Finite Geometry & Friends

A Brussels' Summer School on Finite Geometry

September 20, 2023

Decoding Interleaved Linearized Reed–Solomon Codes

Felicitas Hörmann[1,2] – felicitas.hoermann@dlr.de

joint work with Hannes Bartz[1] and Sven Puchinger[3]

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

[2] School of Computer Science – University of St. Gallen, Switzerland

[3] Hensoldt Sensors GmbH, Germany

DLR

Outline

1. Motivation from Code-Based Cryptography
2. Interleaving in the Sum-Rank Metric
3. Interleaved Linearized Reed–Solomon Codes
4. Implications for Code-Based Cryptography

Code-Based Cryptography

- quantum computers can solve today's cryptographic primitives efficiently

Code-Based Cryptography

- quantum computers can solve today's cryptographic primitives efficiently
  $\Longrightarrow$ urgent need for quantum-safe cryptography

Code-Based Cryptography

- quantum computers can solve today's cryptographic primitives efficiently
  $\Longrightarrow$ urgent need for quantum-safe cryptography

- current standardization project initiated by NIST in 2016

Code-Based Cryptography

- quantum computers can solve today's cryptographic primitives efficiently
  $\Longrightarrow$ urgent need for quantum-safe cryptography

- current standardization project initiated by NIST in 2016
  - one standardized lattice-based key-encapsulation mechanism (KEM)
  - three remaining **code-based** KEM candidates

Code-Based Cryptography

- quantum computers can solve today's cryptographic primitives efficiently
  $\Longrightarrow$ urgent need for quantum-safe cryptography

- current standardization project initiated by NIST in 2016
  - one standardized lattice-based key-encapsulation mechanism (KEM)
  - three remaining **code-based** KEM candidates

- code-based cryptography suffers from large key sizes

Code-Based Cryptography

- quantum computers can solve today's cryptographic primitives efficiently
  $\Longrightarrow$ urgent need for quantum-safe cryptography

- current standardization project initiated by NIST in 2016
  - one standardized lattice-based key-encapsulation mechanism (KEM)
  - three remaining **code-based** KEM candidates

- code-based cryptography suffers from large key sizes
  $\Longrightarrow$ many approaches to mitigate this issue are studied,
  e.g. alternative metrics or codes with high error-correction capability

McEliece Cryptosystem [McEliece, 1978]

Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a linear code of dimension k.

McEliece Cryptosystem [McEliece, 1978]

Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a linear code of dimension k.

public key

- generator matrix $\boldsymbol{G}_{pub} \in \mathbb{F}_{q^m}^{k \times n}$ of $\mathcal{C}$ that does not reveal an efficient decoder
- error weight t

private key

- efficient decoder for $\mathcal{C}$ with decoding radius at least t

McEliece Cryptosystem [McEliece, 1978]

Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a linear code of dimension k.

Alice | Bob

$$\boldsymbol{x} \in \mathbb{F}_{q^m}^k \xrightarrow{\text{encrypt}} \boldsymbol{x}\boldsymbol{G}_{pub} + \boldsymbol{e} \xrightarrow{\text{transmit}} \boldsymbol{x}\boldsymbol{G}_{pub} + \boldsymbol{e} \xrightarrow{\text{decrypt}} \boldsymbol{x} \in \mathbb{F}_{q^m}^k$$

random $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$
of weight t

public key

- generator matrix $\boldsymbol{G}_{pub} \in \mathbb{F}_{q^m}^{k \times n}$ of $\mathcal{C}$ that does not reveal an efficient decoder
- error weight t

private key

- efficient decoder for $\mathcal{C}$ with decoding radius at least t

Outline

1. Motivation from Code-Based Cryptography
2. Interleaving in the Sum-Rank Metric
3. Interleaved Linearized Reed–Solomon Codes
4. Implications for Code-Based Cryptography

