

# The extended and generalized rank weight enumerator of a code

Relinde Jurrius  
Free University of Brussels

Ruud Pellikaan  
Eindhoven University of Technology

`g.r.pellikaan@tue.nl`

## Abstract

This paper investigates the rank weight enumerator of a code 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 use the notion of counting polynomials, to define the (extended) rank weight enumerator, since in this generality the set of codewords of a given rank weight is no longer finite. Also the extended and generalized rank weight enumerator are studied in analogy with previous work on codes with respect to the Hamming metric.

## Keywords

Rank weight enumerator,  $r$ -the generalized rank weight

## 1 Introduction

In previous work [7, 8] the weight enumerator  $W_C(X, Y)$  of a code  $C$  over a finite field  $\mathbb{F}_q$  with respect to the Hamming distance was generalized to the extended weight enumerator  $W_C(X, Y, T)$  for arbitrary fields, such that  $W_C(X, Y, q^m) = W_{C \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m}}(X, Y)$  for a code  $C$  over  $\mathbb{F}_q$  and its extension  $C \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m}$  over  $\mathbb{F}_{q^m}$ . Also the  $r$ -th generalized weight enumerator  $W_C^{(r)}(X, Y)$  was considered and it was shown that it is determined by the extended weight enumerator, and conversely that the collection of  $W_C^{(r)}(X, Y)$  for  $r = 1, \dots, k$ , where  $k$  is the dimension of  $C$ , determine  $W_C(X, Y, T)$ . Furthermore MacWilliams identities were proved both for  $W_C(X, Y, T)$  and  $W_C^{(r)}(X, Y)$ .

This paper investigates the rank weight enumerator of a code over  $L$ , where  $L$  is a finite field 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 [2, 1].

The notion of counting polynomials [12, 13, 14] is used to define the (extended) rank weight enumerator  $W_C^R(X, Y, T)$  for a  $\mathbb{F}_{q^m}$ -linear code  $C$  with respect to the rank distance, since in this generality the set of codewords of a given rank weight is no longer finite. Also, the  $r$ -th generalized rank weight enumerator  $W_C^{R,r}(X, Y)$  is defined. It is shown that it is determined by the extended rank weight enumerator, and conversely that the collection of  $W_C^{R,r}(X, Y)$  for  $r = 1, \dots, k$  determines  $W_C^R(X, Y, T)$ . Finally MacWilliams identities are proved both for  $W_C^R(X, Y, T)$  and  $W_C^{R,r}(X, Y)$  as a generalization of the work of Gadouleau-Yan [5] and Gluesing [6].

Let  $K$  be a field and let  $L$  be a finite Galois extension of  $K$ . Choose a basis  $\alpha_1, \dots, \alpha_m$  of  $L$  as a vector space over  $K$ . If  $C$  is an  $L$ -linear code of length  $n$ , that is an  $L$ -linear subspace of  $L^n$ , then with the element  $\mathbf{c} = (c_1, \dots, c_n)$  of  $C$  an  $m \times n$  matrix  $M(\mathbf{c})$  is associated where the  $j$ -th column of  $M(\mathbf{c})$  consists of the coordinates of  $c_j$  with respect to the chosen basis:  $c_j = \sum_{i=1}^m c_{ij} \alpha_i$ . So  $M(\mathbf{c})$  has entries  $c_{ij}$ . The rank weight  $\text{wt}_R(\mathbf{c}) = \text{rk}(\mathbf{c})$  of  $\mathbf{c}$  is by definition the rank of the matrix  $M(\mathbf{c})$ . The rank distance is defined by  $d_R(\mathbf{x}, \mathbf{y}) = \text{rk}(\mathbf{x} - \mathbf{y})$ . This defines a metric on the collection of all  $m \times n$  matrices. The rank distance of the code is  $d_R(C) = \min\{\text{rk}(\mathbf{c}) : \mathbf{c} \in C, \mathbf{c} \neq 0\}$ .

