<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>On the existence of generalized rank weights</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author(s)</strong></td>
<td>Oggier, Frederique; Sboui, Adnen</td>
</tr>
<tr>
<td><strong>Date</strong></td>
<td>2012</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td><a href="http://hdl.handle.net/10220/9133">http://hdl.handle.net/10220/9133</a></td>
</tr>
<tr>
<td><strong>Rights</strong></td>
<td>© 2012 IEICE.</td>
</tr>
</tbody>
</table>
On the Existence of Generalized Rank Weights

Frédérique Oggier and Adnen Shboui
Division of Mathematical Sciences
School of Physical and Mathematical Sciences
Nanyang Technological University, Singapore
Email:{frederique,ASboui}@ntu.edu.sg

Abstract—We consider rank metric codes. We introduce a definition of generalized rank weights, that represents a counterpart of generalized “Hamming weights” with respect to the rank metric. We motivate our definition by the security drop behavior of rank metric wiretap network codes, by analogy to the way generalized Hamming weights characterize linear wiretap codes. We give some examples and properties to support our definition.

I. INTRODUCTION

Linear rank-metric codes [1], [2] are linear \((n, k)\) codes over some finite field \(\mathbb{F}_q^m\), that is linear codes of dimension \(k\) and length \(n\), where every codeword is expanded into an \(m \times n\) matrix with coefficients in \(\mathbb{F}_q\) (by fixing an \(\mathbb{F}_q\)-basis of \(\mathbb{F}_q^m\)). The metric used is then the rank of every matrix codeword, instead of the Hamming distance, which explains the term “rank metric codes”. Optimal codes with respect to the rank metric are called maximum rank distance (MRD) codes. Rank metric codes have been well studied, in terms of bounds (see e.g. [3] for a Gilbert bound) and decoding (e.g. [4]). A regain of interest in rank metric codes has been witnessed recently, thanks to their applications to network coding (e.g. for error control [5] and [6] for security).

Generalized Hamming weights, as the name suggests, are weights defined on subcodes of a linear code, which generalize the notion of Hamming distance. It was shown by Wei [7] that the generalized Hamming weights characterize the performance of linear codes over wiretap channels, a channel where a legitimate transmitter and receiver communicate confidential messages in the presence of an eavesdropper. To determine the generalized Hamming weights of classical codes is difficult in general (see e.g [8] for some results).

The contribution of this paper is to address the existence of generalized weights for rank metric codes, referred to as “generalized rank weights”. This is motivated by the fact that rank metric codes have been used as wiretap codes in the context of network coding, and it would make sense that their performance in terms of security is described by some “generalized rank weights”, by analogy to the case studied by Wei for linear codes. After recalling standard preliminaries about rank metric codes, we study rank metric wiretap codes in Section III, and characterize the drop in security for MRD codes. In Section IV, we give a definition of generalized rank weights. We analyze the second rank distance for MRD codes. General (possibly non-MRD) codes are treated in Section V, where we show that in fact the rank distance of the dual code indeed characterizes the number of taps needed by the eavesdropper to get a first leaking in security. The question of defining generalized rank weights open many questions, some of which are summarized in conclusion.

II. PRELIMINARIES

Let \(q\) be a prime power, and let \(\mathbb{F}_q^m\) denote the finite field with \(q^m\) elements. Consider a vector \(a = (a_1, a_2, \ldots, a_n)\) in \(\mathbb{F}_q^m\), \(m \geq n\), and let \(\nu_1, \ldots, \nu_m\) be an \(\mathbb{F}_q\)-basis of \(\mathbb{F}_q^m\). We can write

\[
a_j = \sum_{i=1}^{m} a_{ij} \nu_i, \ j = 1, \ldots, n.
\]

By writing each \(a_j\) as an \(m\)-dimensional column vector \((a_{1j}, \ldots, a_{mj})^T\) with respect to the chosen basis, the vector \(a\) can be accordingly expanded into the matrix

\[
A = \begin{bmatrix}
a_{11} & a_{12} & \cdots & a_{1n} \\
a_{21} & a_{22} & \cdots & a_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
a_{m1} & a_{m2} & \cdots & a_{mn}
\end{bmatrix}.
\]

