On the similarities between generalized rank and Hamming weights and their applications to network coding

Umberto Martínez-Peñas

Department of Mathematical Sciences, Aalborg University, Denmark

July 9, 2015

Abstract

Rank weights and generalized rank weights have been proven to characterize error and erasure correction, and information leakage in linear network coding, in the same way as the Hamming weights and generalized Hamming weights describe classical error and erasure correction, and information leakage in secret sharing. Many similarities between both cases have been studied in the literature. Although many definitions, results and proofs are similar in both cases, it might seem that they are essentially different. The aim of this paper is to further relate both weights and generalized weights, show that the results and proofs in both cases are actually essentially the same, and see the significance of these similarities in network coding. Some of the new results in the rank case also have new consequences in the Hamming case.

Keywords: Rank weight, generalized rank weight, rank distance, rank-metric codes, network coding, network error correction, secure network coding.

MSC: 94B05, 94B65, 94C99.

1 Introduction

Linear network coding has been intensively studied during the last decade [1, 4, 15, 16, 17, 23, 24, 28, 29]. In this model [1, 16], a source transmits $n$ packets through $n$ outgoing links, and in each node of the network, linear combinations of the received packets are generated and sent. At the end, a sink node receives $N$ packets from $N$ ingoing links, containing linear combinations of the original $n$ packets.

In this context, errors are considered as erroneous packets that appear on some links, and erasures are considered as the deficiency of the rank of the matrix that describes the received $N$ packets as combinations of the $n$ sent packets [17, 21]. In secure network coding, an adversary (or several) may compromise the security of the network by doing

*umberto@math.aau.dk
three things: introducing \( t \) erroneous packets on \( t \) different links, modifying the coefficient matrix and obtaining information from the sent packets by wiretapping several links \([17, 23, 24]\).

In classical error and erasure correction \([13]\) and secret sharing \([5, 18, 22]\), the original message or secret is encoded into a vector \( \mathbf{c} = (c_1, c_2, \ldots, c_n) \in \mathbb{F}_q^n \), where \( \mathbb{F}_q \) is some finite field. Then, errors, erasures and information leakage happen component-wise. This means that some components of \( \mathbf{c} \) may be wrong (errors), some components may be erased (erasures), and a wiretapping adversary may obtain some components (information leakage). However, in linear network coding all this happen on some linear combinations: errors are wrong combinations, erasures are losses of combinations, and information leakage is considered in the form of leaked combinations.

In the classical case, Hamming weights and generalized Hamming weights have been used since the origins (see \([13, 27]\)), and they have been proven to be suitable tools for error and erasure correction and secret sharing. On the other hand, in recent years there have been several attempts to find a suitable weight and generalized weight to study linear network coding \([15, 17, 21, 23, 28]\). Finally, rank weights and generalized rank weights, introduced in \([9]\) and \([17, 21]\), respectively, have been proven to describe exactly the worst case error and erasure correction capability \([17, 23, 24]\), and worst case information leakage on networks \([17, 24]\).

Many similarities between the Hamming weights and rank weights have been considered since the paper \([9]\), and for generalized ones since \([17, 21]\). However, most of the results and proofs for rank weights given in the literature are apparently similar but essentially different from those relative to Hamming weights.

The aim of this paper is to give some alternative definitions of rank weights \([9]\) and generalized rank weights \([7, 14, 17, 21]\), and then show that most of the well-known results for Hamming weights, classical error and erasure correction and classical secret sharing, can be directly translated to rank weights, network error and erasure correction and information leakage on networks, once the right definitions and tools are introduced.

Some of the results in this paper are new, and some have already been given in the literature, but for which we give an alternative proof which works in the exact same way as that of the Hamming case.

The new results in this paper are distributed as follows: First in the second section we give some preliminary tools, already given in the literature, most of which follow from \([25]\). In the third section, we gather alternative definitions of rank weights and generalized rank weights from the literature, and propose some new definitions, proving the equivalence between all of them. In the fourth section, we study linear equivalences of codes, that is, vector space isomorphisms between codes that preserve rank weights (and generalized rank weights), which allow to say when two codes perform exactly equally in secure network coding. We establish new characterizations of these equivalences, which also give a connection with information leakage, and obtain the minimum possible lengths of codes, up to these equivalences. In the fifth section, we establish a way to derive bounds on generalized rank weights from bounds on generalized Hamming weights, and give a list of some of these bounds. In the rest of the section, we discuss what the
Singleton bound in the rank case can be, establishing a new alternative version of the Singleton bound. In the sixth section, we introduce the concept of rank-punctured codes, which plays the same role as the classical punctured codes, and which are a main tool for the study of rank weights, erasure correction and information leakage, since punctured codewords are conceptually the same as codewords with erasures. We give and prove a collection of results using this rank-puncturing, in analogy with the Hamming case. Finally, in the seventh section, we revisit some of the results regarding error and erasure correction and information leakage on networks. We obtain some relations regarding information leakage and duality, and propose a slightly different decoder than that of \cite{17, 23}, proving also the characterization of the correction capability of non-linear (in particular, $F_q$-linear) coding schemes, which has not been stated nor proven yet.

2 Definitions and preliminaries

Let $q$ be a prime power and $m$ and $n$, two positive integers. All vectors are considered to be row vectors, and we use the notation $A^T$ to denote the transpose of a matrix $A$. We will use the network model in \cite{17, 23}, where a vector $c \in F_q^n$ is sent through a network with $n$ outgoing links from the source node and where the receiver obtains $y = cA^T + e$, for some coefficient matrix $A \in F_q^{N \times n}$ and some error vector $e \in F_q^N$ (more details will be given in the last section).

A code in $F_q^n$ is just a subset $C \subset F_q^n$, whose length is defined as $n$. This length corresponds to the number of outgoing links from the source in the network. Therefore, $m$ and $n$ do not play a symmetric role. Although it is usual in the literature to only consider the case $n \leq m$, we consider all cases, and we argue as follows (see also \cite{17, Section I.A} for more details): on the one hand, in some Internet protocols, the size of each packet ($m$) is bounded by some parameters of the protocol, whereas the number of outgoing links ($n$) is not necessarily bounded. On the other hand, since many computations are carried out over the extension field $F_q^m$, requiring $m \geq n$ may extremely increase the computational complexity of the encoding and decoding.

We say that $C$ is linear (respectively $F_q$-linear) if it is an $F_q^m$-linear subspace (respectively $F_q$-linear). The term non-linear is used for all codes.

On the other hand, we define a coding scheme (or secret sharing scheme) with message (or secret) set $S$ as a family of disjoint nonempty subsets of $F_q^m$, $P_S = \{C_x\}_{x \in S}$, together with a probability distribution over each of these sets. This corresponds to \cite{17} Definition 7. The scheme is said to be linear if $S = F_q^\ell$, where $0 < \ell \leq n$, and $\alpha C_x + \beta C_y \subset C_{\alpha x + \beta y}$, for all $\alpha, \beta \in F_q^m$ and all $x, y \in F_q^\ell$. Similarly in the $F_q$-linear case (where $S = F_q$, $0 < \ell \leq mn$).

The encoding in the coding scheme is performed as follows: for each $x \in S$, we choose at random (with the chosen distribution) an element $c \in C_x$. With these definitions, the concept of coding scheme generalizes the concept of code, since a code is a coding scheme where $\#C_x = 1$, for each $x \in S$, and thus no probability distribution is required. In
the same way, linear and $\mathbb{F}_q$-linear coding schemes generalize linear and $\mathbb{F}_q$-linear codes, respectively.

The main motivation for introducing coding schemes is to increase the uncertainty about the sent message when an eavesdropper wiretaps some links in the network, as shown in [17] for linear schemes.

An equivalent way to describe linear (and $\mathbb{F}_q$-linear) coding schemes is by pairs of linear codes. We choose linear codes $C_2 \subset C_1 \subset \mathbb{F}_q^n$, a linear space $W$ such that $C_1 = C_2 \oplus W$ and an isomorphism $\psi : \mathbb{F}_q^{\ell} \rightarrow W$, where $\ell = \dim(C_1/C_2)$. Then we define the sets $C_x = \psi(x) + C_2$. If we choose the probability distribution to be uniform, then the encoding can be done as follows: Take uniformly at random $c' \in C_2$ and define $c = \psi(x) + c'$.

This formulation is an extension of Shamir’s scheme [22] and Massey’s scheme [5, Section 3.1], and it is established in [5, Section 4.2], where it is claimed in an informal way that it includes all possible linear coding schemes. We now state this in a formal way, omitting the proof, which is straightforward. The $\mathbb{F}_q$-linear case is completely analogous.

**Proposition 1.** Given a linear coding scheme $P_S = \{C_x\}_{x \in S}$, define $C_1 = \bigcup_{x \in S} C_x$ and $C_2 = C_0$ (recall that $S = \mathbb{F}_q^{\ell}$). Then, $C_1$ and $C_2$ are linear codes in $\mathbb{F}_q^n$ and

1. $C_2 \subset C_1$.

2. The relation given in $C_1$ by $c \sim d$ if, and only if, there exists $x \in \mathbb{F}_q^{\ell}$ such that $c, d \in C_x$, is an equivalence relation that satisfies the following:

$$c \sim d \iff c - d \in C_2.$$ In particular, $P_S = C_1/C_2$.

3. The map $\mathbb{F}_q^{\ell} \rightarrow P_S = C_1/C_2 : x \mapsto C_x$ is a vector space isomorphism.

In particular, if we take a subspace $W \subset C_1$ such that $C_1 = C_2 \oplus W$, then we can canonically define an isomorphism $\psi : \mathbb{F}_q^{\ell} \rightarrow W$ by $C_x \cap W = \{\psi(x)\}$. Of course, it satisfies that $C_x = \psi(x) + C_2$.

On the other hand, if $d : \mathbb{F}_q^n \times \mathbb{F}_q^n \rightarrow \mathbb{N}$ is the rank (respectively Hamming) distance [9, 13], we define the minimum rank (respectively Hamming) distance of the coding scheme $P_S$ as

$$d(P_S) = \min\{d(c_1, c_2) \mid c_1 \in C_{x_1}, c_2 \in C_{x_2}, x_1 \neq x_2\}. \quad (1)$$

For codes we obtain the usual definition of minimum distance. For general coding schemes, it is basically the minimum of the distances between the sets $C_x, x \in S$.

Now we turn to rank weights. We first observe the following obvious fact from linear algebra.
Lemma 1. Let $\alpha_1, \alpha_2, \ldots, \alpha_m$ and $\beta_1, \beta_2, \ldots, \beta_m$ be two bases of $\mathbb{F}_q^n$ over $\mathbb{F}_q$, and let $c \in \mathbb{F}_q^n$ be a vector. It can be written in a unique way as

$$c = \sum_{i=1}^{m} c_i \alpha_i = \sum_{i=1}^{m} d_i \beta_i,$$

where $c_i, d_i \in \mathbb{F}_q$. Moreover,

$$\langle c_1, c_2, \ldots, c_m \rangle_{\mathbb{F}_q} = \langle d_1, d_2, \ldots, d_m \rangle_{\mathbb{F}_q} \subset \mathbb{F}_q^n.$$

Definition 1. Choose one of such bases $\alpha_1, \alpha_2, \ldots, \alpha_m$, and a vector $c \in \mathbb{F}_q^n$. We define the rank support of $c$ as

$$G(c) = \langle c_1, c_2, \ldots, c_m \rangle_{\mathbb{F}_q},$$

where $c = \sum_i c_i \alpha_i$ and $c_i \in \mathbb{F}_q^n$. This is the same notation as [17, Section II.D]

From the previous lemma it follows that $G(c)$ does not depend on the choice of the basis. However, from now on, we fix one such basis $\alpha_1, \alpha_2, \ldots, \alpha_m$.

Definition 2. We define the rank weight of $c$ as $\text{wt}_R(c) = \dim(G(c))$, and for each linear subspace $D \subset \mathbb{F}_q^n$, we define its rank support as $G(D) = \sum_{d \in D} G(d)$ and its rank weight as $\text{wt}_R(D) = \dim(G(D))$.

The definition of rank weight was introduced in [9] and the definition of rank support and rank weight of a linear subspace has been introduced in [14].

Remark 1. We can associate each vector $c \in \mathbb{F}_q^n$ with a matrix over $\mathbb{F}_q$, which we denote as follows:

$$\mu(c) = \begin{pmatrix}
    c_{1,1} & c_{1,2} & \cdots & c_{1,n} \\
    c_{2,1} & c_{2,2} & \cdots & c_{2,n} \\
    \vdots & \vdots & \ddots & \vdots \\
    c_{m,1} & c_{m,2} & \cdots & c_{m,n}
\end{pmatrix},$$

where $c = \sum_i c_i \alpha_i$ and $c_i = (c_{i,1}, c_{i,2}, \ldots, c_{i,n}) \in \mathbb{F}_q$. Note that $\alpha_i e_j$, where $e_j$ is the canonical basis of $\mathbb{F}_q^n$, for $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$, is a basis of $\mathbb{F}_q^n$ over $\mathbb{F}_q$. It follows that $\mu : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^{m \times n}$ is an $\mathbb{F}_q$-linear vector space isomorphism. Moreover, the rank support of $c$ is the row space of $\mu(c)$, which we denote by $\text{row}(\mu(c))$, and the rank weight of $c$ is the rank of $\mu(c)$, denoted by $\text{Rk}(\mu(c))$.

