Universal secure rank-metric coding schemes with optimal communication overheads *

Umberto Martínez-Peñas †

Department of Mathematical Sciences, Aalborg University, Denmark

Abstract

We study the problem of reducing the communication overhead from a noisy wire-tap channel or storage system where data is encoded as a matrix, when more columns (or their linear combinations) are available. We present its applications to reducing communication overheads in universal secure linear network coding and secure distributed storage with crisscross errors and erasures and in the presence of a wire-tapper. Our main contribution is a method to transform coding schemes based on linear rank-metric codes, with certain properties, to schemes with lower communication overheads. By applying this method to pairs of Gabidulin codes, we obtain coding schemes with optimal information rate with respect to their security and rank error correction capability, and with universally optimal communication overheads, when \( n \leq m \), being \( n \) and \( m \) the number of columns and number of rows, respectively. Moreover, our method can be applied to other families of maximum rank distance codes when \( n > m \). The downside of the method is generally expanding the packet length, but some practical instances come at no cost.

Keywords: Communication overheads, crisscross error-correction, decoding bandwidth, information-theoretical security, rank-metric codes.

MSC: 94A60, 94A62, 94B99.

1 Introduction

Universal secure linear network coding with errors and erasures was first studied in [22], where rank-metric coding schemes were proposed to protect messages sent over a linearly coded network from link errors, erasures and information leakage to a wire-tapper. Similarly, rank-metric codes have been applied to storage systems where data is stored as a matrix and where errors and erasures affect several rows and/or columns, also called crisscross errors and erasures [21]. These errors and erasures have been recently motivated by correlated and mixed failures in distributed storage systems where data

---

*Parts of this paper have been accepted for presentation at the IEEE International Symposium on Information Theory, Aachen, Germany, June 2017. [19]
†umberto@math.aau.dk
is stored in several data centers (columns), which in turn store several blocks of data (rows). See [14].

In this paper, we study how to reduce the communication overhead from such a noisy wire-tap channel or storage system to the receiver, when more columns, or their linear combinations, are available: Less ingoing links to the receiver fail in the network case, or more data centers are available and contacted in the distributed storage case. As it has been noticed in secret sharing in the literature [2, 13, 24], which corresponds to Hamming-metric erasure-correction and security, if more pieces of data (columns in our case) are available, they can be preprocessed via subpacketization so that the overall transmitted information from the channel or storage system to the receiver is reduced.

A similar concept of subpacketization has been recently developed for Reed-Solomon codes in [10]. In another direction, coding schemes recovering part of the encoded data (a node in a storage system, for instance), with respect to the Hamming metric, have already been studied, giving rise to regenerating codes [5, 6, 20], which reduce communication bandwidth, and locally repairable codes [9, 12, 23], which reduce the number of contacted nodes. The latter codes have been recently extended to the rank metric in [14]. In contrast, our aim is to recover the whole uncoded data while reducing the communication bandwidth, as in [2, 13, 24], but with respect to the rank metric and, as a consequence, with respect to the crisscross metric.

We illustrate and motivate the problem with a pair of examples. The details of the constructions will be given in Subsection 5.1.

**Example 1.** Consider a linearly coded network, as in [22, Sec. VII-A], over a finite field of size \( q = 256 \) (8-bit symbols), with packet length \( m = 2048 \), number of outgoing links \( n = 40 \), at least \( N \geq n \) ingoing links to the sink, and where \( \mu \leq 8 \) links may be wire-tapped and \( \rho \leq 16 \) ingoing links to the sink may fail.

In [22, Th. 11], a coding scheme is given with optimal information rate \( \frac{16}{40} \), able to correct the given number of erasures and secure under the given number of observations over such network, independently of its inner code (universally). The overall communication overhead from the last ingoing links to the sink is of 8 packets: The source wants to transmit 16 uncoded packets and the sink receives 24 encoded packets.

Thanks to Theorem 2 and dividing each packet into 32 subpackets of length 64 each, we will obtain a coding scheme with the same parameters, but such that the overall communication overhead at the ingoing links to the sink is of 4 packets (the minimum possible) if none of them fail (only 20 packets are received by the sink).

**Example 2.** Let again \( n = 40 \) and \( m = 2048 \), and consider a distributed storage system where data is stored as an \( m \times n \) matrix over the same finite field \( (q = 256) \), where each column corresponds to a data center that stores \( n \) symbols over \( \mathbb{F}_q \), that is, 40 8-bit symbols. Assume that \( \rho \) data centers may fail or not be available, errors occur along \( t \) rows and/or columns due to certain correlations, and a wire-tapper eavesdrops \( \mu \) data centers. Assume also that \( \rho + 2t \leq 16 \) and \( \mu \leq 8 \).

As in the previous example, the use of a pair of maximum rank distance codes allows to obtain the desired reliability and security while achieving the optimal information
rate 16/40 (see [21]), with a communication overhead of 8 packets from the contacted data centers to the receiver. Again, in this work we obtain a coding scheme with the same parameters but where the communication overhead is reduced to 4 packets (the minimum possible) if no errors occur and all data centers are available and contacted.

The paper is organized as follows: In Section 2, we establish the information-theoretical setting, defining coherent linearized noisy wire-tap channels, which we take from [22], and we establish a method of subpacketization that allows to use linear codes over the extension field. In Section 3, we define communication overheads for these linearized channels and give lower bounds on these parameters similar to those in [13]. In Section 4, we give the main contribution of this paper, which is a general method to transform coding schemes based on pairs of linear rank-metric codes, with certain properties, into coding schemes with lower communication overheads. In Section 5, we apply Gabidulin codes [8, 21] to obtain coding schemes with optimal information rates and communication overheads for \( n \leq m \), which can be seen as a rank-metric analog of the constructions in [2, 13]. However, our method allows us to correct errors, and not only erasures as in the secret sharing case [2, 13], and can be applied to other families of maximum rank distance codes, such as those in [7] for \( n > m \). Finally, in Section 6, we discuss the applications in universal secure linear network coding and secure distributed storage with crisscross errors and erasures.

Notation

Throughout the paper, we fix a prime power \( q \) and positive integers \( m, n, N, \alpha, \ell, t, \rho \) and \( \mu \). We denote by \( \mathbb{F}_q \) the finite field with \( q \) elements, \( \mathbb{F}_q^n \) denotes the set of row vectors of length \( n \) over \( \mathbb{F}_q \), and \( \mathbb{F}_q^{m \times n} \) denotes the set of \( m \times n \) matrices over \( \mathbb{F}_q \). In this paper, a code is a subset of either \( \mathbb{F}_q^n \) or \( \mathbb{F}_q^{m \times n} \), whose linearity properties are specified in each case. For an \( \mathbb{F}_q^{m \times n} \)-linear code \( C \subseteq \mathbb{F}_q^m \), we will denote by \( C^\perp \) its dual code with respect to the usual \( \mathbb{F}_q^m \)-bilinear inner product. We also use the notation \([n] = \{1, 2, \ldots, n\}\) and \([m, n] = \{m, m + 1, \ldots, n\}\) whenever \( m \leq n \), and we denote by \( H(X) \), \( H(X \mid Y) \) and \( I(X; Y) \) the entropy, conditional entropy and mutual information of the random variables \( X \) and \( Y \), respectively (see [3]), where logarithms will always be taken with base \( q \).

2 Information-theoretical setting and preliminaries

2.1 Coherent linearized channels and coset coding schemes

We will consider the secret message \( S \) to be a uniform random variable in \( S = \mathbb{F}_q^{\alpha m \times \ell} \), and we will consider noisy wire-tap channels (which can also be thought of as distributed storage systems) as given in [22]:

**Definition 1 (Coherent linearized channel [22])**. We define a coherent linearized noisy wire-tap channel with \( t \) errors, \( \rho \) erasures with erasure matrix \( A \in \mathbb{F}_q^{N \times n} \) of rank at least \( n - \rho \), and \( \mu \) observations as a channel with input a variable \( X \in X = \mathbb{F}_q^{\alpha m \times \ell} \), output
to the receiver $Y \in \mathcal{Y} = \mathbb{F}_q^{\alpha m \times N}$, and output to the eavesdropper $W \in \mathcal{W} = \mathbb{F}_q^{\alpha m \times \mu}$, together with a conditional probability distribution $P(Y, W | X)$ such that

$$\mathcal{Y}_X = \{ Y \in \mathbb{F}_q^{\alpha m \times N} \mid Y = XA^T + E, \quad E \in \mathbb{F}_q^{\alpha m \times N}, \text{Rk}(E) \leq t \},$$

$$\mathcal{W}_X = \{ W \in \mathbb{F}_q^{\alpha m \times \mu} \mid W = XB^T, B \in \mathbb{F}_q^{\mu \times N} \},$$

where $\mathcal{Y}_X = \{ Y \in \mathcal{Y} \mid P(Y|X) > 0 \}$ and $\mathcal{W}_X = \{ W \in \mathcal{W} \mid P(W|X) > 0 \}$, for a given $X \in \mathcal{X}$.