We will denote by \(\lambda : \mathbb{F}_q^m \to \mathbb{F}_q^{m \times n}\) the map that sends \(a\) to \(\lambda(a) = A\). The rank over \(\mathbb{F}_q\) of the vector \(a\) [1] is defined as

\[
\text{rk}(a|\mathbb{F}_q) = \text{rank}(\lambda(a)).
\]

For \(a, b\) two \(n\)-dimensional vectors over \(\mathbb{F}_q^{m}\), we have

\[
d_R(a, b) = \text{rk}(a - b|\mathbb{F}_q) = \text{rank}(\lambda(a) - \lambda(b)),
\]

which is shown to be a metric over \(\mathbb{F}_q^m\) called the rank metric or rank distance. For a family of \(n\)-dimensional vectors over \(\mathbb{F}_q^m\), its minimum rank distance \(d_R\) is the minimum rank distance over all possible pairs of distinct vectors.

To an \((n, k)\) linear code \(C\) over \(\mathbb{F}_q^m\) with Hamming distance \(d_H(C)\) corresponds a rank metric code \(\lambda(C)\) with rank distance \(d_R(\lambda(C))\). The connection between both distances was already established in [1], namely

\[
d_R(\lambda(C)) \leq d_H(C) \leq n - k + 1
\]

by the Singleton bound. An \((n,k)\) code \(C\) such that \(d_R(\lambda(C)) = n - k + 1\) is called a maximum rank distance (MRD) code.

Let \(H\) be an \((n - k) \times n\) parity check matrix of the \((n, k)\) code \(C\), that is \(C = \{y \in \mathbb{F}_q^m, Hy^T = 0\}\) is the kernel of \(H\). The dual code \(C^\perp\) has generator matrix \(H\), that is \(C^\perp\) is an \((n, n - k)\) code given by \(C^\perp = \{xH, \ x \in \mathbb{F}_q^{m-k}\}\).
Proposition 1: [1] If $C$ is an $(n, k)$ MRD code, then its dual is an $(n, n - k)$ MRD code, satisfying
$$d_R(\lambda(C^\perp)) = k + 1.$$ 

The MRD Gabidulin codes are described as follows [1]. Let $h_1, \ldots, h_n \in \mathbb{F}_q$ be linearly independent over $\mathbb{F}_q$ and choose a positive integer $d \leq n$. Then
$$H = \begin{bmatrix} h_1 & \cdots & h_n \\ h_1^d & \cdots & h_n^d \\ \vdots \\ h_1^{d-2} & \cdots & h_n^{d-2} \end{bmatrix}$$

is the parity check matrix of an MRD code $C$ of length $n$ and rank distance $d_R(\lambda(C)) = d$. The corresponding generator matrix is of the form
$$G = \begin{bmatrix} g_1 & \cdots & g_n \\ g_1^d & \cdots & g_n^d \\ \vdots \\ g_1^{d-1} & \cdots & g_n^{d-1} \end{bmatrix}$$

where $k = n - d + 1$ and $g_1, \ldots, g_n \in \mathbb{F}_q$ are linearly independent over $\mathbb{F}_q$.

Notation: we may drop the indices $H$ of $d_H$ and $R$ of $d_R$ whenever the context is clear, that is, $d(C)$ refers to the Hamming distance of $C$, while $d(\lambda(C))$ is its rank distance.

III. MRD Wiretap Network Codes

Let $H$ be a $k \times n$ matrix over $\mathbb{F}_q$. Let $s = (s_1, \ldots, s_k)$ be a secret message to be sent over a wiretap channel, i.e., a channel between Alice and Bob, two legitimate parties, in the presence of an eavesdropper Eve. A typical wiretap encoding [9] consists of choosing uniformly at random both a secret $s$ and a vector $x = (x_1, \ldots, x_n)$ such that
$$s^T = Hx^T,$$