Some Weights

Consider $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$ and define

- its **Hamming weight**

$$\mathrm{wt}_H(\boldsymbol{x}) := |\{i \in \{1, \ldots, n\} : x_i \neq 0\}|,$$

Some Weights

Consider $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$ and define

- its **Hamming weight**

$$\mathrm{wt}_H(\boldsymbol{x}) := |\{i \in \{1, \ldots, n\} : x_i \neq 0\}|,$$

- its **rank weight**

$$\mathrm{wt}_{rk}(\boldsymbol{x}) := \mathrm{rk}_q(\boldsymbol{x}),$$

  where $\mathrm{rk}_q(\boldsymbol{x})$ is the maximum number of $\mathbb{F}_q$-linearly independent entries of $\boldsymbol{x}$,

Some Weights

Consider $\boldsymbol{x} = \left(\boldsymbol{x}^{(1)} \; \boldsymbol{x}^{(2)} \cdots \boldsymbol{x}^{(\ell)} \right) \in \mathbb{F}_{q^m}^n$ and define

- its **Hamming weight**

$$\mathrm{wt}_H(\boldsymbol{x}) := |\{i \in \{1, \dots, n\} : x_i \neq 0\}|,$$

- its **rank weight**

$$\mathrm{wt}_{rk}(\boldsymbol{x}) := \mathrm{rk}_q(\boldsymbol{x}),$$

  where $\mathrm{rk}_q(\boldsymbol{x})$ is the maximum number of $\mathbb{F}_q$-linearly independent entries of $\boldsymbol{x}$,
- and its **sum-rank weight** (with respect to a fixed length partition)

$$\mathrm{wt}_{\Sigma R}(\boldsymbol{x}) := \sum_{i=1}^{\ell} \mathrm{rk}_q\left(\boldsymbol{x}^{(i)}\right) = \mathrm{rk}_q\left(\boldsymbol{x}^{(1)}\right) + \mathrm{rk}_q\left(\boldsymbol{x}^{(2)}\right) + \cdots + \mathrm{rk}_q\left(\boldsymbol{x}^{(\ell)}\right).$$

Some Metrics

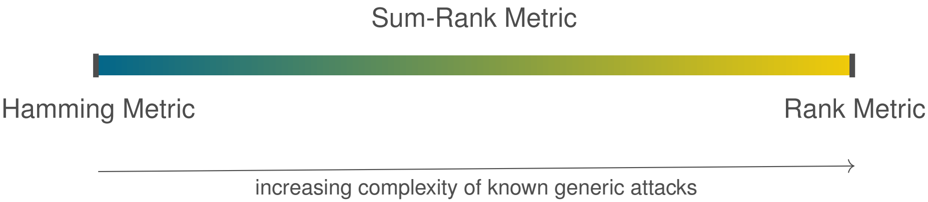
The **metrics** for $\star \in \{H, rk, \Sigma R\}$ are $d_\star(\boldsymbol{x}, \boldsymbol{y}) = \mathrm{wt}_\star(\boldsymbol{x} - \boldsymbol{y})$ for all $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_{q^m}^n$.

Some Metrics

The **metrics** for $\star \in \{H, rk, \Sigma R\}$ are $d_\star(\boldsymbol{x}, \boldsymbol{y}) = \mathrm{wt}_\star(\boldsymbol{x} - \boldsymbol{y})$ for all $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_{q^m}^n$.

Some Metrics

The **metrics** for $\star \in \{H, rk, \Sigma R\}$ are $d_\star(\boldsymbol{x}, \boldsymbol{y}) = \mathrm{wt}_\star(\boldsymbol{x} - \boldsymbol{y})$ for all $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_{q^m}^n$.



Some Metrics

The **metrics** for $\star \in \{H, rk, \Sigma R\}$ are $d_\star(\boldsymbol{x}, \boldsymbol{y}) = \mathrm{wt}_\star(\boldsymbol{x} - \boldsymbol{y})$ for all $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_{q^m}^n$.