In [22], it is shown that a linearly coded network over $\mathbb{F}_q$ with link errors, erasures and information leakage, and where the last coding coefficients are known to the receiver, can be modelled as a coherent linearized noisy wire-tap channel. We will focus on this scenario and discuss how to translate the results to the distributed storage scenario with crisscross errors and erasures in Subsection 6.2, since the latter can be seen as a simpler case.

As encoders, we consider coset coding schemes as in [16, Def. 7], which are a particular case of those in [22].

**Definition 2 (Coset coding schemes [16]).** A coset coding scheme over the field $\mathbb{F}_q$ with secret message set $S = \mathbb{F}_q^{\alpha m \times \ell}$ and coded message set $\mathcal{X} = \mathbb{F}_q^{\alpha m \times n}$ is a randomized function

$$F : \mathbb{F}_q^{\alpha m \times \ell} \longrightarrow \mathbb{F}_q^{\alpha m \times n},$$

where, for every $S \in \mathbb{F}_q^{\alpha m \times \ell}$, $C = F(S)$ is the uniform random variable over a set $\mathcal{C}_S \subseteq \mathbb{F}_q^{\alpha m \times n}$. To allow correct decoding, we also assume that $\mathcal{C}_S \cap \mathcal{C}_T = \emptyset$ if $S \neq T$.

Finally, we define the information rate of the scheme as

$$R = \frac{\log_q(\#S)}{\log_q(\#\mathcal{X})} = \frac{\alpha m \ell}{\alpha mn} = \frac{\ell}{n}. \quad (1)$$

In linear network coding, universal reliability and security means correcting a number of link errors and erasures and being secure under a number of link observations, independently of the network inner code. This leads in [22] to the following definition:

**Definition 3 (Universal schemes [22]).** We say that the coset coding scheme $F : \mathbb{F}_q^{\alpha m \times \ell} \longrightarrow \mathbb{F}_q^{\alpha m \times n}$ is:

1. Universally $t$-error and $\rho$-erasure-correcting if, for every coherent linearized channel with $t$ errors, $\rho$ erasures and erasure matrix $A \in \mathbb{F}_q^{N \times n}$, there exists a decoding function $D_A : \mathcal{Y} \longrightarrow S$ such that

$$D_A(Y) = S,$$

for all $Y \in \bigcup_{X \in \mathcal{C}_S} \mathcal{Y}_X$ and all $S \in \mathcal{X}$.

2. Universally secure under $\mu$ observations if, for every coherent linearized channel with $\mu$ observations, it holds that

$$H(S|W) = H(S),$$

or equivalently $I(S;W) = 0$, for all $W \in \bigcup_{X \in \mathcal{C}_S} \mathcal{W}_X$ and all $S \in \mathcal{X}$.
2.2 Using linear codes over the extension field

In what follows, we will make use of codes that are linear over the extension field $\mathbb{F}_q^m$. To that end, we need to see how to identify matrices in $\mathbb{F}_q^{m \times n}$ with matrices in $\mathbb{F}_q^{m \times n}$.

**Definition 4.** Fix a basis $\gamma_1, \gamma_2, \ldots, \gamma_m$ of $\mathbb{F}_q^m$ as a vector space over $\mathbb{F}_q$, and define the map

$$\varphi_n : \mathbb{F}_q^{m \times n} \to \mathbb{F}_q^{m \times n}$$

(2)

as follows: Given a matrix $C \in \mathbb{F}_q^{m \times n}$ with entries $c_{i,j} \in \mathbb{F}_q$, for $i = 1, 2, \ldots, \alpha$ and $j = 1, 2, \ldots, n$, we define $\varphi_u(C)$ as the unique $\alpha m \times n$ matrix with coefficients $d_{i,j} \in \mathbb{F}_q$, for $l = 1, 2, \ldots, \alpha m$ and $j = 1, 2, \ldots, n$, such that

$$c_{i,j} = \sum_{u=1}^{m} d_{(i-1)m+u,j} \gamma_u,$$

for $i = 1, 2, \ldots, \alpha$ and $j = 1, 2, \ldots, n$. Finally, we define the rank over $\mathbb{F}_q$ of a matrix $E \in \mathbb{F}_q^{m \times n}$ as the rank over $\mathbb{F}_q$ of the matrix $\varphi_n(E) \in \mathbb{F}_q^{m \times n}$, and we denote it by $\text{Rk}_q(E)$.

The key result is that the effect of coherent linearized noisy wire-tap channels in Definition remains unchanged by the map $\varphi_n$, as we will now see:

**Lemma 1.** Let $C \in \mathbb{F}_q^{m \times n}, A \in \mathbb{F}_q^{N \times n}$ and $E \in \mathbb{F}_q^{m \times N}$. It holds that

$$\varphi_N (C A^T + E) = \varphi_n(C) A^T + \varphi_N(E),$$

and $\text{Rk}_q(E) = \text{Rk}(\varphi_N(E))$ by definition.

**Proof.** The additive property of $\varphi_n$ is clear from the definition, so we may assume that $E = 0$. Denote the entries of $C$ and $\varphi_n(C)$ as in Definition and let $a_{v,j}, \tilde{c}_{i,j}$ and $\tilde{d}_{i,j}$ be the entries of $A, C A^T$ and $\varphi_N (C A^T)$, respectively, for $v = 1, 2, \ldots, N, i = 1, 2, \ldots, \alpha, l = 1, 2, \ldots, \alpha m$ and $j = 1, 2, \ldots, n$. It holds that

$$\tilde{c}_{i,j} = \sum_{v=1}^{n} c_{i,v} a_{j,v} = \sum_{v=1}^{n} \left( \sum_{u=1}^{m} d_{(i-1)m+u,v} \gamma_u \right) a_{j,v}$$

$$= \sum_{u=1}^{m} \left( \sum_{v=1}^{n} d_{(i-1)m+u,v} \right) a_{j,v},$$

but it also holds that

$$\tilde{c}_{i,j} = \sum_{u=1}^{m} \tilde{d}_{(i-1)m+u,j} \gamma_u,$$

for $i = 1, 2, \ldots, \alpha$ and $j = 1, 2, \ldots, n$. Since $\gamma_1, \gamma_2, \ldots, \gamma_m$ is a basis of $\mathbb{F}_q^m$ over $\mathbb{F}_q$ and $\sum_{v=1}^{n} d_{(i-1)m+u,v} a_{j,v} \in \mathbb{F}_q$, for $i = 1, 2, \ldots, \alpha$, and $j = 1, 2, \ldots, n$, we conclude that

$$\tilde{d}_{(i-1)m+u,j} = \sum_{v=1}^{n} d_{(i-1)m+u,v} a_{j,v},$$
for \( i = 1, 2, \ldots, \alpha, u = 1, 2, \ldots, m \) and \( j = 1, 2, \ldots, n \), which means that \( \varphi_N(CA^T) = \varphi_n(C)A^T \), and the result follows.

Hence we may identify the sets \( \mathbb{F}_q^{m \times n} \) and \( \mathbb{F}_q^{n \times m} \), seen as \( \mathbb{F}_q \)-linear vector spaces together with the metric given by the rank and the function \( R(\mathbb{F}_q) \), respectively. We will do this repeatedly throughout the paper.

To conclude the section, we recall the construction of coset coding schemes in [16, Def. 4] based on pairs of \( \mathbb{F}_q^m \)-linear codes with \( \alpha = 1 \) (no subpacketization).

**Definition 5 (Nested coset coding schemes [16])**. A nested coset coding scheme (with \( \alpha = 1 \)) is a coset coding scheme such that \( C_2 = \varphi(S) + C_1 \), where \( C_2 \subseteq C_1 \subseteq \mathbb{F}_q^n \) are \( \mathbb{F}_q^m \)-linear codes and \( \varphi : \mathbb{F}_q^m \rightarrow \mathcal{W} \) is a vector space isomorphism over \( \mathbb{F}_q \), for an \( \mathbb{F}_q^m \)-linear space \( \mathcal{W} \subseteq \mathbb{F}_q^n \) such that \( C_1 = C_2 \oplus \mathcal{W} \), where \( \oplus \) denotes the direct sum of vector spaces.

To measure the reliability and security of these coding schemes, we need the concept of relative minimum rank distance, which is a particular case of [16, Def. 2]:

**Definition 6 (Relative minimum rank distance [16])**. Given \( \mathbb{F}_q^m \)-linear codes \( C_2 \subseteq C_1 \subseteq \mathbb{F}_q^n \), we define their relative minimum rank distance as

\[
d_R(C_1, C_2) = \min \{ R(\mathbb{F}_q)(e) \mid e \in C_1, e \notin C_2 \}.
\]

The minimum rank distance of a single code \( C \subseteq \mathbb{F}_q^n \) is defined as \( d_R(C) = d_R(C, \{0\}) \).

The next result, which follows directly from [16, Cor. 5 and Th. 4], gives the mentioned reliability and security performance of nested coset coding schemes. Recall that we denote by \( C^\perp \) the dual of an \( \mathbb{F}_q^m \)-linear code \( C \subseteq \mathbb{F}_q^n \) with respect to the usual \( \mathbb{F}_q^m \)-bilinear inner product in \( \mathbb{F}_q^n \).

