




An Error-Code Perspective on Metzner–Kapturowski-like Decoders

Thomas Jerkovits , *Graduate Student Member, IEEE*, Felicitas
Hörmann , *Graduate Student Member, IEEE*, Hannes Bartz , *Member, IEEE*

Abstract

In this paper we consider a Metzner–Kapturowski-like decoding algorithm for high-order interleaved sum-rank-metric codes, offering a novel perspective on the decoding process through the concept of an error code. The error code, defined as the linear code spanned by the vectors forming the error matrix, provides a more intuitive understanding of the decoder’s functionality and new insights.

The proposed algorithm can correct errors of sum-rank weight up to $d - 2$, where d is the minimum distance of the constituent code, given a sufficiently large interleaving order. The decoder’s versatility is highlighted by its applicability to any linear constituent code, including unstructured or random codes. The computational complexity is $O(\max\{n^3, n^2s\})$ operations over \mathbb{F}_{q^m} , where n is the code length and s is the interleaving order.

We further explore the success probability of the decoder for random errors, providing an efficient algorithm to compute an upper bound on this probability. Additionally, we derive bounds and approximations for the success probability when the error weight exceeds the unique decoding radius, showing that the decoder maintains a high success probability in this regime.

Our findings suggest that this decoder could be a valuable tool for the design and security analysis of code-based cryptosystems using interleaved sum-rank-metric codes. The new insights into the decoding process and the high success probability of the algorithm even beyond the unique decoding radius underscore its potential to contribute to various coding-related applications.

Index Terms

Channel coding, decoding, sum-rank metric, interleaved codes, Metzner–Kapturowski, code-based cryptography, cryptanalysis, high-order interleaving

I. INTRODUCTION

The need for post-quantum cryptography has become increasingly important due to recent advances in the design and realization of quantum computers. This has led to the National Insti-

tute of Standards and Technology (NIST)’s post-quantum cryptography standardization process, which has shown that many promising candidates for key encapsulation mechanisms (KEMs) belong to the family of code-based systems. Three of these candidates are still in the current 4th round [1].

Most code-based cryptosystems are based on the McEliece cryptosystem [2], which uses a public code that can only be efficiently decoded with knowledge of the secret key as its trapdoor. However, a major drawback of code-based cryptosystems is their large public key sizes when compared to other schemes based on, e.g., lattices or isogenies. Completely unstructured (i.e., random) codes require a large key size, while the usage of highly structured codes often results in vulnerabilities that can be exploited in structural attacks.

Interleaving has been proposed as one approach to mitigate the key-size issue in variants of the McEliece cryptosystem based on interleaved codes in the Hamming and rank metric [3]–[5]. By allowing for a larger decoding radius and a higher error weight, denoted by t , interleaving increases the attack cost for the same-sized parameters. This effectively reduces the public-key size while maintaining the same security level. The interleaving order, denoted by s , plays a crucial role in the decoding process and the overall performance of the cryptosystem.

There exist list and probabilistic unique decoders for interleaved Reed–Solomon (RS) codes in the Hamming metric [6], for interleaved Gabidulin codes in the rank metric [7], and for interleaved linearized Reed–Solomon (LRS) codes in the sum-rank metric [8]. However, these decoders are tailored to a particular code family and explicitly exploit the code structure. In contrast, the Metzner–Kapturowski decoder, originally proposed in the Hamming metric, exploits a high interleaving order s to successfully decode errors with high probability, independent of the constituent code [9]. This purely linear-algebraic decoder has been further studied and generalized to the rank [10] and sum-rank metric [11].

The sum-rank metric is part of a metric family that includes both the Hamming and the rank metric as special cases and can be seen as a blend of these two metrics. In this framework, codeword vectors are discretely organized into blocks of equal length. The sum-rank metric offers a balanced approach between the Hamming and rank metric, potentially making it more challenging for adversaries to exploit system vulnerabilities.

Compared to the Hamming metric, the rank metric has a higher generic decoding complexity for a given error weight. However, for the same decoding “attack complexity”, it allows for smaller error weights and therefore smaller code parameters, which in turn leads to smaller key

sizes.

However, many rank-metric cryptosystems rely on highly structured codes, which have been subject to attacks and have been broken in some cases. Significantly, many attacks effective in the Hamming metric may prove ineffective in the rank metric and vice versa (e.g. [12]). Given this unique attribute, the sum-rank metric offers a balanced approach, potentially making it more resistant to attacks that exploit vulnerabilities specific to either the Hamming or rank metric. By carefully choosing the block size and the number of blocks, the sum-rank metric can be tuned to achieve a desired balance between security and key size. This flexibility makes the sum-rank metric an attractive option for designing code-based cryptosystems that are secure against quantum and classical attacks while maintaining practical key sizes.

The goal of this paper is twofold: (1) to provide more intuition about Metzner–Kapturowski-like decoders by using an interpretation involving an *error code* and (2) to extend the results from our previous work [11]. For (1), we make a connection to a code that we call the error code, which is spanned by the s rows of the error matrix. This perspective allows us to provide a more intuitive understanding of the decoding process by relating it to properties of the error code. Furthermore, this new error-code perspective enables us to simplify proofs and derive new interpretations for the special cases in the Hamming and rank metric. For (2), we investigate the success probability for high interleaving orders but randomly chosen errors that are not necessarily full-rank. We provide an algorithm to efficiently compute and upper bound this probability and present a more precise analysis of the decoding condition and bounds on its occurrence probability for arbitrary error weight. We derive lower and upper bounds, as well as an approximation for the success probability, in the case of $t \geq d - 1$, where d is the minimum distance of the underlying code, using random coding techniques. We also provide simulation results to support the tightness of our analysis. The outcome of this analysis reveals that the success probability remains relatively high even for $t \geq d - 1$. We provide examples to illustrate these bounds and approximation.

We present a Metzner–Kapturowski-like decoding algorithm for high-order interleaved sum-rank-metric codes with an arbitrary linear constituent code that can correct errors of sum-rank weight t up to $t < n - k$, where n and k denote the length and dimension of the linear constituent code, respectively. Remarkably, the proposed algorithm works for any linear constituent code, including unstructured or random codes, making it highly versatile. The computational complexity of the algorithm is in the order of $O(\max\{n^3, n^2s\})$ operations over \mathbb{F}_{q^m} . 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. This gives valuable insights for the design of McEliece-like cryptosystems based on interleaved codes in the sum-rank metric. Since the sum-rank metric generalizes both the Hamming and the rank metric, the original Metzner–Kapturowski decoder [9] as well as its rank-metric analog [10] can be recovered from our proposal.

II. PRELIMINARIES

A. Notation

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

$$\text{ext} : \mathbb{F}_{q^m} \rightarrow \mathbb{F}_q^{m \times 1}$$

such that $\alpha = \mathbf{b} \cdot \text{ext}(\alpha)$.

For a vector $\mathbf{v} = [v_1, \dots, v_n] \in \mathbb{F}_{q^m}^n$, the notation is extended element-wise as follows

$$\text{ext}(\mathbf{v}) = [\text{ext}(v_1), \dots, \text{ext}(v_n)] \in \mathbb{F}_q^{m \times n},$$

where $\text{ext}(\mathbf{v})$ is a matrix with columns $\text{ext}(v_i) \in \mathbb{F}_q^{m \times 1}$ for $i = 1, \dots, n$.

Similarly, for a matrix $\mathbf{M} = [M_{i,j}] \in \mathbb{F}_{q^m}^{k \times n}$, the notation is extended element-wise as follows

$$\text{ext}(\mathbf{M}) = \begin{bmatrix} \text{ext}(M_{1,1}) & \cdots & \text{ext}(M_{1,n}) \\ \vdots & \ddots & \vdots \\ \text{ext}(M_{k,1}) & \cdots & \text{ext}(M_{k,n}) \end{bmatrix} \in \mathbb{F}_q^{mk \times n},$$

where $\text{ext}(\mathbf{M})$ is a matrix obtained by replacing each element $M_{i,j}$ of \mathbf{M} with its corresponding column-wise expansion $\text{ext}(M_{i,j}) \in \mathbb{F}_q^{m \times 1}$, for $i = 1, \dots, k$ and $j = 1, \dots, n$.

For a matrix \mathbf{A} of size $a \times b$ and entries $A_{i,j}$ for $i \in \{1, \dots, a\}$ and $j \in \{1, \dots, b\}$, we define

the submatrix notation

$$\mathbf{A}_{[c:d],[e:f]} := \begin{bmatrix} A_{c,e} & \cdots & A_{c,f} \\ \vdots & \ddots & \vdots \\ A_{d,e} & \cdots & A_{d,f} \end{bmatrix}.$$

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

B. Sum-Rank-Metric Codes

Let $\mathbf{n} = [n_1, \dots, n_\ell] \in \mathbb{N}^\ell$ with $n_i > 0$ for all $i \in \{1, \dots, \ell\}$ be a length partition¹ of n , i.e., $n = \sum_{i=1}^{\ell} n_i$. Further, let $\mathbf{x} = [\mathbf{x}^{(1)} \mid \mathbf{x}^{(2)} \mid \cdots \mid \mathbf{x}^{(\ell)}] \in \mathbb{F}_{q^m}^n$ be a vector over a finite field \mathbb{F}_{q^m} with $\mathbf{x}^{(i)} \in \mathbb{F}_{q^m}^{n_i}$ for each $i \in \{1, \dots, \ell\}$. The rank of each block $\mathbf{x}^{(i)}$ is defined as $\text{rk}_q(\mathbf{x}^{(i)}) := \text{rk}_q(\text{ext}(\mathbf{x}^{(i)}))$, where $\text{ext}(\mathbf{x}^{(i)}) \in \mathbb{F}_q^{m \times n_i}$ is the column-wise expansion of $\mathbf{x}^{(i)}$ over \mathbb{F}_q .

The *sum-rank weight* of \mathbf{x} with respect to the length partition \mathbf{n} is defined as

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

and the *sum-rank distance* between two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{F}_{q^m}^n$ is given by

$$d_{\Sigma R}^{(\mathbf{n})}(\mathbf{x}, \mathbf{y}) := \text{wt}_{\Sigma R}^{(\mathbf{n})}(\mathbf{x} - \mathbf{y}).$$

Note that the sum-rank metric coincides with the Hamming metric when $\ell = n$ (i.e., $n_i = 1$ for all $i \in \{1, \dots, \ell\}$) and reduces to the rank metric when $\ell = 1$.

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 \mathbf{n}), dimension $k := \dim_{q^m}(\mathcal{C})$ and minimum (sum-rank) distance

$$d := \min\{d_{\Sigma R}^{(\mathbf{n})}(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in \mathcal{C}, \mathbf{x} \neq \mathbf{y}\}.$$

To emphasize its parameters, we write $\mathcal{C}[\mathbf{n}, k, d]$ in the following.

C. 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

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

a single constituent code.

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

$$\mathcal{IC}[s; \mathbf{n}, k, d] := \left\{ \begin{bmatrix} \mathbf{c}_1 \\ \vdots \\ \mathbf{c}_s \end{bmatrix} : \mathbf{c}_j \in \mathcal{C}[\mathbf{n}, k, d] \right\} \subseteq \mathbb{F}_{q^m}^{s \times n}.$$

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

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

or equivalently as

$$\mathbf{C} = [\mathbf{C}^{(1)} \mid \mathbf{C}^{(2)} \mid \dots \mid \mathbf{C}^{(\ell)}]$$

where

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

for all $i \in \{1, \dots, \ell\}$.

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

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

where

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

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

D. The Error Support

Let $\mathbf{E} \in \mathbb{F}_q^{s \times n}$ be the error matrix with $\text{wt}_{\Sigma R}^{(n)}(\mathbf{E}) = t$. Then \mathbf{E} can be decomposed as

$$\mathbf{E} = \mathbf{A}\mathbf{B}, \quad (2)$$

where $\mathbf{A} = [\mathbf{A}^{(1)} \mid \mathbf{A}^{(2)} \mid \dots \mid \mathbf{A}^{(\ell)}] \in \mathbb{F}_q^{s \times t}$ is a block matrix with submatrices $\mathbf{A}^{(i)} \in \mathbb{F}_q^{s \times t_i}$ satisfying $\text{rk}_q(\mathbf{A}^{(i)}) = t_i$, and

$$\mathbf{B} = \text{diag}(\mathbf{B}^{(1)}, \dots, \mathbf{B}^{(\ell)}) \in \mathbb{F}_q^{t \times n} \quad (3)$$

is a block-diagonal matrix with submatrices $\mathbf{B}^{(i)} \in \mathbb{F}_q^{t_i \times n_i}$ satisfying $\text{rk}_q(\mathbf{B}^{(i)}) = t_i$ for all $i \in \{1, \dots, \ell\}$ (see [13, Lemma 10]).

The rank support $\text{supp}_R(\mathbf{E}^{(i)})$ and the dual rank support $\text{supp}_R^\perp(\mathbf{E}^{(i)})$ of one block $\mathbf{E}^{(i)}$ for $i \in \{1, \dots, \ell\}$ are defined as the row space of $\mathbf{E}^{(i)}$ and its orthogonal complement, respectively

$$\begin{aligned} \text{supp}_R(\mathbf{E}^{(i)}) &:= \mathcal{R}_q(\mathbf{E}^{(i)}) = \mathcal{R}_q(\mathbf{B}^{(i)}), \\ \text{supp}_R^\perp(\mathbf{E}^{(i)}) &:= \mathcal{R}_q(\mathbf{E}^{(i)})^\perp = \mathcal{R}_q(\mathbf{B}^{(i)})^\perp. \end{aligned}$$

The second equality in each line follows from (2) and [14, Theorem 1].

The sum-rank support of the error \mathbf{E} with sum-rank weight t is then defined as

$$\begin{aligned} \text{supp}_{\Sigma R}(\mathbf{E}) &:= \text{supp}_R(\mathbf{E}^{(1)}) \times \text{supp}_R(\mathbf{E}^{(2)}) \times \dots \times \text{supp}_R(\mathbf{E}^{(\ell)}) \\ &= \mathcal{R}_q(\mathbf{B}^{(1)}) \times \mathcal{R}_q(\mathbf{B}^{(2)}) \times \dots \times \mathcal{R}_q(\mathbf{B}^{(\ell)}). \end{aligned} \quad (4)$$

Additionally, we define the dual sum-rank support as

$$\begin{aligned} \text{supp}_{\Sigma R}^\perp(\mathbf{E}) &:= \text{supp}_R^\perp(\mathbf{E}^{(1)}) \times \text{supp}_R^\perp(\mathbf{E}^{(2)}) \times \dots \times \text{supp}_R^\perp(\mathbf{E}^{(\ell)}) \\ &= \mathcal{R}_q(\mathbf{B}^{(1)})^\perp \times \mathcal{R}_q(\mathbf{B}^{(2)})^\perp \times \dots \times \mathcal{R}_q(\mathbf{B}^{(\ell)})^\perp. \end{aligned}$$

Given two supports $\text{supp}_{\Sigma R}(\mathbf{E}_1)$ and $\text{supp}_{\Sigma R}(\mathbf{E}_2)$, we denote

$$\text{supp}_{\Sigma R}(\mathbf{E}_1) \subseteq \text{supp}_{\Sigma R}(\mathbf{E}_2)$$

if $\text{supp}_R(\mathbf{E}_1^{(i)}) \subseteq \text{supp}_R(\mathbf{E}_2^{(i)})$ holds for all $i \in \{1, \dots, \ell\}$. The notation \subset follows the same principle but implies a strict subset.

Finally, we define

$$\mathbb{F}_q^n := \mathbb{F}_q^{n_1} \times \cdots \times \mathbb{F}_q^{n_\ell}.$$

III. DECODING OF HIGH-ORDER INTERLEAVED SUM-RANK-METRIC CODES

In this section, we propose a Metzner–Kapturowski-like decoder for the sum-rank metric, which generalizes the decoders presented in [9], [10], [15]. The proposed decoder can correct errors of sum-rank weight t up to $d - 2$ in general. Additionally, under specific conditions, the decoder can correct errors of sum-rank weight t up to $n - k - 1$, where n is the length of the code and k is the dimension of the code. The following assumptions are required for the decoder to succeed:

- *High-order condition:* The interleaving order s is greater than or equal to the sum-rank weight of the error, i.e., $s \geq t$.
- *Full-rank condition:* The error matrix has full \mathbb{F}_{q^m} -rank, i.e., $\text{rk}_{q^m}(\mathbf{E}) = t$.

It is worth noting that the full-rank condition automatically implies the high-order condition, as the \mathbb{F}_{q^m} -rank of a matrix $\mathbf{E} \in \mathbb{F}_{q^m}^{s \times n}$ cannot exceed the interleaving order s .

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

$$\mathbf{H} = [\mathbf{H}^{(1)} \mid \mathbf{H}^{(2)} \mid \cdots \mid \mathbf{H}^{(\ell)}] \in \mathbb{F}_{q^m}^{(n-k) \times n}$$

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

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

that is corrupted by an error matrix \mathbf{E} of sum-rank weight $\text{wt}_{\Sigma R}^{(n)}(\mathbf{E}) = t$ assuming the *high-order* and *full-rank* conditions.

As with the original Metzner–Kapturowski algorithm and its adaptation to the rank metric, the presented decoding algorithm consists of two steps:

- 1) The decoder determines the error support $\text{supp}_{\Sigma R}(\mathbf{E})$.
- 2) Erasure decoding is performed using the syndrome matrix $\mathbf{S} = \mathbf{H}\mathbf{Y}^\top = \mathbf{H}\mathbf{E}^\top$ to recover the error \mathbf{E} itself.

The following result is adapted from [13] and shows how the error matrix \mathbf{E} can be reconstructed from the sum-rank support $\text{supp}_{\Sigma R}(\mathbf{E})$ and the syndrome matrix \mathbf{S} . We relax the original condition to make the result more applicable.

