On defining generalized rank weights

Relinde Jurrius* Ruud Pellikaan†

Computational Aspects and
Mathematical Methods for Finite Fields
special session of
Applications of Computer Algebra, ACA 2015
23 July 2015, Kalamata, Greece

Abstract

This paper investigates the generalized rank weights, with a definition implied by the study of the generalized rank weight enumerator. We study rank metric codes over L, where L is a finite extension of a field K. This is a generalization of the case where $K = \mathbb{F}_q$ and $L = \mathbb{F}_{q^m}$ of Gabidulin codes to arbitrary characteristic. We show equivalence to previous definitions, in particular the ones by Kurihara-Matsumoto-Uyematsu [12, 13], Oggier-Sboui [15] and Ducoat [6]. As an application of the notion of generalized rank weights, we discuss codes that are degenerate with respect to the rank metric.

1 Introduction

Error-correcting codes with the rank distance were introduced by Gabidulin [7]. Recently they have gained a lot of interest because of their application to network coding. In network coding, messages are not transmitted over a single channel, but over a network of channels. This application induced a lot of theoretical research to rank metric codes.

Many notions in the theory for codes with the Hamming metric have an equivalent notion for codes with the rank metric. We studied the rank-metric equivalent of the weight enumerator and several generalizations of it [10]. From this theory, a definition of the generalized rank weights follows. These

*relinde.jurrius@unine.ch
†g.r.pellikaan@tue.nl

are the rank metric equivalence of the generalized Hamming weights. Definitions of the generalized rank weights were already proposed: we show here that the definition that follows from our work leads to the same values as all of the proposed definitions. In particular, this means all previously proposed definitions are equivalent for rank metric codes over finite fields.
This paper investigates the generalized rank weights of a code over L, where L is a finite Galois extension of a field K. This is a generalization of the case where $K = \mathbb{F}_q$ and $L = \mathbb{F}_{q^m}$ of Gabidulin codes [7] to arbitrary characteristic as considered by Augot-Loidreau-Robert [2, 1].
As a small application of the generalized rank weights, we discuss the concept of degenerate codes.

2 Rank metric codes and weights

Let K be a field and let L be a finite Galois extension of K. A *rank metric code* is an L-linear subspace of L^n. To all codewords we associate a matrix as follows. Choose a basis $B = \{\alpha_1, \ldots, \alpha_m\}$ of L as a vector space over K. Let $\mathbf{c} = (c_1, \ldots, c_n) \in L^n$. The $m \times n$ matrix $M_B(\mathbf{c})$ is associated to $\mathbf{c}$ where the j-the column of $M_B(\mathbf{c})$ consists of the coordinates of c_j with respect to the chosen basis: $c_j = \sum_{i=1}^m c_{ij}\alpha_i$. So $M_B(\mathbf{c})$ has entries c_{ij}.
The K-linear row space in K^n and the rank of $M_B(\mathbf{c})$ do not depend on the choice of the basis B, since for another basis B' there exists an invertible matrix A such that $M_B(\mathbf{c}) = AM_{B'}(\mathbf{c})$. The rank weight $\mathrm{wt}_R(\mathbf{c}) = \mathrm{rk}(\mathbf{c})$ of $\mathbf{c}$ is by definition the rank of the matrix $M_B(\mathbf{c})$, or equivalently the dimension over K of the row space of $M_B(\mathbf{c})$. This definition follows from the rank distance, that is defined by $d_R(\mathbf{x}, \mathbf{y}) = \mathrm{rk}(\mathbf{x} - \mathbf{y})$. The rank distance is in fact a metric on the collection of all $m \times n$ matrices, see [7, 2].
The following is from [10, Definition 1].

Definition 1. Let C be an L-linear code. Let $\mathbf{c} \in C$. Then $\mathrm{Rsupp}(\mathbf{c})$, the *rank support* of $\mathbf{c}$ is the K-linear row space of $M_B(\mathbf{c})$. So $\mathrm{wt}_R(\mathbf{c})$ is the dimension of $\mathrm{Rsupp}(\mathbf{c})$. Let D be an L-linear subcode of C. Then $\mathrm{Rsupp}(D)$, the *rank support* of D is the K-linear space generated by the $\mathrm{Rsupp}(\mathbf{d})$ for all $\mathbf{d} \in D$. Then $\mathrm{wt}_R(D)$, the *rank support weight* of D is the dimension of $\mathrm{Rsupp}(D)$.

Note that this definition is the rank metric case of the support weights, or weights of subcodes, of codes over the Hamming metric. An *isometry* with respect to the rank metric is an automorphism of L^n that preserves the rank distance. The following theorem characterizes when we call two rank metric codes "equivalent":

Theorem 2. *The group $Iso(L^n)$ of isometries of L^n with respect to the rank distance is generated by the scalar multiplications $\lambda : L^n \to L^n$ with λ in L^* given by $\lambda\mathbf{x} = (\lambda x_1, \ldots, \lambda x_n)$, and the general linear group $GL(n; K)$ of invertible $n \times n$ matrices with entries in K. The group $Iso(L^n)$ is isomorphic to the product group $L^*/K^* \times GL(n; K)$*

Proof. The proof in [3] and [4, Theorem 1] in case of finite fields is easily generalized. □

We prove some basic properties of the rank weight and rank support.

