Unifying notions of generalized weights for universal security on wire-tap networks

Umberto Martínez-Peñas*1 and Ryutaroh Matsumoto2

1Department of Mathematical Sciences, Aalborg University, Denmark
2Department of Information and Communications Engineering, Tokyo Institute of Technology, Japan

Abstract

Universal security over a network with linear network coding has been intensively studied. However, previous linear codes used for this purpose were linear over a larger field than that used on the network. In this work, we introduce new parameters (relative dimension/rank support profile and relative generalized matrix weights) for linear codes that are linear over the field used in the network, measuring the universal security performance of these codes. The proposed new parameters enable us to use maximum rank distance linear codes for all possible parameters, as opposed to previous works, and also enable us to add universal security to the recently proposed list-decodable rank-metric codes by Guruswami et al. We give several properties of the new parameters: monotonicity, Singleton-type lower and upper bounds, a duality theorem, and definitions and characterizations of equivalences and degenerateness of linear codes. Finally, we show that our parameters strictly extend relative dimension/length profile and relative generalized Hamming weights, respectively, and relative dimension/intersection profile and relative generalized rank weights, respectively. The duality theorems for generalized Hamming weights and generalized rank weights can be deduced as special cases of the proposed duality theorem for generalized matrix weights. Moreover, generalized matrix weights are larger than Delsarte generalized weights.

Keywords: Network coding, rank weight, relative dimension/rank support profile, relative generalized matrix weight, universal secure network coding.

MSC: 15A03, 15B33, 94B05, 94C99.

1 Introduction

Linear network coding was first studied in [1] and [2], and allows to realize higher throughput than the conventional store-and-forward network. In this context, security over the network, meaning information leakage to a wire-tapping adversary, was first considered in [3]. The approach in [3] and later the approach in [10], allow to see the network case as a generalization of secret sharing, which is a generalization of the wire-tap channel of type II [29]. However, both approaches require knowing and/or modifying the underlying linear network code, which does not allow to perform, for instance, random linear network coding [17].

*umberto@math.aau.dk
The use of outer coding on the source node was proposed in [11] to protect messages from information leakage knowing but without modifying the underlying linear network code. Later, the use of linear (block) codes as outer codes was proposed in [33] to protect messages from errors together with information leakage to a wire-tapping adversary, depending only on the number of errors and wire-tapped links, and not depending on the underlying linear network code. In particular, optimal parameters are obtained in [33] for security over noiseless networks for some restricted packet lengths.

This approach was further investigated in [21], where relative generalized rank weights (RGRW) and relative dimension/intersection profile (RDIP) were introduced to measure simultaneously the security performance and correction capability of pairs of linear codes, which are used for coset coding as in [36].

Unfortunately, the codes proposed in [33] and [21] are linear over a finite field $\mathbb{F}_{q^m}$, where $m$ is the packet length, if the linear network coding is performed over the finite field $\mathbb{F}_q$. This restricts the achievable parameters, requires performing computations over the larger field $\mathbb{F}_{q^m}$ and leaves out important codes, such as the codes obtained in [16], which are the first list-decodable rank-metric codes whose list sizes are polynomial in the code length. Moreover, even though there exist maximum rank distance codes (see [6]) that can be applied for all number of outgoing links from the source, all packet lengths and all dimensions over $\mathbb{F}_q$, the maximum rank distance codes considered in [33] and [21] only include Gabidulin codes [13] and some reducible codes [14], for which the previous parameters are restricted.

In this work, we study the security performance of codes and coset coding schemes that are linear over the smaller field $\mathbb{F}_q$. In particular, our study includes all maximum rank distance codes that are linear over $\mathbb{F}_q$ [6] and allows to consider the list-decodable codes in [16].

By use of RGMWs, we obtain a construction of secure list-decodable rank-metric codes that allows to convey at least $(1 - 2\varepsilon)$ times the information sent by pairs of Gabidulin codes [21], for some $\varepsilon > 0$, offers at least the same security against information leakage and is able to list-decode roughly twice as many rank errors.

We propose two quantities of linear code pairs: their relative dimension/rank support profile (RDRP) and relative generalized matrix weight (RGMW), which exactly measure the worst case information leakage and correction capability. The RDRP strictly extend both the relative dimension/length profile (RDLP) [12, 24] and the relative dimension/intersection profile (RDIP) [21]. On the other hand, the RGMW strictly extend both relative generalized Hamming weights (RGHW) [24, 35] and relative generalized rank weights (RGRW) [21], and are larger (strictly in some cases) than Delsarte generalized weights [31].

We also study monotonicity of RDRP and RGMW, give Singleton-type upper and lower bounds and give a duality theorem relating the GMW of a linear code with those of its dual code. We prove that this duality theorem has as consequences the duality theorems for generalized Hamming weights [35] and generalized rank weights [8]. We then study vector space isomorphisms between linear codes and coset coding schemes that preserve security performance and obtain ranges of possible parameters and minimum parameters of linear codes up to these vector space isomorphism.

The organization of the paper is as follows. After some preliminaries in Section II, we introduce in Section III the main new parameters of nested linear code pairs (RDRP and RGMW) and give their monotonicity properties. In Section IV, we prove that RDRP and RGMW exactly measure the worst case information leakage on networks. Next we introduce matrix information distributions, information spaces and secrecy spaces. We conclude by giving optimal linear coset coding schemes for noiseless networks for all possible parameters, in contrast to previous works. In Section V, we show how to add universal security to the list-decodable codes in [16] using linear coset coding schemes and the study in the previous sections. In Section VI, we study
2 Coset coding schemes for universal security in linear network coding

2.1 Notation

Let \( q \) be a prime power and \( m \) and \( n \), two positive integers. We denote by \( F \) an arbitrary field and by \( \mathbb{F}_q \) the finite field with \( q \) elements. \( \mathbb{F}^n \) denotes the vector space of row vectors of length \( n \) with components in \( F \), and \( \mathbb{F}^{m \times n} \) denotes the vector space of \( m \times n \) matrices with components in \( F \). For a vector space \( V \) over \( F \) and a subset \( A \subseteq V \), we denote by \( \langle A \rangle \) the vector space generated by \( A \) over \( F \), and we denote by \( \dim(V) \) the dimension of \( V \) over \( F \). Finally, \( A^T \in \mathbb{F}^{n \times m} \) denotes the transposed of a matrix \( A \in \mathbb{F}^{m \times n} \), and the symbols + and \( \oplus \) denote the sum and direct sum of vector spaces, respectively.

Throughout the paper, a (block) code in \( \mathbb{F}^{m \times n} \) (respectively, in \( \mathbb{F}^n \)) is a subset of \( \mathbb{F}^{m \times n} \) (respectively, of \( \mathbb{F}^n \)), and it is called linear if it is a vector space.

2.2 Linear network coding model

Consider a network with several sources and several sinks. A given source transmits a message \( x \in \mathbb{F}_q^\ell \) through the network to multiple sinks. To that end, that source encodes the message as a collection of \( n \) packets of length \( m \), seen as a matrix \( C \in \mathbb{F}_q^{m \times n} \). We consider linear network coding on the network, first considered in [1, 22] and formally defined in [20, Definition 1], which allows to reach the network capacity. This means that a given sink receives a matrix of the form

\[
Y = CA^T \in \mathbb{F}_q^{m \times N},
\]

where \( A \in \mathbb{F}_q^{N \times n} \) is called the transfer matrix corresponding to the considered source and sink. This matrix may be randomly chosen if random linear network coding is applied [17].

2.3 Universal secure communication over networks

In secure or reliable network coding, two of the main problems addressed in the literature are the following:

1. Error and erasure correction [21, 32, 33]: An adversary and/or a noisy channel may introduce errors on some links of the network and/or modify the transfer matrix. In this case, the sink receives a matrix of the form

\[
Y = CA^T + E \in \mathbb{F}_q^{m \times N},
\]
where \( A' \in \mathbb{F}_{q}^{N \times n} \) is the modified transfer matrix, and \( E \in \mathbb{F}_{q}^{m \times N} \) is the final error matrix. In this case, we say that \( t = \text{Rk}(E) \) errors and \( \rho = n - \text{Rk}(A') \) erasures occurred, where \( \text{Rk} \) denotes the rank of a matrix.

2. Information leakage \([3, 10, 11, 21, 33]\): A wire-tapping adversary listens to \( \mu > 0 \) links of the network, obtaining a matrix of the form \( CB^T \in \mathbb{F}_{q}^{m \times \mu} \), for some matrix \( B \in \mathbb{F}_{q}^{\mu \times n} \). When considering information leakage, we assume that the messages sent by different sources have no correlations, since then they do not give information about each other on the network by \([21, \text{Proposition 5}]\).

The main tool used in the literature to tackle these problems is outer coding in the source node, as defined in the next subsection. Recall from \([33]\) that such outer codes are called “universal secure” if they provide security as in the previous items for fixed numbers of wire-tapped links \( \mu \), errors \( t \) and erasures \( \rho \), independently of the transfer matrix \( A \) used. This implies that no previous knowledge or modification of the transfer matrix is required and random linear network coding \([17]\) may be applied.

2.4 Coset coding schemes for outer codes

Coding techniques for protecting messages simultaneously from errors and information leakage to a wire-tapping adversary was first studied by Wyner in \([36]\). In \([36, \text{p. 1374}]\), the general concept of coset coding scheme, as we will next define, was first introduced for this purpose. We use the formal definition in \([21, \text{Definition 7}]\):

**Definition 1 (Coset coding schemes \([21, 36]\)).** A coset coding scheme over the field \( \mathbb{F} \) with message set \( S \) is a family of disjoint nonempty subsets of \( \mathbb{F}^{m \times n} \), \( \mathcal{P}_S = \{C_x\}_{x \in S} \).

**Definition 2 (Linear coset coding schemes \([26, \text{Definition 2}]\)).** A coset coding scheme as in the previous definition is said to be linear if \( S = \mathbb{F}^{\ell} \), for some \( 0 < \ell \leq mn \), and

\[
    aC_x + bC_y \subseteq C_{ax+by} ,
\]

for all \( a, b \in \mathbb{F} \) and all \( x, y \in \mathbb{F}^{\ell} \).

The encoding in the coset coding scheme is given in \([21, \text{Definition 7}]\) as follows: for each \( x \in S \), choose at random (with uniform distribution) an element \( C \in C_x \).

With these definitions, the concept of coset coding scheme generalizes the concept of (block) code, since a code is a coset coding scheme where \( \#C_x = 1 \), for each \( x \in S \). In the same way, linear coset coding schemes generalize linear (block) codes.

An equivalent way to describe linear coset coding schemes is by nested linear code pairs, introduced in \([37, \text{Section III.A}]\). We use the description in \([3, \text{Subsection 4.2}]\).

**Definition 3 (Nested linear code pairs \([4, 37]\)).** A nested linear code pair is a pair of linear codes \( C_2 \subsetneq C_1 \subseteq \mathbb{F}^{m \times n} \). Choose a vector space \( W \) such that \( C_1 = C_2 \oplus W \) and a vector space isomorphism \( \psi : \mathbb{F}^{\ell} \rightarrow W \), where \( \ell = \dim(C_1/C_2) \). Then we define the sets \( C_x = \psi(x) + C_2 \), for \( x \in \mathbb{F}^{\ell} \). They form a linear coding scheme called nested coset coding scheme \([21]\).

**Remark 1.** As observed in \([29]\), for the wire-tap channel of type II, linear code pairs of the form \( C \subseteq \mathbb{F}^{m \times n} \) are suitable for protecting information from leakage on noiseless channels.

We recall here that the concept of linear coding schemes and nested coset coding schemes are exactly the same. An object in the first family uniquely defines an object in the second family and vice versa. This is formally proven in \([26, \text{Proposition 1}]\).
Finally, we recall that the exact universal error and erasure correction capability of a nested coset coding scheme was found, in terms of the rank metric, first in [32, Section IV.C] for the case of one code that is maximum rank distance, then in [33, Theorem 2] for the general case of one linear code, then in [21, Theorem 4] for the case where both codes are linear over an extension field \(F_{q^m}\), and finally in [26, Theorem 9] for the general case (linear over \(F_q\) and non-linear).

3 New parameters of linear coset coding schemes for universal security on networks

3.1 Rank supports and matrix modules

It is already known in the literature [19, 21, 26] that the concept of support (or Hamming support) of a vector in classical coding theory corresponds in network coding to the concept of rank support or row space of a matrix. For both types of support, it is usual to attach a vector space. We recall this in the following definitions.

**Definition 4 (Row space and rank).** For a matrix \(C \in F_{m \times n}\), we define its row space \(\text{Row}(C)\) as the vector space in \(F^n\) generated by its rows. As usual, we define its rank as \(\text{Rk}(C) = \dim(\text{Row}(C))\).

**Definition 5 (Rank support and rank weight [19, Definition 1]).** Given a vector space \(C \subseteq F_{m \times n}\), we define its rank support as

\[
\text{RSupp}(C) = \sum_{C \subseteq \mathcal{V}} \text{Row}(C) \subseteq F^n.
\]

We also define the rank weight of the space \(C\) as

\[
\text{wt}_R(C) = \dim(\text{RSupp}(C)).
\]

Obviously, \(\text{RSupp}(\langle\{C\}\rangle) = \text{Row}(C)\) and \(\text{wt}_R(\langle\{C\}\rangle) = \text{Rk}(C)\), for every matrix \(C \in F_{m \times n}\).

**Definition 6 (Rank support spaces).** Given a vector space \(L \subseteq F^n\), we define its rank support space \(\mathcal{V}_L \subseteq F_{m \times n}\) as

\[
\mathcal{V}_L = \{ V \in F_{m \times n} | \text{Row}(V) \subseteq L \}.
\]

The following properties are straightforward:

**Lemma 1.** Let \(L \subseteq F^n\) be a vector space. The following hold:

1. \(\mathcal{V}_L\) is a vector space and the correspondence \(L \mapsto \mathcal{V}_L\) between subspaces of \(F^n\) and rank support spaces is a bijection with inverse \(\mathcal{V}_L \mapsto \text{RSupp}(\mathcal{V}_L) = L\).

2. If \(C \subseteq F_{m \times n}\) is a vector space and \(L = \text{RSupp}(C)\), then \(\mathcal{V}_L\) is the smallest rank support space containing \(C\).