Lemma 1 (Column-Erasure Decoder [13, Theorem 13]) Let $\mathbf{B} = \text{diag}(\mathbf{B}^{(1)}, \dots, \mathbf{B}^{(\ell)}) \in \mathbb{F}_q^{t \times n}$ be a basis of the error support $\text{supp}_{\Sigma R}(\mathbf{E})$ of the error matrix $\mathbf{E} \in \mathbb{F}_{q^m}^{s \times n}$, and let $\mathbf{S} = \mathbf{H}\mathbf{E}^\top \in \mathbb{F}_{q^m}^{(n-k) \times s}$ be the corresponding syndrome matrix.

Assume that $\mathbf{H}\mathbf{B}^\top$ is full-rank. Then, the error matrix \mathbf{E} can be uniquely recovered as $\mathbf{E} = \mathbf{A}\mathbf{B}$, where $\mathbf{A} \in \mathbb{F}_{q^m}^{s \times t}$ is the unique solution of the linear system

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

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

Remark 1 From [13, Lemma 12], it directly follows that for $t < d$, the condition that $\mathbf{H}\mathbf{B}^\top$ is full-rank is always satisfied.

A. Recovering the Error Support

Let $\mathbf{t} = [t_1, \dots, t_\ell]$ denote the rank profile of the error matrix \mathbf{E} , where $t_i = \text{rk}_q(\mathbf{E}^{(i)})$ for $i \in \{1, \dots, \ell\}$. In the following, we assume that \mathbf{E} fulfills the full-rank condition, i.e., its \mathbb{F}_{q^m} -rank is equal to its sum-rank weight t . Note that the full-rank condition is satisfied if and only if $\text{rk}_{q^m}(\mathbf{A}) = t$ for an every $\mathbf{A} \in \mathbb{F}_{q^m}^{s \times t}$ as in (2). Under these assumptions, we have that the rows of \mathbf{E} span an \mathbb{F}_{q^m} -linear $[\mathbf{n}, t]$ code, denoted as

$$\mathcal{E} := \mathcal{R}_{q^m}(\mathbf{E}), \quad (5)$$

which we refer to as the *error code*.

Let $\mathbf{G}_\mathcal{E} \in \mathbb{F}_{q^m}^{t \times n}$ denote the generator matrix of \mathcal{E} . Note that we can decompose $\mathbf{G}_\mathcal{E}$ as

$$\mathbf{G}_\mathcal{E} = \mathbf{A}_\mathcal{E}\mathbf{B}, \quad (6)$$

where $\mathbf{A}_\mathcal{E} = [\mathbf{A}_\mathcal{E}^{(1)} \mid \dots \mid \mathbf{A}_\mathcal{E}^{(\ell)}] \in \mathbb{F}_{q^m}^{t \times t}$ with $\text{rk}_{q^m}(\mathbf{A}_\mathcal{E}) = t$ and \mathbf{B} is the same matrix as defined in the error decomposition (2) and (3). Each block $\mathbf{A}_\mathcal{E}^{(i)}$ is a matrix of size $t \times t_i$. The rank profile \mathbf{t} determines the ranks of the individual blocks $\mathbf{A}_\mathcal{E}^{(i)}$, i.e., $\text{rk}_{q^m}(\mathbf{A}_\mathcal{E}^{(i)}) = t_i$.

It follows directly from the definition (5) of the error code, that

$$\text{supp}_{\Sigma R}(\mathcal{E}) = \text{supp}_{\Sigma R}(\mathbf{E}).$$

Because of this property, we say that the error code \mathcal{E} is *support-restricted by the row support of \mathbf{E}* with $\mathcal{E} \subset \mathbb{F}_q^n$.

Let us now consider the parity-check matrix of the error code \mathcal{E} , denoted by $\mathbf{H}_{\mathcal{E}} \in \mathbb{F}_{q^m}^{(n-t) \times n}$. By definition of the parity-check matrix, we have $\mathbf{G}_{\mathcal{E}} \mathbf{H}_{\mathcal{E}}^{\top} = \mathbf{0}$.

Lemma 2 *Let $\mathbf{H}_{\mathcal{E}} = [\mathbf{H}_{\mathcal{E}}^{(1)} \mid \dots \mid \mathbf{H}_{\mathcal{E}}^{(\ell)}] \in \mathbb{F}_{q^m}^{(n-t) \times n}$ be the parity-check matrix of the $[\mathbf{n}, t]$ error code \mathcal{E} with length partition \mathbf{n} . Then, we have*

$$\text{supp}_{\Sigma R}(\mathbf{H}_{\mathcal{E}}) = \text{supp}_{\Sigma R}^{\perp}(\mathbf{E}).$$

Proof: Since $\mathbf{H}_{\mathcal{E}}$ is a parity-check matrix of \mathcal{E} , we have $\text{rk}_{q^m}(\mathbf{H}_{\mathcal{E}}) = n - t$. With respect to the sum-rank metric, we can partition the parity-check matrix of the error code as

$$\mathbf{H}_{\mathcal{E}} = [\mathbf{H}_{\mathcal{E}}^{(1)} \mid \dots \mid \mathbf{H}_{\mathcal{E}}^{(\ell)}] \quad (7)$$

such that $\mathbf{H}_{\mathcal{E}}^{(i)} \in \mathbb{F}_{q^m}^{(n-t) \times n_i}$ for all $i \in \{1, \dots, \ell\}$.

To satisfy the check equations, we must have

$$\mathbf{G}_{\mathcal{E}} \mathbf{H}_{\mathcal{E}}^{\top} = \mathbf{0} \Leftrightarrow (\mathbf{A}_{\mathcal{E}} \mathbf{B}) \mathbf{H}_{\mathcal{E}}^{\top} = \mathbf{0} \Leftrightarrow \mathbf{B} \mathbf{H}_{\mathcal{E}}^{\top} = \mathbf{0}.$$

From (7) and the block-diagonal structure of \mathbf{B} (see (3)), it follows that

$$\mathbf{B}^{(i)} \mathbf{H}_{\mathcal{E}}^{(i)\top} = \mathbf{0} \quad \forall i \in \{1, \dots, \ell\}.$$

By the rank-nullity theorem and since $\mathbf{B}^{(i)}$ is over \mathbb{F}_q , we have $\dim(\mathcal{R}_q(\mathbf{H}_{\mathcal{E}}^{(i)})) \leq n_i - t_i$ for all $i \in \{1, \dots, \ell\}$. However, since $\mathbf{H}_{\mathcal{E}}$ must have $n - t$ many \mathbb{F}_{q^m} -linearly independent rows and $\sum_{i=1}^{\ell} n_i - t_i = n - t$, we conclude that $\dim(\mathcal{R}_q(\mathbf{H}_{\mathcal{E}}^{(i)})) = n_i - t_i$, and hence

$$\mathcal{R}_q(\mathbf{H}_{\mathcal{E}}^{(i)}) = \mathcal{R}_q(\mathbf{B}^{(i)})^{\top} \quad \forall i \in \{1, \dots, \ell\}.$$

By the definition of the sum-rank support, this concludes the proof. \blacksquare

Theorem 1 *Let \mathcal{C} be an \mathbb{F}_{q^m} -linear $[\mathbf{n}, k]$ sum-rank-metric code with generator matrix $\mathbf{G} \in \mathbb{F}_{q^m}^{k \times n}$, parity-check matrix $\mathbf{H} \in \mathbb{F}_{q^m}^{(n-k) \times n}$, and minimum sum-rank distance d . Let $\mathbf{E} = \mathbf{A}\mathbf{B} \in \mathbb{F}_{q^m}^{s \times n}$ be a matrix with $\mathbf{A} \in \mathbb{F}_{q^m}^{s \times t}$, $\mathbf{B} \in \mathbb{F}_q^{t \times n}$, $\text{rk}_{q^m}(\mathbf{E}) = t$, and $\text{wt}_{\Sigma R}^{(n)}(\mathbf{E}) = t$. Let $t \leq n - k - 1$ and suppose that*

$$\text{rk}_{q^m} \left(\mathbf{H} \begin{bmatrix} \mathbf{B} \\ \mathbf{b} \end{bmatrix}^{\top} \right) = t + 1 \quad \forall \mathbf{b} \in \mathbb{F}_q^n \setminus \text{supp}_{\Sigma R}(\mathbf{E}) \text{ s.t. } \text{wt}_{\Sigma R}^{(n)}(\mathbf{b}) = 1. \quad (8)$$

Further, denote by $\mathbf{G}_\mathcal{E} \in \mathbb{F}_{q^m}^{t \times n}$ the generator matrix of the error code $\mathcal{E} := \mathcal{R}_{q^m}(\mathbf{E})$. Consider the \mathbb{F}_{q^m} -linear code $\mathcal{S} = \mathcal{E} + \mathcal{C}$ defined as

$$\mathcal{S} := \mathcal{R}_{q^m}(\mathbf{G}_\mathcal{S}) \quad (9)$$

with generator matrix

$$\mathbf{G}_\mathcal{S} := \begin{bmatrix} \mathbf{G} \\ \mathbf{E} \end{bmatrix}.$$

Then, for any valid parity-check matrix $\mathbf{H}_\mathcal{S} \in \mathbb{F}_{q^m}^{(n-k-t) \times n}$ of the \mathbb{F}_{q^m} -linear $[\mathbf{n}, k+t]$ sum-rank-metric code \mathcal{S} , we have

$$\text{supp}_{\Sigma R}^\perp(\mathbf{H}_\mathcal{S}) = \text{supp}_{\Sigma R}(\mathbf{E}). \quad (10)$$

Proof: First, partition $\mathbf{H}_\mathcal{S}$ into blocks according to the length partition \mathbf{n} , i.e.,

$$\mathbf{H}_\mathcal{S} = \left[\mathbf{H}_\mathcal{S}^{(1)} \mid \cdots \mid \mathbf{H}_\mathcal{S}^{(\ell)} \right]$$

with $\mathbf{H}_\mathcal{S}^{(i)} \in \mathbb{F}_{q^m}^{(n-k-t) \times n_i}$ for all $i \in \{1, \dots, \ell\}$. We want to show that $\text{supp}_{\Sigma R}^\perp(\mathbf{H}_\mathcal{S}) = \text{supp}_{\Sigma R}(\mathbf{E})$.

By the definition of the support for the sum-rank metric, this means that we need to show that

$$\text{supp}_R^\perp(\mathbf{H}_\mathcal{S}^{(i)}) = \text{supp}_R(\mathbf{E}^{(i)}) = \mathcal{R}_q(\mathbf{B}^{(i)}) \quad \forall i \in \{1, \dots, \ell\}.$$

Define $\mu_i := \text{rk}_q(\mathbf{H}_\mathcal{S}^{(i)})$ for all $i \in \{1, \dots, \ell\}$. Then, $\mathbf{H}_\mathcal{S}^{(i)}$ can be decomposed as

$$\mathbf{H}_\mathcal{S}^{(i)} = \mathbf{C}_\mathcal{S}^{(i)} \mathbf{D}_\mathcal{S}^{(i)}$$

with $\mathbf{C}_\mathcal{S}^{(i)} \in \mathbb{F}_{q^m}^{(n-k-t) \times \mu_i}$, $\mathbf{D}_\mathcal{S}^{(i)} \in \mathbb{F}_q^{\mu_i \times n_i}$, and $\text{rk}_q(\mathbf{C}_\mathcal{S}^{(i)}) = \text{rk}_q(\mathbf{D}_\mathcal{S}^{(i)}) = \mu_i$.

Recall from the definition of the sum-rank support (4) and its dual support (10) that we have

$$\text{supp}_{\Sigma R}^\perp(\mathbf{H}_\mathcal{S}) = \mathcal{R}_q(\mathbf{D}_\mathcal{S}^{(1)})^\perp \times \cdots \times \mathcal{R}_q(\mathbf{D}_\mathcal{S}^{(\ell)})^\perp$$

and

$$\text{supp}_{\Sigma R}(\mathbf{E}) = \mathcal{R}_q(\mathbf{B}^{(1)}) \times \cdots \times \mathcal{R}_q(\mathbf{B}^{(\ell)}),$$

respectively. The goal is to show that $\mathcal{R}_q(\mathbf{D}_\mathcal{S}^{(i)})^\perp = \mathcal{R}_q(\mathbf{B}^{(i)})$ for all $i \in \{1, \dots, \ell\}$, which is equivalent to proving $\mathcal{R}_q(\mathbf{D}_\mathcal{S}^{(i)}) = \mathcal{R}_q(\mathbf{B}^{(i)})^\perp$. This will be achieved in two steps:

- 1) Show that $\mathcal{R}_q(\mathbf{D}_\mathcal{S}^{(i)}) \subseteq \mathcal{R}_q(\mathbf{B}^{(i)})^\perp$ for all $i \in \{1, \dots, \ell\}$.

- 2) Demonstrate that $\mu_i < \dim(\mathcal{R}_q(\mathbf{B}^{(i)})^\perp) = n_i - t_i$ is not possible for any $i \in \{1, \dots, \ell\}$, implying $\mu_i = n_i - t_i$ and hence $\mathcal{R}_q(\mathbf{D}_S^{(i)}) = \mathcal{R}_q(\mathbf{B}^{(i)})^\perp$ for all $i \in \{1, \dots, \ell\}$.

Step 1: Proving $\mathcal{R}_q(\mathbf{D}_S^{(i)}) \subseteq \mathcal{R}_q(\mathbf{B}^{(i)})^\perp$ for all $i \in \{1, \dots, \ell\}$.

To prove $\mathcal{R}_q(\mathbf{D}_S^{(i)}) \subseteq \mathcal{R}_q(\mathbf{B}^{(i)})^\perp$, we instead show that $\mathcal{R}_q(\mathbf{B}^{(i)}) \subseteq \mathcal{R}_q(\mathbf{D}_S^{(i)})^\perp$. By definition, \mathbf{H}_S is a parity-check matrix for $\mathcal{S} = \mathcal{E} + \mathcal{C}$. Thus,

$$\mathbf{H}_S \mathbf{G}_\mathcal{E}^\top = \mathbf{0} \quad \Leftrightarrow \quad \mathbf{H}_S \mathbf{B}^\top \mathbf{A}_\mathcal{E}^\top = \mathbf{0}$$

where $\mathbf{G}_\mathcal{E}$ is the generator matrix of the error code as defined in (6). Since $\mathbf{A}_\mathcal{E} \in \mathbb{F}_{q^m}^{t \times m}$ is non-singular, we have that

$$\mathbf{H}_S \mathbf{B}^\top = \mathbf{0} \Leftrightarrow \mathbf{H}_S^{(i)} \mathbf{B}^{(i)\top} = \mathbf{0} \quad \forall i \in \{1, \dots, \ell\}. \quad (11)$$

This implies that all rows of $\mathbf{B}^{(i)}$ are in the \mathbb{F}_{q^m} -right kernel of $\mathbf{H}_S^{(i)}$, and since $\mathbf{B}^{(i)}$ is over \mathbb{F}_q , we have that $\mathcal{R}_q(\mathbf{B}^{(i)}) \subseteq \mathcal{R}_q(\mathbf{D}_S^{(i)})^\perp$. Consequently, $\mathcal{R}_q(\mathbf{D}_S^{(i)}) \subseteq \mathcal{R}_q(\mathbf{B}^{(i)})^\perp$.

Step 2: Showing that $\mu_i < \dim(\mathcal{R}_q(\mathbf{B}^{(i)})^\perp) = n_i - t_i$ is impossible for any $i \in \{1, \dots, \ell\}$. Since $\mathcal{R}_q(\mathbf{D}_S^{(i)}) \subseteq \mathcal{R}_q(\mathbf{B}^{(i)})^\perp$, $\mu_i > n_i - t_i$ is not possible for any $i \in \{1, \dots, \ell\}$. Assume that $\mu_{i'} < n_{i'} - t_{i'}$ for at least one $i' \in \{1, \dots, \ell\}$, i.e., let $\mu_{i'} = n_{i'} - t_{i'} - \delta \in \mathbb{Z}$ with $\delta > 0$. Without loss of generality, set $i' = \ell$.

Given that $\text{rk}_q(\mathbf{D}_S^{(\ell)}) = n_\ell - t_\ell - \delta$, there exists a full-rank matrix $\mathbf{Q}^{(\ell)} \in \mathbb{F}_q^{n_\ell \times n_\ell}$ that allows us to bring $\mathbf{D}_S^{(\ell)}$ into column-echelon form. Hence,

$$\mathbf{D}_S^{(\ell)} \mathbf{Q}^{(\ell)} = \left[\underbrace{\mathbf{0}}_{\in \mathbb{F}_q^{(n_\ell - t_\ell - \delta) \times (t_\ell + \delta)}} \mid \tilde{\mathbf{D}}_S^{(\ell)} \right]$$

where $\tilde{\mathbf{D}}_S^{(\ell)} \in \mathbb{F}_q^{(n_\ell - t_\ell - \delta) \times (n_\ell - t_\ell - \delta)}$ with $\text{rk}_q(\tilde{\mathbf{D}}_S^{(\ell)}) = n_\ell - t_\ell - \delta$.

Further, let

$$\mathbf{Q}^{(\ell)} = [\mathbf{Q}_1^{(\ell)} \mid \mathbf{Q}_2^{(\ell)}]$$

with $\mathbf{Q}_1^{(\ell)} \in \mathbb{F}_q^{n_\ell \times (t_\ell + \delta)}$ and $\mathbf{Q}_2^{(\ell)} \in \mathbb{F}_q^{n_\ell \times (n_\ell - t_\ell - \delta)}$. Since $\mathbf{Q}^{(\ell)}$ is full-rank, we have that $\mathbf{Q}_1^{(\ell)}$ is full-rank too, i.e., $\text{rk}_q(\mathbf{Q}_1^{(\ell)}) = t_\ell + \delta$. Thus,

$$\mathbf{D}_S^{(\ell)} \mathbf{Q}_1^{(\ell)} = \mathbf{0}. \quad (12)$$

That means we can multiply (12) from the right with some full-rank transformation matrix

$\mathbf{T} \in \mathbb{F}_q^{(t_\ell+\delta) \times (t_\ell+\delta)}$ such that

$$\mathbf{D}_S^{(\ell)} \underbrace{\left[\mathbf{B}^{(\ell)\top} \mid \tilde{\mathbf{B}}^{(\ell)\top} \right]}_{=\mathbf{Q}_1^{(\ell)\top} \mathbf{T}} = \mathbf{0}. \quad (13)$$

Define the following block-diagonal matrix

$$\mathbf{Q} = \begin{bmatrix} \mathbf{B}^{(1)} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{B}^{(2)} & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{B}^{(\ell)} \\ \mathbf{0} & \mathbf{0} & \dots & \tilde{\mathbf{B}}^{(\ell)} \end{bmatrix} \in \mathbb{F}_q^{(t+\delta) \times n}.$$

Then we have that

$$\mathbf{D}_S \mathbf{Q}^\top = \mathbf{0} \quad (14)$$

since $\mathbf{D}_S^{(i)} \mathbf{B}^{(i)\top} = \mathbf{0}$ for $i \in \{1, \dots, \ell - 1\}$ and by assumption (13), $\mathbf{D}_S^{(\ell)} \left[\mathbf{B}^{(\ell)\top} \mid \tilde{\mathbf{B}}^{(\ell)\top} \right] = \mathbf{0}$.