Proposition 3. *Let C be an L-linear code.*
(1) *Let $\mathbf{x} \in L^n$ and $\alpha \in L^*$. Then* $\mathrm{Rsupp}(\alpha\mathbf{x}) = \mathrm{Rsupp}(\mathbf{x})$.
(2) *Let $\mathbf{x}, \mathbf{y} \in L^n$. Then* $\mathrm{Rsupp}(\mathbf{x} + \mathbf{y}) \subseteq \mathrm{Rsupp}(\mathbf{x}) + \mathrm{Rsupp}(\mathbf{y})$.
(3) *Let $\mathbf{x}, \mathbf{y} \in L^n$. Then* $\mathrm{wt}_R(\mathbf{x} + \mathbf{y}) \leq \mathrm{wt}_R(\mathbf{x}) + \mathrm{wt}_R(\mathbf{y})$.
(4) *If $\mathbf{g}_1, \ldots, \mathbf{g}_k$ generate C as an L-linear space, then* $\mathrm{Rsupp}(C)$ *is the K-linear sum of the* $\mathrm{Rsupp}(\mathbf{g}_i)$, *$i = 1, \ldots, k$.*

Proof. (1) Let $B = \{\alpha_1, \ldots, \alpha_m\}$ be a basis of L as a vector space over K. Let $\alpha \in L^*$. Then $B' = \{\alpha\alpha_1, \ldots, \alpha\alpha_m\}$ is another basis of L as a vector space over K. Now $\mathrm{Rsupp}(\mathbf{x})$ is the row space of $M_B(\mathbf{x})$. But this row space does not depend on the chosen basis. Hence $\mathrm{Rsupp}(\alpha\mathbf{x})$ is the row space of $M_{B'}(\alpha\mathbf{x})$ and this row space is equal to $\mathrm{Rsupp}(\mathbf{x})$, since $M_{B'}(\alpha\mathbf{x}) = M_B(\mathbf{x})$.
(2) The matrix $M_B(\mathbf{x})$ has entries x_{ij} with $x_j = \sum_{i=1}^m x_{ij}\alpha_i$, and $M_B(\mathbf{y})$ has entries y_{ij} with $y_j = \sum_{i=1}^m y_{ij}\alpha_i$. So $M_B(\mathbf{x}+\mathbf{y})$ has entries $x_{ij}+y_{ij}$, since $x_j + y_j = \sum_{i=1}^m (x_{ij}+y_{ij})\alpha_i$. Now $\mathrm{Rsupp}(\mathbf{x})$, $\mathrm{Rsupp}(\mathbf{y})$ and $\mathrm{Rsupp}(\mathbf{x}+\mathbf{y})$ are equal to the row spaces of $M_B(\mathbf{x})$, $M_B(\mathbf{y})$ and $M_B(\mathbf{x}+\mathbf{y})$, respectively. Therefore $\mathrm{Rsupp}(\mathbf{x}+\mathbf{y}) \subseteq \mathrm{Rsupp}(\mathbf{x}) + \mathrm{Rsupp}(\mathbf{y})$, since $M_B(\mathbf{x}+\mathbf{y}) = M_B(\mathbf{x}) + M_B(\mathbf{y})$.
(3) This is a direct consequence of (2), since $\mathrm{wt}_R(\mathbf{x}) = \dim \mathrm{Rsupp}(\mathbf{x})$ and $\dim(I + J) \leq \dim(I) + \dim(J)$ for subspaces I and J of K^n.
(4) Let $\mathbf{g}_1, \ldots, \mathbf{g}_k$ generate C as an L-linear space. Then $\mathrm{Rsupp}(C)$ contains the K-linear sum of the $\mathrm{Rsupp}(\mathbf{g}_i)$, by definition. Conversely, let $\mathbf{c} \in C$. Then $\mathbf{c} = \sum_{i=1}^k \lambda_i \mathbf{g}_i$ is in the K-linear sum of the $\mathrm{Rsupp}(\mathbf{g}_i)$, by applying (1) and (2) repeatedly. Therefore $\mathrm{Rsupp}(C)$ is contained in the K-linear sum of the $\mathrm{Rsupp}(\mathbf{g}_i)$. □

Definition 4. Let $K = \mathbb{F}_q$ and $L = \mathbb{F}_{q^m}$. Let C be an L-linear code. Then for every $r = 0, \ldots, k$ the *generalized rank weight enumerator* is defined by

$$W_C^{R,r}(X, Y) = \sum_{w=0}^{n} A_w^{R,r} X^{n-w} Y^w,$$

where $A_w^{R,r}$ is the number of subcodes of C of dimension r and rank weight w. This is well-defined, since L^n is finite.

Just like with the weight enumerator and the minimum distance, a special case of interest is the first nonzero coefficient of these polynomials.

Definition 5. Let C be an L-linear code. Then $d_{R,r}(C)$, the r-th *generalized rank weight* of the code C is the minimal rank support weight of a subcode D of C of dimension r. That is:

$$d_{R,r}(C) = \min_{\substack{D \subseteq C \\ \dim(D)=r}} \mathrm{wt}_R(D).$$

The above is not the only proposed definition of the generalized rank weights. The first proposal of a definition of the r-th generalized rank weight was given by Kurihara-Matsumoto-Uyematsu [12, 13]. An alternative was given by Oggier-Sboui [15] and Ducoat [6]. Both definitions were motivated by applications. Before we discuss these definitions, we develop some more theory about rank metric codes.