Rank support spaces will prove to have very interesting algebraic properties. In particular, we will prove that they coincide with the family of left submodules of the left module \(F_{m \times n}\) over the (non-commutative) ring \(F_{m \times n}\). We recall these definitions for completeness:

**Definition 7 (Matrix modules).** We say that a set \(\mathcal{V} \subseteq F_{m \times n}\) is a matrix module if

1. \(V + W \in \mathcal{V}\), for every \(V, W \in \mathcal{V}\), and
2. \( MV \in \mathcal{V} \), for every \( M \in \mathbb{F}^{m \times m} \) and every \( V \in \mathcal{V} \).

We denote by \( M(\mathbb{F}^{m \times n}) \) the family of matrix modules in \( \mathbb{F}^{m \times n} \).

We may now prove the following characterizations:

**Theorem 1.** Fix a set \( \mathcal{V} \subseteq \mathbb{F}^{m \times n} \). The following are equivalent:

1. \( \mathcal{V} \) is a matrix module. That is, \( \mathcal{V} \in M(\mathbb{F}^{m \times n}) \).

2. \( \mathcal{V} \) is a rank support space. That is, there exists a subspace \( \mathcal{L} \subseteq \mathbb{F}^{n} \) such that \( \mathcal{V} = \mathcal{V}_\mathcal{L} \).

3. \( \mathcal{V} \) is linear and has a basis of the form \( B_{i,j} \), for \( i = 1, 2, \ldots, m \) and \( j = 1, 2, \ldots, k \), where there are vectors \( b_1, b_2, \ldots, b_k \in \mathbb{F}^{n} \) such that \( B_{i,j} \) has the vector \( b_j \) in the \( i \)-th row and the rest of its rows are zero vectors.

4. There exists a matrix \( B \in \mathbb{F}^{\mu \times n} \), for some positive integer \( \mu \), such that

\[
\mathcal{V} = \{ V \in \mathbb{F}^{m \times n} \mid VB^T = 0 \}.
\]

In addition, the relation between items 2, 3 and 4 is that \( b_1, b_2, \ldots, b_k \) are a basis of \( \mathcal{L} \), \( B \) is a (possibly not full-rank) parity check matrix of \( \mathcal{L} \) and \( \dim(\mathcal{L}) = n - \text{Rk}(B) \).

**Proof.** We prove the following implications:

- \( 1 \implies 2 \): It holds that \( \mathcal{V} \) is a vector space. Let \( \mathcal{L} = \text{RSupp}(\mathcal{V}) \), and take \( v \in \mathcal{L} \). There exist \( V_1, V_2, \ldots, V_s \in \mathcal{V} \) and \( v_j \in \text{Row}(V_j) \), for \( j = 1, 2, \ldots, s \), such that \( v = \sum_{j=1}^{s} v_j \).

  For fixed \( 1 \leq i \leq m \) and \( 1 \leq j \leq s \), it is well-known that there exists \( M_{i,j} \in \mathbb{F}^{m \times m} \) such that \( M_{i,j}V_j \) has \( v_j \) as its \( i \)-th row and the rest of its rows are zero vectors. Since \( \mathcal{V} \) is closed under sums of matrices, we conclude that \( \mathcal{V}_\mathcal{L} \subseteq \mathcal{V} \) and therefore both are equal.

- \( 2 \iff 3 \): Assume item 2 and let \( b_1, b_2, \ldots, b_k \) be a basis of \( \mathcal{L} \), and let \( B_{i,j} \) be as in item 3. It is immediate to see that \( \mathcal{V} = \langle \{ B_{i,j} \mid 1 \leq i \leq m, 1 \leq j \leq k \} \rangle \). The reversed implication follows in the same way by defining \( \mathcal{L} = \langle b_1, b_2, \ldots, b_k \rangle \subseteq \mathbb{F}^{n} \).

- \( 2 \implies 4 \): Let \( B \in \mathbb{F}^{\mu \times n} \) be a parity check matrix of \( \mathcal{L} \). That is, a generator matrix of the dual \( \mathcal{L}^⊥ \subseteq \mathbb{F}^{n} \). Then it holds by definition that \( \mathcal{V} \in \mathbb{F}^{m \times n} \) has all its rows in \( \mathcal{L} \) if, and only if, \( VB^T = 0 \). Hence the result follows.

- \( 4 \implies 1 \): Trivial.

The following immediate consequence follows:

**Corollary 1.** Given a subspace \( \mathcal{L} \subseteq \mathbb{F}^{n} \), it holds that

\[
\dim(\mathcal{V}_\mathcal{L}) = m \dim(\mathcal{L}).
\]

We conclude by studying the duality of matrix modules. We consider the following inner product in \( \mathbb{F}^{m \times n} \). See [30] for more details.
Definition 8 (Hilbert-Schmidt or trace product). Given matrices \( C, D \in \mathbb{F}^{m \times n} \), we define its Hilbert-Schmidt product, or trace product, as

\[
(C, D) = \text{Trace}(CD^T)
\]

\[
= \sum_{i=1}^{m} c_i \cdot d_i = \sum_{i=1}^{m} \sum_{j=1}^{n} c_{i,j} d_{i,j} \in \mathbb{F},
\]

where \( c_i \) and \( d_i \) are the rows of \( C \) and \( D \), respectively, and where \( c_{i,j} \) and \( d_{i,j} \) are their components, respectively.

Given a vector space \( \mathcal{C} \subseteq \mathbb{F}^{m \times n} \), we denote by \( \mathcal{C}^\perp \) its dual:

\[
\mathcal{C}^\perp = \{ D \in \mathbb{F}^{m \times n} \mid (C, D) = 0, \forall C \in \mathcal{C} \}.
\]

Observe that the trace product coincides with the usual inner product if we see \( \mathbb{F}^{m \times n} \) as the vector space of row vectors \( \mathbb{F}^{mn} \), and therefore all the well-known properties of duality and vector spaces of the usual inner product immediately hold for the trace product. For completeness, we list the following, which we will use throughout the paper. For linear codes \( \mathcal{C}, \mathcal{D} \subseteq \mathbb{F}^{m \times n} \), it holds that

\[
\dim(\mathcal{C}^\perp) = mn - \dim(\mathcal{C}), \quad \mathcal{C} \subseteq \mathcal{D} \iff \mathcal{D}^\perp \subseteq \mathcal{C}^\perp,
\]

\[
\mathcal{C}^\perp = \mathcal{C}, \quad (\mathcal{C} + \mathcal{D})^\perp = \mathcal{C}^\perp \cap \mathcal{D}^\perp, \quad (\mathcal{C} \cap \mathcal{D})^\perp = \mathcal{C}^\perp + \mathcal{D}^\perp.
\]

We also have the following:

**Proposition 1.** If \( \mathcal{V} \in M(\mathbb{F}^{m \times n}) \), then \( \mathcal{V}^\perp \in M(\mathbb{F}^{m \times n}) \). More concretely, for any subspace \( \mathcal{L} \subseteq \mathbb{F}^n \), it holds that

\[
\dim(\mathcal{V}^\perp) = mn - \dim(\mathcal{V}), \quad \mathcal{C} \subseteq \mathcal{D} \iff \mathcal{D}^\perp \subseteq \mathcal{C}^\perp,
\]

\[
\mathcal{C}^\perp = \mathcal{C}, \quad (\mathcal{C} + \mathcal{D})^\perp = \mathcal{C}^\perp \cap \mathcal{D}^\perp, \quad (\mathcal{C} \cap \mathcal{D})^\perp = \mathcal{C}^\perp + \mathcal{D}^\perp.
\]

**Proof.** By Theorem 1, we just need to prove the second statement. We see from the definitions that \( \mathcal{V}(\mathcal{L}^\perp) \subseteq (\mathcal{V}(\mathcal{L}))^\perp \). By computing dimensions and using (1) we see that both are equal. \( \square \)

Finally, we have the following straightforward extension of Forney’s dualities lemmas [12, Lemmas 1 and 2]:

**Lemma 2 (Forney’s duality [12]).** Given vector spaces \( \mathcal{C}, \mathcal{V} \subseteq \mathbb{F}^{m \times n} \), it holds that

\[
\dim(\mathcal{V}) - \dim((\mathcal{C}^\perp) \cap \mathcal{V}) = \dim(\mathcal{C}) - \dim(\mathcal{C} \cap (\mathcal{V}^\perp)).
\]

### 3.2 New parameters of linear coset coding schemes

**Definition 9 (Relative Dimension/Rank support Profile).** Given nested linear codes \( \mathcal{C}_2 \subseteq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n} \), and \( 0 \leq \mu \leq n \), we define its \( \mu \)-th relative dimension/rank support profile (RDRP) as

\[
K_{M,\mu}(\mathcal{C}_1, \mathcal{C}_2) = \max \{ \dim(\mathcal{C}_1 \cap \mathcal{V}_L) - \dim(\mathcal{C}_2 \cap \mathcal{V}_L) \mid \mathcal{L} \subseteq \mathbb{F}^n, \dim(\mathcal{L}) \leq \mu \}.
\]

Observe that, since we are taking maximums, it holds that

\[
K_{M,\mu}(\mathcal{C}_1, \mathcal{C}_2) = \max \{ \dim(\mathcal{C}_1 \cap \mathcal{V}_L) - \dim(\mathcal{C}_2 \cap \mathcal{V}_L) \mid \mathcal{L} \subseteq \mathbb{F}^n, \dim(\mathcal{L}) = \mu \}.
\]
Definition 10 (Relative Generalized Matrix Weight). Given nested linear codes \( C_2 \subseteq C_1 \subseteq \mathbb{F}^{m \times n} \), and \( 1 \leq r \leq \ell = \dim(C_1/C_2) \), we define its \( r \)-th relative generalized matrix weight (RGMW) as

\[
d_{M,r}(C_1, C_2) = \min \{ \dim(L) \mid L \subseteq F^n, \\
\dim(C_1 \cap V_L) - \dim(C_2 \cap V_L) \geq r \}.
\]

In particular, for a linear code \( C \subseteq \mathbb{F}^{m \times n} \), and \( 1 \leq r \leq \dim(C) \), we define its \( r \)-th generalized matrix weight (GMW) as

\[
d_{M,r}(C) = d_{M,r}(C, \{0\}).
\]

Observe that it obviously holds that

\[
d_{M,r}(C_1, C_2) \geq d_{M,r}(C_1),
\]

for all nested linear codes \( C_2 \subseteq C_1 \subseteq \mathbb{F}^{m \times n} \), and all \( 1 \leq r \leq \ell = \dim(C_1/C_2) \).

We next obtain the following characterization of RGMW that gives an analogous description to the original definition of generalized Hamming weights by Wei [35]:

Theorem 2. Given nested linear codes \( C_2 \subseteq C_1 \subseteq \mathbb{F}^{m \times n} \), and an integer \( 1 \leq r \leq \dim(C_1/C_2) \), it holds that

\[
d_{M,r}(C_1, C_2) = \min \{ \wt_R(D) \mid D \subseteq C_1, D \cap C_2 = \{0\}, \\
\dim(D) = r \}.
\]

Proof. Denote by \( d_r \) the number on the left-hand side and by \( d'_r \) the number on the right-hand side. We prove both inequalities:

\( d_r \leq d'_r \): Take a vector space \( D \subseteq C_1 \) such that \( D \cap C_2 = \{0\} \), \( \dim(D) = r \) and \( \wt_R(D) = d'_r \). Define \( L = \text{RSupp}(D) \).

Since \( D \subseteq V_L \), we have that \( \dim((C_1 \cap V_L)/(C_2 \cap V_L)) \geq \dim((C_1 \cap D)/(C_2 \cap D)) = \dim(D) = r \).

Hence \( d_r \leq \dim(L) = \wt_R(D) = d'_r \).

\( d_r \geq d'_r \): Take a vector space \( L \subseteq \mathbb{F}^n \), such that \( \dim((C_1 \cap V_L)/(C_2 \cap V_L)) \geq r \) and \( \dim(L) = d_r \).

There exists a vector space \( D \subseteq C_1 \cap V_L \) with \( D \cap C_2 = \{0\} \) and \( \dim(D) = r \). We have that \( \text{RSupp}(D) \subseteq L \), since \( D \subseteq V_L \), and hence \( d_r = \dim(L) \geq \wt_R(D) \geq d'_r \).

\( \square \)

Thanks to this characterization, we may connect RGMW with the rank distance [6]. Recall the definition of minimum rank distance of a linear nested coset coding scheme, which is a particular case of [20, Equation (1)], and which is based on the analogous concept for the Hamming metric given in [9]:

\[
d_R(C_1, C_2) = \min \{ \text{Rk}(C) \mid C \in C_1, C \notin C_2 \}.
\]

The following result follows immediately from the previous theorem and the definitions:

Corollary 2 (Minimum rank distance of coding schemes). Given nested linear codes \( C_2 \subseteq C_1 \subseteq \mathbb{F}^{m \times n} \), it holds that

\[
d_R(C_1, C_2) = d_{M,1}(C_1, C_2).
\]

We now prove the connection between RDRP and RGMW, and their monotonicity properties:
Proposition 2 (Connection between RDRP and RGMW). Given nested linear codes $C_2 \subseteq C_1 \subseteq \mathbb{F}^{m \times n}$ and $1 \leq r \leq \dim(C_1/C_2)$, it holds that

$$d_{M,r}(C_1,C_2) = \min\{\mu \mid K_{M,\mu}(C_1,C_2) \geq r\}.$$  

Proof. It is proven as [21, Proof of Lemma 4].

Proposition 3 (Monotonicity of RDRP). Given nested linear codes $C_2 \subseteq C_1 \subseteq \mathbb{F}^{m \times n}$, and $0 \leq \mu \leq n - 1$, it holds that $K_{M,0}(C_1,C_2) = 0$, $K_{M,n}(C_1,C_2) = \dim(C_1/C_2)$ and

$$0 \leq K_{M,\mu+1}(C_1,C_2) - K_{M,\mu}(C_1,C_2) \leq m.$$

Proof. The only property that is not trivial from the definitions is $K_{M,\mu+1}(C_1,C_2) - K_{M,\mu}(C_1,C_2) \leq m$. Consider $L \subseteq \mathbb{F}^n$ with $\dim(L) \leq \mu + 1$ and $\dim(C_1 \cap V_L) - \dim(C_1 \cap V_{L'}) = K_{M,\mu+1}(C_1,C_2)$.

