Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2008, Article ID 754021, 13 pages
doi:10.1155/2008/754021

Research Article

MacWilliams Identity for Codes with the Rank Metric

Maximilien Gadouleau and Zhiyuan Yan

Department of Electrical and Computer Engineering, Lehigh University, Bethlehem, PA 18015, USA

Correspondence should be addressed to Maximilien Gadouleau, magc@lehigh.edu

Received 10 November 2007; Accepted 3 March 2008

Recommended by Andrej Stefanov

The MacWilliams identity, which relates the weight distribution of a code to the weight distribution of its dual code, is useful in determining the weight distribution of codes. In this paper, we derive the MacWilliams identity for linear codes with the rank metric, and our identity has a different form than that by Delsarte. Using our MacWilliams identity, we also derive related identities for rank metric codes. These identities parallel the binomial and power moment identities derived for codes with the Hamming metric.

1. INTRODUCTION

The MacWilliams identity for codes with the Hamming metric [1], which relates the Hamming weight distribution of a code to the weight distribution of its dual code, is useful in determining the Hamming weight distribution of codes. This is because if the dual code has a small number of codewords or equivalence classes of codewords under some known permutation group, its weight distribution can be obtained by exhaustive examination. It also leads to other identities for the weight distribution such as the Pless identities [1, 2].

Although the rank has long been known to be a metric implicitly and explicitly (e.g., see [3]), the rank metric was first considered for error-control codes (ECCs) by Delsarte [4]. The potential applications of rank metric codes to wireless communications [5, 6], public-key cryptosystems [7], and storage equipments [8, 9] have motivated a steady stream of works [8–20] that focus on their properties. The majority of previous works focus on rank distance properties, code construction, and efficient decoding of rank metric codes, and the seminal works in [4, 9, 10] have made significant contribution to these topics. Independently in [4, 9, 10], a Singleton bound (up to some variations) on the minimum rank distance of codes was established, and a class of codes achieving the bound with equality was constructed. We refer to this class of codes as Gabidulin codes henceforth. In [4, 10], analytical expressions to compute the weight distribution of linear codes achieving the Singleton bound with equality were also derived. In [8], it was shown that Gabidulin codes are optimal for correcting crisscross errors (referred to as lattice-pattern errors in [8]). In [9], it was shown that Gabidulin codes are also optimal in the sense of a Singleton bound in crisscross weight, a metric considered in [9, 12, 21] for crisscross errors. Decoding algorithms were introduced for Gabidulin codes in [9, 10, 22, 23].

In [4], the counterpart of the MacWilliams identity, which relates the rank distance enumerator of a code to that of its dual code, was established using association schemes. However, Delsarte's work lacks an expression of the rank weight enumerator of the dual code as a functional transformation of the enumerator of the code. In [24, 25], Grant and Varanasi defined a *different* rank weight enumerator and established a functional transformation between the rank weight enumerator of a code and that of its dual code.

In this paper we show that, similar to the MacWilliams identity for the Hamming metric, the rank weight distribution of any linear code can be expressed as a functional transformation of that of its dual code. It is remarkable that our MacWilliams identity for the rank metric has a similar form to that for the Hamming metric. Similarly, an intermediate result of our proof is that the rank weight enumerator of the dual of any vector depends on only the rank weight of the vector and is related to the rank weight enumerator of a maximum rank distance (MRD) code. We also derive additional identities that relate moments of the rank weight distribution of a linear code to those of its dual code.

Our work in this paper differs from those in [4, 24, 25] in several aspects.

(i) In this paper, we consider a rank weight enumerator different from that in [24, 25], and solve the original problem of determining the functional transformation of rank weight enumerators between dual codes as defined by Delsarte.

(ii) Our proof, based on character theory, does not require the use of association schemes as in [4] or combinatorial arguments as in [24, 25].

(iii) In [4], the MacWilliams identity is given between the rank distance enumerator sequences of two dual array codes using the generalized Krawtchouk polynomials. Our identity is equivalent to that in [4] for linear rank metric codes, although our identity is expressed using different parameters which are shown to be the generalized Krawtchouk polynomials as well. We also present this identity in the form of a functional transformation (cf. Theorem 1). In such a form, the MacWilliams identities for both the rank and the Hamming metrics are similar to each other.

(iv) The functional transformation form allows us to derive further identities (cf. Section 4) between the rank weight distribution of linear dual codes. We would like to stress that the identities between the moments of the rank distribution proved in this paper are novel and were not considered in the aforementioned papers.

We remark that both the matrix form [4, 9] and the vector form [10] for rank metric codes have been considered in the literature. Following [10], in this paper the vector form over $\mathrm{GF}(q^m)$ is used for rank metric codes although their rank weight is defined by their corresponding code matrices over $\mathrm{GF}(q)$ [10]. The vector form is chosen in this paper since our results and their derivations for rank metric codes can be readily related to their counterparts for Hamming metric codes.

The rest of the paper is organized as follows. Section 2 reviews some necessary backgrounds. In Section 3, we establish the MacWilliams identity for the rank metric. We finally study the moments of the rank distributions of linear codes in Section 4.

2. PRELIMINARIES

2.1. *Rank metric, MRD codes, and rank weight enumerator*

Consider an n-dimensional vector $\mathbf{x} = (x_0, x_1, \dots, x_{n-1}) \in \mathrm{GF}(q^m)^n$. The field $\mathrm{GF}(q^m)$ may be viewed as an m-dimensional vector space over $\mathrm{GF}(q)$. The rank weight of $\mathbf{x}$, denoted as $\mathrm{rk}(\mathbf{x})$, is defined to be the *maximum* number of coordinates in $\mathbf{x}$ that are linearly independent over $\mathrm{GF}(q)$ [10]. Note that all ranks are with respect to $\mathrm{GF}(q)$ unless otherwise specified in this paper. The coordinates of $\mathbf{x}$ thus span a linear subspace of $\mathrm{GF}(q^m)$, denoted as $\mathfrak{S}(\mathbf{x})$, with dimension equal to $\mathrm{rk}(\mathbf{x})$. For all $\mathbf{x}, \mathbf{y} \in \mathrm{GF}(q^m)^n$, it is easily verified that $d_R(\mathbf{x}, \mathbf{y}) \overset{\text{def}}{=} \mathrm{rk}(\mathbf{x} - \mathbf{y})$ is a metric over $\mathrm{GF}(q^m)^n$ [10], referred to as the *rank metric* henceforth. The *minimum rank distance* of a code $\mathcal{C}$, denoted as $d_R(\mathcal{C})$, is simply the minimum rank distance over all possible pairs of distinct codewords. When there is no ambiguity about $\mathcal{C}$, we denote the minimum rank distance as d_R.

Combining the bounds in [10, 26] and generalizing slightly to account for nonlinear codes, we can show that the cardinality K of a code $\mathcal{C}$ over $\mathrm{GF}(q^m)$ with length n and minimum rank distance d_R satisfies

$$K \leq \min\left\{q^{m(n-d_R+1)}, q^{n(m-d_R+1)}\right\}. \tag{1}$$

In this paper, we call the bound in (1) the Singleton bound for codes with the rank metric, and refer to codes that attain the Singleton bound as maximum rank distance (MRD) codes. We refer to MRD codes over $\mathrm{GF}(q^m)$ with length $n \leq m$ and with length $n > m$ as Class-I and Class-II MRD codes, respectively. For any given parameter set n, m, and d_R, explicit construction for linear or nonlinear MRD codes exists. For $n \leq m$ and $d_R \leq n$, generalized Gabidulin codes [16] constitute a *subclass* of linear Class-I MRD codes. For $n > m$ and $d_R \leq m$, a Class-II MRD code can be constructed by transposing a generalized Gabidulin code of length m and minimum rank distance d_R over $\mathrm{GF}(q^n)$, although this code is not necessarily linear over $\mathrm{GF}(q^m)$. When $n = lm$ ($l \geq 2$), linear Class-II MRD codes of length n and minimum distance d_R can be constructed by a Cartesian product $\mathcal{G}^l \overset{\text{def}}{=} \mathcal{G} \times \cdots \times \mathcal{G}$ of an (m, k) linear Class-I MRD code $\mathcal{G}$ [26].

For all $\mathbf{v} \in \mathrm{GF}(q^m)^n$ with rank weight r, the rank weight function of $\mathbf{v}$ is defined as $f_R(\mathbf{v}) = y^r x^{n-r}$. Let $\mathcal{C}$ be a code of length n over $\mathrm{GF}(q^m)$. Suppose there are A_i codewords in $\mathcal{C}$ with rank weight i $(0 \leq i \leq n)$. Then the rank weight enumerator of $\mathcal{C}$, denoted as $W_{\mathcal{C}}^R(x, y)$, is defined to be

$$W_{\mathcal{C}}^R(x, y) \overset{\text{def}}{=} \sum_{\mathbf{v} \in \mathcal{C}} f_R(\mathbf{v}) = \sum_{i=0}^{n} A_i y^i x^{n-i}. \tag{2}$$

2.2. *Hadamard transform*

Definition 1 (see [1]). Let $\mathbb{C}$ be the field of complex numbers. Let $a \in \mathrm{GF}(q^m)$ and let $\{1, \alpha_1, \dots, \alpha_{m-1}\}$ be a basis set of $\mathrm{GF}(q^m)$. We thus have $a = a_0 + a_1\alpha_1 + \cdots + a_{m-1}\alpha_{m-1}$, where $a_i \in \mathrm{GF}(q)$ for $0 \leq i \leq m-1$. Finally, letting $\zeta \in \mathbb{C}$ be a primitive qth root of unity, $\chi(a) \overset{\text{def}}{=} \zeta^{a_0}$ maps $\mathrm{GF}(q^m)$ to $\mathbb{C}$.

Definition 2 (Hadamard transform [1]). For a mapping f from $\mathrm{GF}(q^m)^n$ to $\mathbb{C}$, the *Hadamard transform* of f, denoted as $\hat{f}$, is defined to be

$$\hat{f}(\mathbf{v}) \overset{\text{def}}{=} \sum_{\mathbf{u} \in \mathrm{GF}(q^m)^n} \chi(\mathbf{u} \cdot \mathbf{v}) f(\mathbf{u}), \tag{3}$$

where $\mathbf{u} \cdot \mathbf{v}$ denotes the inner product of $\mathbf{u}$ and $\mathbf{v}$.

2.3. Notations

In order to simplify notations, we will occasionally denote the vector space $\mathrm{GF}(q^m)^n$ as F. We denote the number of vectors of rank u $(0 \le u \le \min\{m,n\})$ in $\mathrm{GF}(q^m)^n$ as $N_u(q^m,n)$. It can be shown that $N_u(q^m,n) = \begin{bmatrix} n \\ u \end{bmatrix}\alpha(m,u)$ [10], where $\alpha(m,0) \overset{\mathrm{def}}{=} 1$ and $\alpha(m,u) \overset{\mathrm{def}}{=} \prod_{i=0}^{u-1}(q^m - q^i)$ for $u \ge 1$. The $\begin{bmatrix} n \\ u \end{bmatrix}$ term is often referred to as a Gaussian polynomial [27], defined as $\begin{bmatrix} n \\ u \end{bmatrix} \overset{\mathrm{def}}{=} \alpha(n,u)/\alpha(u,u)$. Note that $\begin{bmatrix} n \\ u \end{bmatrix}$ is the number of u-dimensional linear subspaces of $\mathrm{GF}(q)^n$. We also define $\beta(m,0) \overset{\mathrm{def}}{=} 1$ and $\beta(m,u) \overset{\mathrm{def}}{=} \prod_{i=0}^{u-1}\begin{bmatrix} m-i \\ 1 \end{bmatrix}$ for $u \ge 1$. These terms are closely related to Gaussian polynomials: $\beta(m,u) = \begin{bmatrix} m \\ u \end{bmatrix}\beta(u,u)$ and $\beta(m+u,m+u) = \begin{bmatrix} m+u \\ u \end{bmatrix}\beta(m,m)\beta(u,u)$. Finally, $\sigma_i \overset{\mathrm{def}}{=} i(i-1)/2$ for $i \ge 0$.

