On defining generalized rank weights

Relinde Jurrius[1], Ruud Pellikaan[2]

[1] *Institut de Mathémathiques, Université de Neuchátel. E-mail: relinde.jurrius@unine.ch*
[2] *Dept. of Mathematics, Eindhoven University of Technology. E-mail: g.r.pellikaan@tue.nl*

1 Introduction

Error-correcting codes with the rank distance were introduced by Gabidulin [4]. 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 [6]. From this theory, a definition of the generalized rank weights follows. These are the rank metric equivalence of the generalized Hamming weights.

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 [4] to arbitrary characteristic as considered by Augot-Loidreau-Robert [1, 2].

We show equivalence to previous definitions, in particular the ones by Kurihara-Matsumoto-Uyematsu [8, 9], Oggier-Sboui [10] and Ducoat [3].

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 $B = \{\alpha_1, \dots, \alpha_m\}$ of L as a vector space over K. Let $\mathbf{c} = (c_1, \dots, c_n) \in L^n$. 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 [4, 1].

The following is from [6, 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 $\mathrm{Rsupp}(D)$.

Definition 2. 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.

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 [8, 9]. An alternative was given by Oggier-Sboui [10] and Ducoat [3]. Both definitions were motivated by applications.

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 $\mathrm{supp}(C) = \{j | c_j \neq 0 \text{ for some } \mathbf{c} \in C\}$. The subcode $C(J)$ is defined in [7] and [5, Definition 5.1] for a subset J of $\{1,\dots,n\}$ 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 $j \in \{1,\dots,n\}$. Let $J = \mathrm{supp}(C)$. Then $C(j)$ has codimension one in C for all $j \in J$.

For the definition of $C(J)$ in the context of the rank metric we give the following analogous definition as given in [6, Definition 2].

Definition 3. 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 4. *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.*

Proposition 5. *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

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

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 6. 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 code* $C \otimes L$ as the subspace of L^n formed by taking all L-linear combinations of words of C.

Theorem 7. *Let $\mathbf{c} \in C$. Then the rows of the matrix $M(\mathbf{c})$ are elements of the trace code $\mathrm{Tr}(C)$ and*

$$\mathrm{Rsupp}(C) = \mathrm{Tr}(C)$$

.

Corollary 8. *Let D be a subcode of the L-linear code C. Then*

$$\mathrm{Rsupp}(D) = \mathrm{Tr}(D) \quad \textit{and thus}$$

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

5 Equivalent definitions

We will now discuss previous definitions of the generalized Hamming weights and to what extend they are consistent with Definition 2. The definition of Oggier-Sboui in [10] is, in our notation, as follows:

Definition 9. 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

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

Note that this definition is equivalent to Definition 2, since a subcode D contains a word of maximal rank weight by Proposition 5. Kurihara-Matsumoto-Uyematsu [8, 9] define the *relative generalized rank weights*, that induce the following definition of the generalized rank weights:

Definition 10. 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 9 and 10 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 [3] 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 9, but with D^* instead of D in the maximum. The proof of the following theorem is largely inspired by Ducoat; note that it works more general over L instead of $\mathbb{F}_{q^m}$:

Theorem 11. *Let L be a Galois extension of K. Let C be an L-linear code. Then Definitions 10 and 2 give the same values, that is,*

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

We now state the equivalence between Definitions 9 and the variation of 2 as used before.

Theorem 12. *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*

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

References

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

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

[3] J. Ducoat, *Generalized rank weights: a duality statement*, arXiv:1306.3899v2, 2014.

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

[5] R.P.M.J. Jurrius and R. Pellikaan, *Codes, arrangements and matroids*, Series on Coding Theory and Cryptology **8**, World Scientific, Algebraic Geometry Modeling in Information Theory, E. Martínez-Moro (ed.), pp. 219–325 (2013).

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

[7] K.L. Katsman and M.A. Tsfasman, *Spectra of algebraic-geometric codes*, Problemy Peredachi Informatsii **23**, pp. 19–34 (1987).

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

[9] J. Kurihara, R. Matsumoto T. and Uyematsu, *Relative generalized rank weight of linear codes and its applications to network coding*, arXiv:1301.5482v1, 2013.

[10] F. Oggier, F. and A. Sboui, *On the existence of generalized rank weights*, IEEE ISIT-2012, International Syposium on Information Theory, pp. 406–410 (2012).