Take $L' \subseteq L$ with $\dim(L') = \dim(L) - 1$. Using [1], a simple computation shows that

$$\dim(C_1 \cap V_L) + m \geq \dim(C_1 \cap V_{L'}).$$

Since $\dim(C_1 \cap V_L') \leq \dim(C_1 \cap V_L)$, it holds that

$$\dim(C_1 \cap V_L) - \dim(C_1 \cap V_{L'}) + m \geq \dim(C_1 \cap V_L) - \dim(C_1 \cap V_{L}),$$

and the result follows.

Proposition 4 (Monotonicity of RGMW). Given nested linear codes $C_2 \subseteq C_1 \subseteq \mathbb{F}^{m \times n}$ with $\ell = \dim(C_1/C_2)$, it holds that

$$0 \leq d_{M,r+1}(C_1,C_2) - d_{M,r}(C_1,C_2) \leq \min\{m,n\},$$

for $1 \leq r \leq \ell - 1$, and

$$d_{M,r}(C_1,C_2) + 1 \leq d_{M,r+m}(C_1,C_2),$$

for $1 \leq r \leq \ell - m$.

Proof. The first inequality in the first equation is obvious. We now prove the second inequality. By Theorem 2, there exists a subspace $D \subseteq C_1$ with $D \cap C_2 = \{0\}$, $\dim(D) = r$ and $\text{wt}_R(D) = d_{M,r}(C_1,C_2)$. Now take $D \in C_1$ not contained in $D \oplus C_2$, and consider $D' = D \oplus \langle\{D\}\rangle$. We see from the definitions that $\text{RSupp}(D') \subseteq \text{RSupp}(D) + \text{Row}(D)$, and hence

$$\text{wt}_R(D') \leq \text{wt}_R(D) + \text{Rk}(D) \leq d_{M,r}(C_1,C_2) + \min\{m,n\}.$$  

Therefore it follows that $d_{M,r+1}(C_1,C_2) \leq d_{M,r}(C_1,C_2) + \min\{m,n\}$.

The last inequality follows from Proposition 2 and Proposition 3.

4 Universal security performance of linear coset coding schemes

4.1 Measuring information leakage on networks

In this subsection, we consider the problem of information leakage on the network, see Subsection 2.3, item 2.
Assume that a given source wants to convey the message $x \in \mathbb{F}_q^n$, which we assume is a random variable with uniform distribution over $\mathbb{F}_q^n$. Following Subsection 2.3, the source encodes $x$ into a matrix $C \in \mathbb{F}_q^{m \times n}$ using nested linear codes $C_2 \subsetneq C_1 \subseteq \mathbb{F}_q^{m \times n}$. We also assume that the distributions used in the encoding are all uniform (see Subsection 2.4).

According to the information leakage model in Subsection 2.3, item 2, a wire-tapping adversary obtains $CB^T \in \mathbb{F}_q^{m \times \mu}$, for some matrix $B \in \mathbb{F}_q^{\mu \times n}$.

Recall from [5] the definition of mutual information of two random variables $X$ and $Y$:

$$I(X; Y) = H(Y) - H(Y \mid X),$$

where $H(Y)$ denotes the entropy of $Y$ and $H(Y \mid X)$ denotes the conditional entropy of $Y$ given $X$, and where we take logarithms with base $q$ (see [5] for more details).

**Proposition 5.** Given nested linear codes $C_2 \subsetneq C_1 \subseteq \mathbb{F}_q^{m \times n}$, a matrix $B \in \mathbb{F}_q^{\mu \times n}$, and the uniform random variables $x$ and $CB^T$, as in the previous paragraphs, it holds that

$$I(x; CB^T) = \dim(C_1^\perp \cap V_L) - \dim(C_1 \cap V_L),$$

where $I(x; CB^T)$ is as in [2], and where $L = \text{Row}(B)$.

**Proof.** Define the map $f : \mathbb{F}_q^{m \times n} \rightarrow \mathbb{F}_q^{m \times \mu}$ given by

$$f(D) = DB^T,$$

for the matrix $B \in \mathbb{F}_q^{\mu \times n}$. Observe that $f$ is a linear map. It follows that

$$H(CB^T) = H(f(C)) = \log_q(\#f(C_1)) = \dim(f(C_1)) = \dim(C_1) - \dim(\ker(f) \cap C_1),$$

where the last equality is the well-known first isomorphism theorem. On the other hand, we may similarly compute the conditional entropy:

$$H(CB^T \mid x) = H(f(C) \mid x) = \log_q(\#f(C_2)) = \dim(f(C_2)) = \dim(C_2) - \dim(\ker(f) \cap C_2).$$

However, it holds that $\ker(f) = V_L^\perp \subseteq \mathbb{F}_q^{m \times n}$ by Theorem [1] since $B$ is a parity check matrix of $L^\perp$. Therefore

$$I(x; CB^T) = H(CB^T) - H(CB^T \mid x) = (\dim(C_1) - \dim(V_L \cap C_1)) - (\dim(C_2) - \dim(V_L \cap C_2)).$$

Finally, the result follows by Lemma [2] and Proposition [1].

The following theorem follows from the previous proposition and the definitions:

**Theorem 3 (Worst case information leakage).** Given nested linear codes $C_2 \subsetneq C_1 \subseteq \mathbb{F}_q^{m \times n}$, and integers $0 \leq \mu \leq n$ and $1 \leq r \leq \dim(C_1/C_2)$, it holds that

1. $r = K_{M,\mu}(C_2^\perp, C_1^\perp)$ is the maximum information (number of bits multiplied by $\log_q(2)$) about the sent message that can be obtained by wire-tapping at most $\mu$ links of the network.

2. $\mu = d_{M,r}(C_2^\perp, C_1^\perp)$ is the minimum number of links that an adversary needs to wire-tap in order to obtain at least $r$ units of information (number of bits multiplied by $\log_q(2)$) of the sent message.
As a particular case, we see that the minimum rank distance of the pair $C_1^+ \subseteq C_2^+$ (recall (4)) tells how many links an adversary may listen to without obtaining any information about the sent message:

**Corollary 3.** Given nested linear codes $C_2 \subseteq C_1 \subseteq F^{m \times n}$, it holds that $t = d_R(C_1^+, C_2^+) - 1$ is the maximum number of links that an adversary may listen to without obtaining any information about the sent message.

**Proof.** It follows directly from the previous theorem and Corollary 2.

### 4.2 Information distributions, information spaces and secrecy spaces

Proposition 5 and more concretely Equation (6), state that the information leaked to an adversary that obtains $CB^T$, for some matrix $B \in F^{n \times n}$, depends only on $L = \text{Row}(B)$. This motivates the definition of matrix information distributions, which are defined as the collection of row spaces $\text{Row}(B)$ for which $CB^T$ gives a fixed amount of information ($r \log_2(q)$ bits for some $r$):

**Definition 11 (Matrix information distributions).** Given nested linear codes $C_2 \subseteq C_1 \subseteq F^{m \times n}$, and an integer $1 \leq r \leq \dim(C_1/C_2)$, we define the $r$-th matrix information distribution of the given code pair as

$$I_{m,r}(C_1, C_2) = \{ L \subseteq F^n \mid \dim(C_2^+ \cap V_L) - \dim(C_1^+ \cap V_L) = r \}.$$ 

As in [26 Proposition 14] for Hamming access structures and [26 Proposition 15] for rank access structures, we observe that the matrix information distributions of a pair $C_2 \subseteq C_1 \subseteq F^{m \times n}$ uniquely determine the matrix information distributions of the “dual” pair $C_1^+ \subseteq C_2^+ \subseteq F^{m \times n}$. This is analogous to the McWilliams identities for weight distributions and means that row spaces that give $r \log_2(q)$ bits of information for the pair $C_2 \subseteq C_1$ are determined by row spaces that give $(\dim(C_1/C_2) - r) \log_2(q)$ bits of information for the dual pair $C_1^+ \subseteq C_2^+$.

**Proposition 6.** For a collection of subspaces $A \subseteq \{ L \subseteq F^n \mid L \text{ is a subspace} \}$, define its dual as

$$A^* = \{ L^* \mid L \in A \}.$$

Then, for given nested linear codes $C_2 \subseteq C_1 \subseteq F^{m \times n}$, and an integer $1 \leq r \leq \ell = \dim(C_1/C_2)$, it holds that

$$I_{m,r}(C_2^+, C_1^+) = I_{m,\ell-r}(C_1, C_2)^*.$$

**Proof.** It follows from the fact that

$$\dim(C_2^+ \cap V_L) - \dim(C_1^+ \cap V_L) + \dim(C_1 \cap V_{L^*}) - \dim(C_2 \cap V_{L^*}) = \ell,$$

for any subspace $L \subseteq F^n$, which follows from Lemma 2 and Proposition 3.

On the other hand, it is of special interest to see which spaces give no information about the sent message, for security purposes, and which spaces give all information about the sent message, for recovery purposes.

**Definition 12 (Information and secrecy spaces).** Given nested linear codes $C_2 \subseteq C_1 \subseteq F^{m \times n}$ and given a subspace $L \subseteq F^n$, we say that $L$ is an information space (respectively, a secrecy space) for $C_2 \subseteq C_1$ if $L \in I_{m,0}(C_1, C_2)$ (respectively, $L \in I_{m,0}(C_1, C_2)$), where $\ell = \dim(C_1/C_2)$.
Remark 2. Observe that, if \( \mathcal{L} \subseteq \mathcal{L}' \) (respectively, \( \mathcal{L}' \subseteq \mathcal{L} \)) and \( \mathcal{L} \) is an information space (respectively, a secrecy space), then so is \( \mathcal{L}' \). Therefore, the collection of information spaces (respectively, secrecy spaces) can be seen as a linearized version of access structures (respectively, adversary structures) in secret sharing, as defined in [13].

On the other hand, in Corollary 4, Subsection 4.3, we will see that matrix information distributions extend access structures of ramp secret sharing schemes constructed using linear codes, as in [13] Section II. In Corollary 4, Subsection 5.4, we will also see that matrix information distributions extend the rank access structures of nested linear code pairs, as in [20] Definition 14.

Observe also that information spaces have already been defined in the context of rank-metric codes and coding schemes in [20] Definition 12. Due to the definition given in [20] and the discussion in [20] Subsection VI-D, the next proposition shows that our definition and the definition in [20] actually coincide:

**Proposition 7.** Fix nested linear codes \( \mathcal{C}_2 \subseteq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n} \), with \( \ell = \dim(\mathcal{C}_1/\mathcal{C}_2) \), and a subspace \( \mathcal{L} \subseteq \mathbb{F}^n \) with generator matrix \( A \in \mathbb{F}^{m \times n} \), and define the map \( \varphi_A : \mathbb{F}^{m \times n} \rightarrow \mathbb{F}^{m \times \ell} \) by \( \varphi_A(C) = CA^T \). The following hold:

1. \( \mathcal{L} \) is an information space for \( \mathcal{C}_2 \subsetneq \mathcal{C}_1 \) if, and only if, \( \varphi_A(C + C_2) = \varphi_A(D + C_2) \) implies that \( C + C_2 = D + C_2 \), for all \( C,D \in \mathcal{C}_1 \).

2. \( \mathcal{L} \) is a secrecy space for \( \mathcal{C}_2 \subsetneq \mathcal{C}_1 \) if, and only if, \( \varphi_A(C + C_2) = \varphi_A(D + C_2) \), for all \( C,D \in \mathcal{C}_1 \).

**Proof.** We prove item 1, being the proof of item 2 analogous.

Assume that \( \mathcal{L} \in \mathcal{I}_{\mathcal{M}_1}(\mathcal{C}_1, \mathcal{C}_2) \). This means by definition that \( \dim(C_2^j \cap \mathcal{V}_L) - \dim(C_1^j \cap \mathcal{V}_L) = \ell \).

By Lemma 2 and Proposition 11 this means that \( \dim(C_1 \cap \mathcal{V}_{L^+}) - \dim(C_2 \cap \mathcal{V}_{L^+}) = 0 \), that is, \( C_1 \cap \mathcal{V}_{L^+} = C_2 \cap \mathcal{V}_{L^+} \).

Now assume that \( \varphi_A(C + C_2) = \varphi_A(D + C_2) \) for \( C,D \in \mathcal{C}_1 \). This implies that \( (C - D)A^T \in \varphi_A(C_2) \), that is, \( (C - D)A^T = E^T \), with \( E \in \mathcal{C}_2 \). In other words, \( (C - D - E)A^T = 0 \), which implies that \( C - D - E \in \mathcal{C}_1 \cap \mathcal{V}_{L^+} = C_2 \cap \mathcal{V}_{L^+} \). Therefore \( C - D \in \mathcal{C}_2 \) and \( C + C_2 = D + C_2 \).

On the other hand, now assume that \( \varphi_A(C + C_2) = \varphi_A(D + C_2) \) implies that \( C + C_2 = D + C_2 \), for all \( C,D \in \mathcal{C}_1 \). Take now \( C \in \mathcal{C}_1 \cap \mathcal{V}_{L^+} \). Then \( CA^T = 0 \in \varphi_A(C_2) \). Therefore \( C \in \mathcal{C}_2 \cap \mathcal{V}_{L^+} \), and we conclude that \( C_1 \cap \mathcal{V}_{L^+} = C_2 \cap \mathcal{V}_{L^+} \).

As we saw before, this implies that \( \dim(C_2^j \cap \mathcal{V}_L) - \dim(C_1^j \cap \mathcal{V}_L) = \ell \) and hence \( \mathcal{L} \) is an information space. \( \square \)

Remark 3. The map \( \varphi_A \) in the previous proposition can be seen as the procedure of puncturing codewords on the space \( \mathcal{L} \) in the context of the rank metric (see [20] Section VI]). Observe also that, in this sense, a punctured collection of packets is a collection of linear combinations of packets, as the ones obtained by the sink node in the network or a wire-tapping adversary (in the absence of errors).

Therefore, the previous proposition states that \( \mathcal{L} \) is an information space (respectively, secrecy space) if, and only if, we may (respectively, we may not) tell the difference between the original sent packets and any other possible sent packets by looking at the received linear combinations.

### 4.3 Optimal linear coset coding schemes for noiseless networks

In this subsection, we obtain linear coding schemes built from nested linear code pairs \( \mathcal{C} \supsetneq \mathcal{C} \subseteq \mathbb{F}^{m \times n} \) with optimal universal security parameters in the case of finite fields \( \mathbb{F} = \mathbb{F}_q \). Recall from Subsection 4.3 that these linear coding schemes are suitable for noiseless networks, as noticed in [20] (see also Remark 1).
Definition 13. For a nested linear code pair of the form \( C \subseteq \mathbb{F}_q^{m \times n} \), we define its information parameter as \( \ell = \dim(\mathbb{F}_q^{m \times n} / C) = \dim(C^\perp) \), that is the maximum number of \( \log_q(q) \) bits of information that the source can convey, and its security parameter \( t \) as the maximum number of links that an adversary may listen to without obtaining any information about the sent message.

