Turk J Math
26 (2002) , 465 – 473.

A MacWilliams Type Identity

İrfan Şiap

Abstract

A MacWilliams identity for a ρ complete weight enumerator of linear spaces of matrices with entries from the ring $\mathbb{F}_q[u]/(u^r - a)$, where $a \in \mathbb{F}_q$, endowed with a non-Hamming metric is proved.

Key Words: MacWilliams identity, complete weight enumerator, codes over $\mathbb{F}_q[u]/(u^r - a)$.

1. Introduction

There has been a recent growth of interest in linear codes with respect to a newly defined non-Hamming metric grown as the Rosenbloom-Tsfassman metric (RT, or ρ, in short) [8]. Let $\mathbb{F}_q$ denote a finite field with q elements. A MacWilliams identity for T and H ρ weight enumerators of codes over $\mathcal{M}_{n\times s}(\mathbb{F}_q)$ ($n \times s$ matrices over a finite field with q elements) is proved in [2]. Also, a ρ complete weight enumerator is defined and a MacWilliams identity for the ρ complete weight enumerator of codes over $\mathcal{M}_{n\times s}(\mathbb{F}_q)$ is proved in [6]. MacWilliams identities for the ρ-complete weight enumerator of codes over $\mathbb{Z}_4$ (integers modulo 4) and Galois rings are given in [4] and [9], respectively. In this paper, we prove a MacWilliams identity for linear spaces of matrices with entries from the ring $\mathbb{F}_q[u]/(u^r - a)$, where $a \in \mathbb{F}_q$.

Let R denote the ring $\mathbb{F}_q[u]/(u^r - a)$ where $a \in \mathbb{F}_q$ and r be a positive integer. A new non-Hamming ρ metric on linear spaces over finite fields has been recently introduced in [8]. We state the definitions for $\mathcal{M}_{n\times s}(R)$. Let $A = (a_0, a_1, \ldots , a_{s-1}) \in R^s$. First, we define the ρ weight of A by

2000 Mathematical Subject Classification: 9405,94B60

$$w_N(A) = \begin{cases} \max\{i|a_i \neq 0\} + 1, & a_i \neq 0, \\ 0, & A = \mathbf{0}. \end{cases} \tag{1}$$

Let $A = (a_0, a_1, \ldots, a_{s-1}), B = (b_0, b_1, \ldots, b_{s-1}) \in R^s$.

$$\rho(A, B) = w_N(A - B).$$

Let $P_i = (p_{i0}, p_{i1}, \ldots, p_{i,s-1}), Q_i = (q_{i0}, q_{i1}, \ldots, q_{i,s-1}) \in R^s$. $P = (P_1, P_2, \ldots, P_n)^T$, $Q = (Q_1, Q_2, \ldots, Q_n)^T \in \mathcal{M}_{n\times s}(R)$ where T denotes the transpose of the matrix. Now we extend this definition to matrices. Let

$$\rho(P, Q) = \sum_{i=1}^{n} \rho(P_i, Q_i). \tag{2}$$

ρ is a metric over $\mathcal{M}_{n\times s}(R)$.

Definition 1.1 *An R submodule C of R^n is called a linear code of length n.*

The inner product of P_i and Q_i is defined by

$$\langle P_i, Q_i \rangle = \sum_{j=0}^{s-1} p_{ij} q_{i,s-1-j} \tag{3}$$

and this is extended to inner product of $P = (P_1, P_2, \ldots, P_n)^T$,
$Q = (Q_1, Q_2, \ldots, Q_n)^T \in \mathcal{M}_{n\times s}(R)$ as

$$\langle P, Q \rangle = \sum_{i=1}^{n} \langle P_i, Q_i \rangle. \tag{4}$$

Let $C \subset R$ be a linear code. $w_r(C) = |\{\boldsymbol{u} \in C | w_H(P) = r\}|, \quad 0 \leq r \leq ns$ is called the ρ *weight spectrum* of the code, and the *weight enumerator* ρ is defined by

$$W(C|z) = \sum_{r=0}^{n} w_r(C) z^r = \sum_{P \in C} z^{w_N(P)}. \tag{5}$$

Example 1: Let $R' = \mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 1$. Let C_1, C_2 be two linear codes over $\mathcal{M}_{2\times 2}(R')$ defined as

$$C_1 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} u+1 & 0 \\ u+1 & 0 \end{pmatrix} \right\}, C_2 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & u+1 \\ 0 & 0 \end{pmatrix} \right\}. \tag{6}$$

The ρ weight enumerators of the above codes are the same, i.e $1 + z^2$.