Now, without loss of generality, let $\delta = 1$. By the decoding condition (8), we have that

$$\text{rk}_{q^m}(\mathbf{H}\mathbf{Q}^\top) = t + 1$$

must hold. Thus, there exists a vector $\mathbf{g} \in \mathcal{R}_{q^m}(\mathbf{H})$ such that

$$\mathbf{g}\mathbf{Q}^\top = \begin{bmatrix} 0 & \dots & 0 & g_{t+1} \end{bmatrix} \neq \begin{bmatrix} 0 & \dots & 0 \end{bmatrix} \in \mathbb{F}_{q^m}^{t+1}.$$

Since the first t leftmost positions of $\mathbf{g}\mathbf{Q}^\top$ are zero, by (11) and the fact that the matrix formed by the t leftmost columns in \mathbf{Q}^\top forms a basis of all $\mathcal{R}_q(\mathbf{B}^{(i)})^\perp$ for all $i \in \{1, \dots, \ell\}$, which are also bases for $\mathcal{R}_{q^m}(\mathbf{B}^{(i)})^\perp$ for all $i \in \{1, \dots, \ell\}$, this implies that $\mathbf{g} \in \mathcal{R}_{q^m}(\mathbf{B})^\perp$.

Also recall that \mathbf{H}_S fulfills the parity-check constraints for both codes simultaneously: the error code \mathcal{E} and the component code \mathcal{C} . That means that

$$\begin{aligned} \mathcal{S} = \mathcal{C} + \mathcal{E} &\Leftrightarrow \mathcal{S}^\perp = \mathcal{C}^\perp \cap \mathcal{E}^\perp \\ &\Leftrightarrow \mathcal{R}_{q^m}(\mathbf{H}_S) = \mathcal{R}_{q^m}(\mathbf{H}) \cap \mathcal{R}_{q^m}(\mathbf{B})^\perp. \end{aligned}$$

Since for this specific \mathbf{g} we have that $\mathbf{g} \in \mathcal{R}_{q^m}(\mathbf{H})$ and also $\mathbf{g} \in \mathcal{R}_{q^m}(\mathbf{B})^\perp$, it follows that $\mathbf{g} \in \mathcal{R}_{q^m}(\mathbf{H}_S)$. Expanding \mathbf{g} over \mathbb{F}_q also implies that there exists a vector $\mathbf{g}' \in \mathcal{R}_q(\mathbf{H}_S) = \mathcal{R}_q(\mathbf{D}_S)$

such that

$$\mathbf{g}'\mathbf{Q}^\top = \begin{bmatrix} 0 & \dots & 0 & g'_{t+1} \end{bmatrix} \neq \begin{bmatrix} 0 & \dots & 0 \end{bmatrix} \in \mathbb{F}_q^{t+1}.$$

But by (14), for all $\mathbf{g}' \in \mathcal{R}_q(\mathbf{D}_S)$ we need to have that

$$\mathbf{g}'\mathbf{Q}^\top = \begin{bmatrix} 0 & \dots & 0 & 0 \end{bmatrix} \in \mathbb{F}_q^{t+1}.$$

This constitutes a contradiction, and thus $\mu_\ell < n_\ell - t_\ell$ is not possible. This also holds for any other $i' \neq \ell$, and therefore $\mu_i < n_i - t_i$ is not possible for any $i \in \{1, \dots, \ell\}$.

When $\delta = 1$, we obtain one additional zero column in $\mathbf{g}'\mathbf{Q}^\top$. Similarly, when $\delta = 2$, we get two additional zero columns. Since a contradiction arises for $\delta = 1$, it follows that the assumption cannot hold for any $\delta > 1$ as well. For $\delta = 0$, we do not get a contradiction, and thus $\mu_i = n_i - t_i$ for all $i \in \{1, \dots, \ell\}$ is the only valid option.

This proves that $\mathcal{R}_q(\mathbf{D}_S^{(i)}) = \mathcal{R}_q(\mathbf{B}^{(i)})^\perp$ for all $i \in \{1, \dots, \ell\}$, and therefore $\mathcal{R}_q(\mathbf{D}_S^{(i)})^\perp = \mathcal{R}_q(\mathbf{B}^{(i)})$ for all $i \in \{1, \dots, \ell\}$, hence $\text{supp}_{\Sigma R}^\perp(\mathbf{H}_S) = \text{supp}_{\Sigma R}(\mathbf{E})$. ■

Remark 2 *Due to the properties of the error code and the relationship $\mathbf{Y} = \mathbf{C} + \mathbf{E}$, the following row spaces over \mathbb{F}_{q^m} are the same*

$$\mathcal{R}_{q^m} \left(\begin{bmatrix} \mathbf{G} \\ \mathbf{G}_\mathcal{E} \end{bmatrix} \right) = \mathcal{R}_{q^m} \left(\begin{bmatrix} \mathbf{G} \\ \mathbf{E} \end{bmatrix} \right) = \mathcal{R}_{q^m} \left(\begin{bmatrix} \mathbf{G} \\ \mathbf{Y} \end{bmatrix} \right).$$

Thus, the rows of all three matrices are generating sets for the code $\mathcal{S} = \mathcal{C} + \mathcal{E}$.

Note, that a parity-check matrix \mathbf{H}_S for \mathcal{S} can be obtained by stacking \mathbf{G}_S with \mathbf{Y} and then performing Gaussian elimination. This fact leads to the following observation for very high interleaving orders.

Remark 3 *The error-code perspective on the Metzner–Kapturowski-like algorithm allows for new insights for very high-order interleaving orders, i.e., for $s \geq k + t$. In particular, if the rows of the transmitted codeword \mathbf{C} form a generating set for \mathcal{C} , i.e., if $\text{rk}_{q^m}(\mathbf{C}) = k$ and the error matrix \mathbf{E} fulfills the full-rank condition, we have that $\text{rk}_{q^m}(\mathbf{Y}) = k + t$ and the rows of \mathbf{Y} form a generating set for $\mathcal{S} = \mathcal{C} + \mathcal{E}$.*

This allows us to compute a parity-check matrix \mathbf{H}_S for \mathcal{S} directly from the received matrix \mathbf{Y} as a basis for the right \mathbb{F}_{q^m} -kernel of \mathbf{Y} and recover the support of the error as $\text{supp}_{\Sigma R}^\perp(\mathbf{H}_S) =$

$\text{supp}_{\Sigma R}(\mathbf{E})$ (see (10) in Theorem 1). Remarkably, we can recover the support of the error \mathbf{E} without knowing the codes \mathcal{C} and \mathcal{S} .

This observation could be relevant for cryptosystems which rely on (secret) very high-order interleaved codes, since the knowledge of the error support could reduce the security level significantly, see e.g. [16].

We now present a theorem that establishes a direct connection between the syndrome matrix \mathbf{S} and the parity-check matrix \mathbf{H}_S of the sum code $\mathcal{S} = \mathcal{C} + \mathcal{E}$. This theorem provides a straightforward method to compute \mathbf{H}_S from \mathbf{S} as used in the existing Metzner–Kapturowski variants for the Hamming and the rank metric.

Theorem 2 *Let $\mathcal{IC}[s; \mathbf{n}, k, d]$ be an \mathbb{F}_{q^m} -linear interleaved sum-rank-metric code with component code \mathcal{C} , which has parity-check matrix $\mathbf{H} \in \mathbb{F}_{q^m}^{(n-k) \times n}$. Let $\mathbf{E} \in \mathbb{F}_{q^m}^{s \times n}$ be an error matrix with $\text{rk}_{q^m}(\mathbf{E}) = t$ and $\text{wt}_{\Sigma R}^{(n)}(\mathbf{E}) = t \leq n - k - 1$ and let \mathcal{E} be the error code spanned by the rows of \mathbf{E} . The received word is $\mathbf{Y} = \mathbf{C} + \mathbf{E}$, where $\mathbf{C} \in \mathcal{IC}$. The syndrome matrix is $\mathbf{S} = \mathbf{H}\mathbf{Y}^\top = \mathbf{H}\mathbf{E}^\top$, where $\mathbf{S} \in \mathbb{F}_{q^m}^{(n-k) \times s}$.*

Let $\mathbf{P} \in \mathbb{F}_{q^m}^{(n-k) \times (n-k)}$ be a full-rank matrix such that $\mathbf{P}\mathbf{S}$ is in row-echelon form, i.e.,

$$\mathbf{P}\mathbf{S} = \begin{bmatrix} \mathbf{S}' \\ \mathbf{0} \end{bmatrix} \longrightarrow \mathbf{P}\mathbf{H} = \begin{bmatrix} \mathbf{H}' \\ \mathbf{H}_S \end{bmatrix}$$

where $\mathbf{S}' \in \mathbb{F}_{q^m}^{t \times s}$, $\mathbf{H}' \in \mathbb{F}_{q^m}^{t \times n}$ then $\mathbf{H}_S \in \mathbb{F}_{q^m}^{(n-k-t) \times n}$ is a parity-check matrix for the sum-rank-metric code $\mathcal{S} = \mathcal{E} + \mathcal{C}$ as defined in (9).

Proof: Since \mathbf{P} is invertible, multiplying both sides of $\mathbf{S} = \mathbf{H}\mathbf{E}^\top$ by \mathbf{P} yields

$$\mathbf{P}\mathbf{S} = \mathbf{P}\mathbf{H}\mathbf{E}^\top.$$

As \mathbf{H} has full row rank $\text{rk}_{q^m}(\mathbf{H}) = n - k$ and $\text{rk}_{q^m}(\mathbf{E}) = t$, we have

$$\text{rk}_{q^m}(\mathbf{S}) = \text{rk}_{q^m}(\mathbf{H}\mathbf{E}^\top) = \min\{\text{rk}_{q^m}(\mathbf{H}), \text{rk}_{q^m}(\mathbf{E})\} = \min\{n - k, t\} = t.$$

By the rank-nullity theorem, $\text{rk}_{q^m}(\mathbf{P}\mathbf{S}) = \text{rk}_{q^m}(\mathbf{S}) = t$, so $\mathbf{P}\mathbf{S}$ has t non-zero rows. As $\mathbf{P}\mathbf{S}$ is in row-echelon form, we can write

$$\mathbf{P}\mathbf{S} = \begin{bmatrix} \mathbf{S}' \\ \mathbf{0} \end{bmatrix},$$

where $\mathbf{S}' \in \mathbb{F}_{q^m}^{t \times s}$ has full row rank.

Partitioning $\mathbf{P}\mathbf{H}$ conformally with $\mathbf{P}\mathbf{S}$, we have

$$\mathbf{P}\mathbf{H} = \begin{bmatrix} \mathbf{H}' \\ \mathbf{H}_S \end{bmatrix},$$

where $\mathbf{H}' \in \mathbb{F}_{q^m}^{t \times n}$ and $\mathbf{H}_S \in \mathbb{F}_{q^m}^{(n-k-t) \times n}$. Since $\mathbf{P}\mathbf{H}\mathbf{E}^\top = \mathbf{P}\mathbf{S}$, we have

$$\begin{bmatrix} \mathbf{H}' \\ \mathbf{H}_S \end{bmatrix} \mathbf{E}^\top = \begin{bmatrix} \mathbf{S}' \\ \mathbf{0} \end{bmatrix},$$

which implies $\mathbf{H}_S \mathbf{E}^\top = \mathbf{0}$. As the rows of \mathbf{E} span \mathcal{E} , this means \mathbf{H}_S satisfies the parity-check equations for \mathcal{E} . By construction, \mathbf{H}_S also satisfies the parity-check equations for \mathcal{C} , as it is a submatrix of $\mathbf{P}\mathbf{H}$. And since \mathbf{H}_S has $n - k - t$ rows and is of full-rank, it is a parity-check matrix for the sum-rank-metric code \mathcal{S} defined in (9), which contains both \mathcal{C} and \mathcal{E} . ■

B. A Metzner–Kapturowski-like Decoding Algorithm

Using Theorem 1 and Theorem 2, 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 \mathbf{H}_S is computed from the syndrome matrix \mathbf{S} , the rank support of each block can be recovered independently using the results from Theorem 1. This corresponds to finding a basis in the form of a matrix $\mathbf{B}^{(i)} \in \mathbb{F}_q^{t_i \times n_i}$ such that $\text{ext}(\mathbf{H}_S^{(i)})(\mathbf{B}^{(i)})^\top = \mathbf{0}$ for all $i \in \{1, \dots, \ell\}$, where t_i is determined by the rank-nullity theorem as $t_i = n_i - \text{rk}_q(\mathbf{H}_S^{(i)})$ according to (10).

Theorem 3 *Let \mathbf{C} be a codeword of an s -interleaved sum-rank-metric code $\mathcal{IC}[s; \mathbf{n}, k, d]$ and let \mathbf{H} be the parity-check matrix of the corresponding constituent code \mathcal{C} . Furthermore, let $\mathbf{E} \in \mathbb{F}_{q^m}^{s \times n}$ be an error matrix of sum-rank weight $\text{wt}_{\Sigma R}^{(n)}(\mathbf{E}) = t$ that fulfills $t \leq s$ (high-order condition) and $\text{rk}_{q^m}(\mathbf{E}) = t$ (full-rank condition). Let \mathbf{B} be a basis of the \mathbb{F}_q -row space of \mathbf{E} . If (8) holds, then \mathbf{C} can be uniquely recovered from the received word $\mathbf{Y} = \mathbf{C} + \mathbf{E}$ using Algorithm 1 in a time complexity equivalent to*

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

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

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

Input : Parity-check matrix \mathbf{H} of \mathcal{C} , Received word $\mathbf{Y} = \mathbf{C} + \mathbf{E}$ with

$$\mathbf{C} \in \mathcal{IC}[s; \mathbf{n}, k, d] \text{ and } \text{wt}_{\Sigma R}^{(n)}(\mathbf{E}) = \text{rk}_{q^m}(\mathbf{E}) = t$$

Output: Transmitted codeword \mathbf{C}

- 1 $\mathbf{S} \leftarrow \mathbf{H}\mathbf{Y}^\top \in \mathbb{F}_{q^m}^{(n-k) \times s}$
 - 2 Compute $\mathbf{P} \in \mathbb{F}_{q^m}^{(n-k) \times (n-k)}$ s.t. $\mathbf{P}\mathbf{S} = \text{REF}(\mathbf{S})$
 - 3 $\mathbf{H}_S = \left[\mathbf{H}_S^{(1)} \mid \mathbf{H}_S^{(2)} \mid \dots \mid \mathbf{H}_S^{(\ell)} \right] \leftarrow (\mathbf{P}\mathbf{H})_{[t+1:n-k], [1:n]} \in \mathbb{F}_{q^m}^{(n-t-k) \times n}$
 - 4 **for** $i \in \{1, \dots, \ell\}$ **do**
 - 5 $\left[\right.$ Compute $\mathbf{B}^{(i)} \in \mathbb{F}_q^{t_i \times n_i}$ s.t. $\text{ext}(\mathbf{H}_S^{(i)})(\mathbf{B}^{(i)})^\top = \mathbf{0}$, where $t_i = n_i - \text{rk}_q(\mathbf{H}_S^{(i)})$
 - 6 $\mathbf{B} \leftarrow \text{diag}(\mathbf{B}^{(1)}, \mathbf{B}^{(2)}, \dots, \mathbf{B}^{(\ell)}) \in \mathbb{F}_q^{t \times n}$
 - 7 Compute $\mathbf{A} \in \mathbb{F}_{q^m}^{s \times t}$ s.t. $(\mathbf{H}\mathbf{B}^\top)\mathbf{A}^\top = \mathbf{S}$
 - 8 $\mathbf{C} \leftarrow \mathbf{Y} - \mathbf{A}\mathbf{B} \in \mathbb{F}_{q^m}^{s \times n}$
 - 9 **return** \mathbf{C}
-

Proof: Lemma 1 states that the error matrix \mathbf{E} can be factored as $\mathbf{E} = \mathbf{A}\mathbf{B}$. The decoding procedure in Algorithm 1 starts by finding a basis \mathbf{B} of the error support $\text{supp}_{\Sigma R}(\mathbf{E})$ and then uses erasure decoding with respect to Lemma 1 to recover \mathbf{A} . The matrix \mathbf{B} is computed by transforming \mathbf{S} into row-echelon form using a transformation matrix \mathbf{P} (see Line 2). In Line 3, \mathbf{H}_S is obtained by choosing the last $n - k - t$ rows of $\mathbf{P}\mathbf{H}$. According to Theorem 2, the matrix \mathbf{H}_S serves as a parity-check matrix for both the error code \mathcal{E} associated with the error matrix \mathbf{E} and the component code \mathcal{C} . Then using Theorem 1 for each block (see Line 5) we find a matrix $\mathbf{B}^{(i)}$ whose rows form a basis for $\mathcal{R}_q\left(\text{ext}(\mathbf{H}_S^{(i)})\right)^\top$ and therefore a basis for $\text{supp}_R(\mathbf{E}^{(i)})$ for all $i \in \{1, \dots, \ell\}$. The matrix \mathbf{B} is the block-diagonal matrix formed by $\mathbf{B}^{(i)}$ (cf. (3) and see Line 6) for $i \in \{1, \dots, \ell\}$. Finally, \mathbf{A} can be computed from \mathbf{B} and \mathbf{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 $\mathbf{S} = \mathbf{H}\mathbf{Y}^\top$ can be computed in at most $O(n^2s)$ operations in \mathbb{F}_{q^m} .
- Line 2: The transformation of $[\mathbf{S} \mid \mathbf{I}]$ into row-echelon form requires

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

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

- Line 3: The product $(\mathbf{PH})_{[t+1:n-k],[1:n]}$ can be computed requiring at most

$$O(n(n-k-t)(n-k)) \subseteq O(n^3)$$

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

- Line 5: The transformation of $[\text{ext}(\mathbf{H}_S^{(i)})^\top \mid \mathbf{I}^\top]^\top$ into column-echelon form requires $O(n_i^2((n-k-t)m+n_i))$ operations in \mathbb{F}_q per block. Overall we get

$$O\left(\sum_{i=1}^{\ell} n_i^2((n-k-t)m+n_i)\right) \subseteq O(n^3m)$$

operations in \mathbb{F}_q since we have that $O\left(\sum_{i=1}^{\ell} n_i^2\right) \subseteq O(n^2)$.