which is the actual transmitted vector. In other words, the secret $s$ labels a coset, and random bits are used to pick a codeword within that coset. If the wiretap channel is a network implementing linear network coding over $\mathbb{F}_q$, then the eavesdropper can listen to $\mu$ network edges of her choice, and each of them carries an $\mathbb{F}_q$-linear combination $\sum_{i=1}^n b_{ji}x_i$, $b_{ji} \in \mathbb{F}_q$, $j = 1, \ldots, \mu$ of the transmitted symbols $x_1, \ldots, x_n$. The matrix $B = (b_{ji}) \in \mathbb{F}_q^{\mu \times n}$ summarizes what Eve learns, namely she can form the system of equations $w^T = Bx^T$. The matrix $B$ is assumed to be full rank, since a stronger assumption is always made on the eavesdropper, and the case which brings the most information is to assume linear independency among the chosen edges. The following result is known [10]. The notations $S, W$ and $X$ refer to random variables with realization $s, w$ and $x$ respectively.

Theorem 1: Assume that the transmitter Alice uses the above coset encoding scheme, and the eavesdropper observes $W^T = Bx^T$, with $B \in \mathbb{F}_q^{\mu \times n}$. If the entropy $H(S)$ of the secret $S$ satisfies $H(S) = k = n - \mu$, then
$$I(S; W) = 0 \iff \langle H \rangle \cap \langle B \rangle = 0,$$

where $\langle H \rangle, \langle B \rangle$ denote the row space of $H$ and $B$. Set
$$M = \begin{bmatrix} H \\ B \end{bmatrix}.$$ 

The condition $\langle H \rangle \cap \langle B \rangle = 0$ is equivalent to $\dim(\langle H \rangle \cap \langle B \rangle) = 0$ or to
$$\text{rank} \begin{bmatrix} H \\ B \end{bmatrix} = \text{rank}(H) + \text{rank}(B).$$

In [10], both the network code and the wiretap code are codes over $\mathbb{F}_q$, that is both $B$ and $H$ have coefficients in $\mathbb{F}_q$ ($m = 1$). As a result, it is not possible to find a $H$ such that $\text{rank}(M) = \text{rank}(H) + \text{rank}(B)$ for every $B$. In [6], the authors propose to use for $H$ the parity check matrix of a rank metric code over $\mathbb{F}_q$. The underlying idea is that the network code matrix $B$ still has coefficients in $\mathbb{F}_q$, however $H$ now has coefficients in $\mathbb{F}_{q^m}$, and it is thus possible to find $H$ such that $\text{rank}(M) = \text{rank}(H) + \text{rank}(B)$ for every $B$. More precisely [6]:

Theorem 2: Let $C$ be an $(n, n - k)$ linear code over $\mathbb{F}_{q^m}$ with parity check matrix $H \in \mathbb{F}_{q^m}^{k \times n}$. If $d(\lambda(C)) = k + 1$ and $\mu \leq n - k$ then
$$\text{rank}(M) = \text{rank}(H) + \text{rank}(B),$$

for all $B \in \mathbb{F}_q^{\mu \times n}$. Conversely, if $\mu = n - k$ then the above holds only if $d(\lambda(C)) = k + 1$.

Suppose now that Alice uses an $(n, n - k)$ code $C$ such that $d(\lambda(C)) = k + 1$. If $\mu = n - k + 1$, then $M$ becomes an $(k + n - k + 1) \times n$ matrix, whose rank can be at most $n$. Since $\text{rank}(M) = n$ when $\mu = n - k$, and
$$\text{rank}(M) = \text{rank}(H) + \text{rank}(B) - \dim(\langle H \rangle \cap \langle B \rangle),$$

we have that $\dim(\langle H \rangle \cap \langle B \rangle) = 1$, and security is compromised. Indeed, the adversary Eve knows the network code, thus knows $B, H$ and that $Bx^T = w^T$. Let $B_1$ and $H_1$ denote the rows of $B$ and $H$ respectively. Since $\dim(\langle H \rangle \cap \langle B \rangle) = 1$, there exist $\lambda_1, \ldots, \lambda_{n+1}$ not all zero such that
$$\sum_{i=1}^k \lambda_i H_i + \sum_{j=1}^{n-k+1} \lambda_{k+j} B_j = 0,$$

and
$$\sum_{i=1}^k \lambda_i H_i x^T + \sum_{j=1}^{n-k+1} \lambda_{k+j} B_j x^T = 0,$$

or, in terms of the secret vector $s = (s_1, \ldots, s_k)$ and the observed data $w = (w_1, \ldots, w_{n-k+1})$
$$\sum_{i=1}^k \lambda_i s_i + \sum_{j=1}^{n-k+1} \lambda_{k+j} w_j = 0.$$
so that
\[ s_i = H_i x^T = \sum_j \lambda_{i,j} B_j x^T = \sum_j \lambda_{i,j} w_j. \]

