_{i=1}^{\ell} \dim \langle B_i \rangle_{F_q} \leq \deg(p)
$$

is satisfied.

Equality holds if and only if $p$ divides $\prod_{i=1}^{\ell} (x^m - N_m(a_i))$. 
Linearized Reed–Solomon Codes

Definition [Martínez-Peñas, 2018]

Consider \( \mathbb{F}_q \)-linearly independent code locators \( \beta_1^{(i)}, \ldots, \beta_{n_i}^{(i)} \) for each \( i = 1, \ldots, \ell \) and evaluation parameters \( a := (a_1, \ldots, a_\ell) \in \mathbb{F}_q^\ell \) from different nontrivial conjugacy classes of \( \mathbb{F}_{q^m} \).

The **linearized Reed–Solomon code** \( \text{LRS}[\theta, \beta, a, \ell; n, k] \) is the row space of the matrix

\[
G = \left( G^{(1)} \mid \cdots \mid G^{(\ell)} \right)
\]

with

\[
G^{(i)} = \begin{pmatrix}
\beta_1^{(i)} & \cdots & \beta_{n_i}^{(i)} \\
\mathcal{D}_{a_i}(\beta_1^{(i)}) & \cdots & \mathcal{D}_{a_i}(\beta_{n_i}^{(i)}) \\
\vdots & \ddots & \vdots \\
\mathcal{D}_{a_i}^{k-1}(\beta_1^{(i)}) & \cdots & \mathcal{D}_{a_i}^{k-1}(\beta_{n_i}^{(i)})
\end{pmatrix}
\]

\( \in \mathbb{F}_{q^m}^{k \times n_i} \) for all \( 1 \leq i \leq \ell \).
Channel and Error Model

The codeword $c$ is transmitted through the channel and is received as $y = c + e$ with error $e$ of sum-rank weight $\tau$.

**Definition**

Consider a vector $x = \left( x^{(1)} \mid \cdots \mid x^{(\ell)} \right) \in \mathbb{F}_{q^m}^n$ that is divided into $\ell$ blocks $x^{(i)} \in \mathbb{F}_{q^m}^n$ for $i = 1, \ldots, \ell$.

The **sum-rank weight** of $x$ is defined as $\text{wt}_{\Sigma R}(x) := \sum_{i=1}^{\ell} \text{rk}_{\mathbb{F}_q}(x^{(i)})$. 


Error Decomposition in the Sum-Rank Metric

\[ e = e_F + e_R + e_C = a_F \cdot B_F + a_R \cdot B_R + a_C \cdot B_C \]

- \( e_F \) and \( e_C \) are matrices of rank \( t_F \) and \( t_C \) respectively.
- \( e_R \) is a matrix of rank \( t_R \).

- \( a_F \) and \( a_C \) are vectors of length \( m \).
- \( B_F \) and \( B_C \) are matrices of dimensions \( t_F \times n \) and \( t_C \times n \) respectively.

\( e_F \) contains \( t_F \) full errors, \( e_R \) contains \( t_R \) row erasures, and \( e_C \) contains \( t_C \) column erasures.
Error-Erasure Decoding of Linearized Reed–Solomon Codes

Theorem [Hörmann, Bartz, and Puchinger, 2022]

Consider a linearized Reed–Solomon code $\text{LRS}[\theta, \beta, \xi, \ell; n, k]$. If the number of full errors $t_F$, of row erasures $t_R$ and of column erasures $t_C$ satisfies $2t_F + t_R + t_C \leq n - k$, then the proposed decoder can recover the transmitted codeword requiring at most $O(n^2)$ operations in $\mathbb{F}_{q^m}$. 
Decoding Steps for the ESP Variant

precompute

\[ s = yH^\top \quad \text{and} \quad s(x) = \sum_{i=1}^{n-k} s_i x_i^{l-1} \]

\[ x_C = B_C \alpha^\top \]

\[ \lambda_C \text{ and } \sigma_R \]

compute

\[ s_{RC}(x) = \sigma_R(x) \cdot s(x) \cdot \overline{\lambda_C}(x) \]

solve the ESP key equation to recover \( \sigma_F \)

recover \( \sigma_C \) and compute \( \sigma = \sigma_C \cdot \sigma_F \cdot \sigma_R \)

recover \( \sigma_C \) and \( \sigma_F \) by solving \( Ax^\top = \tilde{s}^\top \)

return \( c = y - e \)

compute \( e = a_F \cdot B_F + a_R \cdot B_R + a_C \cdot B_C \)

return \( c = y - e \)
Problem Statement

Root-Finding Problem for Skew Polynomials

Input:
- \( p \in \mathbb{F}_{q^m}[x; \theta] \)
- \( a_1, \ldots, a_\ell \in \mathbb{F}_{q^m}^\ast \) belonging to distinct conjugacy classes of \( \mathbb{F}_{q^m} \)

Task:
For all \( i = 1, \ldots, \ell \), find an \( \mathbb{F}_q \)-basis \( B_i \subseteq \mathbb{F}_{q^m} \) of the root space of \( p \) with respect to generalized operator evaluation with parameter \( a_i \), i.e. such that
\[
p(b)_{a_i} = 0 \quad \text{for all} \quad b \in \langle B_i \rangle_{\mathbb{F}_q}.
\]
Conventional Approach

Given $p \in \mathbb{F}_{q^m}[x; \theta]$ and $a_1, \ldots, a_\ell \in \mathbb{F}_{q^m}^*$ belonging to distinct conjugacy classes of $\mathbb{F}_{q^m}$.

