Finite Commutative Rings with a MacWilliams Type Relation for the m-Spotty Hamming Weight Enumerators

Ashkan Nikseresht

Department of Mathematics, Institute for Advanced Studies in Basic Sciences,
Gava Zang, 45137-66731, Zanjan, Iran
E-mail: ashkan_nikseresht@yahoo.com

Abstract

Let $R$ be a finite commutative ring. We prove that a MacWilliams type relation between the m-spotty weight enumerators of a linear code over $R$ and its dual hold, if and only if, $R$ is a Frobenius (equivalently, Quasi-Frobenius) ring, if and only if, the number of maximal ideals and minimal ideals of $R$ are the same, if and only if, for every linear code $C$ over $R$, the dual of the dual $C$ is $C$ itself. Also as an intermediate step, we present a new and simpler proof for the commutative case of Wood’s theorem which states that $R$ has a generating character if and only if $R$ is a Frobenius ring.

Keywords and Phrases: MacWilliams identity; m-spotty Hamming weight enumerator; generating character; Frobenius ring.
Mathematical Subject Classification: 11T71; 13M99.

1 Introduction

Throughout this paper, all rings are finite, commutative and with identity and $R$ denotes a ring.

First we recall some concepts of the theory of error correcting and error detecting codes. Suppose that $F = R^n$ is the free $R$-module of rank $n$. A submodule $C$ of $F$ is called a linear code of length $n$ over $R$ and each element of $C$ is called a codeword.
in $C$. Let $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in F$. By $x \cdot y$ we mean $\sum_{i=1}^{n} x_i y_i$. Now $C^\perp = \{x \in F | \forall c \in C, x \cdot c = 0\}$ is again a linear code of length $n$ over $R$, called the dual of $C$. Also the number of nonzero coordinates of $c$, denoted by $w(c)$, is called the Hamming weight of $c$.

Let $N = nb$ and $c = (c_{11}, c_{12}, \ldots, c_{1b}, c_{21}, \ldots, c_{2b}, \ldots, c_{n1}, \ldots, c_{nb})$ be a code of length $N$. Then $c_i = (c_{i1}, c_{i2}, \ldots, c_{ib})$ is called the $i$'th byte of $c$. Fix a number $1 \leq t \leq b$. An error $e$ is called a spotty byte error, if $t$ or fewer bits within a $b$-byte are in error ([16]). The number of spotty byte errors of an error $e$ is denoted by $w_M(e)$ and is called the $m$-spotty (Hamming) weight (or $m$-spotty $t/b$-weight) of $e$, that is, $w_M(e) = \sum_{i=1}^{n} \left\lceil \frac{w(e_i)}{t} \right\rceil$, where $e_i$ is the $i$'th byte of $e$. Note that in the case $t = 1$, this the usual Hamming weight.

The concepts of spotty byte errors and $m$-spotty weight of codewords, introduced in [16] and [14] respectively, are used in detecting and correcting multiple errors in byte error control codes which play an important role in computer memory systems (see, for example, [4, 7, 15]).

The $m$-spotty Hamming weight and several other “$m$-spotty weights” (such as $m$-spotty Lee weight, $m$-spotty Rosenbloom-Tsfasman weight, ...) are defined to measure the size of spotty byte errors. To study these metrics and to investigate properties of spotty byte error detecting and correcting codes, the weight enumerator polynomials are introduced and investigated. The $m$-spotty $t/b$-weight enumerator (or the $m$-spotty Hamming weight enumerator) of a linear code $C$ is $A_C(z) = \sum_{c \in C} z^{w_M(c)}$. The reader is referred to [9, Theorem 2] and the notes before that, to see an example of an application of this weight enumerator in studying $m$-spotty byte error detecting and $m$-spotty byte error correcting properties of codes.

In the case that $t = 1$ and $R$ is a field, the MacWilliams identity which relates $A_C(z)$ and $A_{C^\perp}(z)$ ([8, Theorem 5.2.9]) is a well-known theorem and is very useful in studying the properties of a linear code $C$ (see [8, Section 5.2]). Thus many authors have tried to generalize this identity. In particular, Wood in [17] showed that this identity (for the usual Hamming weight, that is, $t = 1$) hold for a finite ring $R$ (not necessarily commutative) if and only if $R$ is a Frobenius ring. Also recently many researchers tried to show that a similar relation holds for different $m$-spotty weight enumerators of byte error control codes (see for example [3, 4, 9–13]).