3. MACWILLIAMS IDENTITY FOR THE RANK METRIC

3.1. q-product, q-transform, and q-derivative

In order to express the MacWilliams identity in polynomial form as well as to derive other identities, we introduce several operations on homogeneous polynomials.

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 $i, j \ge 0$ in turn are real functions of m, and are assumed to be zero unless otherwise specified.

Definition 3 (q-product). The *q-product* of $a(x,y;m)$ and $b(x,y;m)$ is defined to be the homogeneous polynomial of degree $(r+s)$ $c(x,y;m) \overset{\mathrm{def}}{=} a(x,y;m) * b(x,y;m) = \sum_{u=0}^{r+s} c_u(m) y^u x^{r+s-u}$, with

$$c_u(m) = \sum_{i=0}^{u} q^{is} a_i(m) b_{u-i}(m-i). \tag{4}$$

We will denote the q-product by $*$ henceforth. For $n \ge 0$, the nth 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 $n \ge 1$.

We provide some examples to illustrate the concept. It is easy to verify that $x * y = yx$, $y * x = qyx$, $yx * x = qyx^2$, and $yx * (q^m - 1)y = (q^m - q)y^2 x$. Note that $x * y \neq y * x$. It is easy to verify that the q-product is neither commutative nor distributive in general. However, it is commutative and distributive in some special cases as described below.

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 $a_l(x,y;m) \overset{\mathrm{def}}{=} [x + (q^m - 1)y]^{[l]}$ and $b_l(x,y;m) \overset{\mathrm{def}}{=} (x - y)^{[l]}$ are 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 $l \ge 0$, $y^{[l]} = q^{\sigma_l} y^l$ and $x^{[l]} = x^l$. Furthermore,*

$$\begin{aligned} a_l(x,y;m) &= \sum_{u=0}^{l} \begin{bmatrix} l \\ u \end{bmatrix} \alpha(m,u) y^u x^{l-u}, \\ b_l(x,y;m) &= \sum_{u=0}^{l} \begin{bmatrix} l \\ u \end{bmatrix} (-1)^u q^{\sigma_u} y^u x^{l-u}. \end{aligned} \tag{5}$$

Note that $a_l(x,y;m)$ is the rank weight enumerator of $\mathrm{GF}(q^m)^l$. The proof of Lemma 2, which goes by induction on l, is easy and hence omitted.

Definition 4 (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 5 (q-derivative [28]). For $q \ge 2$, the q-derivative at $x \neq 0$ of a real-valued function $f(x)$ is defined as

$$f^{(1)}(x) \overset{\mathrm{def}}{=} \frac{f(qx) - f(x)}{(q-1)x}. \tag{6}$$

For any real number a, $[f(x) + ag(x)]^{(1)} = f^{(1)}(x) + ag^{(1)}(x)$ for $x \neq 0$. For $\nu \ge 0$, we will denote the νth q-derivative (with respect to x) of $f(x,y)$ as $f^{(\nu)}(x,y)$. The 0th q-derivative of $f(x,y)$ is defined to be $f(x,y)$ itself.

Lemma 3. *For $0 \le \nu \le l$, $(x^l)^{(\nu)} = \beta(l,\nu)x^{l-\nu}$. The νth q-derivative of $f(x,y) = \sum_{i=0}^{r} f_i y^i x^{r-i}$ is given by $f^{(\nu)}(x,y) = \sum_{i=0}^{r-\nu} f_i \beta(i,\nu) y^i x^{r-i-\nu}$. Also,*

$$\begin{aligned} a_l^{(\nu)}(x,y;m) &= \beta(l,\nu) a_{l-\nu}(x,y;m), \\ b_l^{(\nu)}(x,y;m) &= \beta(l,\nu) b_{l-\nu}(x,y;m). \end{aligned} \tag{7}$$

The proof of Lemma 3, which goes by induction on ν, is easy and hence omitted.

Lemma 4 (Leibniz rule for the q-derivative). *For two homogeneous polynomials $f(x,y)$ and $g(x,y)$ with degrees r and s, respectively, the νth $(\nu \ge 0)$ q-derivative of their q-product is given by*

$$[f(x,y) * g(x,y)]^{(\nu)} = \sum_{l=0}^{\nu} \begin{bmatrix} \nu \\ l \end{bmatrix} q^{(\nu-l)(r-l)} f^{(l)}(x,y) * g^{(\nu-l)}(x,y). \tag{8}$$

The proof of Lemma 4 is given in Appendix A.

The q^{-1}-derivative is similar to the q-derivative.

Definition 6 (q^{-1}-derivative). For $q \ge 2$, the q^{-1}-derivative at $y \neq 0$ of a real-valued function $g(y)$ is defined as

$$g^{\{1\}}(y) \overset{\mathrm{def}}{=} \frac{g(q^{-1}y) - g(y)}{(q^{-1} - 1)y}. \tag{9}$$

For any real number a, $[f(y) + ag(y)]^{\{1\}} = f^{\{1\}}(y) + ag^{\{1\}}(y)$ for $y \neq 0$. For $\nu \ge 0$, we will denote the νth

q^{-1}-derivative (with respect to y) of $g(x,y)$ as $g^{\{\nu\}}(x,y)$. The 0th q^{-1}-derivative of $g(x,y)$ is defined to be $g(x,y)$ itself.

Lemma 5. *For $0 \leq \nu \leq l$, the νth q^{-1}-derivative of y^l is $(y^l)^{\{\nu\}} = q^{\nu(1-n)+\sigma_\nu}\beta(l,\nu)y^{l-\nu}$. Also,*

$$\begin{aligned} a_l^{\{\nu\}}(x,y;m) &= \beta(l,\nu)q^{-\sigma_\nu}\alpha(m,\nu)a_{l-\nu}(x,y;m-\nu), \\ b_l^{\{\nu\}}(x,y;m) &= (-1)^\nu\beta(l,\nu)b_{l-\nu}(x,y;m). \end{aligned} \tag{10}$$

The proof of Lemma 5 is similar to that of Lemma 3 and is hence omitted.

Lemma 6 (Leibniz rule for the q^{-1}-derivative). *For two homogeneous polynomials $f(x,y;m)$ and $g(x,y;m)$ with degrees r and s, respectively, the νth ($\nu \geq 0$) q^{-1}-derivative of their q-product is given by*

$$\begin{aligned} &\left[f(x,y;m)*g(x,y;m)\right]^{\{\nu\}} \\ &\quad = \sum_{l=0}^{\nu}\begin{bmatrix}\nu \\ l\end{bmatrix} q^{l(s-\nu+l)} f^{\{l\}}(x,y;m)*g^{\{\nu-l\}}(x,y;m-l). \end{aligned} \tag{11}$$

The proof of Lemma 6 is given in Appendix B.

3.2. 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 $\mathbf{v} \in \mathrm{GF}(q^m)^n$ is an arbitrary vector and $\langle\mathbf{v}\rangle \overset{\text{def}}{=} \{a\mathbf{v} : a \in \mathrm{GF}(q^m)\}$. Note that $\langle\mathbf{v}\rangle$ can be viewed as an $(n,1)$ linear code over $\mathrm{GF}(q^m)$ with a generator matrix $\mathbf{v}$. It is remarkable that the rank weight enumerator of $\langle\mathbf{v}\rangle^\perp$ depends on only the rank of $\mathbf{v}$.

Berger [14] has determined that linear isometries for the rank distance are given by the scalar multiplication by a nonzero element of $\mathrm{GF}(q^m)$, and multiplication on the right by a nonsingular matrix $\mathbf{B} \in \mathrm{GF}(q)^{n\times n}$. We say that two codes C and C' are rank-equivalent if there exists a linear isometry f for the rank distance such that $f(C) = C'$.

Lemma 7. *Suppose $\mathbf{v}$ has rank $r \geq 1$. Then $\mathcal{L} = \langle\mathbf{v}\rangle^\perp$ is rank-equivalent to $\mathcal{C} \times \mathrm{GF}(q^m)^{n-r}$, where $\mathcal{C}$ is an $(r, r-1, 2)$ MRD code and $\times$ denotes Cartesian product.*

Proof. We can express $\mathbf{v}$ as $\mathbf{v} = \bar{\mathbf{v}}\mathbf{B}$, where $\bar{\mathbf{v}} = (v_0,\ldots,v_{r-1},0\ldots,0)$ has rank r, and $\mathbf{B} \in \mathrm{GF}(q)^{n\times n}$ has full rank. Remark that $\bar{\mathbf{v}}$ is the parity-check of $\mathcal{C} \times \mathrm{GF}(q^m)^{n-r}$, where $\mathcal{C} = \langle(v_0,\ldots,v_{r-1})\rangle^\perp$ is an $(r,r-1,2)$ MRD code. It can be easily checked that $\mathbf{u} \in \mathcal{L}$ if and only if $\bar{\mathbf{u}} \overset{\text{def}}{=} \mathbf{u}\mathbf{B}^T \in \langle\bar{\mathbf{v}}\rangle^\perp$. Therefore, $\langle\bar{\mathbf{v}}\rangle^\perp = \mathcal{L}\mathbf{B}^T$, and hence $\mathcal{L}$ is rank-equivalent to $\langle\bar{\mathbf{v}}\rangle^\perp = \mathcal{C} \times \mathrm{GF}(q^m)^{n-r}$. □

We hence derive the rank weight enumerator of an $(r,r-1,2)$ MRD code. Note that the rank weight distribution of linear Class-I MRD codes has been derived in [4, 10]. However, we will not use the result in [4, 10], and instead derive the rank weight enumerator of an $(r,r-1,2)$ MRD code directly.

Proposition 1. *Suppose $\mathbf{v}_r \in \mathrm{GF}(q^m)^r$ has rank r ($0 \leq r \leq m$). The rank weight enumerator of $\mathcal{L}_r = \langle\mathbf{v}\rangle^\perp$ depends on only r and is given by*

$$W^R_{\mathcal{L}_r}(x,y) = q^{-m}\left\{\left[x + (q^m-1)y\right]^{[r]} + (q^m-1)(x-y)^{[r]}\right\}. \tag{12}$$

Proof. We first prove that the number of vectors with rank r in $\mathcal{L}_r$, denoted as $A_{r,r}$, depends only on r and is given by

$$A_{r,r} = q^{-m}\left[\alpha(m,r) + (q^m-1)(-1)^r q^{\sigma_r}\right] \tag{13}$$

by induction on r ($r \geq 1$). Equation (13) clearly holds for $r = 1$. Suppose (13) holds for $r = \bar{r}-1$.

We consider all the vectors $\mathbf{u} = (u_0,\ldots,u_{\bar{r}-1}) \in \mathcal{L}_{\bar{r}}$ such that the first $\bar{r}-1$ coordinates of $\mathbf{u}$ are linearly independent. Remark that $u_{\bar{r}-1} = -v_{\bar{r}-1}^{-1}\sum_{i=0}^{\bar{r}-2}u_i v_i$ is completely determined by $u_0,\ldots,u_{\bar{r}-2}$. Thus there are $N_{\bar{r}-1}(q^m,\bar{r}-1) = \alpha(m,\bar{r}-1)$ such vectors $\mathbf{u}$. Among these vectors, we will enumerate the vectors $\mathbf{t}$ whose last coordinate is a linear combination of the first $\bar{r}-1$ coordinates, that is, $\mathbf{t} = (t_0,\ldots,t_{\bar{r}-2},\sum_{i=0}^{\bar{r}-2}a_i t_i) \in \mathcal{L}_{\bar{r}}$ where $a_i \in \mathrm{GF}(q)$ for $0 \leq i \leq \bar{r}-2$.

