

MacWilliams Identity for the Rank Metric

Maximilien Gadouleau and Zhiyuan Yan
 Department of Electrical and Computer Engineering
 Lehigh University, PA 18015, USA
 E-mails: {magc, yan}@lehigh.edu

Abstract—This paper investigates the relationship between the rank weight distribution of a linear code and that of its dual code. The main result of this paper is that, similar to the MacWilliams identity for the Hamming metric, the rank weight distribution of any linear code can be expressed as an analytical expression of that of its dual code. Remarkably, our new identity has a similar form to the MacWilliams identity for the Hamming metric. Our new identity provides a significant analytical tool to the rank weight distribution analysis of linear codes. We use a linear space based approach in the proof for our new identity, and adapt this approach to provide an alternative proof of the MacWilliams identity for the Hamming metric. Finally, we determine the relationship between moments of the rank distribution of a linear code and those of its dual code, and provide an alternative derivation of the rank weight distribution of maximum rank distance codes.

I. INTRODUCTION

The rank metric has attracted some attention due to its relevance to wireless communications [1], [2], public-key cryptosystems [3], and storage equipments (see, for example, [4]). Due to these applications, there is a steady stream of work that focus on general properties of codes with the rank metric [4]–[14]. Despite these works, many open problems remain for rank metric codes. For example, it is unknown how to derive the rank weight distribution for any given linear code except when the code is a maximum rank distance (MRD) code [5]. Besides the minimum rank distance, the rank weight distribution is an important property of any rank metric code, and determines its error performance in applications.

In this paper, we investigate the rank weight properties of linear codes. The main result of this paper is that, similar to the MacWilliams identity for the Hamming metric, the rank weight distribution of any linear code can be expressed as an analytical expression of that of its dual code. Our new identity is a significant analytical tool for both rank weight distribution and hence error performance analysis of linear codes. To our best knowledge, no similar result exists in the literature. It is also remarkable that our new MacWilliams identity for the rank metric has a similar form to that for the Hamming metric. Despite the similarity, our new identity is proved using a different approach based on linear spaces. Using the same approach, we give an alternative proof of the MacWilliams identity for the Hamming metric. Based on our new identity, we also derive an expression that relates moments of the rank distribution of a linear code to those of its dual code, and provide an alternative derivation for the rank weight distribution of MRD codes.

The rest of the paper is organized as follows. Section II reviews necessary backgrounds in an effort to make this paper self-contained. Section III-A introduces the concepts of q -product and q -derivative for homogeneous polynomials, and investigates their properties. Using these tools, Sections III-B and III-C prove the MacWilliams identity for the rank metric, and Section III-D derives the relationship between the moments of the rank distribution of a linear code and those of its dual code. We also provide an alternative derivation of the rank distribution of MRD codes in Section III-E. Some examples are provided in Section III-F to illustrate our results. Finally, Section IV adapts the approach in Sections III-B and III-C to provide an alternative proof of the MacWilliams identity for the Hamming metric. All the proofs have been omitted due to limited space, and they will be presented at the conference.

II. PRELIMINARIES

A. Rank metric

Consider an n -dimensional vector $\mathbf{x} = (x_0, x_1, \dots, x_{n-1}) \in \text{GF}(q^m)^n$. Assume $\{\alpha_0, \alpha_1, \dots, \alpha_{m-1}\}$ is a basis set of $\text{GF}(q^m)$ over $\text{GF}(q)$, then for $j = 0, 1, \dots, n-1$, x_j can be written as $x_j = \sum_{i=0}^{m-1} x_{i,j} \alpha_i$, where $x_{i,j} \in \text{GF}(q)$ for $i = 0, 1, \dots, m-1$. Hence, x_j can be expanded to an m -dimensional column vector $(x_{0,j}, x_{1,j}, \dots, x_{m-1,j})^T$ with respect to the basis set $\{\alpha_0, \alpha_1, \dots, \alpha_{m-1}\}$. Let \mathbf{X} be the $m \times n$ matrix obtained by expanding all the coordinates of \mathbf{x} . That is,

$$\mathbf{X} = \begin{pmatrix} x_{0,0} & x_{0,1} & \cdots & x_{0,n-1} \\ x_{1,0} & x_{1,1} & \cdots & x_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ x_{m-1,0} & x_{m-1,1} & \cdots & x_{m-1,n-1} \end{pmatrix},$$

where $x_j = \sum_{i=0}^{m-1} x_{i,j} \alpha_i$. The *rank norm* of the vector \mathbf{x} (over $\text{GF}(q)$), denoted as $\text{rk}(\mathbf{x}|\text{GF}(q))$, is defined to be the rank of the matrix \mathbf{X} over $\text{GF}(q)$, i.e., $\text{rk}(\mathbf{x}|\text{GF}(q)) \stackrel{\text{def}}{=} \text{rank}(\mathbf{X})$ [5]. In this paper, all the ranks are over the base field $\text{GF}(q)$ unless otherwise specified. To simplify notations, we denote the rank norm of \mathbf{x} as $\text{rk}(\mathbf{x})$ henceforth.