This suggests \( \dim(\langle H \rangle \cap \langle B \rangle) \) as a measure of the information gained by the adversary Eve. In the particular case we started with, when \( d(\lambda(C)) = k + 1 \), we see that when \( \mu = n - k + r, \ r \geq 1 \), then
\[ \dim(\langle H \rangle \cap \langle B \rangle) = r. \]

Indeed, when Eve gets to tap \( \mu = n - k + r \) edges, then \( \mathcal{M} \) becomes a \((k + n - k + r) \times n\) matrix, whose rank is \( n \) (since it reached \( n \) already after listening to \( n - k \) edges), and
\[
\begin{align*}
\lambda &= \text{rank}(M) \\
&= \text{rank}(H) + \text{rank}(B) - \dim(\langle H \rangle \cap \langle B \rangle) \\
&= k + n - k + r - \dim(\langle H \rangle \cap \langle B \rangle).
\end{align*}
\]

This behavior is not without remembering how the performance of a wiretap code \( \mathcal{M} \) is characterized by its rank metric [7]. Recall that given an \((n, k)\) code \( \mathcal{C} \), its \( r \)-dimensional subcodes, \( 1 \leq r \leq k \), are obtained as the span of \( r \) linearly independent vectors in \( \mathcal{C} \). Then for a given \( r \), the support of an \( r \)-dimensional subcode \( \mathcal{D} \) is the set of coordinates for which there is at least one codeword with non-zero coefficient:
\[
\chi(\mathcal{D}) = \{ i, \text{ there exists } a \in \mathcal{D} \text{ with } a_i \neq 0 \}.
\]

The smallest support of an \( r \)-dimensional subcode \( \mathcal{D} \) of \( \mathcal{C} \) is called the \( r \)th generalized Hamming weight of \( \mathcal{C} \):
\[
d_r(\mathcal{C}) = \min \{ \chi(\mathcal{D}) \mid \mathcal{D} \text{ a subcode of dimension } r \}.
\]

If \( r = 1 \), subcodes are generated by one codeword (that is, they only contain the multiples of a codeword), and
\[
d_1(\mathcal{C}) = d_H(\mathcal{C}).
\]

As in the scheme explained above for a wiretap network code, a linear \((n, n - k)\) code \( \mathcal{C} \) with parity check matrix a \( k \times n \) matrix \( H \) can be used as a wiretap code, to encode a secret of length \( k \). The generalized Hamming weights of the dual code \( \mathcal{C}^\perp \) give the number \( \mu \) of taps at which the equivocation at the eavesdropper drops [7], or in other words, where her knowledge of the secret increases.

In particular, if \( \mathcal{C} \) is an \((n, n - k)\) maximal distance separable (MDS) code, its dual code \( \mathcal{C}^\perp \) is an \((n, k)\) code known to be MDS, thus such that \( d_r(\mathcal{C}^\perp) = n - k + 1 \). As shown in [8], the generalized Hamming weights of \( \mathcal{C}^\perp \) are
\[
d_r(\mathcal{C}^\perp) = n - k + r, \ r \geq 1.
\]

An \((n, k)\) code \( \mathcal{C} \) satisfying \( d_r(\mathcal{C}) = n - k + r \) is said to be \( r \)-MDS [8].

This suggests that \( \mu = n - k + r \) for which
\[ \dim(\langle H \rangle \cap \langle B \rangle) = r, \]
that is the value of \( \mu \) for which the adversary knowledge of \( s \) increases, plays the role of a generalized rank weight, that is a generalized weight \( d_r(\lambda(\mathcal{C}^\perp)) \) with respect to the rank metric. Note that when \( r = 1, \mu = n - k + 1 \), and indeed
\[
d_1(\lambda(\mathcal{C}^\perp)) = n - k + 1,
\]

since when \( d_1(\lambda(\mathcal{C})) = k + 1 \), the \((n, n - k)\) \( \mathcal{C} \) code is MRD, whose dual \( \mathcal{C}^\perp \) is also MRD (see Proposition 1), thus satisfying \( d_1(\lambda(\mathcal{C}^\perp)) = n - k + 1 \).