Remark that $\mathbf{t} \in \mathcal{L}_{\bar{r}}$ if and only if $(t_0,\ldots,t_{\bar{r}-2}) \cdot (v_0 + a_0 v_{\bar{r}-1},\ldots,v_{\bar{r}-2} + a_{\bar{r}-2}v_{\bar{r}-1}) = 0$. It is easy to check that $\mathbf{v}(\mathbf{a}) = (v_0 + a_0 v_{\bar{r}-1},\ldots,v_{\bar{r}-2} + a_{\bar{r}-2}v_{\bar{r}-1})$ has rank $\bar{r}-1$. Therefore, if $a_0,\ldots,a_{\bar{r}-2}$ are fixed, then there are $A_{\bar{r}-1,\bar{r}-1}$ such vectors $\mathbf{t}$. Also, suppose $\sum_{i=0}^{\bar{r}-2}t_i v_i + v_{\bar{r}-1}\sum_{i=0}^{\bar{r}-2}b_i t_i = 0$. Hence $\sum_{i=0}^{\bar{r}-2}(a_i - b_i)t_i = 0$, which implies $\mathbf{a} = \mathbf{b}$ since t_i's are linearly independent. That is, $\langle\mathbf{v}(\mathbf{a})\rangle^\perp \cap \langle\mathbf{v}(\mathbf{b})\rangle^\perp = \{\mathbf{0}\}$ if $\mathbf{a} \neq \mathbf{b}$. We conclude that there are $q^{\bar{r}-1}A_{\bar{r}-1,\bar{r}-1}$ vectors $\mathbf{t}$. Therefore, $A_{\bar{r},\bar{r}} = \alpha(m,\bar{r}-1) - q^{\bar{r}-1}A_{\bar{r}-1,\bar{r}-1} = q^{-m}[\alpha(m,\bar{r}) + (q^m-1)(-1)^{\bar{r}}q^{\sigma_{\bar{r}}}]$.

Denote the number of vectors with rank p in $\mathcal{L}_r$ as $A_{r,p}$. We have $A_{r,p} = \left[\begin{smallmatrix} r \\ p\end{smallmatrix}\right]A_{p,p}$ [10], and hence $A_{r,p} = \left[\begin{smallmatrix} r \\ p\end{smallmatrix}\right]q^{-m}[\alpha(m,p) + (q^m-1)(-1)^p q^{\sigma_p}]$. Thus, $W^R_{\mathcal{L}_r}(x,y) = \sum_{p=0}^{r}A_{r,p}x^{r-p}y^p = q^{-m}\{[x + (q^m-1)y]^{[r]} + (q^m-1)(x-y)^{[r]}\}$. □

We comment that Proposition 1 in fact provides the rank weight distribution of any $(r,r-1,2)$ MRD code.

Lemma 8. *Let $\mathcal{C}_0 \subseteq \mathrm{GF}(q^m)^r$ be a linear code with rank weight enumerator $W^R_{\mathcal{C}_0}(x,y)$, and for $s \geq 0$, let $W^R_{\mathcal{C}_s}(x,y)$ be the rank weight enumerator of $\mathcal{C}_s \overset{\text{def}}{=} \mathcal{C}_0 \times \mathrm{GF}(q^m)^s$. Then $W^R_{\mathcal{C}_s}(x,y)$ is given by*

$$W^R_{\mathcal{C}_s}(x,y) = W^R_{\mathcal{C}_0}(x,y)*\left[x + (q^m-1)y\right]^{[s]}. \tag{14}$$

Proof. For $s \geq 0$, denote $W^R_{\mathcal{C}_s}(x,y) = \sum_{u=0}^{r+s}B_{s,u}y^u x^{r+s-u}$. We will prove that

$$B_{s,u} = \sum_{i=0}^{u}q^{is}B_{0,i}\begin{bmatrix} s \\ u-i\end{bmatrix}\alpha(m-i,u-i) \tag{15}$$

by induction on s. Equation (15) clearly holds for $s = 0$. Now assume (15) holds for $s = \bar{s}-1$. For any $\mathbf{x}_{\bar{s}} = (x_0,\ldots,x_{r+\bar{s}-1}) \in \mathcal{C}_{\bar{s}}$, we define $\mathbf{x}_{\bar{s}-1} = (x_0,\ldots,x_{r+\bar{s}-2}) \in \mathcal{C}_{\bar{s}-1}$. Then $\mathrm{rk}(\mathbf{x}_{\bar{s}}) = u$ if and only if either $\mathrm{rk}(\mathbf{x}_{\bar{s}-1}) = u$ and

$x_{r+\bar{s}-1} \in \mathfrak{S}(\mathbf{x}_{\bar{s}-1})$ or $\mathrm{rk}(x_{\bar{s}-1}) = u-1$ and $x_{r+\bar{s}-1} \notin \mathfrak{S}(\mathbf{x}_{\bar{s}-1})$. This implies $B_{\bar{s},u} = q^u B_{\bar{s}-1,u} + (q^m - q^{u-1})B_{\bar{s}-1,u-1} = \sum_{i=0}^{u} q^{i\bar{s}} B_{0,i} \left[{\bar{s} \atop u-i} \right] \alpha(m-i, u-i)$. □

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

Proposition 2. *For $\mathbf{v} \in \mathrm{GF}(q^m)^n$ with rank $r \geq 0$, the rank weight enumerator of $\mathscr{L} = \langle \mathbf{v} \rangle^{\perp}$ depends on only r, and is given by*

$$W_{\mathscr{L}}^{R}(x,y) = q^{-m}\{[x + (q^m-1)y]^{[n]} + (q^m-1)(x-y)^{[r]} * [x+(q^m-1)y]^{[n-r]}\}. \tag{16}$$

3.3. MacWilliams identity for the rank metric

Using the results in Section 3.2, we now derive the MacWilliams identity for rank metric codes. Let $\mathcal{C}$ be an (n,k) linear code over $\mathrm{GF}(q^m)$, let $W_{\mathcal{C}}^{R}(x,y) = \sum_{i=0}^{n} A_i y^i x^{n-i}$ be its rank weight enumerator, and let $W_{\mathcal{C}^{\perp}}^{R}(x,y) = \sum_{j=0}^{n} B_j y^j x^{n-j}$ be the rank weight enumerator of its dual code $\mathcal{C}^{\perp}$.

Theorem 1. *For any (n,k) linear code $\mathcal{C}$ and its dual code $\mathcal{C}^{\perp}$ over $\mathrm{GF}(q^m)$,*

$$W_{\mathcal{C}^{\perp}}^{R}(x,y) = \frac{1}{|\mathcal{C}|} \overline{W}_{\mathcal{C}}^{R}(x+(q^m-1)y, x-y), \tag{17}$$

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

$$\sum_{j=0}^{n} B_j y^j x^{n-j} = q^{-mk} \sum_{i=0}^{n} A_i (x-y)^{[i]} * [x+(q^m-1)y]^{[n-i]}. \tag{18}$$

Proof. We have $\mathrm{rk}(\lambda \mathbf{u}) = \mathrm{rk}(\mathbf{u})$ for all $\lambda \in \mathrm{GF}(q^m)^*$ and all $\mathbf{u} \in \mathrm{GF}(q^m)^n$. We want to determine $\hat{f}_R(\mathbf{v})$ for all $\mathbf{v} \in \mathrm{GF}(q^m)^n$. By Definition 2, we can split the summation in (3) into two parts:

$$\hat{f}_R(\mathbf{v}) = \sum_{\mathbf{u} \in \mathscr{L}} \chi(\mathbf{u} \cdot \mathbf{v}) f_R(\mathbf{u}) + \sum_{\mathbf{u} \in F \setminus \mathscr{L}} \chi(\mathbf{u} \cdot \mathbf{v}) f_R(\mathbf{u}), \tag{19}$$

where $\mathscr{L} = \langle \mathbf{v} \rangle^{\perp}$. If $\mathbf{u} \in \mathscr{L}$, then $\chi(\mathbf{u} \cdot \mathbf{v}) = 1$ by Definition 1, and the first summation is equal to $W_{\mathscr{L}}^{R}(x,y)$. For the second summation, we divide vectors into groups of the form $\{\lambda \mathbf{u}_1\}$, where $\lambda \in \mathrm{GF}(q^m)^*$ and $\mathbf{u}_1 \cdot \mathbf{v} = 1$. We remark that for $\mathbf{u} \in F \setminus \mathscr{L}$ (see [1, Chapter 5, Lemma 9]):

$$\sum_{\lambda \in \mathrm{GF}(q^m)^*} \chi(\lambda \mathbf{u}_1 \cdot \mathbf{v}) f_R(\lambda \mathbf{u}_1) = f_R(\mathbf{u}_1) \sum_{\lambda \in \mathrm{GF}(q^m)^*} \chi(\lambda) = -f_R(\mathbf{u}_1). \tag{20}$$

Hence the second summation is equal to $(-1/(q^m-1)) W_{F\setminus\mathscr{L}}^{R}(x,y)$. This leads to $\hat{f}_R(\mathbf{v}) = (1/(q^m-1))[q^m W_{\mathscr{L}}^{R}(x,y) - W_{F}^{R}(x,y)]$. Using $W_{F}^{R}(x,y) = [x+(q^m-1)y]^{[n]}$ and Proposition 2, we obtain $\hat{f}_R(\mathbf{v}) = (x-y)^{[r]} * [x+(q^m-1)y]^{[n-r]}$, where $r = \mathrm{rk}(\mathbf{v})$.

By [1, Chapter 5, Lemma 11], any mapping f from F to $\mathbb{C}$ satisfies $\sum_{\mathbf{v} \in \mathcal{C}^{\perp}} f(\mathbf{v}) = (1/|\mathcal{C}|) \sum_{\mathbf{v} \in \mathcal{C}} \hat{f}(\mathbf{v})$. Applying this result to $f_R(\mathbf{v})$ and using Definition 4, we obtain (17) and (18). □

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

Corollary 1. *It holds that*

$$B_j = \frac{1}{|\mathcal{C}|} \sum_{i=0}^{n} A_i P_j(i; m, n), \tag{21}$$

where

$$P_j(i;m,n) \overset{\text{def}}{=} \sum_{l=0}^{j} \begin{bmatrix} i \\ l \end{bmatrix} \begin{bmatrix} n-i \\ j-l \end{bmatrix} (-1)^l q^{\sigma_l} q^{l(n-i)} \alpha(m-l, j-l). \tag{22}$$

Proof. We have $(x-y)^{[i]} * (x+(q^m-1)y)^{[n-i]} = \sum_{j=0}^{n} P_j(i; m,n) y^j x^{n-j}$. The result follows Theorem 1. □

Note that although the analytical expression in (21) is similar to that in [4, (3.14)], $P_j(i;m,n)$ in (22) are different from $P_j(i)$ in [4, (A10)] and their alternative forms in [29]. We can show the following:

Proposition 3. *$P_j(x;m,n)$ in (22) are the generalized Krawtchouk polynomials.*

The proof is given in Appendix C. Proposition 3 shows that $P_j(x;m,n)$ in (22) are an alternative form for $P_j(i)$ in [4, (A10)], and hence our results in Corollary 1 are equivalent to those in [4, Theorem 3.3]. Also, it was pointed out in [29] that $P_j(x;m,n)/P_j(0;m,n)$ is actually a basic hypergeometric function.

4. MOMENTS OF THE RANK DISTRIBUTION

4.1. Binomial moments of the rank distribution

In this section, 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 [1, page 131].