In particular, in [12], a MacWilliams type identity for the $m$-spotty weight enumerators of linear codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2$ is established, where $u^2 = 0$. This identity is then generalized to linear codes over the ring $\frac{\mathbb{F}_2[u]}{(u^2)}$ in [3] and to the rings
The main aim of this paper is to show that, similar to the wood’s result on the usual Hamming weight enumerators, a MacWilliams type relation for the m-spotty Hamming weight enumerators of linear codes over a finite commutative ring $R$ is valid, if and only if $R$ is a Frobenius ring (see Theorem (3.5)).

A key concept in proving the MacWilliams relation, is the notion of a character. Let $G$ be a finite Abelian group and denote the multiplicative group of complex numbers of absolute value 1 by $\mathbb{C}_1$. A group homomorphism $\chi : G \rightarrow \mathbb{C}_1$ is called a character of $G$. By a character of a ring $R$, we mean a character of the additive group of $R$. A character $\chi$ of $G$ is said be trivial (or principal) if $\chi(g) = 1$ for each $g \in G$.

To prove our main result we need to show that $R$ has a special type of character—which we call a sum-zero character (see Definition (2.1)) and is also called a generating character in the literature— if and only if $R$ is a Frobenius ring. Indeed this was proved in [17, Theorem 3.10] (without the commutative assumption), but since that proof uses deep algebraic concepts, here in Section 2, we present a new and simpler proof in the commutative case.

2 A Characterization of Rings with a Sum-Zero Character

First, we present the definition of a sum-zero character.

**Definition 2.1.** Assume that $\chi$ is a character of $R$. We say that $\chi$ is sum-zero, when $\sum_{r \in I} \chi(r) = 0$ for each nonzero ideal $I$ of $R$.

The following example shows that there are rings which do not have any sum-zero characters.

**Example 2.2.** Let $R = \mathbb{Z}_2[X,Y]/I$, where $I = \langle X^2, Y^2, XY \rangle$. Denote the images of $X,Y$ in $R$ by $x,y$, respectively and assume that $\chi$ is a sum-zero character of $R$. Note that for each $r \in R$, we have $\chi(r)^2 = \chi(2r) = \chi(0) = 1$, so $\chi(r) = \pm 1$. If $\chi(x) = 1$, then $\sum_{r \in (x)} \chi(r) = 2 \neq 0$, thus $\chi(x) = -1$. By a similar argument $\chi(y) = \chi(x+y) = -1$. Therefore, we get $-1 = \chi(x+y) = \chi(x)\chi(y) = 1$. From this contradiction we conclude that there is no sum-zero character on $R$.

We will use the following lemmas to characterize rings with a sum-zero character.
Lemma 2.3 ([17, Theorem 5.2.1]). Let \( \chi \) be a character of a finite Abelian group \( G \). Then

\[
\sum_{g \in G} \chi(g) = \begin{cases} 
0 & \text{\( \chi \) is nontrivial} \\
|G| & \text{\( \chi \) is trivial}
\end{cases}
\]

In [17], a character \( \chi \) is called a generating character when every character of \( R \) is of the form \( \chi^r \) for some \( r \in R \), where \( \chi^r(x) = \chi(rx) \). It follows the previous lemma and [17, Lemma 4.1] that a generating character is exactly the same as a sum-zero character.

Lemma 2.4. Let \( G \) be a finite Abelian group and \( 0 \neq g \in G \). Then there is a character \( \chi \) of \( G \) with \( \chi(g) \neq 1 \).

Proof. Note that \( G \cong \bigoplus_{i=1}^{k} \mathbb{Z}_{q_i} \), for some \( k \in \mathbb{N} \) and prime powers \( q_i \). Assume that \( j \) is such that \( p_j(g) \neq 0 \) where \( p_j \) is the canonical projection \( G \to \mathbb{Z}_{q_j} \). Set \( \omega \) to be the \( q_j \)th primitive root of unity. Then it is easy to see that the character \( \chi \) defined by \( \chi(\bar{a}) = \omega^a \) for \( \bar{a} \in \mathbb{Z}_{q_j} \) and \( \chi(x) = 1 \) for every \( x \in \mathbb{Z}_{q_i} \) with \( i \neq j \), has the required property. \( \square \)

Now we can state and prove the main results of this section. Recall that the socle of \( R \) is the sum of minimal ideals of \( R \) (see [1, p. 118]).