Due to Corollary 3, it holds that \( t = d_R(C^\perp) - 1 \). We study two problems:

1. Find a nested linear code pair \( C \subseteq \mathbb{F}_q^{m \times n} \) with maximum possible security parameter \( t \) when \( m, n, q \) and the information parameter \( \ell \) are fixed and given.

2. Find a nested linear code pair \( C \subseteq \mathbb{F}_q^{m \times n} \) with maximum possible information parameter \( \ell \) when \( m, n, q \) and the security parameter \( t \) are fixed and given.

Thanks to Corollary 3 and the Singleton bound on the dimension of rank-metric codes [6, Theorem 5.4], we may give upper bounds on the attainable parameters in the previous two problems:

Proposition 8. Given a nested linear code pair \( C \subseteq \mathbb{F}_q^{m \times n} \) with information parameter \( \ell \) and security parameter \( t \), it holds that:

\[
\ell \leq \max\{m, n\} \left(\min\{m, n\} - t\right),
\]

\[
t \leq \min\{m, n\} - \left\lceil \frac{\ell}{\max\{m, n\}} \right\rceil.
\]

In particular, \( \ell \leq mn \) and \( t \leq \min\{m, n\} \).

Proof. Recall that \( \ell = \dim(\mathbb{F}_q^{m \times n} / C) = \dim(C^\perp) \) and, due to Corollary 3, \( t = d_R(C^\perp) - 1 \). Hence the result follows from the Singleton bound on dimensions of linear codes given in [6, Theorem 5.4]:

\[
\dim(C^\perp) \leq \max\{m, n\} \left(\min\{m, n\} - d_R(C^\perp) + 1\right).
\]

On the other hand, the existence of linear codes in \( \mathbb{F}_q^{m \times n} \) attaining the Singleton bound on their dimensions, for all possible choices of \( m, n \) and minimum rank distance \( d_R \) [6, Theorem 6.3], leads to the following existence result on optimal linear coding schemes for noiseless networks.

Theorem 4. For all choices of positive integers \( m \) and \( n \), and all finite fields \( \mathbb{F}_q \), the following hold:

1. For every positive integer \( \ell \leq mn \), there exists a nested linear code pair \( C \subseteq \mathbb{F}_q^{m \times n} \) with information parameter \( \ell \) and security parameter \( t = \min\{m, n\} - \left\lceil \ell / \max\{m, n\} \right\rceil \).

2. For every positive integer \( t \leq \min\{m, n\} \), there exists a nested linear code pair \( C \subseteq \mathbb{F}_q^{m \times n} \) with security parameter \( t \) and information parameter \( \ell = \max\{m, n\} \left(\min\{m, n\} - t\right) \).

Remark 4. We remark here that, to the best of our knowledge, only the linear coding schemes in item 2 in the previous theorem, for the special case \( n \leq m \), have been obtained in the literature. It corresponds to [53, Theorem 7].

Using cartesian products of maximum rank distance codes as in [53, Subsection VII-C], linear coding schemes as in item 2 in the previous theorem can be obtained when \( n > m \), for the restricted parameters \( n = ln \) and \( t = mk' \), where \( l \) and \( k' < m \) are positive integers.

Therefore, the previous theorem completes the search for linear coding schemes with optimal security parameters for noiseless networks.
5 Universal secure list-decodable rank-metric codes

In this section, we will see how to build a nested linear code pair $C_2 \subseteq C_1 \subseteq \mathbb{F}_q^{m \times n}$ that can be used to list-decode rank errors, which naturally appear on the network, whose list sizes are polynomial on the code length, while being universal secure under a given number of wire-tapped links. We will also compare the obtained parameters with those obtained when choosing $C_1$ and $C_2$ as Gabidulin maximum rank distance (MRD) codes [13].

5.1 Linear coset coding schemes using Gabidulin MRD codes

Assume now that $n \leq m$ and $C_2 \subseteq C_1 \subseteq \mathbb{F}_q^{m \times n}$ are maximum rank distance (MRD) linear codes (such as Gabidulin codes [13]) of dimensions $\dim(C_1) = mk_1$ and $\dim(C_2) = mk_2$ (recall that, by the Singleton bound [9], dimensions of MRD codes when $n \leq m$ are multiple of $m$).

The linear coset coding scheme constructed from this nested linear code pair satisfies the following properties:

1. The information parameter is $\ell = m(k_1 - k_2)$.
2. The secrecy parameter is $t = k_2$.
3. If the number of rank errors is $e \leq \frac{m-k_2}{2}$, then rank error-correction can be performed, giving a unique solution.

5.2 List-decodable linear coset coding schemes for the rank metric

Assume now that $n$ divides $m$. For the same positive integers $1 \leq k_2 < k_1 \leq n$ as in the previous section, and for fixed $\varepsilon > 0$ and positive integer $s$, we may construct a linear coset coding scheme from a nested linear code pair $C_2 \subseteq C_1 \subseteq \mathbb{F}_q^{m \times n}$, with the following properties:

1. The information parameter is $\ell \geq m(k_1 - k_2)(1 - 2\varepsilon)$.
2. The secrecy parameter is $t \geq k_2$.
3. If the number of rank errors is $e \leq \frac{s}{s+1}(n - k_1)$, then rank-metric list-decoding allows to obtain in polynomial time a list (of uncoded secret messages) of size $q^{O(s^2/\varepsilon^2)}$, which is polynomial in the code length $n$.

Therefore, we may obtain the same security performance as in the previous section, an information parameter that is at least $1-2\varepsilon$ times the one in the previous section, and can list-decode in polynomial time (with list of polynomial size) roughly $n - k_1$ errors, which is twice as many as in the previous section.

Now we see the construction. Fix a basis $\alpha_1, \alpha_2, \ldots, \alpha_m$ of $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_q$, such that $\alpha_1, \alpha_2, \ldots, \alpha_n$ generate $\mathbb{F}_q^n$. We define the matrix representation map $M_\alpha : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^{m \times n}$ associated to the previous basis by

$$M_\alpha(c) = (c_{i,j})_{1 \leq i \leq m, 1 \leq j \leq n}, \quad (10)$$

where $c_i = (c_{i,1}, c_{i,2}, \ldots, c_{i,n}) \in \mathbb{F}_q^n$, for $i = 1, 2, \ldots, m$, are the unique vectors in $\mathbb{F}_q^n$ such that $c = \sum_{i=1}^m \alpha_i c_i$. The map $M_\alpha : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^{m \times n}$ is an $\mathbb{F}_q$-linear vector space isomorphism.

Recall that a $q$-linearized polynomial over $\mathbb{F}_q^n$ is a polynomial of the form $F(x) = \sum_{i=0}^d F_i x^{q^i}$, where $F_1 \in \mathbb{F}_q^n$. Denote also $\text{ev}_\alpha(F(x)) = (F(\alpha_1), F(\alpha_2), \ldots, F(\alpha_n)) \in \mathbb{F}_q^n$, and finally define

$$C_2 = \{ \text{ev}_\alpha(F(x)) \mid F_i = 0, \quad \alpha \in \mathbb{F}_q^n \},$$
where 

\[ H \]

are the \( k \times n \)-linear vector spaces described in [16, Theorem 8].

Now we prove the previous three items:

1. The information parameter \( \ell \) coincides with the dimension of the linear code

\[ W = \{ M_\alpha (\text{ev}_\alpha(F(x))) \mid F_0 \in H_0, \ldots, F_{k_1-k_2-1} = \text{ev}_\alpha(F_{i-1}) \} \]

which is at least \( m(k_1-k_2)(1-2\varepsilon) \) by [16, Theorem 8], as explained in [16, page 2713].

2. By Corollary 3, the secrecy parameter is \( t = d_R(C_2^1, C_1^+ \perp) - 1 \geq d_R(C_2^1) - 1 \). Since \( C_2 \) is MRD, then so is its trace dual \( [6] \), which means that \( d_R(C_2^1) = k_2 + 1 \), and the result follows.

3. We first perform list-decoding using the code \( C_1 \), and obtain in polynomial time a list that is an \( (s-1, m/n, k_1) \)-periodic subspace of \( \mathbb{F}_{q^m}^{k_1} \) by [16, Lemma 16] (recall the definition of periodic subspace from [16, Definition 9]).

Project this periodic subspace onto the first \( k_1-k_2 \) coordinates, which still gives a periodic subspace, and intersect it with \( H_0 \times H_1 \times \cdots \times H_{k_1-k_2-1} \). Such intersection is an \( \mathbb{F}_q \)-linear affine space of dimension at most \( O(s^2/\varepsilon^2) \), as in the proof of [16, Theorem 17], hence the result follows.

6 Basic properties of RDRP and RGMW

6.1 Upper and lower Singleton bounds

**Theorem 5 (Upper Singleton bound).** Given nested linear codes \( C_2 \subseteq C_1 \subseteq \mathbb{F}^{m \times n} \) and \( 1 \leq r \leq \ell = \text{dim}(C_1/C_2) \), it holds that

\[
md_{M,r}(C_1, C_2) \leq mn - \ell + r + m - 1,
\]

which implies that

\[
d_{M,r}(C_1, C_2) \leq \left\lfloor \frac{\ell - r + 1}{m} \right\rfloor + 1.
\]  

(11)

**Proof.** First of all, we have that \( md_{M,\ell}(C_1, C_2) \leq mn \) by [11]. Therefore the case \( r = \ell \) follows.

For the general case, assume that \( 1 \leq r \leq \ell - hm \), where the integer \( h \geq 0 \) is the maximum possible. That is, \( r + (h+1)m > \ell \). Using Proposition 4, we obtain

\[
md_{M,r}(C_1, C_2) \leq md_{M,\ell}(C_1, C_2) - hm
\]

\[
\leq md_{M,\ell}(C_1, C_2) - hm \leq mn - \ell + r + m - 1,
\]

where the last equality follows from \( md_{M,\ell}(C_1, C_2) \leq mn \) and \( r + (h+1)m - 1 \geq \ell \).

Setting \( r = 1 \) and using Corollary 2 for a nested linear code pair and the pair obtained by transposing matrices, the following bound follows, which extends the Singleton bound [9] to nested linear code pairs:
Corollary 4. Given nested linear codes $C_2 \subseteq C_1 \subseteq \mathbb{F}^{m \times n}$, it holds that
$$\dim(C_1/C_2) \leq \max\{m, n\}(\min\{m, n\} - d_R(C_1, C_2) + 1).$$

Remark 5. In view of [23, Proposition 1] or [24, Equation (24)], it is natural to wonder whether a sharper bound of the form
$$d_{M,n}(C_1, C_2) \leq n - \left\lfloor \frac{\dim(C_1) - r + 1}{m} \right\rfloor + 1$$
holds. However, this is not the case in general, as the following example shows.

Example 1. Consider $m = 2$, the canonical basis $e_1, e_2, \ldots, e_n$ of $\mathbb{F}^n$, and the linear codes
$$C_1 = \mathbb{F}^2 \times e_1, e_2, \ldots, e_n$$
and
$$C_2 = \left\langle \begin{pmatrix} e_1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} e_2 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} e_n \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \right\rangle.$$

Observe that $\ell = \dim(C_1/C_2) = n$. A bound as in the previous remark would imply that $d_{M,n}(C_1, C_2) \leq \left\lfloor \frac{n}{2} \right\rfloor$. However, a direct inspection shows that $d_{M,n}(C_1, C_2) = n$, since all vectors $e_1, e_2, \ldots, e_n$ must lie in the row space of any $D$ with $C_1 = C_2 \oplus D$.

On the other hand, we have the following general lower bound:

Theorem 6 (Lower Singleton bound). Given nested linear codes $C_2 \subseteq C_1 \subseteq \mathbb{F}^{m \times n}$ and $1 \leq r \leq \dim(C_1/C_2)$, it holds that $md_{M,r}(C_1, C_2) \geq r$, which implies that
$$d_{M,r}(C_1, C_2) \geq \left\lceil \frac{r}{m} \right\rceil.$$(12)

Proof. We just need to observe the following. Take a subspace $D \subseteq \mathbb{F}^{m \times n}$ and define $L = \text{RSupp}(D)$. We have that $D \subseteq V_L$. Using (1), we see that
$$m\text{wt}_R(D) = m\dim(V_L) = \dim(V_L) \geq \dim(D).$$

The result follows from this and Theorem 2.

6.2 The duality theorem for GMW

It is well-known that, in the Hamming case, all generalized Hamming weights of a linear code determine uniquely those of the corresponding dual code. This is known as Wei’s Duality Theorem [35, Theorem 3]. In this subsection, we prove an analogous result for the generalized matrix weights of a linear code $C \subseteq \mathbb{F}^{m \times n}$ and its dual $C^\perp$. As we will see in Corollary 8.1 and in Corollary 11 Subsection 8.2, this theorem has as consequences the duality theorem for generalized rank weights [8] and the duality theorem for generalized Hamming weights [35].

The presentation of the subsection is inspired by [31, Section 6], whereas the main proofs are inspired by [26] Appendix B]. The work [31] deals with Delsarte generalized weights and [26] deals with generalized rank weights. Both are different from each other and from generalized matrix weights. In Section 8 we will see the relation between them.

Fix a linear code $C \subseteq \mathbb{F}^{m \times n}$ and $1 \leq r \leq \dim(C)$. We will use the notation $C_L = C \cap V_L$ throughout the subsection, for a subspace $L \subseteq \mathbb{F}^n$. We start by rewriting Proposition 2 as follows:

$$d_{M,r}(C) = \min\{\mu \mid \max\{\dim(C_L) \mid L \subseteq \mathbb{F}^n, \dim(L) = \mu\} \geq r\}. \quad (13)$$

16
The following result is analogous to [31, Theorem 37], which deals with duality of Delsarte generalized weights instead of generalized matrix weights. The proof is however inspired by [26, Appendix B].

**Lemma 3.** Given a linear code $C \subseteq \mathbb{F}^{m \times n}$ with $k = \dim(C)$, and given $1 \leq r \leq k$ and $1 \leq s \leq mn - k$, it holds that

$$d_{M,s}(C^\perp) \neq n + 1 - d_{M,r}(C)$$

if $r = p + k + r'm$ and $s = p + s'm$, for some integers $p, r', s' \in \mathbb{Z}$.