Proposition 4. *For $0 \leq \nu \leq n$,*

$$\sum_{i=0}^{n-\nu} \begin{bmatrix} n-i \\ \nu \end{bmatrix} A_i = q^{m(k-\nu)} \sum_{j=0}^{\nu} \begin{bmatrix} n-j \\ n-\nu \end{bmatrix} B_j. \tag{23}$$

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

$$\sum_{i=0}^{n} A_i y^i x^{n-i} = q^{m(k-n)} \sum_{j=0}^{n} B_j b_j(x,y;m) * a_{n-j}(x,y;m). \tag{24}$$

Next, we apply the q-derivative with respect to x to (24) ν times. By Lemma 3 the left-hand side (LHS) becomes $\sum_{i=0}^{n-\nu}\beta(n-i,\nu)A_i y^i x^{n-i-\nu}$, while the RHS reduces to $q^{m(k-n)}\sum_{j=0}^{n}B_j\psi_j(x,y)$ by Lemma 4, where

$$\begin{aligned}\psi_j(x,y) &\overset{\text{def}}{=} \left[b_j(x,y;m)*a_{n-j}(x,y;m)\right]^{(\nu)}\\ &= \sum_{l=0}^{\nu}\begin{bmatrix}\nu\\ l\end{bmatrix} q^{(\nu-l)(j-l)} b_j^{(l)}(x,y)*a_{n-j}^{(\nu-l)}(x,y;m).\end{aligned} \tag{25}$$

By Lemma 3, $b_j^{(l)}(x,y;m)=\beta(j,l)(x-y)^{[j-l]}$ and $a_{n-j}^{(\nu-l)}(x,y;m)=\beta(n-j,\nu-l)a_{n-j-\nu+l}(x,y;m)$. It can be verified that for any homogeneous polynomial $b(x,y;m)$ and for any $s\geq 0$, $(b*a_s)(1,1;m)=q^{ms}b(1,1;m)$. Also, for $x=y=1$, $b_j^{(l)}(1,1;m)=\beta(j,j)\delta_{j,l}$. We hence have $\psi_j(1,1)=0$ for $j>\nu$, and $\psi_j(1,1)=\genfrac{[}{]}{0pt}{}{\nu}{j}\beta(j,j)\beta(n-j,\nu-j)q^{m(n-\nu)}$ for $j\leq\nu$. Since $\beta(n-j,\nu-j)=\genfrac{[}{]}{0pt}{}{n-j}{\nu-j}\beta(\nu-j,\nu-j)$ and $\beta(\nu,\nu)=\genfrac{[}{]}{0pt}{}{\nu}{j}\beta(j,j)\beta(\nu-j,\nu-j)$, then $\psi_j(1,1)=\genfrac{[}{]}{0pt}{}{n-j}{\nu-j}\beta(\nu,\nu)q^{m(n-\nu)}$. Applying $x=y=1$ to the LHS and rearranging both sides using $\beta(n-i,\nu)=\genfrac{[}{]}{0pt}{}{n-i}{\nu}\beta(\nu,\nu)$, we obtain (23). □

Proposition 4 can be simplified if ν is less than the minimum distance of the dual code.

Corollary 2. *Let d'_R be the minimum rank distance of $\mathcal{C}^{\perp}$. If $0\leq\nu<d'_R$, then*

$$\sum_{i=0}^{n-\nu}\begin{bmatrix}n-i\\ \nu\end{bmatrix}A_i = q^{m(k-\nu)}\begin{bmatrix}n\\ \nu\end{bmatrix}. \tag{26}$$

Proof. We have $B_0=1$ and $B_1=\cdots=B_\nu=0$. □

Using the q^{-1}-derivative, we obtain another identity.

Proposition 5. *For $0\leq\nu\leq n$,*

$$\begin{aligned}&\sum_{i=\nu}^{n}\begin{bmatrix}i\\ \nu\end{bmatrix}q^{\nu(n-i)}A_i\\ &\quad= q^{m(k-\nu)}\sum_{j=0}^{\nu}\begin{bmatrix}n-j\\ n-\nu\end{bmatrix}(-1)^j q^{\sigma_j}\alpha(m-j,\nu-j)q^{j(\nu-j)}B_j.\end{aligned} \tag{27}$$

The proof of Proposition 5 is similar to that of Proposition 4, and is given in Appendix D. Following [1], we refer to the LHS of (23) and (27) as binomial moments of the rank distribution of $\mathcal{C}$. Similarly, when either ν is less than the minimum distance d'_R of the dual code, or ν is greater than the diameter (maximum distance between any two codewords) δ'_R of the dual code, Proposition 5 can be simplified.

Corollary 3. *If $0\leq\nu<d'_R$, then*

$$\sum_{i=\nu}^{n}\begin{bmatrix}i\\ \nu\end{bmatrix}q^{\nu(n-i)}A_i = q^{m(k-\nu)}\begin{bmatrix}n\\ \nu\end{bmatrix}\alpha(m,\nu). \tag{28}$$

For $\delta'_R<\nu\leq n$,

$$\sum_{i=0}^{\nu}\begin{bmatrix}n-i\\ n-\nu\end{bmatrix}(-1)^i q^{\sigma_i}\alpha(m-i,\nu-i)q^{i(\nu-i)}A_i = 0. \tag{29}$$

Proof. Apply Proposition 5 to $\mathcal{C}$, and use $B_1=\cdots=B_\nu=0$ to prove (28). Apply Proposition 5 to $\mathcal{C}^{\perp}$, and use $B_\nu=\cdots=B_n=0$ to prove (29). □

4.2. *Pless identities for the rank distribution*

In this section, we consider the analogues of the Pless identities [1, 2], in terms of Stirling numbers. The q-Stirling numbers of the second kind $S_q(\nu,l)$ are defined [30] to be

$$S_q(\nu,l) \overset{\text{def}}{=} \frac{q^{-\sigma_l}}{\beta(l,l)}\sum_{i=0}^{l}(-1)^i q^{\sigma_i}\begin{bmatrix}l\\ i\end{bmatrix}\begin{bmatrix}l-i\\ 1\end{bmatrix}^{\nu}, \tag{30}$$

and they satisfy

$$\begin{bmatrix}m\\ 1\end{bmatrix}^{\nu} = \sum_{l=0}^{\nu}q^{\sigma_l}S_q(\nu,l)\beta(m,l). \tag{31}$$

The following proposition can be viewed as a q-analogue of the Pless identity with respect to x [2, P_2].

Proposition 6. *For $0\leq\nu\leq n$,*

$$q^{-mk}\sum_{i=0}^{n}\begin{bmatrix}n-i\\ 1\end{bmatrix}^{\nu}A_i = \sum_{j=0}^{\nu}B_j\sum_{l=0}^{\nu}\begin{bmatrix}n-j\\ n-l\end{bmatrix}\beta(l,l)S_q(\nu,l)q^{-ml+\sigma_l}. \tag{32}$$

Proof. We have

$$\begin{aligned}\sum_{i=0}^{n}\begin{bmatrix}n-i\\ 1\end{bmatrix}^{\nu}A_i &= \sum_{i=0}^{n}A_i\sum_{l=0}^{\nu}q^{\sigma_l}S_q(\nu,l)\begin{bmatrix}n-i\\ l\end{bmatrix}\beta(l,l) \qquad (33)\\ &= \sum_{l=0}^{\nu}q^{\sigma_l}\beta(l,l)S_q(\nu,l)\sum_{i=0}^{n}\begin{bmatrix}n-i\\ l\end{bmatrix}A_i\\ &= \sum_{l=0}^{\nu}q^{\sigma_l}\beta(l,l)S_q(\nu,l)q^{m(k-l)}\sum_{j=0}^{l}\begin{bmatrix}n-j\\ n-l\end{bmatrix}B_j\\ &= q^{mk}\sum_{j=0}^{\nu}B_j\sum_{l=0}^{\nu}\begin{bmatrix}n-j\\ n-l\end{bmatrix}q^{\sigma_l}\beta(l,l)S_q(\nu,l)q^{-ml}, \qquad (34)\end{aligned}$$

where (33) follows (31) and (34) is due to Proposition 4. □

Proposition 6 can be simplified when ν is less than the minimum distance of the dual code.

Corollary 4. *For $0\leq\nu<d'_R$,*

$$\begin{aligned}q^{-mk}\sum_{i=0}^{n}\begin{bmatrix}n-i\\ 1\end{bmatrix}^{\nu}A_i &= \sum_{l=0}^{\nu}\beta(n,l)S_q(\nu,l)q^{-ml+\sigma_l} \qquad (35)\\ &= q^{-mn}\sum_{i=0}^{n}\begin{bmatrix}n-i\\ 1\end{bmatrix}^{\nu}\begin{bmatrix}n\\ i\end{bmatrix}\alpha(m,i). \qquad (36)\end{aligned}$$

Proof. Since $B_0 = 1$ and $B_1 = \cdots = B_\nu = 0$, (32) directly leads to (35). Since the right-hand side of (35) is transparent to the code, without loss of generality we choose $\mathcal{C} = \mathrm{GF}(q^m)^n$ and (36) follows naturally. □

Unfortunately, a q-analogue of the Pless identity with respect to y [2, P$_1$] cannot be obtained due to the presence of the $q^{\nu(n-i)}$ term in the LHS of (27). Instead, we derive its q^{-1}-analogue. We denote $p \overset{\text{def}}{=} q^{-1}$ and define the functions $\alpha_p(m,u)$, $\begin{bmatrix} n \\ u \end{bmatrix}_p$, $\beta_p(m,u)$ similarly to the functions introduced in Section 2.3, only replacing q by p. It is easy to relate these q^{-1}-functions to their counterparts: $\alpha(m,u) = p^{-mu-\sigma_u}(-1)^u\alpha_p(m,u)$, $\begin{bmatrix} n \\ u \end{bmatrix} = p^{-u(n-u)}\begin{bmatrix} n \\ u \end{bmatrix}_p$, and $\beta(m,u) = p^{-u(m-u)-\sigma_u}\beta_p(m,u)$.

Proposition 7. *For* $0 \le \nu \le n$,

$$p^{mk}\sum_{i=0}^{n}\begin{bmatrix} i \\ 1 \end{bmatrix}_p^{\nu} A_i$$
$$=\sum_{j=0}^{\nu} B_j p^{j(m+n-j)}\sum_{l=j}^{\nu}\beta_p(l,l)S_p(\nu,l)(-1)^l\begin{bmatrix} n-j \\ n-l \end{bmatrix}_p\alpha_p(m-j,l-j). \tag{37}$$

The proof of Proposition 7 is given in Appendix E.

Corollary 5. *For* $0 \le \nu < d'_R$,

$$p^{mk}\sum_{i=0}^{n}\begin{bmatrix} i \\ 1 \end{bmatrix}_p^{\nu} A_i = \sum_{l=0}^{\nu}\beta_p(n,l)S_p(\nu,l)\alpha_p(m,l)(-1)^l. \tag{38}$$

Proof. Note that $B_0 = 1$ and $B_1 = \cdots = B_\nu = 0$. □

4.3. Further results on the rank distribution

For nonnegative integers λ, μ, and ν, and a linear code $\mathcal{C}$ with rank weight distribution $\{A_i\}$, we define

$$T_{\lambda,\mu,\nu}(\mathcal{C}) \overset{\text{def}}{=} q^{-mk}\sum_{i=0}^{n}\begin{bmatrix} i \\ \lambda \end{bmatrix}^{\mu} q^{\nu(n-i)}A_i, \tag{39}$$

whose properties are studied below. We refer to

$$T_{0,0,\nu}(\mathcal{C}) \overset{\text{def}}{=} q^{-mk}\sum_{i=0}^{n} q^{\nu(n-i)}A_i \tag{40}$$

as the νth *q-moment* of the rank distribution of $\mathcal{C}$. We remark that for any code $\mathcal{C}$, the 0th order q-moment of its rank distribution is equal to 1. We first relate $T_{\lambda,1,\nu}(\mathcal{C})$ and $T_{1,\mu,\nu}(\mathcal{C})$ to $T_{0,0,\nu}(\mathcal{C})$.