- Line 7: According to Lemma 1, this step can be done in $O((n-k)^3m^2)$ operations over \mathbb{F}_q .
- Line 8: The product $\mathbf{AB} = [\mathbf{A}^{(1)}\mathbf{B}^{(1)} \mid \mathbf{A}^{(2)}\mathbf{B}^{(2)} \mid \dots \mid \mathbf{A}^{(\ell)}\mathbf{B}^{(\ell)}]$ can be computed in $O\left(\sum_{i=1}^{\ell} st_i n_i\right) \subseteq O(sn^2)$ and the difference of $\mathbf{Y} - \mathbf{AB}$ 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 $O(n^3m^2)$ and their execution complexity can be bounded by $O(n^3)$ operations in \mathbb{F}_{q^m} (see [17]).

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

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.

IV. FURTHER RESULTS AND REMARKS

A. Probabilistic Decoding for Uniform Random Errors

In practical settings, the full-rank condition may not always hold. Therefore, we consider the performance of the decoder when the error is drawn uniformly at random from the set of all error matrices of a given sum-rank weight t . We then derive an upper bound on the error probability, which, for fixed code parameters, decays exponentially with respect to the difference between the error weight t and the interleaving order s .

Note that we still require the high-order condition, i.e., $s \geq t$. Otherwise, no error can possibly satisfy the full-rank condition since

$$\text{rk}_{\mathbb{F}_q^m}(\mathbf{E}) \leq \sum_{i=1}^{\ell} \text{rk}_{\mathbb{F}_q^m}(\mathbf{E}^{(i)}) \leq \sum_{i=1}^{\ell} \text{rk}_q(\mathbf{E}^{(i)}) = \sum_{i=1}^{\ell} t_i = t$$

holds, and \mathbf{E} has size $s \times n$ (with $s \leq n$).

For the sake of simplicity in the analysis, we focus on the case where the length partition $\mathbf{n} = [n_1, \dots, n_\ell]$ has constant block lengths, i.e., there exists a positive integer η such that $n_i = \eta$ for all $i \in \{1, \dots, \ell\}$.

We introduce the following sets, which are integral to the proofs of the forthcoming theorems in this section.

First define μ as the maximum possible \mathbb{F}_q -rank of each block of the error matrix, given by

$$\mu := \min\{sm, \eta\}. \quad (15)$$

Next, we define the set of all possible rank profiles $\mathbf{t} = [t_1, \dots, t_\ell]$ for any error matrix with ℓ blocks and sum-rank weight t , where each component t_i is bounded by μ as

$$\mathcal{T}_{t, \ell, \mu} := \left\{ \mathbf{t} \in \{0, \dots, \mu\}^\ell : \sum_{i=1}^{\ell} t_i = t \right\}.$$

This set will be used to enumerate all possible rank profiles.

For a given length partition \mathbf{n} , we define the set of all error matrices with sum-rank weight t as follows

$$\mathcal{E}_t^{(\mathbf{n})} := \left\{ \mathbf{E} = [\mathbf{E}^{(1)} \mid \dots \mid \mathbf{E}^{(\ell)}] \in \mathbb{F}_{q^m}^{s \times n} : \text{wt}_{\Sigma R}^{(\mathbf{n})}(\mathbf{E}) = \sum_{i=1}^{\ell} \text{rk}_q(\mathbf{E}^{(i)}) = t \right\}.$$

This set contains all possible error matrices with the specified sum-rank weight t and length partition \mathbf{n} . For a fixed rank profile we define

$$\mathcal{E}_t^{(\mathbf{n})} := \{ \mathbf{E} = [\mathbf{E}^{(1)} \mid \dots \mid \mathbf{E}^{(\ell)}] \in \mathbb{F}_{q^m}^{s \times n} : \text{rk}_q(\mathbf{E}^{(i)}) = t_i \}.$$

and from (2) we have that we can decompose the error into $\mathbf{E} = \mathbf{A}\mathbf{B}$ with $\mathbf{A} \in \mathbb{F}_{q^m}^{s \times t}$ and $\mathbf{B} \in \mathbb{F}_q^{t \times n}$ with \mathbf{A} and \mathbf{B} both of full-rank. Let us define the set of all possible matrices \mathbf{A}

$$\mathcal{A}_t := \left\{ \mathbf{A} \in \mathbb{F}_{q^m}^{s \times t} : \text{wt}_{\Sigma R}^{(t)}(\mathbf{A}) = t \right\} \quad (16)$$

and all possible matrices \mathbf{B} as

$$\mathcal{B}_t := \{\text{diag}(\mathbf{B}^{(1)}, \dots, \mathbf{B}^{(\ell)}) \in \mathbb{F}_q^{t \times n} : \text{rk}_q(\mathbf{B}^{(i)}) = t_i \text{ and } \mathbf{B}^{(i)} \in \mathbb{F}_q^{t_i \times \eta} \forall i \in \{1, \dots, \ell\}\}. \quad (17)$$

When drawing \mathbf{E} uniformly at random from $\mathcal{E}_t^{(n)}$ the marginal distribution for the corresponding rank profile $\mathbf{t} \in \mathcal{T}_{t, \ell, \mu}$ is given by

$$\Pr[\mathbf{t}] = \frac{1}{|\mathcal{E}_t^{(n)}|} \prod_{i=1}^{\ell} \text{NM}_q(sm, \eta, t_i)$$

where $\text{NM}_q(sm, \eta, t_i)$ denotes the number of matrices over \mathbb{F}_q of size $sm \times \eta$ of rank t_i which can be computed as (see [13])

$$\text{NM}_q(sm, \eta, t_i) = \prod_{j=0}^{t_i-1} \frac{(q^{sm} - q^j)(q^\eta - q^j)}{q^{t_i} - q^j}.$$

Lemma 3 *For a given rank profile $\mathbf{t} = [t_1, t_2, \dots, t_\ell]$ of the error \mathbf{E} , the probability that \mathbf{E} has \mathbb{F}_{q^m} -rank equal to t , given \mathbf{t} is then*

$$\begin{aligned} \Pr[\text{rk}_{q^m}(\mathbf{E}) = t \mid \mathbf{t}] &= \Pr[\text{rk}_{q^m}(\mathbf{A}) = t \mid \mathbf{t}] \\ &= \frac{\prod_{j=0}^{t-1} (q^{sm} - q^{jm})}{\prod_{i=1}^{\ell} \prod_{j=0}^{t_i-1} (q^{sm} - q^j)} \end{aligned}$$

where \mathbf{A} is a matrix drawn uniformly at random from the set defined in (16).

Proof: Every error matrix \mathbf{E} can be decomposed as in (2), i.e., $\mathbf{E} = \mathbf{A}\mathbf{B}$. Since \mathbf{A} is the only part influencing the \mathbb{F}_{q^m} -rank of \mathbf{E} and is unique if an arbitrary block-diagonal matrix \mathbf{B} with $\mathcal{R}_q(\mathbf{B}) = \mathcal{R}_q(\mathbf{E})$ is fixed (see, e.g., [14, Theorem 1]), we obtain

$$\Pr[\text{rk}_{q^m}(\mathbf{E}) = t \mid \mathbf{t}] = \Pr[\text{rk}_{q^m}(\mathbf{A}) = t \mid \mathbf{t}].$$

Recall that \mathcal{B}_t is defined in (17) as the set of all block-diagonal matrices \mathbf{B} with $\mathcal{R}_q(\mathbf{B}) = \mathcal{R}_q(\mathbf{E})$ and rank profile \mathbf{t} . By the law of total probability, we then have

$$\begin{aligned} \Pr[\text{rk}_{q^m}(\mathbf{E}) = t \mid \mathbf{t}] &= \sum_{\mathbf{B} \in \mathcal{B}_t} \Pr[\text{rk}_{q^m}(\mathbf{A}) = t \mid \mathbf{t}, \mathbf{B}] \cdot \Pr[\mathbf{B} \mid \mathbf{t}] \\ &= \sum_{\mathbf{B} \in \mathcal{B}_t} \Pr[\text{rk}_{q^m}(\mathbf{A}) = t \mid \mathbf{t}] \cdot \Pr[\mathbf{B} \mid \mathbf{t}] \\ &= \Pr[\text{rk}_{q^m}(\mathbf{A}) = t \mid \mathbf{t}], \end{aligned}$$

where we used the fact that $\Pr[\mathbf{B} | \mathbf{t}] = \frac{1}{|\mathcal{B}_t|}$ since \mathbf{B} is uniformly distributed over \mathcal{B}_t . The probability $\Pr[\text{rk}_{\mathbb{F}_q}(\mathbf{A}) = t | \mathbf{t}]$ can be computed as

$$\Pr[\text{rk}_{\mathbb{F}_q}(\mathbf{A}) = t | \mathbf{t}] = \frac{|\{\mathbf{A}' \in \mathbb{F}_{q^m}^{s \times t} : \text{wt}_{\Sigma R}^{(\mathbf{t})}(\mathbf{A}') = \text{rk}_{\mathbb{F}_q}(\mathbf{A}') = t\}|}{|\{\mathbf{A}' \in \mathbb{F}_{q^m}^{s \times t} : \text{wt}_{\Sigma R}^{(\mathbf{t})}(\mathbf{A}') = t\}|}.$$

Consider any matrix $\mathbf{A} \in \{\mathbf{A}' \in \mathbb{F}_{q^m}^{s \times t} : \text{rk}_{\mathbb{F}_q}(\mathbf{A}') = t\}$. Since \mathbf{A} is full-rank over \mathbb{F}_{q^m} and $s \geq t$, we can make several observations about the ranks of its blocks $\mathbf{A}^{(i)}$. First, the \mathbb{F}_{q^m} -rank of each block $\mathbf{A}^{(i)}$ is equal to its corresponding rank profile component, i.e., $\text{rk}_{\mathbb{F}_q}(\mathbf{A}^{(i)}) = t_i$. Moreover, the \mathbb{F}_q -rank of each block $\mathbf{A}^{(i)}$ is lower bounded by its \mathbb{F}_{q^m} -rank, meaning that $t_i \leq \text{rk}_q(\mathbf{A}^{(i)})$. At the same time, the \mathbb{F}_q -rank of each block $\mathbf{A}^{(i)}$ is upper bounded by $\min(t_i, s)$, because the rank of a matrix cannot exceed its number of rows or columns. In this case, each block $\mathbf{A}^{(i)}$ has dimensions $s \times t_i$, so its \mathbb{F}_q -rank is at most $\min\{t_i, s\}$. However, since $t = \sum_{i=1}^{\ell} t_i \leq s$, we have $t_i \leq s$ for all $i \in \{1, \dots, \ell\}$, which implies that $\min\{t_i, s\} = t_i$. By combining the lower and upper bounds, we conclude that $\text{rk}_q(\mathbf{A}^{(i)}) = t_i$ for all $i \in \{1, \dots, \ell\}$. This implies that for any $\mathbf{A} \in \{\mathbf{A}' \in \mathbb{F}_{q^m}^{s \times t} : \text{rk}_{\mathbb{F}_q}(\mathbf{A}') = t\}$ we have that $\text{wt}_{\Sigma R}^{(\mathbf{t})}(\mathbf{A}) = t$ and therefore, we have the following equality

$$\{\mathbf{A}' \in \mathbb{F}_{q^m}^{s \times t} : \text{wt}_{\Sigma R}^{(\mathbf{t})}(\mathbf{A}') = \text{rk}_{\mathbb{F}_q}(\mathbf{A}') = t\} = \{\mathbf{A}' \in \mathbb{F}_{q^m}^{s \times t} : \text{rk}_{\mathbb{F}_q}(\mathbf{A}') = t\}$$

and hence

$$\Pr[\text{rk}_{\mathbb{F}_q}(\mathbf{A}) = t | \mathbf{t}] = \frac{|\{\mathbf{A}' \in \mathbb{F}_{q^m}^{s \times t} : \text{rk}_{\mathbb{F}_q}(\mathbf{A}') = t\}|}{|\{\mathbf{A}' \in \mathbb{F}_{q^m}^{s \times t} : \text{wt}_{\Sigma R}^{(\mathbf{t})}(\mathbf{A}') = t\}|} = \frac{\prod_{j=0}^{t-1} (q^{sm} - q^{jm})}{\prod_{i=1}^{\ell} \prod_{j=0}^{t_i-1} (q^{sm} - q^j)}$$

where $\prod_{j=0}^{t-1} (q^{sm} - q^{jm})$ is the number of all full-rank matrices of size $s \times t$ over \mathbb{F}_{q^m} and $\prod_{i=1}^{\ell} \prod_{j=0}^{t_i-1} (q^{sm} - q^j)$ is the number of all matrices in $\mathbb{F}_{q^m}^{s \times t}$ with sum-rank weight t with corresponding length partition \mathbf{t} (see [13]). \blacksquare

Lemma 4 *Let \mathbf{E} be an error matrix drawn uniformly at random from the set $\mathcal{E}_t^{(n)}$. Then, the probability that $\text{rk}_{\mathbb{F}_q}(\mathbf{E}) = t$ is given by*

$$\Pr[\text{rk}_{\mathbb{F}_q}(\mathbf{E}) = t] = \frac{\prod_{j=0}^{t-1} (q^{sm} - q^{jm})}{|\mathcal{E}_t^{(n)}|} \cdot \sum_{\mathbf{t} \in \mathcal{T}_{t, \ell, \mu}} \prod_{i=1}^{\ell} \begin{bmatrix} \eta \\ t_i \end{bmatrix}_q. \quad (20)$$

Proof: Recall the sets \mathcal{A}_t and \mathcal{B}_t defined in (16) and (17), respectively.

According to Lemma 3, for a fixed rank profile \mathbf{t} , we can draw $\mathbf{A} \in \mathcal{A}_t$ and $\mathbf{B} \in \mathcal{B}_t$

independently and uniformly from their corresponding domains and obtain $\mathbf{E} = \mathbf{A}\mathbf{B}$ with $\text{wt}_{\Sigma R}^{(n)}(\mathbf{E}) = t$ such that \mathbf{E} is uniformly drawn at random from \mathcal{E}_t .

This means the probability $\Pr[\text{rk}_{\text{qm}}(\mathbf{E}) = t]$ is

$$\begin{aligned} \Pr[\text{rk}_{\text{qm}}(\mathbf{E}) = t] &= \sum_{\mathbf{t} \in \mathcal{T}_{t,\ell,\mu}} \Pr[\mathbf{t}] \cdot \Pr[\text{rk}_{\text{qm}}(\mathbf{A}) = t \mid \mathbf{t}] \\ &= \sum_{\mathbf{t} \in \mathcal{T}_{t,\ell,\mu}} \frac{\prod_{i=1}^{\ell} \text{NM}_q(sm, \eta, t_i)}{|\mathcal{E}_t^{(n)}|} \cdot \frac{\prod_{j=0}^{t-1} (q^{sm} - q^{jm})}{\prod_{i=1}^{\ell} \prod_{j=0}^{t_i-1} (q^{sm} - q^j)} \\ &= \frac{\prod_{j=0}^{t-1} (q^{sm} - q^{jm})}{|\mathcal{E}_t^{(n)}|} \cdot \sum_{\mathbf{t} \in \mathcal{T}_{t,\ell,\mu}} \frac{\prod_{i=1}^{\ell} \text{NM}_q(sm, \eta, t_i)}{\prod_{i=1}^{\ell} \prod_{j=0}^{t_i-1} (q^{sm} - q^j)}. \end{aligned}$$

Here, we first apply the law of total probability to express $\Pr[\text{rk}_{\text{qm}}(\mathbf{E}) = t]$ as a sum over all possible rank profiles $\mathbf{t} \in \mathcal{T}_{t,\ell,\mu}$. Then, we use the fact that \mathbf{A} and \mathbf{B} are drawn independently and uniformly from their respective domains to compute the conditional probability $\Pr[\text{rk}_{\text{qm}}(\mathbf{A}) = t \mid \mathbf{t}]$.