3 Some codes related to C

With respect to the Hamming distance and a k-dimensional $\mathbb{F}_q$-linear code C, the support of C is defined by $\mathrm{supp}(C) = \{j \mid c_j \neq 0 \text{ for some } \mathbf{c} \in C\}$. The subcode $C(J)$ is defined in [11] and [9, Definition 5.1] for a subset J of $\{1, \ldots, n\}$ with complement J^c by:

$$C(J) = \{\ \mathbf{c} \in C \mid \mathrm{supp}(\mathbf{c}) \subseteq J^c\ \}.$$

Define $C(j) = C(\{j\})$ for $j \in \{1, \ldots, n\}$. Let $J = \mathrm{supp}(C)$, then $C(j)$ has codimension 1 in C for all $j \in J$. In fact, $C(j)$ is the code C punctured in position j, but without the removing of the zeros in this position.

We claim that if $n < q$, then there exists a $\mathbf{c} \in C$ such that $\mathrm{supp}(\mathbf{c}) = \mathrm{supp}(C)$. Suppose $n < q$. Then $|J| < q$ and

$$\bigcup_{j \in J} C(j) \neq C,$$

since

$$\left| \bigcup_{j \in J} C(j) \right| \leq |J| q^{k-1} < q^k = |C|.$$

Let $\mathbf{c} \in C \setminus \bigcup_{j \in J} C(j)$. Then $\mathrm{supp}(\mathbf{c}) \subseteq \mathrm{supp}(C) = J$. Furthermore $\mathbf{c} \notin C(j)$ for all $j \in J$. So $c_j \neq 0$ for all $j \in J$. Hence $J = \mathrm{supp}(\mathbf{c}) = \mathrm{supp}(C)$.

We will now translate this statement to rank metric codes. Notice that the statements "$I \subseteq J^c$" and "$I \cap J = \emptyset$" are equivalent for two subsets I and J of $\{1, \ldots, n\}$. These statements would translate into "$I \subset J^\perp$" and "$I \cap J = \{0\}$", respectively, for subspaces I and J of K^n, but these are not equivalent. For the definition of $C(J)$ in the context of the rank metric we give the following analogous definition as given in [10, Definition 2].

Definition 6. Let L be a finite field extension of the field K. Let C be an L-linear code. For a K-linear subspace J of K^n we define:

$$C(J) = \{ \mathbf{c} \in C \mid \mathrm{Rsupp}(\mathbf{c}) \subseteq J^\perp \}$$

From this definition it is clear that $C(J)$ is a K-linear subspace of C, but in fact it is also an L-linear subspace.

Lemma 7. *Let C be an L-linear code of length n and let J be a K-linear subspace of K^n. Then $\mathbf{c} \in C(J)$ if and only if $\mathbf{c} \cdot \mathbf{y} = 0$ for all $\mathbf{y} \in J$. Furthermore $C(J)$ is an L-linear subspace of C.*

Proof. The following statements are equivalent:

$$\begin{gathered}
\mathbf{c} \in C(J) \\
\textstyle\sum_{j=1}^n c_{ij} y_j = 0 \text{ for all } \mathbf{y} \in J \text{ and } i = 1, \ldots, m \\
\textstyle\sum_{i=1}^m (\sum_{j=1}^n c_{ij} y_j) \alpha_i = 0 \text{ for all } \mathbf{y} \in J \\
\textstyle\sum_{j=1}^n (\sum_{i=1}^m c_{ij} \alpha_i) y_j = 0 \text{ for all } \mathbf{y} \in J \\
\textstyle\sum_{j=1}^n c_j y_j = 0 \text{ for all } \mathbf{y} \in J \\
\mathbf{c} \cdot \mathbf{y} = 0 \text{ for all } \mathbf{y} \in J
\end{gathered}$$

Hence $C(J) = \{\mathbf{c} \in C \mid \mathbf{c} \cdot \mathbf{y} = 0 \text{ for all } \mathbf{y} \in J\}$. From this description it follows straightforwardly that $C(J)$ is an L-linear subspace of C. □

Corollary 8. *Let C be an L-linear code of length n. Let J be a K-linear subspace of K^n. Then $\dim_L(C(J)) \geq \dim_L(C) - \dim_K(J)$.*

Proof. This follows directly from Lemma 7. □

Remark 9. Let I be a K-linear subspace of K^n and $J = \mathrm{Rsupp}(C)$. Then $C = C(I)$ if and only if $I \subseteq J^\perp$, since the following statements are equivalent:

$$\begin{gathered}
C = C(I) \\
\mathrm{Rsupp}(\mathbf{c}) \subseteq I^\perp \text{ for all } \mathbf{c} \in C \\
\mathrm{Rsupp}(C) \subseteq I^\perp \\
J \subseteq I^\perp \\
I \subseteq J^\perp
\end{gathered}$$

Hence, it is not necessarily the case that $\dim_L(C(I)) \geq \dim_L(C) - 1$ for all one dimensional subspaces I of J, since we might have that $J \subseteq J^\perp$.