Lemma 9. *For nonnegative integers λ, μ, and ν,*

$$T_{\lambda,1,\nu}(\mathcal{C}) = \frac{1}{\alpha(\lambda,\lambda)}\sum_{l=0}^{\lambda}\begin{bmatrix} \lambda \\ l \end{bmatrix}(-1)^l q^{\sigma_l} q^{n(\lambda-l)}T_{0,0,\nu-\lambda+l}(\mathcal{C}), \tag{41}$$

$$T_{1,\mu,\nu}(\mathcal{C}) = (1-q)^{-\mu}\sum_{a=0}^{\mu}\binom{\mu}{a}(-1)^a q^{an}T_{0,0,\nu-a}(\mathcal{C}). \tag{42}$$

The proof of Lemma 9 is given in Appendix F. We now consider the case where ν is less than the minimum distance of the dual code.

Proposition 8. *For* $0 \le \nu < d'_R$,

$$T_{0,0,\nu}(\mathcal{C}) = \sum_{j=0}^{\nu}\begin{bmatrix} \nu \\ j \end{bmatrix}\alpha(n,j)q^{-mj} \tag{43}$$

$$= q^{-mn}\sum_{i=0}^{n}\begin{bmatrix} n \\ i \end{bmatrix}\alpha(m,i)q^{\nu(n-i)} \tag{44}$$

$$= q^{-m\nu}\sum_{l=0}^{\nu}\begin{bmatrix} \nu \\ l \end{bmatrix}\alpha(m,l)q^{n(\nu-l)}. \tag{45}$$

The proof of Proposition 8 is given in Appendix G. Proposition 8 hence shows that the νth q-moment of the rank distribution of a code is transparent to the code when $\nu < d'_R$. As a corollary, we show that $T_{\lambda,1,\nu}(\mathcal{C})$ and $T_{1,\mu,\nu}(\mathcal{C})$ are also transparent to the code when $0 \le \lambda, \mu \le \nu < d'_R$.

Corollary 6. *For* $0 \le \lambda, \mu \le \nu < d'_R$,

$$\begin{aligned} T_{\lambda,1,\nu}(\mathcal{C}) &= q^{-mn}\begin{bmatrix} n \\ \lambda \end{bmatrix}\sum_{i=\lambda}^{n}\begin{bmatrix} n-\lambda \\ i-\lambda \end{bmatrix} q^{\nu(n-i)}\alpha(m,i), \\ T_{1,\mu,\nu}(\mathcal{C}) &= q^{-mn}\sum_{i=0}^{n}\begin{bmatrix} i \\ 1 \end{bmatrix}^{\mu} q^{\nu(n-i)}\begin{bmatrix} n \\ i \end{bmatrix}\alpha(m,i). \end{aligned} \tag{46}$$

Proof. By Lemma 9 and Proposition 8, $T_{\lambda,1,\nu}(\mathcal{C})$ and $T_{1,\mu,\nu}(\mathcal{C})$ are transparent to the code. Thus, without loss of generality we assume $\mathcal{C} = \mathrm{GF}(q^m)^n$ and (46) follows. □

4.4. Rank weight distribution of MRD codes

The rank weight distribution of linear Class-I MRD codes was given in [4, 10]. Based on our results in Section 4.1, we provide an alternative derivation of the rank distribution of linear Class-I MRD codes, which can also be used to determine the rank weight distribution of Class-II MRD codes.

Proposition 9 (rank distribution of linear Class-I MRD codes). *Let $\mathcal{C}$ be an (n,k,d_R) linear Class-I MRD code over* $\mathrm{GF}(q^m)(n \le m)$*, 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* $0 \le i \le n - d_R$,

$$A_{d_R+i} = \begin{bmatrix} n \\ d_R+i \end{bmatrix}\sum_{j=0}^{i}(-1)^{i-j}q^{\sigma_{i-j}}\begin{bmatrix} d_R+i \\ d_R+j \end{bmatrix}\left(q^{m(j+1)}-1\right). \tag{47}$$

Proof. It can be shown that for two sequences of real numbers $\{a_j\}_{j=0}^{l}$ and $\{b_i\}_{i=0}^{l}$ such that $a_j = \sum_{i=0}^{j}\begin{bmatrix} l-i \\ l-j \end{bmatrix}b_i$ for $0 \le j \le l$, we have $b_i = \sum_{j=0}^{i}(-1)^{i-j}q^{\sigma_{i-j}}\begin{bmatrix} l-j \\ l-i \end{bmatrix}a_j$ for $0 \le i \le l$.

By Corollary 2, we have $\sum_{i=0}^{j}\begin{bmatrix} n-d_R-i \\ n-d_R-j \end{bmatrix}A_{d_R+i} = \begin{bmatrix} n \\ n-d_R-j \end{bmatrix}(q^{m(j+1)}-1)$ for $0 \le j \le n-d_R$. Applying the result above to $l = n-d_R$,

$a_j = [{n \atop n-d_R-j}](q^{m(j+1)}-1)$, and $b_i = A_{d_R+i}$, we obtain

$$A_{d_R+i} = \sum_{j=0}^{i}(-1)^{i-j}q^{\sigma_{i-j}}\begin{bmatrix} n \\ d_R+i\end{bmatrix}\begin{bmatrix} d_R+i \\ d_R+j\end{bmatrix}(q^{m(j+1)}-1). \tag{48}$$

□

We remark that the above rank distribution is consistent with that derived in [4, 10]. Since Class-II MRD codes can be constructed by transposing linear Class-I MRD codes and the transposition operation preserves the rank weight, the weight distributions Class-II MRD codes can be obtained accordingly.

APPENDICES

The proofs in this section use some well-known properties of Gaussian polynomials [27]: $[{n \atop k}] = [{n \atop n-k}]$, $[{n \atop k}][{k \atop l}] = [{n \atop l}][{n-l \atop n-k}]$, and

$$\begin{bmatrix} n \\ k\end{bmatrix} = \begin{bmatrix} n-1 \\ k\end{bmatrix} + q^{n-k}\begin{bmatrix} n-1 \\ k-1\end{bmatrix} \tag{A.1}$$

$$= q^k\begin{bmatrix} n-1 \\ k\end{bmatrix} + \begin{bmatrix} n-1 \\ k-1\end{bmatrix} \tag{A.2}$$

$$= \frac{q^n-1}{q^{n-k}-1}\begin{bmatrix} n-1 \\ k\end{bmatrix} \tag{A.3}$$

$$= \frac{q^{n-k+1}-1}{q^k-1}\begin{bmatrix} n \\ k-1\end{bmatrix}. \tag{A.4}$$

A. PROOF OF LEMMA 4

We consider homogeneous polynomials $f(x,y;m) = \sum_{i=0}^{r} f_i y^i x^{r-i}$ and $u(x,y;m) = \sum_{i=0}^{r} u_i y^i x^{r-i}$ of degree r as well as $g(x,y;m) = \sum_{j=0}^{s} g_j y^j x^{s-j}$ and $v(x,y;m) = \sum_{j=0}^{s} v_j y^j x^{s-j}$ of degree s. First, we need a technical lemma.

Lemma 10. *If $u_r = 0$, then*

$$\frac{1}{x}(u(x,y;m)*v(x,y;m)) = \frac{u(x,y;m)}{x}*v(x,y;m). \tag{A.5}$$

If $v_s = 0$, then

$$\frac{1}{x}(u(x,y;m)*v(x,y;m)) = u(x,qy;m)*\frac{v(x,y;m)}{x}. \tag{A.6}$$

Proof. Suppose $u_r = 0$. Then $u(x,y;m)/x = \sum_{i=0}^{r-1} u_i y^i x^{r-1-i}$. Hence

$$\begin{aligned}\frac{u(x,y;m)}{x}*v(x,y;m) &= \sum_{k=0}^{r+s-1}\left(\sum_{l=0}^{k} q^{ls}u_l(m)v_{k-l}(m-l)\right)y^k x^{r+s-1-k} \\ &= \frac{1}{x}(u(x,y;m)*v(x,y;m)).\end{aligned} \tag{A.7}$$

Suppose $v_s = 0$. Then $v(x,y;m)/x = \sum_{j=0}^{s-1} v_j y^j x^{s-1-j}$. Hence

$$\begin{aligned} u(x,qy;m)*\frac{v(x,y;m)}{x} &= \sum_{k=0}^{r+s-1}\left(\sum_{l=0}^{k} q^{l(s-1)}q^l u_l(m)v_{k-l}(m-l)\right)y^k x^{r+s-1-k} \\ &= \frac{1}{x}(u(x,y;m)*v(x,y;m)).\end{aligned} \tag{A.8}$$

□

We now give a proof of Lemma 4.

Proof. In order to simplify notations, we omit the dependence of the polynomials f and g on the parameter m. The proof goes by induction on ν. For $\nu = 0$, the result is trivial. For $\nu = 1$, we have

$$\begin{aligned} &[f(x,y)*g(x,y)]^{(1)} \\ &= \frac{1}{(q-1)x}[f(qx,y)*g(qx,y) - f(qx,y)*g(x,y) \\ &\qquad + f(qx,y)*g(x,y) - f(x,y)*g(x,y)] \\ &= \frac{1}{(q-1)x}[f(qx,y)*(g(qx,y)-g(x,y)) \\ &\qquad + (f(qx,y)-f(x,y))*g(x,y)] \\ &= f(qx,qy)*\frac{g(qx,y)-g(x,y)}{(q-1)x} + \frac{f(qx,y)-f(x,y)}{(q-1)x}*g(x,y), \end{aligned} \tag{A.9}$$

$$= q^r f(x,y)*g^{(1)}(x,y) + f^{(1)}(x,y)*g(x,y), \tag{A.10}$$

where (A.9) follows Lemma 10.

Now suppose (8) is true for $\nu = \overline{\nu}$. In order to further simplify notations, we omit the dependence of the various polynomials in x and y. We have

$$\begin{aligned} &(f*g)^{(\overline{\nu}+1)} \\ &= \sum_{l=0}^{\overline{\nu}}\begin{bmatrix}\overline{\nu} \\ l\end{bmatrix} q^{(\overline{\nu}-l)(r-l)}[f^{(l)}*g^{(\overline{\nu}-l)}]^{(1)} \\ &= \sum_{l=0}^{\overline{\nu}}\begin{bmatrix}\overline{\nu} \\ l\end{bmatrix} q^{(\overline{\nu}-l)(r-l)}(q^{r-l}f^{(l)}*g^{(\overline{\nu}-l+1)} + f^{(l+1)}*g^{(\overline{\nu}-l)}) \end{aligned} \tag{A.11}$$

$$\begin{aligned} &= \sum_{l=0}^{\overline{\nu}}\begin{bmatrix}\overline{\nu} \\ l\end{bmatrix} q^{(\overline{\nu}+1-l)(r-l)}f^{(l)}*g^{(\overline{\nu}-l+1)} \\ &\quad + \sum_{l=1}^{\overline{\nu}+1}\begin{bmatrix}\overline{\nu} \\ l-1\end{bmatrix} q^{(\overline{\nu}+1-l)(r-l+1)}f^{(l)}*g^{(\overline{\nu}-l+1)} \\ &= \sum_{l=1}^{\overline{\nu}}\left(\begin{bmatrix}\overline{\nu} \\ l\end{bmatrix} + q^{\overline{\nu}+1-l}\begin{bmatrix}\overline{\nu} \\ l-1\end{bmatrix}\right)q^{(\overline{\nu}+1-l)(r-l)}f^{(l)} \\ &\quad *g^{(\overline{\nu}-l+1)} + q^{(\overline{\nu}+1)r}f*g^{(\overline{\nu}+1)} + f^{(\overline{\nu}+1)}*g \\ &= \sum_{l=0}^{\overline{\nu}+1}\begin{bmatrix}\overline{\nu}+1 \\ l\end{bmatrix} q^{(\overline{\nu}+1-l)(r-l)}f^{(l)}*g^{(\overline{\nu}-l+1)}, \end{aligned} \tag{A.12}$$

where (A.11) follows (A.10), and (A.12) follows (A.1). □

B. PROOF OF LEMMA 6

We consider homogeneous polynomials $f(x,y;m) = \sum_{i=0}^{r} f_i y^i x^{r-i}$ and $u(x,y;m) = \sum_{i=0}^{r} u_i y^i x^{r-i}$ of degree r as well as $g(x,y;m) = \sum_{j=0}^{s} g_j y^j x^{s-j}$ and $v(x,y;m) = \sum_{j=0}^{s} v_j y^j x^{s-j}$ of degree s. First, we need a technical lemma.