Theorem 2.5. Assume that \( R \) has a unique maximal ideal \( \mathfrak{M} \). Then \( R \) has a sum-zero character if and only if \( R \) has a unique minimal ideal.

Proof. First assume that \( \chi \) is a sum-zero character of \( R \). Suppose that \( \frac{R}{\mathfrak{M}} \cong \mathbb{F}_q \), where \( q = p^k \) for a prime number \( p \) and \( k \in \mathbb{N} \). Since \( \mathfrak{M} \) is the only maximal ideal of \( R \), we have \( \mathfrak{M}V = 0 \) where \( V \) denotes the socle of \( R \). Therefore, \( V \) is an \( \frac{R}{\mathfrak{M}} \)-module, that is, a \( \mathbb{F}_q \)-vector space. Also ideals of \( R \) contained in \( V \) are exactly the \( \mathbb{F}_q \)-subspaces of \( V \).

Assume that \( \dim_{\mathbb{F}_q} V = s \).

Let \( \omega \) be a \( p \)th primitive root of unity and \( \psi : \langle \omega \rangle \to \mathbb{F}_p \) be the map with \( \psi(\omega^i) = i \). Since \( \chi(v)^p = \chi(pv) = \chi(0) = 1 \) for each \( v \in V \) and because \( \chi|_V \) is nontrivial by (2.3), we have \( \chi(V) = \langle \omega \rangle \). Set \( U \) to be the kernel of the \( \mathbb{F}_p \)-linear transformation \( \phi = \psi \circ \chi|_V \). Since \( \phi \) is onto, we see that \( \dim_{\mathbb{F}_q} U = sk - 1 \).

According to (2.3), \( \chi|_V \) is nontrivial for each one-dimensional \( \mathbb{F}_q \)-subspace \( V' \) of \( V \) (because \( V' \) is an ideal of \( R \)). So \( V' \nsubseteq U \) and \( \dim_{\mathbb{F}_q} V' \cap U \leq k - 1 \). Thus \( |V' \backslash U| \geq p^k - p^{k-1} \). There are \( \frac{q^s - 1}{q - 1} \) different one-dimensional \( \mathbb{F}_q \)-subspaces of \( V \), each two of which have zero intersection. Thus we must have \( |V \backslash U| \geq \frac{q^s - 1}{q - 1} (p^k - p^{k-1}) \). Hence

\[
p^k - p^{k-1} \geq \frac{q^s - 1}{q - 1} (p^k - p^{k-1}) \iff p^{k(s-1)} \geq \frac{q^s - 1}{q - 1}
\]
\[
\Leftrightarrow q^{s-1} \geq \sum_{i=0}^{s-1} q^i \Leftrightarrow s = 1.
\]

Consequently, \( V \) is one-dimensional as a \( \mathbb{F}_q \)-vector space and hence \( R \) has exactly one minimal ideal.

Conversely, assume that \( R \) has exactly one minimal ideal \( I \). Let \( 0 \neq r \in I \). By (2.4), there is a character \( \chi \) of \( R \) with \( \chi(r) \neq 1 \). Since for each ideal \( J \) of \( R \), we have \( r \in I \subseteq J \), we conclude that \( \chi|_J \) is nontrivial. Hence \( \chi \) is sum-zero by (2.3). \( \square \)

**Corollary 2.6.** A finite commutative ring \( R \) has a sum-zero character, if and only if the number of maximal ideals and the number of minimal ideals of \( R \) are the same.