**Lemma 2 ([16])**. Given \( \mathbb{F}_q^m \)-linear codes \( C_2 \subseteq C_1 \subseteq \mathbb{F}_q^n \), the nested coset coding scheme in Definition 5 is universally \( t \)-error and \( \rho \)-erasure-correcting if, and only if, \( 2t + \rho < d_R(C_1, C_2) \), and is universally secure under \( \mu \) observations if, and only if, \( \mu < d_R(C_1^\perp, C_2^\perp) \).

Observe that \( d_R(C_1) \leq d_R(C_1, C_2) \) and \( d_R(C_2^\perp) \leq d_R(C_2^\perp, C_1^\perp) \), hence the minimum rank distances of \( C_1 \) and \( C_2^\perp \) give sufficient conditions on the number of correctable errors and erasures and on the number of links that may be wire-tapped without information leakage, respectively.

### 3 Communication overheads in coherent linearized channels

In this section we formalize how, as in communication efficient secret sharing [2, 13, 24], if a coset coding scheme is able to correct \( t \) errors and \( \rho \) erasures, but \( d > n - \rho \) pieces of information are available (the rank of \( A \) is at least \( d \)), then we may reduce
the communication overhead from the channel to the receiver by making use of the additional \( d - n + \rho > 0 \) linearly independent rows of \( A \). Observe that only erasures, and not errors, are considered in the Hamming analog described in [2, 13, 24].

Let \( F : \mathbb{F}_q^{d \times \ell} \rightarrow \mathbb{F}_q^{\alpha m \times n} \) be a coset coding scheme, let \( A \in \mathbb{F}_q^{d \times n} \) be of rank \( d \) (if \( A \in \mathbb{F}_q^{N \times n} \) has rank \( d < N \), we may delete or ignore linearly dependent rows), let \( a_1, a_2, \ldots, a_d \in \mathbb{F}_q^n \) be its rows, and let \( E_{A,i} : \mathbb{F}_q^{\alpha m} \rightarrow \mathbb{F}_q^{\beta_i m} \) be preprocessing functions, where \( 1 \leq \beta_i \leq \alpha \), for \( i = 1, 2, \ldots, d \). We define their correction capability with respect to \( F \) as follows:

**Definition 7.** For a full-rank matrix \( A \in \mathbb{F}_q^{d \times n} \), the preprocessing functions \( E_{A,i} : \mathbb{F}_q^{\alpha m} \rightarrow \mathbb{F}_q^{\beta_i m} \), for \( i = 1, 2, \ldots, d \), are \( t \)-error-correcting with respect to the coset coding scheme \( F : \mathbb{F}_q^{\alpha m \times \ell} \rightarrow \mathbb{F}_q^{\alpha m \times n} \) if there exists a decoding function \( D_A : \prod_{i=1}^d \mathbb{F}_q^{\beta_i m} \rightarrow \mathbb{F}_q^{\alpha m \times \ell} \) such that

\[
D_A \left( \left( E_{A,i} \left( Ca_i^T + e_i \right) \right)_{i=1}^d \right) = S,
\]

(3)

for all \( C \in C_S \), all \( S \in \mathbb{F}_q^{\alpha m \times \ell} \) and all error matrices \( E \in \mathbb{F}_q^{\alpha m \times d} \) of rank at most \( t \) with columns \( e_1, e_2, \ldots, e_d \in \mathbb{F}_q^{\alpha m} \).

We define then the decoding bandwidth and communication overhead as \( q \)-analogs of those in [13 Def. 2]:

**Definition 8 (Decoding bandwidth and communication overhead).** For a full-rank matrix \( A \in \mathbb{F}_q^{d \times n} \) and functions \( E_{A,i} : \mathbb{F}_q^{\alpha m} \rightarrow \mathbb{F}_q^{\beta_i m} \), for \( i = 1, 2, \ldots, d \), we define their decoding bandwidth and communication overhead, respectively, as

\[
DB(A) = \frac{\sum_{i=1}^d \beta_i m}{\alpha m} = \sum_{i=1}^d \frac{\beta_i}{\alpha} \quad \text{and} \quad CO(A) = \sum_{i=1}^d \frac{\beta_i}{\alpha} - \ell.
\]

Thus, if a packet is a vector in \( \mathbb{F}_q^{\alpha m} \), then the decoding bandwidth is the amount (which need not be an integer due to the subpacketization) of packets that the receiver obtains, or needs to obtain, from the channel, and the communication overhead is the difference with respect to the original number of uncoded packets.

Observe that, fixing \( n \) and \( \ell \) (thus the information rate), we may only focus on communication overheads, since both behave equally.

To measure the quality of a coset coding scheme, we need the following two bounds. The first is given in [22 Th. 12] and can be seen as a \( q \)-analog of the bound in [13 Prop. 1], although considering also errors and not only erasures:

**Proposition 1 ([22]).** If the coset coding scheme \( F : \mathbb{F}_q^{\alpha m \times \ell} \rightarrow \mathbb{F}_q^{\alpha m \times n} \) is universally \( t \)-error and \( \rho \)-erasure-correcting, and universally secure under \( \mu \) observations, then

\[
\ell \leq n - 2t - \rho - \mu.
\]

Next we give a \( q \)-analog of the bound in [13 Th. 1], again adding the effect of errors, which was not considered in [13]:
Proposition 2. If the coset coding scheme \( F : \mathbb{F}_q^{am \times t} \rightarrow \mathbb{F}_q^{am \times n} \) is universally secure under \( \mu \) observations, then for a full-rank matrix \( A \in \mathbb{F}_q^{d \times n} \) and preprocessing functions \( E_{A,i} : \mathbb{F}_q^{am} \rightarrow \mathbb{F}_q^{\beta \times m}, \) for \( i = 1, 2, \ldots, d \), that are \( t \)-error-correcting with respect to \( F \), it holds that:

\[
\text{CO}(A) \geq \frac{\ell(2t + \mu)}{d - 2t - \mu},
\]

(5)

Proof. We may assume without loss of generality that \( \beta_1 \leq \beta_2 \leq \ldots \leq \beta_d \) as in the proof of [13, Th. 1].

First, we prove that the preprocessing functions \( E_{A,i} : \mathbb{F}_q^{am} \rightarrow \mathbb{F}_q^{\beta \times m} \), for \( i = 1, 2, \ldots, d - 2t \) are \( 0 \)-error-correcting with respect to \( F : \mathbb{F}_q^{am \times \ell} \rightarrow \mathbb{F}_q^{am \times n} \). If they were not, then there would exist \( C_1 \in C_{S_1} \) and \( C_2 \in C_{S_2} \), with \( S_1 \neq S_2 \), such that

\[
\left( E_{A,i} \left( C_1 a_i^T \right) \right)_{i=1}^{d-2t} = \left( E_{A,i} \left( C_2 a_i^T \right) \right)_{i=1}^{d-2t}.
\]

On the other hand, there exist \( e_i \in \mathbb{F}_q^m \) such that \( C_1 a_i^T + e_i = C_2 a_i^T \), for \( i = d - 2t + 1, d - 2t + 2, \ldots, d - t \), and \( C_1 a_i^T = C_2 a_i^T + e_i \), for \( i = d - t + 1, d - t + 2, \ldots, d \). Thus we see that the preprocessing functions \( E_{A,i} : \mathbb{F}_q^{am} \rightarrow \mathbb{F}_q^{\beta \times m} \), for \( i = 1, 2, \ldots, d \), cannot be \( t \)-error-correcting with respect to \( F \), which is a contradiction.

Next, defining \( f_i = E_{A,i} \left( C a_i^T \right) \), where \( C = F(S) \), for \( i = 1, 2, \ldots, d - 2t \) and \( S \in \mathbb{F}_q^{am \times \ell} \), we may prove exactly as in the proof of [13, Th. 1] that

\[
\sum_{i=1}^{d-2t} \frac{\beta_i}{\alpha} \geq \frac{\ell(d - 2t)}{d - 2t - \mu},
\]

(6)

and also

\[
\frac{\beta_{d-2t-\mu}}{\alpha} \geq \frac{\ell}{d - 2t - \mu}.
\]

(7)

Now using that \( \beta_{d-2t-\mu} \leq \beta_{d-2t-\mu+1} \leq \ldots \leq \beta_d \), and combining Equations (6) and (7), we conclude that

\[
\text{DB}(A) = \left( \sum_{i=1}^{d-2t} \frac{\beta_i}{\alpha} \right) + \left( \sum_{i=d-2t+1}^{d} \frac{\beta_i}{\alpha} \right) \geq \frac{\ell(d - 2t)}{d - 2t - \mu} + \frac{2t}{d - 2t - \mu} = \frac{\ell d}{d - 2t - \mu},
\]

and the bound on \( \text{CO}(A) \) follows by substracting \( \ell \) to this inequality. \( \square \)