The rank weight of a subspace $D \subset \mathbb{F}_q^n$ is then the rank of the matrix obtained by appending all rows of all matrices corresponding to the vectors in $D$. It can be shown [17, Proposition 3 (4)] that we can take the vectors in a basis of $D$.

Note that $G(c) = G(\langle c \rangle)$ and thus $\text{wt}_R(c) = \text{wt}_R(\langle c \rangle)$, for every $c \in \mathbb{F}_q^n$. Finally we define some tools (see also [25, Section II]):
Definition 3. We define the trace map as follows
\[
\text{Tr} : \mathbb{F}_q^m \rightarrow \mathbb{F}_q : x \mapsto \sum_{i=0}^{m-1} x^{q^i},
\]
and component-wise on vectors. Raising to the power \( q \) is also defined component-wise on vectors. For each linear subspace \( D \subset \mathbb{F}_q^n \), we define its Galois closure as
\[
D^* = \sum_{i=0}^{m-1} D^{q^i};
\]
its trace code as \( \text{Tr}(D) \), its subfield code as \( D|_{\mathbb{F}_q} \), and its extended code as \( D \otimes \mathbb{F}_q^m \), that is, the code generated by \( D \) over \( \mathbb{F}_q^m \), \( (D)_{\mathbb{F}_q^m} \subset \mathbb{F}_q^m \).

We say that \( D \) is Galois closed if \( D = D^* \).

Note that \( \text{Tr} \) is \( \mathbb{F}_q \)-linear and \( D^* \) is the smallest Galois closed linear code containing \( D \). Moreover, a linear subspace \( D \subset \mathbb{F}_q^n \) is Galois closed if, and only if \( D^q \subset D \), which is equivalent to \( D^q = D \).

We now remind some tools that we will need later. The following lemma is a well-known basic result in linear algebra and commutative algebra. We remind the short proof for convenience.

**Lemma 2.** For every linear subspace \( D \subset \mathbb{F}_q^n \), we have that \( \dim_{\mathbb{F}_q}(D) = \dim_{\mathbb{F}_q^m}(D \otimes \mathbb{F}_q^m) \).

**Proof.** Take a basis for \( D \) over \( \mathbb{F}_q \), \( u_1, u_2, \ldots, u_k \), then they generate \( D \otimes \mathbb{F}_q^m \). Now take a linear combination of them over \( \mathbb{F}_q^m \) which equals zero. It can be expressed as \( \sum_{i,j} \lambda_{i,j} \alpha_j u_i = 0 \), \( \lambda_{i,j} \in \mathbb{F}_q \). Therefore, \( \sum_j (\sum_i \lambda_{i,j} u_i) \alpha_j = 0 \), which implies that \( \sum_i \lambda_{i,j} u_i = 0 \), for all \( j \), and thus \( \lambda_{i,j} = 0 \), for all \( i \) and \( j \). \( \square \)

The following is a particular case of [11, Lemma 6]. It also follows from the material in [25, Section II].

**Lemma 3.** For every linear code \( C \subset \mathbb{F}_q^n \), we have that \( C|_{\mathbb{F}_q} \subset \text{Tr}(C) \).

The following proposition easily follows from [25, Lemma 1]:

**Proposition 2.** For every linear code \( C \subset \mathbb{F}_q^m \) of dimension \( k \), the following are equivalent:

1. \( C \) is Galois closed.
2. \( C \) admits a basis of vectors in \( \mathbb{F}_q^n \).
3. \( C \) has a basis consisting of vectors of rank weight 1.
4. \( C = C|_{\mathbb{F}_q} \otimes \mathbb{F}_q^m \).
\[ C = \text{Tr}(C) \otimes \mathbb{F}_{q^m} \]
\[ \text{Tr}(C) = C|_{\mathbb{F}_{q^m}} \]
\[ \dim(\text{Tr}(C)) = k \]
\[ \dim(C|_{\mathbb{F}_{q^m}}) = k \]

We give a final tool, which is due to Delsarte [6, Theorem 2]:

**Lemma 4 (Delsarte).** For every linear code \( C \subset \mathbb{F}_{q^m}^n \), we have that
\[
(C|_{\mathbb{F}_{q^m}})^\perp = \text{Tr}(C)\perp, \quad \text{and} \quad (C\perp)|_{\mathbb{F}_{q^m}} = (\text{Tr}(C)\perp).
\]

### 3 Equivalent definitions of rank weights and generalized rank weights

In this section we recall the definition of generalized rank weight [17, 21], together with its relative version [17], and prove the equality of this definition with others, one of which have already been proposed in [14], and some of which are new. The original definition [17] is the most suitable for describing information leakage. However, the other definitions will be of crucial importance regarding error correction, bounds, equivalences, and other properties that we will see in the next sections.

First, we start by giving alternative expressions for rank weights. Note that, although generalized rank weights will be defined for linear codes, these equivalent definitions of rank weights can be used to treat minimum rank distances and rank weight distributions of non-linear codes. On the other hand, remember the definition of Hamming weight of a linear subspace \( D \subset \mathbb{F}_{q^m}^n \) [13, 27]:
\[
\text{wt}_H(D) = \# \{ i \in \{1,2,\ldots,n\} \mid \exists d \in D \text{ such that } d_i \neq 0 \}.
\]

**Theorem 1.** For any linear subspace \( D \subset \mathbb{F}_{q^m}^n \), we have that
\[
\text{wt}_R(D) = \text{wt}_R(D^*) = \dim(\text{Tr}(D)) = \dim(D^*) = \\
= \min\{\text{wt}_H(\varphi_B(D)) \mid B \subset \mathbb{F}_q^n \text{ is a basis of } \mathbb{F}_{q^m}^n \},
\]
where \( \varphi_B : \mathbb{F}_{q^m}^n \rightarrow \mathbb{F}_{q^m}^n \) is the linear map defined as \( \varphi_B(c) = x \), where \( c = \sum_i x_i v_i \) and \( B = \{v_i\}_i \). In particular, for every vector \( c \in \mathbb{F}_{q^m}^n \), we have that
\[
\text{wt}_R(c) = \min\{\text{wt}_H(x) \mid c = \sum_i x_i v_i, B = \{v_i\} \subset \mathbb{F}_q^n \text{ is a basis of } \mathbb{F}_{q^m}^n \}.
\]

We will prove Theorem 1 at the end of the section. The equality \( \text{wt}_R(D) = \dim(\text{Tr}(D)) \) in the first line follows directly from [14, Theorem 16], and the equality \( \dim(D^*) = \dim(\text{Tr}(D)) \) is immediate from Proposition 2. In [17, Lemma 11], the equality \( \text{wt}_R(D) = \dim(D^*) \) is proven when \( \dim(D) = 1 \). Therefore, we attribute the equalities in the first
line to a combination of [25] with [17], for \( \dim(D) = 1 \), and with [14] for the general case. The equality with the last value is new. Here we will give a different and elementary proof of the theorem. On the other hand, we will see that the value \( \dim(D^*) \) plays the same role as \( \dim(V_I) \) for Hamming weights, where \( I = \text{Supp}(D) = \{ i \mid \exists d \in D, d_i \neq 0 \} \) and \( V_I = \{ c \in \mathbb{F}_{q^m}^n \mid c_i = 0, \forall i \notin I \} \), and therefore it is natural to be considered.

**Lemma 5.** For every linear subspace \( D \subset \mathbb{F}^n_{q^m} \), it holds that \( \text{wt}_R(D) \leq \text{wt}_H(D) \).

**Proof.** It will immediately follow from the previous theorem. To see it from the definitions, take \( i \) and assume that \( d_i = 0 \), for all \( d \in D \), then all matrices \( \mu(d) \), where \( d \in D \), have zeroes in the \( i \)-th column. Therefore, according to the last part of Remark 1, the rank weight of \( D \) is at most \( n \) minus the number of such indices, which is the Hamming weight of \( D \).

Observe that a study of rank weights of linear subspaces of a code \( C \) has the following interest in error correction: any vector \( c \in D \), satisfies \( \text{wt}_R(c) \leq \text{wt}_R(D) \), and in the case \( n \leq m \), there exists \( c \in D \) that satisfies the equality [14, Proposition 10]. Therefore, knowing which subspaces have lower weights helps to locate vectors with low weight.

Now we define generalized rank weights and their relative version, introduced in [17]. Recall the definition of generalized Hamming weight of a code \( C \) [27], and relative generalized Hamming weight of a code pair \( C_2 \subset C_1 \) [20]:

\[
d_{H,r}(C) = \min\{ \#I \mid I \subset \{1,2,\ldots,n\}, \dim(C \cap V_I) \geq r \},
\]

\[
M_{H,r}(C_1,C_2) = \min\{ \#I \mid I \subset \{1,2,\ldots,n\}, \dim((C_1 \cap V_I)/(C_2 \cap V_I)) \geq r \}.
\]

**Definition 4.** For a linear code \( C \subset \mathbb{F}^n_{q^m} \) and \( 1 \leq r \leq \dim(C) \), we define its \( r \)-th generalized rank weight as

\[
d_{R,r}(C) = \min\{ \dim V \mid V \subset \mathbb{F}^n_{q^m}, V = V^*, \dim(C \cap V) \geq r \}.
\]

For a code pair \( C_2 \subset C_1 \subset \mathbb{F}^n_{q^m} \), we define its \( r \)-th relative generalized rank weight as

\[
M_{R,r}(C_1,C_2) = \min\{ \dim V \mid V \subset \mathbb{F}^n_{q^m}, V = V^*, \dim((C_1 \cap V)/(C_2 \cap V)) \geq r \}.
\]

**Theorem 2.** For a linear code \( C \subset \mathbb{F}^n_{q^m} \) and \( 1 \leq r \leq k = \dim(C) \), the following numbers are equal:

\[
d_{R,r}(C) = \min\{ \dim V \mid V \subset \mathbb{F}^n_{q^m}, V = V^*, \dim(C \cap V) \geq r \},
\]

\[
\min\{ \text{wt}_R(D) \mid D \subset C, \dim(D) = r \},
\]

\[
\min\{ d_{H,r}(\varphi_B(C)) \mid B \subset \mathbb{F}^n_q \text{ is a basis of } \mathbb{F}^n_{q^m} \},
\]

\[
n - \max\{ \dim(L_U^G) \mid U \subset \mathbb{F}^k_{q^m}, \dim(U) = k - r \},
\]

where \( G \) is a generator matrix of \( C \), \( \varphi_B \) is as in Theorem [1] and \( L_U^G = \{ x \in \mathbb{F}^n_q \mid Gx^T \in U \} \).
The first definition is due to Kurihara et al. [17] Definition 2, and the second one is due to Jurrius and Pellikaan [14] Definition 5, proven to be equivalent in [14] Theorem 21. Definitions (6) and (7) are new. Definition (7) is an analogous description as that of [12] Lemma 1 for generalized Hamming weights, and is expressed in terms of a generator matrix of the code.

Remark 2. In [21] Section IV] and [7] Section II] another equivalent definition is given (with a slight difference in [21]), and proven to be equivalent to the first one in [7], when \( n \leq m \):

\[
d_{R,r}(C) = \min \{ \max \{ \text{wt}_R(x) \mid x \in D^* \} \mid D \subset C \text{ and } \dim(D) = r \}.
\]

Theorem 3. For a code pair \( C_2 \subsetneq C_1 \subset \mathbb{F}_{q^m}^n \) and \( 1 \leq r \leq \ell = \dim(C_1/C_2) \), the following numbers are equal:

\[
M_{R,r}(C_1,C_2) = \min \{ \dim(V) \mid V \subset \mathbb{F}_{q^m}^n, V = V^* \}, \quad \dim((C_1 \cap V)/(C_2 \cap V))^r \}
\]

\[
\min \{ \text{wt}_R(D) \mid D \subset C_1, D \cap C_2 = 0, \dim(D) = r \},
\]

\[
\min \{ M_{H,r}(\varphi_B(C_1),\varphi_B(C_2)) \mid B \subset \mathbb{F}_q^n \text{ is a basis of } \mathbb{F}_q^n \},
\]

\[
n - \max \{ \dim(L_i) \mid U \subset \mathbb{F}_{q^m}^n, \dim(U) = k_1 - r, \dim(U^I) = k_2 \},
\]

where \( \varphi_B \) is as in Theorem 1. \( G \) is a generator matrix of \( C_1 \), the first \( k_2 \) rows of \( G \) are a basis of \( C_2 \) and \( U^I \) is the projection of \( U \) onto the first \( k_2 \) coordinates.

Now, the last definition is analogous to [30] Lemma 2 for the Hamming case. Note that, for a linear coding scheme \( \mathcal{P}_S \) built from \( C_2 \subsetneq C_1 \), we have that \( d_R(\mathcal{P}_S) = M_{R,1}(C_1,C_2) \).