**Proof.** Note that \( R \) is Artinian and hence by \[2\,\text{Theorem 8.7}\] \( R \cong R_1 \times R_2 \times \cdots \times R_k \), where each \( R_i \) is local. Thus the ideals of \( R \) are of the form \( I_1 \times I_2 \times \cdots \times I_k \) where \( I_i \) is an ideal of \( R_i \). Therefore, the number of maximal ideals of \( R \) (that is, \( k \)) and the number of minimal ideals of \( R \) are the same, if and only if each \( R_i \) has a unique minimal ideal, if and only if each \( R_i \) has a sum-zero character \( \chi_i \) by (2.6). But if \( \chi \) is a sum-zero character of \( R \), then it is easy to see that \( \chi_i = \chi|_{I_i} \) is a sum-zero character of \( R_i \) and conversely, if each \( \chi_i \) is a sum-zero character of \( R_i \), then \( \chi((r_1, r_2, \ldots, r_k)) = \prod_{i=1}^{k} \chi_i(r_i) \) is a sum-zero character of \( R \). \( \square \)

The ring \( R \) is called *quasi-Frobenius* (or QF) if \( R \) is Artinian and injective as an \( R \)-module (see \[1\,\text{P. 333}]\). Also \( R \) is called Frobenius if the socle of \( R \) is isomorphic to \( R/J(R) \), where \( J(R) \) denotes the Jacobson radical of \( R \). It follows easily from \[1\,\text{Corollary 31.4}\], that a finite commutative ring \( R \) is QF if and only if it is Frobenius if and only if the number of minimal ideals and the number of maximal ideals of \( R \) are equal. Thus we get:

**Corollary 2.7.** A finite commutative ring has a sum-zero character, if and only if it is QF (equivalently, Frobenius).

Also by \[1\,\text{Theorem 30.7}\], for an Artinian ring (and in particular a finite ring) \( R \), being QF is equivalent to satisfying the double annihilator condition, that is, \( \text{Ann}(\text{Ann}(I)) = I \) for every ideal \( I \) of \( R \). The rings satisfying the double annihilator condition are also studied under the name *co-m rings*, see for example \[3\,\text{p. 6}]\.
3 A MacWilliams Type Relation for Rings with a Sum-Zero Character

In the sequel, we fix positive integers $n, b$ and $1 \leq t \leq b$ and set $N = nb$. Also as in the introduction, if $c$ is a codeword of length $N$, by $c_i$ we mean the $i$’th byte of $c$. Furthermore, $C$ is assumed to be a linear code of length $N$ over $R$.

For a codeword $c \in R^N$, let $\alpha_s$ ($1 \leq s \leq b$) be the number of bytes with Hamming weight $s$. Then $w_M(c) = \sum_{s=0}^{b} \left[ \frac{s}{t} \right] \alpha_s$. Assume that for each $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_b)$, $A_\alpha$ denotes the number of codewords in $C$ with the bytewise Hamming weight distribution $\alpha$. Then

$$A_C(z) = \sum_{\alpha_0 + \alpha_1 + \cdots + \alpha_b = n} A_\alpha \prod_{s=0}^{b} (z^\left[ \frac{s}{t} \right])^{\alpha_s},$$

where $A_C(z)$ is the m-spotty $t/b$-wight enumerator of $C$.

**Definition 3.1.** Let $r = |R|$. For any $0 \leq s \leq b$ set

$$g_s(z) = \sum_{i=0}^{s} \sum_{j=i}^{b} (-1)^i (r-1)^{j-i} \binom{b-s}{j-i} \binom{s}{i} z^\left[ \frac{s}{t} \right].$$

Then we say that a ring $R$ satisfies the generalized MacWilliams relation (or satisfies the GMR), if for every $n, b, t \in \mathbb{N}$ with $1 \leq t \leq b$ and every linear code $C$ of length $N = nb$ over $R$, we have

$$A_{C^\perp}(z) = \frac{1}{|C|} \sum_{\alpha_0 + \alpha_1 + \cdots + \alpha_b = n} A_\alpha \prod_{s=0}^{b} (g_s(z))^{\alpha_s},$$

where $A_\alpha$’s are as above.

Note that in the case $t = 1$, $g_s(z) = (1-z)^s (1+(r-1)z)^{b-s}$. Hence it can readily be checked that the equality of the above definition in the case $t = 1$ turns into

$$A_{C^\perp}(z) = \frac{(1+(r-1)z)^N}{|C|} A_C \left( \frac{1-z}{1+(r-1)z} \right),$$

which is the usual MacWilliams identity (see [8, Theorem 5.2.9]).