Let $C_1^{\perp}$ and $C_2^{\perp}$ be the dual codes of C_1 and C_2, respectively. Since both $C_1^{\perp}$ and $C_2^{\perp}$ contain 128 elements, we give their weight enumerators only:

$$W(C_1^{\perp} \mid z) = 1 + 6z + 17z^2 + 24z^3 + 80z^4, \text{ and} \tag{7}$$
$$W(C_2^{\perp} \mid z) = 1 + 4z + 21z^2 + 30z^3 + 72z^4.$$

As seen in the above example, although the ρ-weight enumerators of codes C_1 and C_2 are the same, the ρ-weight enumerators of the duals are different. In the field case, the same problem first was seen in [2] where it was resolved by considering the orbits of linear spaces of matrices. In [2], T and H weight enumerators are defined the and MacWilliams identities of these enumerators are proven. To overcome this problem, in the next section we first define a ρ complete weight enumerator and prove its MacWilliams' identity. Further, given the ρ complete weight enumerator of a code one can easily define and determine the T and H weight enumerators for matrices over $\mathbb{F}_q[u]/(u^r - a)$ originally defined in [2] for matrices over fields.

2. The complete weight enumerator

To overcome the problem that occured in the above example, we define a weight enumerator that preserves the order of the entries of the matrices and carries more information about the code. In order to state and prove the identity, we identify a linear space of $n \times s$ matrices with the linear space of $n \times 1$ matrices having polynomial entries and restate the definitions:

$$\varphi_1 : \mathcal{M}_{1\times s}(R) \rightarrow R[x]/(x^s)$$
$$(p_0, p_1, \dots, p_{s-1}) \rightarrow p_0 + p_1 x + \cdots + p_{s-1}x^{s-1}.$$

Let $P_i = (p_{i0}, p_{i1}, \dots, p_{i,s-1})$, and $P = [P_1, \dots, P_n]^T$. We extend φ_1 to

$$\varphi : \mathcal{M}_{n\times s}(R) \rightarrow \mathcal{M}_{n\times 1}(R[x]/(x^s))$$
$$P \rightarrow (p_{00} + p_{01}x + \cdots + p_{0,s-1}x^{s-1}, \dots, p_{n0} + p_{01}x + \cdots + p_{n,s-1}x^{s-1})^T.$$

The maps defined above are R-module isomorphisms. The ρ weight of a polynomial $p(x) \in R[x]/(x^s)$ is simply equal to $\deg(p(x)) + 1$, i.e.

$$w_H(p(x)) = \deg(p(x)) + 1. \tag{8}$$

Let $p(x) = p_0 + \cdots + p_{s-1}x^{s-1} \in R[x]/(x^s)$. The lth $(0 \le l \le s-1)$ coefficient of $p(x)$ is defined by

$$c_l(p(x)) = p_l. \tag{9}$$

Let $P(x) = (P_1(x), \ldots, P_n(x))^T$, and $Q(x) = (Q_1(x), \ldots, Q_n(x))^T \in \mathcal{M}_{n\times s}(R[x]/(x^s))$, where $P_i(x) = p_{i0} + p_{i1}x + \cdots + p_{i,s-1}x^{s-1}$, and $Q_i(x) = q_{i0} + q_{i1}x + \cdots + q_{i,s-1}x^{s-1}$. The inner product of $P(x)$ and $Q(x)$ defined in the previous section becomes

$$\langle P(x), Q(x)\rangle = \sum_{i=0}^{n} c_{s-1}(P_i(x)Q_i(x)). \tag{10}$$

The *Hamming weight* of an element $a \in R$ is defined by

$$w(a) = \begin{cases} 0, & \text{if } a = 0 \\ 1, & \text{otherwise.} \end{cases} \tag{11}$$