Sum-Rank Metric

Hamming Metric

Rank Metric

increasing complexity of known generic attacks

structural attacks
broke many proposals

Interleaved Codes

For a linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ and an interleaving order $s \in \mathbb{N}^*$, define

- the **vertically interleaved code**

$$\mathrm{VInt}(\mathcal{C}, s) := \left\{ \boldsymbol{C} = \begin{pmatrix} \boldsymbol{c}_1 \\ \vdots \\ \boldsymbol{c}_\ell \end{pmatrix} : \boldsymbol{c}_j \in \mathcal{C} \text{ for all } j = 1, \dots, s \right\} \subseteq \mathbb{F}_{q^m}^{s \times n},$$

Interleaved Codes

For a linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ and an interleaving order $s \in \mathbb{N}^*$, define

- the **vertically interleaved code**

$$\mathrm{VInt}(\mathcal{C}, s) := \left\{ \boldsymbol{C} = \begin{pmatrix} \boldsymbol{c}_1 \\ \vdots \\ \boldsymbol{c}_\ell \end{pmatrix} : \boldsymbol{c}_j \in \mathcal{C} \text{ for all } j = 1, \dots, s \right\} \subseteq \mathbb{F}_{q^m}^{s \times n},$$

- and the **horizontally interleaved code**

$$\mathrm{HInt}(\mathcal{C}, s) := \left\{ \boldsymbol{c} = (\boldsymbol{c}_1 \mid \cdots \mid \boldsymbol{c}_\ell) : \boldsymbol{c}_j \in \mathcal{C} \text{ for all } j = 1, \dots, s \right\} \subseteq \mathbb{F}_{q^m}^{sn}.$$

Sum-Rank Weight of Vertically Interleaved Vectors

Choose an interleaving order $s \in \mathbb{N}^*$.
For $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_s \in \mathbb{F}_{q^m}^n$, consider the matrix $\boldsymbol{X} \in \mathbb{F}_{q^m}^{s \times n}$ with

$$\boldsymbol{X} = \begin{pmatrix} \boldsymbol{x}_1 \\ \boldsymbol{x}_2 \\ \vdots \\ \boldsymbol{x}_s \end{pmatrix} = \begin{pmatrix} \boxed{\boldsymbol{x}_1^{(1)} \ \boldsymbol{x}_1^{(2)} \ \cdots \ \boldsymbol{x}_1^{(\ell)}} \\ \boxed{\boldsymbol{x}_2^{(1)} \ \boldsymbol{x}_2^{(2)} \ \cdots \ \boldsymbol{x}_2^{(\ell)}} \\ \vdots \\ \boxed{\boldsymbol{x}_s^{(1)} \ \boldsymbol{x}_s^{(2)} \ \cdots \ \boldsymbol{x}_s^{(\ell)}} \end{pmatrix}.$$

Sum-Rank Weight of Vertically Interleaved Vectors

Choose an interleaving order $s \in \mathbb{N}^*$. For $\boldsymbol{x}_1, \dots, \boldsymbol{x}_s \in \mathbb{F}_{q^m}^n$, consider the matrix $\boldsymbol{X} \in \mathbb{F}_{q^m}^{s \times n}$ with

$$\boldsymbol{X} = \begin{pmatrix} \boldsymbol{x}_1 \\ \boldsymbol{x}_2 \\ \vdots \\ \boldsymbol{x}_s \end{pmatrix} = \begin{pmatrix} \boxed{\boldsymbol{x}_1^{(1)} \; \boldsymbol{x}_1^{(2)} \; \cdots \; \boldsymbol{x}_1^{(\ell)}} \\ \boxed{\boldsymbol{x}_2^{(1)} \; \boldsymbol{x}_2^{(2)} \; \cdots \; \boldsymbol{x}_2^{(\ell)}} \\ \vdots \\ \boxed{\boldsymbol{x}_s^{(1)} \; \boldsymbol{x}_s^{(2)} \; \cdots \; \boldsymbol{x}_s^{(\ell)}} \end{pmatrix}.$$

The sum-rank weight of $\boldsymbol{X}$ is

$$\mathrm{wt}_{\Sigma R}(\boldsymbol{X}) = \mathrm{rk}_q \begin{pmatrix} \boldsymbol{x}_1^{(1)} \\ \boldsymbol{x}_2^{(1)} \\ \vdots \\ \boldsymbol{x}_s^{(1)} \end{pmatrix} + \mathrm{rk}_q \begin{pmatrix} \boldsymbol{x}_1^{(2)} \\ \boldsymbol{x}_2^{(2)} \\ \vdots \\ \boldsymbol{x}_s^{(2)} \end{pmatrix} + \dots + \mathrm{rk}_q \begin{pmatrix} \boldsymbol{x}_1^{(\ell)} \\ \boldsymbol{x}_2^{(\ell)} \\ \vdots \\ \boldsymbol{x}_s^{(\ell)} \end{pmatrix}.$$