One can view the theory of rank metric codes as a  $q$ -analogue for a finite field  $\mathbb{F}_q$ , and more generally as the  $T$ -analogue where  $T$  is a variable for an arbitrary field  $K$ , of the theory of codes with the Hamming metric. The  $q$ -analogue in combinatorics is often a generalization of a concept or expression involving a new parameter  $q$  that returns to the original concept or expression as  $q \rightarrow 1$ . For instance the  $q$ -analogue of a finite set of  $n$  elements is the vector space  $\mathbb{F}_q^n$ .

The basis of  $q$ -analogues is the  $q$ -analogue of a number, defined by  $[n]_q = \frac{q^n - 1}{q - 1}$ , or more generally  $[n]_T = \frac{T^n - 1}{T - 1}$ . The  $T$ -analogue of a finite set is a finite vector space. We list the  $T$ -analogues of some operations on subsets:

subsets of $\{1, \dots, n\}$	subspaces of $K^n$
$\emptyset$	$\{0\}$
intersection	intersection
union	sum
complement	orthoplement
size	dimension

Furthermore, the Newton binomial  $\binom{n}{k}$  counts the number of subsets of  $\{1, \dots, n\}$  of size  $k$ . So the  $q$ -analogue is given by the Gaussian binomial, or  $q$ -binomial  $\begin{bmatrix} n \\ k \end{bmatrix}_q$  which counts the number of subspaces of  $\mathbb{F}_q^n$  of dimension  $k$ . More generally the  $T$ -analogue is the  $T$ -binomial

$$\begin{bmatrix} n \\ k \end{bmatrix}_T = \frac{(T^n - 1) \cdots (T^{n-k+1} - 1)}{(T - 1) \cdots (T^k - 1)}$$

which is a polynomial in  $T$  and can be considered as the counting polynomial [12, 13, 14] of the Grassmann variety of  $k$ -dimensional subspaces of an  $n$  dimensional vector space.

The translation is not always unambiguous. Since for subsets  $x$  and  $y$  the condition  $x \cap y = \emptyset$  would translate in this way into  $x \cap y = \{0\}$  for subspaces  $x$  and  $y$ . But the condition  $x \cap y = \emptyset$  for subsets  $x$  and  $y$ , is equivalent to  $x \subseteq y^c$ , the complement of  $y$  and this would translate into  $x \subseteq y^\perp$ , the orthoplement for subspaces  $x$  and  $y$ . Here the orthoplement or dual  $x^\perp$  of a subspace  $x$  of  $K^n$  is defined by  $x^\perp = \{\mathbf{b} \in K^n : \mathbf{a} \cdot \mathbf{b} = 0 \text{ for all } \mathbf{a} \in x\}$  with respect the standard inner product  $\mathbf{a} \cdot \mathbf{b} = \sum_{i=1}^n a_i b_i$  for vectors  $\mathbf{a}, \mathbf{b} \in K$ .

The interpretation of the extended and generalized rank weight enumerator in terms of the Tutte polynomial needs the generalization of the notion of a  $q$ -matroid and more generally of a  $K$ -matroid and their corresponding  $q$ -Tutte and  $K$ -Tutte polynomials, respectively. This will be pursued in a subsequent paper.

## 2 Some codes related to $C$

The previous mentioned translation gives for instance the following. The support of a vector  $\mathbf{c} \in K^n$  is defined by  $\text{supp}(\mathbf{c}) = \{j : c_j \neq 0\}$  and the Hamming weight of this vector is  $\text{wt}_H(\mathbf{c}) = |\text{supp}(\mathbf{c})|$ . Let  $C$  be a  $K$ -linear code of length  $n$ . Then the minimum Hamming distance  $d_H(C)$  is given by the minimum of  $\text{wt}_H(\mathbf{c})$  for all nonzero  $\mathbf{c} \in C$ . Let  $J$  be a subset of  $\{1, \dots, n\}$  with complement  $J^c$ . Then the subcode  $C(J)$  is defined in [9] and [8, Definition 5.1] by

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

Analogously the following definitions are given.