Next, we simplify the expression using the definition of the Gaussian binomial coefficient:

$$\begin{aligned} \Pr[\text{rk}_{\text{qm}}(\mathbf{E}) = t] &= \frac{\prod_{j=0}^{t-1} (q^{sm} - q^{jm})}{|\mathcal{E}_t^{(n)}|} \cdot \sum_{\mathbf{t} \in \mathcal{T}_{t,\ell,\mu}} \frac{\prod_{i=1}^{\ell} \prod_{j=0}^{t_i-1} \frac{(q^{sm} - q^j)(q^{\eta} - q^j)}{(q^{t_i} - q^j)}}{\prod_{i=1}^{\ell} \prod_{j=0}^{t_i-1} (q^{sm} - q^j)} \\ &= \frac{\prod_{j=0}^{t-1} (q^{sm} - q^{jm})}{|\mathcal{E}_t^{(n)}|} \cdot \sum_{\mathbf{t} \in \mathcal{T}_{t,\ell,\mu}} \prod_{i=1}^{\ell} \prod_{j=0}^{t_i-1} \frac{(q^{\eta} - q^j)}{(q^{t_i} - q^j)} \\ &= \frac{\prod_{j=0}^{t-1} (q^{sm} - q^{jm})}{|\mathcal{E}_t^{(n)}|} \cdot \sum_{\mathbf{t} \in \mathcal{T}_{t,\ell,\mu}} \prod_{i=1}^{\ell} \left[\eta \right]_{t_i, q}. \end{aligned}$$

In the first step, we rewrite the numerator using the definition of $\text{NM}_q(sm, \eta, t_i)$. Then, we cancel out the common terms in the numerator and denominator, leaving only the Gaussian binomial coefficients in the final expression, which completes the proof. \blacksquare

At first glance, the expression in (20) does not appear to be computationally efficient. However, in [18], it was shown that the term $|\mathcal{E}_t^{(n)}|$ can be efficiently computed using a dynamic programming approach. Inspired by this, we propose a similar procedure to compute the right-hand side of (20). To this end, let us define

$$\Phi_{q,\eta}(t, \ell) := \sum_{\mathbf{t} \in \mathcal{T}_{t,\ell,\mu}} \prod_{i=1}^{\ell} \left[\eta \right]_{t_i, q}$$

where $\Phi_{q,\eta}(t, \ell)$ represents the sum over all possible rank profiles \mathbf{t} for a given sum-rank weight t . For each rank profile, the q-binomial coefficient $\begin{bmatrix} \eta \\ t_i \end{bmatrix}_q$ counts the number of subspaces of dimension t_i in an η -dimensional space over \mathbb{F}_q . This expression can be computed recursively as

$$\Phi_{q,\eta}(t, \ell) = \begin{cases} \begin{bmatrix} \eta \\ t \end{bmatrix}_q & \text{if } \ell = 1 \\ \sum_{t'=0}^{\min\{\eta, t\}} \begin{bmatrix} \eta \\ t' \end{bmatrix}_q \cdot \Phi_{q,\eta}(t - t', \ell - 1) & \text{else} \end{cases}. \quad (21)$$

The recursive relation can be understood as follows: For the base case, when $\ell = 1$, there is only one block, and the number of subspaces of dimension t in an η -dimensional space over \mathbb{F}_q is given by the q-binomial coefficient $\begin{bmatrix} \eta \\ t \end{bmatrix}_q$. For $\ell > 1$, we consider all possible dimensions t' for the first block, ranging from 0 to $\min\{\eta, t\}$. For each choice of t' , we multiply the number of subspaces of dimension t' in the first block, given by $\begin{bmatrix} \eta \\ t' \end{bmatrix}_q$, with the number of ways to distribute the remaining sum-rank weight $t - t'$ among the remaining $\ell - 1$ blocks, recursively computed by $\Phi_{q,\eta}(t - t', \ell - 1)$.

Algorithm 2: Compute $\Phi_{q,\eta}(t, \ell)$

Input : Parameters: q, η, t and ℓ

Output : $\Phi_{q,\eta}(t, \ell)$

Initialize: $N(t', \ell') = 0 \quad \forall t' \in \{1, \dots, t\}$ and $\ell' \in \{1, \dots, \ell\}$

```

1 for  $t' \in \{1, \dots, t\}$  do
2    $\lfloor N(t', 1) \leftarrow \begin{bmatrix} \eta \\ t' \end{bmatrix}_q$ 
3 for  $\ell' \in \{2, \dots, \ell\}$  do
4   for  $t'' \in \{1, \dots, t\}$  do
5      $\lfloor N(t', \ell') \leftarrow \sum_{t''=0}^{\min\{\eta, t'\}} N(t' - t'', \ell' - 1) \cdot \begin{bmatrix} \eta \\ t'' \end{bmatrix}_q$ 
6 return  $N(t, \ell)$ 

```

Theorem 4 *Algorithm 2 is correct and requires $\ell \cdot t^2$ integer multiplications.*

Proof: The correctness of Algorithm 2 follows from the recursive relationship established in (21) with the base cases $\Phi_{q,\eta}(t, 1) = \begin{bmatrix} \eta \\ t \end{bmatrix}_q$.

Regarding the complexity, the algorithm performs $\ell \cdot t^2$ integer multiplications. This is because, for each $\ell' \in \{2, \dots, \ell\}$ and each $t' \in \{1, \dots, t\}$, the inner loop runs over $\min\{\eta, t'\}$ values,

leading to at most t iterations per combination of ℓ' and t' . Thus, the total number of iterations is $\ell \cdot t^2$. ■

Corollary 1 *The success probability in (20) can be computed with polynomially-bounded complexity.*

Proof: The success probability in (20) is given by

$$\frac{\prod_{j=0}^{t-1} (q^{sm} - q^{jm})}{|\mathcal{E}_t^{(n)}|} \cdot \sum_{\mathbf{t} \in \mathcal{T}_{t,\ell,\mu}} \prod_{i=1}^{\ell} \begin{bmatrix} \eta \\ t_i \end{bmatrix}_q.$$

We analyze the complexity of computing each term in this expression:

- $|\mathcal{E}_t^{(n)}|$ can be computed with polynomially bounded complexity, as shown in [13].
- $\sum_{\mathbf{t} \in \mathcal{T}_{t,\ell,\mu}} \prod_{i=1}^{\ell} \begin{bmatrix} \eta \\ t_i \end{bmatrix}_q$ can be computed with polynomially bounded complexity according to Theorem 4.
- The computation of $\prod_{j=0}^{t-1} (q^{sm} - q^{jm})$ is also polynomially bounded. The terms q^{sm} and q^{jm} can be computed using repeated squaring, and their differences and products involve polynomially-bounded integer operations.

The overall complexity is dominated by the complexity of computing $|\mathcal{E}_t^{(n)}|$ and the term $\sum_{\mathbf{t} \in \mathcal{T}_{t,\ell,\mu}} \prod_{i=1}^{\ell} \begin{bmatrix} \eta \\ t_i \end{bmatrix}_q$, both of which are polynomially bounded. Thus, the success probability can be computed with polynomially bounded complexity. ■

Theorem 5 *Let $\mathcal{IC}[s; \mathbf{n}, k, d]$ be an \mathbb{F}_{q^m} -linear homogeneous s -interleaved sum-rank-metric code with component code \mathcal{C} of minimum sum-rank distance d , and let $t \leq \min\{s, d - 2\}$. Furthermore, let*

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

where \mathbf{C} is a codeword of the interleaved code $\mathcal{IC}[s; \mathbf{n}, k, d]$ and $\mathbf{E} \in \mathbb{F}_{q^m}^{s \times n}$ is an error matrix uniformly drawn at random from $\mathcal{E}_t^{(n)}$. Then the probability that Algorithm 1 cannot decode, which is the probability that $\text{rk}_{q^m}(\mathbf{E}) \neq t$, is bounded from above as

$$\Pr[\text{rk}_{q^m}(\mathbf{E}) \neq t] \leq tq^{-m(s-t+1)}. \quad (22)$$

Proof: From Lemma 4, we have

$$\Pr[\text{rk}_{q^m}(\mathbf{E}) = t] = \frac{\prod_{j=0}^{t-1} (q^{sm} - q^{jm})}{|\mathcal{E}_t^{(n)}|} \cdot \sum_{t \in \mathcal{T}_{t,\ell,\mu}} \prod_{i=1}^{\ell} \left[\begin{matrix} \eta \\ t_i \end{matrix} \right]_q.$$

Next, we consider the following inequality to bound the denominator $|\mathcal{E}_t^{(n)}|$

$$\begin{aligned} |\mathcal{E}_t^{(n)}| &= \sum_{t \in \mathcal{T}_{t,\ell,\mu}} \prod_{i=1}^{\ell} \left[\begin{matrix} \eta \\ t_i \end{matrix} \right]_q \prod_{j=0}^{t_i-1} (q^{sm} - q^j) \\ &\leq \sum_{t \in \mathcal{T}_{t,\ell,\mu}} \prod_{i=1}^{\ell} \left[\begin{matrix} \eta \\ t_i \end{matrix} \right]_q \prod_{j=0}^{t_i-1} q^{sm} \\ &= \sum_{t \in \mathcal{T}_{t,\ell,\mu}} \left(\prod_{i=1}^{\ell} \left[\begin{matrix} \eta \\ t_i \end{matrix} \right]_q \right) q^{smt}. \end{aligned}$$

Using this inequality, we can further bound $\Pr[\text{rk}_{q^m}(\mathbf{E}) = t]$ as follows

$$\begin{aligned} \Pr[\text{rk}_{q^m}(\mathbf{E}) = t] &\geq \frac{\prod_{j=0}^{t-1} (q^{sm} - q^{jm})}{q^{smt}} \\ &= \prod_{j=0}^{t-1} (1 - q^{m(j-s)}) \geq 1 - tq^{m(t-s-1)}. \end{aligned}$$

At this point, we have the same equation as in the rank-metric case. The last step follows from [10, Theorem 10].

Finally, the claim of the theorem follows from the fact that

$$\Pr[\text{rk}_{q^m}(\mathbf{E}) \neq t] = 1 - \Pr[\text{rk}_{q^m}(\mathbf{E}) = t].$$

■

In Figure 1, we show the actual value of the failure probability, using Algorithm 2 to evaluate (20) and compare with the derived upper bound from (22). The failure probability is presented in logarithmic scale (base 10) versus the difference between the interleaving order s and the sum-rank error weight t for two different parameter sets.

Figure 1a illustrates the failure probability for very small code parameters, with $q = 2$, $m = 2$, $n = 10$, and $t = 4$. On the other hand, Figure 1b shows the failure probability for larger, but still relatively small, code parameters, with $q = 2$, $m = 10$, $n = 30$, and $t = 11$.

From these plots, we can observe several key points:

- 1) As the code parameters increase, the difference in failure probability between the rank

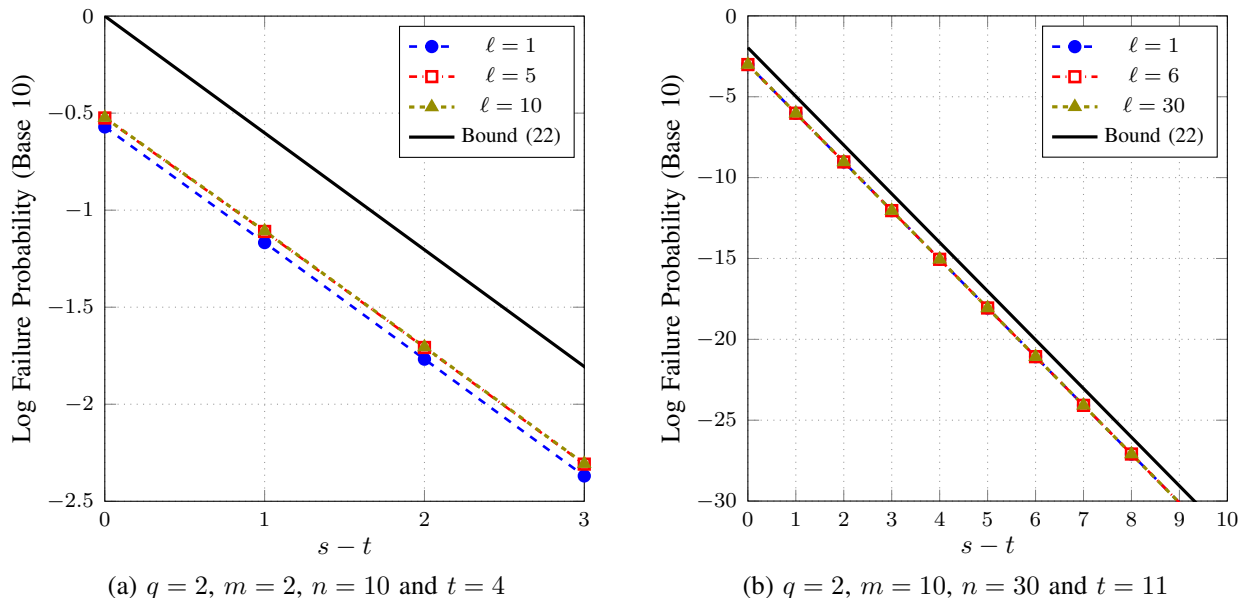


Fig. 1: Logarithmic failure probability vs. $s - t$ for different values of ℓ with q, m, n and t .

metric ($\ell = 1$), sum-rank metric ($1 < \ell < n$), and Hamming metric ($\ell = n$) becomes negligibly small. This suggests that for sufficiently large code parameters, the choice of metric has a diminishing impact on the failure probability.

- 2) The failure probability declines exponentially fast as $s - t$ increases, which is expected based on the expression of the upper bound in (22).
- 3) The gap between the upper bound and the actual failure probability narrows as the code parameters increase. In Figure 1b, with larger code parameters, the bound and the actual values are more closely aligned compared to Figure 1a. This suggests that the derived upper bound becomes tighter and more accurate for larger code parameters.

B. Decoding Radius

For the decoder presented in Algorithm 1 to succeed and uniquely recover the error, the following conditions must be satisfied:

- 1) The error matrix \mathbf{E} must satisfy the high-order and full-rank conditions, i.e., $s \geq t$ and $\text{rk}_{q^m}(\mathbf{E}) = t$. Note that the full-rank condition already implies a high interleaving order, since for \mathbf{E} to have rank t , the interleaving order s must be at least t .

2) The parity-check matrix \mathbf{H} must satisfy the condition in (8), which can be expressed as

$$\text{rk}_{\mathbb{F}_q^m} \left(\mathbf{H} \begin{bmatrix} \mathbf{B} \\ \mathbf{b} \end{bmatrix}^\top \right) = t + 1 \quad \forall \mathbf{b} \in \mathbb{F}_q^n \setminus \text{supp}_{\Sigma R}(\mathbf{E}) \text{ s.t. } \text{wt}_{\Sigma R}^{(n)}(\mathbf{b}) = 1$$

where \mathbf{B} is a basis of the row support of the error with respect to the sum-rank metric as in (3).

For $t \leq d-2$, the second condition is always true, which can be shown by applying [13, Lemma 8]. However, for $t \geq d-1$, the decoder becomes probabilistic and returns a unique solution to the decoding problem only if the second condition is satisfied. When considering the average over all error matrices \mathbf{E} , the probability of this condition being met becomes a property of the code itself, as it depends on the parity-check matrix \mathbf{H} and therefore on the code's distance spectrum. Note that the decoder in Algorithm 1 can correct errors with a maximum weight of $t \leq \min\{n-k-1, \mu\ell\}$. The term $n-k-1$ ensures that the common parity-check matrix of the error code and the component code has at least one non-zero row, which is necessary for successful decoding. The term $\mu\ell$ represents the maximum sum-rank weight for the given parameters, as defined in (1), with μ given in (15).

Figure 2 illustrates the decoding regions for Algorithm 1 when the error matrix \mathbf{E} satisfies the full-rank condition, i.e., $\text{rk}_{\mathbb{F}_q^m}(\mathbf{E}) = t$. This condition is crucial for the success of the decoding algorithm. Figure 3 further explores the relationships between various conditions and the decoding success for error matrices drawn uniformly at random. It shows that when the conditions as in Theorem 5 are met, such as $s-t$ or m being large, the probability of the full-rank condition being satisfied is high. Consequently, this leads to two important results: (1) unique decoding is always possible for $t \leq d-2$ when the full-rank condition is satisfied, and (2) decoding is possible with high probability for $t \leq n-k-1$ when m is large.

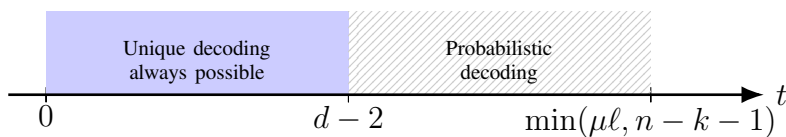


Fig. 2: Illustration of the decoding regions for Algorithm 1 if full-rank condition is satisfied.

Theorem 6 Let $\mathbf{H} \in \mathbb{F}_{q^m}^{(n-k) \times n}$ be a matrix chosen uniformly at random from $\mathbb{F}_{q^m}^{(n-k) \times n}$. We assume that q^m is large enough such that the probability of \mathbf{H} having full \mathbb{F}_{q^m} -rank is close to

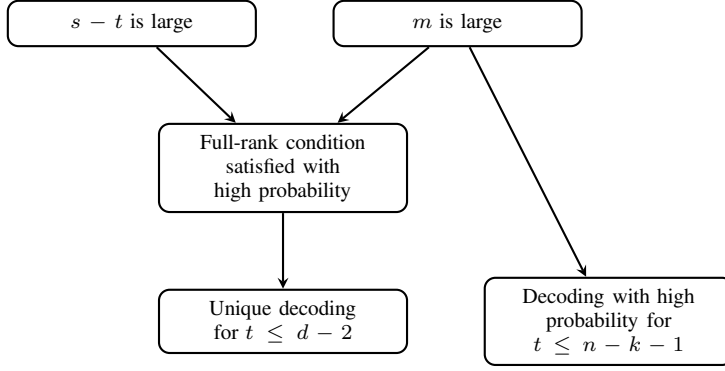


Fig. 3: Relationships between parameters, conditions and decoding success for uniform errors.

1. Consider an error matrix \mathbf{E} picked uniformly at random from the set $\mathcal{E}_t^{(n)}$, where \mathbf{E} , \mathbf{A} , and \mathbf{B} are as in (2), and $\text{wt}_{\Sigma R}^{(n)}(\mathbf{E}) = t = \sum_{i=1}^{\ell} t_i$, satisfying the full-rank condition, i.e., $\text{rk}_{q^m}(\mathbf{E}) = t$. Then, on average, the probability that the condition (8) is satisfied is bounded from below and above as follows

$$P_{\text{LB}} \leq \Pr[(8) \text{ is satisfied}] \leq P_{\text{UB}}$$

where

$$P_{\text{LB}} := \left(1 - \frac{1}{|\mathcal{E}_t^{(n)}|} \cdot \sum_{\mathbf{t} \in \mathcal{T}_{t, \ell, \mu}} \prod_{i=1}^{\ell} \text{NM}_q(sm, \eta, t_i) \cdot \frac{N_{\mathbf{t}}}{q^{m(n-k-t)}} \right) \cdot \prod_{j=0}^{t-1} \left(1 - \frac{1}{q^{m(n-k-j)}} \right) \quad (23)$$

with

$$N_{\mathbf{t}} := \min\{q^{m(n-k)}, \sum_{i=1}^{\ell} (q^{n_i} - q^{t_i})\} \quad (24)$$

and

$$P_{\text{UB}} := \prod_{j=0}^{t-1} \left(1 - \frac{1}{q^{m(n-k-j)}} \right).$$

Proof: The proof consists of two parts, one for the lower bound and one for the upper bound.