Remark 3. Note that, since \( V_I^* = V_I \), for all \( I \subset \{1,2,\ldots,n\} \), it follows from the definitions that \( d_{R,r}(C) \leq d_{H,r}(C) \), for every linear code \( C \) and every \( 1 \leq r \leq \dim(C) \), as remarked in [17] Remark 1. This also follows from [4] and Lemma 4. Similarly for relative weights.

We will give the proofs of these last three theorems at the end of the section. First, we will prove some lemmas that we will need for this purpose, which also give properties that we will use later.

The next lemma is analogous to the fact that \( \text{wt}_H(D) = \text{wt}_H(V_I) \), where \( I = \text{Supp}(D) \).

Lemma 6. For every linear subspace \( D \subset \mathbb{F}_{q^m}^n \), we have that \( \text{wt}_R(D) = \text{wt}_R(D^*) \).

Proof. Let \( d \in \mathbb{F}_{q^m}^n \), \( d = d_1a_1 + d_2a_2 + \cdots + d_na_m \), with \( d_i \in \mathbb{F}_q^n \). It holds that \( d^* = d_1a_1^* + d_2a_2^* + \cdots + d_ma_m^* \). Thus, it follows that \( G(d^*) \subset G(d) \), and thus \( G(D^*) \subset G(D) \). The other inclusion follows from \( D \subset D^* \), so the result follows.
On the other hand, the next lemma is analogous to the fact that \( \text{wt}_H(V_I) = \dim(V_I) \), and the subspaces \( V_I \) are the only ones satisfying this. It follows easily from Proposition 2 but we give the proof for convenience.

**Lemma 7.** A linear code \( C \subset \mathbb{F}_q^n \) is Galois closed if, and only if, \( \text{wt}_R(C) = \dim(C) \).

**Proof.** Assume that \( C \) is Galois closed. We can also assume that \( \alpha_1 = 1 \in \mathbb{F}_q \). It follows from this choice of basis \( (\alpha_1 = 1) \) that \( C|\mathbb{F}_q \subset G(C) \), and thus from Proposition 2 we obtain that \( \dim_{\mathbb{F}_q}(C) = \dim_{\mathbb{F}_q}(C|\mathbb{F}_q) \leq \text{wt}_R(C) \).

On the other hand, \( C \) admits a basis in \( \mathbb{F}_q^n \) (by Proposition 2), say \( u_1, u_2, \ldots, u_k \). Since every vector \( c \in C \) can be written as \( c = \sum_j c_j \alpha_j \), where \( c_j \in \langle u_1, u_2, \ldots, u_k \rangle \mathbb{F}_q \), we conclude that \( G(c) \subset C|\mathbb{F}_q \), and thus \( \text{wt}_R(C) \leq \dim_{\mathbb{F}_q}(C|\mathbb{F}_q) = \dim_{\mathbb{F}_q^n}(C) \), where the last equality follows from Proposition 2.

Now assume that \( \text{wt}_R(C) = \dim(C) \). Then, \( \dim(C) = \text{wt}_R(C) = \text{wt}_R(C^*) = \dim(C^*) \), and the middle equality is the previous lemma, and the last equality follows from the direct implication of this lemma. Therefore \( C = C^* \) and we are done. \( \square \)

The following lemma is [13] Theorem 16, but we give an elementary proof.

**Lemma 8.** For every linear code \( C \subset \mathbb{F}_q^n \), we have that \( G(C) = \text{Tr}(C) \).

**Proof.** First, if \( c \in C \) is written as \( c = \sum_i c_i \alpha_i \), with \( c_i \in \mathbb{F}_q^n \), then \( \text{Tr}(c) = \sum_i \text{Tr}(\alpha_i) c_i \in G(c) \), and thus \( \text{Tr}(C) \subset G(C) \).

On the other hand,

\[
\dim(G(C)) = \text{wt}_R(C) = \text{wt}_R(C^*) = \dim(C^*) = \dim(\text{Tr}(C^*)) = \dim(\text{Tr}(C)) ,
\]

where the second equality follows from Lemma 6 the third one from Lemma 7 the fourth one from Proposition 2 and the last one from the fact that \( \text{Tr}(C^*) = \text{Tr}(C) \), and the result follows. \( \square \)

**Remark 4.** Observe that, for any linear space \( D \subset \mathbb{F}_q^n \), it holds that \( D^* = G(D) \otimes \mathbb{F}_q \) or, equivalently, \( G(D) = (D^*)|\mathbb{F}_q \), and \( \dim_{\mathbb{F}_q}(G(D)) = \dim_{\mathbb{F}_q^n}(D^*) \). This is analogous to the fact that the support \( I = \text{Supp}(D) \) is what defines the space \( V_I \), and the size of the support measures the dimension of \( V_I \).

**Lemma 9.** For every linear subspace \( D \subset \mathbb{F}_q^n \), we have that

\[
\text{wt}_R(D) = \min\{\text{wt}_H(\varphi_B(D)) \mid B \subset \mathbb{F}_q^n \text{ is a basis of } \mathbb{F}_q^n \}.
\]

**Proof.** We first proof the inequality \( \leq \): Since \( B \subset \mathbb{F}_q^n \), it follows that \( \varphi_B(c^\theta) = \varphi_B(c)^\theta \), for all \( c \in \mathbb{F}_q^n \), and therefore, \( \varphi_B(D^*) = \varphi_B(D)^* \). Hence \( \text{wt}_R(D) = \text{wt}_R(\varphi_B(D)) \leq \text{wt}_H(\varphi_B(D)) \), where the last inequality follows from Lemma 5.

Now we proof the inequality \( \geq \): Since \( D^* \) is Galois closed, it has a basis \( v_1, v_2, \ldots, v_s \in \mathbb{F}_q^n \), which can be extended to a basis \( B = \{v_1, v_2, \ldots, v_n\} \subset \mathbb{F}_q^n \) of \( \mathbb{F}_q^n \). Then \( \text{Supp}(\varphi_B(D)) \subset \{1, 2, \ldots, s\} \), since \( \varphi_B(v_i) = e_i \), where the vectors \( e_i \) constitute the canonical basis. Therefore, \( \text{wt}_R(D) = \dim(D^*) \geq \text{wt}_H(\varphi_B(D)) \), and the inequality follows. \( \square \)
Finally, we will now prove Theorem 1, Theorem 2 and Theorem 3.

Proof of Theorem 1. The equality $\text{wt}_R(D) = \text{wt}_R(D^*)$ follows from Lemma 6, the equality $\text{wt}_R(D^*) = \dim(D^*)$ follows from Lemma 7, and the equality $\dim(D^*) = \dim(\text{Tr}(D))$ follows from Proposition 2 and the fact that $\text{Tr}(D^*) = \text{Tr}(D)$. The last equality follows from Lemma 9.

Proof of Theorem 2. The equality between (4) and (5) is proven in [14, Theorem 21], and the equality between (5) and (6) follows from Theorem 1 or Lemma 9. Finally, we prove the equality between (5) and (7). Fix $U \subset F_{q^m}^n$ with $\dim(U) = k - r$, and define $V = U^\perp$ and $D = \{ vG \mid v \in V \}$. It holds that $\dim(D) = r$, and for any $x \in F_q^n$, $Gx^T \in U \iff vGx^T = 0, \forall v \in V \iff d \cdot x = 0, \forall d \in D \iff x \in D^\perp$, and thus $L_I^J = (D^\perp)|_{F_q^n}$. Using Theorem 1 and Delsarte’s Lemma 4, $$\text{wt}_R(D) = \dim(\text{Tr}(D)) = n - \dim(L_I^J),$$ and we are done.

Proof of Theorem 3. It is analogous to the proof of Theorem 2.

4 Equivalences of codes

The purpose of this section is to characterize the $F_{q^m}$-linear vector space isomorphisms $\phi : V \rightarrow V'$ that preserve rank weights, where $V, V'$ are Galois closed. A first characterization has been given in [3, Theorem 1], for $V = V' = F_{q^m}^n$. We will see that, due to these characterizations, equivalent codes are guaranteed to exactly perform in the same way in secure network coding, and not only regarding worst cases (which would be guaranteed just by having the same minimum rank distance). Moreover, in contrast with [3], we consider equivalent codes with different lengths, which allows to consider equivalent codes that can be applied to networks with different number of outgoing links. As a consequence, we will see which is the minimum possible length of a code equivalent to a given one, that is, which is the minimum number of outgoing links that a given code requires.

First, define the sets $\Upsilon(F_{q_m}^n)$ and $\Lambda(F_{q_m}^n)$ as the set of Galois closed linear subspaces of $F_{q_m}^n$ and the set of subspaces of the form $V_I$ for some $I \subset J = \{1, 2, \ldots, n\}$, respectively, as in [17]. We will write just $\Upsilon$ and $\Lambda$ if there is no confusion on the space $F_{q_m}^n$. For convenience, we also define $L_I = \{ c \in F_q^n \mid c_i = 0, \text{ if } i \notin I \}$.

The rank weights are defined in terms of the spaces in $\Upsilon$ (see [4] or [17]), and the Hamming weights are defined in terms of the spaces in $\Lambda$ (see [2], [18] or [17]). We will use this analogy in the rest of the paper.

The proof of the following theorem is analogous to the rank case, and therefore we omit it.
Theorem 4. Given an $F_{q^m}$-linear vector space isomorphism $\phi : V \rightarrow V'$, where $V \in \Lambda(F_{q^m})$ and $V' \in \Lambda(F_{q^m})$, the following are equivalent:

1. If $c \in V$ and $\text{wt}_H(c) = 1$, then $\text{wt}_H(\phi(c)) = 1$.

2. $\phi$ preserves Hamming weights, that is, $\text{wt}_H(\phi(c)) = \text{wt}_H(c)$, for all $c \in V$.

3. For all linear subspaces $D \subset V$, it holds that $\text{wt}_H(\phi(D)) = \text{wt}_H(D)$.

4. For all $U \in \Lambda(F_{q^m})$, $U \subset V$, it holds that $\phi(U) \in \Lambda(F_{q^m})$.

5. $\phi$ is a monomial map. That is, if $V = V_I$ and $V' = V_J$, with $N = |I| = |J|$, then there exists a bijection $\sigma : I \rightarrow J$ and elements $\gamma_1, \gamma_2, \ldots, \gamma_N \in F_{q^m}$ such that $\phi(e_i) = \gamma_i e_{\sigma(i)}$, for all $i \in I$.

We will say that $\phi$ is a Hamming weight preserving transformation or a Hamming equivalence.

For rank weights we have a similar characterization.

Theorem 5. Given an $F_{q^m}$-linear vector space isomorphism $\phi : V \rightarrow V'$, where $V \in \Upsilon(F_{q^m})$ and $V' \in \Upsilon(F_{q^m})$, the following are equivalent:

1. If $c \in V$ and $\text{wt}_R(c) = 1$, then $\text{wt}_R(\phi(c)) = 1$.

2. $\phi$ preserves rank weights, that is, $\text{wt}_R(\phi(c)) = \text{wt}_R(c)$, for all $c \in V$.

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

4. For all $U \in \Upsilon(F_{q^m})$, $U \subset V$, it holds that $\phi(U) \in \Upsilon(F_{q^m})$.

5. There exists $\beta \in F_{q^m}^*$ and an $F_{q^m}$-linear vector space isomorphism $\phi' : V \rightarrow V'$ such that $\phi'(V|F_q) \subset V'|F_q$ and $\phi(c) = \beta \phi'(c)$, for every $c \in V$. Equivalently, there exists a matrix $A \in F_{q^m}^{n \times n'}$ and $\beta \in F_{q^m}^*$ such that $\phi(c) = \beta cA$, for every $c \in V$.

We will say that $\phi$ is a rank weight preserving transformation or a rank-metric equivalence.

Proof. It is obvious that item 2 implies item 1 and item 3 implies item 2.

We now see that item 4 implies item 3. First, the number of sets in the family $\Upsilon(F_{q^m})$ that are contained in $V$ is the same as the number of sets in the family $\Upsilon(F_{q^m})$ that are contained in $V'$, since $\dim(V) = \dim(V')$. It follows that, given a linear subspace $U \subset V$, $U \in \Upsilon(F_{q^m})$ if, and only if, $\phi(U) \in \Upsilon(F_{q^m})$. Now given a linear subspace $D \subset V$, since $D^*$ is the smallest set in $\Upsilon(F_{q^m})$ that contains $D$, it follows that $\phi(D^*) = \phi(D)^*$. Therefore, $\text{wt}_R(D) = \dim(D^*) = \dim(\phi(D)^*) = \dim(\phi(D^*)) = \text{wt}_R(\phi(D))$.