Sum-Rank Weight of Horizontally Interleaved Vectors

Choose an interleaving order $s \in \mathbb{N}^*$.
For $\boldsymbol{x}_1, \dots, \boldsymbol{x}_s \in \mathbb{F}_{q^m}^n$, consider the vector $\boldsymbol{x} \in \mathbb{F}_{q^m}^{sn}$ with

$$\begin{aligned}\boldsymbol{x} &= (\boldsymbol{x}_1 \mid \boldsymbol{x}_2 \mid \cdots \mid \boldsymbol{x}_s) \\ &= \left(\boxed{\boldsymbol{x}_1^{(1)} \; \boldsymbol{x}_1^{(2)} \cdots \boldsymbol{x}_1^{(\ell)}} \; \boxed{\boldsymbol{x}_2^{(1)} \; \boldsymbol{x}_2^{(2)} \cdots \boldsymbol{x}_2^{(\ell)}} \cdots \boxed{\boldsymbol{x}_s^{(1)} \; \boldsymbol{x}_s^{(2)} \cdots \boldsymbol{x}_s^{(\ell)}} \right).\end{aligned}$$

Sum-Rank Weight of Horizontally Interleaved Vectors

Choose an interleaving order $s \in \mathbb{N}^*$.
For $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_s \in \mathbb{F}_{q^m}^n$, consider the vector $\boldsymbol{x} \in \mathbb{F}_{q^m}^{sn}$ with

$$\boldsymbol{x} = (\boldsymbol{x}_1 \mid \boldsymbol{x}_2 \mid \cdots \mid \boldsymbol{x}_s)$$
$$= \left(\boxed{\boldsymbol{x}_1^{(1)} \; \boldsymbol{x}_1^{(2)} \cdots \boldsymbol{x}_1^{(\ell)}} \; \boxed{\boldsymbol{x}_2^{(1)} \; \boldsymbol{x}_2^{(2)} \cdots \boldsymbol{x}_2^{(\ell)}} \cdots \boxed{\boldsymbol{x}_s^{(1)} \; \boldsymbol{x}_s^{(2)} \cdots \boldsymbol{x}_s^{(\ell)}} \right).$$

The sum-rank weight of $\boldsymbol{x}$ is

$$\mathrm{wt}_{\Sigma R}(\boldsymbol{x}) =$$

$$\mathrm{rk}_q \left(\boxed{\boldsymbol{x}_1^{(1)} \; \boldsymbol{x}_2^{(1)} \cdots \boldsymbol{x}_s^{(1)}} \right) + \mathrm{rk}_q \left(\boxed{\boldsymbol{x}_1^{(2)} \; \boldsymbol{x}_2^{(2)} \cdots \boldsymbol{x}_s^{(2)}} \right) + \ldots + \mathrm{rk}_q \left(\boxed{\boldsymbol{x}_1^{(\ell)} \; \boldsymbol{x}_2^{(\ell)} \cdots \boldsymbol{x}_s^{(\ell)}} \right).$$

Outline

1. Motivation from Code-Based Cryptography
2. Interleaving in the Sum-Rank Metric
3. Interleaved Linearized Reed–Solomon Codes
4. Implications for Code-Based Cryptography

Linearized Reed–Solomon Codes

Choose

- **code locators** $\beta = (\beta^{(1)} \mid \cdots \mid \beta^{(\ell)}) \in \mathbb{F}_{q^m}^n$ whose blocks $\beta^{(i)}$ contain $\mathbb{F}_q$-linearly independent elements
- and **evaluation parameters** $\xi = (\xi_1, \dots, \xi_\ell) \in \mathbb{F}_{q^m}^\ell$ belonging to pairwise distinct nontrivial θ-conjugacy classes of $\mathbb{F}_{q^m}$ (i.e., $\forall i_1 \neq i_2 \ \nexists c \in \mathbb{F}_{q^m}^* : \theta(c)\xi_{i_1} c^{-1} = \xi_{i_2}$).

