On Decoding High-Order Interleaved Sum-Rank-Metric Codes

Thomas Jerkovits[1,3](✉), Felicitas Hörmann[1,2], and Hannes Bartz[1]

[1] Institute of Communications and Navigation, German Aerospace Center (DLR), Wessling, Germany
{thomas.jerkovits,felicitas.hoermann,hannes.bartz}@dlr.de
[2] School of Computer Science, University of St. Gallen, St. Gallen, Switzerland
[3] Institute for Communications Engineering, Technical University of Munich (TUM), Munich, Germany

Abstract. We consider decoding of vertically homogeneous interleaved sum-rank-metric codes with high interleaving order s, that are constructed by stacking s codewords of a single constituent code. We propose a Metzner–Kapturowski-like decoding algorithm that can correct errors of sum-rank weight $t \leq d-2$, where d is the minimum distance of the code, if the interleaving order $s \geq t$ and the error matrix fulfills a certain rank condition. The proposed decoding algorithm generalizes the Metzner–Kapturowski(-like) decoders in the Hamming metric and the rank metric and has a computational complexity of $O\big(\max\{n^3, n^2 s\}\big)$ operations in $\mathbb{F}_{q^m}$, where n is the length of the code. The scheme performs linear-algebraic operations only and thus works for any interleaved linear sum-rank-metric code. We show how the decoder can be used to decode high-order interleaved codes in the skew metric. Apart from error control, the proposed decoder allows to determine the security level of code-based cryptosystems based on interleaved sum-rank metric codes.

1 Introduction

The development of quantum-secure cryptosystems is crucial in view of the recent advances in the design and the realization of quantum computers. As it is reflected in the number of submissions during the NIST's post-quantum cryptography standardization process for key encapsulation mechanisms (KEMs), many promising candidates belong to the family of code-based systems of which still three candidates are in the current 4th round [1]. Code-based cryptography is mostly based on the McEliece cryptosystem [11] whose trapdoor is that the public code can only be efficiently decoded if the secret key is known.

Variants of the McEliece cryptosystem based on interleaved codes in the Hamming and the rank metric were proposed in [4,7,19]. Interleaving is a well-known technique in coding theory that enhances a code's burst-error-correction capability. The idea is to stack a fixed number s of codewords of a constituent code over a field $\mathbb{F}_{q^m}$ in a matrix and thus to transform burst errors into errors occurring at the same position in each codeword. Equivalently, these errors can

J.-C. Deneuville (Ed.): CBCrypto 2022, LNCS 13839, pp. 90–109, 2023.
https://doi.org/10.1007/978-3-031-29689-5_6

be seen as symbol errors in a vector code over the extension field $\mathbb{F}_{q^{ms}}$. There exist list and/or probabilistic unique decoders for interleaved Reed–Solomon (RS) codes in the Hamming metric [8] as well as for interleaved Gabidulin codes in the rank metric [9] and for interleaved Reed–Solomon (LRS) codes in the sum-rank metric [2].

All of the mentioned decoders are tailored to a particular code family and explicitly exploit the code structure. In contrast, Metzner and Kapturowski proposed a decoder which works for interleaved Hamming-metric codes with *any* linear constituent code. The decoding algorithm only requires a high interleaving order s as well as a linear-independence constraint on the error [14]. Variants of the linear-algebraic Metzner–Kapturowski algorithm were further studied in [5,6,12,13,15,21], often under the name vector-symbol decoding (VSD). Moreover, Puchinger, Renner and Wachter-Zeh adapted the algorithm to the rank-metric case in [18,20].

This affects the security level of McEliece variants that are based on interleaved codes in the Hamming and the rank metric as soon as the interleaving order s is too large (i.e. $s \geq t$ for error weight t). Cryptosystems based on interleaved codes with small interleaving order are not affected. Their security level can be evaluated based on information-set-decoding (ISD) algorithms (see e.g. [16] for an adaptation of Prange's algorithm to interleaved Hamming-metric codes).

Contribution. We present a Metzner–Kapturowski-like decoding algorithm for high-order interleaved sum-rank-metric codes with an arbitrary linear constituent code. This gives valuable insights for the design of McEliece-like cryptosystems based on interleaved codes in the sum-rank metric. The proposed algorithm is purely linear-algebraic and can guarantee to correct errors of sum-rank weight $t \leq d - 2$ if the error matrix has full $\mathbb{F}_{q^m}$-rank t, where d is the minimum distance of the code. The computational complexity of the algorithm is in the order of $O\big(\max\{n^3, n^2 s\}\big)$ operations over $\mathbb{F}_{q^m}$, where $s \geq t$ is the interleaving order and n denotes the length of the linear constituent code. Note, that the decoding complexity is independent of the code structure of the constituent code since the proposed algorithm exploits properties of high-order interleaving only. Since the sum-rank metric generalizes both the Hamming and the rank metric, the original Metzner–Kapturowski decoder [14] as well as its rank-metric analog [18,20] can be recovered from our proposal.

2 Preliminaries

Let q be a power of a prime and let $\mathbb{F}_q$ denote the finite field of order q and $\mathbb{F}_{q^m}$ an extension field of degree m. We use $\mathbb{F}_q^{a\times b}$ to denote the set of all $a \times b$ matrices over $\mathbb{F}_q$ and $\mathbb{F}_{q^m}^b$ for the set of all row vectors of length b over $\mathbb{F}_{q^m}$.

Let $\boldsymbol{b} = (b_1, \ldots, b_m) \in \mathbb{F}_{q^m}^m$ be a fixed (ordered) basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. We denote by $\mathrm{ext}(\alpha)$ the column-wise expansion of an element $\alpha \in \mathbb{F}_{q^m}$ over $\mathbb{F}_q$ (with respect to $\boldsymbol{b}$), i.e.

$$\mathrm{ext} : \mathbb{F}_{q^m} \mapsto \mathbb{F}_q^m$$

such that $\alpha = \boldsymbol{b} \cdot \text{ext}(\alpha)$. This notation is extended to vectors and matrices by applying $\text{ext}(\cdot)$ in an element-wise manner.

By $[a : b]$ we denote the set of integers $[a : b] := \{i : a \leq i \leq b\}$. For a matrix $\boldsymbol{A}$ of size $a \times b$ and entries $A_{i,j}$ for $i \in [1 : a]$ and $j \in [1 : b]$, we define the submatrix notation

$$\boldsymbol{A}_{[c:d],[e:f]} := \begin{pmatrix} A_{c,e} & \dots & A_{c,f} \\ \vdots & \ddots & \vdots \\ A_{d,e} & \dots & A_{d,f} \end{pmatrix}.$$

The $\mathbb{F}_{q^m}$-linear row space of a matrix $\boldsymbol{A}$ over $\mathbb{F}_{q^m}$ is denoted by $\mathcal{R}_{q^m}(\boldsymbol{A})$. Its $\mathbb{F}_q$-linear row space is defined as $\mathcal{R}_q(\boldsymbol{A}) := \mathcal{R}_q(\text{ext}(\boldsymbol{A}))$. We denote the row-echelon form and the (right) kernel of $\boldsymbol{A}$ as $\text{REF}(\boldsymbol{A})$ and $\ker_r(\boldsymbol{A})$, respectively.

2.1 Sum-Rank-Metric Codes

Let $\boldsymbol{n} = (n_1, \dots, n_\ell) \in \mathbb{N}^\ell$ with $n_i > 0$ for all $i \in [1 : \ell]$ be a length partition[1] of n, i.e. $n = \sum_{i=1}^{\ell} n_i$. Further let $\boldsymbol{x} = (\boldsymbol{x}^{(1)} \mid \boldsymbol{x}^{(2)} \mid \dots \mid \boldsymbol{x}^{(\ell)}) \in \mathbb{F}_{q^m}^n$ be a vector over a finite field $\mathbb{F}_{q^m}$ with $\boldsymbol{x}^{(i)} \in \mathbb{F}_{q^m}^{n_i}$. For each $\boldsymbol{x}^{(i)}$ define the rank $\text{rk}_\text{q}(\boldsymbol{x}^{(i)}) := \text{rk}_\text{q}(\text{ext}(\boldsymbol{x}^{(i)}))$ where $\text{ext}(\boldsymbol{x}^{(i)})$ is a matrix in $\mathbb{F}_q^{m \times n_i}$ for all $i \in [1 : \ell]$. The *sum-rank weight* of $\boldsymbol{x}$ with respect to the length partition $\boldsymbol{n}$ is defined as

$$\text{wt}_{\Sigma R}(\boldsymbol{x}) := \sum_{i=1}^{\ell} \text{rk}_q(\boldsymbol{x}^{(i)})$$

and the *sum-rank distance* of two vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_{q^m}^n$ is defined as $d_{\Sigma R}(\boldsymbol{x}, \boldsymbol{y}) := \text{wt}_{\Sigma R}(\boldsymbol{x} - \boldsymbol{y})$. Note that the sum-rank metric equals the Hamming metric for $\ell = n$ and is equal to the rank metric for $\ell = 1$.

An $\mathbb{F}_{q^m}$*-linear sum-rank-metric code* $\mathcal{C}$ is an $\mathbb{F}_{q^m}$-subspace of $\mathbb{F}_{q^m}^n$. It has length n (with respect to a length partition $\boldsymbol{n}$), dimension $k := \dim_{q^m}(\mathcal{C})$ and minimum (sum-rank) distance $d := \min\{d_{\Sigma R}(\boldsymbol{x}, \boldsymbol{y}) : \boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}\}$. To emphasize its parameters, we write $\mathcal{C}[\boldsymbol{n}, k, d]$ in the following.

2.2 Interleaved Sum-Rank-Metric Codes and Channel Model

A (vertically) s-interleaved code is a direct sum of s codes of the same length n. In this paper we consider *homogeneous* interleaved codes, i.e. codes obtained by interleaving codewords of *a single* constituent code.

Definition 1 (Interleaved Sum-Rank-Metric Code). *Let $\mathcal{C}[\boldsymbol{n}, k, d] \subseteq \mathbb{F}_{q^m}^n$ be an $\mathbb{F}_{q^m}$-linear sum-rank-metric code of length n with length partition $\boldsymbol{n} = (n_1, n_2, \dots, n_\ell) \in \mathbb{N}^\ell$ and minimum sum-rank distance d. Then the corresponding (homogeneous) s-interleaved code is defined as*

$$\mathcal{IC}[s; \boldsymbol{n}, k, d] := \left\{ \begin{pmatrix} \boldsymbol{c}_1 \\ \vdots \\ \boldsymbol{c}_s \end{pmatrix} : \boldsymbol{c}_j = (\boldsymbol{c}_j^{(1)} \mid \dots \mid \boldsymbol{c}_j^{(\ell)}) \in \mathcal{C}[\boldsymbol{n}, k, d] \right\} \subseteq \mathbb{F}_{q^m}^{s \times n}.$$

[1] Note that this is also known as (integer) composition into exactly ℓ parts in combinatorics.