Proposition 10. *Let $L = \mathbb{F}_{q^m}$ and $K = \mathbb{F}_q$. Let C be an L-linear code. If $m \geq n$, then there exists a $\mathbf{c} \in C$ such that*

$$\mathrm{Rsupp}(\mathbf{c}) = \mathrm{Rsupp}(C).$$

Proof. First, note that the inclusion $\mathrm{Rsupp}(\mathbf{c}) \subseteq \mathrm{Rsupp}(C)$ holds for all $\mathbf{c} \in C$. Let $k = \dim_L(C)$ and $J = \mathrm{Rsupp}(C)$. Then we have

$$\left| \bigcup_{\substack{\dim(I)=1 \\ C(I)\neq C}} C(I) \right| \leq \frac{q^n - 1}{q - 1} q^{m(k-1)} < q^{mk} = |C|.$$

In the first inequality, we use that the number of one dimensional subspaces of K^n is $\frac{q^n-1}{q-1}$, since $K = \mathbb{F}_q$. In the second inequality, we use that $n \leq m$ so $\frac{q^n-1}{q-1} < q^m$. It follows that

$$\bigcup_{\substack{\dim(I)=1 \\ C(I)\neq C}} C(I) \neq C.$$

Let $\mathbf{c} \in C \setminus \bigcup_{\dim(I)=1, C(I)\neq C} C(I)$. Then by definition $\mathrm{Rsupp}(\mathbf{c}) \subseteq J$. Now suppose $\mathrm{Rsupp}(\mathbf{c}) \neq J$. Then $\mathrm{Rsupp}(\mathbf{c})$ is contained in a codimension 1 subspace of J, hence there exists a codimension 1 subspace H of K^n such that $\mathrm{Rsupp}(\mathbf{c}) \subseteq H$ and $J \cap H \neq J$.
Let $I = H^\perp$. Then I is a 1-dimensional subspace of K^n with $\mathrm{Rsupp}(\mathbf{c}) \subseteq H = I^\perp$, so $\mathbf{c} \in C(I)$. Now $C(I) = C$ by the choice of $\mathbf{c}$, hence $\mathrm{Rsupp}(\mathbf{x}) \subseteq I^\perp = H$ for all $\mathbf{x} \in C$. Therefore $J = \mathrm{Rsupp}(C) \subseteq H$. This is a contradiction, since $J \cap H \neq J$. So $\mathrm{Rsupp}(\mathbf{c}) = \mathrm{Rsupp}(C)$. □

Remark 11. We could not proof nor disproof this proposition for arbitrary field K and a finite extension L of degree $m \geq n$. The following example gives a counterexample in the case $m < n$.

Example 12. Let $K = \mathbb{F}_2$, $m = 3$ and $L = \mathbb{F}_8$. Let $\alpha \in L$ with $\alpha^3 = 1 + \alpha$. Let C be the L-linear code in L^4 generated by $\mathbf{a} = (1, \alpha, \alpha^2, \alpha^3)$ and $\mathbf{b} = (1, \alpha, \alpha^2, \alpha^4)$. Then $\mathrm{Rsupp}(C) = K^4 \neq \mathrm{Rsupp}(\mathbf{c})$ for all $\mathbf{c} \in C$, since $\dim \mathrm{Rsupp}(\mathbf{c}) \leq m = 3$.

Proposition 13. *Let $L = \mathbb{F}_{q^m}$ and $K = \mathbb{F}_q$. Let $\mathbf{x}, \mathbf{y} \in L^n$. Let $I = \mathrm{Rsupp}(\mathbf{x})$ and $J = \mathrm{Rsupp}(\mathbf{y})$. If $m \geq n$, then there are constants $\alpha, \beta \in L$ such that $\mathrm{Rsupp}(\alpha\mathbf{x} + \beta\mathbf{y}) = I + J$.*

Proof. This is a consequence of Proposition 10. □

4 Galois closure and trace

Before we can give the various definitions of the generalized rank weights, we introduce the framework in which we study them.

Definition 14. Let L/K be a Galois extension. Let $C \subseteq L^n$ be an L-linear subspace. The *trace map* $\mathrm{Tr} : L^n \to K^n$ is the component-wise extension of the trace map $\mathrm{Tr} : L \to K$. The *restriction* of C is defined by $C|_K = C \cap K^n$. The *Galois closure* C^* of C is the smallest subspace of L^n that contains C and that is closed under the component-wise action of the Galois group of L/K. A subspace is called *Galois closed* if and only if it is equal to its own Galois closure.
If C is a K-linear subspace, then we define the *extension codes* $C \otimes L$ as the subspace of L^n formed by taking all L-linear combinations of words of C.

We can summarize the above relations in the following diagram:

$$\begin{tikzcd}
C \arrow[r, "\mathrm{Gal}(L/K)"] \arrow[dr, "\mathrm{Tr}(\mathbf{c})"] & C^* \\
C|_K \arrow[u, hook] \arrow[r, hook] & \mathrm{Tr}(C) \arrow[u, "\otimes L"']
\end{tikzcd}$$

The codes on the top row are over L, those on the lower row over K. The following Theorem is based on Giorgetti-Previtali [8]:

Theorem 15. *Let L/K be a Galois extension. Let C be an L-linear code. Then the following statements are equivalent:*

- *C is Galois closed: $C = C^*$.*
- *C is the extension of its restriction: $C = (C|_K) \otimes L$.*
- *C has a basis over K^n.*
- *The trace of C is equal to its restriction: $\mathrm{Tr}(C) = C|_K$.*

Interpreted in the diagram above, this theorem says that the two codes at the top are the same if and only if the two codes on the bottom are the same. This leads to an interesting observation about rank metric codes.