Lemma 11. *If* $u_0 = 0$*, then*

$$\frac{1}{y}(u(x,y;m)*v(x,y;m)) = q^s \frac{u(x,y;m)}{y} * v(x,y;m-1). \tag{B.1}$$

If $v_0 = 0$*, then*

$$\frac{1}{y}(u(x,y;m)*v(x,y;m)) = u(x,qy;m)*\frac{v(x,y;m)}{y}. \tag{B.2}$$

Proof. Suppose $u_0 = 0$. Then $u(x,y;m)/y = \sum_{i=0}^{r-1} u_{i+1} x^{r-1-i} y^i$. Hence

$$\begin{aligned} q^s \frac{u(x,y;m)}{y} * v(x,y;m-1) &= q^s \sum_{k=0}^{r+s-1} \left(\sum_{l=0}^{k} q^{ls} u_{l+1} v_{k-l}(m-1-l) \right) x^{r+s-1-k} y^k \\ &= q^s \sum_{k=1}^{r+s} \left(\sum_{l=1}^{k} q^{(l-1)s} u_l v_{k-l}(m-l) \right) x^{r+s-k} y^{k-1} \\ &= \frac{1}{y}(u(x,y;m)*v(x,y;m)). \end{aligned} \tag{B.3}$$

Suppose $v_0 = 0$. Then $v(x,y;m)/y = \sum_{j=0}^{s-1} v_{j+1} x^{s-1-j} y^j$. Hence

$$\begin{aligned} u(x,qy;m)*\frac{v(x,y;m)}{y} &= \sum_{k=0}^{r+s-1} \left(\sum_{l=0}^{k} q^{l(s-1)} q^l u_l v_{k-l+1}(m-l) \right) x^{r+s-1-k} y^k \\ &= \sum_{k=1}^{r+s} \left(\sum_{l=0}^{k-1} q^{ls} u_l v_{k-l}(m-l) \right) x^{r+s-k} y^{k-1} \\ &= \frac{1}{y}(u(x,y;m)*v(x,y;m)). \end{aligned} \tag{B.4}$$

□

We now give a proof of Lemma 6.

Proof. The proof goes by induction on ν, and is similar to that of Lemma 4. For $\nu = 0$, the result is trivial. For $\nu = 1$ we can easily show, by using Lemma 11, that

$$\begin{aligned} &[f(x,y;m)*g(x,y;m)]^{\{1\}} \\ &= f(x,y;m)*g^{\{1\}}(x,y;m) + q^s f^{\{1\}}(x,y;m)*g(x,y;m-1) \end{aligned} \tag{B.5}$$

It is thus easy to verify the claim by induction on ν. □

C. PROOF OF PROPOSITION 3

Proof. It was shown in [29] that the generalized Krawtchouk polynomials are the only solutions to the recurrence

$$P_{j+1}(i+1;m+1,n+1) = q^{j+1} P_{j+1}(i+1;m,n) - q^j P_j(i;m,n) \tag{C.1}$$

with initial conditions $P_j(0;m,n) = \begin{bmatrix} n \\ j \end{bmatrix} \alpha(m,j)$. Clearly, our polynomials satisfy these initial conditions. We hence show that $P_j(i;m,n)$ satisfy the recurrence in (C.1). We have

$$\begin{aligned} &P_{j+1}(i+1;m+1,n+1) \\ &= \sum_{l=0}^{i+1} \begin{bmatrix} i+1 \\ l \end{bmatrix} \begin{bmatrix} n-i \\ j+1-l \end{bmatrix} (-1)^l q^{\sigma_l} q^{l(n-i)} \alpha(m+1-l, j+1-l) \\ &= \sum_{l=0}^{i+1} \begin{bmatrix} i+1 \\ l \end{bmatrix} \begin{bmatrix} m+1-l \\ j+1-l \end{bmatrix} (-1)^l q^{\sigma_l} q^{l(n-i)} \alpha(n-i, j+1-l) \\ &= \sum_{l=0}^{i+1} \left\{ q^l \begin{bmatrix} i \\ l \end{bmatrix} + \begin{bmatrix} i \\ l-1 \end{bmatrix} \right\} \left\{ q^{j+1-l} \begin{bmatrix} m-l \\ j+1-l \end{bmatrix} + \begin{bmatrix} m-l \\ j-l \end{bmatrix} \right\} \\ &\quad \times (-1)^l q^{\sigma_l} q^{l(n-i)} \alpha(n-i, j+1-l), \end{aligned} \tag{C.2}$$

$$\begin{aligned} &= \sum_{l=0}^{i} \begin{bmatrix} i \\ l \end{bmatrix} q^{j+1} \begin{bmatrix} m-l \\ j+1-l \end{bmatrix} (-1)^l q^{\sigma_l} q^{l(n-i)} \alpha(n-i, j+1-l) \\ &+ \sum_{l=0}^{i} q^l \begin{bmatrix} i \\ l \end{bmatrix} \begin{bmatrix} m-l \\ j-l \end{bmatrix} (-1)^l q^{\sigma_l} q^{l(n-i)} \alpha(n-i, j+1-l) \\ &+ \sum_{l=1}^{i+1} \begin{bmatrix} i \\ l-1 \end{bmatrix} q^{j+1-l} \begin{bmatrix} m-l \\ j+1-l \end{bmatrix} (-1)^l q^{\sigma_l} q^{l(n-i)} \alpha(n-i, j+1-l) \\ &+ \sum_{l=1}^{i+1} \begin{bmatrix} i \\ l-1 \end{bmatrix} \begin{bmatrix} m-l \\ j-l \end{bmatrix} (-1)^l q^{\sigma_l} q^{l(n-i)} \alpha(n-i, j+1-l), \end{aligned} \tag{C.3}$$

where (C.2) follows (A.2). Let us denote the four summations in the right-hand side of (C.3) as A, B, C, and D, respectively. We have $A = q^{j+1} P_{j+1}(i;m,n)$, and

$$B = \sum_{l=0}^{i} \begin{bmatrix} i \\ l \end{bmatrix} \begin{bmatrix} m-l \\ j-l \end{bmatrix} (-1)^l q^{\sigma_l} q^{l(n-i)} \alpha(n-i, j-l) (q^{n-i+l} - q^j), \tag{C.4}$$

$$\begin{aligned} C &= \sum_{l=0}^{i} \begin{bmatrix} i \\ l \end{bmatrix} q^{j-l} \begin{bmatrix} m-l-1 \\ j-l \end{bmatrix} (-1)^{l+1} q^{\sigma_{l+1}} q^{(l+1)(n-i)} \alpha(n-i, j-l) \\ &= -q^{j+n-i} \sum_{l=0}^{i} \begin{bmatrix} i \\ l \end{bmatrix} \begin{bmatrix} m-l \\ j-l \end{bmatrix} (-1)^l q^{\sigma_l} q^{l(n-i)} \alpha(n-i, j-l) \frac{q^{m-j}-1}{q^{m-l}-1}, \end{aligned} \tag{C.5}$$

$$D = -q^{n-i}\sum_{l=0}^{i}\begin{bmatrix} i \\ l \end{bmatrix}\begin{bmatrix} m-l \\ j-l \end{bmatrix}(-1)^l q^{\sigma_l} q^{l(n-i)} \alpha(n-i, j-l) q^l \frac{q^{j-l}-1}{q^{m-l}-1}, \tag{C.6}$$

where (C.5) follows (A.3) and (C.6) follows both (A.3) and (A.4). Combining (C.4), (C.5), and (C.6), we obtain

$$\begin{aligned} B + C + D = &\sum_{l=0}^{i}\begin{bmatrix} i \\ l \end{bmatrix}\begin{bmatrix} m-l \\ j-l \end{bmatrix}(-1)^l q^{\sigma_l} q^{l(n-i)} \alpha(n-i, j-l) \\ &\times \left\{q^{n-i+l} - q^j - q^{n-i}\frac{q^m - q^j}{q^{m-l}-1} - q^{n-i}\frac{q^j - q^l}{q^{m-l}-1}\right\} \\ = &-q^j P_j(i; m, n). \end{aligned} \tag{C.7}$$

□

D. PROOF OF PROPOSITION 5

Before proving Proposition 5, we need two technical lemmas.

Lemma 12. *For all m, ν, and l,*

$$\begin{aligned} \delta(m, \nu, j) &\overset{\text{def}}{=} \sum_{i=0}^{j}\begin{bmatrix} j \\ i \end{bmatrix}(-1)^i q^{\sigma_i}\alpha(m-i, \nu) \\ &= \alpha(\nu, j)\alpha(m-j, \nu-j)q^{j(m-j)}. \end{aligned} \tag{D.1}$$

Proof. The proof goes by induction on j. The claim trivially holds for $j = 0$. Let us suppose it holds for $j = \bar{j}$. We have

$$\begin{aligned} &\delta(m, \nu, \bar{j}+1) \\ &= \sum_{i=0}^{\bar{j}+1}\begin{bmatrix} \bar{j}+1 \\ i \end{bmatrix}(-1)^i q^{\sigma_i}\alpha(m-i, \nu) \\ &= \sum_{i=0}^{\bar{j}+1}\left(q^i\begin{bmatrix} \bar{j} \\ i \end{bmatrix} + \begin{bmatrix} \bar{j} \\ i-1 \end{bmatrix}\right)(-1)^i q^{\sigma_i}\alpha(m-i, \nu) \\ &= \sum_{i=0}^{\bar{j}} q^i\begin{bmatrix} \bar{j} \\ i \end{bmatrix}(-1)^i q^{\sigma_i}\alpha(m-i, \nu) + \sum_{i=1}^{\bar{j}+1}\begin{bmatrix} \bar{j} \\ i-1 \end{bmatrix}(-1)^i q^{\sigma_i}\alpha(m-i, \nu) \\ &= \sum_{i=0}^{\bar{j}} q^i\begin{bmatrix} \bar{j} \\ i \end{bmatrix}(-1)^i q^{\sigma_i}\alpha(m-i, \nu) - \sum_{i=0}^{\bar{j}}\begin{bmatrix} \bar{j} \\ i \end{bmatrix}(-1)^i q^{\sigma_{i+1}}\alpha(m-1-i, \nu) \\ &= \sum_{i=0}^{\bar{j}} q^i\begin{bmatrix} \bar{j} \\ i \end{bmatrix}(-1)^i q^{\sigma_i}\alpha(m-1-i, \nu-1)q^{m-1-i}(q^\nu - 1) \\ &= q^{m-1}(q^\nu - 1)\delta(m-1, \nu-1, \bar{j}) \\ &= \alpha(\nu, \bar{j}+1)\alpha(m-\bar{j}-1, \nu-\bar{j}-1)q^{(\bar{j}+1)(m-\bar{j}-1)}, \end{aligned} \tag{D.2}$$

where (D.2) follows (A.2). □

Lemma 13. *For all n, ν, and j,*

$$\begin{aligned} \theta(n, \nu, j) &\overset{\text{def}}{=} \sum_{l=0}^{j}\begin{bmatrix} j \\ l \end{bmatrix}\begin{bmatrix} n-j \\ \nu-l \end{bmatrix} q^{l(n-\nu)}(-1)^l q^{\sigma_l}\alpha(\nu-l, j-l) \\ &= (-1)^j q^{\sigma_j}\begin{bmatrix} n-j \\ n-\nu \end{bmatrix}. \end{aligned} \tag{D.3}$$