Each codeword $\boldsymbol{C} \in \mathcal{IC}[s; \boldsymbol{n}, k, d]$ can be written as

$$\boldsymbol{C} = \left(\begin{array}{c|c|c|c} \boldsymbol{c}_1^{(1)} & \boldsymbol{c}_1^{(2)} & \dots & \boldsymbol{c}_1^{(\ell)} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{c}_s^{(1)} & \boldsymbol{c}_s^{(2)} & \dots & \boldsymbol{c}_s^{(\ell)} \end{array}\right) \in \mathbb{F}_{q^m}^{s \times n}$$

or equivalently as

$$\boldsymbol{C} = (\boldsymbol{C}^{(1)} \mid \boldsymbol{C}^{(2)} \mid \cdots \mid \boldsymbol{C}^{(\ell)})$$

where

$$\boldsymbol{C}^{(i)} := \begin{pmatrix} \boldsymbol{c}_1^{(i)} \\ \boldsymbol{c}_2^{(i)} \\ \vdots \\ \boldsymbol{c}_s^{(i)} \end{pmatrix} \in \mathbb{F}_{q^m}^{s \times n_i}$$

for all $i \in [1 : \ell]$.

As a channel model we consider the additive sum-rank channel

$$\boldsymbol{Y} = \boldsymbol{C} + \boldsymbol{E}$$

where

$$\boldsymbol{E} = (\boldsymbol{E}^{(1)} \mid \boldsymbol{E}^{(2)} \mid \dots \mid \boldsymbol{E}^{(\ell)}) \in \mathbb{F}_{q^m}^{s \times n}$$

with $\boldsymbol{E}^{(i)} \in \mathbb{F}_{q^m}^{s \times n_i}$ and $\mathrm{rk}_q(\boldsymbol{E}^{(i)}) = t_i$ for all $i \in [1 : \ell]$ is an error matrix with $\mathrm{wt}_{\Sigma R}(\boldsymbol{E}) = \sum_{i=1}^{\ell} t_i = t$.

3 Decoding of High-Order Interleaved Sum-Rank-Metric Codes

In this section, we propose a Metzner–Kapturowski-like decoder for the sum-rank metric, that is a generalization of the decoders proposed in [14,18,20]. Similar to the Hamming- and the rank-metric case, the proposed decoder works for errors of sum-rank weight t up to $d-2$ that satisfy the following conditions:

- *High-order condition:* The interleaving order $s \geq t$,
- *Full-rank condition:* Full $\mathbb{F}_{q^m}$-rank error matrices, i.e., $\mathrm{rk}_{\mathrm{q^m}}(\boldsymbol{E}) = t$.

Note that the full-rank condition implies the high-order condition since the $\mathbb{F}_{q^m}$-rank of a matrix $\boldsymbol{E} \in \mathbb{F}_{q^m}^{s \times n}$ is at most s.

Throughout this section we consider a homogeneous s-interleaved sum-rank-metric code $\mathcal{IC}[s; \boldsymbol{n}, k, d]$ over a field $\mathbb{F}_{q^m}$ with a constituent code $\mathcal{C}[\boldsymbol{n}, k, d]$ defined by a parity-check matrix

$$\boldsymbol{H} = (\boldsymbol{H}^{(1)} \mid \boldsymbol{H}^{(2)} \mid \dots \mid \boldsymbol{H}^{(\ell)}) \in \mathbb{F}_{q^m}^{(n-k) \times n}$$

with $\boldsymbol{H}^{(i)} \in \mathbb{F}_{q^m}^{(n-k)\times n_i}$. The goal is to recover a codeword $\boldsymbol{C} \in \mathcal{IC}[s;\boldsymbol{n},k,d]$ from the matrix

$$\boldsymbol{Y} = \boldsymbol{C} + \boldsymbol{E} \in \mathbb{F}_{q^m}^{s\times n}$$

that is corrupted by an error matrix $\boldsymbol{E}$ of sum-rank weight $\mathrm{wt}_{\Sigma R}(\boldsymbol{E}) = t$ assuming *high-order* and *full-rank* condition.

As the Metzner–Kapturowski algorithm and its adaptation to the rank metric, the presented decoding algorithm consists of two steps. The decoder first determines the error support from the syndrome matrix $\boldsymbol{S} = \boldsymbol{H}\boldsymbol{Y}^\top$. Secondly, erasure decoding is performed to recover the error $\boldsymbol{E}$ itself.

3.1 The Error Support

The error matrix $\boldsymbol{E}$ can be decomposed as

$$\boldsymbol{E} = \boldsymbol{A}\boldsymbol{B} \tag{1}$$

where $\boldsymbol{A} = (\boldsymbol{A}^{(1)} \mid \boldsymbol{A}^{(2)} \mid \dots \mid \boldsymbol{A}^{(\ell)}) \in \mathbb{F}_{q^m}^{s\times t}$ with $\boldsymbol{A}^{(i)} \in \mathbb{F}_{q^m}^{s\times t_i}$ and $\mathrm{rk_q}(\boldsymbol{A}^{(i)}) = t_i$ and

$$\boldsymbol{B} = \mathrm{diag}\,(\boldsymbol{B}^{(1)}, \dots, \boldsymbol{B}^{(\ell)}) \in \mathbb{F}_q^{t\times n} \tag{2}$$

with $\boldsymbol{B}^{(i)} \in \mathbb{F}_q^{t_i\times n_i}$ and $\mathrm{rk_q}(\boldsymbol{B}^{(i)}) = t_i$ for all $i \in [1:\ell]$ (see [17, Lemma 10]). The rank support of one block $\boldsymbol{E}^{(i)}$ is defined as

$$\mathrm{supp}_R\left(\boldsymbol{E}^{(i)}\right) := \mathcal{R}_q\left(\boldsymbol{E}^{(i)}\right) = \mathcal{R}_q\left(\boldsymbol{B}^{(i)}\right).$$

The sum-rank support for the error $\boldsymbol{E}$ with sum-rank weight t is then defined as

$$\begin{aligned}\mathrm{supp}_{\Sigma R}(\boldsymbol{E}) :=& \,\mathrm{supp}_R\left(\boldsymbol{E}^{(1)}\right) \times \mathrm{supp}_R\left(\boldsymbol{E}^{(2)}\right) \times \dots \times \mathrm{supp}_R\left(\boldsymbol{E}^{(\ell)}\right) \\ =& \,\mathcal{R}_q\left(\boldsymbol{B}^{(1)}\right) \times \mathcal{R}_q\left(\boldsymbol{B}^{(2)}\right) \times \dots \times \mathcal{R}_q\left(\boldsymbol{B}^{(\ell)}\right).\end{aligned} \tag{3}$$

The following result from [17] shows how the error matrix $\boldsymbol{E}$ can be reconstructed from the sum-rank support and the syndrome matrix $\boldsymbol{S}$.

Lemma 1 (Column-Erasure Decoder [17, Theorem 13]). *Let $t < d$ and $\boldsymbol{B} = \mathrm{diag}\,(\boldsymbol{B}^{(1)}, \dots, \boldsymbol{B}^{(\ell)}) \in \mathbb{F}_q^{t\times n}$ be a basis of the row space of the error matrix $\boldsymbol{E} \in \mathbb{F}_{q^m}^{s\times n}$ and $\boldsymbol{S} = \boldsymbol{H}\boldsymbol{E}^\top \in \mathbb{F}_{q^m}^{(n-k)\times \ell}$ be the corresponding syndrome matrix. Then, the error is given by $\boldsymbol{E} = \boldsymbol{A}\boldsymbol{B}$ with $\boldsymbol{A}$ being the unique solution of the linear system*

$$\boldsymbol{S} = (\boldsymbol{H}\boldsymbol{B}^\top)\boldsymbol{A}^\top$$

and $\boldsymbol{E}$ can be computed in $O\big((n-k)^3 m^2\big)$ operations over $\mathbb{F}_q$.

3.2 Recovering the Error Support

In the following we show how to recover the sum-rank support $\mathrm{supp}_{\Sigma R}(\boldsymbol{E})$ of the error $\boldsymbol{E}$ given the syndrome matrix

$$\boldsymbol{S} = \boldsymbol{H}\boldsymbol{Y}^\top = \boldsymbol{H}\boldsymbol{E}^\top = \sum_{i=1}^{\ell} \boldsymbol{H}^{(i)}(\boldsymbol{E}^{(i)})^\top$$

and the parity-check matrix $\boldsymbol{H}$ of the sum-rank-metric code $\mathcal{IC}[s; \boldsymbol{n}, k, d]$. Let $\boldsymbol{P} \in \mathbb{F}_{q^m}^{(n-k)\times(n-k)}$ with $\mathrm{rk}_{\mathrm{q^m}}(\boldsymbol{P}) = n-k$ be such that $\boldsymbol{PS} = \mathrm{REF}(\boldsymbol{S})$. Further, let $\boldsymbol{H}_{\mathrm{sub}}$ be the rows of $\boldsymbol{PH}$ corresponding to the zero rows in $\boldsymbol{PS}$, i.e. we have

$$\boldsymbol{PS} = \begin{pmatrix} \boldsymbol{S}' \\ \boldsymbol{0} \end{pmatrix} \quad \text{and} \quad \boldsymbol{PH} = \begin{pmatrix} \boldsymbol{H}' \\ \boldsymbol{H}_{\mathrm{sub}} \end{pmatrix}$$

where $\boldsymbol{S}'$ and $\boldsymbol{H}'$ have the same number of rows. Since $\boldsymbol{P}$ performs $\mathbb{F}_{q^m}$-linear row operations on $\boldsymbol{H}$, the ℓ blocks of $\boldsymbol{PH}$ are preserved, i.e. we have that

$$\boldsymbol{H}_{\mathrm{sub}} = \left(\boldsymbol{H}_{\mathrm{sub}}^{(1)} \,|\, \boldsymbol{H}_{\mathrm{sub}}^{(2)} \,|\, \dots \,|\, \boldsymbol{H}_{\mathrm{sub}}^{(\ell)}\right).$$

The following lemma is a generalization of [18, Lemma 3] to the sum-rank metric.