First, we show the lower bound. Condition (8) can only be satisfied if $\mathbf{H}\mathbf{B}^{\top}$ is of full \mathbb{F}_{q^m} -rank. Since \mathbf{H} is chosen uniformly at random, $\mathbf{H}\mathbf{B}^{\top}$ is also a matrix uniformly distributed over

$\mathbb{F}_{q^m}^{(n-k) \times t}$. The probability of $\mathbf{H}\mathbf{B}^\top$ having full \mathbb{F}_{q^m} -rank is given by

$$p_1 := \prod_{j=0}^{t-1} \left(1 - \frac{1}{q^{m(n-k-j)}} \right).$$

Now, consider a specific vector $\mathbf{b} \in \mathbb{F}_q^n \setminus \text{supp}_{\Sigma R}(\mathbf{E})$ and append it to \mathbf{B} . Note that for the bound we omit the restriction with $\text{wt}_{\Sigma R}^{(n)}(\mathbf{b}) = 1$. The probability that $\mathbf{H}[\mathbf{B}^\top \mid \mathbf{b}^\top]$ is of full \mathbb{F}_{q^m} -rank, given that $\mathbf{H}\mathbf{B}^\top$ is of full \mathbb{F}_{q^m} -rank, is equal to

$$p_2 := \left(1 - \frac{1}{q^{m(n-k-t)}} \right)$$

which is the probability that the $(t+1)$ -th additional column in $\mathbf{H}[\mathbf{B}^\top \mid \mathbf{b}^\top]$ is linearly independent of the t remaining columns. This must hold true for any $\mathbf{b} \in \mathbb{F}_q^n \setminus \text{supp}_{\Sigma R}(\mathbf{E})$ simultaneously. Define the event \mathcal{Z}_i as the $(t+1)$ -th column in $\mathbf{H}[\mathbf{B}^\top \mid \mathbf{b}_i^\top]$ for a given $\mathbf{b}_i \in \mathbb{F}_q^n \setminus \text{supp}_{\Sigma R}(\mathbf{E})$ being linearly dependent on the remaining t columns, with $i \in \{1, \dots, N_t\}$ and

$$N_t \geq \min\{q^{m(n-k)}, |\mathbb{F}_q^n \setminus \text{supp}_{\Sigma R}(\mathbf{E})|\}.$$

The cardinality $|\mathbb{F}_q^n \setminus \text{supp}_{\Sigma R}(\mathbf{E})|$ is given by

$$\sum_{i=1}^{\ell} (q^{n_i} - q^{t_i}),$$

which is the sum of the cardinalities of the blocks that correspond to $|\mathbb{F}_q^{n_i} \setminus \mathcal{R}_q(\mathbf{B}^{(i)})| = q^{n_i} - q^{t_i}$.

By applying the union bound on the events \mathcal{Z}_i , the probability that (8) is not satisfied is bounded from above as

$$\begin{aligned} \Pr[(8) \text{ is not satisfied}] &\leq (1 - p_1) + p_1 \cdot \sum_{\mathbf{t} \in \mathcal{T}_{t,\ell,\mu}} \Pr[\mathbf{t}] \cdot \Pr \left[\bigcup_{i=1}^{N_t} \mathcal{Z}_i \right] \\ &\leq (1 - p_1) + p_1 \cdot \sum_{\mathbf{t} \in \mathcal{T}_{t,\ell,\mu}} \Pr[\mathbf{t}] \cdot \sum_{i=1}^{N_t} \Pr[\mathcal{Z}_i] \end{aligned}$$

where $\Pr[\mathbf{t}]$ is the marginal distribution of the rank profiles, given by

$$\Pr[\mathbf{t}] = \frac{1}{|\mathcal{E}_t^{(n)}|} \prod_{i=1}^{\ell} \text{NM}_q(sm, \eta, t_i).$$

Now, assuming that all \mathcal{Z}_i are independent, we have that for a given \mathbf{t} ,

$$\Pr[\mathcal{Z}_i] = 1 - p_2 = \frac{1}{q^{m(n-k-t)}}.$$

Therefore,

$$\begin{aligned} \Pr[(8) \text{ is not satisfied}] &\leq (1 - p_1) + p_1 \cdot \sum_{\mathbf{t} \in \mathcal{T}_{t,\ell,\mu}} \Pr[\mathbf{t}] \cdot \sum_{i=1}^{N_{\mathbf{t}}} \Pr[\mathcal{Z}_i] \\ &= (1 - p_1) + p_1 \cdot \sum_{\mathbf{t} \in \mathcal{T}_{t,\ell,\mu}} \frac{1}{|\mathcal{E}_{\mathbf{t}}^{(n)}|} \prod_{i=1}^{\ell} \text{NM}_q(sm, \eta, t_i) \cdot \sum_{i=1}^{N_{\mathbf{t}}} \frac{1}{q^{m(n-k-t)}} \\ &= (1 - p_1) + p_1 \cdot \sum_{\mathbf{t} \in \mathcal{T}_{t,\ell,\mu}} \frac{1}{|\mathcal{E}_{\mathbf{t}}^{(n)}|} \prod_{i=1}^{\ell} \text{NM}_q(sm, \eta, t_i) \cdot \frac{N_{\mathbf{t}}}{q^{m(n-k-t)}}. \end{aligned}$$

Consequently,

$$\begin{aligned} \Pr[(8) \text{ is satisfied}] &= 1 - \Pr[(8) \text{ is not satisfied}] \\ &\geq 1 - \left((1 - p_1) + p_1 \cdot \sum_{\mathbf{t} \in \mathcal{T}_{t,\ell,\mu}} \frac{1}{|\mathcal{E}_{\mathbf{t}}^{(n)}|} \prod_{i=1}^{\ell} \text{NM}_q(sm, \eta, t_i) \cdot \frac{N_{\mathbf{t}}}{q^{m(n-k-t)}} \right) \\ &= p_1 - p_1 \cdot \sum_{\mathbf{t} \in \mathcal{T}_{t,\ell,\mu}} \frac{N_{\mathbf{t}} \cdot \prod_{i=1}^{\ell} \text{NM}_q(sm, \eta, t_i)}{|\mathcal{E}_{\mathbf{t}}^{(n)}| \cdot q^{m(n-k-t)}} \\ &= p_1 \cdot \left(1 - \sum_{\mathbf{t} \in \mathcal{T}_{t,\ell,\mu}} \frac{N_{\mathbf{t}} \cdot \prod_{i=1}^{\ell} \text{NM}_q(sm, \eta, t_i)}{|\mathcal{E}_{\mathbf{t}}^{(n)}| \cdot q^{m(n-k-t)}} \right) \\ &= \left(1 - \sum_{\mathbf{t} \in \mathcal{T}_{t,\ell,\mu}} \frac{N_{\mathbf{t}} \cdot \prod_{i=1}^{\ell} \text{NM}_q(sm, \eta, t_i)}{|\mathcal{E}_{\mathbf{t}}^{(n)}| \cdot q^{m(n-k-t)}} \right) \prod_{j=0}^{t-1} \left(1 - \frac{1}{q^{m(n-k-j)}} \right) \end{aligned}$$

which establishes the lower bound P_{LB} .

For the upper bound, we observe that the probability that condition (8) is satisfied is upper bounded by the event that at least one matrix $\mathbf{H}[\mathbf{B}^\top \mid \mathbf{b}^\top] \in \mathbb{F}_{q^m}^{(n-k) \times (t+1)}$ is of full \mathbb{F}_{q^m} -rank, where $\mathbf{b} \in \mathbb{F}_q^n \setminus \text{supp}_{\Sigma R}(\mathbf{E})$. This probability is equal to the probability that a random matrix in $\mathbb{F}_{q^m}^{(n-k) \times (t+1)}$ is of full \mathbb{F}_{q^m} -rank (see [19]), which is given by

$$P_{\text{UB}} := \prod_{j=0}^t \left(1 - \frac{1}{q^{m(n-k-j)}} \right).$$

This completes the proof. ■

C. Simulation Results

We now investigate the tightness of the upper and lower bounds on the failure probability of condition (8) derived in Theorem 6. While these bounds provide theoretical guarantees, they may not always give a precise estimate of the actual failure probability. To assess their accuracy and explore alternative approximations, we conduct simulations.

The following presents an approximation obtained by modifying the proof of Theorem 6. Although this approximation does not provide strict bounds, it may yield more realistic estimates of the failure probability and serves as a basis for comparison with the simulated results.

If, in the proof of Theorem 6, we ignore the dependence of the events \mathcal{Z}_i for $i \in \{1, \dots, N_t\}$, we obtain neither a lower nor an upper bound on the failure/success probability of condition (8) for a random parity-check matrix \mathbf{H} . Nevertheless, we state the expression under that circumstance and use it as an approximation. We then show through simulation that this approximation provides a more realistic estimate of the success probability for relative small η . From the proof of Theorem 6, it is straightforward to show that, in this case,

$$\Pr[\text{condition (8) is satisfied}] \approx \prod_{j=0}^{t-1} \left(1 - \frac{1}{q^{m(n-k-j)}}\right) \cdot \sum_{\mathbf{t} \in \mathcal{T}_{t,\ell,\mu}} \Pr[\mathbf{t}] \left(1 - \frac{1}{q^{m(n-k-t)}}\right)^{N_t}. \quad (25)$$

It is worth noting that, in the case of the Hamming metric, the events \mathcal{Z}_i for $i \in \{1, \dots, N_t\}$ are actually independent. This is because the rows of the matrix \mathbf{B} consist solely of (scaled) unit vectors. For the Hamming metric, we have $N_t = n - t$. When multiplying \mathbf{B}^\top on the right side of \mathbf{H} , we effectively select specific columns of \mathbf{H} . Moreover, for any additional unit vector \mathbf{b} , we select another column from \mathbf{H} to form $\mathbf{H} \cdot [\mathbf{B}^\top \mid \mathbf{b}^\top]$, choosing from the remaining $n - t$ columns. Given the assumption that the entries of \mathbf{H} are independently and uniformly distributed, these selected columns are also independent.

In contrast, this independence does not hold for the rank metric. In the rank-metric case, the matrices \mathbf{B}^\top and $[\mathbf{B}^\top \mid \mathbf{b}^\top]$ can be any full-rank matrices, rather than being limited to (scaled) unit vectors. Consequently, when multiplying these matrices on the right side of \mathbf{H} , we obtain linear combinations of the columns of \mathbf{H} rather than simply selecting individual columns. These linear combinations introduce dependencies among the events \mathcal{Z}_i , violating the independence assumption.

We investigate the tightness of the upper and lower bounds on the failure probability of condition (8) derived in Theorem 6 by comparing them with simulated values and an approximation

(given in (25)). The simulation was performed using a Monte Carlo approach with 10^5 samples for each point. Each sample involved picking a random parity-check matrix and evaluating the failure probability. We have implemented the simulation with the help of the computer-algebra system SageMath [20].

Figure 4 shows parameters $\eta = 1$, $\ell = 24$, $n = 24$, $q = 2$, $m = 2$, and $k = 8$, which correspond to the Hamming metric. In this case, we observe that the approximation closely matches the simulated values, and both the upper and lower bounds hold. This reinforces our theory that the approximation is exact in the Hamming-metric case. In Figures 5 and 6, we increase η to 2 and 3, respectively, while keeping the code parameters constant (i.e., length and dimension). As we move away from the Hamming metric by increasing η , we observe that the approximation becomes less accurate, and the lower bound provides a better estimate. In all plots, the upper bound is relatively loose compared to the lower bound.

Notably, for all scenarios, the success probability for $t = 14$, which is the second-largest value possible to decode for the given code parameters, stays above 40%, which is a relatively high success probability.

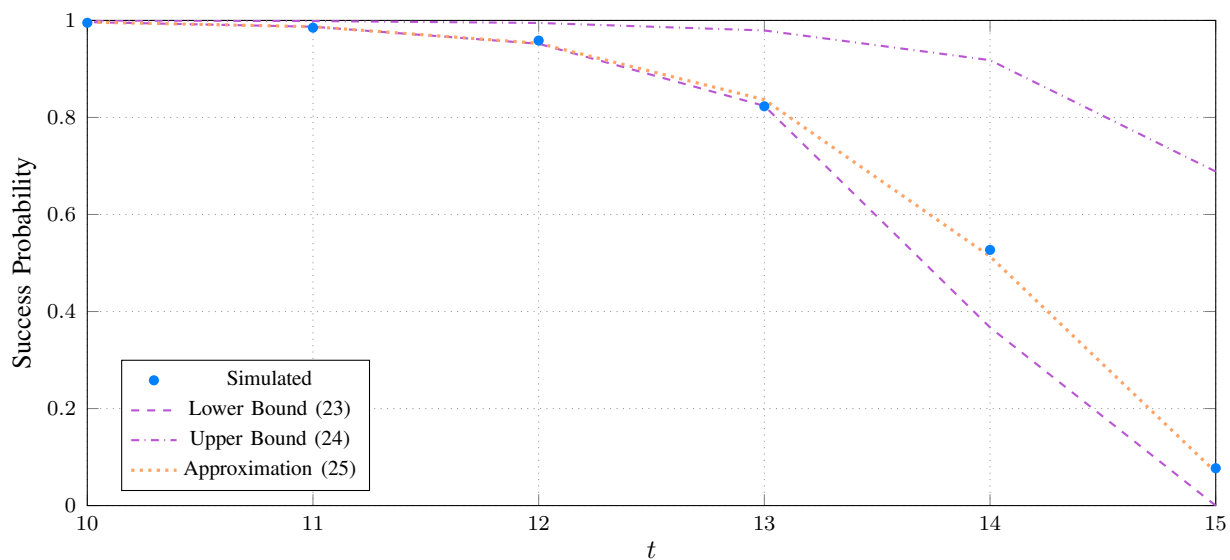


Fig. 4: Success probability vs error weight t for $q = 2$, $m = 2$, $n = 24$, $k = 8$, $\eta = 1$, and $\ell = 24$ with interleaving order $s = t$.

D. Examples

In this section, we present two examples to illustrate the decoding process using Algorithm 1 with small code parameters and randomly chosen codes. The first example demonstrates a

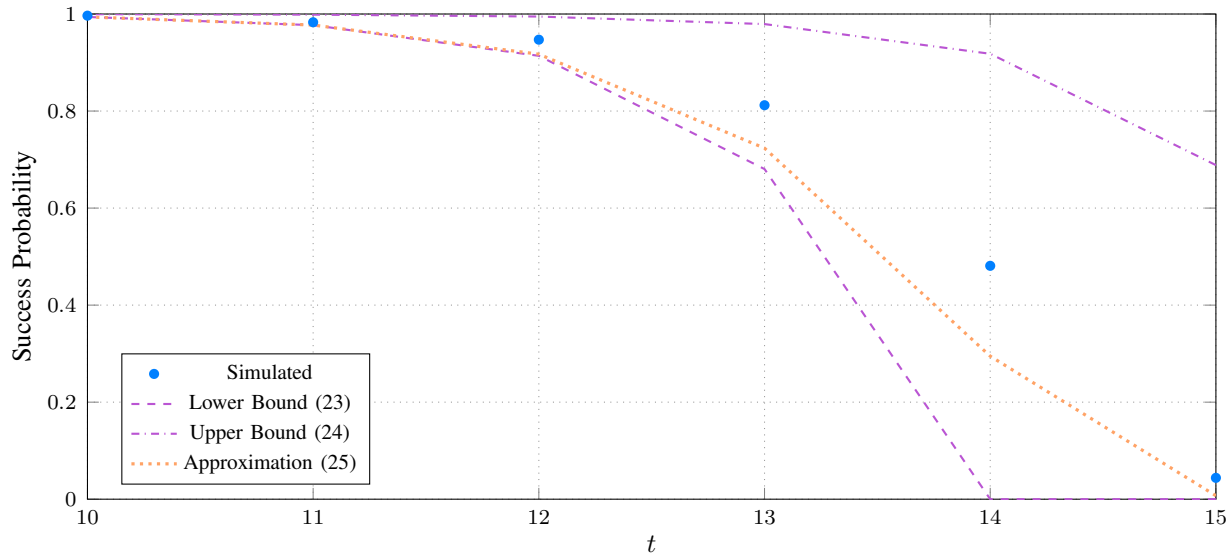


Fig. 5: Success probability vs error weight t for $q = 2$, $m = 2$, $n = 24$, $k = 8$, $\eta = 2$, and $\ell = 12$ with interleaving order $s = t$.