**Proof.** Assume that equality holds for a pair of such $r$ and $s$. Write $d_{M,r}(C) = \mu$. Then Equation (13) implies that

$$\max \{ \dim(L) \mid L \subseteq \mathbb{F}^n, \dim(L) = \mu \} \geq r,$$

and $\mu$ is the minimum integer with such property. Now write $d_{M,s}(C^\perp) = \nu = n + 1 - \mu$. In the same way, Equation (13) implies that

$$\max \{ \dim((C^\perp)L) \mid L \subseteq \mathbb{F}^n, \dim(L) = \nu \} \geq s.$$

On the other hand, given a subspace $L \subseteq \mathbb{F}^n$ with $\dim(L) = \nu$, we have that

$$\dim(C_L^\perp) = \dim(C \cap (V_L)^\perp) = k - mn + \dim((C^\perp)L),$$

where the first equality follows from Proposition [1] and the second equality follows from Lemma [2] and Equation (1). Therefore, it holds that

$$\max \{ \dim(L) \mid L \subseteq \mathbb{F}^n, \dim(L) = \mu - 1 \} \geq k - mn + s = k - mn - m + m\mu + s.$$

From the fact that $\mu$ is the minimum integer satisfying Equation (14), and from Equation (15), we conclude that

$$k - mn - m + m\mu + s < r.$$

Now if we interchange the roles of $C$ and $C^\perp$, and the roles of $r$ and $s$, then we automatically interchange the roles of $\mu$ and $n + 1 - \mu$, and the roles of $k$ and $mn - k$. Therefore, we may also conclude that

$$k - mn + m\mu + s > r.$$

Using the expressions $r = p + k + r'm$ and $s = p + s'm$, and dividing everything by $m$, the previous two inequalities are, respectively

$$s' - n - 1 + \mu < r' \quad \text{and} \quad s' - n + \mu > r',$$

which contradict each other. Hence the lemma follows. 

As in [31, Corollary 38], we may conclude the following for generalized matrix weights.

**Theorem 7 (Duality theorem).** Given a linear code $C \subseteq \mathbb{F}^{m \times n}$ with $k = \dim(C)$, and given an integer $p \in \mathbb{Z}$, define

$$W_p(C) = \{ d_{M,p+rm}(C) \mid r \in \mathbb{Z}, 1 \leq p + rm \leq k \},$$

$$\overline{W}_p(C) = \{ n + 1 - d_{M,p+rm}(C) \mid r \in \mathbb{Z}, 1 \leq p + rm \leq k \}.$$

Then it holds that

$$\{1, 2, \ldots, n\} = W_p(C^\perp) \cup \overline{W}_{p+k}(C),$$

where the union is disjoint.
Proof. First, \( W_p(C^\perp) \) and \( W_{p+k}(C) \) are disjoint by the previous lemma. On the other hand, both are contained in \( \{1, 2, \ldots, n\} \) by definition. Hence it suffices to prove that \( \#W_p(C^\perp) + \#W_{p+k}(C) = n \).

The rest of the proof can be word by word translated from the proof of [31, Corollary 38], since we just need to use the monotonicity properties in Proposition 4. We may assume without loss of generality that \( 1 \leq p \leq m \). By Proposition 4, we see that

\[
\#W_p(C^\perp) = \lfloor \frac{mn - k - p}{m} \rfloor + 1,
\]

and

\[
\#W_{p+k}(C) = \lfloor \frac{p + k - 1}{m} \rfloor,
\]

and a straightforward calculation shows that

\[
\lfloor \frac{mn - k - p}{m} \rfloor + \lfloor \frac{p + k - 1}{m} \rfloor = n - 1,
\]

and we are done.

Corollary 5. Given a linear code \( C \subseteq \mathbb{F}^{m \times n} \), its generalized matrix weights uniquely determine those of \( C^\perp \).

6.3 Linear codes whose dimensions are divisible by the packet length

In this subsection, we look at linear codes whose dimensions are divisible by the packet length \( m \). Observe that in such case, we may consider the original uncoded message \( x \in \mathbb{F}^d \) as a matrix \( X \in \mathbb{F}^{m \times k} \), where \( \dim(C) = mk \). That is, the uncoded information is a collection of \( k \) packets of length \( m \).

Recall that a linear code is called maximum rank distance (MRD) if equality in (9) holds (for the primary code or, equivalently, for its dual), and hence if \( n \leq m \), its dimension is divisible by \( m \). In the next proposition, we see that generalized matrix weights of MRD linear codes for \( n \leq m \) are all given by \( m \), \( n \) and \( \dim(C) \), and all attain the upper Singleton bound (11):

Proposition 9. Let \( C \subseteq \mathbb{F}^{m \times n} \) be a linear code with \( \dim(C) = mk \). The following are equivalent if \( n \leq m \):

1. \( C \) is maximum rank distance (MRD).
2. \( d_R(C) = n - k + 1 \).
3. \( d_{M,r}(C) = n - k + \left\lfloor \frac{r - 1}{m} \right\rfloor + 1 \), for all \( 1 \leq r \leq mk \).

Proof. Item 1 and item 2 are equivalent by definition, and item 3 obviously implies item 2 by choosing \( r = 1 \).

Now assume item 2 and let \( 1 \leq r \leq mk \). Let \( r = hm + s \), with \( h \geq 0 \) and \( 0 \leq s < m \). We need to distinguish the cases \( s > 0 \) and \( s = 0 \), and prove only the first case, being the second analogous. By Proposition 4 we have that

\[
d_{M,r}(C) \geq h + d_{M,s}(C) \geq h + d_R(C) = n - k + h + 1.
\]

On the other hand, \( \lfloor (mk - r + 1)/m \rfloor = k - h \), and therefore the bound (11) implies that

\[
d_{M,r}(C) \leq n - k + h + 1,
\]

and hence \( d_{M,r}(C) = n - k + \lfloor (r - 1)/m \rfloor + 1 \) since \( \lfloor (r - 1)/m \rfloor = h \), and item 3 follows.
Regarding the lower Singleton bound, we see in the next proposition that rank support spaces are also characterized by having the minimum possible GMW in view of the lower Singleton bound (12):

**Proposition 10.** Let \( C \subseteq \mathbb{F}^{m \times n} \) be a linear code with \( \dim(C) = mk \). The following are equivalent:

1. \( C \) is a rank support space. That is, there exists a subspace \( \mathcal{L} \subseteq \mathbb{F}^n \) such that \( C = \mathcal{V}_\mathcal{L} \).
2. \( d_{M,km}(C) = k \).
3. \( d_{M,r}(C) = \lceil r/m \rceil \), for all \( 1 \leq r \leq mk \).

**Proof.** Assume that \( C = \mathcal{V}_\mathcal{L} \), as in item 1. By taking a sequence of subspaces \( \{0\} \supseteq \mathcal{L}_1 \supseteq \mathcal{L}_2 \supseteq \cdots \supseteq \mathcal{L}_k = \mathcal{L} \), we see that \( d_{M,r}(C) \leq \dim(\mathcal{L}_r) = r \), for \( 1 \leq r \leq k \) and \( 0 \leq p \leq m - 1 \), since \( \dim(C \cap \mathcal{V}_{\mathcal{L}_r}) = \dim(\mathcal{V}_{\mathcal{L}_r}) = mr \geq mr - p \). Hence item 3 follows.

It is trivial that item 3 implies item 2.

Finally, assume item 2. Take a subspace \( \mathcal{L} \subseteq \mathbb{F}^n \) such that \( \dim(\mathcal{L}) = d_{M,km}(C) = k \) and \( \dim(C \cap \mathcal{V}_\mathcal{L}) \geq mk \). By definition and by (11), it holds that \( \dim(C \cap \mathcal{V}_\mathcal{L}) \geq mk = \dim(\mathcal{V}_\mathcal{L}) \), which implies that \( C \cap \mathcal{V}_\mathcal{L} = \mathcal{V}_\mathcal{L} \), or in other words, \( \mathcal{V}_\mathcal{L} \subseteq C \). Since \( \dim(C) = mk = \dim(\mathcal{V}_\mathcal{L}) \), we see that \( \mathcal{V}_\mathcal{L} = C \) and item 1 follows.

### 7 Security equivalences of linear coset coding schemes and minimum parameters

In this section, we study when two nested linear code pairs \( C_2 \subseteq C_1 \subseteq \mathbb{F}^{m \times n} \) and \( C_2' \subseteq C_1' \subseteq \mathbb{F}^{m' \times n'} \) have the same security or reliability performance, meaning they perform equally regarding information leakage and error correction.

In this sense, we study the minimum possible parameters \( m \) and \( n \) for a linear code, which correspond to the packet length and the number of outgoing links from the source node (see Subsection 2.2).

#### 7.1 Security equivalences and rank isometries

Due to Corollary 5, the first parameter that two linear coset coding schemes need to share in order to behave equally in universal secure network coding is their minimum rank distance.

**Definition 14 (Rank isometries).** We say that a map \( \phi : \mathcal{V} \to \mathcal{W} \) between vector spaces \( \mathcal{V} \subseteq \mathbb{F}^{m \times n} \) and \( \mathcal{W} \subseteq \mathbb{F}^{m' \times n'} \) is a rank isometry if it is a vector space isomorphism and \( \text{Rk}(\phi(V)) = \text{Rk}(V) \), for all \( V \in \mathcal{V} \). In that case, we say that \( \mathcal{V} \) and \( \mathcal{W} \) are rank isometric.

We have the following result, which was first proven in [25, Theorem 1] for square matrices and the complex field \( \mathbb{F} = \mathbb{C} \). In [27, Proposition 3] it is observed that the square condition is not necessary and it may be proven for arbitrary fields:

**Proposition 11 ([25, 27]).** If \( \phi : \mathbb{F}^{m \times n} \to \mathbb{F}^{m \times n} \) is a rank isometry, then there exist invertible matrices \( A \in \mathbb{F}^{m \times m} \) and \( B \in \mathbb{F}^{n \times n} \) such that

1. \( \phi(C) = ACB \), for all \( C \in \mathbb{F}^{m \times n} \), or
2. \( \phi(C) = AC^T B \), for all \( C \in \mathbb{F}^{m \times n} \),

where the latter case can only happen if \( m = n \).

On the other hand, in view of Proposition 5, we may define security equivalences as those vector space isomorphisms that preserve rank support spaces, that is, matrix modules:

**Definition 15 (Security equivalences).** We say that a map \( \phi : V \rightarrow W \) between matrix modules \( V \in M(\mathbb{F}^{m \times n}) \) and \( W \in M(\mathbb{F}^{m \times n'}) \) is a security equivalence if it is a vector space isomorphism and \( \phi(U) \subseteq W \) is a matrix module.

Two nested linear code pairs \( C_2 \subseteq C_1 \subseteq \mathbb{F}^{m \times n} \) and \( C'_2 \subseteq C'_1 \subseteq \mathbb{F}^{m \times n'} \) are said to be security equivalent if there exist matrix modules \( V \in M(\mathbb{F}^{m \times n}) \) and \( W \in M(\mathbb{F}^{m \times n'}) \), containing \( C_1 \) and \( C'_1 \), respectively, and a security equivalence \( \phi : V \rightarrow W \) with \( \phi(C_1) = C'_1 \) and \( \phi(C_2) = C'_2 \).

The following result is inspired by [26, Theorem 5], which treats a particular case.

**Theorem 8.** Let \( \phi : V \rightarrow W \) be a vector space isomorphism between matrix modules \( V \in M(\mathbb{F}^{m \times n}) \) and \( W \in M(\mathbb{F}^{m \times n'}) \), and consider the following properties:

(P 1) There exist full-rank matrices \( A \in \mathbb{F}^{m \times m} \) and \( B \in \mathbb{F}^{n \times n'} \) such that \( \phi(C) = ACB \), for all \( C \in V \).

(P 2) A subspace \( U \subseteq V \) is a matrix module if, and only if, \( \phi(U) \) is a matrix module. That is, \( \phi \) is a security equivalence.

(P 3) For all subspaces \( D \subseteq V \), it holds that \( \text{wt}_R(\phi(D)) = \text{wt}_R(D) \).

(P 4) \( \phi \) is a rank isometry.

Then the following implications hold:

\( (P 1) \iff (P 2) \iff (P 3) \implies (P 4) \).

In particular, a security equivalence is a rank isometry and, in the case \( V = W = \mathbb{F}^{m \times n} \) and \( m \neq n \), the converse holds by Proposition 11.

**Proof.** See Appendix A. \( \square \)

**Remark 6.** Unfortunately, the implication \( (P 3) \implies (P 4) \) not always holds. Take for instance \( m = n \) and the map \( \phi : \mathbb{F}^{m \times m} \rightarrow \mathbb{F}^{m \times m} \) given by \( \phi(C) = C^T \), for all \( C \in \mathbb{F}^{m \times m} \).

**Remark 7.** Observe that security equivalences preserve (relative) generalized matrix weights and distributions of rank weights of vector subspaces, and they are the only rank isometries with these properties.

**Remark 8.** The topic of linear transformations \( \phi : \mathbb{F}^{m \times n} \rightarrow \mathbb{F}^{m \times n} \) preserving some specified property has been intensively studied in the literature, where the term “Frobenius map” is generally used for maps of the form of Proposition 11. When \( m = n \), it is proven in [7, Theorem 3] that Frobenius maps are characterized by being those preserving invertible matrices and, in [25], they are characterized by being those preserving ranks, those preserving determinants and those preserving eigenvalues.

To the best of our knowledge, the previous theorem has not been obtained in the literature yet.
7.2 Minimum parameters of linear codes

In this subsection, we study the minimum parameters $m$ and $n$ for which there exists a linear code that is security equivalent to a given one. Recall from Subsection 2.2 that $m$ corresponds to the packet length used in the network, and $n$ corresponds to the number of outgoing links from the source node.

Definition 16 (minimum length). For a linear code $C \subseteq \mathbb{F}^{m \times n}$, we define its minimum link length $n(C)$, or just minimum length, as the minimum integer such that there exist a linear code $C' \subseteq \mathbb{F}^{m \times n(C)}$ that is security equivalent to $C$.

We may easily relate the last GMW of a linear code with its minimum link length. It can be seen as an extension of [26, Proposition 3].

Proposition 12. For a linear code $C \subseteq \mathbb{F}^{m \times n}$ of dimension $k$, it holds that

$$n(C) = d_{M,k}(C).$$

Moreover, there exists a linear code $C' \subseteq \mathbb{F}^{m \times n'}$ that is security equivalent to $C$ if, and only if, $n' \geq d_{M,k}(C)$.