To prove that item 5 implies item 4, it is enough to show that, for a given subspace $U \subset V$, if $U^q \subset U$, then $\phi(U)^q \subset \phi(U)$. Take bases $B = \{v_1, v_2, \ldots, v_N\}$ and $B' = \{v'_1, v'_2, \ldots, v'_N\}$ of $V$ and $V'$ in $F_q^m$, respectively, such that $v'_i = \phi(v_i)$. Take $u \in U$,
and write it as \( u = \sum_{i,j} \lambda_{ij} \alpha_j v_i \), where \( \lambda_{ij} \in \mathbb{F}_q \). Then \( \phi(u)^q = \sum_{i,j} \lambda_{ij} \beta^q \alpha^q_j v_i \). Since \( \phi(u)^q = \sum_{i,j} \lambda_{ij} \beta \alpha^q_j v_i \in \phi(U) \), it follows that \( \phi(u)^q \in \phi(U) \).

Finally, we prove that item 1 implies item 5, which is a slight modification of the proof given in [3]. Taking a basis of \( V \) in \( \mathbb{F}_q^m \) as before, it holds that \( \phi(v_i) = \beta_i u_i \), for some \( u_i \in \mathbb{F}_q^n \) and \( \beta_i \in \mathbb{F}_q^m \). Since \( \phi \) is an isomorphism, the vectors \( u_i \) are linearly independent.

Now take \( i \neq j \) and assume that \( \beta_i \neq a_{i,j} \beta_j \), for every \( a_{i,j} \in \mathbb{F}_q \). Then there exists a basis of \( \mathbb{F}_q^m \) over \( \mathbb{F}_q \) that contains \( \beta_i \) and \( \beta_j \). Therefore \( \phi(v_i + v_j) = \beta_i u_i + \beta_j u_j \), but \( \operatorname{wt}_R(\phi(v_i + v_j)) = \operatorname{wt}_R(v_i + v_j) = 1 \) and also \( \operatorname{wt}_R(\beta_i u_i + \beta_j u_j) = 2 \), since \( u_i \) and \( u_j \) are linearly independent.

We have reached an absurd, so there exists \( a_{i,j} \in \mathbb{F}_q^* \) such that \( \beta_i = a_{i,j} \beta_j \), for all \( i, j \). Defining \( \beta = \beta_1 = a_{1,j} \beta_j \) and \( v_i = a_{1,i}^{-1} u_i \), we obtain a description of \( \phi \) as in item 5. \( \square \)

This motivates the following definition.

**Definition 5.** We say that two (non-linear) codes \( C \subset \mathbb{F}_q^n \) and \( C' \subset \mathbb{F}_q^m' \) are rank-metric equivalent if there exists a rank-metric equivalence \( \phi \) between \( V \) and \( V' \) such that \( \phi(C) = C' \), where \( C \subset V \in \Upsilon(\mathbb{F}_q^n) \) and \( C' \subset V' \in \Upsilon(\mathbb{F}_q^m') \). Similarly for Hamming equivalent codes.

**Remark 5.** Observe that item 2 states that equivalent codes behave exactly in the same way regarding error and erasure correction, and not just in worst cases, since corresponding codewords have the same rank weight. On the other hand, item 4 states that equivalent linear codes behave exactly in the same way regarding information leakage, and not only in worst cases, since the information leaked by wiretapping links is measured by the dimension of \( C \cap U \), for some \( U \in \mathcal{T} \), as stated in [17, Lemma 7]. The previous theorem thus states that one property is preserved if, and only if, the other is preserved.

The same holds for the Hamming case, where item 4 states that equivalent codes behave exactly in the same way regarding information leakage in secret sharing [10, 18], and item 2 states that equivalent codes behave exactly in the same way regarding usual error and erasure correction.

Item 1 states that it is only necessary for codes to be equivalent that they behave in the same way regarding “unitary” errors.

**Remark 6.** Observe that, due to the equivalence between items 2 and 3, rank weight preserving transformations preserve not only minimum rank distances and rank weight distributions, but also generalized rank weights and generalized rank weight distributions.

**Remark 7.** In the Hamming case, if \( \phi : C_1 \rightarrow C_2 \) is an \( \mathbb{F}_q^m \)-linear vector space isomorphism that preserves Hamming weights, for arbitrary linear codes \( C_1 \subset \mathbb{F}_q^n \) and \( C_2 \subset \mathbb{F}_q^m \), then it can be extended to a Hamming weight preserving isomorphism \( \tilde{\phi} : V_i \rightarrow V_j \), where \( I = \operatorname{Supp}(C_1) \) and \( J = \operatorname{Supp}(C_2) \). This is known as MacWilliams extension theorem (see [13, Section 7.9]).

However, this is not true in the rank case. For a counterexample, see [2, Example 2.9 (a)].
As a consequence, we can now establish the following relations between Hamming and rank weights:

**Theorem 6.** For any linear codes $D, C \subset \mathbb{F}_{q^n}$, we have that

\[
\begin{align*}
\text{wt}_R(D) &= \min \{ \text{wt}_H(\phi(D)) \mid \phi : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_{q^n} \text{ is a rank-metric equivalence} \}, \\
\text{d}_r(C) &= \min \{ d_{H,r}(\phi(C)) \mid \phi : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_{q^n} \text{ is a rank-metric equivalence} \},
\end{align*}
\]

where $1 \leq r \leq k = \dim(C)$. Moreover, if $n \leq m$, we have that

\[
\begin{align*}
\text{wt}_H(D) &= \max \{ \text{wt}_R(\phi(D)) \mid \phi : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_{q^n} \text{ is a Hamming equivalence} \}, \\
\text{d}_{H,k}(C) &= \max \{ d_{R,k}(\phi(C)) \mid \phi : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_{q^n} \text{ is a Hamming equivalence} \}.
\end{align*}
\]

**Proof.** The first two equalities follow from the previous theorem, together with Theorem 4 and Theorem 2, respectively.

To conclude, we need to prove that there exists a Hamming equivalence $\phi$ such that $\text{wt}_H(D) = \text{wt}_R(\phi(D))$. By taking a suitable Hamming equivalence, we may assume that $D$ has a generator matrix $G$ of the following form: the rows in $G$ (a basis for $D$) are $g_1, g_2, \ldots, g_r$, and there exist $0 = t_0 < t_1 < t_2 < \ldots < t_r \leq n$ such that, for every $i = 1, 2, \ldots, r$, $g_{i,j} = 1$ if $t_{i-1} < j \leq t_i$, and $g_{i,j} = 0$ if $t_i < j$. Observe that $t_r = \text{wt}_H(D)$.

Finally, choose a basis $\gamma_1, \gamma_2, \ldots, \gamma_m$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and define the Hamming equivalence $\phi(c_1, c_2, \ldots, c_n) = (\gamma_1 c_1, \gamma_2 c_2, \ldots, \gamma_n c_n)$. Then, $\phi(D)$ has a generator matrix whose rows are $h_i = \phi(g_i)$, which satisfy that $h_{i,j} = \gamma_j$ if $t_{i-1} < j \leq t_i$, and $h_{i,j} = 0$ if $t_i < j$.

It follows that $G(\phi(D)) = \sum_{i=1}^r G(h_i) = V_I$, where $I = \{1, 2, \ldots, t_r\}$, and we are done. \qed

Now we turn to degenerate codes in the rank case, extending the study in [14, Section 6].

**Definition 6.** A linear code $C \subset \mathbb{F}_{q^n}$ is rank degenerate if it is rank-metric equivalent to a linear code $C' \subset \mathbb{F}_{q^{n'}}$ with $n' < n$.

Hamming degenerate codes are defined in the analogous way. As in the Hamming case, rank degenerate codes are identified by looking at their last generalized rank weight. This is the definition of rank degenerate codes used in [14]. However, note that our definition actually states whether a given code does not require the given length, which in network coding means whether a code can be implemented with less outgoing links from the source node (note that it is obvious that a given code can be implemented with more outgoing links, by extending it trivially).

Note that, from the previous theorem, for every $V \in \mathcal{Y}(\mathbb{F}_{q^n})$, and every basis $B \subset \mathbb{F}_q$ of $V$, the $\mathbb{F}_{q^n}$-linear map $\psi_B : V \rightarrow F_{q^n}^{\dim(V)}$, given by $\psi_B(c) = x$, if $B = \{v_i\}$ and $c = \sum_i x_i v_i$, is a rank-metric equivalence.
Lemma 10. A linear code $C \subset \mathbb{F}_q^n$ of dimension $k$ is rank degenerate if, and only if, $d_{R,k}(C) < n$, or equivalently, $C^* \neq \mathbb{F}_q^n$.

Proof. If $C$ is rank degenerate, it is rank equivalent to a linear code $C' \subset \mathbb{F}_q^{n'}$ with $n' < n$. Therefore, $d_{R,k}(C) = d_{R,k}(C') \leq n' < n$.

Now assume that $C^* \neq \mathbb{F}_q^n$. Take $V = C^*$ and $\psi_B$ as before. If $C' = \psi_B(C)$, then it is rank-metric equivalent to $C$, and $C' \subset \mathbb{F}_q^\dim(C^*)$, where $\dim(C^*) < n$.

Therefore, $d_{R,k}(C)$ gives the minimum possible length (minimum number of outgoing links required by $C$) of a linear code that is rank equivalent to $C$. On the other hand, we obtain the following result. The first part is [14, Corollary 30].

Proposition 3. If $mk < n$, then every linear code $C \subset \mathbb{F}_q^n$ of dimension $k$ is rank degenerate. On the other hand, if $mk \geq n$, then there exists a code $C \subset \mathbb{F}_q^n$ of dimension $k$ that is not rank degenerate.

Proof. The first part follows from the previous lemma and the fact that $\dim(C^*) \leq mk$.

Now, if $mk \geq n$, choose $\lambda_{i,j}^{(i)} \in \mathbb{F}_q$, for $1 \leq i \leq k$, $1 \leq j \leq n$ and $1 \leq l \leq m$, such that $\langle \{x_{l,i}\}_{i,j} \rangle = \mathbb{F}_q^n$, where $x_{l,i} = \sum_j \lambda_{l,j}^{(i)} e_j$ and $e_j$ is the canonical basis of $\mathbb{F}_q^n$. This is possible since $mk \geq n$.

On the other hand, define $u_i = \sum_j \alpha_i x_{l,i} \in \mathbb{F}_q^n$, and $C' = \langle u_1, u_2, \ldots, u_k \rangle$. Then, $C'^* = \mathbb{F}_q^n$ and $\dim(C') \leq k$. Taking $C' \subset C$, with $\dim(C) = k$, we obtain the desired code.

5 Bounds on generalized rank weights

In this section we establish a method to derive bounds on generalized rank weights from bounds on generalized Hamming weights, and afterwards we discuss what the Singleton bound can be for generalized rank weights. Due to [17, Lemma 7 and Theorem 2], bounds on generalized rank weights directly translate into bounds on worst case information leakage on networks, and therefore are of significant importance. Some attempts to give bounds similar to the ones in the Hamming case have been made [7, 17, 21]. Here we prove that most of the bounds in the Hamming case can be directly translated to the rank case.

Note that, since the rank weights are smaller than or equal to the Hamming weights (by Lemma 5), every bound of the form

$$
M \geq g_{s_1, s_2, \ldots, s_N}(d_{s_1}(C), d_{s_2}(C), \ldots, d_{s_N}(C)),
$$

that is valid for Hamming weights, where $g_{s_1, s_2, \ldots, s_N}$ is increasing in each component, is obviously also valid for rank weights. This is the case of the classical Singleton or Griesmer bounds [13, Section 7.10]. On the other hand, the next result is not straightforward if we do not use (6).
Theorem 7. Fix numbers \( k \) and \( 1 \leq r, s \leq k \), and functions \( f_{r,s}, g_{r,s} : \mathbb{N} \to \mathbb{R} \), which may also depend on \( n, m, k \) and \( q \). If \( g_{r,s} \) is increasing, then every bound of the form

\[
f_{r,s}(d_r(C)) \geq g_{r,s}(d_s(C))
\]

that is valid for generalized Hamming weights, for any linear code \( C \subset \mathbb{F}_q^m \) with \( \dim(C) = k \), is also valid for generalized rank weights. The same holds for relative weights.

Proof. From Theorem 2 there exists a basis \( B \subset \mathbb{F}_q^n \) of \( \mathbb{F}_q^n \) such that \( d_{R,r}(C) = d_{H,r}(\varphi_B(C)) \). Therefore,

\[
f_{r,s}(d_{R,r}(C)) = f_{r,s}(d_{H,r}(\varphi_B(C))) \geq g_{r,s}(d_{H,s}(\varphi_B(C))) \geq g_{r,s}(d_{R,s}(C)),
\]

where the last inequality follows again from Theorem 2. Similarly for relative weights. \( \square \)

Remark 8. The previous theorem is also valid, with the same proof, for the more general bounds

\[
f_{r,s_1,s_2,\ldots,s_N}(d_r(C)) \geq g_{r,s_1,s_2,\ldots,s_N}(d_{s_1}(C), d_{s_2}(C), \ldots, d_{s_N}(C)),
\]

where \( g_{r,s_1,s_2,\ldots,s_N} \) is increasing in each component. However, most of the bounds in the literature are of the form of the previous theorem.