To characterize rings which satisfy the GMR, we need the following lemmas.

**Lemma 3.2.** Suppose that $C$ is a linear code of length $N$ over $R$ and $V$ is a $\mathbb{C}$-vector space. Let $\chi$ be a sum-zero character of $R$ and $f : R^N \to V$ be any map. If

$$\hat{f}(u) = \sum_{v \in R^N} \chi(u \cdot v) f(v)$$
for each $u \in R^N$, then
\[ \sum_{v \in C} f(v) = \frac{1}{|C|} \sum_{u \in C} \hat{f}(u). \]

**Proof.** The proof is quite similar to [12, Lemma 2.8].

**Lemma 3.3.** Suppose that $\chi$ is a sum-zero character of $R$ and $y \in R$. Then
\[ \sum_{x \in R} \chi(xy) = \begin{cases} 0, & y \neq 0 \\ |R|, & y = 0 \end{cases}. \]

**Proof.** If $y = 0$, then $\chi(xy) = 1$ for each $x \in R$ and the result follows. Suppose $y \neq 0$ and let $I$ be the annihilator ideal of $y$ in $R$. Note that $x_1y = x_2y \iff x_1 - x_2 \in I$. Thus
\[ \sum_{x \in R} \chi(xy) = \sum_{y' \in Ry \, xy = y'} \chi(y') = |I| \sum_{y' \in Ry} \chi(y') = 0, \]
since $\chi$ is sum-zero.

For a codeword $v$ of length $b$, by $\text{supp}(v)$ we mean the set of indices $i$ such that $v_i \neq 0$.

**Lemma 3.4.** Let $u$ be a codeword of length $b$ over $R$ with $w(u) = s$. If $\chi$ is a sum-zero character of $R$ and $r = |R|$, then
\[ \sum_{v \in E} \chi(u \cdot v) = (-1)^i (r - 1)^{j-i} \binom{b - s}{j - i}, \]
where $E$ is the set of all $v \in R^b$ such that $\text{supp}(v) \cap \text{supp}(u) = \{a_1, a_2, \ldots, a_i\}$ and $w(v) = j$.

**Proof.** For each $v \in E$, we have $\chi(u \cdot v) = \chi \left( \sum_{k=1}^{i} u_{a_k} v_{a_k} \right) = \prod_{k=1}^{i} \chi(u_{a_k} v_{a_k})$. Noting that we have $(b - s)(r - 1)^{j-i}$ ways to choose the $j - i$ nonzero coordinates of $v$ which are not in $\text{supp}(u)$, we see that
\begin{align*}
\sum_{v \in E} \chi(u \cdot v) &= \binom{b - s}{j - i} (r - 1)^{j-i} \sum_{0 \neq u_{a_1} \in R} \sum_{0 \neq u_{a_2} \in R} \cdots \sum_{0 \neq u_{a_i} \in R} \prod_{k=1}^{i} \chi(u_{a_k} v_{a_k}) \\
&= \binom{b - s}{j - i} (r - 1)^{j-i} \prod_{k=1}^{i} \sum_{0 \neq u_{a_k} \in R} \chi(u_{a_k} v_{a_k}) \\
&= \binom{b - s}{j - i} (r - 1)^{j-i} \prod_{k=1}^{i} \left( \sum_{x \in R} \chi(xu_{a_k}) - \chi(0) \right) \\
&= \binom{b - s}{j - i} (r - 1)^{j-i}(-1)^i,
\end{align*}
where the last equality holds by (3.3).
Theorem 3.5. For a finite commutative ring \( R \) with \( |R| = r \) the following are equivalent.

(i) \( R \) has a sum-zero character \( \chi \);

(ii) \( R \) is QF (equivalently, Frobenius);

(iii) The number of minimal ideals of \( R \) is equal to the number of maximal ideals of \( R \);

(iv) \( R \) satisfies the GMR;

(v) \(|C^\perp| = \frac{r^N}{|C|} \), for any linear code \( C \) of length \( N \) over \( R \);

(vi) \((C^\perp)^\perp = C\) for any linear code over \( R \).

Proof. (i)–(iii) are equivalent by (2.6) and (2.7).