4 A general construction based on linear rank-metric codes

In this section, given a nested coset coding scheme (Definition 5) able to correct \( t_0 \) errors and \( \rho_0 \) erasures, for fixed positive integers \( t_0 \) and \( \rho_0 \), and given an arbitrary set \( \mathcal{D} \subseteq [n - \rho_0, n] \) such that \( n - \rho_0 \in \mathcal{D} \) (in particular for \( \mathcal{D} = [n - \rho_0, n] \)), we construct a coset coding scheme able to correct \( t_0 \) errors and any \( n - d \) erasures with lower communication
overheads than the original scheme, for all $d \in D$. Moreover, both the original scheme and the modified one are universally secure under the same number of observations. The downside of the method is multiplying the packet length of the original coset coding scheme by a parameter $\alpha$, depending on the involved codes, to achieve the desired subpacketization. The main result of the section is the following:

**Theorem 1.** Take $\mathbb{F}_{q^m}$-linear codes $C_2 \subsetneq C_1 \subseteq \mathbb{F}_{q^m}^{n}$, a positive integer $\rho_0$ such that $\rho_0 < d_R(C_1, C_2)$, and choose any subset $D \subseteq [n - \rho_0, n]$ such that $n - \rho_0 \in D$. Denote $D = \{d_1, d_2, \ldots, d_h\}$, where $d_h = n - \rho_0 < d_{h-1} < \ldots < d_2 < d_1$, and assume that there exists a sequence of nested $\mathbb{F}_{q^m}$-linear codes

$$C_1 = C^{(h)} \subsetneq C^{(h-1)} \subsetneq \ldots \subsetneq C^{(2)} \subsetneq C^{(1)} \subseteq \mathbb{F}_{q^m}^{n}$$

such that

$$d_R\left(C^{(j)} \setminus C^{(j+1)}\right) \geq n - d_j + 1,$$

for $j = 1, 2, \ldots, h$. Define then $k_1 = \dim(C_1)$, $k_2 = \dim(C_2)$, $\ell = k_1 - k_2$, $\alpha_j = k^{(j)} - k_2$ for $j = 1, 2, \ldots, h$, and

$$\alpha = \text{LCM}(\alpha_1, \alpha_2, \ldots, \alpha_h).$$

There exists a coset coding scheme $F : \mathbb{F}_{q^m}^{\alpha \times \ell} \to \mathbb{F}_{q^m}^\alpha$ that is universally $t$-error and $\rho$-erasure-correcting if $2t + \rho < d_R(C_1, C_2)$, and is universally secure under $\mu$ observations if $\mu < d_R(C_2^{(1)}, C^{(1)}_1)$.

In addition, for any $d \in D$ and any full-rank matrix $A \in \mathbb{F}_q^{d \times n}$, there exist pre-processing functions $E_{A,i} : \mathbb{F}_{q^m}^\alpha \to \mathbb{F}_{q^m}^{d}$ for $i = 1, 2, \ldots, d$, which are $t$-error-correcting with respect to $F$, whenever $2t < d_R(C^{(j)}, C_2) - n + d$, and such that

$$\text{CO}(A) = \frac{\ell (d - k^{(j)} + k_2)}{k^{(j)} - k_2},$$

where $k^{(j)} = \dim(C^{(j)})$, for $j$ such that $d = d_j$.

### 4.1 Description of the construction for Theorem 1

Let the notation be as in Theorem 1 and take a generator matrix $G_2 \in \mathbb{F}_{q^m}^{k_2 \times n}$ of $C_2$ and a generator matrix $G_1 \in \mathbb{F}_{q^m}^{k_1 \times n}$ of $C_1$ of the form

$$G_1 = \begin{pmatrix} G_2 \\ G_c \end{pmatrix} \in \mathbb{F}_{q^m}^{k_1 \times n},$$

for some matrix $G_c \in \mathbb{F}_{q^m}^{k_2 \times n}$. Decreasingly in $j = h - 1, h - 2, \ldots, 2, 1$, take a generator matrix $G^{(j)} \in \mathbb{F}_{q^m}^{k^{(j)} \times n}$ of $C^{(j)}$ of the form

$$G^{(j)} = \begin{pmatrix} G^{(j+1)} \\ G_c^{(j)} \end{pmatrix} \in \mathbb{F}_{q^m}^{k^{(j)} \times n},$$

9
for some matrix $G^{(j+1)}_c \in \mathbb{F}_{q^m}^{(k^{(j)} - k^{(j+1)}) \times n}$. Next define the following positive integers, which are analogous to the integers defined in [13, Eq. (11)]:

$$p_j = \begin{cases} \frac{\ell_{\alpha}}{\alpha_1} \frac{\alpha_1}{\alpha_j} & \text{if } j = 1, \\ \frac{\ell_{\alpha}}{\alpha_j} & \text{if } 1 < j \leq h. \end{cases}$$

Let $S \in \mathbb{F}_{q^m}^{p \times \ell}$ be the secret message and generate uniformly at random a matrix $R \in \mathbb{F}_{q^m}^{p \times k_2}$. Divide $S$ and $R$ as follows:

$$S = \begin{pmatrix} S_1 \\ S_2 \\ \vdots \\ S_h \end{pmatrix}, \quad R = \begin{pmatrix} R_1 \\ R_2 \\ \vdots \\ R_h \end{pmatrix},$$

where

$$S_j \in \mathbb{F}_{q^m}^{p_j \times \ell} \quad \text{and} \quad R_j \in \mathbb{F}_{q^m}^{p_j \times k_2},$$

for $j = 1, 2, \ldots, h$. Next, we define the matrices

$$
\begin{align*}
M_1 &= (R_1 \quad S_1 \quad D_{1,1} \quad D_{1,2} \ldots \quad D_{1,h-1}), \\
M_2 &= (R_2 \quad S_2 \quad D_{2,1} \quad D_{2,2} \ldots \quad 0), \\
M_3 &= (R_3 \quad S_3 \quad D_{3,1} \quad D_{3,2} \ldots \quad 0), \\
&\vdots \\
M_{h-1} &= (R_{h-1} \quad S_{h-1} \quad D_{h-1,1} \quad 0 \ldots \quad 0), \\
M_h &= (R_h \quad S_h \quad 0 \quad 0 \ldots \quad 0),
\end{align*}
$$

where $M_u \in \mathbb{F}_{q^m}^{p_u \times k^{(1)}}$, and where the matrices $D_{u,v} \in \mathbb{F}_{q^m}^{p_u \times (\alpha_{h-v} - \alpha_{h-v+1})}$ are defined iteratively as follows: For $v = 1, 2, \ldots, h - 1$, the components of the $v$-th column block

$$\begin{pmatrix} D_{1,v} \\ D_{2,v} \\ \vdots \\ D_{h-v,v} \end{pmatrix} \in \mathbb{F}_{q^m}^{\ell_{\alpha}/(\alpha_{h-v} - \alpha_{h-v+1})},$$

are the components (after some fixed rearrangement) of

$$(S_{h-v+1}|D_{h-v+1,1}|D_{h-v+1,2}| \ldots |D_{h-v+1,v-1}),$$

whose size is $p_{h-v+1} \times \alpha_{h-v+1}$ (observe that $p_{j+1} \alpha_{j+1} = (\alpha_j - \alpha_{j+1}) \ell_{\alpha}/\alpha_j$). For convenience, we define the matrices

$$M'_j = \begin{pmatrix} M_1 \\ M_2 \\ \vdots \\ M_j \end{pmatrix} \in \mathbb{F}_{q^m}^{\ell_{\alpha}/\alpha_j \times k^{(1)}}, \quad (8)$$
for \( j = 1, 2, \ldots, h \).

Finally, we define the coset coding scheme \( F : \mathbb{F}_q^{\alpha \times \ell} \to \mathbb{F}_q^{\alpha \times n} \) by

\[
C = F(S) = M'G^{(1)} \in \mathbb{F}_q^{\alpha \times n}.
\] (9)

To conclude, we define \( E_{A,i} : \mathbb{F}_q^{\alpha} \to \mathbb{F}_q^{t\alpha/\alpha_j} \) as follows. For \( j = 1, 2, \ldots, h \), for \( i = 1, 2, \ldots, d_j \), and for a full-rank matrix \( A \in \mathbb{F}_q^{d_j \times n} \), we define \( E_{A,i}(y_i) \in \mathbb{F}_q^{t\alpha/\alpha_j} \) by restricting \( y_i \in \mathbb{F}_q^{\alpha} \) to its first \( t\alpha/\alpha_j \) rows.