The rank norm of \mathbf{x} is also the number of coordinates in \mathbf{x} that are linearly independent over $\text{GF}(q)$ [5]. The field $\text{GF}(q^m)$ may be viewed as an m -dimensional vector space over $\text{GF}(q)$. The coordinates of \mathbf{x} thus span a linear subspace of $\text{GF}(q^m)$, denoted as $\mathfrak{S}(\mathbf{x})$, and the rank of \mathbf{x} is the dimension of $\mathfrak{S}(\mathbf{x})$.

For all $\mathbf{x}, \mathbf{y} \in \text{GF}(q^m)^n$, it is easily verified that $d_r(\mathbf{x}, \mathbf{y}) \stackrel{\text{def}}{=} \text{rk}(\mathbf{x} - \mathbf{y})$ is a metric over $\text{GF}(q^m)^n$, referred to as the *rank metric* henceforth [5]. The *minimum rank distance* of a code, denoted as d_r , is simply the minimum rank distance over all possible pairs of distinct codewords.

B. The Singleton bound and MRD codes

The minimum rank distance of a code can be specifically bounded. First, the minimum rank distance d_r of a code of length n over $\text{GF}(q^m)$ is obviously bounded above by $\min\{m, n\}$. Codes that satisfy $d_r = m$ are studied in [8]. Also, it can be shown that $d_r \leq d_h$ [5], where d_h is the minimum Hamming distance of the same code. Due to the Singleton bound on the minimum Hamming distance of block codes [15], the minimum rank distance of a block code of length n ($n \leq m$) and cardinality M over $\text{GF}(q^m)$ thus satisfies

$$d_r \leq n - \log_{q^m} M + 1. \quad (1)$$

As in [5], we refer to codes that achieve the equality in Eq. (1) as MRD codes. It is also shown that the dual of any MRD code is also an MRD code [5]. Clearly MRD codes are the counterparts of maximum distance separable (MDS) codes.

C. Weight enumerator and Hadamard transform

We restrict our attention to the Hamming metric and the rank metric only henceforth in this paper.

Definition 1 (Weight function): Let d be a metric over $\text{GF}(q^m)^n$, and define $w(\mathbf{v}) = d(\mathbf{0}, \mathbf{v})$ as a weight over $\text{GF}(q^m)^n$. Suppose $\mathbf{v} \in \text{GF}(q^m)^n$ has weight r , then the weight function of \mathbf{v} is defined as $f_w(\mathbf{v}) = y^r x^{n-r}$.

We shall henceforth denote the Hamming weight function and the rank weight function as f_h and f_r respectively. Note that n is the maximum weight for both f_h and f_r .

Definition 2: Let \mathcal{C} be a code of length n over $\text{GF}(q^m)$. Suppose there are A_i codewords in \mathcal{C} with weight i , then the weight enumerator of \mathcal{C} , denoted as $W_{\mathcal{C}}(x, y)$, is defined as

$$W_{\mathcal{C}}^w(x, y) \stackrel{\text{def}}{=} \sum_{\mathbf{v} \in \mathcal{C}} f_w(\mathbf{v}) = \sum_{i=0}^n A_i y^i x^{n-i}.$$

Definition 3 (Hadamard transform [15]): Let \mathbb{C} be the field of complex numbers. Let $a \in \text{GF}(q^m)$ and let $\{1, \alpha_1, \dots, \alpha_{m-1}\}$ be a basis set of $\text{GF}(q^m)$. We thus have $a = a_0 + a_1\alpha_1 + \dots + a_{m-1}\alpha_{m-1}$. Finally, let $\zeta \in \mathbb{C}$ be a primitive q -th root of unity. We define $\chi(a) \stackrel{\text{def}}{=} \zeta^{a_0}$. For a mapping f from F to \mathbb{C} , the *Hadamard transform* of f , denoted as \hat{f} , is given by

$$\hat{f}(\mathbf{v}) \stackrel{\text{def}}{=} \sum_{\mathbf{u} \in F} \chi(\mathbf{u} \cdot \mathbf{v}) f(\mathbf{u}). \quad (2)$$

D. Notations

In order to simplify notations, we shall occasionally denote the vector space $\text{GF}(q^m)^n$ as F . We denote the number of vectors of rank u ($0 \leq u \leq \min\{m, n\}$) in $\text{GF}(q^m)^n$ as $N_u(q^m, n)$. It can be shown that $N_u(q^m, n) = \begin{bmatrix} n \\ u \end{bmatrix} \alpha(m, u)$, where $\alpha(m, u)$ is defined as follows: $\alpha(m, 0) = 1$ and $\alpha(m, u) = \prod_{i=0}^{u-1} (q^m - q^i)$ for $u \geq 1$. The $\begin{bmatrix} n \\ u \end{bmatrix}$ term is the

Gaussian binomial [16], defined as $\begin{bmatrix} n \\ u \end{bmatrix} = \alpha(n, u)/\alpha(u, u)$. Note that $\begin{bmatrix} n \\ u \end{bmatrix}$ is the number of u -dimensional linear subspaces of $\text{GF}(q)^n$. We also define $\beta(m, 0) \stackrel{\text{def}}{=} 1$ and $\beta(m, u) \stackrel{\text{def}}{=} \prod_{i=0}^{u-1} \begin{bmatrix} m-i \\ 1 \end{bmatrix}$ for $u > 0$, which are used in Section III-A. These terms are closely related to the Gaussian binomial: $\beta(m, u) = \begin{bmatrix} m \\ u \end{bmatrix} \beta(u, u)$ and $\beta(m+u, m+u) = \begin{bmatrix} m+u \\ u \end{bmatrix} \beta(m, m) \beta(u, u)$.