(ii) \( \Rightarrow \) (iv): Let \( C \) be a linear code of length \( N \) over \( R \) and \( A_\alpha \) be as in (3.1). Apply lemma (3.2) with \( f : R^N \to \mathbb{C}[z] \) defined by \( f(v) = z^{w_M(v)} \). Thus by (3.2), we get

\[
A_{C^\perp}(z) = \sum_{v \in C^\perp} \hat{f}(v) = \frac{1}{|C|} \sum_{u \in C} \hat{f}(u).
\]

But

\[
\hat{f}(u) = \sum_{v \in R^N} \chi(u \cdot v)z^{w_M(v)} = \sum_{v_1 \in R^b} \sum_{v_2 \in R^b} \cdots \sum_{v_n \in R^b} \left( \prod_{k=1}^{n} \chi(u_k \cdot v_k) \right) \left( \prod_{k=1}^{n} z^{w(v_k)} \right)
\]

Let \( s_k = w(u_k) \). According to (3.4), \( \sum_{v_k} \chi(u_k \cdot v_k) = (-1)^i(r-1)^{-i} \binom{b-s_k}{j-i} \binom{s_k}{i} \), where the summation runs through all \( v_k \in R^b \) with \( w(v_k) = j \) and \( |\text{supp}(v_k) \cap \text{supp}(u_k)| = i \). Thus if we set \( \binom{k}{l} = 0 \) for \( k < 0 \) or \( k > l \), then

\[
\sum_{v_k \in R^b, \ w(v_k) = j} \chi(u_k \cdot v_k) = \sum_{i=0}^{s_k} (-1)^i(r-1)^{-i} \binom{b-s_k}{j-i} \binom{s_k}{i}
\]

and hence

\[
\sum_{v_k \in R^b, \ w(v_k) = j} \chi(u_k \cdot v_k)z^{w(v_k)} = g_{s_k}(z).
\]

Therefore, \( \hat{f}(u) = \prod_{k=1}^{n} g_{s_k}(z) = \prod_{s=0}^{b} (g_s(z))^{\alpha_s} \), where \( \alpha_s \) is the number of bytes of \( u \) with hamming weight \( s \). Now by (3.2),

\[
A_{C^\perp}(z) = \frac{1}{|C|} \sum_{u \in C} \hat{f}(u) = \frac{1}{|C|} \sum_{\alpha_0 + \alpha_1 + \cdots + \alpha_s = n} A_\alpha \prod_{s=0}^{b} (g_s(z))^{\alpha_s}.
\]
Apply (iv) with $n = t = 1$ and $b = N$ to the code $C$ to get

$$A_{C^\perp}(z) = \frac{1}{|C|} \sum_{s=0}^{b} A'_s g_s(z),$$

where $A'_s$ denotes the number of codewords in $C$ with $w(c) = s$. As in the remarks after (3.1), in this case, $g_s(z) = (1 - z)^s(1 + (r - 1)z)^{b-s}$. Thus $g_s(1) = 0$ unless $s = 0$ and $g_0(1) = r^b$. Also the only codeword with zero Hamming weight is 0, that is, $A'_0 = 1$. Now the result follows from the fact that $A_{C^\perp}(1) = |C^\perp|$, by the definition of weight enumerator of a code.

It is clear that always $C \subseteq (C^\perp)^\perp$. But by (vi), we have $|C| = |(C^\perp)^\perp|$ and (vi) follows.

Since every ideal $I$ of $R$ is a linear code of length 1 over $R$, by (vi) we get $\text{Ann}(\text{Ann}(I)) = I$ for each such $I$. But this means that $R$ is QF by [1, Theorem 30.7].

Example 3.6. Let $R$ be the ring in Example (2.2) and $\mathfrak{M} = \langle x, y \rangle$ be the maximal ideal of $R$. Then $|\mathfrak{M}| = 4$ and $\mathfrak{M}^\perp = \text{Ann}(\mathfrak{M}) = \mathfrak{M}$. Thus $|\mathfrak{M}| |\mathfrak{M}^\perp| \neq 8 = |R|$ and hence $R$ does not satisfy the equivalent conditions of the previous theorem. Also it is easy to check that $(\langle x \rangle^\perp)^\perp = \mathfrak{M} \neq \langle x \rangle$.

References