4.2 Proof of Theorem 1

Let the notation be as in Theorem 1 and as in the previous subsection. We prove each statement in Theorem 1 separately:

1) The coset coding scheme is universally \( t \)-error and \( \rho \)-erasure-correcting if \( 2t + \rho < d_R(C_1,C_2) \): Take \( A \in \mathbb{F}_q^{N \times n} \) of rank at least \( n - \rho \) and an error matrix \( E \in \mathbb{F}_q^{\alpha \times N} \) such that \( \text{Rk}_q(E) \leq t \). Divide \( E \) in the same way as \( S \) and \( R \), that is,

\[
E = \begin{pmatrix}
E_1 \\
E_2 \\
\vdots \\
E_h
\end{pmatrix} \in \mathbb{F}_q^{\alpha \times N},
\]

where \( E_j \in \mathbb{F}_q^{\alpha \times N} \), and observe that \( \text{Rk}_q(E_j) \leq \text{Rk}_q(E) \leq t \), for \( j = 1, 2, \ldots, h \). From

\[
(S_h|R_h|0)G^{(1)}A^T + E_h = (S_h|R_h)G_1A^T + E_h
\]

we obtain \( S_h \) by Lemma 2 since \( \text{Rk}_q(E_h) \leq t \) and \( 2t + \rho < d_R(C_1,C_2) \). By definition, we have obtained \( D_{u,1} \), for \( u = 1, 2, \ldots, h - 1 \). Hence substracting \( D_{u-1,1}C_1^{(h)}A^T \) from \( (S_h-1|R_{h-1}|D_{h-1,1}|0)G^{(1)}A^T + E_{h-1} \), we may obtain \( (S_h-1|R_{h-1})G_1A^T + E_{h-1} \), and thus we obtain \( S_{h-1} \) again by Lemma 2. Now, we have also obtained \( D_{u,2} \), for \( u = 1, 2, \ldots, h - 2 \). Proceeding iteratively in the same way, we see that we may obtain all the matrices \( S_j \), for \( j = 1, 2, \ldots, h \), and thus we obtain the whole message \( S \).

2) The coset coding scheme is universally secure under any \( \mu < d_R(C_2^+,C_1^+) \) observations: We first need the following preliminary lemma, which follows from [15] Th. 3:

**Lemma 3.** Let \( B \in \mathbb{F}_q^{n \times n} \) and let \( C_2 \subseteq \supseteq C_1 \subseteq \mathbb{F}_q^{m} \) be \( \mathbb{F}_q^{m} \)-linear codes. If \( \text{Rk}(B) < d_R(C_2^+,C_1^+) \), then

\[
C_2B^T = C_1B^T,
\]

where \( CB^T = \{cB^T \mid c \in C \} \subseteq \mathbb{F}_q^{\mu} \), for a code \( C \subseteq \mathbb{F}_q^{\mu} \).

**Proof.** See Appendix A.  \( \square \)
Take $B \in \mathbb{F}_q^{\alpha \times n}$, and assume that the eavesdropper obtains

$$W = CB^T = M_i G^{(1)} B^T \in \mathbb{F}_q^{\alpha \times \mu}.$$  

The random variable $W$ has support inside the $\mathbb{F}_q$-linear vector space

$$C^{(1)}_{B,\alpha} = \{ MG^{(1)} B^T \mid M \in \mathbb{F}_q^{\alpha \times k^{(1)}} \} \subseteq \mathbb{F}_q^{\alpha \times \mu}.$$  

Recall from [3, Th. 2.6.4] that, if a random variable $X$ has support in the set $\mathcal{X}$, then $H(X) \leq \log_q(\#\mathcal{X})$. Hence

$$H(W) \leq \log_q \left( \#C^{(1)}_{B,\alpha} \right) = m \dim(C^{(1)}_{B,\alpha}) = \alpha m \dim(C^{(1)} B^T),$$

where dimensions are taken over $\mathbb{F}_q$. On the other hand, using the analogous notation $C_{2B,\alpha}$ for $C_2$ instead of $C^{(1)}$, it holds that

$$H(W \mid S) = \log_q \left( \#C_{2B,\alpha} \right) = m \dim(C_{2B,\alpha}) = \alpha m \dim(C_{2B} B^T),$$

since, given a value of $S$, the variable $W$ is a uniform random variable over an $\mathbb{F}_q$-linear affine space obtained by translating the vector space $C_{2B,\alpha}$. Hence we obtain that

$$0 \leq I(S; W) = H(W) - H(W \mid S) \leq \alpha m \left( \dim(C_{2B} B^T) - \dim(C_{2B} B^T) \right) = 0,$$

where the last equality follows from Lemma [3]. Thus $I(S; W) = 0$ and we are done.

3) The preprocessing functions are $t$-error-correcting for any $2t < d_R(C^{(j)}, C_2) - n + d$, where $d = d_j$: Fix $d \in D$ and a full-rank matrix $A \in \mathbb{F}_q^{d \times n}$, and let $E_{A,i} : \mathbb{F}_q^m \rightarrow \mathbb{F}_q^{\alpha / \alpha_j}$ be preprocessing functions as in the previous subsection, for $i = 1, 2, \ldots, d$, and where $j$ is such that $d = d_j$.

Let $E \in \mathbb{F}_q^{\alpha \times d}$ be an error matrix such that $\text{Rk}_q(E) \leq t$, and let $e_1, e_2, \ldots, e_d \in \mathbb{F}_q^\alpha$ be its columns. By definition, $E_{A,i} (Ca^T + e_i)$ is the $i$-th column of

$$M_j' G^{(1)} A^T + E_j' \in \mathbb{F}_q^{\alpha / \alpha_j \times d},$$

for $i = 1, 2, \ldots, d$, and a submatrix $E_j' \in \mathbb{F}_q^{\alpha / \alpha_j \times d}$ of $E$, which thus satisfies that $\text{Rk}_q(E_j') \leq \text{Rk}_q(E) \leq t$. Therefore, we may obtain the matrix $M_j'$ as in item 1, since $2t + n - d < d_R(C^{(j)}, C_2)$. By definition, the matrices $S_1, S_2, \ldots, S_j$ are contained in $M_j'$. Moreover, the matrices $D_1, h, j, D_2, h, j, \ldots, D_j, h, j$ are also contained in $M_j'$, and from them we obtain by definition $S_{j+1}$ and $D_{j+1,1}, D_{j+1,2}, \ldots, D_{j+1,h, j}$. Now, the matrices $D_{1, h-j-1}, D_{2, h-j-1}, \ldots, D_{j, h-j-1}$ are contained in $M_j'$ and we also have $D_{j+1,h-j-1}$, hence we may obtain by definition $S_{j+2}$ and $D_{j+2,1}, D_{j+2,2}, \ldots, D_{j+2,h-j-2}$. Continuing iteratively in this way, we may obtain all $S_1, S_2, \ldots, S_h$ and hence the message $S$.

Finally, we have that

$$\text{CO}(A) = \sum_{i=1}^{d} \frac{\beta_i}{\alpha} - \ell = \sum_{i=1}^{d} \frac{\ell \alpha}{\alpha_j \alpha} - \ell = \ell d - \ell \frac{(\ell \alpha_j)}{\alpha_j} = \ell \left( \frac{(d - \alpha_j) + k_2}{\ell j} - k_2 \right).$$
5 MRD codes and coset coding schemes with optimal communication overheads

In this section, we apply Theorem 1 to pairs of Gabidulin codes [8, 21] and their cartesian products [7]. The first family yields optimal coset coding schemes when \( n \leq m \) in the sense of (4) and (5), and the second family constitutes a family of maximum rank distance (MRD) codes when \( n > m \) [7, Cor. 1].

We recall the definition of MRD codes for convenience of the reader. The Singleton bound for an arbitrary (linear or not) code \( C \subseteq \mathbb{F}_q^n \) was first given in [4, Th. 6.3]:

\[
\#C \leq q^{\max\{m,n\} - \min\{m,n\} + d_R(C) + 1}.
\]

We then say that \( C \) is MRD if equality holds in (10). In another direction, a Singleton bound on the relative minimum rank distance of a pair of \( \mathbb{F}_q^m \)-linear codes \( C_2 \subseteq C_1 \subseteq \mathbb{F}_q^n \) was first given in [16, Prop. 3]:

\[
d_R(C_1, C_2) \leq \min \left\{ n - \dim(C_1), \frac{m(n - \dim(C_1))}{n - \dim(C_2)} \right\} + 1.
\]

Thus if \( C_1 \) is MRD and \( n \leq m \), then equality is satisfied in (11).

5.1 Coset coding schemes based on Gabidulin codes

In this subsection we will make use of Gabidulin codes, which were introduced independently in [8, Sec. 4] and [21, Sec. III]. Throughout this subsection, we will assume that \( n \leq m \).