**Definition 1.** Let  $C$  be an  $L$ -linear code of length  $n$ . Let  $\mathbf{c} \in C$ . Let  $J$  be a  $K$ -linear subspace of  $K^n$ . Then  $\text{Rsupp}(\mathbf{c})$ , the *rank support* of  $\mathbf{c}$  is by definition the row space of  $M(\mathbf{c})$ . The *rank weight* of  $\mathbf{c}$  is  $\text{wt}_R(\mathbf{c}) = \dim(\text{Rsupp}(\mathbf{c}))$ .

**Definition 2.** For a  $K$ -linear subspace  $J$  of  $K^n$  we define:

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

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 3.** 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  $\mathbf{c} \cdot \mathbf{y}$  for all  $\mathbf{y} \in J$ . Furthermore  $C(J)$  is an  $L$ -linear subspace of  $C$ .

**Definition 4.** Let  $C$  be an  $L$ -linear code of length  $n$ . Let  $J$  be a  $K$ -linear subspace of  $K^n$  of dimension  $t$  with generator matrix  $Y$ . Define the map  $\pi_J : L^n \rightarrow L^t$  by  $\pi_J(\mathbf{x}) = \mathbf{x}Y^T$ , and  $C_J = \pi_J(C)$ .

**Lemma 5.** Let  $C$  be an  $L$ -linear code of length  $n$ . Let  $J$  be a  $K$ -linear subspace of  $K^n$  of dimension  $t$  with generator matrix  $Y$ . Then  $\pi_J$  is an  $L$ -linear map and  $C_J$  is an  $L$ -linear code of length  $t$  and its dimension does not depend on the chosen generator matrix. Furthermore we have an exact sequence of vector spaces:

$$0 \longrightarrow C(J) \longrightarrow C \longrightarrow C_J \longrightarrow 0.$$

**Definition 6.** Let  $C$  be an  $L$ -linear code of length  $n$ . Let  $J$  be a  $K$ -linear subspace of  $K^n$  of dimension  $t$ . Define  $l(J) = \dim_L C(J)$  and  $r(J) = \dim_L C_J$ .

The following corollary is the analogon of [8, Lemma 5.1].

**Corollary 7.** Let  $C$  be an  $L$ -linear code of length  $n$  and dimension  $k$ . Let  $J$  be a  $K$ -linear subspace of  $K^n$ . Then  $l(J) + r(J) = k$ .

The following lemma is the analogon of [8, Lemma 5.2].

**Lemma 8.** Let  $C$  be an  $L$ -linear code of length  $n$ . Let  $d_R$  and  $d_R^\perp$  be the minimum rank distance of  $C$  and  $C^\perp$ , respectively. Let  $J$  be a  $K$ -linear subspace of  $K^n$  of dimension  $t$ . Let  $l(J) = \dim_L C(J)$ . Then

$$l(J) = \begin{cases} k - t & \text{for all } t < d_R^\perp \\ 0 & \text{for all } t > n - d_R \end{cases}$$

### 3 Extended rank weight enumerator

Let  $K$  be a field and  $L$  a finite field extension of degree  $m$ . Let  $\nu$  be the counting polynomial in the variable  $T$  with respect to the field  $K$ .

**Definition 9.** Let  $C$  be an  $L$ -linear code of length  $n$ . Let  $\mathcal{A}_w^R = \{\mathbf{c} \in C : \text{wt}_R(\mathbf{c}) = w\}$  and  $A_w^R(T) = \nu(\mathcal{A}_w^R)$ . The (extended) rank weight enumerator is given by

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

**Definition 10.** Let  $C$  be an  $L$ -linear code of length  $n$ . Let  $\mathcal{B}_J^R = C(J)$  for a subspace  $J$  of  $K^n$ . Let

$$\begin{aligned} \mathcal{B}_t^R &= \{(J, \mathbf{c}) : J \subseteq K^n \text{ subspace of dimension } t, \mathbf{c} \in C(J)\}, \\ \mathcal{B}_{t,l}^R &= \{J : J \subseteq K^n \text{ subspace of dimension } t, l(J) = l\}. \end{aligned}$$

Let  $B_J^R(T)$ ,  $B_t^R(T)$  and  $B_{t,l}^R(T)$  be the counting polynomials of  $\mathcal{B}_J^R$ ,  $\mathcal{B}_t^R$  and  $\mathcal{B}_{t,l}^R$ , respectively.