Lemma 2. *Let* $\boldsymbol{H} = (\boldsymbol{H}^{(1)} \,|\, \boldsymbol{H}^{(2)} \,|\, \dots \,|\, \boldsymbol{H}^{(\ell)}) \in \mathbb{F}_{q^m}^{(n-k)\times n}$ *be a parity-check matrix of a sum-rank-metric code* $\mathcal{C}$ *and let* $\boldsymbol{S} = \boldsymbol{H}\boldsymbol{E}^\top \in \mathbb{F}_{q^m}^{(n-k)\times s}$ *be the syndrome matrix of an error*

$$\boldsymbol{E} = (\boldsymbol{E}^{(1)} \,|\, \boldsymbol{E}^{(2)} \,|\, \dots \,|\, \boldsymbol{E}^{(\ell)}) \in \mathbb{F}_{q^m}^{s\times n}$$

of sum-rank weight $\mathrm{wt}_{\Sigma R}(\boldsymbol{E}) = t < n-k$ *where* $\boldsymbol{E}^{(i)} \in \mathbb{F}_{q^m}^{s\times n_i}$ *with* $\mathrm{rk}_q(\boldsymbol{E}^{(i)}) = t_i$ *for all* $i \in [1:\ell]$*. Let* $\boldsymbol{P} \in \mathbb{F}_{q^m}^{(n-k)\times(n-k)}$ *be a matrix with* $\mathrm{rk}_{q^m}(\boldsymbol{P}) = n-k$ *such that* $\boldsymbol{PS}$ *is in row-echelon form. Then,* $\boldsymbol{PS}$ *has at least* $n-k-t$ *zero rows. Let* $\boldsymbol{H}_{sub}$ *be the submatrix of* $\boldsymbol{PH}$ *corresponding to the zero rows in* $\boldsymbol{PS}$*. Then we have that*

$$\mathcal{R}_{q^m}(\boldsymbol{H}_{sub}) = \ker_r(\boldsymbol{E})_{q^m} \cap \mathcal{C}^\perp \iff \mathcal{R}_{q^m}(\boldsymbol{H}_{sub}) = \ker_r(\boldsymbol{E})_{q^m} \cap \mathcal{R}_{q^m}(\boldsymbol{H}).$$

Proof. Since $\boldsymbol{E}^{(i)}$ has $\mathbb{F}_q$-rank t_i, its $\mathbb{F}_{q^m}$-rank is at most t_i for all $i \in [1:\ell]$. Since $t = \sum_{i=1}^{\ell} t_i$, $\boldsymbol{E}$ has at most $\mathbb{F}_{q^m}$-rank t as well. Hence, the $\mathbb{F}_{q^m}$-rank of $\boldsymbol{S}$ is at most t and thus at least $n-k-t$ of the $n-k$ rows of $\boldsymbol{PS}$ are zero.

The rows of $\boldsymbol{PH}$ and therefore also the rows of $\boldsymbol{H}_{\mathrm{sub}}$ are in the row space of $\boldsymbol{H}$, i.e. in the dual code $\mathcal{C}^\perp$. Since $\boldsymbol{H}_{\mathrm{sub}}\boldsymbol{E}^\top = \boldsymbol{0}$ the rows of $\boldsymbol{H}_{\mathrm{sub}}$ are in the kernel of $\boldsymbol{E}$. It is left to show that the rows of $\boldsymbol{H}_{\mathrm{sub}}$ span the entire intersection space. Write

$$\boldsymbol{PS} = \begin{pmatrix} \boldsymbol{S}' \\ \boldsymbol{0} \end{pmatrix} \quad \text{and} \quad \boldsymbol{PH} = \begin{pmatrix} \boldsymbol{H}' \\ \boldsymbol{H}_{\mathrm{sub}} \end{pmatrix}$$

where $\boldsymbol{S}'$ and $\boldsymbol{H}'$ have the same number of rows and $\boldsymbol{S}'$ has full $\mathbb{F}_{q^m}$-rank. Let $\boldsymbol{v} = (\boldsymbol{v}_1, \boldsymbol{v}_2) \in \mathbb{F}_{q^m}^{n-k}$ and let

$$\boldsymbol{h} = \boldsymbol{v} \cdot \begin{pmatrix} \boldsymbol{H}' \\ \boldsymbol{H}_{\text{sub}} \end{pmatrix}$$

be a vector in the row space of $\boldsymbol{PH}$ and in the kernel of $\boldsymbol{E}$. Since $\boldsymbol{H}_{\text{sub}}\boldsymbol{E}^\top = \boldsymbol{0}$ we have that $\boldsymbol{0} = \boldsymbol{h}\boldsymbol{E}^\top = \boldsymbol{v}_1\boldsymbol{H}'\boldsymbol{E}^\top = \boldsymbol{v}_1\boldsymbol{S}'$. This implies that $\boldsymbol{v}_1 = \boldsymbol{0}$ since the rows of $\boldsymbol{S}'$ are linearly independent and thus $\boldsymbol{h}$ is in the row space of $\boldsymbol{H}_{\text{sub}}$. □

Lemma 3 shows that the kernel $\ker_r(\boldsymbol{E})_{q^m}$ of the error $\boldsymbol{E}$ is connected with the kernel of the matrix $\boldsymbol{B}$ if the $\mathbb{F}_{q^m}$-rank of the error is t, i.e. if the full-rank condition is satisfied.

Lemma 3. *Let $\boldsymbol{E} = (\boldsymbol{E}^{(1)} \mid \boldsymbol{E}^{(2)} \mid \ldots \mid \boldsymbol{E}^{(\ell)}) \in \mathbb{F}_{q^m}^{s \times n}$ be an error of sum-rank weight $\mathrm{wt}_{\Sigma R}(\boldsymbol{E}) = t$ where $\boldsymbol{E}^{(i)} \in \mathbb{F}_{q^m}^{s \times n_i}$ with $\mathrm{rk}_q(\boldsymbol{E}) = t_i$ for all $i \in [1:\ell]$. If $\mathrm{rk}_{q^m}(\boldsymbol{E}) = t$ (full-rank condition), then*

$$\ker_r(\boldsymbol{E})_{q^m} = \ker_r(\boldsymbol{B})_{q^m}$$

where $\boldsymbol{B} \in \mathbb{F}_q^{t \times n}$ is any basis for the $\mathbb{F}_q$-row space of $\boldsymbol{E}$ of the form (2). Further, it holds that

$$\ker_r(\boldsymbol{E}^{(i)})_{q^m} = \ker_r(\boldsymbol{B}^{(i)})_{q^m}, \quad \forall i \in [1:\ell].$$

Proof. Let $\boldsymbol{E}$ have $\mathbb{F}_{q^m}$-rank t and let $\boldsymbol{E} = \boldsymbol{AB}$ be a decomposition of the error as in (1) such that $\boldsymbol{E}^{(i)} = \boldsymbol{A}^{(i)}\boldsymbol{B}^{(i)}$ for all $i \in [1:\ell]$. Since $\mathrm{rk}_{q^m}(\boldsymbol{E}) = t$ implies that $\mathrm{rk}_{q^m}(\boldsymbol{A}) = t$, we have that $\ker_r(\boldsymbol{A})_{q^m} = \{\boldsymbol{0}\}$. Hence, for all $\boldsymbol{v} \in \mathbb{F}_{q^m}^n$, $(\boldsymbol{AB})\boldsymbol{v}^\top = \boldsymbol{0}$ if and only if $\boldsymbol{B}\boldsymbol{v}^\top = \boldsymbol{0}$ which is equivalent to

$$\ker_r(\boldsymbol{E})_{q^m} = \ker_r(\boldsymbol{AB})_{q^m} = \ker_r(\boldsymbol{B})_{q^m}. \tag{4}$$

Assume a vector $\boldsymbol{v} = (\boldsymbol{v}^{(1)} \mid \boldsymbol{v}^{(2)} \mid \ldots \mid \boldsymbol{v}^{(\ell)}) \in \mathbb{F}_{q^m}^n$ and let $\boldsymbol{v}^{(i)} \in \mathbb{F}_{q^m}^{n_i}$ be any element in $\ker_r(\boldsymbol{B}^{(i)})_{q^m}$. Due to the block-diagonal structure of $\boldsymbol{B}$ (see (2)) we have that

$$\boldsymbol{B}\boldsymbol{v}^\top = \boldsymbol{0} \quad \Longleftrightarrow \quad \boldsymbol{B}^{(i)}(\boldsymbol{v}^{(i)})^\top = \boldsymbol{0}, \quad \forall i \in [1:\ell]$$

which is equivalent to

$$\boldsymbol{v} \in \ker_r(\boldsymbol{B})_{q^m} \quad \Longleftrightarrow \quad \boldsymbol{v}^{(i)} \in \ker_r(\boldsymbol{B}^{(i)})_{q^m}, \quad \forall i \in [1:\ell]. \tag{5}$$

Combining (4) and (5) yields the result. □

Combining Lemma 2 and Lemma 3 finally allows us to recover the sum-rank support of $\boldsymbol{E}$.

Theorem 1. *Let $\boldsymbol{E} = (\boldsymbol{E}^{(1)} \mid \boldsymbol{E}^{(2)} \mid \ldots \mid \boldsymbol{E}^{(\ell)}) \in \mathbb{F}_{q^m}^{s \times n}$ be an error of sum-rank weight $\mathrm{wt}_{\Sigma R}(\boldsymbol{E}) = t \leq d-2$ where $\boldsymbol{E}^{(i)} \in \mathbb{F}_{q^m}^{s \times n_i}$ with $\mathrm{rk}_q(\boldsymbol{E}^{(i)}) = t_i$ for all $i \in [1:\ell]$. If $s \geq t$ (high-order condition) and $\mathrm{rk}_{q^m}(\boldsymbol{E}) = t$ (full-rank condition), then*

$$\mathcal{R}_q\left(\boldsymbol{E}^{(i)}\right) = \ker_r\left(\mathit{ext}(\boldsymbol{H}_{\mathit{sub}}^{(i)})\right)_q, \quad \forall i \in [1:\ell]. \tag{6}$$

Proof. In the following, we prove that the $\mathbb{F}_q$-row space of the extended $\boldsymbol{H}_{\mathrm{sub}}$ instead of the $\mathbb{F}_{q^m}$-row space of $\boldsymbol{H}_{\mathrm{sub}}$ is equal to the $\mathbb{F}_q$-kernel of $\boldsymbol{B}$, i.e.,

$$\mathcal{R}_q(\mathrm{ext}(\boldsymbol{H}_{\mathrm{sub}})) = \ker_r(\boldsymbol{B})_q.$$

Recall that $\mathcal{R}_q\big(\boldsymbol{E}^{(i)}\big) = \mathcal{R}_q\big(\boldsymbol{B}^{(i)}\big)$ holds for all $i \in [1:\ell]$ according to the definition of the error decomposition (1). With this in mind, the statement of the theorem is equivalent to showing $\ker_r(\boldsymbol{B}^{(i)})_q = \mathcal{R}_q\Big(\mathrm{ext}(\boldsymbol{H}_{\mathrm{sub}}^{(i)})\Big)$ for all $i \in [1:\ell]$ since $\mathcal{R}_q\big(\boldsymbol{B}^{(i)}\big)^{\perp} = \ker_r(\boldsymbol{B}^{(i)})_q$ and $\ker_r\left(\mathrm{ext}(\boldsymbol{H}_{\mathrm{sub}}^{(i)})\right)_q^{\perp} = \mathcal{R}_q\Big(\mathrm{ext}(\boldsymbol{H}_{\mathrm{sub}}^{(i)})\Big)$ hold.