Definition 9 ([8, 21]). Fix a basis \( \gamma_1, \gamma_2, \ldots, \gamma_m \) of \( \mathbb{F}_q^m \) as a vector space over \( \mathbb{F}_q \), and let \( 0 \leq k \leq n \). The Gabidulin code of dimension \( k \) and length \( n \) over \( \mathbb{F}_q^m \), constructed from the previous basis, is the \( \mathbb{F}_q^m \)-linear code \( G_k \subseteq \mathbb{F}_q^n \) with parity-check matrix given by

\[
\begin{pmatrix}
\gamma_1 & \gamma_2 & \gamma_3 & \cdots & \gamma_n \\
\gamma_1^q & \gamma_2^q & \gamma_3^q & \cdots & \gamma_n^q \\
\gamma_1^{q^2} & \gamma_2^{q^2} & \gamma_3^{q^2} & \cdots & \gamma_n^{q^2} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\gamma_1^{q^{n-k-1}} & \gamma_2^{q^{n-k-1}} & \gamma_3^{q^{n-k-1}} & \cdots & \gamma_n^{q^{n-k-1}}
\end{pmatrix}
\in \mathbb{F}_{q^m}^{(n-k) \times n}.
\]

It was proven in [8, Th. 6] and [21, Th. 2] that the code \( G_k \subseteq \mathbb{F}_q^n \) satisfies

\[
\dim(G_k) = k, \quad \text{and} \quad d_R(G_k) = n - k + 1,
\]

constituting thus a family of MRD codes covering all parameters when \( n \leq m \). Moreover it is clear from the definition that, for a fixed basis of \( \mathbb{F}_q^m \) over \( \mathbb{F}_q \), they form a nested sequence of codes:

\[
\{0\} = G_0 \subsetneq G_1 \subsetneq G_2 \subsetneq \cdots \subsetneq G_{n-1} \subsetneq G_n = \mathbb{F}_q^n.
\]

Thus the next theorem follows directly from Theorem 1.
Theorem 2. Choose integers \( k_2, k_1, t_0 \) and \( \rho_0 \) such that \( 0 \leq k_2 < k_1 \leq n \) and \( 2t_0 + \rho_0 = n - k_1 \), and choose any subset \( \mathcal{D} \subseteq [n - \rho_0, n] \) such that \( n - \rho_0 \in \mathcal{D} \).

Now, fix a basis of \( \mathbb{F}_{q^m} \) over \( \mathbb{F}_q \), let \( \mathcal{C}_2 \subseteq \mathcal{C}_1 \subseteq \mathbb{F}_{q^m} \) be \( \mathbb{F}_{q^m} \)-linear Gabidulin codes of dimensions \( k_2 \) and \( k_1 \) (that is, \( \mathcal{G}_{k_2} \) and \( \mathcal{G}_{k_1} \), respectively), and denote the elements in \( \mathcal{D} \) by \( d_h = n - \rho_0 < d_{h-1} < \ldots < d_2 < d_1 \).

The coset coding scheme \( F : \mathbb{F}_{q^m}^{\alpha_1} \rightarrow \mathbb{F}_{q^m}^{\alpha_2} \) in Theorem 4 based on this pair of codes and the subsequence of \( \mathcal{B} \) given by the Gabidulin codes \( \mathcal{C}^{(j)} = \mathcal{G}_{d_j - 2t_0} \), that is, \( k^{(j)} = d_j - 2t_0 \), for \( j = 1, 2, \ldots, h \), satisfies \( \ell = k_1 - k_2 \), is universally \( \ell \)-error and \( \rho \)-erasures-correcting if \( 2t + \rho \leq n - k_1 \), and is universally secure under \( \mu \) observations if \( \mu \leq k_2 \). In particular, the scheme is optimal in the sense of (4). Moreover, it holds that

\[
\alpha = \text{LCM}(d_1 - 2t_0 - k_2, d_2 - 2t_0 - k_2, \ldots, d_h - 2t_0 - k_2).
\]

In addition, for any \( d \in \mathcal{D} \) and any full-rank matrix \( A \in \mathbb{F}_q^{d \times n} \), there exist preprocessing functions \( E_{A, i} : \mathbb{F}_{q^m}^\alpha \rightarrow \mathbb{F}_q^{\alpha m/(d - 2t_0 - k_2)} \), for \( i = 1, 2, \ldots, d \), which are \( t_0 \)-error-correcting and satisfying equality in (3), hence having optimal communication overheads for all \( d \in \mathcal{D} \).

Observe that the packet length \( m \) of the original Gabidulin codes is multiplied by \( \alpha \), which depends only on the maximum number of observations, the number of correctable errors and the set of possible erasures \( \mathcal{D} \).

However, there are instances as Example 1 where, due to a particular subpacketization, we need not expand the packet length, hence we obtain a strict improvement on the communication overheads at no cost on the rest of the parameters.

We now give the details of Example 1 and Example 2, which share the same construction: With the given parameters, the construction in [22, Th. 11] gives \( \ell = 16 \) by choosing \( k_1 = 24 \) and \( k_2 = 8 \). However, decomposing the packet length as \( \alpha m = 2048 \), with \( m = 64 \) and \( \alpha = 32 \), we may choose \( \mathcal{D} = \{24, 40\} \), \( k^{(1)} = 40 \), \( k_1 = 24 \) and \( k_2 = 8 \), thus \( \alpha_1 = 32, \alpha_2 = 16 \), and \( \alpha = 32 \), and the example follows.

5.2 Coset coding schemes based on MRD cartesian products

In this subsection, we will make use of cartesian products of Gabidulin codes, which yield again MRD codes, but in the case \( n > m \), in contrast with plain Gabidulin codes as in the previous subsection. To the best of our knowledge, this is the only known family of MRD \( \mathbb{F}_{q^m} \)-linear codes in \( \mathbb{F}_{q^m}^n \) when \( n > m \).

Throughout this subsection, we will assume that \( n = ln \), for some positive integer \( l \). Take another integer \( 1 \leq k \leq m \), and consider the cartesian product

\[
\mathcal{C} = \mathcal{G}_k^l \subseteq \mathbb{F}_{q^m}^n,
\]

where \( \mathcal{G}_k \subseteq \mathbb{F}_{q^m} \) is a Gabidulin code as in Definition 9. It is proven in [7, Cor. 1] that

\[
\dim(C) = lk, \quad \text{and} \quad d_R(C) = m - k + 1, \quad (14)
\]
and therefore \( C \) is MRD. Since the codes \( G_{k} \) can be taken in a nested sequence for a fixed basis of \( \mathbb{F}_{q^{m}} \) over \( \mathbb{F}_{q} \), as in Equation (13), the next result also follows directly from Theorem 1.

**Theorem 3.** Choose integers \( k_1, k_2, t_0 \) and \( \rho_0 \) such that \( 0 \leq k_2 < k_1 \leq m \) and \( 2t_0 + \rho_0 = m - k_1 \), and choose any subset \( D \subseteq [n - \rho_0, n] \) with elements \( d_h = n - \rho_0 < d_{h-1} < \ldots < d_2 < d_1 \).

Define \( k^{(j)} = d_j - (l - 1)m - 2t_0 \) and the \( \mathbb{F}_{q^m} \)-linear codes

\[
C_2 = G_{k_2}^{l}, \quad C^{(j)} = G_{k^{(j)}}^{l} \subseteq \mathbb{F}_{q^m},
\]

for \( j = 1, 2, \ldots, h \), and observe that \( k^{(h)} = k_1 \), hence \( C^{(h)} = C_1 = G_{k_1}^{l} \).

The coset coding scheme \( F : \mathbb{F}_{q^m}^{d \times \ell} \rightarrow \mathbb{F}_{q^m}^{n \times n} \) in Theorem 1 based on these codes satisfies \( \ell = l(k_1 - k_2) \), is universally \( t \)-error and \( \rho \)-erasure-correcting if \( 2t + \rho < m - k_1 \), and is universally secure under \( \mu \) observations if \( \mu \leq k_2 \). Moreover, it holds that

\[
\alpha = \text{LCM} \{l(d_j - 2t_0 - k_2) - (l - 1)n \mid j = 1, 2, \ldots, h\}.
\]

In addition, for any \( d \in D \) and any full-rank matrix \( A \in \mathbb{F}_{d \times n} \), there exist preprocessing functions \( E_{A,i} : \mathbb{F}_{q^m}^{d} \rightarrow \mathbb{F}_{q^{d \times m}}^{l(d - 2t_0 - k_2) - (l - 1)n} \), for \( i = 1, 2, \ldots, d \), which are \( t_0 \)-error-correcting and such that

\[
\text{CO}(A) = \frac{\ell(l(2t_0 + k_2) + (l - 1)(n - d))}{l(d - 2t_0 - k_2) - (l - 1)n}.
\]

Observe that the particular case \( l = 1 \) corresponds to the particular case \( n = m \) in Theorem 2.

### 6 Applications

#### 6.1 Universal secure linear network coding

Consider a network with \( n \) outgoing links from a source and \( N \) ingoing links to a sink, and where the source wants to transmit \( \ell \) packets, encoded into \( n \) packets (all of the same length), to the sink. Linear network coding, introduced in \([1,15,17]\), consists in sending linear combinations over \( \mathbb{F}_q \) of the received packets at each node of the network, which increases throughput with respect to storing and forwarding.

In this scenario, link errors and erasures expand through the network and an eavesdropper may obtain linear combinations of the sent packets. Thus if the coefficients of the final linear combinations are known to the receiver, then a linearly coded network, with link errors, erasures and observations, can be modelled as a coherent linearized noisy wire-tap channel \([22]\), as in Definition 1.