III. MACWILLIAMS IDENTITY FOR THE RANK METRIC

A. q -product and q -derivative of homogeneous polynomials

Definition 4 (q -product): Let $a(x, y; m) = \sum_{i=0}^r a_i(m) y^i x^{r-i}$ and $b(x, y; m) = \sum_{j=0}^s b_j(m) y^j x^{s-j}$ be two homogeneous polynomials in x and y of degrees r and s respectively with coefficients $a_i(m)$ and $b_j(m)$ respectively. $a_i(m)$ and $b_j(m)$ for $i, j \geq 0$ in turn are real functions of m , and are assumed to be zero unless otherwise specified. The q -product of $a(x, y; m)$ and $b(x, y; m)$ is defined to be the homogeneous polynomial of degree $(r+s)$ $c(x, y; m) \stackrel{\text{def}}{=} a(x, y; m) * b(x, y; m) = \sum_{u=0}^{r+s} c_u(m) y^u x^{r+s-u}$, with

$$c_u(m) = \sum_{i=0}^u q^{is} a_i(m) b_{u-i}(m-i).$$

For $n \geq 0$ the n -th q -power of $a(x, y; m)$ is defined recursively: $a(x, y; m)^{[0]} = 1$ and $a(x, y; m)^{[n]} = a(x, y; m)^{[n-1]} * a(x, y; m)$ for $n \geq 1$.

To illustrate the q -product, we provide some examples of the q -product. We have $x*y = yx$, $y*x = qyx$, $yx*x = qyx^2$, and $yx*(q^m-1)y = (q^m-q)y^2x$. Note that $x*y \neq y*x$. It is easy to verify that the q -product is in general non-commutative. However, it is commutative for some special cases.

Lemma 1: Suppose $a(x, y; m) = a$ is a constant independent from m , then $a(x, y; m) * b(x, y; m) = b(x, y; m) * a(x, y; m) = ab(x, y; m)$. Also, if $\deg[c(x, y; m)] = \deg[a(x, y; m)]$, then $[a(x, y; m) + c(x, y; m)] * b(x, y; m) = a(x, y; m) * b(x, y; m) + c(x, y; m) * b(x, y; m)$, and $b(x, y; m) * [a(x, y; m) + c(x, y; m)] = b(x, y; m) * a(x, y; m) + b(x, y; m) * c(x, y; m)$.

The homogeneous polynomials $a_l(x, y; m) \stackrel{\text{def}}{=} [x + (q^m - 1)y]^{[l]}$ and $b_l(x, y; m) \stackrel{\text{def}}{=} (x - y)^{[l]}$ turn out to be very important to our derivations below. The following lemma provides the analytical expressions of $a_l(x, y; m)$ and $b_l(x, y; m)$.

Lemma 2: For $i \geq 0$, $\sigma_i \stackrel{\text{def}}{=} \frac{i(i-1)}{2}$. For $l \geq 0$, we have $y^{[l]} = q^{\sigma_l} y^l$ and $x^{[l]} = x^l$. Furthermore,

$$a_l(x, y; m) = \sum_{u=0}^l \begin{bmatrix} l \\ u \end{bmatrix} \alpha(m, u) y^u x^{l-u}, \quad (3)$$

$$b_l(x, y; m) = \sum_{u=0}^l \begin{bmatrix} l \\ u \end{bmatrix} (-1)^u q^{\sigma_u} y^u x^{l-u}. \quad (4)$$

Note that $a_l(x, y; m)$ is the rank weight enumerator of $\text{GF}(q^m)^l$.

Definition 5 (q -transform): We define the q -transform of $a(x, y; m) = \sum_{i=0}^r a_i(m) y^i x^{r-i}$ as the homogeneous polynomial $\bar{a}(x, y; m) = \sum_{i=0}^r a_i(m) y^{[i]} * x^{[r-i]}$.

Definition 6 (q-derivative [17]): For $q \geq 2$, the q -derivative for $x \neq 0$ of a real-valued function $f(x)$ is defined as

$$f^{(1)}(x) \stackrel{\text{def}}{=} \frac{f(qx) - f(x)}{(q-1)x}.$$

The q -derivative operator is linear. For $\nu \geq 0$, we shall denote the partial ν -th q -derivative of $f(x, y)$ (with respect to x) as $f^{(\nu)}(x, y)$. The 0-th q -derivative of $f(x, y)$ is defined to be $f(x, y)$ itself.