In [12] and [26, Part I, Section III.A], many of these kind of bounds are given for generalized Hamming weights. One of these (a particular case of [26, Corollary 3.6]) is proven for rank weights in [7, Proposition II.3], using (4). Some of these are also valid for relative weights (see [30] Proposition 1 and Proposition 2) or [31]). We next list some of these bounds, where \( 1 \leq r \leq s \leq k \), and \( d_j = d_{R,j}(C) \), for all \( j \). Note that monotonicity is one of this bounds, and therefore it does not need a specific proof. Also recall that linear codes in this paper are \( \mathbb{F}_q^m \)-linear, and hence the field size is \( q^m \), not \( q \).

1. Monotonicity:

\[
d_{r+1} \geq d_r + 1,
\]

2. Griesmer-type ([26 bound (14))):

\[
d_r \geq \sum_{i=0}^{r-1} \left\lceil \frac{d_1}{q^m i} \right\rceil,
\]

3. Griesmer-type ([26 bound (16))):

\[
d_s \geq d_r + \sum_{i=0}^{s-r} \left\lceil \frac{(q^m - 1)d_r}{(q^mr - 1)q^mi} \right\rceil,
\]

4. [12, Theorem 1] or [26 bound (18)):

\[
(q^{ms} - 1)d_r \leq (q^{ms} - q^{m(s-r)})d_s.
\]
5. [12] Corollary 1:

\[(q^{mr} - 1)d_1 \leq (q^{mr} - q^{m(r-1)})d_r,\]

6. [7] Proposition II.3:

\[(q^{mr} - 1)d_{r-1} \leq (q^{mr} - q^m)d_r,\]

7. [20] bound (20):

\[d_r \geq n - \left\lfloor \frac{(q^{m(k-r)} - 1)(n - d_s)}{q^{m(k-s)} - 1} \right\rfloor.\]

**Remark 9.** A trivial lower bound that is valid for every linear code is
\[d_{R,r}(C) \geq r,\] for all \(1 \leq r \leq k.\) Observe that a linear code \(C\) satisfies that \(d_{R,r}(C) = r,\) for every \(1 \leq r \leq k\) if, and only if, \(C\) is Galois closed. This gives another characterization of Galois closed spaces to those in Proposition 2, in terms of generalized rank weights. In the Hamming case, \(d_{H,r}(C) = r,\) for every \(1 \leq r \leq k\) if, and only if, \(C = V_I,\) for some \(I \subset \{1, 2, \ldots, n\}.\)

In the rest of the section, we discuss the possible extensions of the Singleton bound to rank weights. We start by giving a brief overview of the bounds in the literature that resemble the usual Singleton bound, both for a linear code \(C \subset \mathbb{F}_q^n\) and a code pair \(C_2 \subset C_1 \subset \mathbb{F}_q^n: \)

\[d_{R,r}(C) \leq \begin{cases} n - k + r & [17], \\ (m - 1)k + r & [17], \\ \frac{m}{n}(n - k) + 1, \text{ if } r = 1 & [19], \end{cases} \]

\[M_{R,s}(C_1, C_2) \leq \begin{cases} n - k_1 + s & [17], \\ (m - 1)(k_1 - k_2) + s & [17], \\ \frac{m(n-k_1)}{n-k_2} + 1, \text{ if } s = 1 & [17], \end{cases} \]

where \(1 \leq r \leq k = \dim(C)\) and \(1 \leq s \leq k_1 - k_2,\) \(k_1 = \dim(C_1)\) and \(k_2 = \dim(C_2).\)

As a tool for future bounds, we establish the following one. It shows how to obtain bounds for all generalized weights from bounds on the first one or the last one.

**Lemma 11.** For every linear code \(C \subset \mathbb{F}_q^n,\) and for every \(1 \leq r \leq k - 1,\) \(k = \dim(C),\) it holds that

\[1 \leq d_{R,r+1}(C) - d_{R,r}(C) \leq m.\]

The same bound applies to relative generalized rank weights.

**Proof.** It is enough to prove that, if \(D \subset D'\) and \(\dim(D') = \dim(D) + 1,\) then \(\text{wt}_R(D') \leq \text{wt}_R(D) + m.\) Take \(d \in D'\) such that \(D' = D \oplus \langle d \rangle.\) Then \(D'^* \subset D^* + \langle d \rangle^*,\) and the result follows, since \(\text{wt}_R(d) \leq m.\) \(\square\)

Note that this bound implies that a reciprocal of Theorem 4 is not possible: Take for instance \(m = 1,\) then we have the bound \(d_{R,r+1} = d_{R,r} + 1,\) which holds for all linear codes. However, the bound \(d_{H,r+1} = d_{H,r} + 1\) does not hold for all linear codes.
The case \( r = 1 \) of the following bound was established and proven by Loidreau in [19] and for relative weights by Kurihara et al. in [17, Proposition 3]. The general case follows from these and the previous lemma.

**Proposition 4** (Alternative Singleton bound). If \( n > m \), then for every linear code \( C \subset \mathbb{F}_{q^m}^n \), and every \( 1 \leq r \leq k = \text{dim}(C) \),

\[
d_{R,r}(C) \leq \frac{m}{n}(n-k) + m(r-1) + 1.
\]

For a code pair \( C_2 \subsetneq C_1 \subset \mathbb{F}_{q^m}^n \), with \( k_i = \text{dim}(C_i) \), \( i = 1,2 \), and every \( 1 \leq r \leq \text{dim}(C_1/C_2) \),

\[
M_{R,r}(C_1,C_2) \leq \frac{m(n-k_1)}{n-k_2} + m(r-1) + 1.
\]

Now, for generalized rank weights, it is easy to see that this bound is sharper than the usual Singleton bound if, and only if,

\[
r \leq \left\lfloor \frac{n(n-1) - (n-m)k}{n(m-1)} \right\rfloor,
\]

which is a number in \((1,k]\) if \( n \leq mk \) (the case where the code is not necessarily rank degenerate). However, as it is usual, we will define \( r \)-MRD codes as those such that \( d_{R,r} = n-k+r \). MRD will mean 1-MRD.

We also obtain the bound \( d_{R,r}(C) \leq rm \) from the previous lemma, by induction on \( r \). Therefore, the overview of the Singleton bound becomes now as follows, with notation as above, which improves the bounds in the previous overview:

\[
d_{R,r}(C) \leq \begin{cases} n - k + r, \\ rm, \\ \frac{m}{n}(n-k) + m(r-1) + 1, \end{cases} \quad M_{R,s}(C_1,C_2) \leq \begin{cases} n - k_1 + s, \\ sm, \\ \frac{m(n-k_1)}{n-k_2} + m(s-1) + 1. \end{cases}
\]

**Remark 10.** The bound \( d_{R,r}(C) \leq rm \) is sharper than the alternative Singleton bound if, and only if, \( n \geq mk \). We know that in this case, \( C \) is rank degenerate. Therefore, for codes that are not rank degenerate, the usual and alternative Singleton bounds are the sharpest ones.

**Remark 11.** When \( n \leq m \) the usual Singleton bound is the sharpest general upper bound on the rank distance, since Gabidulin codes (see [9]) are MRD and may have length \( n \), for all \( n \leq m \), and dimension \( k \), for all \( 1 \leq k \leq n \).

Since the alternative Singleton bound is sharper for \( r = 1 \) when \( n > m \), it follows immediately that, given \( 1 \leq k \leq n \), and \( m \), there exists an MRD code over \( \mathbb{F}_{q^m}^n \), with length \( n \) and dimension \( k \), if and only if, \( n \leq m \). This gives a result analogous to the MDS conjecture (see [13, page 265]) for the rank distance – although in this case it is not a conjecture.

Also note that the inequality (12) gives a lower bound on the number \( r \) such that \( C \) is \( r \)-MRD.
Remark 12. One might ask if a bound of the form $d_{R, r}(C) \leq \frac{m}{n}(n-k)+r$ holds, when $n > m$. However, this is not true even for $r=2$. Take for example $m=2$, $n=4$, $\alpha \in \mathbb{F}_q^2 \setminus \mathbb{F}_q$, and the code $C = \langle (1, \alpha, 0, 0), (0, 0, \alpha, 1) \rangle$, which has dimension $k=2$. It is easy to see that $C^\perp$ has dimension 4, since $(1, \alpha, 0, 0), (1, \alpha^3, 0, 0), (0, 0, \alpha, 1)$ and $(0, 0, \alpha^3, 1)$ are linearly independent over $\mathbb{F}_q$. Thus, for $r = k = 2$,

$$d_{R, 2}(C) = 4, \quad \text{and} \quad \frac{m}{n}(n-k)+r = \frac{2}{4}(4-2)+2 = 3.$$ 

Moreover, we see that $d_{R, 2}(C)$ attains the alternative Singleton bound.

We conclude the section with a simple fact that connects $r$-MRD codes with $r$-MDS codes, and which follows directly from (9).

Proposition 5. A linear code $C \subset \mathbb{F}_{q^m}^n$ is $r$-MRD if, and only if, $\varphi_B(C)$ is $r$-MDS, for all bases $B \subset \mathbb{F}_q^m$ of $\mathbb{F}_{q^m}$.

Thus, if $C$ is a Gabidulin code [9], it is obviously MDS, but also the codes $\varphi_B(C)$ are MDS. It can also be easily shown that the codes $\varphi_B(C)$ are again Gabidulin codes. Therefore, to prove that they are MRD, it is only necessary to prove that they are MDS.

6 Rank-puncturing and rank-shortening

In this section we discuss what are the operations on rank-metric codes analogous to puncturing and shortening [13, Section 1.5]. The main importance of the concept of puncturing is that a punctured codeword is essentially the same as a codeword with erasures, as in the Hamming case. Recall that the shortened and punctured codes of a given code $C \subset \mathbb{F}_q^m$ on the coordinates in the set $I \subset J$ are defined, respectively, as

$$C_I = C \cap V_I = \{ c \in C \mid c_i = 0, \forall i \notin I \}, \quad C^I = \{ (c_i)_{i \in I} \mid c \in C \}.$$ 

On the other hand, for a linear subspace $L \subset \mathbb{F}_q^n$, fix another subspace $L' \subset \mathbb{F}_q^n$ such that $\mathbb{F}_q^r = L' \perp L$. We then define the projection map

$$\pi_{L, L'} : \mathbb{F}_{q^m}^n \longrightarrow V' = L' \oplus \mathbb{F}_q^m,$$

such that $\pi_{L, L'}(c) = c_1$, where $c = c_1 + c_2$, $c_1 \in V'= L' \oplus \mathbb{F}_q^m$ and $c_2 \in V' = L' \perp \mathbb{F}_q^m$. We then write $C^{L, L'} = \pi_{L, L'}(C)$, for a (non-linear) code $C \subset \mathbb{F}_{q^m}$.

Lemma 12. For any two subspaces $L', L'' \subset \mathbb{F}_q^n$ such that $\mathbb{F}_q^n = L' \oplus L' = L'' \oplus L''$, and for any code $C \subset \mathbb{F}_{q^m}$, we have that the codes $C^{L, L'}$ and $C^{L, L''}$ are rank-metric equivalent in a canonical way.

Proof. Define $\phi : V' \longrightarrow V''$ by $\phi(c) = \pi_{L, L''}(c)$, where $V' = L' \oplus \mathbb{F}_q^m$ and $V'' = L'' \oplus \mathbb{F}_q^m$. It is easy to see that $\phi$ is a rank-metric equivalence, since $\phi(L') = L''$, and on the other hand, $\phi(O^{L, L'}) = C^{L, L''}$. \qed
Therefore, the next definition of rank-punctured code is consistent.

**Definition 7.** For every $F_q$-linear space $L \subset F_q^n$, and every code $C \subset F_q^{n_m}$, we define its rank-punctured and rank-shortened codes over $L$ as $C^L = C^{L,L'}$ and $C_L = C \cap V$, respectively, for some $L'$ as before, where $V = L \otimes F_q^{n_m}$.

Similarly, for a coding scheme $P_S = \{C_x\}_{x \in S}$, we can define its rank-punctured and rank-shortened schemes over $L$ as $P_S^L = \{C_x^L\}_{x \in S}$ and $P_{SL} = \{C_{xL}\}_{x \in S}$, respectively. For a linear coding scheme built from $C_2 \subset C_1 \subset F_q^{n_m}$, they are the schemes built from $C_2^L \subset C_1^L$ and $C_{2L} \subset C_{1L}$.

Observe that it is not always true that $C_L \subset C^L$, as opposed to the usual shortening and puncturing. On the other hand, we see that, for every $I \subset J$, $V_I \in \Upsilon$. Then, it is easy to see that $C^I = C^{L_I}$ and $C_I = C_{L_I}$, regarded as subspaces of $V_I$. Thus the previous definition extends the usual definition of punctuating and shortening. For brevity, we will use just the words puncturing and shortening for rank-puncturing and rank-shortening, respectively.

**Remark 13.** Note that, given $L \subset F_q^n$, there may be more than one subspace $L' \subset F_q^n$ such that $F_q^n = L' \oplus L^\perp$ (later we will actually see how to obtain them). If $V = L \otimes F_q^{n_m}$, then $V^\perp = L^\perp \otimes F_q^{n_m}$, and what we are doing is finding a subspace $V' \in \Upsilon$ such that $F_q^{n_m} = V' \oplus V^\perp$.