Assume that the packet length is at least \( n \), and fix positive integers \( t, \rho \) and \( \mu \) with \( 2t + \rho + \mu < n \) and \( \rho \leq N \). In \([22]\) Th. 11 a construction (pairs of Gabidulin codes) is given such that \( \ell = n - 2t - \rho - \mu \), which is optimal due to \([4]\).
However, assuming that $q$ is big enough and the erasure matrix $A \in \mathbb{F}_q^{N \times n}$ (see Definition 1) is taken at random as in [11], then it will be full-rank with high probability and $\rho$ can be thought of as a number of erased ingoing links to the sink, due to noise, link failure or the action of the adversary.

Theorem 2 gives an alternative construction to [22, Th. 11] with optimal $\ell = n - 2t - \rho - \mu$, where if more than $n - \rho$ ingoing links to the sink are available, the sink can contact the corresponding nodes after exchanging feedback on the number of available nodes, and reduce the communication overhead (hence the amount of packets received by the sink) to its optimal value in view of (5).

6.2 Secure distributed storage with crisscross errors and erasures

Errors and erasures occurring along several rows and/or columns of a matrix over $\mathbb{F}_q$ are called **crisscross errors and erasures** in the literature, and can happen in memory chips and magnetic tapes, for instance (see [21]). Recently, crisscross error and erasure-correction has gained attention in the context of distributed storage where data is stored in several data centers (columns), which in turn store several blocks of data (rows), where mixed and/or correlated failures may occur (see [14]).

In this work, we consider a storage system where data is stored as an $\alpha m \times n$ matrix over $\mathbb{F}_q$, where columns are thought of as data centers that are contacted to obtain information from, and rows are blocks of data expanding across the different data centers and sharing correlated errors. More formally, we consider column erasures (equivalently, data centers being available and contacted) together with crisscross errors and where an eavesdropper may listen to a number of columns (data centers).

We formalize crisscross error-correction in the following definitions, which we take from [21, Sec. 1]:

**Definition 10 (Crisscross weights [21]).** A cover of a matrix $E \in \mathbb{F}_{q}^{\alpha m \times n}$ is a pair of sets $X \subseteq [\alpha m]$ and $Y \subseteq [n]$ such that if $e_{i,j} \neq 0$, then $i \in X$ or $j \in Y$. We then define the crisscross weight of $E$ as

$$\text{wt}_c(E) = \min \{ \#X + \#Y \mid (X, Y) \subseteq [\alpha m] \times [n] \text{ is a cover of } E \}.$$  \hfill (15)

We may then formalize crisscross error and erasure-correction, together with security, as follows:

**Definition 11.** For a subset $I \subseteq [n]$, define the matrix $P_I \in \mathbb{F}_q^{\#I \times n}$ as that constituted by the rows of the $n \times n$ identity matrix indexed by $I$. We say that the coset coding scheme $F : \mathbb{F}_q^{\alpha m \times \ell} \rightarrow \mathbb{F}_q^{\alpha m \times n}$ is:

1. Crisscross $t$-error and $\rho$-erasure-correcting if, for every $I \subseteq [n]$ with $\#I = n - \rho$, there exist a decoding function $D_I : \mathbb{F}_q^{\alpha m \times (n-\rho)} \rightarrow \mathbb{F}_q^{\alpha m \times \ell}$ such that

$$D_I \left( C P_I^T + E \right) = S,$$

for all $C \in \mathcal{C}_S$, all $E \in \mathbb{F}_q^{\alpha m \times (n-\rho)}$ with $\text{wt}_c(E) \leq t$, and all $S \in \mathbb{F}_q^{\alpha m \times \ell}$.  

16
2. Secure under $\mu$ column-observations if

$$H(W \mid S) = H(S),$$

for any matrix $W \in \mathbb{F}_q^{\alpha m \times \mu}$ constituted by $\mu$ columns of $C = F(S)$, for all $S \in \mathbb{F}_q^{\alpha m \times \ell}$.

In this scenario, pieces of data correspond to columns, instead of linear combinations of columns, hence we will consider preprocessing functions $E_{I,i} : \mathbb{F}_q^{\alpha m} \rightarrow \mathbb{F}_q^{\beta_i m}$ depending on a subset of columns $I \subseteq [n]$, where $i \in I$. Hence we may formalize the crisscross error-correction capability of preprocessing functions as follows:

**Definition 12.** For a subset $I \subseteq [n]$ with $d = \#I$, the preprocessing functions $E_{I,i} : \mathbb{F}_q^{\alpha m} \rightarrow \mathbb{F}_q^{\beta_i m}$, for $i = 1, 2, \ldots, d$, are $t$-crisscross error-correcting with respect to $F$ if there exists a decoding function $D_I : \prod_{i=1}^d \mathbb{F}_q^{\beta_i m} \rightarrow \mathbb{F}_q^{\alpha m \times \ell}$ such that

$$D_I \left( (E_{I,i}(c_i + e_i))_{i=1}^d \right) = S,$$

where $C \in C_S$ and $c_i$ denotes the $i$-th column of $C$, for $i = 1, 2, \ldots, d$, for all $S \in \mathbb{F}_q^{\alpha m \times \ell}$ and all error matrices $E \in \mathbb{F}_q^{\alpha m \times d}$ of crisscross weight at most $t$ with columns $e_1, e_2, \ldots, e_d \in \mathbb{F}_q^{\alpha m}$.

The decoding bandwidth and communication overhead of such functions are defined as in Definition 8.

We now see that the bounds (4) and (5) also hold in this context:

**Proposition 3.** If the coset coding scheme $F : \mathbb{F}_q^{\alpha m \times \ell} \rightarrow \mathbb{F}_q^{\alpha m \times n}$ is crisscross $t$-error and $\rho$-erasure-correcting, and secure under $\mu$ column-observations, then

$$\ell \leq n - 2t - \rho - \mu.$$  \hspace{1cm} (17)

Moreover, for a subset $I \subseteq [n]$ with $d = \#I$ and preprocessing functions $E_{I,i} : \mathbb{F}_q^{\alpha m} \rightarrow \mathbb{F}_q^{\beta_i m}$, for $i = 1, 2, \ldots, d$, that are $t$-crisscross error-correcting with respect to $F$, it holds that:

$$\text{CO}(I) \geq \frac{\ell(2t + \mu)}{d - 2t - \mu}.$$ \hspace{1cm} (18)

**Proof.** Define $\rho' = \rho + 2t$. We will prove that $F$ is $\rho'$-crisscross erasure-correcting. If it is not, then there exists a subset $I \subseteq [n]$ with $\#I = n - \rho'$, and there exist $C_1 \in C_{S_1}$ and $C_2 \in C_{S_2}$, where $S_1 \neq S_2$, such that

$$C_1 P^T_I = C_2 P^T_I.$$

Next take a set of the form $I_1 = I \cup J_1 \cup J_2$, where $\#I_1 = n - \rho$ and $t = \#J_1 = \#J_2$ (recall that $n - \rho = n - \rho' + 2t$). There exist matrices $E_1, E_2 \in \mathbb{F}_q^{\alpha m \times (n - \rho)}$ of crisscross weight at most $t$ such that

$$C_1 P^T_{I_1} + E_1 = C_2 P^T_{I_1} + E_2.$$
Hence $F$ cannot be crisscross $t$-error and $\rho$-erasu re-correcting, and we reach a contradiction. Now, this implies that $F$ is a classical secret sharing scheme with alphabet $\mathbb{F}_q^{\alpha m}$, reconstruction $\rho'$ and privacy $\mu$. Thus it follows directly from [13, Th. 1] that

$$\ell \leq n - \rho' - \mu = n - \rho - 2t - \mu,$$

and we are done.

Finally, the bound (18) can be proven in the same way as the bound (14).

To conclude, we observe that a coset coding scheme, together with preprocessing functions, which are universally (rank) error and erasure-correcting and universally secure in the sense of Definitions 3 and 7 are also crisscross erasure and error-correcting and secure under a given number of column observations in the sense of Definitions 11 and 12, with exactly the same parameters. Thus all constructions in this paper can be directly translated into the context of this subsection.

For illustration purposes, we show how to translate Theorem 2 to this context, thus obtaining coset coding schemes which are optimal in the sense of (17) and (18) for all parameters, whenever $n \leq m$.

**Corollary 1.** Assume $n \leq m$, choose integers $k_2, k_1, t_0$ and $\rho_0$ such that $0 \leq k_2 < k_1 \leq n$ and $2t_0 + \rho_0 = n - k_1$, and choose any subset $D \subseteq [n - \rho_0, n]$ with elements $d_h = n - \rho_0 < d_{h-1} < \ldots < d_2 < d_1$.

The coset coding scheme $F : \mathbb{F}_q^{\alpha \times \ell} \rightarrow \mathbb{F}_q^{\alpha \times n}$ in Theorem 4 with these parameters satisfies $\ell = k_1 - k_2$, is crisscross $t_0$-error and $\rho_0$-erasu re-correcting if $2t_0 + \rho_0 \leq n - k_1$, and is secure under $\mu$ column-observations if $\mu \leq k_2$. In particular, the scheme is optimal in the sense of (17). Moreover, it holds that

$$\alpha = \text{LCM}(d_1 - 2t_0 - k_2, d_2 - 2t_0 - k_2, \ldots, d_h - 2t_0 - k_2).$$

In addition, for any $d \in D$ and any subset $I \subseteq [n]$ with $d = \#I$, there exist preprocessing functions $E_{I,i} : \mathbb{F}_q^{\alpha \times \ell} \rightarrow \mathbb{F}_q^{\alpha \times (d-2t_0-k_2)}$, for $i = 1, 2, \ldots, d$, which are $t_0$-crisscross error-correcting and satisfying equality in (18), hence having optimal communication overheads for all $d \in D$.