Proof. We just need to prove the second statement. First, if $C' \subseteq \mathbb{F}^{m \times n'}$ is security equivalent to $C$, then $d_{M,k}(C') = d_{M,k}(C' \cap V_C) \leq n'$.

On the other hand, assume that $n' \geq d_{M,k}(C)$. Take a subspace $C \subseteq \mathbb{F}^n$ with $d = \dim(L) = d_{M,k}(C)$ and $d_{M,k}(C)$ gives $\dim(V_C) \geq k$, which implies that $C \subseteq V_C$. Take a generator matrix $A \in \mathbb{F}^{d \times n}$ of $L$. There exists a full-rank matrix $A' \in \mathbb{F}^{n \times d}$ such that $AA' = I \in \mathbb{F}^{d \times d}$. The linear map $\phi : V_C \rightarrow \mathbb{F}^{m \times d}$, given by $\phi(V) = VA'$, for $V \in V$, is a vector space isomorphism. By dimensions, we just need to see that it is onto. Take $W \in \mathbb{F}^{m \times d}$. It holds that $W = WI = WAA' = \phi(WA)$, and $WA \in V_C$ by definition.

On the other hand, $\phi$ is a security equivalence by Theorem 8. Therefore $\phi(C) \subseteq \mathbb{F}^{m \times d}$ is security equivalent to $C$. Finally, we see that appending zero columns to matrices in $\phi(C)$ gives security equivalent codes to $C$ for any $n' \geq 1$, and we are done.

Remark 9. The previous proposition implies that a linear code $C \subseteq \mathbb{F}^{m \times n}$ can be applied, with the same security performance, over any network that uses packet length $m$ and the number of outgoing links from the source is at least $d_{M,k}(C)$.

Finally, we may give the following lower bound on the minimum packet length of a linear code that is rank isometric to a given one. In view of Proposition 11 and Theorem 8, rank isometries and security equivalences are close concepts, even though the second is slightly stronger in some cases.

Corollary 6. For a linear code $C \subseteq \mathbb{F}^{m \times n}$, define the transposed linear code

$$C^T = \{C^T | C \in C\} \subseteq \mathbb{F}^{n \times m}.$$ 

If $m' \geq d_{M,k}(C^T)$, where $k = \dim(C)$, then there exists a linear code $C' \subseteq \mathbb{F}^{m' \times n}$ that is rank isometric to $C$.

Proof. It follows from Theorem 8 and Proposition 12.

Remark 10. Recall from Corollary 8 that rank isometric codes behave equally regarding the maximum number of links that an adversary may wire-tap without obtaining any information about the sent message.

Therefore, if we want to use a linear code $C \subseteq \mathbb{F}^{m \times n}$ on a network with $n$ outgoing links from the source node, we may apply $C$ with any packet length $m' \geq d_{M,k}(C^T)$ while preserving its security behaviour as in the previous paragraph, by the previous corollary.
7.3 Degenerate codes

In this subsection, we study degenerate codes, which by the study in the previous subsection, can be applied to networks with less outgoing links or, by transposing matrices, with smaller packet length. This study constitutes an extension to the linear case of the study in [19, Section 6] and [26, Subsection IV-B].

**Definition 17 (Degenerate codes).** We say that a linear code \( C \subseteq \mathbb{F}^{m \times n} \) is degenerate if it is security equivalent to a linear code \( C' \subseteq \mathbb{F}^{m \times n'} \) with \( n' < n \).

The following lemma follows immediately from Proposition 12:

**Lemma 4.** A linear code \( C \subseteq \mathbb{F}^{m \times n} \) is degenerate if, and only if, \( d_{M,k}(C) < n \), where \( k = \dim(C) \).

Now we may give characterizations in terms of the minimum rank distance of the dual code thanks to Theorem 7.

**Proposition 13.** Given a linear code \( C \subseteq \mathbb{F}^{m \times n} \), the following hold:

1. Assuming \( \dim(C^\perp) \geq m \), \( C \) is degenerate if, and only if, \( d_{M,m}(C^\perp) = 1 \).
2. If \( d_R(C^\perp) > 1 \), then \( C \) is not degenerate.

**Proof.** From Theorem 7 we know that \( W_k(C) \cup W_0(C^\perp) = \{1, 2, \ldots, n\} \), where the sets on the left-hand side are disjoint, and where \( k = \dim(C) \). Now, the smallest number in \( W_k(C) \) is \( n + 1 - d_{M,k}(C) \), and the smallest number in \( W_0(C^\perp) \) is \( d_{M,m}(C^\perp) \). Item 1 follows from this and the previous lemma. Item 2 follows from item 1 and Proposition 4. \( \square \)

8 Relation with other existing notions of generalized weights

In this section, we study the relation between RGMW and other notions of generalized weights. In particular, we consider the classical generalized Hamming weights [35], relative generalized Hamming weights [24], relative generalized rank weights [21, 28] and Delsarte generalized weights [31].

We also compare RDRP with the relative dimension/length profile from [12, 24] and the relative dimension/intersection profile from [21].

Moreover, we will see that the duality theorems for generalized rank weights and generalized Hamming weights are consequences of Theorem 4.

8.1 RGMW extend relative generalized rank weights

In this subsection, we prove that RGMW extend the relative generalized rank weights defined in [21].

Throughout the subsection, we will consider the extension field \( \mathbb{F}_{q^m} \) of the finite field \( \mathbb{F}_q \), and vector spaces in \( \mathbb{F}_{q^m}^n \) will be considered to be linear over \( \mathbb{F}_{q^m} \). We need the notion of Galois closed spaces [34].

**Definition 18 (Galois closed spaces [34]).** We say that an \( \mathbb{F}_{q^m} \)-linear vector space \( V \subseteq \mathbb{F}_{q^m}^n \) is Galois closed if

\[
V^g = \{(v_1^g, v_2^g, \ldots, v_n^g) | (v_1, v_2, \ldots, v_n) \in V\} \subseteq V.
\]

We denote by \( \Upsilon(\mathbb{F}_{q^m}^n) \) the family of \( \mathbb{F}_{q^m} \)-linear Galois closed vector spaces in \( \mathbb{F}_{q^m}^n \).
Relative dimension/intersection profile and relative generalized rank weights are then defined in [21] as follows:

**Definition 19 (Relative Dimension/Intersection Profile [21, Definition 1])**. Given nested $\mathbb{F}_q$-linear codes $C_2 \subseteq C_1 \subseteq \mathbb{F}_q^n$, and $0 \leq \mu \leq n$, we define their $\mu$-th relative dimension/intersection profile (RDIP) as

$$K_{R,\mu}(C_1, C_2) = \max \{ \dim(C_1 \cap V) - \dim(C_2 \cap V) \mid V \in \mathcal{T}(\mathbb{F}_q^n), \dim(V) \leq \mu \},$$

where dimensions are taken over $\mathbb{F}_q$.

**Definition 20 (Relative Generalized Rank Weights [21, Definition 2])**. Given nested $\mathbb{F}_q$-linear codes $C_2 \subseteq C_1 \subseteq \mathbb{F}_q^n$, and $1 \leq r \leq \ell = \dim(C_1/C_2)$ (over $\mathbb{F}_q$), we define their $r$-th relative generalized rank weight (RGRW) as

$$d_{R,r}(C_1, C_2) = \min \{ \dim(V) \mid V \in \mathcal{T}(\mathbb{F}_q^n), \dim(C_1 \cap V) - \dim(C_2 \cap V) \geq r \},$$

where dimensions are taken over $\mathbb{F}_q$.

We will use the following result from [34]:

**Lemma 5 [34, Lemma 1]**. An $\mathbb{F}_q$-linear vector space $V \subseteq \mathbb{F}_q^n$ is Galois closed if, and only if, it has a basis of vectors in $\mathbb{F}_q$ as a vector space over $\mathbb{F}_q$.

We may now prove the following theorem. Recall the matrix representation map from (10).

**Theorem 9**. Let $\alpha_1, \alpha_2, \ldots, \alpha_m$ be a basis of $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_q$, and let $V \subseteq \mathbb{F}_q^n$ be an arbitrary set. The following are equivalent:

1. $V \subseteq \mathbb{F}_q^n$ is an $\mathbb{F}_q$-linear Galois closed vector space. That is, $V \in \mathcal{T}(\mathbb{F}_q^n)$.
2. $M_\alpha(V) \subseteq \mathbb{F}_q^{m \times n}$ is a matrix module. That is, $M_\alpha(V) \in M(\mathbb{F}_q^{m \times n})$.

**Proof**. We first observe the following. For an arbitrary set $V \subseteq \mathbb{F}_q^n$, the previous lemma states that $V$ is an $\mathbb{F}_q$-linear Galois closed vector space if, and only if, $V$ is $\mathbb{F}_q$-linear and it has a basis over $\mathbb{F}_q$ of the form $v_{i,j} = \alpha_i b_j$, for $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, k$, where $b_1, b_2, \ldots, b_k \in \mathbb{F}_q$. By considering $B_{i,j} = M_\alpha(v_{i,j}) \in \mathbb{F}_q^{m \times n}$, we see that this condition is equivalent to item 3 in Theorem 1 and we are done.

In short, the previous theorem means that the map $M_\alpha$ defines a bijection between $\mathcal{T}(\mathbb{F}_q^n)$ and $M(\mathbb{F}_q^{m \times n})$, preserving inclusions. In other words, it is a lattice isomorphism. Moreover, in view of (1), it holds that

$$\dim(V) = \dim(L),$$

for any $V \in \mathcal{T}(\mathbb{F}_q^n)$, where $L \subseteq \mathbb{F}_q^n$ is such that $M_\alpha(V) = V_L$ and the dimension $\dim(V)$ is taken over the field $\mathbb{F}_q$.

We need one more tool from the literature. For an $\mathbb{F}_q$-linear code $C \subseteq \mathbb{F}_q^n$, we denote by $C^\perp \subseteq \mathbb{F}_q^n$ its dual code with respect to the usual $\mathbb{F}_q$-bilinear inner product in $\mathbb{F}_q^n$. Recall also from [23] the definition of orthogonal bases.

**Lemma 6 [30, Theorem 21]**. If $C \subseteq \mathbb{F}_q^n$ is an $\mathbb{F}_q$-linear code and $\alpha_1, \alpha_2, \ldots, \alpha_m$ and $\alpha'_1, \alpha'_2, \ldots, \alpha'_m$ are orthogonal bases of $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_q$, then

$$M_\alpha(C^\perp) = M_\alpha(C)^\perp.$$
Therefore, the following result follows:

**Corollary 7.** Let $\alpha_1, \alpha_2, \ldots, \alpha_m$ be a basis of $\mathbb{F}_q^m$ as a vector space over $\mathbb{F}_q$. Given nested $\mathbb{F}_q^m$-linear codes $C_2 \subseteq C_1 \subseteq \mathbb{F}_q^n$, and integers $1 \leq r \leq \ell = \dim(C_1/C_2)$ (over $\mathbb{F}_q$), $0 \leq p \leq m - 1$ and $0 \leq \mu \leq n$, we have that

\[
d_{R,r}(C_1, C_2) = d_{M,r-p}(M_{\alpha}(C_1), M_{\alpha}(C_2)),
\]

\[
mK_{R,\mu}(C_1, C_2) = K_{M,\mu}(M_{\alpha}(C_1), M_{\alpha}(C_2)).
\]

Moreover, it holds that $\mathcal{I}_{M,r-p}(M_{\alpha}(C_1), M_{\alpha}(C_2)) = \emptyset$ if $p \neq 0$, and

\[
\mathcal{I}_{M,r}(M_{\alpha}(C_1), M_{\alpha}(C_2)) = \{ \mathcal{L} \subseteq \mathbb{F}_q^n \mid \dim(C_2^\perp \cap M_{\alpha}^{-1}(\mathcal{V}_\mathcal{L})) - \dim(C_1^\perp \cap M_{\alpha}^{-1}(\mathcal{V}_\mathcal{L})) = r \},
\]

where dimensions in the last equality are taken over $\mathbb{F}_q$.

Observe that the last equality shows that the rank access structures of nested linear code pairs defined in [26, Definition 14] are also extended by the matrix information distributions in Definition 11.

To conclude, we see that the duality theorem for GRWs [8] is a direct consequence of Corollary 7 and Theorem 7:

**Corollary 8 ([8]).** Given an $\mathbb{F}_q^m$-linear code $C \subseteq \mathbb{F}_q^n$ of dimension $k$ over $\mathbb{F}_q^m$, denote $d_r = d_{R,r}(C)$ and $d^+_s = d_{R,s}(C^\perp)$, for $1 \leq r \leq k$ and $1 \leq s \leq n - k$. Then

\[
\{1, 2, \ldots, n\} = \{d_1, d_2, \ldots, d_k\}
\]

\[
\cup \{n + 1 - d^+_1, n + 1 - d^+_2, \ldots, n + 1 - d^+_n\}
\]

where the union is disjoint.

**Proof.** It follows from Theorem 7, taking any value of $p$, the previous corollary and Lemma 6.

### 8.2 RGMW extend relative generalized Hamming weights

In this subsection, we see that relative generalized matrix weights also extend relative generalized Hamming weights [24], and therefore generalized matrix weights extend generalized Hamming weights [35].