IV. GENERALIZED RANK WEIGHTS

Motivated by rank metric codes as wiretap network codes, we propose a definition of generalized rank weights.

**Definition 1:** Let \( \mathcal{C} \) be an \((n, k)\) code over \( \mathbb{F}_{q^m} \). We define
\[
d_r(\lambda(\mathcal{C})) := \min_{\mathcal{D} \text{ a subcode of } \mathcal{C} \setminus \mathcal{D} \times \mathcal{X} \in \mathcal{D}} \max_{\dim(\mathcal{D}) = r} \text{rank}(\lambda(\mathcal{X})), \ r = 1, \ldots, k
\]
to be the \( r \)th generalized rank weight of \( \mathcal{C} \).

First we need to check that this definition is consistent with that of \( d_1(\lambda(\mathcal{C})) \). Now
\[
d_1(\lambda(\mathcal{C})) = \min_{\mathcal{D} \text{ a subcode of } \mathcal{C} \setminus \mathcal{D}} \max_{\dim(\mathcal{D}) = 1} \text{rank}(\lambda(\mathcal{X}))
\]

yielding the original definition of \( d_1(\lambda(\mathcal{C})) \) as desired. The third equality holds since \( \text{rank}(\lambda(\alpha x)) = \text{rank}(\lambda(x)) \) for any non-zero \( \alpha \in \mathbb{F}_{q^m} \). Indeed, \( \lambda(\alpha x) = M_{\alpha}, \lambda(x) \) where \( M_{\alpha} \) is a multiplication matrix by \( \alpha \) which is invertible whenever \( \alpha \neq 0 \), and multiplication by a non-singular matrix does not change the rank of \( \lambda(x) \).

Let \( \mathcal{C} \) be an \((n, k)\) MRD code with generator matrix \( H \) of the form (2), that is \( d_1(\lambda(\mathcal{C})) = n - k + 1 \) and
\[
H = \begin{bmatrix}
h_1 & \ldots & h_n \\
h_1' & \ldots & h_n' \\
\vdots & & \vdots \\
h_1^{q^{d_1-2}} & \ldots & h_n^{q^{d_1-2}}
\end{bmatrix}
\]

By definition, we have that
\[
d_2(\lambda(\mathcal{C})) = \min_{\mathcal{D}} \max_{\dim(\mathcal{D}) = 2} \text{rank}(\lambda(\alpha x)), \ \alpha \neq 0
\]

Now define the new parity check matrix
\[
H_1 = \begin{bmatrix}
h_1 & \ldots & h_n \\
h_1' & \ldots & h_n' \\
\vdots & & \vdots \\
h_1^{q^{d_1-2}} & \ldots & h_n^{q^{d_1-2}}
\end{bmatrix}
\]

by adding one row to \( H \). We claim that given \( x, y \in \mathcal{C} \) linearly independent, there exist \( \alpha, \beta \in \mathbb{F}_{q^m} \) such that
\[
H_1(\alpha x^T + \beta y^T) = 0.
\]
Since $x, y \in C$, by definition $H(\alpha x^T + \beta y^T) = 0$ and it is
enough to check that
\[
\begin{bmatrix}
\alpha x_1 + \beta y_1 \\
\vdots \\
\alpha x_n + \beta y_n
\end{bmatrix} = 0,
\]
that is
\[
\alpha (h_1^{q^{d-1}} x_1 + \ldots + h_n^{q^{d-1}} x_n) + \beta (h_1^{q^{d-1}} y_1 + \ldots + h_n^{q^{d-1}} y_n) = 0.
\]
Note that if $A := h_1^{q^{d-1}} x_1 + \ldots + h_n^{q^{d-1}} x_n = 0$, respectively $B := h_1^{q^{d-1}} y_1 + \ldots + h_n^{q^{d-1}} y_n = 0$, then $x$, respectively $y$, is already in the kernel of $H$. We can thus assume that both $A, B \in \mathbb{F}_q^n$ are non-zero, and choose $\alpha = A^{-1}$ and $\beta = -B^{-1}$. We are left to check that $A^{-1} x - B^{-1} y$ is a
non-zero vector. But this follows from the fact that $x$ and $y$ are chosen linearly independent.