First we show that $\mathcal{R}_q(\mathrm{ext}(\boldsymbol{H}_{\mathrm{sub}})) \subseteq \ker_r(\boldsymbol{B})_q$ which, due to the block-diagonal structure of $\boldsymbol{B}$, implies that $\mathcal{R}_q\Big(\mathrm{ext}(\boldsymbol{H}_{\mathrm{sub}}^{(i)})\Big) \subseteq \ker_r(\boldsymbol{B}^{(i)})_q$ for all $i \in [1:\ell]$. Let $\boldsymbol{v} = (\boldsymbol{v}^{(1)} \,|\, \boldsymbol{v}^{(2)} \,|\, \ldots \,|\, \boldsymbol{v}^{(\ell)}) \in \mathbb{F}_{q^m}^n$ with $\boldsymbol{v}^{(i)} \in \mathbb{F}_{q^m}^{n_i}$ for all $i \in [1:\ell]$ be any element in the $\mathbb{F}_{q^m}$-linear row space of $\boldsymbol{H}_{\mathrm{sub}}$. Then, by [18, Lemma 5] we have that each row $\boldsymbol{v}_j$ for $j \in [1:m]$ of $\mathrm{ext}(\boldsymbol{v})$ is in $\mathcal{R}_q(\mathrm{ext}(\boldsymbol{H}_{\mathrm{sub}}))$ which implies that $\boldsymbol{v}_j^{(i)} \in \mathcal{R}_q\Big(\mathrm{ext}(\boldsymbol{H}_{\mathrm{sub}}^{(i)})\Big)$ for all $i \in [1:\ell]$. By Lemma 3 we have that $\boldsymbol{v} \in \ker_r(\boldsymbol{B})_{q^m}$, i.e. we have

$$\boldsymbol{B}\boldsymbol{v}^{\top} = \boldsymbol{0} \quad \Longleftrightarrow \quad \boldsymbol{B}^{(i)}(\boldsymbol{v}^{(i)})^{\top} = \boldsymbol{0}, \quad \forall i \in [1:\ell]$$

where the right-hand side follows from the block-diagonal structure of $\boldsymbol{B}$. Since the entries of $\boldsymbol{B}$ are from $\mathbb{F}_q$, we have that

$$\mathrm{ext}(\boldsymbol{B}\boldsymbol{v}^{\top}) = \boldsymbol{B}\mathrm{ext}(\boldsymbol{v})^{\top} = \boldsymbol{0} \tag{7}$$

which implies that $\boldsymbol{v} \in \ker_r(\boldsymbol{B})_q$ and thus $\mathcal{R}_q(\mathrm{ext}(\boldsymbol{H}_{\mathrm{sub}})) \subseteq \ker_r(\boldsymbol{B})_q$. Due to the block-diagonal structure of $\boldsymbol{B}$ we get from (7) that

$$\mathrm{ext}(\boldsymbol{B}^{(i)}(\boldsymbol{v}^{(i)})^{\top}) = \boldsymbol{B}^{(i)}\mathrm{ext}(\boldsymbol{v}^{(i)})^{\top} = \boldsymbol{0}, \quad \forall i \in [1:\ell] \tag{8}$$

which implies that $\boldsymbol{v}_j^{(i)} \in \ker_r(\boldsymbol{B}^{(i)})_q$ for all $i \in [1:\ell]$ and $j \in [1:m]$. Therefore, we have that $\mathcal{R}_q\Big(\mathrm{ext}(\boldsymbol{H}_{\mathrm{sub}}^{(i)})\Big) \subseteq \ker_r(\boldsymbol{B}^{(i)})_q$, for all $i \in [1:\ell]$.

Next, we show that $\ker_r(\boldsymbol{B}^{(i)})_q = \mathcal{R}_q\Big(\mathrm{ext}(\boldsymbol{H}_{\mathrm{sub}}^{(i)})\Big)$ for all $i \in [1:\ell]$ by showing that

$$r_i := \dim\left(\mathcal{R}_q\Big(\mathrm{ext}(\boldsymbol{H}_{\mathrm{sub}}^{(i)})\Big)\right) = n_i - t_i, \quad \forall i \in [1:\ell].$$

Since $\mathcal{R}_q\Big(\mathrm{ext}(\boldsymbol{H}_{\mathrm{sub}}^{(i)})\Big) \subseteq \ker_r(\boldsymbol{B}^{(i)})_q$ we have that $r_i > n_i - t_i$ is not possible for all $i \in [1:\ell]$.

In the following we show that $r < n-t$ is not possible and therefore $r_i = n_i - t_i$ holds for all $i = [1:\ell]$. Let $\{\boldsymbol{h}_1, \ldots, \boldsymbol{h}_r\} \subseteq \mathbb{F}_q^n$ be a basis for $\mathcal{R}_q(\mathrm{ext}(\boldsymbol{H}_{\mathrm{sub}}))$ and define

$$\boldsymbol{H}_b = \begin{pmatrix} \boldsymbol{h}_1 \\ \boldsymbol{h}_2 \\ \vdots \\ \boldsymbol{h}_r \end{pmatrix} \in \mathbb{F}_q^{r \times n}$$

with $\boldsymbol{h}_j = (\boldsymbol{h}_j^{(1)} \mid \boldsymbol{h}_j^{(2)} \mid \ldots \mid \boldsymbol{h}_j^{(\ell)}) \in \mathbb{F}_q^n$ where $\boldsymbol{h}_j^{(i)} \in \mathcal{R}_q\left(\mathrm{ext}(\boldsymbol{H}_{\mathrm{sub}}^{(i)})\right)$ for $j \in [1:r]$ and $i \in [1:\ell]$. Also define

$$\boldsymbol{H}_b^{(i)} = \begin{pmatrix} \boldsymbol{h}_1^{(i)} \\ \boldsymbol{h}_2^{(i)} \\ \vdots \\ \boldsymbol{h}_r^{(i)} \end{pmatrix} \in \mathbb{F}_q^{r \times n_i}, \quad \forall i \in [1:\ell].$$

By the basis-extension theorem, there exist matrices $\boldsymbol{B}^{(i)''} \in \mathbb{F}_q^{(n_i - t_i) \times n_i}$ such that the matrices

$$\boldsymbol{B}^{(i)'} := \left(\left(\boldsymbol{B}^{(i)}\right)^\top \mid \left(\boldsymbol{B}^{(i)''}\right)^\top \right) \in \mathbb{F}_q^{n_i \times n_i}$$

have $\mathbb{F}_q$-rank n_i for all $i \in [1:\ell]$.

Next define $\check{\boldsymbol{H}}^{(i)} = \boldsymbol{H}_b^{(i)} \boldsymbol{B}^{(i)'} \in \mathbb{F}_q^{r \times n_i}$ for all $i \in [1:\ell]$ and

$$\check{\boldsymbol{H}} := \left(\check{\boldsymbol{H}}^{(1)} \mid \check{\boldsymbol{H}}^{(2)} \mid \ldots \mid \check{\boldsymbol{H}}^{(\ell)}\right) = \boldsymbol{H}_b \cdot \mathrm{diag}\left(\boldsymbol{B}^{(1)'}, \ldots, \boldsymbol{B}^{(\ell)'}\right).$$

Since $\boldsymbol{h}_1^{(i)}, \boldsymbol{h}_2^{(i)}, \ldots, \boldsymbol{h}_r^{(i)}$ are in the right $\mathbb{F}_q$-kernel of $\boldsymbol{B}^{(i)}$ (see (8)) we have that

$$\check{\boldsymbol{H}}^{(i)} = \begin{pmatrix} 0 & \ldots & 0 & \check{h}_{1,t_i+1}^{(i)} & \ldots & \check{h}_{1,n_i}^{(i)} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \ldots & 0 & \check{h}_{r,t_i+1}^{(i)} & \ldots & \check{h}_{r,n_i}^{(i)} \end{pmatrix}$$

for all $i \in [1:\ell]$ and thus $\check{\boldsymbol{H}}$ has at least $t = \sum_{i=1}^{\ell} t_i$ all-zero columns.

By the assumption that $r < n - t$ it follows that $r_i < n_i - t_i$ holds for at least one block. Without loss of generality assume that this holds for the ℓ-th block, i.e. we have $r_\ell < n_\ell - t_\ell$. Then there exists a full-rank matrix

$$\boldsymbol{J} = \left(\begin{array}{c|c} \boldsymbol{I}_{t_\ell} & \boldsymbol{0} \\ \hline \boldsymbol{0} & \widetilde{\boldsymbol{J}} \end{array}\right) \in \mathbb{F}_q^{n_\ell \times n_\ell}$$

with $\widetilde{\boldsymbol{J}} \in \mathbb{F}_q^{(n_\ell - t_\ell) \times (n_\ell - t_\ell)}$ such that the matrix

$$\widetilde{\boldsymbol{H}} = \check{\boldsymbol{H}} \cdot \mathrm{diag}\left(\boldsymbol{I}_{n_1}, \ldots, \boldsymbol{I}_{n_{\ell-1}}, \boldsymbol{J}\right) \tag{9}$$

has at least $t+1$ all-zero columns.