Let $C \subset \mathcal{M}_{n\times s}(R)$ be a linear code with size m. For simplification purposes, let $C = \{A^{(0)}, A^{(1)}, \ldots, A^{(m)}\}$. Also, let

$$A^{(i)} = \begin{pmatrix} a_{10}^{(i)} & a_{11}^{(i)} & \ldots & a_{1,s-1}^{(i)} \\ a_{20}^{(i)} & a_{21}^{(i)} & \ldots & a_{2,s-1}^{(i)} \\ & & \vdots & \\ a_{n0}^{(i)} & a_{n1}^{(i)} & \ldots & a_{n,s-1}^{(i)} \end{pmatrix}, \qquad 0 \le i \le m.$$

Let

$$Y_{ns} = (y_{10}, \ldots, y_{1,s-1}, \ldots, y_{n0}, \ldots, y_{n,s-1}).$$

We define the *complete ρ weight enumerator* of a code C by

$$W_C(Y_{ns}) = \sum_{i=0}^{m} y_{10}^{w(a_{10}^{(i)})} \cdots y_{1,s-1}^{w(a_{1,s-1}^{(i)})} \cdots y_{n0}^{w(a_{n0}^{(i)})} \cdots y_{n,s-1}^{w(a_{n,s-1}^{(i)})}. \tag{12}$$

Note that the complete ρ weight enumerator is a polynomial of ns variables. Further, it is possible to obtain the ρ weight enumerator by specializing the complete ρ weight enumerator.

Example 2: The ρ complete weight enumerators of the codes C_1, C_2 (Example 1) are

$$\begin{aligned} W_{C_1}(Y_{22}) =& 1 + y_{10}y_{20}, \\ W_{C_2}(Y_{22}) =& 1 + y_{21}. \end{aligned}$$

We see that the ρ complete weight enumerators of these codes are different and so are their duals. Here, we do not include the ρ complete weight enumerators of the duals since they contain 128 elements. Note that by letting, $y_{10}^{i_0}y_{11}^{i_1} = z^{2i_1+(1-i_1)i_0}$ and $y_{20}^{i_0}y_{21}^{i_1} = z^{2i_1+(1-i_1)i_0}$, we obtain the ρ weight enumerators (6). Also, replacing the term $\prod_{i=1}^{n} y_{i0}y_{i1}\cdots y_{i,k_i-1}$ with $\prod_{i=1}^{n} z_{k_i}$, we obtain the "T" weight enumerator of a code [2]. A very natural question is given the ρ complete weight enumerator of a code, is it possible to determine the ρ complete weight enumerator of its dual? The answer is the MacWilliams identity that is the goal of this paper and is proved in the sequel. First, we need to state and prove some auxiliary lemmas.

Lemma 2.1 *[3] Let χ be an additive nontrivial character of $\mathbb{F}_q$. Then,*

$$\sum_{\boldsymbol{\alpha}\in\mathbb{F}_q} \chi(\alpha) = 0. \tag{13}$$

We define,

$$\begin{aligned} \phi: \quad & \mathbb{F}_q[u]/(u^r - a) && \to \mathbb{F}_q \\ & \phi(a_0 + ua_1 + \cdots + u^{r-1}a_{r-1}) && = a_{r-1} \end{aligned} \tag{14}$$

Lemma 2.2 *Let χ be an additive nontrivial character of $\mathbb{F}_q$. Let H be an R-submodule of R. Then,*

$$\sum_{\boldsymbol{\alpha}\in H} \chi(\phi(\alpha)) = \begin{cases} 1 & H = \{0\}, \\ 0, & \textit{otherwise.} \end{cases} \tag{15}$$