Since $\alpha x + \beta y$ is in the kernel of $H$, the parity check matrix of a code of rank distance $d_i + 1$, this shows that $\text{rank}(\alpha x + \beta y) > d_i$, and consequently, we have thus shown the following.

Lemma 1: Let $C$ be an $(n, k)$ code which is MRD, with
parity check matrix of the form (2). Then
\[
d_2(\lambda(C)) > d_1(\lambda(C)).
\]

The following definition mimics the notion of 2-MDS codes.

Definition 2: Let $C$ be an $(n, k)$ code. It is said to be 2-MRD if
\[
d_2(\lambda(C)) = n - k + 2.
\]

We will give next an example of code which is a proper 2-MRD code, that is a 2-MRD code which is not MRD.

V. THE CASE OF NON-MRD CODES

So far, we discussed MRD codes as wiretap codes, and though we gave a general definition for generalized rank weights, most of the analysis we provided focused on MRD codes. In this section, we start considering the case of general (non-MRD) codes. We start with a work-out example, to illustrate that the interpretation of rank distance in terms of security (seems to) hold(s) similarly, irrespectively of whether
the code is MRD.

Example 1: Consider the finite field $\mathbb{F}_{2^5}$, that is $q = 2$ and $m = 5$, with $k = 3$ and $n = 5$. Let $w$ denote a primitive element of $\mathbb{F}_{2^5}$ and take for $C$ the $(5,3)$ code whose parity check matrix $H$ is given by
\[
H = \begin{bmatrix}
w & w^2 & 1 & 1 & 0 \\
w^2 & 0 & w & 0 & 1
\end{bmatrix},
\]
and whose generator matrix $G$ is
\[
G = \begin{bmatrix}
w^{30} & 0 & 1 & 0 & 0 \\
w^{29} & 0 & w^{29} & 0 & 1 \\
w^{28} & 0 & w^{28} & 0 & 1
\end{bmatrix}.
\]
It is easy to see that $d_1(\lambda(C)) = 2$. Indeed, a codeword $x \in C$
is of the form
\[
x = (u_1 w^{30} + u_3 w^{29}, u_2 w^{29} + u_3 w^{28}, u_1, u_2, u_3),
\]
with $u_1, u_2, u_3 \in \mathbb{F}_{2^5}$. Now if there were an $x$ such that $\text{rank}(\lambda(x)) = 1$, then all its components would be multiples in $\mathbb{F}_2$ of each other, say of $u_1$ (assuming $u_1 \neq 0$), that is $u_2 = a_2 u_1, u_3 = a_3 u_1, u_2 w^{29} + u_3 w^{28} = a_4 u_1$ and $u_1 w^{30} + u_3 w^{29} = a_5 u_1, a_4, a_5 \in \mathbb{F}_2, i = 1, \ldots, 5$. This gives a system of linear equations which cannot be solved when restricting the coefficients $a_i$ to be in $\mathbb{F}_2$. The same argument can be repeated with either $u_3$ or $u_1$ if $u_1 = 0$. On the other hand, there exists an $x$ such that $\text{rank}(\lambda(x)) = 2$, for example take $u_2 = u_3 = 0$ and $u_1 = 1$, that is
\[
x = (w^{30}, 0, 1, 0, 0).
\]
This code is not MRD, since
\[
d_1(\lambda(C)) = 2 < n - k + 1 = 3.
\]