On the other hand, if $V = V_I \in \Lambda$, then $V_I^\perp = V^\Upsilon$ and $V_I$ is the unique subspace $V' \in \Lambda$ such that $F_q^{n_m} = V' \oplus V^\perp$. Therefore, punctured codes in the Hamming case are defined in a unique way, in contrast with the rank case.

Usually, $C^I$ and $C_I$ are considered as subspaces of $F_q^{n_m}$. This is obvious since $\text{Supp}(C^I) \subset I$ and $V_I$ is Hamming equivalent to $F_q^{n_m}$. For rank metric codes, we can fix bases $B, B'$ of $L, L' \subset F_q^n$, respectively, and consider $\psi_B(C_L)$ and $\psi_B'(C^L)$, where $\psi_B$ and $\psi_B'$ are the rank-metric equivalences defined in Section 4. That is, we can consider that $C_L, C^L \subset F_q^{\dim(L)}$.

Now we turn to properties that can be derived using the puncturing and shortening constructions, in the same way as in the Hamming case. We start with a tool that generalizes Forney’s Lemmas [8, Lemmas 1 and 2] and that is useful to relate dimensions of punctured and shortened codes. Note that [17, Lemma 10] is essentially the second equality in this lemma.

**Lemma 13.** For every linear code $C \subset F_q^{n_m}$ of dimension $k$ and every subspace $L \subset F_q^n$, it holds that
\[
\dim(C^L) = \dim(L) - \dim((C^\perp)_L) = k - \dim(C_L^\perp).
\]

**Proof.** The second equality follows from $C + V^\perp = (C^\perp \cap V)^\perp$, $V = L \otimes F_q^{n_m}$, and the dimension formula: $\dim(C_1 + C_2) + \dim(C_1 \cap C_2) = \dim(C_1) + \dim(C_2)$.

On the other hand, consider the restriction $\pi_{L,L'} : C \rightarrow V'$. We have that $\dim(C^L) = \dim(\pi_{L,L'}(C)) = k - \dim(\ker(\pi_{L,L'})) = k - \dim(C_L^\perp)$. \qed
Using this, we now give a characterization of $r$-MDS codes and $r$-MRD codes in terms of dimensions of punctured codes. We only give the proof in the case of rank weights, since for Hamming weights it is essentially the same proof. We will need the duality theorem for generalized rank weights, which has been established and proven in [7] (we will give a shorter proof in Section 7.1):

**Theorem 8 (Duality).** Given a linear code $C \subset \mathbb{F}_{q^m}^n$ of dimension $k$, write $d_r = d_{R,r}(C)$ for $1 \leq r \leq k$, and $d_s^\perp = d_{R,s}(C^\perp)$, for $1 \leq s \leq n-k$. Then it holds that

$$\{1, 2, \ldots, n\} = \{d_1, d_2, \ldots, d_k\} \cup \{n + 1 - d_1^\perp, n + 1 - d_2^\perp, \ldots, n + 1 - d_{n-k}^\perp\},$$

where the union is disjoint.

Note that, in the next propositions, the equivalence of the two first conditions follows directly from Wei’s duality and its corresponding theorem for rank weights, as proven in [26, Proposition 4.1] and [7, Corollary III.3], respectively. The equivalence between item 2 and item 4 for Hamming weights is proven in [13, Theorem 1.4.15], and the case $r = 1$ ($C$ is MDS) is fully proven in [13, Theorem 2.4.3]. It also generalizes [13, Corollary 1.4.14] and [13, Theorem 1.5.7 (ii)].

**Proposition 6.** The following conditions are equivalent for a linear code $C \subset \mathbb{F}_{q^m}^n$ of dimension $k$, and every $1 \leq r \leq k$:

1. The code $C$ is $r$-MDS.
2. $d_{H,1}(C^\perp) \geq k - r + 2$.
3. For all $I \subset J$ such that $\#I \leq k - r + 1$, we have that $\dim(C^I) = \#I$.
4. For all $I \subset J$ such that $\#I \geq n - k + r - 1$, we have that $\dim((C^\perp)^I) = n - k$.

**Proposition 7.** The following conditions are equivalent for a linear code $C \subset \mathbb{F}_{q^m}^n$ of dimension $k$, and every $1 \leq r \leq k$:

1. The code $C$ is $r$-MRD.
2. $d_{R,1}(C^\perp) \geq k - r + 2$.
3. For all $L \subset \mathbb{F}_q^n$ such that $\dim(L) \leq k - r + 1$, we have that $\dim(C^L) = \dim(L)$.
4. For all $L \subset \mathbb{F}_q^n$ such that $\dim(L) \geq n - k + r - 1$, we have that $\dim((C^\perp)^L) = n - k$.

**Proof.** The equivalence between the first two conditions follows from the duality Theorem and the equivalence between the last two conditions follows from Lemma [13].

Now, we prove that condition 3 implies condition 2. Take $c \in C^\perp \setminus 0$ and assume that $\text{wt}_R(c) = \dim(L) \leq k - r + 1$, where $L = (\langle c \rangle^*)_{\mathbb{F}_q}$. Then by Lemma [13]

$$\dim(L) = \dim(C^L) = \dim(L) - \dim((C^\perp)_L),$$
and thus \((C^\perp)_L = 0\), but this implies that \(c = 0\), which is a contradiction. Thus, \(\text{wtr}_R(c) \geq k - r + 2\).

Finally, we prove that condition 2 implies condition 3. Let \(L \subset F^n_q\) be such that \(\dim(L) \leq k - r + 1\). Then, by the definition of minimum rank distance, we have that \(\dim((C^\perp)_L) = 0\), and thus by Lemma 13,
\[
\dim(C^L) = \dim(L) - \dim((C^\perp)_L) = \dim(L).
\]

After showing how to compute generator matrices for punctured codes, it can be easily proven that the equivalence between items 2 and 3 generalizes [9, Theorem 1].

**Corollary 1.** The smallest integer \(r\) such that \(C\) is \(r\)-MDS is \(r = k - d_{H,1}(C^\perp) + 2\), and similarly for rank weights.

Next, we define the notion of information space, which plays the same role as information sets in the Hamming case: any original codeword can be recovered from the punctured codeword if (and also only if in the linear case) we puncture on an information space. Therefore, information spaces completely describe the erasure correction capability of a code, and not only worst cases.

**Definition 8.** Given a linear code \(C \subset F^n_{q^m}\), we say that a subspace \(L \subset F^n_q\) is an information space for \(C\) if \(\dim((C^\perp)_L) = \dim(C)\). Equivalently, if the restriction \(\pi_{L,L'} : C \rightarrow C^L\) is an \(F_{q^m}\)-linear vector space isomorphism.

For a (non-linear) code \(C \subset F^n_{q^m}\), we say that \(L\) is an information space for \(C\) if \(\pi_{L,L'} : C \rightarrow C^L\) is bijective.

On the other hand, given a code pair \(C_2 \subset C_1 \subset F^n_{q^m}\), we say that \(L\) is an information space for \(C_1, C_2\) if \(\dim(C_1^L/C_2^L) = \dim(C_1/C_2)\). In general, for a coding scheme \(\mathcal{P}_S = \{C_x\}_{x \in S}\), we say that \(L\) is an information space for \(\mathcal{P}_S\) if \(\pi_{L,L'}(C_{x_1}) \cap \pi_{L,L'}(C_{x_2}) = \emptyset\), whenever \(x_1 \neq x_2\).

Observe that a set \(I \subset J\) is an information set for \(C\) if, and only if, \(L_I\) is an information space for \(C\). Note also that \(\pi_{L,L'}\) is always surjective, so it is only necessary to be injective in order to be bijective.

On the other hand, Proposition 7, item 4, shows threshold values on the dimension of a space to guarantee that it is an information space for a given code, in terms of its minimum rank distance, as in the Hamming case.

Now we characterize MRD codes using information spaces, in the same way as MDS codes are characterized using information sets. Note that the result is a particular case of Proposition 7 taking \(r = 1\). After knowing how to compute generator matrices of punctured codes, it can be shown that this proposition is essentially [9, Theorem 2].

**Proposition 8.** A linear code \(C \subset F^n_{q^m}\) is MRD if, and only if, every \(L \subset F^n_q\) with \(\dim(L) = k = \dim(C)\), is an information space for \(C\).
The following two propositions essentially describe erasure correction on networks. The second one also describes the correction capability of punctured codes. They are analogous to [13] Theorem 1.5.7 (ii) and [13] Theorem 1.5.1, respectively. The first one also extends [9] Theorem 1) to non-linear codes.

**Proposition 9.** Given a (non-linear) code \( C \subset \mathbb{F}_q^m \), if \( \rho < d_R(C) \), then every subspace \( L \subset \mathbb{F}_q^n \) with \( \dim(L) \geq n - \rho \) is an information space for \( C \). If \( \rho \geq d_R(C) \), there exists a subspace \( L \subset \mathbb{F}_q^n \) with \( \dim(L) = n - \rho \) which is not an information space for \( C \).

**Proof.** First we prove in the first case that \( \pi_{L,L'} : C \rightarrow C^L \) is injective. Take \( c_1, c_2 \in C \) such that \( \pi_{L,L'}(c_1) = 0 \), where \( c = c_1 - c_2 \). Then, \( c \in V^\perp \), \( V = L \otimes \mathbb{F}_q^m \), and therefore, \( \mathrm{wt}_R(c) \leq \dim(V^\perp) \leq \rho \), which is absurd.

For the second statement, take \( c_1, c_2 \) and \( c = c_1 - c_2 \) such that \( \mathrm{wt}_R(c) = d_R(C) \), write \( D = \langle c \rangle^* = \langle v_1, v_2, \ldots, v_s \rangle \), with \( v_i \in \mathbb{F}_q^n \), and extend this to a basis \( B = \{ v_i \} \) of \( \mathbb{F}_q^n \). Consider \( L^\perp = \langle v_1, v_2, \ldots, v_p \rangle_{\mathbb{F}_q} \), then \( \dim(L) = n - \rho \) and \( \pi_{L,L'}(c_1) = \pi_{L,L'}(c_2) \). \( \square \)

**Proposition 10.** Given a (non-linear) code \( C \subset \mathbb{F}_q^m \) with \( \rho < d_R(C) \), every subspace \( L \subset \mathbb{F}_q^n \) with \( \dim(L) \geq n - \rho \) satisfies that \( d_R(C^L) \geq d_R(C) - \rho \). Moreover, there exists a subspace \( L \subset \mathbb{F}_q^n \) with \( \dim(L) = n - \rho \) such that \( d_R(C^L) = d_R(C) - \rho \).

**Proof.** With the same notation as in the previous proof, we have that \( \mathrm{wt}_R(\pi_{L,L'}(c)) = \dim((\pi_{L,L'}(c))^*) \geq \dim(c^*) - \rho \), and the first statement follows.

Finally, take \( c_1, c_2 \) such that \( \mathrm{wt}_R(c) = d_R(C) \), and write \( D = (c)^* = \langle v_1, v_2, \ldots, v_s \rangle \), with \( v_i \in \mathbb{F}_q^n \), and extend this to a basis \( B = \{ v_i \} \) of \( \mathbb{F}_q^n \). Consider \( L^\perp = \langle v_1, v_2, \ldots, v_p \rangle_{\mathbb{F}_q} \) and \( L' = \langle v_{p+1}, v_{p+2}, \ldots, v_n \rangle_{\mathbb{F}_q} \), then \( \ker(\pi_{L,L'}) \cap D = L^\perp \otimes \mathbb{F}_q^m \), and therefore \( \mathrm{wt}_R(\pi_{L,L'}(c)) = \mathrm{wt}_R(c) - \rho \), and the last statement follows. \( \square \)

We can extend this to (non-linear) coding schemes, just by substituting the code \( C \) with a coding scheme \( P = \{ C_x \}_{x \in S} \). The proof is the same.

We conclude the section showing how to compute punctured codes. In the Hamming case, this is obvious, since we only have to project on some of the coordinates. In the rank case, we need to solve some systems of linear equations, which is still an efficient computation.

**Proposition 11.** Given a subspace \( L \subset \mathbb{F}_q^n \) and one of its generator matrices \( A \) (\( L = \text{row}(A) \) and \( A \) has full rank [13]), we have that a subspace \( L' \subset \mathbb{F}_q^n \) satisfies \( \mathbb{F}_q^n = L' \oplus L^\perp \) if, and only if, it has a generator matrix \( A' \) such that \( A'A^T = I \).

**Proof.** First assume that \( \mathbb{F}_q^n = L' \oplus L^\perp \) and \( B \) is a generator matrix for \( L' \). Take \( x \) such that \( xB A^T = 0 \), then \( xB \in L' \cap L^\perp \) and therefore, \( xB = 0 \), which implies that \( x = 0 \). Hence, \( BA^T \) is full rank and there exists an invertible matrix \( M \) such that \( MBA^T = I \). Taking \( A' = MB \) we obtain the desired matrix.