Proof: If $H = \{0\}$, then $\phi(0) = 0$ and $\chi(0) = 1$. Otherwise, there exists $\beta \neq 0$ such that $\beta \in H$. Without loss of generality, we may assume that $\phi(\beta) \neq 0$ otherwise we can consider $\phi(u^i\beta) \in H$ for a suitable $i = 1, \ldots, r-1$ since H is an R-submodule. It is clear that ϕ is an $\mathbb{F}_q$-module homomorphism. Further, since there exists an element $\beta \in H$ such that $\phi(\beta) \neq 0$ and for any $b \in \mathbb{F}_q$ there exists $\theta = b(\phi(\beta))^{-1}\beta \in H$ such that $\phi(\theta) = b$, ϕ is also surjective. Thus, $H/Ker(\phi) \cong \mathbb{F}_q$, and $\sum_{\boldsymbol{\alpha} \in H} \chi(\phi(\alpha)) = |Ker(\phi)| \sum_{a \in \mathbb{F}_q} \chi(a) = 0$.(Lemma 2.1) $\square$

Lemma 2.3 *Let χ be an additive character of $\mathbb{F}_q$ and ϕ be defined as above. Then,*

$$\sum_{P(x) \in C} \chi\left(\phi\left(\langle P(x), Q(x) \rangle\right)\right) = \begin{cases} 0, & Q(x) \notin C^{\perp}, \\ |C|, & Q(x) \in C^{\perp}. \end{cases}$$

Proof: If $Q(x) \in C^{\perp}$, then it is clear. If $Q(x) \notin C^{\perp}$, then there exists $P(x) \in C$ such that $\langle P(x), Q(x) \rangle \neq 0$. Let $\langle P(x), Q(x) \rangle = \gamma \in R$. Then, the map

$$\varphi_{Q(x)} : C \to R$$
$$P(x) \to \langle P(x), Q(x) \rangle = \sum_{i=0}^{n} c_{s-1}(P_i(x) Q_i(x))$$

is $\mathbb{F}_q$-module homomorphism and $Im\varphi$ is an $\mathbb{F}_q$-submodule of R. Thus, $C/Ker(\varphi_{Q(x)}) \cong Im\varphi$. Hence,

$$\sum_{P(x) \in C} \chi\left(\phi\left(\langle P(x), Q(x) \rangle\right)\right) = |Ker(\varphi_{Q(x)})| \sum_{\alpha \in Im\varphi} \xi(\alpha) = 0, \text{ Lemma 2.2. } \square$$

Lemma 2.4 *Let χ be defined as above and i, j be fixed. Let $p(x) = p_{i0} + p_{i1}x + \cdots + p_{i,s-1}x^{s-1} \in R[x]/(x^s)$. Then,*

$$\sum_{\alpha \in R} \chi(\phi\left(\langle p(x), \alpha x^j \rangle\right)) y_{ij}^{w(\alpha)} = (1 + (q^r - 1) y_{ij})^{1 - w(p_{i,s-1-j})} (1 - y_{ij})^{w(p_{i,s-1-j})}.$$

Proof:

$$\sum_{\alpha \in R} \chi(\phi\left(\langle p(x), \alpha x^j \rangle\right)) y_{ij}^{w(\alpha)} = \sum_{\alpha \in R} \chi(\phi\left(c_{s-1}(p(x)\alpha x^j)\right)) y_{ij}^{w(\alpha)}$$

$$\sum_{\alpha \in R} \chi(\phi\left(p_{i,s-1-j}\alpha\right)) y_{ij}^{w(\alpha)} = \begin{cases} 1 + (q^r - 1) y_{ij}, & p_{i,s-1-j} = 0, \\ 1 - y_{ij}, & p_{i,s-1-j} \neq 0. \end{cases} \quad \text{(Lemma 2.2.)}\square$$

Lemma 2.5 *Let* $f : \mathcal{M}_{n\times 1}(R[x]/(x^s)) \to \mathbb{C}[y_{10}, \ldots, y_{n,s-1}]$ *and* χ *be defined as above. Then,*

$$\sum_{Q(x)\in C^\perp} f(Q(x)) = \frac{1}{|C|}\sum_{P(x)\in C} \hat{f}(P(x))$$

where $\hat{f}(P(x)) = \sum_{Q(x)\in\mathcal{M}_{n\times 1}(R[x]/(x^s))} \chi\left(\phi\left(\langle P(x), Q(x)\rangle\right)\right) f(Q(x))$,
$P(x) = (P_1(x), \ldots, P_n(x))^T$ *and* $Q(x) = (Q_1(x), \ldots, Q_n(x))^T$.