Linearized Reed–Solomon Codes

Choose

- **code locators** $\beta = (\beta^{(1)} \mid \cdots \mid \beta^{(\ell)}) \in \mathbb{F}_{q^m}^n$ whose blocks $\beta^{(i)}$ contain $\mathbb{F}_q$-linearly independent elements
- and **evaluation parameters** $\xi = (\xi_1, \ldots, \xi_\ell) \in \mathbb{F}_{q^m}^\ell$ belonging to pairwise distinct nontrivial θ-conjugacy classes of $\mathbb{F}_{q^m}$ (i.e., $\forall i_1 \neq i_2 \; \nexists c \in \mathbb{F}_{q^m}^* : \theta(c)\xi_{i_1} c^{-1} = \xi_{i_2}$).

We define the **linearized Reed–Solomon (LRS) code** with these parameters as

$$\mathrm{LRS}[\beta, \xi; n, k] = \left\{ f(\beta)_\xi = (f(\beta^{(1)})_{\xi_1} \mid \cdots \mid f(\beta^{(\ell)})_{\xi_\ell}) : f \in \mathbb{F}_{q^m}[x; \theta]_{<k} \right\} \subseteq \mathbb{F}_{q^m}^n.$$

Interleaved Linearized Reed–Solomon Codes

For an LRS code $\mathcal{C} := \mathrm{LRS}[\boldsymbol{\beta}, \boldsymbol{\xi}; \boldsymbol{n}, k]$ and $s \in \mathbb{N}^*$, we consider

- the **vertically interleaved LRS (VILRS) code** $\mathsf{VInt}(\mathcal{C}, s)$

Interleaved Linearized Reed–Solomon Codes

For an LRS code $\mathcal{C} := \mathrm{LRS}[\boldsymbol{\beta}, \boldsymbol{\xi}; \boldsymbol{n}, k]$ and $s \in \mathbb{N}^*$, we consider

- the **vertically interleaved LRS (VILRS) code** $\mathsf{VInt}(\mathcal{C}, s)$
- and the **horizontally interleaved LRS (HILRS) code** $\mathsf{HInt}(\mathcal{C}, s)$.

Interleaved Linearized Reed–Solomon Codes

For an LRS code $\mathcal{C} := \mathrm{LRS}[\boldsymbol{\beta}, \boldsymbol{\xi}; \boldsymbol{n}, k]$ and $s \in \mathbb{N}^*$, we consider

- the **vertically interleaved LRS (VILRS) code** $\mathsf{VInt}(\mathcal{C}, s)$
- and the **horizontally interleaved LRS (HILRS) code** $\mathsf{HInt}(\mathcal{C}, s)$.

We consider probabilistic-unique decoding up to an error weight

$$t \leq \frac{s}{s+1}(n-k).$$

$$\boxed{\begin{array}{c}\text{codeword}\\ \boldsymbol{c}\end{array}} \xrightarrow[\text{of weight } t]{\text{error } \boldsymbol{e}} \boxed{\begin{array}{c}\text{received word}\\ \boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}\end{array}}$$

Decoders for Interleaved LRS Codes

Decoders for VILRS Codes

- Loidreau–Overbeck-like
  [Bartz and Puchinger, 2023]
- interpolation-based
  [Bartz and Puchinger, 2023]
- syndrome-based (error-erasure)
  [Hörmann et al., 2023]

Decoders for HILRS Codes

- syndrome-based (error-erasure)
  [Hörmann et al., 2023]
- Gao-like
  [Hörmann and Bartz, 2023]

Decoders for Interleaved LRS Codes

Decoders for VILRS Codes

- Loidreau–Overbeck-like
  $\mathcal{O}(sn^{\omega}) \subseteq \mathcal{O}(sn^{2.373})$
- interpolation-based
  $\tilde{\mathcal{O}}(s^{\omega}\mathcal{M}(n)) \subseteq \tilde{\mathcal{O}}(s^{2.373}n^{1.635})$
- syndrome-based (error-erasure)
  $\mathcal{O}(sn^2)$

Decoders for HILRS Codes

- syndrome-based (error-erasure)
  $\mathcal{O}(sn^2)$
- Gao-like
  $\tilde{\mathcal{O}}(s^{\omega}\mathcal{M}(n)) \subseteq \tilde{\mathcal{O}}(s^{2.373}n^{1.635})$

$\tilde{\mathcal{O}}$ neglects logarithmic factors, $\omega < 2.373$ is the matrix-multiplication coefficient, and $\mathcal{M}(n) \subseteq \mathcal{O}(n^{1.635})$ denotes the cost of multiplication of two degree-n skew polynomials.