Now assume that \( L' \) has a generator matrix \( A' \) with \( A'A^T = I \). We need to prove that \( L' \cap L^\perp = 0 \). Suppose that \( xA' \in L^\perp \), then \( x = xA'A^T = 0 \), and we are done. \( \square \)
Therefore, to compute subspaces $L'$ with $F_q^n = L' \oplus L^\perp$, we just need to solve the equations $A_i a_i'^T = e_i^T$, $i = 1, 2, \ldots, \dim(L)$. Different solutions give different spaces.

Note that if $A$ is a generator matrix of $L \subset F_q^n$ over $F_q$, then it is a generator matrix of $V = L \otimes F_q^m$ over $F_q^m$.

**Lemma 14.** With the same notation as in the previous proposition, we have that, for every $c \in F_q^m$,

$$\pi_{L,L'}(c) = c A'^T A'.$$

And now we give a method to compute the generator matrix of a punctured code $C_L$, given generator matrices of $C$ and $L$. The proof is straightforward and follows from the previous lemma.

**Proposition 12.** Let $C \subset F_q^n$ be a linear code with generator matrix $G$, and let $L, L' \subset F_q^n$ be subspaces with generator matrices $A$ and $A'$, respectively, and such that $A'A^T = I$.

We have that $GA^T A'$ satisfies that $\text{row}(GA^T A') = C_{L,L'} = C_L$, and thus by deleting linearly dependent rows, we obtain a generator matrix for $C_L$. Moreover, if $L$ is an information space for $C$, then $GA^T A'$ is full rank and therefore it is a generator matrix for $C_L$.

### 7 Secure network coding

In this section we revisit the description of secure linear network coding in view of the results in the previous sections. As in the rest of the paper, the model that we will treat is that of [17], which generalizes the one in [23], and consists in concatenating a code $C \subset F_q^n$, or a coding scheme, with a linear network code.

This means that the encoded codeword $c \in C$ is sent through a network in which we inject the $n$ columns (packets) of $\mu(c)$ on $n$ outgoing links and, in each node, we generate and send a linear combination (with coefficients in $F_q$) of the received packets. The receiver at the sink node obtains $N$ packets from $N$ incoming links. In other words, the receiver should obtain a matrix of the form $Y = \mu(c) A^T$, for certain matrix $A \in F_q^{N \times n}$.

An adversary may compromise the security of the network by doing three things: introducing $t$ erroneous packets on $t$ different links, modifying the matrix $A$ and obtaining information from $c$ by wiretapping several links.

The two first problems mean that the receiver will obtain a matrix of the form

$$Y = \mu(c) A^T + ZD^T = XA^T + E,$$

where $X = \mu(c)$ and $E = ZD^T$, for some matrices $Z \in F_q^{m \times t}$ and $D \in F_q^{N \times t}$. The matrix $A$ is the actual one used in the network, which may be a modification of the intended one. The columns in $Z$ represent the error packets, and the matrix $D$ represents the propagation of these errors through the network. The deficiency in the rank of $A$ represents the erasures. Therefore, we say that $t$ errors and $n - \text{Rk}(A)$ erasures occurred.
As in the literature \[17, 23\], we say that the network code is coherent if the receiver knows the matrix $A$ (the actual one used in the network). Otherwise, we call the network code incoherent.

Note that $\mu(c)A^T = \mu(cA^T)$, where on both sides we use the same basis of $\mathbb{F}_{qm}$ over $\mathbb{F}_q$. Therefore, we can write the previous equation as

$$y = cA^T + e \in \mathbb{F}_{qm}^N,$$

where $e = zD^T$, $z \in \mathbb{F}_q^m$.

In this section we will see how the rank-puncturing and rank-shortening defined previously can describe information leakage and error and erasure correction.

### 7.1 Erasure correction and information leakage revisited

In this subsection we study the problems of erasure correction and information leakage, which are closely related. The amount of leaked information on networks was studied in \[17\]. We will see how the punctured construction can describe this.

Consider a linear coding scheme built from $C_2 \subset C_1 \subset \mathbb{F}_q^n$. Denote by $S$ and $X$ the random variables corresponding to the secret and the shares, respectively, and $\pi_I$ the projection onto the coordinates in $I \subset J$. It was shown in \[18\] that

$$I(S; \pi_I(X)) = \dim((C_2^I)_I/(C_1^I)_I) = \dim(C_1^I/C_2^I),$$

for every $I \subset J$, assuming a uniform distribution, where the last equality follows from Lemma \[13\] and $I(X:Y) = H(X) - H(X|Y)$ is the mutual information of the random variables $X$ and $Y$.

On the other hand, by wiretapping $s$ links in a network, an adversary obtains the variable $XB^T$, for some matrix $B \in \mathbb{F}_q^{s \times n}$. Assuming uniform distributions, and defining $L = \text{row}(B) \subset \mathbb{F}_q^n$, it is proven in \[17\] Lemma \[7\] that

$$I(S; XB^T) = \dim((C_2^L)_L/(C_1^L)_L) = \dim(C_1^L/C_2^L),$$

where the last equality follows from Lemma \[13\].

Therefore, the information leakage is tightly related to the dimension of punctured and shortened codes. However, the space $C_1^L/C_2^L$ plays a deeper role, as we next see. This is analogous to the role that $C_1^I/C_2^I$ plays in the usual case.

If the adversary knows the matrix $B$, then he or she may obtain $\pi_{L,L'}(c) = c\tilde{B}^T\tilde{B}'$, where $\tilde{B}$ is a submatrix of $B$ that is a generator matrix of $L$, and $\tilde{B}'\tilde{B}^T = I$. Assuming uniform distributions, it can be shown that the adversary still obtains the same amount of information from $\pi_{L,L'}(c)$:

$$I(S; XB^T) = I(S; \pi_{L,L'}(X)) = \dim(C_1^L/C_2^L).$$

(15)

Actually, we can effectively compute the set of possible sent secret messages, regardless of the distributions used. If $\psi : \mathbb{F}_q^m \longrightarrow W$ is the map defined at the beginning of Section \[2\] we can see both $\psi$ and $\pi_{L,L'}$ as maps

$$\mathbb{F}_q^m \xrightarrow{\psi} C_1/C_2 \xrightarrow{\pi_{L,L'}} C_1^L/C_2^L,$$

25
where $\psi$ is an isomorphism and $\pi_{L,L'}$ is surjective. Therefore, knowing $c' = \pi_{L,L'}(c + C_2) = \pi_{L,L'}(\psi(x))$, where $c = \psi(x)$, we can obtain the set of possible sent messages, which is

$$(\pi_{L,L'} \circ \psi)^{-1}(c') = x + \ker(\pi_{L,L'} \circ \psi),$$

regardless of the distribution, and in the case of uniform distributions, $\dim(\ker(\pi_{L,L'} \circ \psi)) = \ell - \dim(C^L_1/C^L_2) = H(S) - I(S; \pi_{L,L'}(X)) = H(S|\pi_{L,L'}(X))$.

Moreover, if we know $B$, we can obtain all vectors in $x + \ker(\pi_{L,L'} \circ \psi)$ by performing matrix multiplications and solving systems of linear equations.

Assume that $G_1, G_2, G'$ are generator matrices of $C_1, C_2, W$, respectively, where $C_1 = C_2 \oplus W$, and the first rows of $G_1$ are the rows in $G_2$, and the last rows are the rows in $G'$. Then, for a secret $x \in \mathbb{F}_q^n$, the encoding consists in generating uniformly at random a vector $x_2 \in \mathbb{F}_q^{k_2}$ and defining $c = x_2 G_2 + x G' = (x_2, x) G_1$. Therefore, the projections onto the last $\ell$ coordinates of the solutions of the system $\pi_{L,L'}(c) = \tilde{\pi}(G_1 B^T \tilde{B}')$ will be all the vectors in $x + \ker(\pi_{L,L'} \circ \psi)$.

If $L$ is an information space for $C_2 \subsetneq C_1$, i.e., $\dim(C^L_1/C^L_2) = \ell$, then all solutions of the previous system coincide in the last $\ell$ coordinates, which constitute the secret vector $x \in \mathbb{F}_q^n$.

In particular, using one code $C_1 = C$, $C_2 = 0$, we see that if $L$ is an information space for $C$, then the system $x(G B^T \tilde{B}') = \pi_{L,L'}(c)$ has a unique solution.

Remember from Proposition 26 that if $n - \operatorname{Rk}(B) < d_R(P_S)$, then $L = \operatorname{row}(B)$ is an information space for $P_S$.

Next we give a relation between information leakage and duality, whose philosophy is similar to that of MacWilliams equations, since it means that knowing the information leakage using the code pair $C_2 \subsetneq C_1$ is equivalent to knowing the information leakage using the “dual” code pair $C_1 \perp \subsetneq C_2 \perp$. It is convenient to introduce the definition of access structures:

**Definition 9.** We define the Hamming access structure of the code pair $C_2 \subsetneq C_1$ as the collection of the following sets

$$A(C_1, C_2)_r = \{ I \subset J \mid \dim(C^I_1/C^I_2) = r \},$$

for $0 \leq r \leq \ell = \dim(C_1/C_2)$. Given a set $\mathcal{A} \subset \mathcal{P}(J)$, we define its Hamming dual as $\mathcal{A}^\perp = \{ I \subset J \mid T \in \mathcal{A} \}$.

In the same way, we define the rank access structure of the code pair $C_2 \subsetneq C_1$ as the collection of the following linear subspaces of $\mathbb{F}_q^n$

$$B(C_1, C_2)_r = \{ L \subset \mathbb{F}_q^n \mid \dim(C^L_1/C^L_2) = r \},$$

for $0 \leq r \leq \ell = \dim(C_1/C_2)$. Given a set $\mathcal{B} \subset \{ L \subset \mathbb{F}_q^n \text{ linear subspace} \}$, we define its rank dual as $\mathcal{B}^\perp = \{ L \subset \mathbb{F}_q^n \mid L^\perp \in \mathcal{B} \}$. 
We now present the relation with duality, where the case \( r = 0 \) was already proven in [5, Proof of Theorem 1] for the Massey-type scheme [5, Section 3].

**Proposition 13.** Given a code pair \( C_2 \subsetneq C_1 \subset \mathbb{F}_q^m \) and \( 0 \leq r \leq \ell = \dim(C_1/C_2) \), we have that
\[
A(C_2^\perp, C_1^\perp)_r = A(C_1, C_2)_{\ell-r}.
\]

**Proof.** It follows from the following equality, which follows from Lemma 13,
\[
\dim((C_2^\perp)^I / (C_1^\perp)^I) + \dim(C_1^L / C_2^L) = \ell.
\]

**Proposition 14.** Given a code pair \( C_2 \subsetneq C_1 \subset \mathbb{F}_q^m \) and \( 0 \leq r \leq \ell = \dim(C_1/C_2) \), we have that
\[
B(C_2^\perp, C_1^\perp)_r = B(C_1, C_2)_{\ell-r}.
\]

**Proof.** Again, it follows from the following equality, which follows from Lemma 13,
\[
\dim((C_2^\perp)^L / (C_1^\perp)^L) + \dim(C_1^L / C_2^L) = \ell.
\]

We will now give a different proof of the duality Theorem 8 that follows from these propositions. Note that a theorem analogous to Wei's duality theorem has not been given for relative generalized Hamming weights, nor for the rank case. However, these last two propositions work for any code pair.

We will need [17, Lemma 4], which gives another definition of generalized rank weights:

**Lemma 15.** For any linear code \( C \subset \mathbb{F}_q^m \) and any \( 1 \leq r \leq k \), we have that
\[
d_{R,r}(C) = \min\{j \mid \max\{\dim(C_L) \mid \dim(L) = j\} = r\}.
\]

**Proof of Theorem 8.** By monotonicity and cardinality, it is enough to prove that both sets on the right-hand side are disjoint. Assume that they are not disjoint, then there exist \( i, j, s \) such that \( d_i = j \) and \( d_s = n+1-j \). By the previous lemma, the first equality implies that
\[
\max\{\dim(C_L) \mid \dim(L) = j\} = i.
\]

Now take \( C_1 = C \) and \( C_2 = 0 \) in the previous proposition. From the fact that \( B(\mathbb{F}_q^m, C^\perp)_r = B(C, 0)_{\ell-r} \) and the previous lemma, the second equality implies that
\[
\max\{\dim(C_L) \mid \dim(L) = j-1\} = s + k - n - 1 + j.
\]

Again by the previous lemma, \( i > s + k - n - 1 + j \). Now interchanging the role of \( C \) and \( C^\perp \), which also interchanges the roles of \( i, s \); the roles of \( j, n+1-j \); and the roles of \( k, n-k \); we have that \( i \leq s + k - n - 1 + j \), which is absurd. \( \square \)
Finally, as consequences of Proposition 6 and Proposition 7, we obtain the description of the access structures for MDS and MRD code pairs, respectively:

**Corollary 2.** If both $C_1$ and $C_2$ are MDS, then

$$\dim(C^I_1/C^I_2) = \begin{cases} 
\ell, & \text{if } k_1 \leq \# I, \\
\# I - k_2, & \text{if } k_2 \leq \# I \leq k_1, \\
0, & \text{if } \# I \leq k_2,
\end{cases}$$

for every $I \subset J$.