**Remark 11.** The dimension of  $C(J)$  over  $L$  is  $l(J)$  by definition, so it has dimension  $m \cdot l(J)$  over  $K$ . If  $C$  has dimension  $k$  over  $L$  and the subspace  $J$  of  $K^n$  has dimension  $t$ , then  $k - t \leq l(J) \leq k$ , since  $k - l(J) = r(J) \leq \dim(J)$  by Corollary 7. Hence  $\mathcal{B}_t^R$  is the disjoint union of the  $\mathcal{B}_{t,l}^R$  for  $l \leq k - t$ . Therefore

$$\begin{aligned} B_J^R(T) &= T^{m \cdot l(J)} \\ B_t^R(T) &= \sum_{l=k-t}^k B_{t,l}^R(T) T^{ml} \end{aligned}$$

The following proposition is the analogon of [8, Proposition 5.21].

**Proposition 12.** Let  $C$  be an  $L$ -linear code of length  $n$ . Let  $d_R$  and  $d_R^\perp$  be the minimum rank distance of  $C$  and  $C^\perp$ , respectively. Then

$$B_t^R(T) = \begin{cases} \begin{bmatrix} n \\ t \end{bmatrix}_T \cdot T^{m(k-t)} & \text{for all } t < d^\perp \\ \begin{bmatrix} n \\ t \end{bmatrix}_T & \text{for all } t > n - d \end{cases}$$

*Proof.* If  $t < d^\perp$  or  $t > n - d$ , then  $l(J)$  is constant and equal to  $k - t$  and 0, respectively for all subspaces  $J$  of dimension  $t$  by Lemma 8. The Grassmannian of all subspaces of  $K^n$  of dimension  $t$  has counting polynomial  $\begin{bmatrix} n \\ t \end{bmatrix}_T$ . So the Proposition follows now from Remark 11.  $\square$

The relation between  $B_t^R(T)$  and  $A_w^R(T)$  becomes clear in the next proposition.

**Proposition 13.** *The following formula holds:*

$$B_t^R(T) = \sum_{w=0}^n \begin{bmatrix} n-w \\ t \end{bmatrix}_T A_w^R(T).$$

**Proposition 14.** *The following formula holds:*

$$A_w^R(T) = \sum_{t=n-w}^n (-1)^{t-n+w} T^{\binom{t-n+w}{2}} \begin{bmatrix} t \\ n-w \end{bmatrix}_T B_t^R(T)$$

**Theorem 15.** *The following formula holds:*

$$W_C^R(X, Y, T) = \sum_{t=0}^n \left( B_t^R(T) \prod_{j=0}^{t-1} (X - T^j Y) \right) Y^{n-t}$$

The following proposition is the analogon of [8, Proposition 5.24].

**Proposition 16.** *The following formula holds:*

$$W_C^R(X, Y, T) = \sum_{t=0}^n \left( \sum_{l=k-t}^k B_{t,l}^R(T) T^{ml} \prod_{j=0}^{t-1} (X - T^j Y) \right) Y^{n-t}$$

*Proof.* Follows directly from Theorem 15 and the definition of  $B_t^R(T)$ . □

## 4 Generalized rank weight enumerator

From now on we assume that  $K$  is a finite field. So  $L/K$  is a cyclic Galois extension. The first proposal of a definition of the  $r$ -th generalized rank weight was given by Oggier-Sboui [11]. An alternative was given by Kurihara-Matsumoto-Uyematsu [10]. Ducoat [3] proved that a refinement of the first definition is equivalent to the second definition. We will prove that the refinement can be dropped: the definitions in [10] and [11] are equivalent. They are furthermore equivalent to the following definition, that also holds for general fields  $K$  and  $L$ :