Define $\boldsymbol{D} := \mathrm{diag}\left(\boldsymbol{B}^{(1)'}, \ldots, \boldsymbol{B}^{(\ell-1)'}, \boldsymbol{B}^{(\ell)'}\boldsymbol{J}\right) \in \mathbb{F}_q^{n \times n}$ which has full $\mathbb{F}_q$-rank n. Then we have that $\widetilde{\boldsymbol{H}} = \boldsymbol{H}_b \cdot \boldsymbol{D}$. Since $\boldsymbol{D}$ has full $\mathbb{F}_q$-rank n, the submatrix $\boldsymbol{D}' := \boldsymbol{D}_{[1:n],\mathcal{I}} \in \mathbb{F}_q^{n \times (t+1)}$ has $\mathbb{F}_q$-rank $t+1$, where

$$\mathcal{I} = [1:t_1] \cup [n_1+1 : n_1+t_2] \cup [n_{\ell-2}+1 : n_{\ell-2}+t_{\ell-1}] \cup [n_{\ell-1}+1 : n_{\ell-1}+t_\ell+1]$$

By (9) it follows that

$$\boldsymbol{h}_j \cdot \boldsymbol{D}' = \mathbf{0} \in \mathbb{F}_q^{t+1} \tag{10}$$

for all $j \in [1:r]$. Since $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k)\times n}$ is a parity-check matrix of an $[\boldsymbol{n}, k, d]$ code it has at most $d-1$ $\mathbb{F}_{q^m}$-linearly dependent columns (see [17, Lemma 12]). Since by assumption $t+1 \le d-1$ and $\mathrm{rk_q}(\boldsymbol{D}') = t+1$ we have that $\mathrm{rk_{q^m}}(\boldsymbol{H}\boldsymbol{D}') = t+1$. Thus, there exists a vector $\boldsymbol{g} \in \mathcal{R}_{q^m}(\boldsymbol{H})$ such that

$$\boldsymbol{g}\boldsymbol{D}' = (\mathbf{0}, g'_{t+1}) \in \mathbb{F}_{q^m}^{t+1}$$

with $g'_{t+1} \neq 0$. Since the first t positions of $\boldsymbol{g}\boldsymbol{D}'$ are equal to zero we have that $\boldsymbol{g} \in \mathcal{R}_{q^m}(\boldsymbol{H}_{\mathrm{sub}})$. Expanding the vector $\boldsymbol{g}\boldsymbol{D}'$ over $\mathbb{F}_q$ gives

$$\mathrm{ext}(\boldsymbol{g})\boldsymbol{D}' = \begin{pmatrix} \mathbf{0} & g'_{1,t+1} \\ \mathbf{0} & g'_{2,t+1} \\ \vdots & \vdots \\ \mathbf{0} & g'_{m,t+1} \end{pmatrix} \in \mathbb{F}_q^{m\times(t+1)}$$

where $\mathrm{ext}(g'_{t+1}) = (g'_{1,t+1}, g'_{2,t+1}, \ldots, g'_{m,t+1})^\top \in \mathbb{F}_q^{m\times 1}$. Since $g'_{t+1} \neq 0$ there exists at least one row with index ι in $\mathrm{ext}(\boldsymbol{g}'_{t+1})$ such that $g'_{\iota,t+1} \neq 0$. Let $\boldsymbol{g}_\iota$ be the row in $\mathrm{ext}(\boldsymbol{g})$ for which $\boldsymbol{g}_\iota \boldsymbol{D}'$ is not all-zero. This leads to a contradiction according to (10). Thus $r < n - t$ is not possible and leaves $r = n - t$ and therefore also $r_i = n_i - t_i$ for all $i \in [1:\ell]$ as the only valid option. □

3.3 A Metzner–Kapturowski-Like Decoding Algorithm

Using Theorem 1 we can formulate an efficient decoding algorithm for high-order interleaved sum-rank-metric codes. The algorithm is given in Algorithm 1 and proceeds similar to the Metzner–Kapturowski(-like) decoding algorithms for Hamming- or rank-metric codes. As soon as $\boldsymbol{H}_{\mathrm{sub}}$ is computed from the syndrome matrix $\boldsymbol{S}$, the rank support of each block can be recovered independently using the results from Theorem 1. This corresponds to finding a matrix $\boldsymbol{B}^{(i)}$ with $\mathrm{rk}_q(\boldsymbol{B}^{(i)}) = t_i$ such that $\mathrm{ext}(\boldsymbol{H}_{\mathrm{sub}}^{(i)})(\boldsymbol{B}^{(i)})^\top = \mathbf{0}$ for all $i \in [1:\ell]$ (see (6)).

Theorem 2. *Let* $\boldsymbol{C}$ *be a codeword of a homogeneous* s*-interleaved sum-rank-metric code* $\mathcal{IC}[s; \boldsymbol{n}, k, d]$ *of minimum sum-rank distance* d*. Furthermore, let* $\boldsymbol{E} \in \mathbb{F}_{q^m}^{s\times n}$ *be an error matrix of sum-rank weight* $\mathrm{wt}_{\Sigma R}(\boldsymbol{E}) = t \le d-2$ *that fulfills* $t \le s$ *(*high-order condition*) and* $\mathrm{rk_{q^m}}(\boldsymbol{E}) = t$ *(*full-rank condition*). Then* $\boldsymbol{C}$ *can be uniquely recovered from the received word* $\boldsymbol{Y} = \boldsymbol{C} + \boldsymbol{E}$ *using Algorithm 1 in a time complexity equivalent to*

$$O\big(\max\{n^3, n^2 s\}\big)$$

operations in $\mathbb{F}_{q^m}$*.*

Algorithm 1: Decoding High-Order Interleaved Sum-Rank-Metric Codes

Input : Parity-check matrix $\boldsymbol{H}$, Received word $\boldsymbol{Y}$

Output: Transmitted codeword $\boldsymbol{C}$

1 $\boldsymbol{S} \leftarrow \boldsymbol{H}\boldsymbol{Y}^\top \in \mathbb{F}_{q^m}^{(n-k)\times s}$

2 Compute $\boldsymbol{P} \in \mathbb{F}_{q^m}^{(n-k)\times(n-k)}$ s.t. $\boldsymbol{PS} = \mathrm{REF}(\boldsymbol{S})$

3 $\boldsymbol{H}_{\mathrm{sub}} = \left(\boldsymbol{H}_{\mathrm{sub}}^{(1)} \mid \boldsymbol{H}_{\mathrm{sub}}^{(2)} \mid \dots \mid \boldsymbol{H}_{\mathrm{sub}}^{(\ell)}\right) \leftarrow (\boldsymbol{PH})_{[t+1:n-k],[1:n]} \in \mathbb{F}_{q^m}^{(n-t-k)\times n}$

4 **for** $i = 1, \dots, \ell$ **do**

5   Compute $\boldsymbol{B}^{(i)} \in \mathbb{F}_q^{t_i \times n_i}$ s.t. $\mathrm{ext}(\boldsymbol{H}_{\mathrm{sub}}^{(i)})(\boldsymbol{B}^{(i)})^\top = \boldsymbol{0}$ and $\mathrm{rk}_q(\boldsymbol{B}^{(i)}) = t_i$

6 $\boldsymbol{B} \leftarrow \mathrm{diag}(\boldsymbol{B}^{(1)}, \boldsymbol{B}^{(2)}, \dots, \boldsymbol{B}^{(\ell)}) \in \mathbb{F}_q^{t\times n}$

7 Compute $\boldsymbol{A} \in \mathbb{F}_{q^m}^{s\times t}$ s.t. $(\boldsymbol{H}\boldsymbol{B}^\top)\boldsymbol{A}^\top = \boldsymbol{S}$

8 $\boldsymbol{C} \leftarrow \boldsymbol{Y} - \boldsymbol{AB} \in \mathbb{F}_{q^m}^{s\times n}$

9 **return** $\boldsymbol{C}$

Proof. By Lemma 1 the error matrix $\boldsymbol{E}$ can be decomposed into $\boldsymbol{E} = \boldsymbol{AB}$. Algorithm 1 first determines a basis of the error support $\mathrm{supp}_{\Sigma R}(\boldsymbol{E})$ and then performs erasure decoding to obtain $\boldsymbol{A}$. The matrix $\boldsymbol{B}$ is computed by transforming $\boldsymbol{S}$ into row-echelon form using a transformation matrix $\boldsymbol{P}$ (see Line 2). In Line 3, $\boldsymbol{H}_{\mathrm{sub}}$ is obtained by choosing the last $n-k-t$ rows of $\boldsymbol{PH}$. Then using Theorem 1 for each block (see Line 5) we find a matrix $\boldsymbol{B}^{(i)}$ whose rows form a basis for $\ker_r\left(\mathrm{ext}(\boldsymbol{H}_{\mathrm{sub}}^{(i)})\right)_q$ and therefore a basis for $\mathrm{supp}_R(\boldsymbol{E}^{(i)})$ for all $i \in [1:\ell]$. The matrix $\boldsymbol{B}$ is the block-diagonal matrix formed by $\boldsymbol{B}^{(i)}$ (cf. (2) and see Line 6). Finally, $\boldsymbol{A}$ can be computed from $\boldsymbol{B}$ and $\boldsymbol{H}$ using Lemma 1 in Line 7. Hence, Algorithm 1 returns the transmitted codeword in Line 9. The complexities of the lines in the algorithm are as follows:

- Line 1: The syndrome matrix $\boldsymbol{S} = \boldsymbol{H}\boldsymbol{Y}^\top$ can be computed in at most $O\big(n^2 s\big)$ operations in $\mathbb{F}_{q^m}$.
- Line 2: The transformation of $[\boldsymbol{S} \mid \boldsymbol{I}]$ into row-echelon form requires

$$O\big((n-k)^2(s+n-k)\big) \subseteq O\big(\max\{n^3, n^2 s\}\big)$$

  operations in $\mathbb{F}_{q^m}$.
- Line 3: The product $(\boldsymbol{PH})_{[t+1:n-k],[1:n]}$ can be computed requiring at most $O(n(n-k-t)(n-k)) \subseteq O\big(n^3\big)$ operations in $\mathbb{F}_{q^m}$.
- Line 5: The transformation of $[\mathrm{ext}(\boldsymbol{H}_{\mathrm{sub}}^{(i)})^\top \mid \boldsymbol{I}^\top]^\top$ into column-echelon form requires $O\big(n_i^2((n-k-t)m + n_i)\big)$ operations in $\mathbb{F}_q$ per block. Overall we get $O\Big(\sum_{i=1}^{\ell} n_i^2((n-k-t)m+n_i)\Big) \subseteq O\big(n^3 m\big)$ operations in $\mathbb{F}_q$ since we have that $O\Big(\sum_{i=1}^{\ell} n_i^2\Big) \subseteq O\big(n^2\big)$.

– Line 7: According to Lemma 1, this step can be done in $O\big((n-k)^3m^2\big)$ operations over $\mathbb{F}_q$.
– Line 8: The product $\boldsymbol{AB} = (\boldsymbol{A}^{(1)}\boldsymbol{B}^{(1)} \mid \boldsymbol{A}^{(2)}\boldsymbol{B}^{(2)} \mid \ldots \mid \boldsymbol{A}^{(\ell)}\boldsymbol{B}^{(\ell)})$ can be computed in $\sum_{i=1}^{\ell} O(st_in_i) \subseteq O\big(sn^2\big)$ and the difference of $\boldsymbol{Y} - \boldsymbol{AB}$ can be computed in $O(sn)$ operations in $\mathbb{F}_{q^m}$.

The complexities for Line 5 and Line 7 are given for operations in $\mathbb{F}_q$. The number of $\mathbb{F}_q$-operations of both steps together is in $O\big(n^3m^2\big)$ and their execution complexity can be bounded by $O\big(n^3\big)$ operations in $\mathbb{F}_{q^m}$ (see [3]).