Algorithm (see [Berlekamp, 2015])

For each $i = 1, \ldots, \ell$:

1. Compute for the transformation matrix $P_i \in \mathbb{F}_{q^m}^{m \times m}$ corresponding to the $\mathbb{F}_q$-linear map $p(\cdot)_a : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$, $b \mapsto p(b)_a$ by expanding the vector $(p(b_1)_a, \ldots, p(b_m)_a)$ over $\mathbb{F}_q$.

2. Obtain $B_i$ as basis of the right kernel of $P_i$.

$\implies$ This approach has complexity at least $\ell m^\omega$ operations in $\mathbb{F}_q$ where $\omega < 2.37286$ is the matrix multiplication coefficient (see [Le Gall, 2014]).
Minimal Polynomials with the Same Root Space

Lemma
Fix $a \in \mathbb{F}_{q^m}^*$. Then, $x^m - \mathcal{N}_m(a) \in \mathbb{F}_{q^m}[x; \theta]$ is the minimal polynomial that vanishes on all elements of $\mathbb{F}_{q^m}$ with respect to generalized operator evaluation with parameter $a$.

Proof Sketch: $(x^m - \mathcal{N}_m(a))(b)_a = \mathcal{N}_m(a)(\theta^m(b) - b) = 0$

Proposition
Let $p \in \mathbb{F}_{q^m}[x; \theta]$ be a skew polynomial with root-space $\mathcal{V} \subseteq \mathbb{F}_{q^m}$ with respect to generalized operator evaluation with parameter $a \in \mathbb{F}_{q^m}^*$. Then

$$h(x) := \gcd(x^m - \mathcal{N}_m(a), p(x))$$

is a minimal polynomial of degree $\deg(h) = \dim(\mathcal{V})$ that vanishes on $\mathcal{V}$ with respect to generalized operator evaluation with parameter $a$. 
Root Space and Image

Theorem
Consider a $d$-dimensional $\mathbb{F}_q$-linear subspace $\mathcal{V} \subseteq \mathbb{F}_q^m$ of $\mathbb{F}_q^m$. Let $h(x) \in \mathbb{F}_q^m[x; \theta]$ be the minimal polynomial with root space $\mathcal{V}$ with respect to generalized operator evaluation with parameter $a \in \mathbb{F}_q^*$. Then:

1. 
   \[ g(x) := \text{ldiv} \left( x^m - N_m(a), \ h(x) \right) \in \mathbb{F}_q^m[x; \theta] \]
   is the minimal polynomial of degree $m - d$ whose $\mathbb{F}_q$-linear image with respect to the generalized operator evaluation with parameter $a$ is $\mathcal{V}$.

2. 
   \[ x^m - N_m(a) = h(x)g(x) = g(x)h(x). \]
### Skew Skachek–Roth Algorithm

**Input:**
- $p(x) \in \mathbb{F}_q[x; \theta]$
- $a_1, \ldots, a_\ell \in \mathbb{F}_q^*$ from distinct conjugacy classes

**Output:**
$\mathbb{F}_q$-bases $B_1, \ldots, B_\ell \subseteq \mathbb{F}_q^m$ such that for all $i = 1, \ldots, \ell$:

$$p(b)_{a_i} = 0 \quad \text{for all } b \in B_i$$

- Reduce to minimal polynomial:
  $$h_i(x) := \gcd(x^m - N_m(a_i), p(x))$$

- For each $i = 1, \ldots, \ell$
  - Find “dual” polynomial:
    $$g_i(x) := \text{ldiv}(x^m - N_m(a_i), h_i(x))$$
  - Compute $\mathbb{F}_q$-basis $B_i$ of the image space of $g_i(x)$ probabilistically

- Draw $b \in \mathbb{F}_q^*$ uniformly at random

- While $|B_i| < \deg(g_i)$
  - Add $b$ to $B_i$ if $b \notin \langle B_i \rangle_{\mathbb{F}_q}$
Complexity

Skew Skachek–Roth Algorithm
\( \mathcal{O}(\ell m \deg(p)) \)

Conventional Approach
\( \mathcal{O}(\ell m^\omega) \) with \( \omega < 2.38 \)

Execution time is averaged over 100 randomly chosen
\( p \in \mathbb{F}_{q^m}[x; \theta] \) with \( \deg(p) < (q - 1)m \).
Conclusion

Input:
- \( p \in \mathbb{F}_{q^m}[x; \theta] \)
- \( a_1, \ldots, a_\ell \in \mathbb{F}_{q^m}^{\ast} \) belonging to distinct conjugacy classes of \( \mathbb{F}_{q^m} \)

Task:
For all \( i = 1, \ldots, \ell \), find an \( \mathbb{F}_q \)-basis \( B_i \subseteq \mathbb{F}_{q^m} \) of the root space of \( p \) with respect to generalized operator evaluation with parameter \( a_i \).

Our work . . .
- extends the Skachek–Roth algorithm from [Skachek and Roth, 2008] to skew polynomials with multiple evaluation parameters,
- speeds up the root finding of skew polynomials in practice, and
- can be used e.g. in our error-erasure decoder for linearized Reed–Solomon codes.
References

Algebraic Coding Theory (revised edition).
World Scientific.

Residues of Skew Rational Functions and Linearized Goppa Codes.

Error-Erasure Decoding of Linearized Reed-Solomon Codes in the Sum-Rank Metric.
In IEEE International Symposium on Information Theory (ISIT).
References

  Powers of Tensors and Fast Matrix Multiplication.
  In *Proceedings of the 39th international symposium on symbolic and algebraic computation*, pages 296–303.

  Skew and Linearized Reed–Solomon Codes and Maximum Sum Rank Distance Codes over any Division Ring.

  Theory of Non-Commutative Polynomials.

  Probabilistic Algorithm for Finding Roots of Linearized Polynomials.