Proof. The proof goes by induction on j. The claim trivially holds for $j = 0$. Let us suppose it holds for $j = \bar{j}$. We have

$$\begin{aligned} &\theta(n, \nu, \bar{j}+1) \\ &= \sum_{l=0}^{\bar{j}+1}\begin{bmatrix} \bar{j}+1 \\ l \end{bmatrix}\begin{bmatrix} n-1-\bar{j} \\ \nu-l \end{bmatrix} q^{l(n-\nu)}(-1)^l q^{\sigma_l}\alpha(\nu-l, \bar{j}+1-l) \\ &= \sum_{l=0}^{\bar{j}+1}\left(\begin{bmatrix} \bar{j} \\ l \end{bmatrix} + q^{\bar{j}+1-l}\begin{bmatrix} \bar{j} \\ l-1 \end{bmatrix}\right)\begin{bmatrix} n-1-\bar{j} \\ \nu-l \end{bmatrix} \\ &\quad\times q^{l(n-\nu)}(-1)^l q^{\sigma_l}\alpha(\nu-l, \bar{j}+1-l) \end{aligned} \tag{D.4}$$

$$\begin{aligned} &= \sum_{l=0}^{\bar{j}}\begin{bmatrix} \bar{j} \\ l \end{bmatrix}\begin{bmatrix} n-1-\bar{j} \\ \nu-l \end{bmatrix} q^{l(n-\nu)}(-1)^l q^{\sigma_l}\alpha(\nu-l, \bar{j}-l)\left(q^{\nu-l} - q^{\bar{j}-l}\right) \\ &\quad+ \sum_{l=1}^{\bar{j}+1} q^{\bar{j}-l+1}\begin{bmatrix} \bar{j} \\ l-1 \end{bmatrix}\begin{bmatrix} n-1-\bar{j} \\ \nu-l \end{bmatrix} q^{l(n-\nu)}(-1)^l q^{\sigma_l}\alpha(\nu-l, \bar{j}-l+1), \end{aligned} \tag{D.5}$$

where (D.4) follows (A.1). Let us denote the first and second summations in the right-hand side of (D.5) as A and B, respectively. We have

$$\begin{aligned} A &= (q^\nu - q^{\bar{j}})\sum_{l=0}^{\bar{j}}\begin{bmatrix} \bar{j} \\ l \end{bmatrix}\begin{bmatrix} n-1-\bar{j} \\ \nu-l \end{bmatrix} q^{l(n-1-\nu)}(-1)^l q^{\sigma_l}\alpha(\nu-l, \bar{j}-l) \\ &= (q^\nu - q^{\bar{j}})\theta(n-1, \nu, \bar{j}) \\ &= (q^\nu - q^{\bar{j}})(-1)^{\bar{j}} q^{\sigma_{\bar{j}}}\begin{bmatrix} n-1-\bar{j} \\ n-1-\nu \end{bmatrix}, \end{aligned} \tag{D.6}$$

$$\begin{aligned} B &= \sum_{l=0}^{\bar{j}} q^{\bar{j}-l}\begin{bmatrix} \bar{j} \\ l \end{bmatrix}\begin{bmatrix} n-1-\bar{j} \\ \nu-1-l \end{bmatrix} q^{(l+1)(n-\nu)}(-1)^{l+1} q^{\sigma_{l+1}}\alpha(\nu-1-l, \bar{j}-l) \\ &= -q^{\bar{j}+n-\nu}\sum_{l=0}^{\bar{j}}\begin{bmatrix} \bar{j} \\ l \end{bmatrix}\begin{bmatrix} n-1-\bar{j} \\ \nu-1-l \end{bmatrix} q^{l(n-\nu)}(-1)^l q^{\sigma_l}\alpha(\nu-1-l, \bar{j}-l) \\ &= -q^{\bar{j}+n-\nu}\theta(n-1, \nu-1, \bar{j}) \\ &= -q^{\bar{j}+n-\nu}(-1)^{\bar{j}} q^{\sigma_{\bar{j}}}\begin{bmatrix} n-1-\bar{j} \\ n-\nu \end{bmatrix}. \end{aligned} \tag{D.7}$$

Combining (D.4), (D.6), and (D.7), we obtain

$$\begin{aligned}
&\theta(n,\nu,\bar{j}+1)\\
&= (-1)^{\bar{j}} q^{\sigma_{\bar{j}}}\left\{(q^{\nu}-q^{\bar{j}})\begin{bmatrix} n-1-\bar{j} \\ n-1-\nu \end{bmatrix} - q^{\bar{j}+n-\nu}\begin{bmatrix} n-1-\bar{j} \\ n-\nu \end{bmatrix}\right\}\\
&= (-1)^{\bar{j}+1} q^{\sigma_{\bar{j}+1}}\begin{bmatrix} n-1-\bar{j} \\ n-\nu \end{bmatrix}\left\{-(q^{\nu-\bar{j}}-1)\frac{q^{n-\nu}-1}{q^{\nu-\bar{j}}-1}+q^{n-\nu}\right\} \qquad \text{(D.8)}\\
&= (-1)^{\bar{j}+1} q^{\sigma_{\bar{j}+1}}\begin{bmatrix} n-1-\bar{j} \\ n-\nu \end{bmatrix}, \qquad \text{(D.9)}
\end{aligned}$$

where (D.8) follows (A.4). □

We now give a proof of Proposition 5.

Proof. We apply the q^{-1}-derivative with respect to y to (24) ν times, and we apply $x = y = 1$. By Lemma 5, the LHS becomes

$$\sum_{i=\nu}^{n} q^{\nu(1-i)+\sigma_\nu}\beta(i,\nu)A_i = q^{\nu(1-n)+\sigma_\nu}\beta(\nu,\nu)\sum_{i=\nu}^{n}\begin{bmatrix} i \\ \nu \end{bmatrix} q^{\nu(n-i)}A_i. \qquad \text{(D.10)}$$

The RHS becomes $q^{m(k-n)}\sum_{j=0}^{n} B_j\psi_j(1,1)$, where

$$\begin{aligned}
&\psi_j(x,y)\\
&\overset{\text{def}}{=} \left[b_j(x,y;m) * a_{n-j}(x,y;m)\right]^{\{\nu\}}\\
&= \sum_{l=0}^{\nu}\begin{bmatrix} \nu \\ l \end{bmatrix} q^{l(n-j-\nu+l)} b_j^{\{l\}}(x,y;m) * a_{n-j}^{\{\nu-l\}}(x,y;m-l) \qquad \text{(D.11)}\\
&= \sum_{l=0}^{\nu}\begin{bmatrix} \nu \\ l \end{bmatrix} q^{l(n-j-\nu+l)}(-1)^l\beta(j,l)\beta(n-j,\nu-l)q^{-\sigma_{\nu-l}}\\
&\quad \times b_{j-l}(x,y;m) * \alpha(m-l,\nu-l)a_{n-j-\nu+l}(x,y;m-\nu)\\
&= \beta(\nu,\nu)q^{-\sigma_\nu}\sum_{l=0}^{\nu}\begin{bmatrix} j \\ l \end{bmatrix}\begin{bmatrix} n-j \\ \nu-l \end{bmatrix} q^{l(n-j)}(-1)^l q^{\sigma_l}\\
&\quad \times b_{j-l}(x,y;m) * \alpha(m-l,\nu-l)a_{n-j-\nu+l}(x,y;m-\nu), \qquad \text{(D.12)}
\end{aligned}$$

where (D.11) and (D.12) follow Lemmas 6 and 5, respectively.

We have

$$\begin{aligned}
&\left[b_{j-l} * \alpha(m-l,\nu-l)a_{n-j-\nu+l}\right](1,1;m-\nu)\\
&= \sum_{u=0}^{n-\nu}\left[\sum_{i=0}^{u} q^{i(n-j-\nu+l)}\begin{bmatrix} j-l \\ i \end{bmatrix}(-1)^i q^{\sigma_i}\alpha(m-i-l,\nu-l)\right.\\
&\qquad\qquad \left.\times\begin{bmatrix} n-j-\nu+l \\ u-i \end{bmatrix}\alpha(m-\nu-i,u-i)\right]\\
&= q^{(m-\nu)(n-\nu-j+l)}\sum_{i=0}^{j-l}\begin{bmatrix} j-l \\ i \end{bmatrix}(-1)^i q^{\sigma_i}\alpha(m-l-i,\nu-l)\\
&= q^{(m-\nu)(n-\nu-j+l)}\alpha(\nu-l,j-l)\alpha(m-j,\nu-j)q^{(j-l)(m-j)}, \qquad \text{(D.13)}
\end{aligned}$$

where (D.13) follows Lemma 12. Hence

$$\begin{aligned}
&\psi_j(1,1)\\
&= \beta(\nu,\nu)q^{m(n-\nu)+\nu(1-n)+\sigma_\nu}\alpha(m-j,\nu-j)q^{j(\nu-j)}\\
&\qquad \cdots\sum_{l=0}^{j}\begin{bmatrix} j \\ l \end{bmatrix}\begin{bmatrix} n-j \\ \nu-l \end{bmatrix} q^{l(n-\nu)}(-1)^l q^{\sigma_l}\alpha(\nu-l,j-l)\\
&= \beta(\nu,\nu)q^{m(n-\nu)+\nu(1-n)+\sigma_\nu}\alpha(m-j,\nu-j)q^{j(\nu-j)}(-1)^j q^{\sigma_j}\begin{bmatrix} n-j \\ n-\nu \end{bmatrix}, \qquad \text{(D.14)}
\end{aligned}$$

where (D.14) follows Lemma 13. Incorporating this expression for $\psi_j(1,1)$ in the definition of the RHS and rearranging both sides, we obtain the result. □

E. PROOF OF PROPOSITION 7

Proof. Equation (27) can be expressed in terms of the $\alpha_p(m,u)$ and $\left[\begin{smallmatrix} n \\ u \end{smallmatrix}\right]_p$ functions as

$$\begin{aligned}
&\sum_{i=\nu}^{n}\begin{bmatrix} i \\ \nu \end{bmatrix}_p A_i\\
&\quad = (-1)^{\nu}p^{-mk-\sigma_\nu}\sum_{j=0}^{\nu}\begin{bmatrix} n-j \\ n-\nu \end{bmatrix}_p p^{j(m+n-j)}\alpha_p(m-j,\nu-j)B_j. \qquad \text{(E.1)}
\end{aligned}$$

We obtain

$$\begin{aligned}
&p^{mk}\sum_{i=0}^{n}\begin{bmatrix} j \\ 1 \end{bmatrix}_p^{\nu} A_i\\
&= p^{mk}\sum_{l=0}^{\nu}p^{\sigma_l}\beta_p(l,l)S_p(\nu,l)\sum_{i=l}^{n}\begin{bmatrix} i \\ l \end{bmatrix}_p A_i \qquad \text{(E.2)}\\
&= \sum_{l=0}^{\nu}\beta_p(l,l)S_p(\nu,l)(-1)^l\sum_{j=0}^{l}\begin{bmatrix} n-j \\ n-l \end{bmatrix}_p p^{j(m+n-j)}\alpha_p(m-j,l-j)B_j\\
&= \sum_{j=0}^{\nu}B_j p^{j(m+n-j)}\sum_{l=j}^{\nu}\beta_p(l,l)S_p(\nu,l)(-1)^l\begin{bmatrix} n-j \\ n-l \end{bmatrix}_p\alpha_p(m-j,l-j), \qquad \text{(E.3)}
\end{aligned}$$

where (E.2) and (E.3) follow (31) and (E.1), respectively. □

F. PROOF OF LEMMA 9

Proof. We first prove (41):