Decoders for Interleaved LRS Codes

Decoders for VILRS Codes

- Loidreau–Overbeck-like
  $\mathcal{O}(sn^{\omega}) \subseteq \mathcal{O}(sn^{2.373})$
- **interpolation-based**
  $\tilde{\mathcal{O}}(s^{\omega}\mathcal{M}(n)) \subseteq \tilde{\mathcal{O}}(s^{2.373}n^{1.635})$
- syndrome-based (error-erasure)
  $\mathcal{O}(sn^2)$

Decoders for HILRS Codes

- syndrome-based (error-erasure)
  $\mathcal{O}(sn^2)$
- **Gao-like**
  $\tilde{\mathcal{O}}(s^{\omega}\mathcal{M}(n)) \subseteq \tilde{\mathcal{O}}(s^{2.373}n^{1.635})$

$\tilde{\mathcal{O}}$ neglects logarithmic factors, $\omega < 2.373$ is the matrix-multiplication coefficient, and $\mathcal{M}(n) \subseteq \mathcal{O}(n^{1.635})$ denotes the cost of multiplication of two degree-n skew polynomials.

Outline

1. Motivation from Code-Based Cryptography

2. Interleaving in the Sum-Rank Metric

3. Interleaved Linearized Reed–Solomon Codes

4. Implications for Code-Based Cryptography

Conclusion

- VILRS and HILRS codes are interesting candidates for McEliece-like cryptosystems

Conclusion

- VILRS and HILRS codes are interesting candidates for McEliece-like cryptosystems
  - decoding with respect to the sum-rank metric
  - probabilistic-unique decoding for error weights up to $\frac{s}{s+1}(n-k)$
  - subquadratic decoding complexity

Conclusion

- VILRS and HILRS codes are interesting candidates for McEliece-like cryptosystems
  - decoding with respect to the sum-rank metric
  - probabilistic-unique decoding for error weights up to $\frac{s}{s+1}(n-k)$
  - subquadratic decoding complexity
- VILRS codes can only provide security for low interleaving order $s < t$ [Jerkovits et al., 2023]

Conclusion

- VILRS and HILRS codes are interesting candidates for McEliece-like cryptosystems
  - decoding with respect to the sum-rank metric
  - probabilistic-unique decoding for error weights up to $\frac{s}{s+1}(n-k)$
  - subquadratic decoding complexity
- VILRS codes can only provide security for low interleaving order $s < t$ [Jerkovits et al., 2023]
- (more) investigation of potential attacks needed

References

[Bartz and Puchinger, 2023] Bartz, H. and Puchinger, S. (2023).
Fast Decoding of Interleaved Linearized Reed–Solomon Codes and Variants.
submitted to: IEEE Transactions on Information Theory.

[Hörmann and Bartz, 2023] Hörmann, F. and Bartz, H. (2023).
Fast Gao-like Decoding of Horizontally Interleaved Linearized Reed–Solomon Codes.
accepted at: Code-Based Cryptography: CBCrypto 2023.

[Hörmann et al., 2023] Hörmann, F., Bartz, H., and Puchinger, S. (2023).
Syndrome-Based Error-Erasure Decoding of Interleaved Linearized Reed–Solomon Codes.
to be submitted to: IEEE Transactions on Information Theory.

[Jerkovits et al., 2023] Jerkovits, T., Hörmann, F., and Bartz, H. (2023).
On Decoding High-Order Interleaved Sum-Rank-Metric Codes.
In *Code-Based Cryptography: CBCrypto 2022*, pages 90–109.

[McEliece, 1978] McEliece, R. J. (1978).
A Public-Key Cryptosystem based on Algebraic Coding Theory.
DSN Progress Report, 42–44:114–116.