Theorem 16. *Let $\mathbf{c} \in C$. Then the rows of the matrix $M(\mathbf{c})$ are elements of the trace code $\mathrm{Tr}(C)$ and $\mathrm{Rsupp}(C) = \mathrm{Tr}(C)$.*

Proof. The extension L/K is Galois, so in particular separable. The product defined by $\langle x, y\rangle := \mathrm{Tr}(xy)$ is a K-bilinear non-degenerate inner product on L, see [14, VII, §5, Theorem 9]. For the given K-linear basis $\alpha_1, \ldots, \alpha_m$ of L there exists a K-linear basis $\alpha'_1, \ldots, \alpha'_m$ of L such that $\langle \alpha_i, \alpha'_j\rangle = \delta_{ij}$ is the Kronecker delta function, see [14, VII, §5, Corollary 2]. So $M(\mathbf{c})$ has entries c_{ij} in K such that $c_j = \sum_{i=1}^m c_{ij}\alpha_i$, $\mathbf{c}_i = (c_{i1}, \ldots, c_{in})$ is the i-th row of $M(\mathbf{c})$ and $\mathbf{c} = \sum_{i=1}^m \mathbf{c}_i\alpha_i$. The trace map is K-linear . Hence

$$\mathrm{Tr}(\alpha'_j\mathbf{c}) = \sum_{i=1}^m \mathbf{c}_i\mathrm{Tr}(\alpha_i\alpha'_j) = \sum_{i=1}^m \mathbf{c}_i\delta_{ij} = \mathbf{c}_j.$$

Hence the rows of the matrix $M(\mathbf{c})$ are elements of the trace code $\mathrm{Tr}(C)$. So $\mathrm{Rsupp}(C) \subseteq \mathrm{Tr}(C)$, since $\mathrm{Rsupp}(C)$ is generated by the rows of $M(\mathbf{c})$.
Now we consider the converse inclusion. There exists a $\beta_1 \in L$ such that $\mathrm{Tr}(\beta_1) = 1$. Let $\beta_2, \ldots, \beta_m$ be a K-linear basis of the kernel of Tr. Then $\beta_1, \ldots, \beta_m$ is a K-linear basis of L such that $\mathrm{Tr}(\beta_i)$ is one if $i = 1$ and is zero otherwise. Without loss of generality we may assume that the matrix $M(\mathbf{c})$ is obtained with respect to this basis. So now $M(\mathbf{c})$ has entries c'_{ij} with $c_j = \sum_{i=1}^m c'_{ij}\beta_i$, $\mathbf{c}'_i = (c'_{i1}, \ldots, c'_{in})$ is the i-th row of $M(\mathbf{c})$ and $\mathbf{c} = \sum_{i=1}^m \mathbf{c}'_i\beta_i$. Hence $\mathrm{Tr}(\mathbf{c}) = \sum_{i=1}^m \mathbf{c}'_i\mathrm{Tr}(\beta_i) = \mathbf{c}'_1 \in \mathrm{Rsupp}(C)$. Therefore $\mathrm{Tr}(C) \subseteq \mathrm{Rsupp}(C)$. □

Corollary 17. *Let D be a subcode of the L-linear code C. Then* $\mathrm{Rsupp}(D) = \mathrm{Tr}(D)$ *and thus*

$$d_{R,r}(C) = \min_{\substack{D\subseteq C\\ \dim(D)=r}} \mathrm{wt}_R(D) = \min_{\substack{D\subseteq C\\ \dim(D)=r}} \dim \mathrm{Tr}(C) = \min_{\substack{D\subseteq C\\ \dim(D)=r}} \dim D^*$$

5 Equivalent definitions

We will now discuss previous definitions of the generalized Hamming weights and to what extend they are consistent with Definition 5. The definition of Oggier-Sboui in [15] is, in our notation, as follows:

Definition 18. Consider the field extension $\mathbb{F}_{q^m}/\mathbb{F}_q$. Let C be an $\mathbb{F}_{q^m}$-linear code and let $m \geq n$. Then the r-th generalized rank weight is defined as

$$\min_{\substack{D\subseteq C\\ \dim(D)=r}} \max_{\mathbf{d}\in D} \mathrm{wt}_R(\mathbf{d}).$$

Theorem 19. *Let $L = \mathbb{F}_{q^m}$ and $K = \mathbb{F}_q$. Let C be an L-linear code with $m \geq n$. Then Definitions 18 and 5 give the same values, that is,*

$$d_{R,r}(C) = \min_{\substack{D\subseteq C\\ \dim(D)=r}} \mathrm{wt}_R(D) = \min_{\substack{D\subseteq C\\ \dim(D)=r}} \max_{\mathbf{d}\in D} \mathrm{wt}_R(\mathbf{d}).$$

Proof. By Proposition 10, every subcode D contains a word of maximal rank weight. $\square$