The dual code $C^\perp$ has generator matrix $H$. Thus a generic codeword $x \in C^\perp$ is
\[
x = (u_1 w + u_2 w^2, u_1 w^2, u_1 + u_2 w, u_1, u_2),
\]
and $u_1, u_2 \in \mathbb{F}_2$. It is clear that $d_1(C^\perp) \geq 2$, since $u_1$ and $u_1 w$ are never $\mathbb{F}_2$-linearly dependent, apart if $u_1 = 0$, in which case we get $(u_2 w^2, 0, u_2 w, 0, u_2)$, whose rank is 3. Note that if instead $u_2 = 0$, then the vector $(u_1 w, u_1 w^2, u_1, u_1, 0)$ also has rank 3, so that we need to take $u_1, u_2$ both non-zero to look for a matrix of rank 2. But then this means that $x_1, x_3$ and $x_5$ are $\mathbb{F}_2$-linear combinations of $u_1$ and $u_2 w$, which again (as above, write the system of linear equations) is not possible, and
\[
d_1(C^\perp) = 3.
\]

It can be computed (following Definition 1) numerically that $d_2(C^\perp) = 5$.

To evaluate $C$ as a wiretap code (see Section III), we consider the matrix
\[
M = \begin{bmatrix}
H \\
B
\end{bmatrix}
\]
where $H$ is as in (3) and $B$ is any full rank $\mu \times 5$ matrix in $\mathbb{F}_2$. It can be checked that there is no full rank $2 \times 5$ matrix $B$ with coefficients in $\mathbb{F}_2$ such that $\text{rank}(M) = 3$, that is such that $\dim((H) \cap (B)) = 1$. However such a matrix exists when $\mu = 3$, for example, take
\[
B = \begin{bmatrix}
1 & 0 & 1 & 1 & 0 \\
1 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0
\end{bmatrix},
\]
which clearly has full rank 3. Then
\[
M = \begin{bmatrix}
w & w^2 & 1 & 1 & 0 \\
w^2 & 0 & w & 0 & 1 \\
1 & 0 & 1 & 1 & 0 \\
1 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0
\end{bmatrix},
\]
and the 3rd column is the sum of the 4th one and of $w$ times the 5th one. The rank of $M$ is 4, and $\dim((H) \cap (B)) = 1$.

This is coherent with our interpretation of the rank distance, since the drop in security occurs at
\[
\mu = 3 = d_1(C^\perp).
\]
In fact it can also be computed numerically that \( \dim((H) \cap \langle B \rangle) \) increases from 1 to 2 when \( \mu = 5 \).

**Example 2:** Consider as in the previous example the finite field \( \mathbb{F}_2 \), with primitive element \( w \), with this time \( k = 2 \) and \( n = 5 \). The \((5, 2)\) code \( C \) is obtained by adding one row to the parity check matrix of the previous example, namely, it has parity check matrix

\[
H = \begin{bmatrix}
w & w^2 & 1 & 1 & 0 \\
w^2 & 0 & w & 0 & 1 \\
1 & w & 0 & 1 & 1
\end{bmatrix}.
\]

It can be computed numerically that \( d_1(\lambda(C)) = 3 \), \( d_1(\lambda(C^⊥)) = 2 \), and \( d_2(\lambda(C^⊥)) = 4 \). This illustrates that (i) by adding one row to the parity check matrix, the rank distance has increased from 2 (in the previous example) to 3 (here), (ii) the \((5, 3)\) dual code \( C^⊥ \) is not MRD (\( d_1(\lambda(C^⊥)) = 2 < 3 \)) but is 2-MRD (see Definition 2) since \( d_2(\lambda(C^⊥)) = 4 = 2 + 2 \).

We now show that for general rank metric codes, MRD or not, the drop in security happens at the minimum rank distance of the dual code.

**Proposition 2:** Let \( H \) be an \((n - k) \times n\) parity check matrix of an \((n, k)\) code \( C \) over \( \mathbb{F}_q^m \).

1) If \( B \) is a \((d_1(\lambda(C^⊥)) - 1) \times n\) full rank matrix with coefficients in \( \mathbb{F}_q \), then \( \dim((H) \cap \langle B \rangle) = 0 \).

2) There exists a \( d_1(\lambda(C^⊥)) \times n\) full rank matrix \( B \) with coefficients in \( \mathbb{F}_q^m \) such that \( \dim((H) \cap \langle B \rangle) \geq 1 \).