**Definition 17.** Let  $C$  be an  $L$ -linear code. Let  $D$  be an  $L$ -linear subcode of  $C$ . Then  $\text{Rsupp}(D)$ , the *rank support* of  $D$  is by definition the  $K$ -linear space generated by the  $\text{Rsupp}(\mathbf{d})$  with  $\mathbf{d} \in D$ . Then  $\text{wt}_R(D)$ , the *rank support weight* of  $D$  is by definition the dimension of  $\text{Rsupp}(D)$ .

**Proposition 18.** *Let  $C$  be an  $L$ -linear code and  $D$  a subcode. Then  $\text{Rsupp}(D) = \text{Tr}(D)$ .*

**Definition 19.** 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  $r$ .

Similar definitions and results will be given for the (extended) generalized rank weight enumerator as given in the previous section for the rank weight enumerator.

## 5 MacWilliam's identities

The MacWilliams identities for the rank weight enumerator was obtained by Gadouleau-Yan [5] and Gluesing [6]. This will be given for the extended (generalized) rank weight enumerator.

## 6 Acknowledgement

The first author is supported by VUB-grant GOA62 and the second author thanks Daniel Augot and the Project Grace of INRIA Saclay-Île-de-France et Laboratoire d'Informatique de l'École Polytechnique (LIX) at Palaiseau for their hospitality, the valuable discussions and the opportunity to work on this paper.

## References

- [1] D. Augot. Generalization of Gabidulin codes over rational function fields. In *MTNS-2014, 21st International Symposium on Mathematical Theory of Networks and Systems*, 2014.
- [2] D. Augot, P. Loidreau, and G. Robert. Rank metric and Gabidulin codes in characteristic zero. In *IEEE ISIT-2013, International Symposium on Information Theory*, pages 509–513, 2013.
- [3] J. Ducoat. Generalized rank weights : duality and Griesmer bound. *CoRR*, arXiv:1306.3899v2, 2013.
- [4] È. M. Gabidulin. Theory of codes with maximum rank distance. *Problemy Peredachi Informatsii*, 21(1):3–16, 1985.
- [5] M. Gadouleau and Z. Yan. MacWilliams identity for codes with the rank metric. *EURASIP Journ. Wireless Communications and Networking*, 2008.
- [6] H. Gluesing-Luerssen. Fourier-reflexive partitions and MacWilliams identities for additive codes. *CoRR*, arXiv:1304.1207v1, 2013.
- [7] R.P.M.J. Jurrius. *Codes, arrangements, matroids and their polynomial links*. PhD thesis, Technical University Eindhoven, 2012.
- [8] 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.
- [9] G.L. Katsman and M.A. Tsfasman. Spectra of algebraic-geometric codes. *Problemy Peredachi Informatsii*, 23:19–34, 1987.
- [10] J. Kurihara, R. Matsumoto, and T. Uyematsu. Relative generalized rank weight of linear codes and its applications to network coding. *CoRR*, arXiv:1301.5482v1, 2013.
- [11] F. Oggier and A. Sboui. On the existence of generalized rank weights. In *ISIT-2012 Proceedings*, pages 4066–410, 2012.
- [12] W. Plesken. Counting solutions of polynomial systems via iterated fibrations. *Arch. Math.*, 92(1):44–56, 2009.
- [13] W. Plesken. Gauss-Bruhat decomposition as an example of Thomas decomposition. *Arch. Math.*, 92(2):111–118, 2009.
- [14] W. Plesken and T. Bächler. Counting polynomials for linear codes, hyperplane arrangements, and matroids. *Documenta Mathematica*, 19:285–312, 2014.