Lemma 3: For $\nu \leq n$, the ν -th q -derivative of the function x^n is given by $\beta(n, \nu)x^{n-\nu}$. Also, the ν -th q -derivative of $f(x, y) = \sum_{i=0}^r f_i y^i x^{r-i}$ is given by $f^{(\nu)}(x, y) = \sum_{i=\nu}^r f_i \beta(i, \nu) x^{i-\nu}$.

Lemma 4 (Leibniz rule): For two homogeneous polynomials $f(x, y) = \sum_{i=0}^r f_i y^i x^{r-i}$ and $g(x, y) = \sum_{j=0}^s g_j y^j x^{s-j}$ with degrees r and s respectively, the ν -th ($\nu \geq 1$) q -derivative of their q -product is given by

$$(f(x, y) * g(x, y))^{(\nu)} = \sum_{l=0}^{\nu} \begin{bmatrix} \nu \\ l \end{bmatrix} q^{(\nu-l)(r-l)} \dots f^{(l)}(x, y) * g^{(\nu-l)}(x, y). \quad (5)$$

Next, we derive the q -derivatives of $a_l(x, y; m) = [x + (q^m - 1)y]^{[l]}$ and $b_l(x, y; m) = (x - y)^{[l]}$.

Lemma 5: For $\nu \leq l$ we have

$$a_l^{(\nu)}(x, y; m) = \beta(l, \nu) a_{l-\nu}(x, y; m) \quad (6)$$

$$b_l^{(\nu)}(x, y; m) = \beta(l, \nu) b_{l-\nu}(x, y; m). \quad (7)$$

B. The dual of a vector

As an important step toward our main result, we derive the rank weight enumerator of $\langle \mathbf{v} \rangle^\perp$, where $\mathbf{v} \in \text{GF}(q^m)^n$ is an arbitrary vector and $\langle \mathbf{v} \rangle \stackrel{\text{def}}{=} \{a\mathbf{v} : a \in \text{GF}(q^m)\}$. It is remarkable that the rank weight enumerator of $\langle \mathbf{v} \rangle^\perp$ depends on only the rank of \mathbf{v} .

Definition 7: For $s \geq 1$ the s -th order \mathbf{B} -elementary extension of an (n, k) linear code \mathcal{C}_0 is the $(n + s, k + s)$ linear code defined as $\mathcal{C}_s \stackrel{\text{def}}{=} \{(c_0, \dots, c_{n+s-1}) \in \text{GF}(q^m)^{n+s} \mid (c_0, \dots, c_{n-1}) - (c_n, \dots, c_{n+s-1})\mathbf{B} \in \mathcal{C}_0\}$, where \mathbf{B} is an $s \times n$ matrix over $\text{GF}(q)$. The 0-th order elementary extension of \mathcal{C}_0 is defined to be \mathcal{C}_0 itself.

Lemma 6: Let \mathcal{C}_0 be an (n, k) linear code over $\text{GF}(q^m)$ with generator matrix \mathbf{G}_0 and parity-check matrix \mathbf{H}_0 . The s -th order \mathbf{B} -elementary extension of \mathcal{C}_0 is the $(n + s, k + s)$ linear code \mathcal{C}_s over $\text{GF}(q^m)$ with a generator matrix $\mathbf{G}_s = \left(\begin{array}{c|c} \mathbf{G}_0 & \mathbf{0} \\ \hline \mathbf{B} & \mathbf{I}_s \end{array} \right)$ and a parity-check matrix $\mathbf{H}_s = \left(\begin{array}{c|c} \mathbf{H}_0 & -\mathbf{H}_0\mathbf{B}^T \end{array} \right)$.

Corollary 1: Suppose $\mathbf{v} = (v_0, \dots, v_{n-1}) \in \text{GF}(q^m)^n$ has rank $r \geq 1$. Then $\mathcal{L} = \langle \mathbf{v} \rangle^\perp$ is equivalent to the $(n - r)$ -th order elementary extension of an $(r, r - 1)$ linear code with $d_r = 2$.

It is easy to verify that the $(r, r - 1)$ code with $d_r = 2$ is actually an MRD code as defined in Section II-B.

We hence derive the rank weight enumerator of an $(r, r - 1, 2)$ MRD code. Note that the rank weight distribution of

MRD codes has been derived in [5]. However, we will use our results to give an alternative derivation of the rank weight distribution of MRD codes later, and thus we shall not use the result in [5] here.

Lemma 7: For $r \geq 1$, suppose $\mathbf{v}_r = (v_0, \dots, v_{r-1}) \in \text{GF}(q^m)^r$ has rank $r \leq m$. Then the number of vectors in $\mathcal{L}_r = \langle \mathbf{v}_r \rangle^\perp$ with rank r , denoted as $A_{r,r}$, depends on only r and satisfies $A_{r,r} = \alpha(m, r-1) - q^{r-1}A_{r-1,r-1}$. Furthermore, the rank weight enumerator of \mathcal{L}_r is given by

$$W_{\mathcal{L}_r}^{\mathbf{R}}(x, y) = q^{-m} \left\{ [x + (q^m - 1)y]^{[r]} + (q^m - 1)(x - y)^{[r]} \right\}.$$

The following lemma relates the rank weight enumerator of a code to that of any of its s -th order elementary extensions.