To deal with Hamming weights, it is usual to consider Hamming supports of vectors in $\mathbb{F}_q^n$ and their corresponding Hamming support spaces:

**Definition 21 (Hamming supports).** Given a vector space $\mathcal{C} \subseteq \mathbb{F}_q^n$, we define its Hamming support as

\[
\text{HSupp}(\mathcal{C}) = \{ i \in \{1, 2, \ldots, n\} \mid \exists (c_1, c_2, \ldots, c_n) \in \mathcal{C}, c_i \neq 0 \}.
\]

We also define the Hamming weight of the space $\mathcal{C}$ as

\[
\text{wt}_H(\mathcal{C}) = \#\text{HSupp}(\mathcal{C}).
\]

Finally, for a vector $c \in \mathbb{F}_q^n$, we define its Hamming support as $\text{HSupp}(c) = \text{HSupp}(\langle \{c\} \rangle)$, and its Hamming weight as $\text{wt}_H(c) = \text{wt}_H(\langle \{c\} \rangle)$.
Definition 22 (Hamming support spaces). Given a subset $I \subseteq \{1, 2, \ldots, n\}$, we define its Hamming support space as the vector space in $\mathbb{F}^n$ given by

$$\mathcal{L}_I = \{(c_1, c_2, \ldots, c_n) \in \mathbb{F}^n | c_i = 0, \forall i \notin I\}.$$

We may now define relative generalized Hamming weights and relative dimension/length profile:

Definition 23 (Relative Dimension/Length Profile [12, 24]). Given nested linear codes $C_2 \subseteq C_1 \subseteq \mathbb{F}^n$, and $0 \leq \mu \leq n$, we define their $\mu$-th relative dimension/length profile (RDLP) as

$$K_{H,\mu}(C_1, C_2) = \max \{ \dim(C_1 \cap \mathcal{L}_I) - \dim(C_2 \cap \mathcal{L}_I) | I \subseteq \{1, 2, \ldots, n\}, \#I \leq \mu \}.$$

Definition 24 (Relative Generalized Hamming Weights [24, Section III]). Given nested linear codes $C_2 \subseteq C_1 \subseteq \mathbb{F}^n$, and $1 \leq r \leq \ell = \dim(C_1/C_2)$, we define their $r$-th relative generalized Hamming weight (RGHW) as

$$d_{H,r}(C_1, C_2) = \min \{ \#I | I \subseteq \{1, 2, \ldots, n\} \text{ dim}(C_1 \cap \mathcal{L}_I) - \dim(C_2 \cap \mathcal{L}_I) \geq r \}.$$

As in Theorem 2, it holds that

$$d_{H,r}(C_1, C_2) = \min \{ \text{wt}_H(D) | D \subseteq C_1, D \cap C_2 = \{0\}, \dim(D) = r \}.$$

Given a linear code $C \subseteq \mathbb{F}^n$, we see that its $r$-th generalized Hamming weight [35, Section II] is $d_{H,r}(C) = d_{H,r}(C, \{0\})$, for $1 \leq r \leq \dim(C)$.

To prove that relative generalized matrix weights also extend relative generalized Hamming weights, we need to see vectors in $\mathbb{F}^n$ as matrices in $\mathbb{F}^{n \times n}$. To that end, we introduce the diagonal matrix representation map $\Delta : \mathbb{F}^n \rightarrow \mathbb{F}^{n \times n}$ given by

$$\Delta(c) = \text{diag}(c) = (c_i \delta_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n}, \quad (16)$$

where $c = (c_1, c_2, \ldots, c_n) \in \mathbb{F}^n$ and $\delta_{i,j}$ represents the Kronecker delta. In other words, $\Delta(c)$ is the diagonal matrix whose diagonal vector is $c$.

The map $\Delta : \mathbb{F}^n \rightarrow \mathbb{F}^{n \times n}$ is linear and one to one. It is immediate that

$$\text{Rk}(\Delta(c)) = \text{wt}_H(c).$$

Moreover, we have the following properties.

Proposition 14. Let $D \subseteq \mathbb{F}^n$ be a vector space, and let $I \subseteq \{1, 2, \ldots, n\}$ be a set. The following properties hold:

1. $\text{RSupp}(\Delta(D)) = \mathcal{L}_J \subseteq \mathbb{F}^n$, where $J = \text{HSupp}(D) \subseteq \{1, 2, \ldots, n\}$.

2. For a matrix module $V \subseteq \mathbb{F}^{n \times n}$, if $\Delta(D) = V \cap \Delta(\mathbb{F}^n)$, then $D = \mathcal{L}_J$, for $J = \text{HSupp}(D) \subseteq \{1, 2, \ldots, n\}$.

3. $\text{wt}_R(\Delta(D)) = \text{wt}_H(D)$.

Therefore, the following result holds:
On the other hand, from Theorem 7 it follows that
\[ W(\Delta(C_1), \Delta(C_2)) \]
Proof.
where the union is disjoint.

Corollary 9. Given nested linear codes \( C_2 \subseteq C_1 \subseteq F^n \), and integers \( 1 \leq r \leq \ell = \dim(C_1/C_2) \), and \( 0 \leq \mu \leq n \), we have that
\[ d_{H,r}(C_1, C_2) = d_{M,r}(\Delta(C_1), \Delta(C_2)), \]
\[ K_{H,\mu}(C_1, C_2) = K_{M,\mu}(\Delta(C_1), \Delta(C_2)). \]

Moreover, it holds that
\[ I_{M,\mu}(\Delta(C_1), \Delta(C_2)) = \{ L_i \subseteq F^n | \]
\[ \ dim(C_2^i \cap L_i) - \ dim(C_1^i \cap L_i) = r \}. \]

Observe that the last equality shows that the access structures of ramp secret sharing schemes, constructed using nested linear code pairs, as defined in [15, Section II], are also extended by the matrix information distributions in Definition [11]

On the other hand, just as in [26, Theorem 7], the previous equalities imply that every bound on relative generalized matrix weights must be “less tight” than the corresponding bounds on relative generalized Hamming weights:

Corollary 10. Fix numbers \( \ell \) and \( 1 \leq r, s \leq \ell \), and functions \( f_{r,s}, g_{r,s} : N \rightarrow \mathbb{R} \), which may also depend on \( n, m, \ell \) and \( q = \#F \) if \( F \) is finite. Every bound of the form
\[ f_{r,s}(d_r(C_1, C_2)) \geq g_{r,s}(d_s(C_1, C_2)) \]
that is valid for relative generalized matrix weights, for any pair of linear codes \( C_2 \subseteq L \subseteq C_1 \subseteq F^{n \times n} \) with \( \dim(C_1/C_2) = \ell \), is also valid for relative generalized Hamming weights of a pair of linear codes \( D_2 \subseteq D_1 \subseteq F^n \) with \( \dim(D_1/D_2) = \ell \). The same holds for generalized weights of just one linear code \( C \subseteq F^{n \times n} \) and \( D \subseteq F^n \).

Finally, we see that the duality theorem for GHWs [35] is a direct consequence of Corollary 9 and Theorem 7.

Corollary 11 ([35]). Given a linear code \( C \subseteq F^n \) of dimension \( k \), denote \( d_r = d_{H,r}(C) \) and \( d_s = d_{H,s}(\overline{C}) \), for \( 1 \leq r \leq k \) and \( 1 \leq s \leq n - k \). Then
\[ \{1, 2, \ldots, n\} = \{d_1, d_2, \ldots, d_k\} \]
\[ \cup\{n + 1 - d_1^+, n + 1 - d_2^+, \ldots, n + 1 - d_{n-k}^+\}, \]
where the union is disjoint.

Proof. We will use the notation in Theorem 7 during the whole proof. First of all, by Corollary 9 it holds that \( W_p(\Delta(C)) = \{d_{H,p}(C)\} \) if \( 1 \leq p \) mod \( n \leq k \) and \( W_p(\Delta(C)) = \emptyset \) if \( k + 1 \leq p \) mod \( n \leq n - 1 \) or \( p \) mod \( n = 0 \). Therefore
\[ \bigcup_{p=1}^{n} W_{p-k}(\Delta(C)) = \{d_1, d_2, \ldots, d_k\}. \]

On the other hand, from Theorem 7 it follows that
\[ \left( \bigcup_{p=1}^{n} W_{p-k}(\Delta(C)) \right) \cup \left( \bigcap_{p=1}^{n} W_{p}(\Delta(C)\perp) \right) = \{1, 2, \ldots, n\}, \]
where the union is disjoint. Hence we only need to show that \( n + 1 - d_s^+ \in W_p(\Delta(C)\perp), \) for \( p = 1, 2, \ldots, n \).
Denote by $\mathcal{D}_n \subseteq \mathbb{F}^{n \times n}$ the vector space of matrices with zero components in their diagonals. It holds that $\Delta(\mathcal{C})^\perp = \Delta(\mathcal{C}^\perp) \oplus \mathcal{D}_n$.

Fix $1 \leq s \leq n - k$ and denote $d = d_{H,s}(\mathcal{C}^\perp)$. First, consider a subspace $\mathcal{D} \subseteq \mathcal{C}^\perp$ with $\text{wt}_H(\mathcal{D}) = d$ and $\dim(\mathcal{D}) = s$, and define $\mathcal{D}' \subseteq \Delta(\mathcal{C})^\perp$ as the direct sum of $\Delta(\mathcal{D})$ and all matrices in $\mathcal{D}_n$ with columns in the Hamming support of $\mathcal{D}$. Since $\dim(\mathcal{D}') = d(n-1) + s$ and $\text{wt}_H(\mathcal{D}') = d$, by Theorem 2, it follows that $d_{M,d(n-1)+s}(\Delta(\mathcal{C})^\perp) \leq d$. On the other hand, assume that $d_{M,(d-1)(n-1)+s}(\Delta(\mathcal{C})^\perp) = d' < d$. Let $\mathcal{E} \subseteq \Delta(\mathcal{C})^\perp$ be such that $\text{wt}_H(\mathcal{E}) = d'$ and $\dim(\mathcal{E}) = (d-1)(n-1) + s$. Denote by $\mathcal{E}_D$ the vector space of matrices obtained by removing the elements outside the diagonal of those matrices in $\mathcal{E}$.

Since $\Delta^{-1}(\mathcal{E}_D) \subseteq \mathcal{C}^\perp$, it holds that $\dim(\mathcal{E}_D) < s$ since $\text{wt}_H(\Delta^{-1}(\mathcal{E}_D)) \leq d'$. Since $\mathcal{E} = \mathcal{E}_D \oplus (\mathcal{E} \cap \mathcal{D}_n)$, it follows that $\dim(\mathcal{E} \cap \mathcal{D}_n) = \dim(\mathcal{E}) - \dim(\mathcal{E}_D) > (d-1)(n-1)$. On the other hand, since $\text{wt}_H(\mathcal{E} \cap \mathcal{D}_n) \leq d'$, it follows that $\dim(\mathcal{E} \cap \mathcal{D}_n) \leq (d-1)(n-1)$, a contradiction. Hence

$$d_{M,(d-1)(n-1)+s}(\Delta(\mathcal{C})^\perp) \geq d.$$  \hspace{1cm} (17)

Combining Equation (17) and Equation (18), we conclude that

$$d_{M,(d-1)(n-1)+s+j}(\Delta(\mathcal{C})^\perp) = d,$$

for $j = 0, 1, 2, \ldots, n - 1$, which implies that $n + 1 - d_1^s \in \mathcal{W}_p(\Delta(\mathcal{C})^\perp)$, for $p = 1, 2, \ldots, n$, and we are done. \hfill $\square$

### 8.3 GMW improve Delsarte generalized weights

A notion of generalized weights, called Delsarte generalized weights, for a linear code $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$ has already been proposed in $\text{[31]}$. We will prove that generalized matrix weights are bigger than or equal to Delsarte generalized weights for an arbitrary linear code, and we will prove that the inequality is strict for some linear codes. Together with the study in Subsection 4.1, this implies that Delsarte generalized weights $\text{[31]}$ give lower bounds on worst case information leakage, but not always their exact value.

These weights are defined in terms of optimal anticodes for the rank metric:

**Definition 25 (Maximum rank distance).** For a linear code $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$, we define its maximum rank distance as

$$\text{MaxRk}(\mathcal{C}) = \max\{\text{Rk}(C) \mid C \in \mathcal{C}, C \neq 0\}.$$  \hspace{1cm}

The following bound holds:

**Lemma 7 (\text{[30] Proposition 47})).** For a linear code $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$, it holds that

$$\dim(\mathcal{C}) \leq m\text{MaxRk}(\mathcal{C}).$$  \hspace{1cm} (19)

This leads to the definition of rank-metric optimal anticodes:

**Definition 26 (Optimal anticodes \text{[31] Definition 22})).** We say that a linear code $\mathcal{V} \subseteq \mathbb{F}^{m \times n}$ is a (rank-metric) optimal anticode if equality in (19) holds.

We will denote by $A(\mathbb{F}^{m \times n})$ the family of linear optimal anticodes in $\mathbb{F}^{m \times n}$.

In view of this, Delsarte generalized weights are defined in $\text{[31]}$ as follows:
Definition 27 (Delsarte generalized weights [31, Definition 23]). For a linear code \( C \subseteq \mathbb{F}^{m \times n} \) and an integer \( 1 \leq r \leq \dim(C) \), we define its \( r \)-th Delsarte generalized weight (DGW) as
\[
d_{D,r}(C) = m^{-1} \min \{ \dim(V) \mid V \in A(\mathbb{F}^{m \times n}), \dim(C \cap V) \geq r \}.
\]

Observe that \( d_{D,r}(C) \) is an integer since the dimension of optimal anticodes is a multiple of \( m \) by definition.

We have that matrix modules are optimal anticodes. Due to Theorem 1 and Theorem 9, this result can be seen as [31, Theorem 18] for the case \( \mathbb{F} = \mathbb{F}_q \). We give a short proof for completeness.

Proposition 15 ([31, Theorem 18]). If a set \( V \subseteq \mathbb{F}^{m \times n} \) is a matrix module, then it is a (rank-metric) optimal anticode. In other words, \( M(\mathbb{F}^{m \times n}) \subseteq A(\mathbb{F}^{m \times n}) \).

Proof. Let \( B_{i,j} \), \( i = 1, 2, \ldots, m \) and \( j = 1, 2, \ldots, k \), be a basis of \( V \) as in Theorem 1 item 3. For any \( V = \sum_{i=1}^{m} \sum_{j=1}^{k} \lambda_{i,j} B_{i,j} \in V \), with \( \lambda_{i,j} \in \mathbb{F} \), it holds that
\[
\text{Rk}(V) \leq \dim(\langle b_1, b_2, \ldots, b_k \rangle) = k,
\]
where \( b_1, b_2, \ldots, b_k \) are as in Theorem 1 item 3. Therefore \( \dim(V) = mk \geq m\text{MaxRk}(V) \) and \( V \) is an optimal anticode. \( \square \)

Thus, the next consequence follows from the previous proposition and the corresponding definitions:

Corollary 12. For a linear code \( C \subseteq \mathbb{F}^{m \times n} \) and an integer \( 1 \leq r \leq \dim(C) \), we have that
\[
d_{D,r}(C) \leq d_{M,r}(C).
\]

The next example shows that not all linear optimal anticodes are matrix modules, that is, \( M(\mathbb{F}^{m \times n}) \nsubseteq A(\mathbb{F}^{m \times n}) \) in general. As a consequence, in some cases generalized matrix weights are strictly larger than Delsarte generalized weights:

Example 2. Consider \( m = n = 2 \) and the linear code
\[
C = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\} \subseteq \mathbb{F}^{2 \times 2}.
\]
It holds that \( \dim(C) = 2, m = 2 \) and \( \text{MaxRk}(C) = 1 \). Therefore \( C \) is an optimal anticode. However, it is not a matrix module, since
\[
\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \notin C.
\]

In other words, \( M(\mathbb{F}^{2 \times 2}) \nsubseteq A(\mathbb{F}^{2 \times 2}) \).