$$\begin{aligned}
&q^{-mk}\sum_{i=0}^{n}\begin{bmatrix} i \\ \lambda \end{bmatrix} q^{\nu(n-i)}A_i\\
&= \frac{q^{-mk}}{\alpha(\lambda,\lambda)}\sum_{i=0}^{n}q^{\nu(n-i)}A_i\sum_{l=0}^{\lambda}\begin{bmatrix} \lambda \\ l \end{bmatrix}(-1)^l q^{\sigma_l}q^{i(\lambda-l)}\\
&= \frac{q^{-mk}}{\alpha(\lambda,\lambda)}\sum_{l=0}^{\lambda}\begin{bmatrix} \lambda \\ l \end{bmatrix}(-1)^l q^{\sigma_l}q^{n(\lambda-l)}\sum_{i=0}^{n}q^{(\nu-\lambda+l)(n-i)}A_i \qquad \text{(F.1)}\\
&= \frac{1}{\alpha(\lambda,\lambda)}\sum_{l=0}^{\lambda}\begin{bmatrix} \lambda \\ l \end{bmatrix}(-1)^l q^{\sigma_l}q^{n(\lambda-l)}T_{0,0,\nu-\lambda+l}(\mathfrak{C}),
\end{aligned}$$

where (F.1) follows $\alpha(i,\lambda) = \sum_{l=0}^{\lambda}\left[{\lambda \atop l}\right](-1)^l q^{\sigma_l} q^{i(\lambda-l)}$. We now prove (42): since

$$\begin{bmatrix} i \\ 1 \end{bmatrix}^{\mu} = \left(\frac{1-q^i}{1-q}\right)^{\mu} = \frac{1}{(1-q)^{\mu}}\sum_{a=0}^{\mu}\binom{\mu}{a}(-1)^a q^{ia}, \tag{F.2}$$

we obtain

$$\begin{aligned} T_{1,\mu,\nu}(\mathcal{C}) &= \frac{q^{-mk}}{(1-q)^{\mu}}\sum_{i=0}^{n} q^{\nu(n-i)} A_i \sum_{a=0}^{\mu}\binom{\mu}{a}(-1)^a q^{ia} \\ &= \frac{q^{-mk}}{(1-q)^{\mu}}\sum_{a=0}^{\mu}\binom{\mu}{a}(-1)^a q^{an}\sum_{i=0}^{n} q^{(\nu-a)(n-i)} A_i \\ &= (1-q)^{-\mu}\sum_{a=0}^{\mu}\binom{\mu}{a}(-1)^a q^{an} T_{0,0,\nu-a}(\mathcal{C}). \end{aligned} \tag{F.3}$$

□

G. PROOF OF PROPOSITION 8

Proof. From [27, (3.3.6)], we obtain $\left[{n-i \atop \nu}\right] = (1/\alpha(\nu,\nu)) \times \sum_{l=0}^{\nu}\left[{\nu \atop l}\right](-1)^{\nu-l} q^{\sigma_{\nu-l}} q^{l(n-i)}$, and hence

$$\begin{aligned} & q^{-mk}\sum_{i=0}^{n}\begin{bmatrix} n-i \\ \nu \end{bmatrix} A_i \\ &\quad = q^{-mk}\sum_{i=0}^{n} A_i \frac{1}{\alpha(\nu,\nu)}\sum_{l=0}^{\nu}\begin{bmatrix} \nu \\ l \end{bmatrix}(-1)^{\nu-l} q^{\sigma_{\nu-l}} q^{l(n-i)} \\ &\quad = \frac{q^{-mk}}{\alpha(\nu,\nu)}\sum_{l=0}^{\nu}\begin{bmatrix} \nu \\ l \end{bmatrix}(-1)^{\nu-l} q^{\sigma_{\nu-l}}\sum_{i=0}^{n} q^{l(n-i)} A_i \qquad \text{(G.1)} \\ &\quad = \frac{1}{\alpha(\nu,\nu)}\sum_{l=0}^{\nu}\begin{bmatrix} \nu \\ l \end{bmatrix}(-1)^{\nu-l} q^{\sigma_{\nu-l}} T_{0,0,l}(\mathcal{C}), \end{aligned}$$

where (G.1) follows (40). By Corollary 2, we have for $\nu < d'_R$, $\sum_{l=0}^{\nu}\left[{\nu \atop l}\right](-1)^{\nu-l} q^{\sigma_{\nu-l}} T_{0,0,l}(\mathcal{C}) = q^{-m\nu}\alpha(n,\nu)$, and we obtain

$$\begin{aligned} \sum_{j=0}^{\nu}\begin{bmatrix} \nu \\ j \end{bmatrix}\alpha(n,j) q^{-mj} &= \sum_{j=0}^{\nu}\begin{bmatrix} \nu \\ j \end{bmatrix}\sum_{l=0}^{j}\begin{bmatrix} j \\ l \end{bmatrix}(-1)^{j-l} q^{\sigma_{j-l}} T_{0,0,l}(\mathcal{C}) \\ &= \sum_{l=0}^{\nu} T_{0,0,l}(\mathcal{C})\begin{bmatrix} \nu \\ l \end{bmatrix}\sum_{j=0}^{\nu}\begin{bmatrix} \nu-l \\ j-l \end{bmatrix}(-1)^{j-l} q^{\sigma_{j-l}} \\ &= T_{0,0,\nu}(\mathcal{C}), \end{aligned} \tag{G.2}$$

where (G.2) follows $\sum_{j=0}^{\nu-l}\left[{\nu-l \atop j}\right](-1)^j q^{\sigma_j} = \delta_{\nu,l}$, which in turn is a special case of [27, (3.3.6)]. This proves (43). Thus, $T_{0,0,\nu}(\mathcal{C})$ is transparent to the code, and (44) can be shown by choosing $\mathcal{C} = \mathrm{GF}(q^m)^n$ without loss of generality.

Suppose $S(\nu,n,m) \overset{\text{def}}{=} \sum_{j=0}^{\nu}\left[{\nu \atop j}\right]\alpha(n,j)q^{-mj}$. Then $S(\nu,n,m) = S(n,\nu,m)$ since $\left[{\nu \atop j}\right]\alpha(n,j) = \left[{n \atop j}\right]\alpha(\nu,j)$. Also, combining (43) and (44) yields $S(\nu,n,m) = q^{n(\nu-m)}S(n,m,\nu)$. Therefore, we obtain $S(\nu,n,m) = q^{\nu(n-m)}S(\nu,m,n)$, which proves (45). □

ACKNOWLEDGMENTS

This work was supported in part by Thales Communications Inc. and in part by a grant from the Commonwealth of Pennsylvania, Department of Community and Economic Development, through the Pennsylvania Infrastructure Technology Alliance (PITA). The material in this paper was presented in part at the IEEE International Symposium on Information Theory, Nice, France, June 24–29, 2007.

REFERENCES

[1] F. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, The Netherlands, 1977.

[2] V. Pless, "Power moment identities on weight distributions in error correcting codes," *Information and Control*, vol. 6, no. 2, pp. 147–152, 1963.

[3] L. Hua, "A theorem on matrices over a field and its applications," *Chinese Mathematical Society*, vol. 1, no. 2, pp. 109–163, 1951.

[4] P. Delsarte, "Bilinear forms over a finite field, with applications to coding theory," *Journal of Combinatorial Theory A*, vol. 25, no. 3, pp. 226–241, 1978.

[5] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: performance criterion and code construction," *IEEE Transactions on Information Theory*, vol. 44, no. 2, pp. 744–765, 1998.

[6] P. Lusina, E. M. Gabidulin, and M. Bossert, "Maximum rank distance codes as space-time codes," *IEEE Transactions on Information Theory*, vol. 49, no. 10, pp. 2757–2760, 2003.

[7] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov, "Ideals over a non-commutative ring and their application in cryptology," in *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques (EUROCRYPT '91)*, vol. 547 of *Lecture Notes in Computer Science*, pp. 482–489, Brighton, UK, April 1991.

[8] E. M. Gabidulin, "Optimal codes correcting lattice-pattern errors," *Problems of Information Transmission*, vol. 21, no. 2, pp. 3–11, 1985.

[9] R. M. Roth, "Maximum-rank array codes and their application to crisscross error correction," *IEEE Transactions on Information Theory*, vol. 37, no. 2, pp. 328–336, 1991.

[10] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Problems of Information Transmission*, vol. 21, no. 1, pp. 1–12, 1985.

[11] K. Chen, "On the non-existence of perfect codes with rank distance," *Mathematische Nachrichten*, vol. 182, no. 1, pp. 89–98, 1996.

[12] R. M. Roth, "Probabilistic crisscross error correction," *IEEE Transactions on Information Theory*, vol. 43, no. 5, pp. 1425–1438, 1997.

[13] W. B. Vasantha and N. Suresh Babu, "On the covering radius of rank-distance codes," *Ganita Sandesh*, vol. 13, pp. 43–48, 1999.

[14] T. P. Berger, "Isometries for rank distance and permutation group of Gabidulin codes," *IEEE Transactions on Information Theory*, vol. 49, no. 11, pp. 3016–3019, 2003.

[15] E. M. Gabidulin and P. Loidreau, "On subcodes of codes in rank metric," in *Proceedings of IEEE International Symposium on Information Theory (ISIT '05)*, pp. 121–123, Adelaide, Australia, September 2005.

[16] A. Kshevetskiy and E. M. Gabidulin, "The new construction of rank codes," in *Proceedings of IEEE International Symposium*

on Information Theory (ISIT '05), pp. 2105–2108, Adelaide, Australia, September 2005.

[17] M. Gadouleau and Z. Yan, "Properties of codes with the rank metric," in *Proceedings of IEEE Global Telecommunications Conference (GLOBECOM '06)*, pp. 1–5, San Francisco, Calif, USA, November 2006.

[18] M. Gadouleau and Z. Yan, "Decoder error probability of MRD codes," in *Proceedings of IEEE Information Theory Workshop (ITW '06)*, pp. 264–268, Chengdu, China, October 2006.

[19] M. Gadouleau and Z. Yan, "On the decoder error probability of bounded rank-distance decoders for maximum rank distance codes," to appear in *IEEE Transactions on Information Theory*.

[20] P. Loidreau, "Properties of codes in rank metric," http://arxiv.org/pdf/cs.DM/0610057/.

[21] M. Schwartz and T. Etzion, "Two-dimensional cluster-correcting codes," *IEEE Transactions on Information Theory*, vol. 51, no. 6, pp. 2121–2132, 2005.

[22] G. Richter and S. Plass, "Fast decoding of rank-codes with rank errors and column erasures," in *Proceedings of IEEE International Symposium on Information Theory (ISIT '04)*, p. 398, Chicago, Ill, USA, June-July 2004.

[23] P. Loidreau, "A Welch-Berlekamp like algorithm for decoding Gabidulin codes," in *Proceedings of the 4th International Workshop on Coding and Cryptography (WCC '05)*, vol. 3969, pp. 36–45, Bergen, Norway, March 2005.

[24] D. Grant and M. Varanasi, "Weight enumerators and a MacWilliams-type identity for space-time rank codes over finite fields," in *Proceedings of the 43rd Allerton Conference on Communication, Control, and Computing*, pp. 2137–2146, Monticello, Ill, USA, October 2005.

[25] D. Grant and M. Varanasi, "Duality theory for space-time codes over finite fields," to appear in *Advance in Mathematics of Communications*.

[26] P. Loidreau, "Étude et optimisation de cryptosystèmes à clé publique fondés sur la théorie des codes correcteurs," Ph.D. dissertation, École Polytechnique, Paris, France, May 2001.

[27] G. E. Andrews, *The Theory of Partitions*, vol. 2 of *Encyclopedia of Mathematics and Its Applications*, Addison-Wesley, Reading, Mass, USA, 1976.

[28] G. Gasper and M. Rahman, *Basic Hypergeometric Series*, vol. 96 of *Encyclopedia of Mathematics and Its Applications*, Cambridge University Press, New York, NY, USA, 2nd edition, 2004.

[29] P. Delsarte, "Properties and applications of the recurrence $F(i+1,k+1,n+1) = q^{k+1}F(i,k+1,n) - q^{k}F(i,k,n)$," *SIAM Journal on Applied Mathematics*, vol. 31, no. 2, pp. 262–270, 1976.

[30] L. Carlitz, "q-Bernoulli numbers and polynomials," *Duke Mathematical Journal*, vol. 15, no. 4, pp. 987–1000, 1948.