Lemma 8: Let $\mathcal{C}_0 \subseteq \text{GF}(q^m)^r$ be a linear code with rank weight enumerator $W_{\mathcal{C}_0}^{\mathbf{R}}(x, y)$, and for $s \geq 0$, let $W_{\mathcal{C}_s}^{\mathbf{R}}(x, y)$ be the rank weight enumerator of its s -th order \mathbf{B} -elementary extension \mathcal{C}_s . Then $W_{\mathcal{C}_s}^{\mathbf{R}}(x, y)$ does not depend on \mathbf{B} and is given by

$$W_{\mathcal{C}_s}^{\mathbf{R}}(x, y) = W_{\mathcal{C}_0}^{\mathbf{R}}(x, y) * [x + (q^m - 1)y]^{[s]}. \quad (8)$$

Combining Corollary 1, Lemma 7, and Lemma 8, the rank weight enumerator of $\langle \mathbf{v} \rangle^\perp$ can be determined at last.

Proposition 1: For $\mathbf{v} \in \text{GF}(q^m)^n$ with rank $r \geq 0$, the rank weight enumerator of $\mathcal{L} = \langle \mathbf{v} \rangle^\perp$ depends on only r , and is given by

$$W_{\mathcal{L}}^{\mathbf{R}}(x, y) = q^{-m} \left\{ [x + (q^m - 1)y]^{[n]} + (q^m - 1) \dots (x - y)^{[r]} * [x + (q^m - 1)y]^{[n-r]} \right\}. \quad (9)$$

C. MacWilliams identity

Using the results shown in Section III-B, we now derive the MacWilliams identity for rank metric codes.

Lemma 9: Suppose that for all $\lambda \in \text{GF}(q^m)^*$ and all $\mathbf{u} \in F$, we have $w(\lambda \mathbf{u}) = w(\mathbf{u})$. For $\mathbf{v} \in \text{GF}(q^m)^n$, let us denote $\langle \mathbf{v} \rangle^\perp$ as \mathcal{L} . Then the Hadamard transform of the weight function f_w , denoted as \hat{f}_w , satisfies

$$W_{\mathcal{L}}^{\mathbf{W}}(x, y) = q^{-m} \left[W_F^{\mathbf{W}}(x, y) + (q^m - 1)\hat{f}_w(\mathbf{v}) \right]. \quad (10)$$

Lemma 10: Suppose $\mathbf{v} \in \text{GF}(q^m)^n$ has rank r . Then the Hadamard transform of the rank weight function is given by

$$\hat{f}_r(\mathbf{v}) = (x - y)^{[r]} * [x + (q^m - 1)y]^{[n-r]}. \quad (11)$$

Let \mathcal{C} be an (n, k) linear code over $\text{GF}(q^m)$, and let $W_{\mathcal{C}}^{\mathbf{R}}(x, y) = \sum_{i=0}^n A_i y^i x^{n-i}$ be its rank weight enumerator and $W_{\mathcal{C}^\perp}^{\mathbf{R}}(x, y) = \sum_{j=0}^n B_j y^j x^{n-j}$ be the rank weight enumerator of its dual code \mathcal{C}^\perp .

Theorem 1: For any linear code \mathcal{C} and its dual code \mathcal{C}^\perp ,

$$W_{\mathcal{C}^\perp}^{\mathbf{R}}(x, y) = \frac{1}{|\mathcal{C}|} \bar{W}_{\mathcal{C}}^{\mathbf{R}}(x + (q^m - 1)y, x - y), \quad (12)$$

where $\bar{W}_{\mathcal{C}}^{\mathbf{R}}$ is the q -transform of $W_{\mathcal{C}}^{\mathbf{R}}$. Equivalently,

$$\sum_{j=0}^n B_j y^j x^{n-j} = q^{m(k-n)} \sum_{i=0}^n A_i (x - y)^{[i]} * [x + (q^m - 1)y]^{[n-i]}. \quad (13)$$

Also, B_j 's can be explicitly expressed in terms of A_i 's.

Corollary 2: We have

$$B_j = \frac{1}{|\mathcal{C}|} \sum_{i=0}^n A_i P_j(i; m, n), \quad (14)$$

where

$$P_j(i; m, n) \stackrel{\text{def}}{=} \sum_{l=0}^j \begin{bmatrix} i \\ l \end{bmatrix} \begin{bmatrix} n-i \\ j-l \end{bmatrix} (-1)^l q^{\sigma_l} q^{l(n-i)} \alpha(m-l, j-l). \quad (15)$$

D. Moments of the rank distribution

Next, we investigate the relationship between moments of the rank distribution of a linear code and those of its dual code. Our results parallel those in [15, p. 131].