Kurihara-Matsumoto-Uyematsu [12, 13] define the *relative generalized rank weights*, that induce the following definition of the generalized rank weights:

Definition 20. Consider the field extension $\mathbb{F}_{q^m}/\mathbb{F}_q$. Let C be an $\mathbb{F}_{q^m}$-linear code. Then the r-th generalized rank weight is defined as

$$\min_{\substack{V \subseteq L^n, V=V^* \\ \dim(C \cap V) \geq r}} \dim V.$$

Both of Definitions 18 and 20 have an obvious extension to rank metric codes over the field extension L/K. Where possible, we will show the equivalence between the definitions in as much generality as possible.
Ducoat [6] proved the following for $m \geq n$:

$$\min_{\substack{D \subseteq C \\ \dim(D)=r}} \max_{\mathbf{d} \in D^*} \mathrm{wt}_R(\mathbf{d}) = \min_{\substack{V \subseteq L^n, V=V* \\ \dim(C \cap V) \geq r}} \dim V.$$

The left hand side is almost Definition 18, but with D^* instead of D in the maximum.
The following proof is largely inspired by Ducoat; note that it works more general over L instead of $\mathbb{F}_{q^m}$:

Theorem 21. *Let L be a Galois extension of K. Let C be an L-linear code of dimension k. Let r be an integer such that $0 \leq r \leq k$. Then Definitions 20 and 5 give the same values, that is,*

$$\min_{\substack{V \subseteq L^n, V=V^* \\ \dim(C \cap V) \geq r}} \dim V = \min_{\substack{D \subseteq C \\ \dim D=r}} \dim D^*.$$

Proof. Let V a Galois closed subspace of L^n such that $\dim(C \cap V) \geq r$. (Such a V always exists, since C^* is such a subspace and $r \leq k$.) Let $D \subseteq C \cap V$ with $\dim D = r$. Since V is Galois closed and $D \subseteq V$, we have $D^* \subseteq V$. So D^* is a subspace of smaller dimension than V^* with $\dim(C \cap D^*) \geq r$. On the other hand, for all $D \subseteq C$ with $\dim D = r$, we have that $\dim(C \cap D^*) \geq r$. So the formula follows. $\square$

We will now continue to prove the equivalence of Definition 5 and the variation of Definition 18 that was used by Ducoat [6]. This requires some propositions. For the rest of this section, let L/K be a cyclic Galois extension of degree m — we make this assumption so we can use the results in [2]. Enumerate the elements of the Galois group as θ_i and let $\mathbf{x}^{[i]} = \mathbf{x}^{\theta_i}$ be the (component-wise) action of the Galois group.

Proposition 22. *Let L be a cyclic Galois extension of K. For any $\mathbf{x} \in L^n$ we have*

$$\langle \mathbf{x} \rangle^* = \mathrm{Rsupp}(\mathbf{x}) \otimes L.$$

Proof. First we note that $\langle \mathbf{x} \rangle^* = \langle \mathbf{x}, \mathbf{x}^{[1]}, \ldots, \mathbf{x}^{[m-1]} \rangle$. We prove equality by proving two inclusions. Let $(\alpha_1, \ldots, \alpha_m)$ a basis of L of K and write $\mathbf{x} = \alpha_1 \mathbf{x}_1 + \ldots + \alpha_m \mathbf{x}_m$. This means the $\mathbf{x}_i$ are the rows of $M(\mathbf{x})$. We have that

$$\mathbf{x}^{[i]} = (\alpha_1 \mathbf{x}_1 + \ldots + \alpha_m \mathbf{x}_m)^{[i]} = \alpha_1^{[i]} \mathbf{x}_1 + \ldots + \alpha_m^{[i]} \mathbf{x}_m$$

and $\alpha_j^{[i]} \in L$, so $\mathbf{x}^{[i]} \in \langle \mathbf{x}_1, \ldots, \mathbf{x}_m \rangle \otimes L$ and thus $\langle \mathbf{x} \rangle^* \subseteq \mathrm{Rsupp}(\mathbf{x}) \otimes L$.
For the reverse inclusion we may assume without loss of generality after a permutation of coordinates that the first l columns of $M(\mathbf{x})$ are independent, where l is the rank of $M(\mathbf{x})$, and moreover that $M(\mathbf{x})$ is in reduced row echelon form. Hence $\mathbf{x} = \alpha_1 \mathbf{x}_1 + \ldots + \alpha_l \mathbf{x}_l$ and $\mathbf{x}_j = \mathbf{0}$ for all $l < j \leq m$. Then

$$\mathbf{x}^{[i]} = \alpha_1^{[i]} \mathbf{x}_1 + \ldots + \alpha_l^{[i]} \mathbf{x}_l \quad \text{for all} \quad i = 0, \ldots, l-1.$$

(This holds in fact for $i = 0, \ldots, m-1$, but we only need it up to $i = l-1$.)
The "Vandermonde" matrix with entries $\alpha_j^{[i-1]}$, $1 \leq i, j \leq l$ is invertible by [2, Theorem 3], since the $\alpha_1, \ldots, \alpha_l$ are independent over K. So $\mathbf{x}_j \in \langle \mathbf{x}^{[0]}, \ldots \mathbf{x}^{[l-1]} \rangle \subseteq \langle \mathbf{x} \rangle^*$. Therefore $\mathrm{Rsupp}(\mathbf{x}) \otimes L \subseteq \langle \mathbf{x} \rangle^*$ and we conclude that $\langle \mathbf{x} \rangle^* = \mathrm{Rsupp}(\mathbf{x}) \otimes L$. □

From this Proposition, the following Lemmas follows directly. They are a generalization of I.1 and II.2 of Ducoat [6].