Thus, Algorithm 1 requires $O\big(\max\{n^3, n^2s\}\big)$ operations in $\mathbb{F}_{q^m}$ and $O\big(n^3m^2\big)$ operations in $\mathbb{F}_q$. □

Note that the complexity of Algorithm 1 is not affected by the decoding complexity of the underlying constituent code since a generic code with no structure is assumed.

Example 1. Let $\mathbb{F}_{q^m} = \mathbb{F}_{5^2}$ with the primitive polynomial $x^2 + 4x + 2$ and the primitive element α be given. Further let $\mathcal{IC}[s; \boldsymbol{n}, k, d]$ be an interleaved sum-rank-metric code of length n with $\boldsymbol{n} = (2, 2, 2)$, $k = 2$, $d = 5$, $\ell = 3$ and $s = 3$, defined by a generator matrix

$$\boldsymbol{G} = \left(\begin{array}{cc|cc|cc} \alpha^4 & \alpha^7 & \alpha^{21} & \alpha^4 & \alpha^3 & \alpha^5 \\ \alpha^{20} & \alpha^{11} & \alpha^{10} & \alpha^{21} & \alpha^{17} & \alpha^3 \end{array}\right)$$

and a parity-check matrix

$$\boldsymbol{H} = \left(\begin{array}{cc|cc|cc} 1 & 0 & 0 & 0 & \alpha^8 & \alpha^{19} \\ 0 & 1 & 0 & 0 & \alpha^5 & \alpha^{12} \\ 0 & 0 & 1 & 0 & \alpha^{17} & \alpha \\ 0 & 0 & 0 & 1 & \alpha^{22} & \alpha^{18} \end{array}\right).$$

Suppose that the codeword

$$\boldsymbol{C} = \left(\begin{array}{cc|cc|cc} \alpha^{20} & \alpha^{22} & 1 & \alpha^6 & \alpha^{11} & \alpha^{10} \\ \alpha^{23} & \alpha^7 & \alpha^4 & 0 & \alpha^{17} & \alpha^9 \\ \alpha^{15} & 1 & \alpha^{22} & \alpha^{12} & \alpha^{22} & \alpha^{10} \end{array}\right) \in \mathcal{IC}[s; \boldsymbol{n}, k, d]$$

is corrupted by the error

$$\boldsymbol{E} = \left(\begin{array}{cc|cc|cc} \alpha^{19} & \alpha & \alpha^6 & \alpha^9 & 0 & 0 \\ \alpha^{17} & \alpha^{23} & \alpha^{10} & \alpha^7 & 0 & 0 \\ \alpha^2 & \alpha^8 & \alpha^{15} & \alpha^6 & 0 & 0 \end{array}\right)$$

with $\mathrm{wt}_{\Sigma R}(\boldsymbol{E}) = \mathrm{rk}_{q^m}(\boldsymbol{E}) = t = 3$ and $t_1 = 1, t_2 = 2$ and $t_3 = 0$. The resulting received matrix is

$$\boldsymbol{Y} = \left(\begin{array}{cc|cc|cc} \alpha^{17} & \alpha^8 & \alpha^{18} & \alpha^{16} & \alpha^{11} & \alpha^{10} \\ \alpha^{11} & \alpha^3 & \alpha^{22} & \alpha^7 & \alpha^{17} & \alpha^9 \\ \alpha^7 & \alpha^4 & \alpha^{23} & 1 & \alpha^{22} & \alpha^{10} \end{array}\right).$$

First the syndrome matrix is computed as

$$\boldsymbol{S} = \boldsymbol{H}\boldsymbol{Y}^\top = \begin{pmatrix} \alpha^{19} & \alpha^{17} & \alpha^{2} \\ \alpha & \alpha^{23} & \alpha^{8} \\ \alpha^{6} & \alpha^{10} & \alpha^{15} \\ \alpha^{9} & \alpha^{7} & \alpha^{6} \end{pmatrix}$$

and then $\boldsymbol{P}$

$$\boldsymbol{P} = \begin{pmatrix} 0 & \alpha^{2} & \alpha^{6} & \alpha^{8} \\ 0 & \alpha^{4} & \alpha^{20} & \alpha^{15} \\ 0 & \alpha^{23} & 0 & \alpha^{3} \\ 1 & \alpha^{6} & 0 & 0 \end{pmatrix} \Longrightarrow \boldsymbol{P}\boldsymbol{S} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

with $\mathrm{rk}_{q^m}(\boldsymbol{P}) = 4$. The last $n - k - t = 1$ rows of

$$\boldsymbol{P}\boldsymbol{H} = \left(\begin{array}{cc|cc|cc} 0 & \alpha^{2} & \alpha^{6} & \alpha^{8} & \alpha^{13} & \alpha^{7} \\ 0 & \alpha^{4} & \alpha^{20} & \alpha^{15} & \alpha^{22} & \alpha^{16} \\ 0 & \alpha^{23} & 0 & \alpha^{3} & \alpha^{11} & 1 \\ 1 & \alpha^{6} & 0 & 0 & \alpha^{18} & \alpha^{16} \end{array}\right)$$

gives us $\boldsymbol{H}_{\mathrm{sub}} = (1 \;\; \alpha^6 \,|\, 0 \;\; 0 \,|\, \alpha^{18} \;\; \alpha^{16})$. We expand every block of $\boldsymbol{H}_{\mathrm{sub}}$ over $\mathbb{F}_5$ and get

$$\mathrm{ext}(\boldsymbol{H}_{\mathrm{sub}}^{(1)}) = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}, \quad \mathrm{ext}(\boldsymbol{H}_{\mathrm{sub}}^{(2)}) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad \mathrm{ext}(\boldsymbol{H}_{\mathrm{sub}}^{(3)}) = \begin{pmatrix} 3 & 3 \\ 0 & 3 \end{pmatrix}.$$

We observe that the second block $\boldsymbol{H}_{\mathrm{sub}}^{(2)}$ is zero which corresponds to a full-rank error. Next we compute a basis for each of the right kernels of $\mathrm{ext}(\boldsymbol{H}_{\mathrm{sub}}^{(1)})$, $\mathrm{ext}(\boldsymbol{H}_{\mathrm{sub}}^{(2)})$, and $\mathrm{ext}(\boldsymbol{H}_{\mathrm{sub}}^{(3)})$ which gives us

$$\boldsymbol{B}^{(1)} = \begin{pmatrix} 1 & 2 \end{pmatrix}, \quad \boldsymbol{B}^{(2)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \boldsymbol{B}^{(3)} = (),$$

where $\boldsymbol{B}^{(3)}$ is empty since $\mathrm{ext}(\boldsymbol{H}_{\mathrm{sub}}^{(3)})$ has full rank. The matrix $\boldsymbol{B}$ is then given by

$$\boldsymbol{B} = \mathrm{diag}(\boldsymbol{B}^{(1)}, \boldsymbol{B}^{(2)}, \boldsymbol{B}^{(3)}) = \left(\begin{array}{cc|cc|cc} 1 & 2 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ \hline \end{array}\right).$$

Solving for $\boldsymbol{A}$

$$\boldsymbol{H}\boldsymbol{B}^\top\boldsymbol{A}^\top = \boldsymbol{S}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ \alpha^{6} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \boldsymbol{A}^\top = \begin{pmatrix} \alpha^{19} & \alpha^{17} & \alpha^{2} \\ \alpha & \alpha^{23} & \alpha^{8} \\ \alpha^{6} & \alpha^{10} & \alpha^{15} \\ \alpha^{9} & \alpha^{7} & \alpha^{6} \end{pmatrix}$$

gives

$$\boldsymbol{A}^\top = \begin{pmatrix} \alpha^{19} & \alpha^{17} & \alpha^{2} \\ \alpha^{6} & \alpha^{10} & \alpha^{15} \\ \alpha^{9} & \alpha^{7} & \alpha^{6} \end{pmatrix} \Rightarrow \hat{\boldsymbol{E}} = \boldsymbol{A}\boldsymbol{B} = \left(\begin{array}{cc|cc|cc} \alpha^{19} & \alpha & \alpha^{6} & \alpha^{9} & 0 & 0 \\ \alpha^{17} & \alpha^{23} & \alpha^{10} & \alpha^{7} & 0 & 0 \\ \alpha^{2} & \alpha^{8} & \alpha^{15} & \alpha^{6} & 0 & 0 \end{array}\right)$$

and $\hat{\boldsymbol{E}} = \boldsymbol{E}$. Finally, the codeword $\boldsymbol{C}$ can be recovered as $\boldsymbol{C} = \boldsymbol{Y} - \hat{\boldsymbol{E}}$.

4 Implications for Decoding High-Order Interleaved Skew-Metric Codes

The *skew metric* is closely related to the sum-rank metric and was first considered in [10]. In particular, there exists an isometry between the sum-rank metric and the skew metric for most code parameters (see [10, Theorem 3]).

We show in this section how an interleaved skew-metric code can be constructed from a high-order interleaved sum-rank-metric code. This enables us to apply the presented decoder to the obtained high-order interleaved skew-metric codes and correct errors of a fixed skew weight.

The mentioned isometry can be described and applied to the interleaved context as follows: Let us consider vectors from $\mathbb{F}_{q^m}^n$, where n satisfies the constraints in [10, Theorem 2]. By [10, Theorem 3], there exists an invertible diagonal matrix $\boldsymbol{D} \in \mathbb{F}_{q^m}^{n\times n}$ such that

$$\mathrm{wt}_{\Sigma R}(\boldsymbol{x}\boldsymbol{D}) = \mathrm{wt}_{skew}(\boldsymbol{x}), \qquad \forall \boldsymbol{x} \in \mathbb{F}_{q^m}^n, \tag{11}$$

where for the definition of the skew weight $\mathrm{wt}_{skew}(\cdot)$ see [10, Definition 9]. The skew metric for interleaved matrices has been considered in [2]. Namely, the extension of (11) to $\mathbb{F}_{q^m}^{s\times n}$, we get (see [2])

$$\mathrm{wt}_{\Sigma R}(\boldsymbol{X}\boldsymbol{D}) = \mathrm{wt}_{skew}(\boldsymbol{X}), \qquad \forall \boldsymbol{X} \in \mathbb{F}_{q^m}^{s\times n}. \tag{12}$$

Now consider a linear s-interleaved sum-rank-metric code $\mathcal{IC}[s;\boldsymbol{n},k,d]$ with parity-check matrix $\boldsymbol{H}$. Then by (12) the code

$$\mathcal{IC}_{skew}[s;n,k,d] := \left\{\boldsymbol{C}\boldsymbol{D}^{-1} : \boldsymbol{C} \in \mathcal{IC}[s;\boldsymbol{n},k,d]\right\}$$

is an s-interleaved skew-metric code with minimum skew distance d. Observe that the parity-check matrix of the constituent skew-metric code $\mathcal{C}_{skew}[n,k,d]$ of $\mathcal{IC}_{skew}[s;n,k,d]$ is given by $\boldsymbol{H}_{skew} = \boldsymbol{H}\boldsymbol{D}$.