First, applying Theorem 1 to \mathcal{C}^\perp , we obtain

$$\sum_{i=0}^n A_i y^i x^{n-i} = q^{m(k-n)} \sum_{j=0}^n B_j b_j(x, y; m) * a_{n-j}(x, y; m). \quad (16)$$

By q -differentiating Eq. (16) ν times with respect to x and using the Leibniz rule in Lemma 4 as well as the results in Lemma 5, we obtain

Proposition 2: For $0 \leq \nu \leq n$,

$$\sum_{i=0}^{n-\nu} \begin{bmatrix} n-i \\ \nu \end{bmatrix} A_i = q^{m(k-\nu)} \sum_{j=0}^{\nu} \begin{bmatrix} n-j \\ n-\nu \end{bmatrix} B_j. \quad (17)$$

As in [15], we refer to the left hand side of Eq. (17) as moments of the rank distribution of \mathcal{C} . We remark that the cases where $\nu = 0$ and $\nu = n$ are trivial. Also, Proposition 2 can be simplified if ν is less than the minimum distance of the dual code.

Corollary 3: Let d'_R be the minimum rank distance of \mathcal{C}^\perp . If $\nu < d'_R$, then

$$\sum_{i=0}^{n-\nu} \begin{bmatrix} n-i \\ \nu \end{bmatrix} A_i = q^{m(k-\nu)} \begin{bmatrix} n \\ \nu \end{bmatrix}. \quad (18)$$

E. Rank distribution of MRD codes

The rank distribution of MRD codes was first given in [5]. Based on our results in Section III-D, we provide an alternative derivation of the rank distribution of MRD codes. In this subsection, we assume $n \leq m$.

First, we obtain the following results necessary for our alternative derivation of the rank distribution.

Lemma 11: Let $\{a_j\}_{j=0}^l$ and $\{b_i\}_{i=0}^l$ be two sequences of real numbers. Suppose that for $0 \leq j \leq l$ we have $a_j = \sum_{i=0}^j \begin{bmatrix} l-i \\ j-i \end{bmatrix} b_i$. Then for $0 \leq i \leq l$ we have $b_i = \sum_{j=0}^i (-1)^{i-j} q^{\sigma_{i-j}} \begin{bmatrix} l-j \\ l-i \end{bmatrix} a_j$.

Based on Corollary 3 and using Lemma 11, we can derive the rank distribution of MRD codes when $n \leq m$:

Proposition 3 (Rank distribution of MRD codes): Let \mathcal{C} be an (n, k, d_R) MRD code over $\text{GF}(q^m)$ ($n \leq m$), and let $W_{\mathcal{C}}^R(x, y) = \sum_{i=0}^n A_i y^i x^{n-i}$ be its rank weight enumerator. We then have $A_0 = 1$ and for $0 \leq i \leq n - d_R$,

$$A_{d_R+i} = \begin{bmatrix} n \\ d_R+i \end{bmatrix} \sum_{j=0}^i (-1)^{i-j} q^{\sigma_{i-j}} \begin{bmatrix} d_R+i \\ d_R+j \end{bmatrix} (q^{m(j+1)} - 1). \quad (19)$$

We remark that the above rank distribution is consistent with that derived by Gabidulin in [5].

F. Examples

In this section, we illustrate Theorem 1 and Proposition 2 using some examples. For $m \geq 2$, consider the $(3, 2)$ linear code \mathcal{C}_1 over $\text{GF}(q^m)$ with generator matrix

$$\mathbf{G}_1 = \begin{pmatrix} 1 & \alpha & 1 \\ 1 & \alpha & 0 \end{pmatrix},$$

where α is a primitive element of $\text{GF}(q^m)$. It can be verified that the rank weight enumerator of \mathcal{C}_1 is given by $W_{\mathcal{C}_1}^R(x, y) = x^3 + (q^m - 1)yx^2 + q^2(q^m - 1)y^2x + (q^m - q^2)(q^m - 1)y^3$. Applying Theorem 1, we obtain $W_{\mathcal{C}_1^\perp}^R(x, y) = x^3 + (q^m - 1)y^2x$. We can verify by hand that $W_{\mathcal{C}_1^\perp}^R(x, y)$ is indeed the rank weight enumerator of \mathcal{C}_1^\perp , which has a generator matrix $\mathbf{H}_1 = \begin{pmatrix} -\alpha & 1 & 0 \end{pmatrix}$. For \mathcal{C}_1 , both sides of (17) are given by q^{2m} , $q^m \begin{bmatrix} 3 \\ 1 \end{bmatrix}$, $(q^m - 1 + \begin{bmatrix} 3 \\ 1 \end{bmatrix})$, and 1 for $\nu = 0, 1, 2, 3$ respectively. Note that the results hold when $m = 2 < n = 3$.

For $m \geq 4$, let us now consider the $(4, 2)$ code \mathcal{C}_2 over $\text{GF}(q^m)$ with the following generator matrix

$$\mathbf{G}_2 = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 1 & \alpha^q & \alpha^{2q} & \alpha^{3q} \end{pmatrix}.$$