Observe that optimal crisscross error and erasure-correcting coding schemes can also be obtained by using maximum distance separable (MDS) codes in $\mathbb{F}_q^{\alpha \times n}$, by identifying this vector space with $\mathbb{F}_q^{\alpha m \times n}$, as noticed in [21]. However, such constructions may require extremely large finite fields, for instance $q > \alpha mn$ for Reed-Solomon codes, whereas rankmetric codes allow to obtain optimal coding schemes with the only constraint $n \leq m$, being $q$ unrestricted, allowing in particular using binary fields ($q = 2$).

7 Conclusion and open problems

In this paper, we have studied the problem of reducing the communication overhead on a noisy wire-tap channel or storage system where data is encoded as a matrix. The method
developed in Section 4 allows to reduce the communication overhead, when more columns are available, at the cost of expanding the packet length (number of rows). However, in the optimal case of pairs of Gabidulin codes (Section 5), strict improvements on the communication overheads are possible at no cost on the rest of the parameters, as shown in Example 1 for practical instances in the applications. We leave as open problem to study when the packet length need not be expanded. Another interesting open problem is to extend our method to codes that are linear over the base field $F_q$, instead of the extension field $F_{q^m}$. This would allow to use all possible MRD codes [4].

\section*{A Proof of Lemma 3}

Fix $F_{q^m}$-linear codes $C_2 \not\subseteq C_1 \subseteq F_{q^m}^n$ and a matrix $B \in F_{q^m}^{\mu \times n}$ in the rest of the appendix.

We start with an auxiliary result, which is a particular case of [18, Th. 3]:

\begin{lemma}[18] \label{lemma4}
It holds that
\begin{equation*}
    d_R(C_1, C_2) = \min \{ \rk(A) \mid A \in F_q^{\nu \times n}, \nu \in \mathbb{N}, \text{ and } \dim (C_1 \cap \Row(A)/C_2 \cap \Row(A)) \geq 1 \},
\end{equation*}
where $\Row(A) \subseteq F_{q^m}^n$ denotes the $F_{q^m}$-linear vector space generated by the rows of the matrix $A \in F_q^{\nu \times n}$.
\end{lemma}

Given an $F_{q^m}$-linear code $C \subseteq F_{q^m}^n$, consider the map $C \to CB^T$ defined by $c \mapsto cB^T$, for $c \in C$. It is surjective and its kernel is $C \cap (V^\perp)$, where $V = \Row(B)$. Therefore
\begin{equation*}
    \dim(C) = \dim(CB^T) + \dim \left( C \cap \left( V^\perp \right) \right).
\end{equation*}
Using this equation and computing dimensions, it follows that
\begin{equation*}
    \dim \left( C_1B^T/C_2B^T \right) = \dim \left( C_2^\perp \cap V/C_1^\perp \cap V \right). \quad (19)
\end{equation*}
Now, using that $\rk(B) < d_R(C_2^\perp, C_1^\perp)$ and the previous lemma, it holds that $C_2^\perp \cap V = C_1^\perp \cap V$. Hence the result follows by (19).

\section*{Acknowledgement}

The author gratefully acknowledges the support from The Danish Council for Independent Research (Grant No. DFF-4002-00367 and Grant No. DFF-5137-00076B “EliteForsk-Rejsestipendium”), and is thankful for the guidance of his advisors Olav Geil and Diego Ruano. This manuscript was written in part when the author was visiting the University of Toronto. He greatly appreciates the support and hospitality of Frank R. Kschischang, and is thankful for valuable discussions on this work.
References

[1] R. Ahlswede, N. Cai, S. Y. R. Li, and R. W. Yeung, “Network information flow,” *IEEE Trans. Inform. Theory*, vol. 46, no. 4, pp. 1204–1216, 2000.

[2] R. Bitar and S. E. Rouayheb, “Staircase codes for secret sharing with optimal communication and read overheads,” in *Proc. 2016 IEEE International Symposium on Information Theory (ISIT)*, 2016, pp. 1396–1400.

[3] T. M. Cover and J. A. Thomas, *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing), 2nd Edition*. Wiley-Interscience, 2006.

[4] P. Delsarte, “Bilinear forms over a finite field, with applications to coding theory,” *Journal of Combinatorial Theory, Series A*, vol. 25, no. 3, pp. 226–241, 1978.

[5] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, “Network coding for distributed storage systems,” *IEEE Trans. Inform. Theory*, vol. 56, no. 9, pp. 4539–4551, 2010.

[6] A. G. Dimakis, K. Ramchandran, Y. Wu, and C. Suh, “A survey on network codes for distributed storage,” *Proceedings of the IEEE*, vol. 99, no. 3, pp. 476–489, 2011.

[7] E. M. Gabidulin, A. V. Ourivski, B. Honary, and B. Ammar, “Reducible rank codes and their applications to cryptography,” *IEEE Trans. Inform. Theory*, vol. 49, no. 12, pp. 3289–3293, 2003.

[8] E. M. Gabidulin, “Theory of codes with maximum rank distance,” *Probl. Inf. Transm.*, vol. 21, no. 1, pp. 1–12, 1985.

[9] P. Gopalan, C. Huang, H. Simitci, and S. Yekhanin, “On the locality of codeword symbols,” *IEEE Trans. Inform. Theory*, vol. 58, no. 11, pp. 6925–6934, 2012.

[10] V. Guruswami and M. Wootters, “Repairing Reed-Solomon codes,” in *Proc. 48th Annual ACM Symposium on Theory of Computing*. ACM, 2016, pp. 216–226.

[11] T. Ho, M. Medard, R. Koetter, D. Karger, M. Effros, J. Shi, and B. Leong, “A random linear network coding approach to multicast,” *IEEE Trans. Inform. Theory*, vol. 52, no. 10, pp. 4413–4430, 2006.

[12] C. Huang, M. Chen, and J. Li, “Pyramid codes: Flexible schemes to trade space for access efficiency in reliable data storage systems,” in *Sixth IEEE International Symposium on Network Computing and Applications (NCA 2007)*, 2007, pp. 79–86.

[13] W. Huang, M. Langberg, J. Kliwer, and J. Bruck, “Communication efficient secret sharing,” *IEEE Trans. Inform. Theory*, vol. 62, no. 12, pp. 7195–7206, 2016.
[14] S. Kadhe, S. E. Rouayheb, I. Duursma, and A. Sprintson, “Rank-metric codes with local recoverability,” in Proc. 54th Annual Allerton Conference on Communication, Control, and Computing, 2016.

[15] R. Kötter and M. Medard, “An algebraic approach to network coding,” IEEE/ACM Trans. Networking, vol. 11, no. 5, pp. 782–795, Oct 2003.

[16] J. Kurihara, R. Matsumoto, and T. Uyematsu, “Relative generalized rank weight of linear codes and its applications to network coding,” IEEE Trans. Inform. Theory, vol. 61, no. 7, pp. 3912–3936, 2015.

[17] S. Y. Li, R. Yeung, and N. Cai, “Linear network coding,” IEEE Trans. Inform. Theory, vol. 49, no. 2, pp. 371–381, 2003.

[18] U. Martínez-Peñas, “On the similarities between generalized rank and Hamming weights and their applications to network coding,” IEEE Trans. Inform. Theory, vol. 62, no. 7, pp. 4081–4095, 2016.

[19] ——, “Universal secure rank-metric coding schemes with optimal communication overheads,” in Proc. 2017 IEEE International Symposium on Information Theory (ISIT), Jun 2017.

[20] K. V. Rashmi, N. B. Shah, and P. V. Kumar, “Optimal exact-regenerating codes for distributed storage at the msr and mbr points via a product-matrix construction,” IEEE Trans. Inform. Theory, vol. 57, no. 8, pp. 5227–5239, 2011.

[21] R. M. Roth, “Maximum-rank array codes and their application to crisscross error correction,” IEEE Trans. Inform. Theory, vol. 37, no. 2, pp. 328–336, 1991.

[22] D. Silva and F. R. Kschischang, “Universal secure network coding via rank-metric codes,” IEEE Trans. Inform. Theory, vol. 57, no. 2, pp. 1124–1135, 2011.

[23] I. Tamo and A. Barg, “A family of optimal locally recoverable codes,” IEEE Trans. Inform. Theory, vol. 60, no. 8, pp. 4661–4676, 2014.

[24] H. Wang and D. S. Wong, “On secret reconstruction in secret sharing schemes,” IEEE Trans. Inform. Theory, vol. 54, no. 1, pp. 473–480, 2008.