Lemma 23. *Let L be a cyclic Galois extension of K. For any $\mathbf{x} \in L^n$ we have*

$$\dim(\langle \mathbf{x} \rangle^*) = \mathrm{rk}(M(\mathbf{x})).$$

Lemma 24. *Let L be a cyclic Galois extension of K. For all Galois closed sets V of dimension $n \leq m$ there is an $\mathbf{x} \in V$ such that $V = \langle \mathbf{x} \rangle^*$.*

Proof. Pick a basis for V and let these be rows of $M(\mathbf{x})$. Add extra zero rows. □

The first Lemma originally had the assumption $m \geq n$, but this can be dropped. In the second Lemma we can not do that: the number of basis vectors for $\langle \mathbf{x} \rangle^*$ is equal to the extension degree m, so we can never have $V = \langle \mathbf{x} \rangle^*$ if $\dim V > m$. (See also Example 12.)
We now show the equivalence between Definitions 18 and the variation of 5 as used before.

Theorem 25. *Let L be a cyclic Galois extension of K of degree m. Let C be an L-linear code in L^n with $m \geq n$. Then*

$$\max_{\mathbf{d} \in D^*} \mathrm{rk}(M(\mathbf{d})) = \dim D^*$$

Proof. Because D^* is Galois closed, there is a $\mathbf{d} \in D^*$ such that $D^* = \langle \mathbf{d} \rangle^*$. We also have $\dim(\langle \mathbf{d} \rangle^*) = \mathrm{rk}(M(\mathbf{d}))$, so $\mathrm{rk}(M(\mathbf{d})) = \dim D^*$ and indeed

$$\max_{\mathbf{d} \in D^*} \mathrm{rk}(M(\mathbf{d})) = \dim D^*.$$

□

6 Degenerate codes

As a small application of the generalized rank weights, we discuss the concept of *degenerate* codes. A code C is called degenerate with respect to the Hamming metric in case there is a coordinate such that all codewords are zero at that position. This is equivalent with saying that the Hamming minimum distance of $C^\perp$ is one.

Definition 26. The code C is called degenerate with respect to the rank metric if $d_R(C^\perp) = 1$.

The dual code here is defined as the orthogonal subspace of C in L^n. We give some characteristics of (non)degenerate codes.

Proposition 27. *The code C is degenerate with respect to the rank metric if and only C is rank equivalent with a code such that all its codewords are zero at the last position.*

Proof. Suppose that $d_R(C^\perp) = 1$. Then there is a $\mathbf{h} \in C^\perp$ such that $M_B(\mathbf{h})$ has rank 1. After dividing by the first element of the basis B we may assume that the first element of B is equal to 1. After a change of the basis B we may assume that only the first row of $M_B(\mathbf{h})$ has nonzero entries. Hence $\mathbf{h} \in K^n$, since the first element of B is equal to 1. We can take this $\mathbf{h}$ as the first row of the parity check matrix of C. After a coordinate change of L^n with entries in K, that is a rank isometry, we may assume that we get a rank equivalent code with $\mathbf{h} = (0, \ldots, 0, 1)$. Therefore C is rank equivalent with a code such that all its codewords are zero at the last position.
Clearly the converse also holds. □

Corollary 28. *Let C be an L-linear code of length n and dimension k. Then C is nondegenerate with respect to the rank metric if and only if* $\mathrm{Rsupp}(C) = K^n$ *if and only if* $d_{R,k}(C) = n$.

Proof. Suppose that $\mathrm{Rsupp}(C) \neq K^n$. Then there is a coordinate transformation with entries in K such that $\mathrm{Rsupp}(C) \subseteq K^{n-1} \times \{0\}$. Hence C is degenerate with respect to the rank metric by Proposition 27. Clearly the converse also holds.
The last equivalence follows from the definition of $d_{R,k}(C)$. □

An alternative proof of this theorem uses the following result on duality by Ducoat [6, Theorem I.3]:

Theorem 29. *Let C be an L-linear code with dual $C^\perp$. Then the generalized rank weights of C and $C^\perp$ are related as follows:*

$$\{d_{r,R}(C) \mid 1 \leq r \leq k\} = \{1, \ldots, n\} \setminus \{n + 1 - d_{r,R}(C^\perp) \mid 1 \leq r \leq n - k\}.$$

Alternative proof of Corollary 28. If d is a generalized rank weight of C, then $n + 1 - d$ is not a generalized rak weight of $C^\perp$. So if $d_{R,1}(C^\perp) = 1$, then $n+1-1 = n$ can not be a generalized rank weight of C, so $d_{R,k}(C) < n$. □

Corollary 30. *Let L be an extension of K of degree m. Let C be an L-linear code of length n and dimension k that is nondegenerate with respect to the rank metric. Then $km \geq n$.*