\mathcal{C}_2 is actually a $(4, 2)$ MRD code with $d_R = 3$. Hence, its dual code \mathcal{C}_2^\perp is also a $(4, 2)$ MRD code with $d_R = 3$. The rank weight enumerators of both \mathcal{C}_2 and \mathcal{C}_2^\perp can be readily obtained using Proposition 3, and they are given by $W_{\mathcal{C}_2}^R(x, y) = W_{\mathcal{C}_2^\perp}^R(x, y) = x^4 + \begin{bmatrix} 4 \\ 1 \end{bmatrix} (q^m - 1)y^3x^1 + \{q^{2m} - 1 - \begin{bmatrix} 4 \\ 1 \end{bmatrix} (q^m - 1)\} y^4$. It can be verified that $W_{\mathcal{C}_2}^R(x, y)$ and $W_{\mathcal{C}_2^\perp}^R(x, y)$ satisfy Theorem 1. For \mathcal{C}_2 , it can also be verified that both sides of (17) are q^{2m} , $\begin{bmatrix} 4 \\ 1 \end{bmatrix} q^m$, $\begin{bmatrix} 4 \\ 2 \end{bmatrix}$, $\begin{bmatrix} 4 \\ 1 \end{bmatrix}$, and 1 for $\nu = 0, 1, \dots, 4$ respectively.

Finally, consider the $(7, 4)$ code \mathcal{C}_3 over $\text{GF}(2^4)$ with the following generator matrix

$$\mathbf{G}_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & \beta^3 & \beta^6 & \beta^{12} \\ 0 & 1 & 0 & 0 & \beta^6 & \beta^{12} & 0 \\ 0 & 0 & 1 & 0 & \beta^{12} & 0 & \beta^3 \\ 0 & 0 & 0 & 1 & 0 & \beta^3 & \beta^6 \end{pmatrix},$$

where β is a primitive element of $\text{GF}(2^4)$. Its rank weight enumerator is given by $W_{\mathcal{C}_3}^R(x, y) = x^7 + 105y^2x^5 + 7350y^3x^4 + 58080y^4x^3$, Theorem 1 indicates that the rank weight enumerator of its dual code is given by $W_{\mathcal{C}_3^\perp}^R(x, y) = x^7 + 465y^3x^4 + 3630y^4x^3$, which can be verified using exhaustive search. It can also be verified that both sides of (17) for \mathcal{C}_3 are 2^{16} , 520192, 682752, 196416, 22416, 2772, 127, and 1 for $\nu = 0, 1, \dots, 7$ respectively.

IV. MACWILLIAMS IDENTITY FOR THE HAMMING METRIC

In this section, we adapt the approach used in our proof of Theorem 1 to provide an alternative proof of the MacWilliams identity for the Hamming metric. We first derive the Hamming weight enumerator of $\langle \mathbf{v} \rangle^\perp$, where \mathbf{v} is an arbitrary vector.

Then, using this result and properties of the Hadamard transform, we obtain the MacWilliams identity for the Hamming metric.

Definition 8: For $s \geq 1$, the s -th order coordinate extension of an (n, k) linear code \mathcal{C}_0 is defined as the $(n+s, k+s)$ code $\mathcal{C}_s \stackrel{\text{def}}{=} \{(c_0, \dots, c_{n+s-1}) \in \text{GF}(q^m)^{n+s} \mid (c_0, \dots, c_{n-1}) \in \mathcal{C}_0\}$. The 0-th order coordinate extension of \mathcal{C}_0 is defined as \mathcal{C}_0 itself.

We remark that the s -th order coordinate extension is a special case of the s -th order \mathbf{B} -elementary extension with $\mathbf{B} = \mathbf{0}$.

Lemma 12: Let \mathcal{C}_0 be an (n, k) linear code over $\text{GF}(q^m)$, with a generator matrix \mathbf{G}_0 and a parity-check matrix \mathbf{H}_0 . Then \mathcal{C}_s over $\text{GF}(q^m)$ has a generator matrix $\mathbf{G}_s = \left(\begin{array}{c|c} \mathbf{G}_0 & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I}_s \end{array} \right)$ and a parity-check matrix $\mathbf{H}_s = \left(\begin{array}{c|c} \mathbf{H}_0 & \mathbf{0} \end{array} \right)$.

Corollary 4: Suppose $\mathbf{v} \in \text{GF}(q^m)^n$ has Hamming weight $r \geq 1$. Then $\mathcal{L} = \langle \mathbf{v} \rangle^\perp$ is equivalent to the $(n-r)$ -th order coordinate extension of an $(r, r-1, 2)$ MDS code.

We hence derive the Hamming weight distribution of an $(r, r-1, 2)$ MDS code. Note that [15] gives the Hamming weight distribution of all MDS codes. However, that proof relies on the MacWilliams identity, and thus may not be used here.

Lemma 13: Suppose $\mathbf{v}_r = (v_0, \dots, v_{r-1}) \in \text{GF}(q^m)^r$ has Hamming weight r . Then $\mathcal{L}_r = \langle \mathbf{v}_r \rangle^\perp$ is an $(r, r-1, 2)$ MDS code whose weight enumerator does not depend on \mathbf{v}_r and is given by

$$W_{\mathcal{L}_r}^H(x, y) = q^{-m} \{ [x + (q^m - 1)y]^r + (q^m - 1)(x - y)^r \}.$$

The following lemma relates the Hamming weight enumerator of a code to that of its s -th order coordinate extension.