Let us now study a decoding problem related to the obtained skew-metric code. Consider a matrix $\boldsymbol{Y} = \boldsymbol{C} + \boldsymbol{E}$ where $\boldsymbol{C} \in \mathcal{IC}_{skew}[s;n,k,d]$ and $\boldsymbol{E}$ is an error matrix with $\mathrm{wt}_{skew}(\boldsymbol{E}) = t$. Then (12) implies that we have

$$\widetilde{\boldsymbol{Y}} := (\boldsymbol{C} + \boldsymbol{E})\boldsymbol{D} = \widetilde{\boldsymbol{C}} + \widetilde{\boldsymbol{E}}$$

where $\widetilde{\boldsymbol{C}} \in \mathcal{IC}[s;\boldsymbol{n},k,d]$ and $\mathrm{wt}_{\Sigma R}(\boldsymbol{E}) = t$. Hence, using the isometry from [10, Theorem 3] we can map the decoding problem in the skew metric to the sum-rank metric and vice versa (see also [2]).

In particular, this allows us to use Algorithm 1 to solve the posed decoding problem in the skew metric. The steps to decode a high-order interleaved skew-metric code $\mathcal{IC}_{skew}[s; n, k, d]$ with parity-check matrix $\boldsymbol{H}_{skew}$ (whose parameters comply with [10, Theorem 2]) can be summarized as follows:

1. Compute the transformed received matrix $\widetilde{\boldsymbol{Y}} := (\boldsymbol{C} + \boldsymbol{E})\boldsymbol{D} = \widetilde{\boldsymbol{C}} + \widetilde{\boldsymbol{E}}$ where $\boldsymbol{C} \in \mathcal{IC}_{skew}[s; n, k, d]$ and $\mathrm{wt}_{skew}(\boldsymbol{E}) = t$.
2. Apply Algorithm 1 to $\widetilde{\boldsymbol{Y}}$. If $\mathrm{rk}_{q^m}(\widetilde{\boldsymbol{E}}) = t$, which is equivalent to $\mathrm{rk}_{q^m}(\boldsymbol{E}) = t$, the algorithm recovers $\widetilde{\boldsymbol{C}} \in \mathcal{IC}[s; \boldsymbol{n}, k, d]$.
3. Recover $\boldsymbol{C} \in \mathcal{IC}_{skew}[s; n, k, d]$ as $\boldsymbol{C} = \widetilde{\boldsymbol{C}}\boldsymbol{D}^{-1}$.

Since the first and the third step both require $O(sn)$ operations in $\mathbb{F}_{q^m}$, the overall complexity is dominated by the complexity of Algorithm 1, that is $O\big(\max\{n^3, n^2 s\}\big)$ operations in $\mathbb{F}_{q^m}$.

5 Comparison of Metzner-Kapturowski-Like Decoders in the Hamming, Rank and Sum-Rank Metric

The decoder presented in Algorithm 1 is a generalization of the Metzner–Kapturowski decoder for the Hamming metric [14] and the Metzner–Kapturowski-like decoder for the rank metric [18]. In this section we illustrate how the proposed decoder works in three different metrics: 1.) Hamming metric, 2.) Rank metric and 3.) Sum-rank metric. Note that the Hamming and the rank metric are both special cases of the sum-rank metric. We also show the analogy of the different definitions of the error support for all three cases.

The support for the Hamming-metric case is defined as

$$\mathrm{supp}_H(\boldsymbol{E}) := \{j \,:\, j\text{-th column of } \boldsymbol{E} \text{ is non-zero}\}.$$

In the Hamming metric an error matrix $\boldsymbol{E}$ with t_H errors can be decomposed into $\boldsymbol{E} = \boldsymbol{A}\boldsymbol{B}$, where the rows of $\boldsymbol{B}$ are the unit vectors corresponding to the t_H error positions. This means the support of the error matrix is given by the union of the supports of the rows $\boldsymbol{B}_i$ of $\boldsymbol{B}$ ($\forall i \in [1 : t_H]$), hence

$$\mathrm{supp}_H(\boldsymbol{E}) = \bigcup_{i=1}^{t_H} \mathrm{supp}_H(\boldsymbol{B}_i).$$

If the condition for the Metzner–Kapturowski decoder is fulfilled (*full-rank condition*), then the zero columns in $\boldsymbol{H}_{\mathrm{sub}}$ indicate the error positions and thus give rise to the error support, i.e. we have that

$$\mathrm{supp}_H(\boldsymbol{E}) = [1 : n] \setminus \bigcup_{i=1}^{n-k-t_H} \mathrm{supp}_H(\boldsymbol{H}_{\mathrm{sub},i})$$

where $\boldsymbol{H}_{\mathrm{sub},i}$ is the i-th row of $\boldsymbol{H}_{\mathrm{sub}}$. Figure 1 illustrates how the error support $\mathrm{supp}_H(\boldsymbol{E})$ can be recovered from $\boldsymbol{H}_{\mathrm{sub}}$.

The rank-metric case is similar, except for a different notion for the error support. Again, the error $\boldsymbol{E}$ with $\mathrm{rk}_q(\boldsymbol{E}) = t_R$ can be decomposed as $\boldsymbol{E} = \boldsymbol{A}\boldsymbol{B}$. Then the rank support $\mathrm{supp}_R(\boldsymbol{E})$ of $\boldsymbol{E}$ equals the row space of $\mathrm{ext}(\boldsymbol{B})$, which is spanned by the union of all rows of $\mathrm{ext}(\boldsymbol{B}_i)$ with $\boldsymbol{B}_i$ being the i-th row of $\boldsymbol{B}$. This means the support of $\boldsymbol{E}$ is given by

$$\mathrm{supp}_R(\boldsymbol{E}) = \bigoplus_{i=1}^{t_R} \mathrm{supp}_R(\boldsymbol{B}_i)$$

with $\bigoplus$ being the addition of vector spaces, which means the span of the union of the considered spaces. If the condition on the error matrix (*full-rank condition*) is fulfilled, the rank support of $\boldsymbol{E}$ is given by the kernel of $\mathrm{ext}(\boldsymbol{H}_{\mathrm{sub}})$ [20]. As illustrated in Fig. 2 the row space of $\mathrm{ext}(\boldsymbol{H}_{\mathrm{sub}})$ can be computed by obtaining the span of the union of spaces $\mathrm{supp}_R(\boldsymbol{H}_{\mathrm{sub},i})$, where $\boldsymbol{H}_{\mathrm{sub},i}$ is the i-th row of $\boldsymbol{H}_{\mathrm{sub}}$. Finally, the support of $\boldsymbol{E}$ is given by

$$\mathrm{supp}_R(\boldsymbol{E}) = \left(\bigoplus_{i=1}^{n-k-t_R} \mathrm{supp}_R(\boldsymbol{H}_{\mathrm{sub},i})\right)^{\perp}.$$

For the sum-rank metric we get from (3) that

$$\begin{aligned}\mathrm{supp}_{\Sigma R}(\boldsymbol{E}) &= \mathrm{supp}_R\left(\boldsymbol{B}^{(1)}\right) \times \mathrm{supp}_R\left(\boldsymbol{B}^{(2)}\right) \times \cdots \times \mathrm{supp}_R\left(\boldsymbol{B}^{(\ell)}\right)\\ &= \left(\bigoplus_{i=1}^{n-k-t_1} \mathrm{supp}_R(\boldsymbol{B}_1^{(1)})\right) \times \cdots \times \left(\bigoplus_{i=1}^{n-k-t_\ell} \mathrm{supp}_R(\boldsymbol{B}_\ell^{(\ell)})\right).\end{aligned}$$

According to Theorem 1 we have that

$$\begin{aligned}\mathrm{supp}_{\Sigma R}(\boldsymbol{E}) = \left(\bigoplus_{i=1}^{n-k-t_1} \mathrm{supp}_R(\boldsymbol{H}_{\mathrm{sub},1}^{(1)})\right)^{\perp} \times \dots\\ \cdots \times \left(\bigoplus_{i=1}^{n-k-t_\ell} \mathrm{supp}_R(\boldsymbol{H}_{\mathrm{sub},\ell}^{(\ell)})\right)^{\perp}.\end{aligned}$$

The relation between the error matrix $\boldsymbol{E}$, the matrix $\boldsymbol{H}_{\mathrm{sub}}$ and the error supports for the Hamming metric, rank metric and sum-rank metric are illustrated in Fig. 1, Fig. 2 and Fig. 3, respectively.

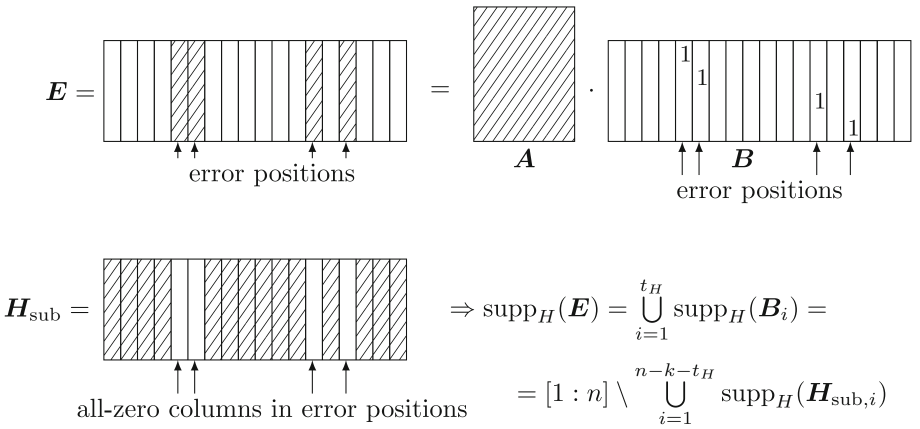

Fig. 1. Illustration of the error support for the Hamming-metric case with $\boldsymbol{E} \in \mathbb{F}_{q^m}^{s \times n}$, $\boldsymbol{A} \in \mathbb{F}_{q^m}^{s \times t_H}$, $\boldsymbol{B} \in \mathbb{F}_{q}^{t_H \times n}$ and $\boldsymbol{H}_{\text{sub}} \in \mathbb{F}_{q^m}^{(n-k-t_H) \times n}$. $\boldsymbol{B}_i$ is the i-th row of $\boldsymbol{B}$ and $\boldsymbol{H}_{\text{sub},i}$ the i-th row of $\boldsymbol{H}_{\text{sub}}$.