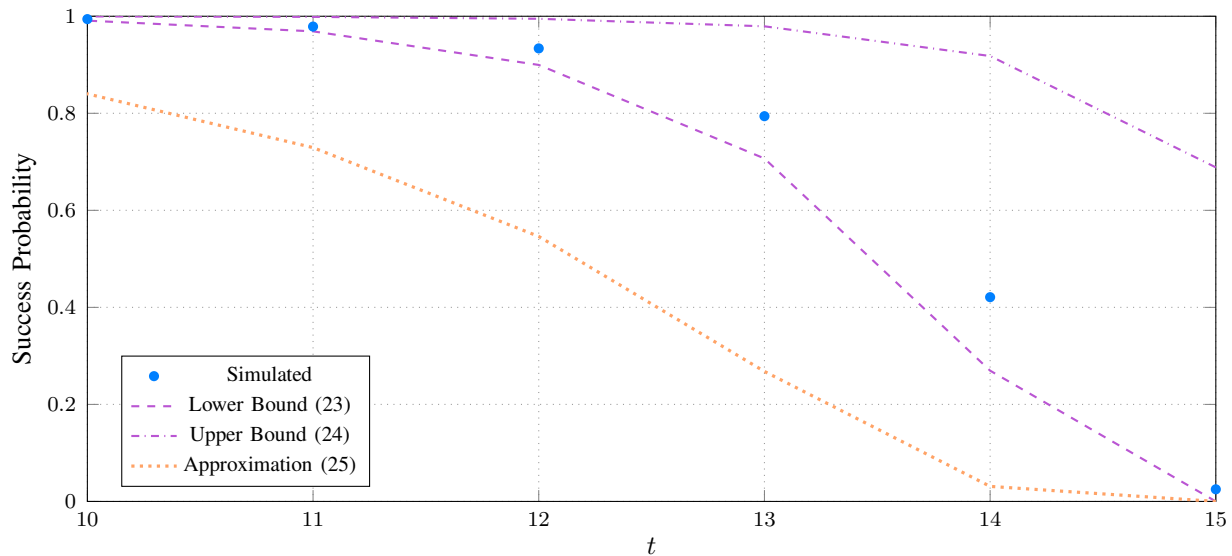


Fig. 6: Success probability vs error weight t for $q = 2$, $m = 2$, $n = 24$, $k = 8$, $\eta = 3$, and $\ell = 8$ with interleaving order $s = t$.

successful decoding, while the second example showcases a decoding failure where the condition in (8) is not satisfied.

Example 1 (Successful Decoding) Let $\mathbb{F}_{q^m} = \mathbb{F}_{2^3}$ with primitive element α and primitive polynomial $\alpha^3 + \alpha + 1$. Consider an interleaved sum-rank-metric code $\mathcal{IC}[s; \mathbf{n}, k, d]$ of length $n = 6$ with $\mathbf{n} = [2, 2, 2]$, $k = 2$, $\eta = 2$, $\ell = 3$, $d = 3$, and $s = 3$, defined by the parity-check

matrix

$$\mathbf{H} = \left[\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \middle| \begin{array}{cc} \alpha^2 + 1 & \alpha \\ 1 & \alpha^2 \\ \alpha & \alpha \\ \alpha^2 + \alpha + 1 & \alpha + 1 \end{array} \right].$$

Suppose the codeword

$$\mathbf{C} = \left[\begin{array}{cc|cc} \alpha^2 + 1 & 1 & 1 & 1 \\ \alpha + 1 & \alpha^2 + \alpha & \alpha^2 & \alpha \\ 0 & 0 & 1 & \alpha \end{array} \middle| \begin{array}{cc} \alpha^2 + \alpha & \alpha + 1 \\ 1 & \alpha + 1 \\ \alpha^2 & 1 \end{array} \right]$$

is corrupted by an error

$$\mathbf{E} = \left[\begin{array}{cc|cc} 0 & \alpha^2 + 1 & \alpha^2 + 1 & \alpha^2 + 1 \\ 1 & 0 & \alpha^2 & \alpha^2 \\ \alpha + 1 & \alpha & \alpha + 1 & \alpha + 1 \end{array} \middle| \begin{array}{cc} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{array} \right]$$

with $\mathbf{C}\mathbf{H}^\top = \mathbf{0}$, $\text{rk}_{\mathbb{q}^m}(\mathbf{E}) = \text{wt}_{\Sigma R}^{(n)}(\mathbf{E}) = 3$ and $\mathbf{t} = [2, 1, 0]$. The received word is $\mathbf{Y} = \mathbf{C} + \mathbf{E}$, given by

$$\mathbf{Y} = \left[\begin{array}{cc|cc} \alpha^2 + 1 & \alpha^2 & \alpha^2 & \alpha^2 \\ \alpha & \alpha^2 + \alpha & 0 & \alpha^2 + \alpha \\ \alpha + 1 & \alpha & \alpha & 1 \end{array} \middle| \begin{array}{cc} \alpha^2 + \alpha & \alpha + 1 \\ 1 & \alpha + 1 \\ \alpha^2 & 1 \end{array} \right].$$

The syndrome $\mathbf{S} = \mathbf{H}\mathbf{Y}^\top$ is computed as

$$\mathbf{S} = \left[\begin{array}{ccc} 0 & 1 & \alpha + 1 \\ \alpha^2 + 1 & 0 & \alpha \\ \alpha^2 + 1 & \alpha^2 & \alpha + 1 \\ \alpha^2 + 1 & \alpha^2 & \alpha + 1 \end{array} \right].$$

We find a matrix $\mathbf{P} \in \mathbb{F}_{\mathbb{q}^m}^{(n-k) \times (n-k)}$ with $\text{rk}_{\mathbb{q}^m}(\mathbf{P}) = n - k = 4$, such as

$$\mathbf{P} = \left[\begin{array}{cccc} 1 & \alpha^2 + 1 & 0 & \alpha^2 + \alpha + 1 \\ \alpha + 1 & \alpha^2 + 1 & 0 & \alpha^2 + 1 \\ \alpha^2 + \alpha + 1 & \alpha + 1 & 0 & \alpha + 1 \\ 0 & 0 & 1 & 1 \end{array} \right],$$

which transforms PS into row-echelon form.

The last $n - k - t = 1$ rows of PH yield

$$\mathbf{H}_S = \left[\begin{array}{cc|cc} 0 & 0 & 1 & 1 \\ \hline & & \alpha^2 + 1 & 1 \end{array} \right].$$

Expanding each sub-block of \mathbf{H}_S over \mathbb{F}_2 yields

$$\text{ext}(\mathbf{H}_S^{(1)}) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad \text{ext}(\mathbf{H}_S^{(2)}) = \begin{bmatrix} 1 & 1 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad \text{ext}(\mathbf{H}_S^{(3)}) = \begin{bmatrix} 1 & 1 \\ 0 & 0 \\ 1 & 0 \end{bmatrix}.$$

Note that $\text{ext}(\mathbf{H}_S^{(1)})$ is an all-zero matrix, indicating that this block corresponds to a full-rank error.

Next, we compute a basis for each of the right kernels of $\text{ext}(\mathbf{H}_S^{(1)})$, $\text{ext}(\mathbf{H}_S^{(2)})$, and $\text{ext}(\mathbf{H}_S^{(3)})$ such that

$$\text{ext}(\mathbf{H}_S^{(1)}) \mathbf{B}^{(1)\top} = \mathbf{0}, \quad \text{ext}(\mathbf{H}_S^{(2)}) \mathbf{B}^{(2)\top} = \mathbf{0}, \quad \text{ext}(\mathbf{H}_S^{(3)}) \mathbf{B}^{(3)\top} = \mathbf{0}$$

and

$$\text{rk}_q(\mathbf{B}^{(1)}) = n_1 - \text{rk}_q(\mathbf{H}_S^{(1)}) = 2,$$

$$\text{rk}_q(\mathbf{B}^{(2)}) = n_2 - \text{rk}_q(\mathbf{H}_S^{(2)}) = 1,$$

$$\text{rk}_q(\mathbf{B}^{(3)}) = n_3 - \text{rk}_q(\mathbf{H}_S^{(3)}) = 0.$$

This gives us

$$\mathbf{B}^{(1)} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in \mathbb{F}_q^{2 \times 2}, \quad \mathbf{B}^{(2)} = \begin{bmatrix} 1 & 1 \end{bmatrix} \in \mathbb{F}_q^{1 \times 2}, \quad \mathbf{B}^{(3)} = \begin{bmatrix} & \end{bmatrix} \in \mathbb{F}_q^{0 \times 2}.$$

The matrix \mathbf{B} is then given by

$$\mathbf{B} = \text{diag}(\mathbf{B}^{(1)}, \mathbf{B}^{(2)}, \mathbf{B}^{(3)}) = \left[\begin{array}{cc|cc|cc} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 1 & 0 & 0 \end{array} \right]$$

Finally, solving for \mathbf{A} , i.e.,

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

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix} \mathbf{A}^\top = \begin{bmatrix} 0 & 1 & \alpha + 1 \\ \alpha^2 + 1 & 0 & \alpha \\ \alpha^2 + 1 & \alpha^2 & \alpha + 1 \\ \alpha^2 + 1 & \alpha^2 & \alpha + 1 \end{bmatrix}$$

yields

$$\mathbf{A}^\top = \begin{bmatrix} 0 & \alpha^2 + 1 & \alpha^2 + 1 \\ 1 & 0 & \alpha^2 \\ \alpha + 1 & \alpha & \alpha + 1 \end{bmatrix}$$

$$\implies \hat{\mathbf{E}} = \mathbf{A}\mathbf{B} = \left[\begin{array}{cc|cc|c} 0 & \alpha^2 + 1 & \alpha^2 + 1 & 0 & 0 \\ 1 & 0 & \alpha^2 & 0 & 0 \\ \alpha + 1 & \alpha & \alpha + 1 & \alpha + 1 & 0 \end{array} \right]$$

and $\hat{\mathbf{E}} = \mathbf{E}$. Note that decoding is possible since $\text{rk}_{\mathbb{F}_q}(\mathbf{H}[\mathbf{B}^\top \mid \mathbf{b}^\top]) = t + 1 = 4$ for all $\mathbf{b} \in \mathbb{F}_q^n \setminus \text{supp}_{\Sigma R}(\mathbf{E})$ such that $\text{wt}_{\Sigma R}^{(n)}(\mathbf{b}) = 1$.

Example 2 (Decoding Failure) Let $\mathbb{F}_{q^m} = \mathbb{F}_{2^2}$ with primitive element α and minimal polynomial $\alpha^2 + \alpha + 1$. Further let $\mathcal{IC}[s; \mathbf{n}, k, d]$ be an interleaved sum-rank-metric code of length $n = 6$ with $\mathbf{n} = [2, 2, 2]$, $k = 2$, $d = 4$, $\eta = 2$, $\ell = 3$ and $s = 3$, defined by the parity-check matrix

$$\mathbf{H} = \left[\begin{array}{cc|cc|cc} 1 & 0 & 0 & \alpha + 1 & 0 & \alpha \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & \alpha & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & \alpha + 1 \end{array} \right].$$

Suppose that the codeword

$$\mathbf{C} = \left[\begin{array}{cc|cc|cc} 0 & \alpha & 1 & \alpha + 1 & \alpha + 1 & 1 \\ \alpha & 0 & \alpha + 1 & \alpha & 1 & \alpha \\ 0 & \alpha & 1 & \alpha + 1 & \alpha + 1 & 1 \end{array} \right]$$

is corrupted by an error

$$\mathbf{E} = \left[\begin{array}{cc|cc|cc} \alpha & 0 & \alpha & \alpha & 0 & 0 \\ 1 & 1 & \alpha+1 & \alpha+1 & 0 & 0 \\ \alpha & 1 & \alpha+1 & \alpha+1 & 0 & 0 \end{array} \right]$$

with $\text{rk}_{\mathbb{F}_m}(\mathbf{E}) = \text{wt}_{\Sigma R}^{(n)}(\mathbf{E}) = 3$ and $\mathbf{t} = [2, 1, 0]$. The resulting received word is then $\mathbf{Y} = \mathbf{C} + \mathbf{E}$ and thus

$$\mathbf{Y} = \left[\begin{array}{cc|cc|cc} \alpha & \alpha & \alpha+1 & 1 & \alpha+1 & 1 \\ \alpha+1 & 1 & 0 & 1 & 1 & \alpha \\ \alpha & \alpha+1 & \alpha & 0 & \alpha+1 & 1 \end{array} \right].$$

The syndrome is then

$$\mathbf{S} = \mathbf{H}\mathbf{Y}^\top = \left[\begin{array}{ccc} \alpha+1 & \alpha+1 & 0 \\ \alpha & \alpha & \alpha \\ 1 & \alpha & \alpha \\ 0 & 0 & 0 \end{array} \right].$$

We can find $\mathbf{P} \in \mathbb{F}_{q^m}^{(n-k) \times (n-k)}$ with $\text{rk}_{\mathbb{F}_m}(\mathbf{P}) = n - k = 4$, hence

$$\mathbf{P} = \left[\begin{array}{cccc} 0 & \alpha & \alpha & 0 \\ \alpha & \alpha & \alpha & 0 \\ \alpha & \alpha+1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right]$$

such that $\mathbf{P}\mathbf{S}$ is in row-echelon form. The last $n - k - t = 1$ rows of

$$\mathbf{P}\mathbf{H} = \left[\begin{array}{cc|cc|cc} 0 & \alpha & \alpha & 1 & 0 & \alpha \\ \alpha & \alpha & \alpha & 0 & 0 & 1 \\ \alpha & \alpha+1 & 0 & \alpha & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & \alpha+1 \end{array} \right]$$

yields

$$\mathbf{H}_S = \left[\begin{array}{cc|cc|cc} 0 & 0 & 0 & 0 & 1 & \alpha+1 \end{array} \right].$$

Next we expand every sub-block of \mathbf{H}_S over \mathbb{F}_2 and obtain

$$\text{ext}(\mathbf{H}_S^{(1)}) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad \text{ext}(\mathbf{H}_S^{(2)}) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad \text{ext}(\mathbf{H}_S^{(3)}) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Next we compute a basis for each of the right kernels of $\text{ext}(\mathbf{H}_S^{(1)})$, $\text{ext}(\mathbf{H}_S^{(2)})$ and $\text{ext}(\mathbf{H}_S^{(3)})$ such that

$$\text{ext}(\mathbf{H}_S^{(1)}) \mathbf{B}^{(1)\top} = \mathbf{0}, \quad \text{ext}(\mathbf{H}_S^{(2)}) \mathbf{B}^{(2)\top} = \mathbf{0}, \quad \text{ext}(\mathbf{H}_S^{(3)}) \mathbf{B}^{(3)\top} = \mathbf{0}$$

and

$$\begin{aligned} \text{rk}_q(\mathbf{B}^{(1)}) &= n_1 - \text{rk}_q(\mathbf{H}_S^{(1)}) = 2, \\ \text{rk}_q(\mathbf{B}^{(2)}) &= n_2 - \text{rk}_q(\mathbf{H}_S^{(2)}) = 2, \\ \text{rk}_q(\mathbf{B}^{(3)}) &= n_3 - \text{rk}_q(\mathbf{H}_S^{(3)}) = 1, \end{aligned}$$

which gives us

$$\mathbf{B}^{(1)} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \mathbf{B}^{(2)} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \mathbf{B}^{(3)} = \begin{bmatrix} & \\ & \end{bmatrix}.$$

The matrix \mathbf{B} is then given by

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

In fact, we have that $\text{rk}_q(\mathbf{B}^{(1)}) + \text{rk}_q(\mathbf{B}^{(2)}) + \text{rk}_q(\mathbf{B}^{(3)}) = 4 > t = 3$, and therefore we cannot uniquely recover the error \mathbf{E} anymore. This is because the decoding condition in (8) is not satisfied, since there exists $\mathbf{b} \in \mathbb{F}_q^n \setminus \text{supp}_{\Sigma R}(\mathbf{E})$ such that $\text{wt}_{\Sigma R}^{(n)}(\mathbf{b}) = 1$ and $\text{rk}_{qm}(\mathbf{H}[\mathbf{B}^\top \mid \mathbf{b}^\top]) \neq t + 1 = 4$. That is, for $\mathbf{b} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$, we have

$$\mathbf{H}[\mathbf{B}^\top \mid \mathbf{b}^\top] = \begin{bmatrix} 1 & 0 & \alpha + 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & \alpha + 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \implies \text{rk}_{qm}(\mathbf{H}[\mathbf{B}^\top \mid \mathbf{b}^\top]) = 3 < 4.$$

E. Special Cases of the Algorithm for Hamming and Rank Metric

The decoder presented in Algorithm 1 is a generalization of the Metzner–Kapturowski decoder for the Hamming metric [9] and the Metzner–Kapturowski-like decoder for the rank metric [15]. In this section, we highlight the differences in how the proposed decoder operates in three distinct metrics: the Hamming metric, the rank metric, and the sum-rank metric. Note that both the Hamming and rank metrics are special cases of the sum-rank metric. We also emphasize the analogous definitions of the error support for all three cases. To differentiate between the error weights in each metric, we use the following notation: t_H for the Hamming metric, t_R for the rank metric, and $t_{\Sigma R}$ for the sum-rank metric.

In the Hamming metric, the support of an error matrix \mathbf{E} is defined as the set of indices corresponding to the non-zero columns of \mathbf{E} , that is,

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

However, this classical support notion does *not* directly coincide with the definition of the sum-rank support from (4). Nonetheless, there is a one-to-one correspondence between these concepts. We demonstrate this by first describing $\text{supp}_{\Sigma R}(\mathbf{E})$ and then relating it to $\text{supp}_H(\mathbf{E})$. Since each of the blocks $\mathbf{E}^{(1)}, \dots, \mathbf{E}^{(\ell)}$ has length one in the Hamming-metric setting, at most one rank error can occur per block. Thus, the i -th block $\mathbf{B}^{(i)}$ in the error decomposition $\mathbf{E} = \mathbf{A} \cdot \text{diag}(\mathbf{B}^{(1)}, \dots, \mathbf{B}^{(\ell)})$ from (2) has size $t_H^{(i)} \times 1$ with $t_H^{(i)} \in \{0, 1\}$. If the i -th block for an $i \in \{1, \dots, \ell\}$ is erroneous, the matrix $\mathbf{B}^{(i)}$ contains one nonzero \mathbb{F}_q element, which implies $\mathcal{R}_q(\mathbf{B}^{(i)}) = \mathbb{F}_q$. If, on the other hand, the block $\mathbf{E}^{(i)}$ is error-free, the matrix $\mathbf{B}^{(i)}$ has size 0×1 and its row space $\mathcal{R}_q(\mathbf{B}^{(i)})$ is the trivial vector space $\{0\} \subseteq \mathbb{F}_q$. Thus, the sum-rank support $\text{supp}_{\Sigma R}(\mathbf{E}) = \mathcal{R}_q(\mathbf{B}^{(1)}) \times \dots \times \mathcal{R}_q(\mathbf{B}^{(\ell)})$ of \mathbf{E} is a Cartesian product containing copies of \mathbb{F}_q and $\{0\}$ in the respective positions. This allows us to define a bijection between the sum-rank support and the classical definition of Hamming support given above. Namely,

$$\text{supp}_H(\mathbf{E}) \mapsto \text{supp}_{\Sigma R}(\mathbf{E}) = \times_{i=1}^n \mathbf{X}_i \text{ with } \mathbf{X}_i = \begin{cases} \mathbb{F}_q & \text{if } i \in \text{supp}_H(\mathbf{E}) \\ \{0\} & \text{if } i \notin \text{supp}_H(\mathbf{E}) \end{cases}$$

maps a subset of the indices $\{1, \dots, n\}$ to the corresponding sum-rank support contained in \mathbb{F}_q^n with $\mathbf{n} = [1, \dots, 1]$. We stick to $\text{supp}_H(\mathbf{E})$ to explain the consequences for decoding in the Hamming metric in the following.