Lemma 14: Let $\mathcal{C}_0 \subseteq \text{GF}(q^m)^r$ be a linear code with Hamming weight enumerator $W_{\mathcal{C}_0}^H(x, y)$, and for $s \geq 0$ let $W_{\mathcal{C}_s}^H(x, y)$ be the weight enumerator of its s -th order coordinate extension \mathcal{C}_s . Then

$$W_{\mathcal{C}_s}^H(x, y) = W_{\mathcal{C}_0}^H(x, y) \cdot [x + (q^m - 1)y]^s. \quad (20)$$

Combining Corollary 4, Lemma 13, and Lemma 14, the Hamming weight distribution of \mathcal{L} can eventually be determined.

Proposition 4: For $\mathbf{v} \in \text{GF}(q^m)^n$ with $w_H(\mathbf{v}) = r$, the Hamming weight enumerator of $\mathcal{L} = \langle \mathbf{v} \rangle^\perp$ depends on only $w_H(\mathbf{v})$, and is given by

$$\begin{aligned} W_{\mathcal{L}}^H(x, y) &= q^{-m} \left\{ [x + (q^m - 1)y]^n + (q^m - 1) \cdots \right. \\ &\quad \left. \cdots (x - y)^r [x + (q^m - 1)y]^{n-r} \right\}. \end{aligned} \quad (21)$$

Lemma 15: Suppose $\mathbf{v} \in \text{GF}(q^m)^n$ has Hamming weight r . Then the Hadamard transform of the Hamming weight function is given by

$$\hat{f}_H(\mathbf{v}) = (x - y)^r [x + (q^m - 1)y]^{n-r}. \quad (22)$$

Using Lemma 15, we finally establish the MacWilliams identity for the Hamming metric.

Theorem 2: For any linear code \mathcal{C} , we have

$$W_{\mathcal{C}^\perp}^H(x, y) = \frac{1}{|\mathcal{C}|} W_{\mathcal{C}}^H(x + (q^m - 1)y, x - y). \quad (23)$$

We remark that the MacWilliams identities for the Hamming and the rank metrics given in Theorems 2 and 1 respectively have exactly the same form except for the q -transform in Eq. (12). Note that Theorem 2 is precisely the MacWilliams identity for the Hamming metric given by Theorem 13 in [15, Chap. 5], although our proof is different from that in [15, Chap. 5]. Finally, we remark that Theorem 13 in [15, Chap. 5] is a special case of the MacWilliams Theorem for complete weight enumerators (see Theorem 10 in [15, Chap. 5]). For the rank metric, it is not clear how we can adapt the concept of complete weight enumerator to give a proof of the MacWilliams identity.

REFERENCES

- [1] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: Performance criterion and code construction," *IEEE Trans. Info. Theory*, vol. 44, pp. 774–765, March 1998.
- [2] P. Lusina, E. M. Gabidulin, and M. Bossert, "Maximum Rank Distance codes as space-time codes," *IEEE Trans. Info. Theory*, vol. 49, pp. 2757–2760, Oct. 2003.
- [3] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov, "Ideals over a non-commutative ring and their application in cryptology," *LNCS*, vol. 573, pp. 482–489, 1991.
- [4] R. M. Roth, "Maximum-rank array codes and their application to crisscross error correction," *IEEE Trans. Info. Theory*, vol. 37, no. 2, pp. 328–336, March 1991.
- [5] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Problems on Information Transmission*, vol. 21, no. 1, pp. 1–12, Jan. 1985.
- [6] N. Suresh Babu, "Studies on rank distance codes," Ph.D Dissertation, IIT Madras, Feb. 1995.
- [7] W. B. Vasantha and N. Suresh Babu, "On the covering radius of rank-distance codes," *Ganita Sandesh*, vol. 13, pp. 43–48, 1999.
- [8] K. N. Manoj and B. Sundar Rajan, "Full Rank Distance codes," *Technical Report, IISc Bangalore*, Oct. 2002.
- [9] W. B. Vasantha and R. J. Selvaraj, "Multi-covering radii of codes with rank metric," *Proc. Information Theory Workshop*, p. 215, Oct. 2002.
- [10] W. B. Vasantha and R. S. Raja Durai, "Maximum rank distance codes with complementary duals: an application to F-adder channel," Dec. 2002.
- [11] U. Sripathi and B. Sundar Rajan, "On the rank distance of cyclic codes," *Proc. IEEE Int. Symp. on Information Theory*, p. 72, July 2003.
- [12] A. Kshevetskiy and E. M. Gabidulin, "The new construction of rank codes," *Proc. IEEE Int. Symp. on Information Theory*, pp. 2105–2108, Sept. 2005.
- [13] E. M. Gabidulin and P. Loidreau, "On subcodes of codes in the rank metric," *Proc. IEEE Int. Symp. on Information Theory*, pp. 121–123, Sept. 2005.
- [14] P. Loidreau, "Properties of codes in rank metric," preprint.
- [15] F. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1977.
- [16] G. E. Andrews, *The Theory of Partitions*, ser. Encyclopedia of Mathematics and its Applications, G.-C. Rota, Ed. Reading, MA: Addison-Wesley, 1976, vol. 2.
- [17] G. Gasper and M. Rahman, *Basic Hypergeometric Series*, 2nd ed., ser. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2004, vol. 96.