**Proof:** 1) Assume \( B \) is a \((d_1(\lambda(C^⊥)) - 1) \times n\) full rank matrix in \( \mathbb{F}_q^m \). If \( \dim((H) \cap \langle B \rangle) \geq 1 \), then there exist \( \lambda_1, \ldots, \lambda_{n-k} \) and \( d_1(\lambda(C^⊥)) \) not all zero such that

\[
\sum_{i=1}^{n-k} \lambda_i H_i + \sum_{j=1}^{d_1(\lambda(C^⊥)) - 1} \lambda_{n-k+j} B_j = 0,
\]

there is \( x = (x_1, x_2) \) such that \( x M = 0 \), or \( x_1 H = -x_2 B \). Set \( a := (x_1, H) \in C^⊥ \subset \mathbb{F}_q^m \) and expand \( a \) into an \( m \times n \) matrix \( A = \lambda(a) \in C^⊥ \). Do the same with the vector \( x_2 \in \mathbb{F}_{q^m}^1 \times (d_1(\lambda(C^⊥)) - 1) \), to obtain a matrix \( \lambda(x_2) = X_2 \).

Because \( B \) is a matrix in \( \mathbb{F}_q^m \), we have that

\[
A = -X_2 B,
\]

thus the rank of \( A \) is \( d_1(\lambda(C^⊥)) - 1 \), a contradiction.

2) It is enough to show the existence of a zero vector \( x \) of length \( n - k + d_1(\lambda(C^⊥)) \) such that \( x M = 0 \) for some \( d_1(\lambda(C^⊥)) \times n \) full rank matrix \( B \) in \( \mathbb{F}_q^m \). Take any non-zero vector \( x_1 \) of length \( n - k \), then \( x_1 H \in C^⊥ \). There exists a vector \( x_1 \) with the property that \( \lambda(x_1 H) \) has rank \( d_1(\lambda(C^⊥)) \).

Thus \( \lambda(x_1 H) \in \mathbb{F}_q^{m \times n} \) can be written as \( x_2 B \) for some \( m \times d_1(\lambda(C^⊥)) \) matrix \( X_2 \) in \( \mathbb{F}_q \) and some matrix \( B \) in \( \mathbb{F}_q^m \) of size \( d_1(\lambda(C^⊥)) \times n \), showing that \( x_1 H = -x_2 B \) for \( x_2 = -\lambda^{-1}(X_2) \). Pick \( x = (x_1, x_2) \).

If \( C \) is an \((n, n - k)\) MRD code, we rederive Theorem 2.

**Corollary 1:** Let \( C \) be an \((n, n - k)\) MRD code over \( \mathbb{F}_q^m \). If \( \mu \leq n - k \) then

\[
\text{rank}(M) = \text{rank}(H) + \text{rank}(B), \text{ for all } B \in \mathbb{F}_q^{\mu \times n}.
\]

**Proof:** If \( C \) is an \((n, n - k)\) MRD code over \( \mathbb{F}_q^m \), then so is its dual (see Proposition 1), and

\[
d_1(\lambda(C^⊥)) = n - k + 1.
\]

Thus for every full rank \((n - k) \times n\) matrix \( B \), \( \dim((H) \cap \langle B \rangle) = 0 \), and \( \text{rank}(M) = \text{rank}(H) + \text{rank}(B) \). Since this is true for every \((n - k) \times n\) matrix \( B \), this is also true for matrices \( B \) with less rows.

**VI. ONGOING AND FUTURE WORK**

The goal of this paper was to address the existence of generalized weights for rank metric codes, called generalized rank weights. We regarded rank metric codes as wiretap network codes, to conjecture what would be a good definition of such weights. We gave some preliminary properties of the proposed definition, all so far supporting the choice of the current definition. In particular we analyzed the second generalized rank distance of MRD codes.

This opens the road to numerous questions: an obvious question that we are currently looking at is to show that generalized rank weights form a strictly increasing chain. Once this is established, it will be natural to study bounds, as well as rank metric codes satisfying these bounds. Generalized Hamming weights have also been studied in the context of network coding in [11]. Another possible interesting question would be to compare both weights.

**ACKNOWLEDGMENT**

The research of F. Oggier and A. Shouai for this work is supported by the Singapore National Research Foundation under Research Grant NRF-RF2009-07.

**REFERENCES**