Proof. Let $P_i = p_{i0} + \cdots + p_{i,s-1}x^{s-1}$ and $Q_i(x) = q_{i0} + \cdots + q_{i,s-1}x^{s-1}$ for $1 \le i \le n$.

$$\begin{aligned}
\sum_{P(x)\in C} \hat{f}(P(x)) &= \sum_{P(x)\in C}\ \sum_{Q(x)\in\mathcal{M}_{n\times 1}(R[x]/(x^s))} \chi\left(\phi\left(\langle P(x), Q(x)\rangle\right)\right) f(Q(x))\\
&= \sum_{P(x)\in C}\ \sum_{Q(x)\in C^\perp} \chi\left(\phi\left(\langle P(x), Q(x)\rangle\right)\right) f(Q(x))\\
&+ \sum_{P(x)\in C}\ \sum_{Q(x)\notin C^\perp} \chi\left(\phi\, \langle P(x), Q(x)\rangle\right)) f(Q(x))\\
&= |C| \sum_{Q(x)\in C^\perp} f(Q(x)). \quad \text{(by Lemma 2.3.)}
\end{aligned}$$

□

Theorem 2.1 *Let* C *be a linear code over* $\mathcal{M}_{n\times s}(R)$. *Then,*

$$\begin{aligned}
&\sum_{Q(x)\in C^\perp} y_{10}^{w(q_{10})}\cdots y_{1,s-1}^{w(q_{1,s-1})}\cdots y_{n0}^{w(q_{n0})}\cdots y_{n,s-1}^{w(q_{n,s-1})}\\
&= \frac{1}{|C|}\left(\prod_{i=1}^{n}\prod_{j=0}^{s-1}(1+(q^r-1)y_{ij})\right)\sum_{P(x)\in C}\prod_{k=1}^{n}\prod_{l=0}^{s-1}\left(\frac{1-y_{kl}}{1+(q^r-1)y_{kl}}\right)^{w(p_{k,s-1-l})}.
\end{aligned}$$

Proof: We take

$$f((Q_1(x), \ldots, Q_n(x))) = y_{10}^{w(q_{10})}\cdots y_{1,s-1}^{w(q_{1,s-1})}\cdots y_{n1}^{w(q_{n0})}\cdots y_{n,s-1}^{w(q_{n,s-1})}.$$

in Lemma 2.5. Then,

$$\hat{f}(P(x)) = \sum_{Q(x)\in\mathcal{M}_{n\times 1}(R[x]/(x^s))} \chi\left(\phi\left(\langle P(x), Q(x)\rangle\right)\right) y_{11}^{w(q_{10})}\cdots y_{1s}^{w(q_{1,s-1})}\cdots y_{n0}^{w(q_{n0})}\cdots y_{ns}^{w(q_{n,s-1})}$$

$$= \sum_{Q(x)\in\mathcal{M}_{n\times 1}(R[x]/(x^s))} \prod_{i=1}^{n} \chi\left(\phi\left(\langle P_i(x), Q_i(x)\rangle\right)\right) y_{11}^{w(q_{10})}\cdots y_{1s}^{w(q_{1,s-1})}\cdots y_{n0}^{w(q_{n0})}\cdots y_{ns}^{w(q_{n,s-1})}$$

$$= \sum_{q_{10}\in R} \chi(\langle\phi\left(P_1(x), q_{10}\right)) y_{10}^{w(q_{10})} \cdots \sum_{q_{1,s-1}\in R} \chi(\langle\phi\left(P_1(x), q_{1,s-1}x^{s-1}\right)) y_{1,s-1}^{w(q_{1,s-1})}$$

$$\cdot \sum_{q_{20}\in R} \chi(\langle\phi\left(P_2(x), q_{20}\right)) y_{20}^{w(q_{20})} \cdots \sum_{q_{2,s-1}\in R} \chi(\phi\left(\langle P_2(x), q_{2,s-1}x^{s-1}\right)) y_{2,s-1}^{w(q_{2,s-1})}$$

$$\vdots$$

$$\cdot \sum_{q_{n0}\in R} \chi(\phi\left(\langle P_n(x), q_{n0}\right)) y_{n0}^{w(q_{n0})} \cdots \sum_{q_{n,s-1}\in R} \chi(\phi\left(\langle P_n(x), q_{n,s-1}x^{s-1}\right)) y_{n,s-1}^{w(q_{n,s-1})}$$