Proof. Let $\mathbf{g}_1, \ldots, \mathbf{g}_k$ be a basis of C. Then $\mathrm{Rsupp}(C)$ is generated by the spaces $\mathrm{Rsupp}(\mathbf{g}_i)$ for $i = 1, \ldots, k$ by Proposition 3. The dimension of $\mathrm{Rsupp}(\mathbf{g}_i)$ is at most m. Hence the dimension of $\mathrm{Rsupp}(C)$ is at most km by Proposition 3. If C is nondegenerate, then $\mathrm{Rsupp}(C) = K^n$ by Corollary 28. Therefore $km \geq n$. □

7 Conclusion

This paper introduced a new definition for the generalized rank weights. This definition is induced by the study of the generalized rank weight enumerator [10]. We investigated the relation between the rank support and the trace code. The fact that the proposed definition of the generalized rank weight enumerator induces a definition of the generalized rank weights that is equivalent to a known definition, supports the definition of the generalized rank weight enumerator.

We showed that our definition is equivalent to that of Kurihara-Matsumoto-Uyematsu [12, 13], even if we extend this definition to codes over arbitrary fields. We also show that our definition of the generalized rank weight is equivalent to the definition of Oggier-Sboui [15]: here we have to assume

$m \geq n$ and that the Galois group of L/K is cyclic.
The fact that the proposed definition of the generalized rank weight enumerator induces a definition of the generalized rank weights that is equivalent to a known definition, supports the definition of the generalized rank weight enumerator.
We believe that the fact that we were able to prove equivalence to the definition of Kurihara-Matsumoto-Uyematsu but only partial equivalence to the definition of Oggier-Sboui, supports the definition of the generalized rank weights of Kurihara-Matsumoto-Uyematsu in favor of the definition of Oggier-Sboui. A similar conclusion can be drawn from the work of Ducoat [6], who proves duality relations for the generalized rank weights.

As an application of the notion of generalized rank weights, we discussed codes that are degenerate with respect to the rank metric.

As further work, we propose to study our definition for Delsarte codes [5, 16]: these are rank metric codes that are linear subspaces of $K^{m\times n}$ that do not necessarily come from a code over L. Our definition, contrary to that of Kurihara-Matsumoto-Uyematsu, is directly applicable to such codes.

8 Acknowledgement

The first author is partially supported by grant GOA62 of the Vrije Universiteit Brussel, Belgium. The second author is indebted to the Aalborg University for a stay during which this research could be finished and that was supported by the Danish Council for Independent Research (Grant No. DFF 4002-00367).

References

[1] D. Augot. Generalization of Gabidulin codes over rational function fields. In *MTNS-2014, 21st International Syposium on Mathematical Theory of Networks and Systems, arxiv:1412.6080v1.pdf*, 2014.

[2] D. Augot, P. Loidreau, and G. Robert. Rank metric and Gabidulin codes in characteristic zero. In *IEEE ISIT-2013, International Syposium on Information Theory*, pages 509–513, 2013.

[3] T.P. Berger. Isometries for rank distance and permutation group of Gabidulin codes. In *Proc. 8th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCTí8)*, pages 30–33, 2002.

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

[5] Ph. Delsarte. Bilinear forms over a finite field, with applications to coding theory. *J. Combin. Theory Ser. A*, 25(3):226–241, 1978.

[6] J. Ducoat. Generalized rank weights: a duality statement. In G. Kyureghyan, G. L. Mullen, and A. Pott, editors, *Topics in Finite Fields*, volume 632 of *Contemporary Mathematics*, pages 101–109. American Mathematical Society, 2015.

[7] È. M. Gabidulin. Theory of codes with maximum rank distance. *Problemy Peredachi Informatsii*, 21(1):3–16, 1985.

[8] M. Giorgetti and A. Previtali. Galois invariance, trace codes and subfield subcodes. *Finite Fields and Their Applications*, 16:96–99, 2010.

[9] R.P.M.J. Jurrius and R. Pellikaan. Codes, arrangements and matroids. In E. Martínez-Moro, editor, *Algebraic Geometry Modeling in Information Theory*, volume 8 of *Series on Coding Theory and Cryptology*, pages 219–325. World Scientific, New Jersey, 2013.

[10] R.P.M.J. Jurrius and R. Pellikaan. The extended and generalized rank weight enumerator. In *Proc. ACA 2014, Applications of Computer Algebra, CACTC@ACA Computer Algebra in Coding Theory and Cryptography, Fordham University, New York*, 2014.

[11] G.L. Katsman and M.A. Tsfasman. Spectra of algebraic-geometric codes. *Problemy Peredachi Informatsii*, 23:19–34, 1987.

[12] J. Kurihara, R. Matsumoto, and T. Uyematsu. New parameters of linear codes expressing security performance of universal secure network coding. In *Communication, Control, and Computing (Allerton), 2012 50th Annual Allerton Conference*, pages 533–540, 2012.

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

[14] S. Lang. *Algebra*. Addison-Wesley Publishing Co., Inc., Reading, Mass., 1965.

[15] F. Oggier and A. Sboui. On the existence of generalized rank weights. In *IEEE ISIT-2012, International Symposium on Information Theory*, pages 406–410, 2012.

[16] A. Ravagnani. Generalized weights: an anticode approach. *CoRR*, abs/1410.7207, 2014.