**Corollary 3.** If both $C_1$ and $C_2$ are MRD, then

$$\dim(C^L_1/C^L_2) = \begin{cases} 
\ell, & \text{if } k_1 \leq \dim(L), \\
\dim(L) - k_2, & \text{if } k_2 \leq \dim(L) \leq k_1, \\
0, & \text{if } \dim(L) \leq k_2,
\end{cases}$$

for every linear subspace $L \subset \mathbb{F}_q^n$.

In general, we can compute the information leaked in many cases, but if the involved codes are not MDS (respectively, MRD), then there is always a collection of sets (respectively, subspaces) for which we do not completely know the information leaked. We first establish this fact for the rank case, which follows from Proposition 7, and give an example in the Hamming case:

**Proposition 15.** Let $C_2 \not\subseteq C_1 \subset \mathbb{F}_q^n$ be a code pair such that $k_i = \dim(C_i)$, $i = 1, 2$, $\ell = k_1 - k_2$, $C_1$ is $r_1$-MRD and $C_2$ is $r_2$-MRD, or equivalently, $d_R(C_1) \geq k_1 - r_1 + 2$ and $d_R(C_2) \geq n - k_2 - r_2 + 2$. If $L \subset \mathbb{F}_q^n$ is a subspace such that $k_2 + r_2 - 1 \leq \dim(L) \leq k_1 - r_1 + 1$, then $\dim(C^L_1/C^L_2) = \dim(L) - k_2$, which only depends on $\dim(L)$ and not on the space $L$.

**Example 1.** If $C_1$ and $C_2$ are algebraic geometric codes constructed from a function field of genus $g$ [20], then we have the Goppa bound [20, Theorem 4.3]: $d_{H,1}(C_i) \geq n - \dim(C_i) + 1 - g$ and $d_{H,1}(C_i^\perp) \geq \dim(C_i) + 1 - g$. It follows from Proposition 6 that, for the code pair $C_2 \not\subseteq C_1$,

$$\dim(C^I_1/C^I_2) = \begin{cases} 
\ell, & \text{if } k_1 + g \leq \# I, \\
\ell - g, & \text{if } k_1 - g < \# I < k_1 + g, \\
\# I - k_2, & \text{if } k_2 + g \leq \# I \leq k_1 - g, \\
g, & \text{if } k_2 - g < \# I < k_2 + g, \\
0, & \text{if } \# I \leq k_2 - g.
\end{cases}$$
7.2 Error and erasure correction revisited

In this subsection we see how the rank-puncturing can describe error and erasure correction in networks. We will follow a slightly different approach than that of [17, 23].

We will treat the coherent case, that is, the case in which the matrix $A$ is known. For simplicity, we will consider the case of one code $C \subset F_{q^m}^n$, which may be non-linear. At the end we will show how to adapt the results to (non-linear) coding schemes. Observe that [17, Theorem 4] only deals with linear (meaning $F_{q^m}$-linear, as in the rest of the paper) coding schemes.

As we saw in the previous subsection, if the sink node receives $y = cA^T$ and the number of erasures is less than $d_R(C)$, we can perform erasure correction. For that, we can take a submatrix $\tilde{A}$ of $A$ which is a generator matrix of $L = \text{row}(A)$, since the other rows in $A$ are redundant. All choices of $\tilde{A}$ will give the same unique solution.

When there are errors, we would also like to take a submatrix as before and the corresponding subvector of $y$. However, it is not clear that the decoder in [17, 23] for $A$ and for $\tilde{A}$ will behave in the same way. We now propose a slightly different approach.

Fix the positive integer $N$ and the matrix $A \in F_{q^m}^{N \times n}$, which is assumed to be known.

For each $c \in F_{q^m}^n$ and $y \in F_{q^m}^N$, define

$$\Delta_A(c, y) = \min \{ r \mid \exists z \in F_{q^m}^r, D \in F_{q^m}^{N \times r} \text{ with } y = cA^T + zD^T \} = \text{wt}_R(y - cA^T),$$

where the last equality is [23, Lemma 4].

Fix nonnegative integers $\rho, t$, with $Rk(A) \geq n - \rho$. We will assume that, if $c \in F_{q^m}^n$ is sent and $y \in F_{q^m}^N$ is received, then $\Delta_A(c, y) \leq t$, or equivalently, that $y = cA^T + e$, with $\text{wt}_R(e) \leq t$.

Define $L = \text{row}(A)$. We will denote $\tilde{A} \subset A$ if $\tilde{A}$ is a submatrix of $A$ that is a generator matrix of $L$. For each $\tilde{A} \subset A$, we will consider the decoder:

$$\hat{c} = \arg\min_{c \in C} \Delta_{\tilde{A}}(c, \tilde{y}),$$

where $\tilde{y}$ is the vector obtained from $y$ taking the coordinates in the same positions as the rows of $\tilde{A}$. We will say that it is infallible [23, Section III.A] if $\hat{c} = c$, when $c$ is the sent message, for every $c \in C$.

In [17, 23], sufficient and necessary conditions for the decoder corresponding to $A$ being infallible are given. We will now state that the same conditions are valid for the decoders corresponding to all the submatrices $\tilde{A}$. In particular, all of them give the correct (and thus, the same) answer.

The main difference is that now the proof only relies on Proposition [23] and Proposition [10] where we do not need the machinery developed in [17, 23], in total analogy with the Hamming case, as proven in [13, Theorem 1.5.1], and for the decoding, we do not need all rows in $A$. Moreover, although it is not difficult to adapt the proof in [17, Theorem 4] for $F_{q^m}$-linear coding schemes, our proof works for any (non-linear) scheme.

Theorem 9. Given a (non-linear) code $C \subset F_{q^m}^n$, if $d_R(C) > 2t + \rho$, then the previous decoders are infallible for every $\tilde{A} \subset A$, and in particular, they all give the same answer.
If \( d_R(C) \leq 2t + \rho \), then there exists a matrix \( A \in \mathbb{F}_q^{N \times n} \) such that for every \( \tilde{A} \subset A \), the previous decoder is not infallible.

**Proof.** First, assume \( d_R(C) > 2t + \rho \) and fix a matrix \( A \in \mathbb{F}_q^{N \times n} \) and \( \tilde{A} \subset A \). Assume also that the sent message is \( c \in C \) and we receive \( y = cA^T + e \), with \( wt_R(e) \leq t \). Define \( \tilde{y} \) and \( \tilde{e} \) as the vectors obtained from \( y \) and \( e \), respectively, taking the coordinates in the same positions as the rows in \( \tilde{A} \). Therefore, \( \tilde{y} = c\tilde{A}^T + \tilde{e} \).

We have that \( Rk(\tilde{A}) = Rk(A) \) and \( wt_R(\tilde{e}) \leq wt_R(e) \leq t \), and on the other hand,

\[
\Delta_{\tilde{A}}(c, \tilde{y}) = wt_R(\tilde{e}) = wt_R(\tilde{e}A'),
\]

where \( A'\tilde{A}^T = I \).

Now, \( c\tilde{A}^T A' = \pi_{L,L'}(c) \) by Lemma 14. Since \( d_R(C^L) > 2t \) by Proposition 10 and since \( L \) is an information space for \( C \) by Proposition 9, \( c \) is the only vector in \( C \) with \( d_R(\tilde{y}A', \pi_{L,L'}(c)) \leq t \), and we are done.

Finally, if \( d_R(C) \leq 2t + \rho \), then take \( A \) such that \( \dim(L) = n - \rho \) and \( d_R(C^L) = d_R(C) - \rho \leq 2t \), which exists by Proposition 10. Then, take \( \tilde{A} \subset A \) and \( c, c' \in C \) such that \( d_R(\pi_{L,L'}(c), \pi_{L,L'}(c')) = d_R(c\tilde{A}^T, c'\tilde{A}^T) \leq 2t \). There exists \( e, e' \in \mathbb{F}_q^m \) such that \( wt_R(e), wt_R(e') \leq t \) and \( c\tilde{A}^T + \tilde{e} = c'\tilde{A}^T + \tilde{e}' \), and hence the decoder associated with \( \tilde{A} \) gives both \( c \) and \( c' \) as solutions.

To adapt this to (non-linear) coding schemes, we just need to replace distances between vectors by distances between cosets

\[
d_R(C_x, C_{x'}) = \min \{ d_R(c, c') \mid c \in C_x, c' \in C_{x'} \},
\]

and the choice of vectors in \( C \) by the choice of representatives of a coset \( C_x \) in \( \mathcal{P}_S \).

To conclude, we show that erasure correction is equivalent to error correction if the rank support of the error vector is known. This is analogous to the fact that usual erasure correction is equivalent to usual error correction where the positions of the errors (the Hamming support of the error vector) are known. This is a basic fact used in many decoding algorithms for the Hamming distance, which now we hope can be translated to the rank case.

**Proposition 16.** Assume that \( c \in C \) and \( y = c + e \), where \( wt_R(e) = t < d_R(C) \) and \( L = G(e) \). Then, \( c \) is the only vector \( c' \in C \) such that \( wt_R(y - c') < d_R(C) \) and \( L = G(y - c') \).

Moreover, if \( A \) is a generator matrix of \( L^\perp \), then \( c \) is the unique solution in \( C \) of the system of equations \( yA^T = xA^T \), where \( x \) is the unknown vector.

**Proof.** Assume that \( y = c + e = c' + e' \), where \( c' \in C \) and \( G(e) = G(e') \). Then \( yA^T = cA^T = c'A^T \). Since \( Rk(A) = n - t \) and \( t < d_R(C) \), it follows from the previous theorem that \( c = c' \).

30
Acknowledgement

The author wish to thank Ryutaroh Matsumoto, Relinde Jurrius and Ruud Pellikaan for important comments on their work, during the stay of the last author at Aalborg University, and Olav Geil and Diego Ruano for fruitful discussions and careful reading of the manuscript, including the fact that the duality theorem follows from Proposition 14. The author also gratefully acknowledges the support from The Danish Council for Independent Research (Grant No. DFF-4002-00367).

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] A. Barra and H. Gluesing-Luerssen. MacWilliams extension theorems and the local-global property for codes over Frobenius rings. *J. Pure Appl. Algebra*, 219(4):703–728, 2015.

[3] T. P. Berger. Isometries for rank distance and permutation group of Gabidulin codes. *IEEE Trans. Inf. Theory*, 49(11):3016–3019, 2003.

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

[5] 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.

[6] P. Delsarte. On subfield subcodes of modified reed-solomon codes (corresp.). *IEEE Trans. Inf. Theory*, 21(5):575–576, 1975.

[7] J. Ducoat. Generalized rank weights : duality and griesmer bound. *CoRR*, abs/1306.3899, 2013.

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

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

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

[11] M. Giorgetti and A. Previtali. Galois invariance, trace codes and subfield subcodes. *Finite Fields Appl.*, 16(2):96–99, 2010.
[12] T. Helleseth, T. Klove, V. I. Levenshtein, and Ø. Ytrehus. Bounds on the minimum support weights. IEEE Trans. Inf. Theory, 41(2):432–440, 1995.

[13] W. C. Huffman and V. Pless. Fundamentals of error-correcting codes. Cambridge University Press, Cambridge, 2003.

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

[15] R. Kötter and F. R. Kschischang. Coding for errors and erasures in random network coding. IEEE Trans. Inf. Theory, 54(8):3579–3591, 2008.

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

[17] 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.

[18] J. Kurihara, T. Uyematsu, and R. Matsumoto. Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized hamming weight. IEICE Transactions, E95-A(11):2067–2075, 2012.

[19] Pierre Loidreau. Properties of codes in rank metric. CoRR, arxiv.org/abs/cs/0610057, 2006.

[20] 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.

[21] F. E. Oggier and A. Sboui. 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.

[22] A. Shamir. How to share a secret. Commun. ACM, 22(11):612–613, November 1979.

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

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

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

[26] M. A. Tsfasman and S. G. Vlăduţ. Geometric approach to higher weights. IEEE Trans. Inf. Theory, 41(6, part 1):1564–1588, 1995. Special issue on algebraic geometry codes.
[27] V. K. Wei. Generalized Hamming weights for linear codes. *IEEE Trans. Inf. Theory*, 37(5):1412–1418, 1991.

[28] S. Yang, R. W. Yeung, and Z. Zhang. Characterization of error correction and detection in a general transmission system. In *Information Theory, 2008. ISIT 2008. IEEE International Symposium on*, pages 812–816, Toronto, Canada, July 6-11 2008.

[29] S. Yang, R. W. Yeung, and Z. Zhang. Weight properties of network codes. *Telecommunications, European Transactions on*, 19(4):371 – 383, 2008. invited paper.

[30] Z. Zhuang, Y. Luo, and B. Dai. Code constructions and existence bounds for relative generalized Hamming weight. *Des. Codes Cryptogr.*, 69(3):275–297, 2013.

[31] Z. Zhuang, Y. Luo, AJ H. Vinck, and B. Dai. Some new bounds on relative generalized hamming weight. In *Communication Technology (ICCT), 2011 IEEE 13th International Conference on*, pages 971–974. IEEE, 2011.