Applying Lemma 2.4,

$$\hat{f}(P(x)) = \prod_{l=0}^{s-1} (1 + (q^r - 1) y_{1l})^{1-w(p_{1,s-1-l})} (1 - y_{1l})^{w(p_{1,s-1-l})}.$$

$$\vdots$$

$$= \prod_{l=0}^{s-1} (1 + (q^r - 1) y_{nl})^{1-w(p_{n,s-1-l})} (1 - y_{nl})^{w(p_{n,s-1-l})}$$

$$= \left(\prod_{i=1}^{n}\prod_{j=0}^{s-1} (1 + (q^r - 1) y_{ij})\right) \prod_{k=1}^{n}\prod_{l=0}^{s-1} \left(\frac{1 - y_{kl}}{1 + (q^r - 1) y_{kl}}\right)^{w(p_{k,s-1-l})} . \square$$

Corollary 2.1 *Let C be a linear code over $\mathcal{M}_{n\times s}(\mathbb{F}_2 + u\mathbb{F}_2)$ with $u^2 = 1$. Then,*

$$\sum_{Q(x)\in C^{\perp}} y_{10}^{w(q_{10})}\cdots y_{1,s-1}^{w(q_{1,s-1})}\cdots y_{n0}^{w(q_{n0})}\cdots y_{n,s-1}^{w(q_{n,s-1})}$$

$$= \frac{1}{|C|}\left(\prod_{i=1}^{n}\prod_{j=0}^{s-1} (1 + 3y_{ij})\right) \sum_{P(x)\in C}\prod_{k=1}^{n}\prod_{l=0}^{s-1} \left(\frac{1 - y_{kl}}{1 + 3y_{kl}}\right)^{w(p_{k,s-1-l})} .$$

Finally, by letting $r = 1, a = 0$ for $\mathbb{F}_q[u]/(u^r - a)$ in the Theorem 2.1 we obtain the MacWilliams identity for linear spaces of matrices over finite fields proved in [6].

The author would like to thank the anonymous referee for his/her valuable remarks and careful reading.

References

[1] B.R. Donald, *Finite Rings with Identity,* Pure and Applied Mathematics Series, Marcel Dekker, New York, 1974.

[2] Steven T. Dougherty and Maxim M. Skriganov, *Duality and the Rosenbloom-Tsfasman Metric,* Moscow Mathematical Journal, Vol. 2 Number 1, p. 83-89, 2002.

[3] F.J. MacWilliams and N.J.A Sloane, *The Theory of Error Correcting Codes*, North-Holland Pub. Co., 1977.

[4] Mehmet Özen, İrfan Şiap and Fethi Çallıalp, *The structure of quaternary codes with respect to Rosenbloom-Tsfasman metric,* to appear.

[5] M.M. Skriganov, *Coding theory and uniform distributions,* St. Petersburg Math. J. Vol 143, No. 2, 2002.

[6] İrfan Şiap, *The Complete Weight Enumerator for Codes over* $\mathcal{M}_{n\times s}(\mathbb{F}_q)$, Lecture Notes on Computer Sciences 2260, p. 20-26, 2001.

[7] İrfan Şiap and Mehmet Özen, *The Complete Weight Enumerator for Codes over* $\mathcal{M}_{n\times s}(R)$, submitted.

[8] M. Yu Rosenbloom and M. A. Tsfasman, *Codes for the m-metric,* Problems of Information Transmission, Vol. 33. No. 1, 45-52, 1997.

[9] Zhe-Xian, Wan, *The MacWilliams Identity for Linear Codes over Galois Rings,* Numbers, Information and Complexity, 2000, p.333-338.

İrfan ŞİAP
Adıyaman Education Faculty,
Gaziantep University
Gaziantep-TURKEY
e-mail: isiap@antep.edu.tr

Received 17.06.2002