On the one hand, we have that \( d_{D,1}(C) = d_{D,2}(C) = 1 \), by [31] Corollary 32], or just by inspection.

On the other hand, it is easy to check that \( d_{M,1}(C) = 1 \), and since \( \text{RSupp}(C) = \mathbb{F}^2 \), it holds that \( d_{M,2}(C) = 2 \). Therefore \( d_{M,2}(C) > d_{D,2}(C) \).

Observe that we may trivially extend this example to any value of \( m = n \), and it holds for an arbitrary field \( \mathbb{F} \).
A Proof of Theorem 8

We will prove each implication, in the following order:

First we prove \((P 1) \implies (P 2)\): Assume that \(\mathcal{U} \subseteq \mathcal{V}\) is a matrix module and take \(U \in \mathcal{U}\) and \(M \in \mathbb{F}^{m \times n}\). Since \(A\) is invertible, there exists \(N \in \mathbb{F}^{m \times m}\) such that \(MA = AN\). Therefore \(M(\mathcal{A}U) = A(\mathcal{N}U)B \in \phi(\mathcal{U})\), since \(NU \in \mathcal{U}\), and we conclude that \(\phi(\mathcal{U})\) is a matrix module. Similarly we may prove that, if \(\phi(\mathcal{U})\) is a matrix module, then \(\mathcal{U}\) is a matrix module.

Now we prove \((P 2) \implies (P 3)\): Let \(\mathcal{L} = \text{RSupp}(\mathcal{D}) \subseteq \mathbb{F}^n\) and \(\mathcal{L}' = \text{RSupp}(\phi(\mathcal{D})) \subseteq \mathbb{F}^{n'}\). It holds that \(\mathcal{V}_C \subseteq \mathcal{V}\) and \(\mathcal{V}_C' \subseteq \mathcal{W}\), and they are the smallest matrix modules in \(\mathcal{V}\) and \(\mathcal{W}\) containing \(\mathcal{D}\) and \(\phi(\mathcal{D})\), respectively, by Lemma 1. Since \(\phi\) preserves matrix modules and their inclusions, we conclude that \(\phi(\mathcal{V}_C) = \mathcal{V}_C'\), which implies that \(\dim(\mathcal{L}) = \dim(\mathcal{L}')\) by Lemma 1, and \((P 3)\) follows.

Next we prove \((P 2) \iff (P 3)\): Assume that \(\mathcal{U} \subseteq \mathcal{V}\) is a matrix module. This means that \(m\text{wt}_R(\mathcal{U}) = \dim(\mathcal{U})\) by Lemma 1. Since \(\phi\) satisfies \((P 3)\) and is a vector space isomorphism, we conclude also by Lemma 1 that \(m\text{wt}_R(\phi(\mathcal{U})) = \dim(\phi(\mathcal{U}))\), and thus \(\phi(\mathcal{U})\) is a matrix module. Similarly we may prove that, if \(\phi(\mathcal{U})\) is a matrix module, then \(\mathcal{U}\) is a matrix module.

Now we prove \((P 3) \implies (P 4)\): Trivial from the fact that \(m\text{wt}_R(\{C\}) = \text{Rk}(C)\), for all \(C \in \mathcal{V}\). Finally we prove \((P 1) \iff (P 2)\): Denote \(\dim(V) = \dim(W) = mk\) and consider bases of \(\mathcal{V}\) and \(\mathcal{W}\) as in Theorem 1 item 3. By defining vector space isomorphisms \(\mathbb{F}^{m \times k} \rightarrow \mathcal{V}\) and \(\mathcal{W} \rightarrow \mathbb{F}^{m \times k}\), sending such bases to the canonical basis of \(\mathbb{F}^{m \times k}\), we see that we only need to prove the result for the particular case \(\mathcal{V} = \mathcal{W} = \mathbb{F}^{m \times n}\).

Denote by \(E_{i,j} \in \mathbb{F}^{m \times n}\) the matrices in the canonical basis, for \(1 \leq i \leq m, 1 \leq j \leq n\), that is, \(E_{i,j}\) has 1 in its \((i,j)\)-th component, and zeroes in its other components.

Consider the matrix module \(\mathcal{U}_j = \langle E_{1,j}, E_{2,j}, \ldots, E_{m,j} \rangle \subseteq \mathbb{F}^{m \times n}\), for \(1 \leq j \leq n\). Since \(\phi(\mathcal{U}_j)\) is a matrix module, it has a basis \(B_{i,j}, i = 1, 2, \ldots, m\), as in Theorem 1 item 3, for a vector \(b_j \in \mathbb{F}^n\). This means that

\[
\phi(E_{i,j}) = \sum_{s=1}^{m} a_{s,i}^{(j)} B_{s,j},
\]

for some \(a_{s,i}^{(j)} \in \mathbb{F}\), for all \(s,i = 1, 2, \ldots, m\) and \(j = 1, 2, \ldots, n\). If we define the matrix \(A^{(j)} \in \mathbb{F}^{m \times m}\) whose \((s,i)\)-th component is \(a_{s,i}^{(j)}\), and \(B \in \mathbb{F}^{n \times n}\) whose \(j\)-th row is \(b_j\), then a simple calculation shows that

\[
\phi(E_{i,j}) = A^{(j)} E_{i,j} B,
\]

and the matrices \(A^{(j)}\) and \(B\) are invertible. If we prove that there exist non-zero \(\lambda_j \in \mathbb{F}\) with \(A^{(j)} = \lambda_j A^{(1)}\), for \(j = 2, 3, \ldots, n\), then we are done, since we can take the vectors \(\lambda_j b_j\) instead of \(b_j\), define \(A = A^{(1)}\), and then it holds that

\[
\phi(E_{i,j}) = AE_{i,j} B,
\]

for all \(i = 1, 2, \ldots, m\) and \(j = 1, 2, \ldots, n\), implying \((P 1)\).

To this end, we first denote by \(a_{i}^{(j)} \in \mathbb{F}^m\) the \(i\)-th column in \(A^{(j)}\) (written as a row vector). Observe that we have already proven that \(\phi\) preserves ranks. Hence \(\text{Rk}(\phi(E_{i,j} + E_{i,1})) = 1\), which means that \(\text{Rk}(A^{(j)} E_{i,j} + A^{(1)} E_{i,1}) = 1\), which implies that there exist \(\lambda_{i,j} \in \mathbb{F}\) with \(a_{i}^{(j)} = \lambda_{i,j} a_{i}^{(1)}\).

On the other hand, a matrix calculation shows that

\[
\phi \left( \sum_{i=1}^{m} \sum_{j=1}^{n} E_{i,j} \right) = \left( \sum_{i=1}^{m} a_{i}^{(1)}, \sum_{i=1}^{m} a_{i}^{(2)}, \ldots, \sum_{i=1}^{m} a_{i}^{(n)} \right) B
\]
\[
\sum_{i=1}^{m} a_i^{(1)}, \sum_{i=1}^{m} \lambda_i, \ldots, \sum_{i=1}^{m} \lambda_i, a_i^{(1)}\right) B.
\]

Since \( \text{Rk}(\sum_{i=1}^{m} \sum_{j=1}^{n} E_{i,j}) = 1 \) and the vectors \( a_i^{(1)}, 1 \leq i \leq m \), are linearly independent, we conclude that \( \lambda_i, j \) depends only on \( j \) and not on \( i \), and we are done.

Acknowledgement

The authors gratefully acknowledge the support from The Danish Council for Independent Research (Grant No. DFF-4002-00367) and from the JSPS (Grant No. 26289116). The first author is also thankful for the support and guidance of his advisors Olav Geil and Diego Ruano.

References

[1] R. Ahlswede, N. Cai, S. Y. R. Li, and R. W. Yeung. Network information flow. IEEE Trans. Inf. Theory, 46(4):1204–1216, July 2000.

[2] N. Cai and R. W. Yeung. Network coding and error correction. Proc. 2002 IEEE Inform. Theory Workshop, pages 119–122, 2002.

[3] N. Cai and R. W. Yeung. Secure network coding. In Proceedings of the IEEE International Symposium on Information Theory., pages 323–, 2002.

[4] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, and V. Vaikuntanathan. Secure computation from random error correcting codes. In Advances in cryptology—EUROCRYPT 2007, volume 4515 of Lecture Notes in Comput. Sci., pages 291–310. Springer, Berlin, 2007.

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

[6] Ph. Delsarte. Bilinear forms over a finite field, with applications to coding theory. Journal of Combinatorial Theory, Series A, 25(3):226 – 241, 1978.

[7] J. Dieudonné. Sur une généralisation du groupe orthogonal à quatre variables. Archiv der Mathematik, 1(4):282–287, 1948.

[8] J. Ducoat. Generalized rank weights: a duality statement. Topics in Finite Fields, 632:101 – 109, 2015.

[9] I. M. Duursma and S. Park. Coset bounds for algebraic geometric codes. Finite Fields Appl., 16(1):36 – 55, 2010.

[10] S. El Rouayheb, E. Soljanin, and A. Sprintson. Secure network coding for wiretap networks of type II. IEEE Trans. Inf. Theory, 58(3):1361–1371, March 2012.

[11] J. Feldman, T. Malkin, R. Servedio, and C. Stein. On the capacity of secure network coding. In Proceedings of the 42nd Annual Allerton Conference on Communication, Control, and Computing., 2004.

[12] G. D. Forney Jr. Dimension/length profiles and trellis complexity of linear block codes. IEEE Trans. Inf. Theory, 40(6):1741–1752, 1994.

[13] E. Gabidulin. Theory of codes with maximum rank distance. Problems Inform. Transmission, 21, 1985.

[14] E. M. Gabidulin, A. V. Ourivski, B. Honary, and B. Ammar. Reducible rank codes and their applications to cryptography. IEEE Trans. Inf. Theory, 49(12):3289–3293, Dec 2003.

[15] O. Geil, S. Martín, R. Matsumoto, D. Ruano, and Y. Luo. Relative generalized hamming weights of one-point algebraic geometric codes. IEEE Trans. Inf. Theory, 60(10), 2014.

[16] V. Guruswami, C. Wang, and C. Xing. Explicit list-decodable rank-metric and subspace codes via subspace designs. IEEE Trans. Inf. Theory, 62(5):2707–2718, May 2016.
[17] T. Ho, M. Medard, R. Koetter, D.R. Karger, M. Effros, J. Shi, and B. Leong. A random linear network coding approach to multicast. *IEEE Trans. Inf. Theory*, 52(10):4413–4430, Oct 2006.

[18] M. Ito, A. Saito, and T. Nishizeki. Secret sharing scheme realizing general access structure. *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, 72(9):56–64, 1989.

[19] R. Jurrius and R. Pellikaan. On defining generalized rank weights. *arXiv:1506.02865*, 2015.

[20] R. Kötter and M. Medard. An algebraic approach to network coding. *IEEE/ACM Trans. Networking*, 11(5):782–795, Oct 2003.

[21] J. Kurihara, R. Matsumoto, and T. Uyematsu. Relative generalized rank weight of linear codes and its applications to network coding. *IEEE Trans. Inf. Theory*, 61(7):3912–3936, July 2015.

[22] S.-Y.R. Li, R.W. Yeung, and Ning Cai. Linear network coding. *IEEE Trans. Inf. Theory*, 49(2):371–381, Feb 2003.

[23] L. Lidl and H. Niederreiter. *Finite Fields*, volume 20. Encyclopedia of Mathematics and its Applications. Addison-Wesley, Amsterdam, 1986.

[24] Y. Luo, C. Mitrpant, A. J. Han Vinck, and K. Chen. Some new characters on the wire-tap channel of type II. *IEEE Trans. Inf. Theory*, 51(3):1222–1229, 2005.

[25] M. Marcus and B. N. Moyls. Linear transformations on algebras of matrices. *Canad. J. Math.*, 11:61–66, 1959.

[26] U. Martínez-Peñas. On the similarities between generalized rank and Hamming weights and their applications to network coding. *IEEE Trans. Inf. Theory*, 62(7):4081–4095, 2016.

[27] K. Morrison. Equivalence for rank-metric and matrix codes and automorphism groups of gabidulin codes. *IEEE Trans. Inf. Theory*, 60(11):7035–7046, Nov 2014.

[28] F. E. Oggier and A. Shbou. On the existence of generalized rank weights. In *Proceedings of the International Symposium on Information Theory and its Applications, ISITA 2012, Honolulu, HI, USA, October 28-31, 2012*, pages 406–410, 2012.

[29] L. H. Ozarow and A. D. Wyner. Wire-tap channel II. chapter Advances in Cryptology: Proceedings of EUROCRYPT 84 A Workshop on the Theory and Application of Cryptographic Techniques Paris, France, April 9–11, 1984, pages 33–50. Springer Berlin Heidelberg, Berlin, Heidelberg, 1985.

[30] A. Ravagnani. Rank-metric codes and their duality theory. *Designs, Codes and Cryptography*, pages 1–20, 2015.

[31] A. Ravagnani. Generalized weights: An anticode approach. *Journal of Pure and Applied Algebra*, 220(5):1946 – 1962, 2016.

[32] D. Silva and F. R. Kschischang. On metrics for error correction in network coding. *IEEE Trans. Inf. Theory*, 55(12):5479–5490, 2009.

[33] D. Silva and F. R. Kschischang. Universal secure network coding via rank-metric codes. *IEEE Trans. Inf. Theory*, pages 1124–1135, 2011.

[34] H. Stichtenoth. On the dimenion of subfield subcodes. *IEEE Trans. Inf. Theory*, 36(1):90–93, Jan 1990.

[35] V. K. Wei. Generalized Hamming weights for linear codes. *IEEE Trans. Inf. Theory*, 37(5):1412–1418, 1991.

[36] A. D. Wyner. The wire-tap channel. *The Bell System Technical Journal*, 54(8):1355–1387, Oct 1975.

[37] R. Zamir, S. Shamai, and U. Erez. Nested linear/lattice codes for structured multiterminal binning. *IEEE Trans. Inf. Theory*, 48(6):1250–1276, Jun 2002.