An error matrix \mathbf{E} with t_H errors in the Hamming metric can be factored into $\mathbf{E} = \mathbf{AB}$, where the rows of \mathbf{B} are (scaled) unit vectors corresponding to the t_H error positions. Consequently, the support of \mathbf{E} is the union of the supports of the rows \mathbf{B}_i of \mathbf{B} ($\forall i \in \{1, \dots, t_H\}$), i.e.,

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

When the full-rank condition for the Metzner–Kapturowski decoder is satisfied, the zero columns in \mathbf{H}_S reveal the error positions and determine the error support. In this case, we have

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

where $\mathbf{H}_{S,i}$ denotes the i -th row of \mathbf{H}_S . Note that this equality corresponds to (10) in the general case. The process of recovering the error support $\text{supp}_H(\mathbf{E})$ from \mathbf{H}_S is depicted in Figure 7.

The rank-metric case is analogous to the Hamming-metric case but with a different definition of the error support. An error matrix \mathbf{E} with rank $\text{rk}_q(\mathbf{E}) = t_R$ can be decomposed as $\mathbf{E} = \mathbf{AB}$. The rank support $\text{supp}_R(\mathbf{E})$ of \mathbf{E} is defined as the row space of \mathbf{B} , which is spanned by the union of all rows \mathbf{B}_i of \mathbf{B} , where \mathbf{B}_i is the i -th row of \mathbf{B} . This coincides exactly with the more general definition in the sum-rank metric from (4) for $\ell = 1$. Thus, the support of \mathbf{E} is given by

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

where \bigoplus denotes the addition of vector spaces, i.e., the span of the union of the considered spaces. If the full-rank condition on the error matrix is satisfied, the rank support of \mathbf{E} can be determined by the \mathbb{F}_q -kernel of \mathbf{H}_S [10]. The \mathbb{F}_q -row space of \mathbf{H}_S can be computed by taking the span of the union of spaces $\text{supp}_R(\mathbf{H}_{S,i})$, where $\mathbf{H}_{S,i}$ is the i -th row of \mathbf{H}_S . Consequently, the support of \mathbf{E} is given by

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

In the sum-rank metric, according to (4), we have

$$\begin{aligned} \text{supp}_{\Sigma R}(\mathbf{E}) &= \text{supp}_R(\mathbf{B}^{(1)}) \times \text{supp}_R(\mathbf{B}^{(2)}) \times \dots \times \text{supp}_R(\mathbf{B}^{(s)}) \\ &= \left(\bigoplus_{j=1}^{n-k-t_{\Sigma R}} \text{supp}_R(\mathbf{B}_j^{(1)}) \right) \times \dots \times \left(\bigoplus_{j=1}^{n-k-t_{\Sigma R}} \text{supp}_R(\mathbf{B}_j^{(\ell)}) \right). \end{aligned}$$

Based on Theorem 1, we have

$$\begin{aligned} \text{supp}_{\Sigma R}(\mathbf{E}) &= \left(\bigoplus_{j=1}^{n-k-t_{\Sigma R}} \text{supp}_R(\mathbf{H}_{S,j}^{(1)}) \right)^\perp \times \dots \\ &\dots \times \left(\bigoplus_{j=1}^{n-k-t_{\Sigma R}} \text{supp}_R(\mathbf{H}_{S,j}^{(s)}) \right)^\perp. \end{aligned}$$

The relation between the error matrix \mathbf{E} , the matrix \mathbf{H}_S , and the error supports for the Hamming metric, rank metric, and sum-rank metric are illustrated in Figures 7, 8, and 9, respectively. In particular, Figure 9 demonstrates the process of determining the sum-rank support $\text{supp}_{\Sigma R}(\mathbf{E})$ from the row spaces of the blocks $\mathbf{H}_S^{(i)}$ for $i \in \{1, \dots, \ell\}$.

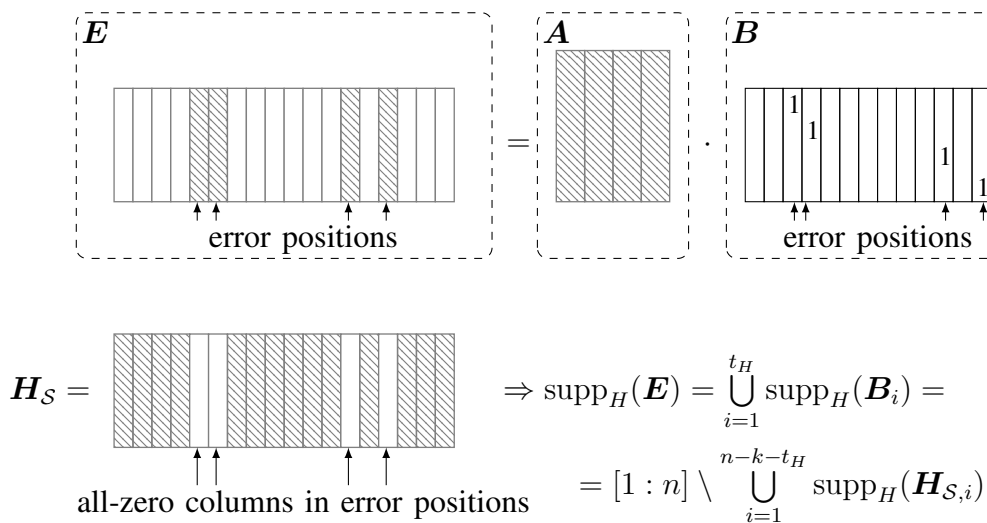


Fig. 7: Illustration of the error support for the Hamming-metric case with $\mathbf{E} = \mathbf{A}\mathbf{B} \in \mathbb{F}_q^{s \times n}$, $\mathbf{A} \in \mathbb{F}_q^{s \times t_H}$, $\mathbf{B} \in \mathbb{F}_q^{t_H \times n}$ and $\mathbf{H}_S \in \mathbb{F}_q^{(n-k-t_H) \times n}$. \mathbf{B}_i is the i -th row of \mathbf{B} and $\mathbf{H}_{S,i}$ the i -th row of \mathbf{H}_S .

V. CONCLUSION

In this paper, we consider a Metzner–Kapturowski-like decoding algorithm tailored for high-order interleaved sum-rank-metric codes. By leveraging the novel concept of an error code, we provided a fresh perspective on the decoding process. This approach not only enhances our understanding of the decoder’s functionality but also offers new insights.

Our proposed algorithm demonstrates significant versatility, being applicable to any linear constituent code, including those that are unstructured or random. This general applicability positions our decoder as a robust tool for a wide range of coding scenarios. Furthermore, the

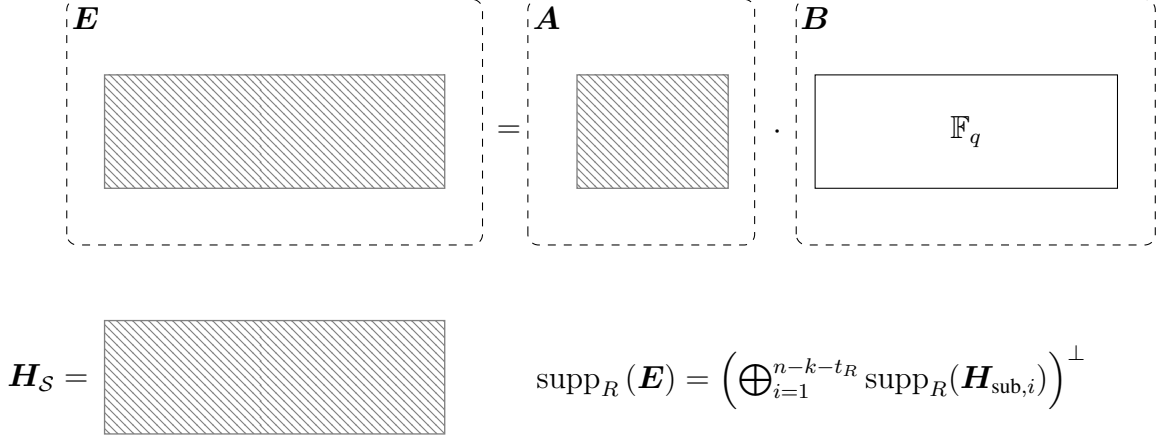
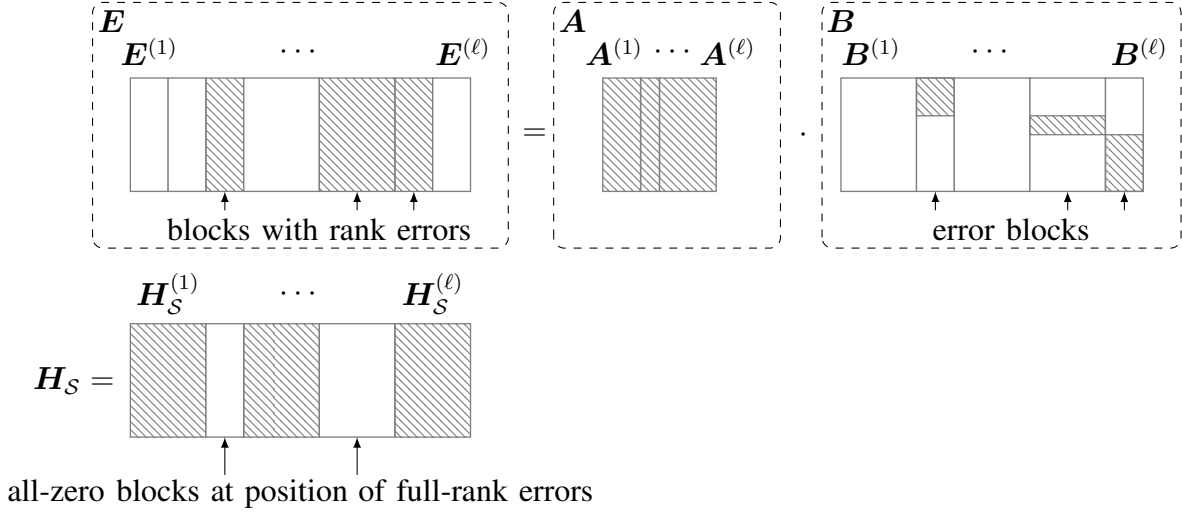


Fig. 8: Illustration of the error support for the rank-metric case with $\mathbf{E} = \mathbf{AB} \in \mathbb{F}_q^{s \times n}$, $\mathbf{A} \in \mathbb{F}_q^{s \times t_R}$, $\mathbf{B} \in \mathbb{F}_q^{t_R \times n}$ and $\mathbf{H}_S \in \mathbb{F}_q^{(n-k-t_R) \times n}$. $\mathbf{H}_{\text{sub},i}$ the i -th row of \mathbf{H}_S .



$$\text{supp}_{\Sigma R}(\mathbf{E}) = \left(\bigoplus_{j=1}^{n-k-t_{\Sigma R}} \text{supp}_R(\mathbf{H}_{S,j}^{(1)}) \right)^\perp \times \cdots \times \left(\bigoplus_{j=1}^{n-k-t_{\Sigma R}} \text{supp}_R(\mathbf{H}_{S,j}^{(s)}) \right)^\perp$$

Fig. 9: Illustration of the error support for the sum-rank-metric case with $\mathbf{E} = \mathbf{AB} \in \mathbb{F}_q^{s \times n}$, $\mathbf{A} \in \mathbb{F}_q^{s \times t_{\Sigma R}}$, $\mathbf{B} \in \mathbb{F}_q^{t_{\Sigma R} \times n}$ and $\mathbf{H}_S \in \mathbb{F}_q^{(n-k-t_{\Sigma R}) \times n}$. $\mathbf{A}^{(i)}$ and $\mathbf{B}^{(i)}$ are the i -th block of \mathbf{A} and \mathbf{B} and $\mathbf{H}_{S,j}^{(i)}$ the j -th row of $\mathbf{H}_S^{(i)}$.

computational complexity of our algorithm, which is on the order of $O(\max\{n^3, n^2s\})$ operations over \mathbb{F}_q , is independent of the code structure of the constituent code. This independence underscores the potential of our approach for practical implementations.

We also explored the success probability of our decoder, both within and beyond the unique decoding radius. Our analysis revealed that the decoder maintains a high success probability

even for error weights exceeding the unique decoding radius.

Our work not only extends the results of previous studies but also provides valuable insights for the design and security analysis of code-based cryptosystems based on interleaved sum-rank-metric codes.

The algorithm considered in this work is designed for interleaved codes in which the constituent codes are aligned vertically, also called vertically interleaved codes. From the error code perspective, this means that the error code's row support is restricted. In an alternative model, the codewords could be aligned horizontally (horizontal interleaving), resulting in the error code's column support being restricted. The adaptation of the considered algorithm to this horizontal interleaving model is not straightforward and remains an open problem.

Future research could explore further optimizations of the decoding algorithm and its application to other metrics.

REFERENCES

- [1] G. Alagic, D. Apon, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, Y.-K. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, and D. Smith-Tone, "Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process," 2022.
- [2] R. J. McEliece, "A Public-Key Cryptosystem Based On Algebraic Coding Theory," *The Deep Space Network Progress Report*, vol. 42-44, pp. 114–116, 1978.
- [3] M. Elleuch, A. Wachter-Zeh, and A. Zeh, "A Public-Key Cryptosystem from Interleaved Goppa Codes," *arXiv preprint arXiv:1809.03024*, 2018.
- [4] L. Holzbaur, H. Liu, S. Puchinger, and A. Wachter-Zeh, "On Decoding and Applications of Interleaved Goppa Codes," in *2019 IEEE International Symposium on Information Theory (ISIT)*, 2019, pp. 1887–1891.
- [5] J. Renner, S. Puchinger, and A. Wachter-Zeh, "Interleaving Loidreau's Rank-Metric Cryptosystem," in *2019 XVI International Symposium "Problems of Redundancy in Information and Control Systems" (REDUNDANCY)*. IEEE, 2019, pp. 127–132.
- [6] V. Y. Krachkovsky and Y. X. Lee, "Decoding for Iterative Reed–Solomon Coding Schemes," *IEEE Transactions on Magnetics*, vol. 33, no. 5, pp. 2740–2742, 1997.
- [7] P. Loidreau and R. Overbeck, "Decoding Rank Errors Beyond the Error Correcting Capability," in *International Workshop on Algebraic and Combinatorial Coding Theory (ACCT)*, Sep. 2006, pp. 186–190.
- [8] H. Bartz and S. Puchinger, "Fast Decoding of Interleaved Linearized Reed—Solomon Codes and Variants," *submitted to: IEEE Transactions on Information Theory*, 2022, available at <https://arxiv.org/abs/2201.01339>.
- [9] J. J. Metzner and E. J. Kapturovski, "A General Decoding Technique Applicable to Replicated File Disagreement Location and Concatenated Code Decoding," *IEEE Transactions on Information Theory*, vol. 36, no. 4, pp. 911–917, 1990.
- [10] J. Renner, S. Puchinger, and A. Wachter-Zeh, "Decoding High-Order Interleaved Rank-Metric Codes," in *2021 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2021, pp. 19–24.
- [11] T. Jerkovits, F. Hörmann, and H. Bartz, "On Decoding High-Order Interleaved Sum-Rank-Metric Codes," in *Code-Based Cryptography*, J.-C. Deneuville, Ed. Cham: Springer Nature Switzerland, 2023, pp. 90–109.

- [12] F. Hörmann, H. Bartz, and A.-L. Horlemann, “Distinguishing and Recovering Generalized Linearized Reed–Solomon Codes,” in *Code-Based Cryptography*, J.-C. Deneuville, Ed. Cham: Springer Nature Switzerland, 2023, vol. 13839, pp. 1–20, series Title: Lecture Notes in Computer Science. [Online]. Available: https://link.springer.com/10.1007/978-3-031-29689-5_1
- [13] S. Puchinger, J. Renner, and J. Rosenkilde, “Generic Decoding in the Sum-Rank Metric,” *IEEE Transactions on Information Theory*, vol. 68, no. 8, 2022.
- [14] G. Matsaglia and G. P. H. Styan, “Equalities and Inequalities for Ranks of Matrices \dagger ,” *Linear and Multilinear Algebra*, vol. 2, no. 3, pp. 269–292, Jan. 1974. [Online]. Available: <http://www.tandfonline.com/doi/abs/10.1080/03081087408817070>
- [15] S. Puchinger, J. Renner, and A. Wachter-Zeh, “Decoding High-Order Interleaved Rank-Metric Codes,” *arXiv preprint arXiv:1904.08774*, 2019.
- [16] A.-L. Horlemann, S. Puchinger, J. Renner, T. Schamberger, and A. Wachter-Zeh, “Information-Set Decoding with Hints,” in *Code-Based Cryptography Workshop*. Springer, 2021, pp. 60–83.
- [17] J.-M. Couveignes and R. Lercier, “Elliptic Periods for Finite Fields,” *Finite Fields and Their Applications*, vol. 15, no. 1, pp. 1–22, 2009.
- [18] S. Puchinger, J. Renner, and J. Rosenkilde, “Generic Decoding in the Sum-Rank Metric,” in *2020 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2020, pp. 54–59.
- [19] R. Lidl and H. Niederreiter, *Finite Fields*, ser. Encyclopedia of Mathematics and its Applications. Cambridge University Press, Oct. 1996, published: Hardcover.
- [20] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 9.8)*, 2023, <https://www.sagemath.org>.