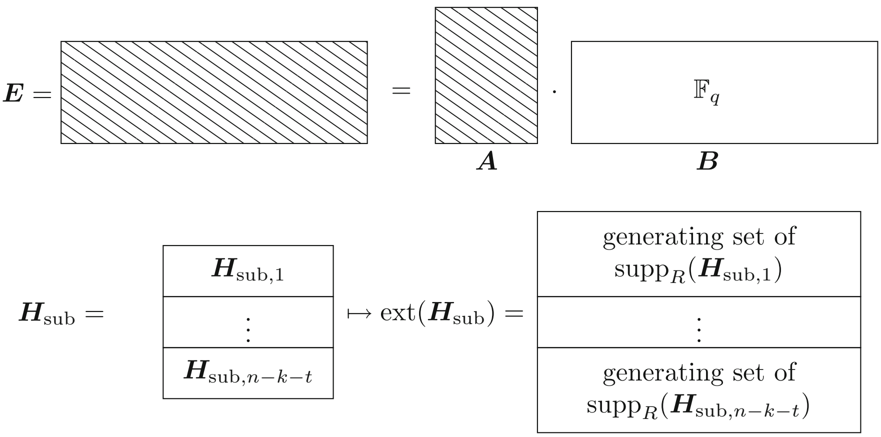

Fig. 2. Illustration of the error support for the rank-metric case with $\boldsymbol{E} \in \mathbb{F}_{q^m}^{s \times n}$, $\boldsymbol{A} \in \mathbb{F}_{q^m}^{s \times t_R}$, $\boldsymbol{B} \in \mathbb{F}_{q}^{t_R \times n}$ and $\boldsymbol{H}_{\text{sub}} \in \mathbb{F}_{q^m}^{(n-k-t_R) \times n}$. $\boldsymbol{B}_i$ is the i-th row of $\boldsymbol{B}$ and $\boldsymbol{H}_{\text{sub},i}$ the i-th row of $\boldsymbol{H}_{\text{sub}}$.

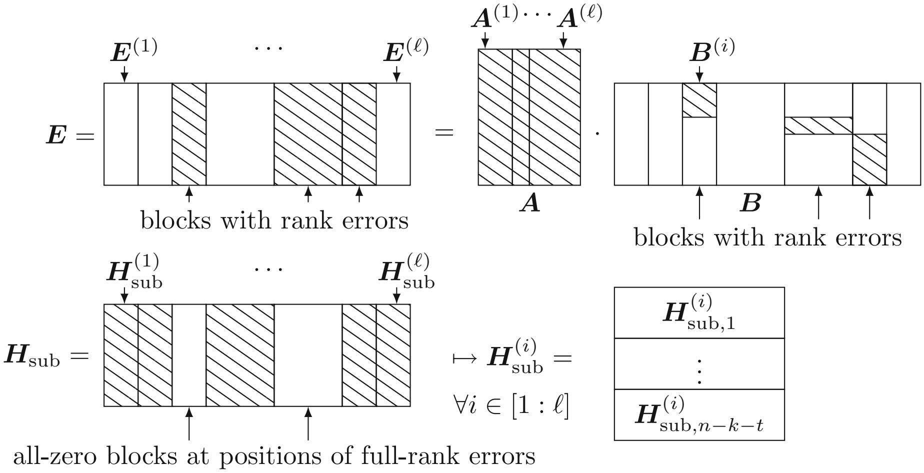

Fig. 3. Illustration of the error support for the sum-rank-metric case with $\boldsymbol{E} \in \mathbb{F}_{q^m}^{s \times n}$, $\boldsymbol{A} \in \mathbb{F}_{q^m}^{s \times t_{\Sigma R}}$, $\boldsymbol{B} \in \mathbb{F}_q^{t_{\Sigma R} \times n}$ and $\boldsymbol{H}_{\mathrm{sub}} \in \mathbb{F}_{q^m}^{(n-k-t_{\Sigma R}) \times n}$. $\boldsymbol{B}_i$ is the i-th row of $\boldsymbol{B}$ and $\boldsymbol{H}_{\mathrm{sub},i}$ the i-th row of $\boldsymbol{H}_{\mathrm{sub}}$.

6 Conclusion

We studied the decoding of homogeneous s-interleaved sum-rank-metric codes that are obtained by vertically stacking s codewords of the same arbitrary linear constituent code $\mathcal{C}$ over $\mathbb{F}_{q^m}$. The proposed Metzner–Kapturowski-like decoder for the sum-rank metric relies on linear-algebraic operations only and has a complexity of $O\big(\max\{n^3, n^2 s\}\big)$ operations in $\mathbb{F}_{q^m}$, where n denotes the length of $\mathcal{C}$. The decoder works for any linear constituent code and therefore the decoding complexity is not affected by the decoding complexity of the constituent code. The proposed Metzner–Kapturowski-like decoder can guarantee to correct error matrices $\boldsymbol{E} \in \mathbb{F}_{q^m}^{s \times n}$ of sum-rank weight $t \leq d - 2$, where d is the minimum distance of $\mathcal{C}$, if $\boldsymbol{E}$ has full $\mathbb{F}_{q^m}$-rank t, which implies the high-order condition $s \geq t$.

As the sum-rank metric generalizes both, the Hamming metric and the rank metric, Metzner and Kapturowski's decoder in the Hamming metric and its analog in the rank metric are both recovered as special cases from our proposal. Moreover, we showed how the presented algorithm can be used to solve the decoding problem of some high-order interleaved skew-metric codes.

Since the decoding process is independent of any structural knowledge about the constituent code, this result has a high impact on the design and the security-level estimation of new code-based cryptosystems in the sum-rank metric. In fact, if high-order interleaved codes are e.g. used in a classical McEliece-like scheme, any error of sum-rank weight $t \leq d-2$ with full $\mathbb{F}_{q^m}$-rank t can be decoded without knowledge of the private key. This directly renders this approach insecure and shows that the consequences of the presented results need to be carefully considered for the design of quantum-resistant public-key systems.

We conclude the paper by giving some further research directions: The proposed decoder is capable of decoding an error correctly as long as it satisfies the full-rank condition and has sum-rank weight at most $d-2$, where d denotes the minimum distance of the constituent code. Similar to Haslach and Vinck's work [6] in the Hamming metric, it could be interesting to abandon the full-rank condition and study a decoder that can also handle linearly dependent errors. Another approach, that has already been pursued in the Hamming and the rank metric [15,18], is to allow error weights exceeding $d-2$ and investigate probabilistic decoding.

Moreover, an extension of the decoder to heterogeneous interleaved codes (cp. [18] for the rank-metric case) and the development of a more general decoding framework for high-order interleaved skew-metric codes can be investigated.

References

1. Alagic, G., et al.: Status report on the third round of the NIST post-quantum cryptography standardization process (2022)
2. Bartz, H., Puchinger, S.: Fast decoding of interleaved linearized Reed-Solomon codes and variants. IEEE Trans. Inf. Theory. arXiv preprint arXiv:2201.01339 (2022)
3. Couveignes, J.M., Lercier, R.: Elliptic periods for finite fields. Finite Fields Appl. **15**(1), 1–22 (2009). https://doi.org/10.1016/j.ffa.2008.07.004
4. Elleuch, M., Wachter-Zeh, A., Zeh, A.: A public-key cryptosystem from interleaved Goppa codes. arXiv preprint arXiv:1809.03024 (2018)
5. Haslach, C., Vinck, A.H.: A decoding algorithm with restrictions for array codes. IEEE Trans. Inf. Theory **45**(7), 2339–2344 (1999)
6. Haslach, C., Vinck, A.H.: Efficient decoding of interleaved linear block codes. In: 2000 IEEE International Symposium on Information Theory (Cat. No. 00CH37060), p. 149. IEEE (2000)
7. Holzbaur, L., Liu, H., Puchinger, S., Wachter-Zeh, A.: On decoding and applications of interleaved Goppa codes. In: 2019 IEEE International Symposium on Information Theory (ISIT), pp. 1887–1891 (2019)
8. Krachkovsky, V.Y., Lee, Y.X.: Decoding for iterative Reed-Solomon coding schemes. IEEE Trans. Magn. **33**(5), 2740–2742 (1997)
9. Loidreau, P., Overbeck, R.: Decoding rank errors beyond the error correcting capability. In: International Workshop on Algebraic and Combinatorial Coding Theory (ACCT), pp. 186–190 (2006)
10. 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)
11. McEliece, R.J.: A public-key cryptosystem based on algebraic coding theory. Coding THV **4244**, 114–116 (1978)
12. Metzner, J.J.: Vector symbol decoding with erasures, errors and symbol list decisions. In: Proceedings IEEE International Symposium on Information Theory, p. 34. IEEE (2002)
13. Metzner, J.J.: Vector symbol decoding with list inner symbol decisions. IEEE Trans. Commun. **51**(3), 371–380 (2003)

14. Metzner, J.J., Kapturowski, E.J.: A general decoding technique applicable to replicated file disagreement location and concatenated code decoding. IEEE Trans. Inf. Theory **36**(4), 911–917 (1990)
15. Oh, K.T., Metzner, J.J.: Performance of a general decoding technique over the class of randomly chosen parity check codes. IEEE Trans. Inf. Theory **40**(1), 160–166 (1994)
16. Porwal, A., Holzbaur, L., Liu, H., Renner, J., Wachter-Zeh, A., Weger, V.: Interleaved Prange: a new generic decoder for interleaved codes. In: Cheon, J.H., Johansson, T. (eds.) Post-Quantum Cryptography (PQCrypto 2022). LNCS, vol. 13512, pp. 69–88. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-17234-2_4
17. Puchinger, S., Renner, J., Rosenkilde, J.: Generic decoding in the sum-rank metric. In: 2020 IEEE International Symposium on Information Theory (ISIT), pp. 54–59. IEEE (2020)
18. Puchinger, S., Renner, J., Wachter-Zeh, A.: Decoding high-order interleaved rank-metric codes. arXiv preprint arXiv:1904.08774 (2019)
19. Renner, J., Puchinger, S., Wachter-Zeh, A.: Interleaving Loidreau's rank-metric cryptosystem. In: 2019 XVI International Symposium "Problems of Redundancy in Information and Control Systems" (REDUNDANCY), pp. 127–132. IEEE (2019)
20. Renner, J., Puchinger, S., Wachter-Zeh, A.: Decoding high-order interleaved rank-metric codes. In: 2021 IEEE International Symposium on Information Theory (ISIT), pp. 19–24. IEEE (2021)
21. Roth, R.M., Vontobel, P.O.: Coding for combined block-symbol error correction. IEEE Trans. Inf. Theory **60**(5), 2697–2713 (2014)