

Chapter 3

MacWilliams Relations

In this chapter, we prove the MacWilliams relations for codes over finite Frobenius commutative rings. These relations are one of the foundational results of algebraic coding theory.

3.1 Introduction to the MacWilliams Relations

The MacWilliams relations are one of the most important foundations of algebraic coding theory. They were first proven by F.J. MacWilliams for codes over fields in [4, 5]. These relations are able to give the weight enumerator of the orthogonal of a code from the weight enumerator of a linear code. They have numerous applications in coding theory and in the connections of coding theory to other branches of mathematics. For example, self-dual codes are codes that are equal to their orthogonals. As such, their weight enumerators are held invariant by the action of the MacWilliams relations. This leads to the natural application of invariant theory to the study of self-dual codes. See Chap. 19 of [6] for an early discussion of this application. Numerous powerful results arose from this connection. See [8] for a detailed description of the connection between self-dual codes and invariant theory.

The MacWilliams relations are so fundamental to the study of codes that it is our opinion that an alphabet is an acceptable alphabet for algebraic coding theory if and only if the alphabet admits MacWilliams relations. In [9], it is shown that the class of Frobenius rings is the class of finite commutative rings that admit such relations and this is precisely why we restrict ourselves to this class of rings. It is also possible to take finite commutative groups as alphabets since there are also MacWilliams relations for these alphabets. There are other possible alphabets, as well, but in this text, we shall restrict ourselves to Frobenius rings and commutative groups.

We begin with the standard definition of the complete weight enumerator. We shall determine MacWilliams relations for this weight enumerator and then use this to obtain MacWilliams relations for other weight enumerators.

Definition 3.1 Let C be a code over an alphabet $A = \{a_0, a_1, \dots, a_{r-1}\}$. The complete weight enumerator for the code C is defined as:

$$cwe_C(x_{a_0}, x_{a_1}, \dots, x_{a_{r-1}}) = \sum_{\mathbf{c} \in C} \prod_{i=0}^{r-1} x_{a_i}^{n_i(\mathbf{c})}, \quad (3.1)$$

where there are $n_i(\mathbf{c})$ occurrences of a_i in the vector \mathbf{c} . The symmetrized weight enumerator of a code C over a group G is given by

$$swe_C(y_0, y_1, \dots, y_r) = \sum_{\mathbf{c} \in C} swt(\mathbf{c}), \quad (3.2)$$

where $swt(\mathbf{c}) = \prod_{i=0}^r x_i^{\beta_i}$ and the elements α_i and $(\alpha_i)^{-1}$ appear β_i times in the vector \mathbf{c} . The Hamming weight enumerator is given by

$$W_C(x, y) = \sum_{\mathbf{c} \in C} x^{n-wt_H(\mathbf{c})} y^{wt_H(\mathbf{c})} = cwe_C(x, y, y, \dots, y). \quad (3.3)$$

For codes over the finite field of order 2, these three weight enumerators coincide. It was in this form that the MacWilliams relations first appeared in [4, 5]. For the Hamming weight enumerator, x is often set to 1, and the weight enumerator is described in terms of y .

Example 3.1 Consider the perfect code given in Example 1.3. This code is a binary code and has weight enumerator

$$W_C(x, y) = x^7 + 7x^4y^3 + 7x^3y^4 + y^7.$$

3.2 MacWilliams Relations for Codes Over Groups

In this section, we begin in a slightly different setting. Namely, we temporarily leave the world of codes over rings and move into codes over finite commutative groups. The reason is that the fundamental structure needed for the MacWilliams relations is the underlying additive group. Moreover, in some instances, it is useful to study additive codes. That is we want to study those codes that are simply subgroups of the underlying group structure, rather than codes that are submodules of R^n . For example, additive codes over \mathbb{F}_4 have received a great deal of attention because of their connection to quantum coding.

We recall that a character of G is a homomorphism $\chi : G \rightarrow \mathbb{C}^*$. Let G be a finite abelian group and fix a duality of G , that is we fix a character table of G . We have a bijective correspondence between the elements of G and those of $\widehat{G} = \{\pi \mid \pi \text{ a character of } G\}$. We note that G and \widehat{G} are isomorphic as groups. However, this isomorphism is not canonical. In general, we simply choose an isomorphism and for each $\alpha \in G$, we denote the corresponding character in \widehat{G} by χ_α . Note that this implies that there would be a different correspondence for a different isomorphism.

In this setting, we say that a code C over G is a subset of G^n . For a code to be linear, we require only that C be an additive subset of G^n (note that we are referring to the operation of G as an additive operation). As an example, consider the code $C = \{(0, 0), (1, 0), (0, 1), (1, 1)\} \subseteq \mathbb{F}_4^2$. This code is a subgroup of the additive group of \mathbb{F}_4^2 , but it is not a vector space since, for example, the vector $\omega(1, 1) = (\omega, \omega)$ is not in the code. Therefore, the code is not a linear code in the sense of a code over a ring.

The standard definition of the Euclidean and Hermitian inner-products do not apply here because we have only one operation. Rather, we introduce a different inner-product which will coincide with the traditional inner-products in the necessary cases.

Definition 3.2 For a code C over G , with a given isomorphism between G and \widehat{G} , define the orthogonal of C to be

$$C^\perp = \{(g_1, g_2, \dots, g_n) \mid \prod_{i=1}^{i=n} \chi_{g_i}(c_i) = 1, \forall (c_1, \dots, c_n) \in C\}.$$

It is imperative to understand that this orthogonal is defined with respect to a specific duality for the group. If we change the duality then we change the orthogonal for the code. In fact, a code can be equal to its dual in one duality and not in another. Despite this very general definition of the orthogonal for codes over groups, for which we shall prove MacWilliams relations, it will turn out that this description leads to MacWilliams relations for codes over Frobenius rings in a canonical way.

To each element of \widehat{G}^n , we associate an element of G^n with the natural correspondence. Since $(\widehat{G})^n = \widehat{G}^n$, the code C^\perp is associated with the set $\{\chi \in \widehat{G}^n \mid \chi(\mathbf{c}) = 1 \text{ for all } \mathbf{c} \in C\}$. This gives that $|C^\perp| = \frac{|\widehat{G}|^n}{|C|} = \frac{|G|^n}{|C|}$ and that $C = (C^\perp)^\perp$.

For a function $f : G \rightarrow A$, where A is a complex algebra, the Fourier Transform \widehat{f} of f is a function $\widehat{f} : \widehat{G} \rightarrow A$ defined by

$$\widehat{f}(\pi) = \sum_{x \in G} \pi(x) f(x). \quad (3.4)$$

The following example shows how the orthogonality relation can change when the isomorphism between the group and its character group changes. When this is done the orthogonality relation can change significantly.

Example 3.2 Consider the character tables given in Example 2.6.

χ_1	0	1	ω	$1 + \omega$	χ_2	0	1	ω	$1 + \omega$
0	1	1	1	1	0	1	1	1	1
1	1	-1	-1	1	1	1	1	-1	-1
ω	1	-1	1	-1	ω	1	-1	-1	1
$1 + \omega$	1	1	-1	-1	$1 + \omega$	1	-1	1	-1

Note that each row gives the character associated to the element that indexes that row. Hence there are four characters represented in each table corresponding to the four elements of the group. For the duality generated by χ_1 , we have that ω is a self-orthogonal element. Then the code $C_1 = \{0, \omega\}$ is a linear code over the additive group of \mathbb{F}_4 and satisfies $C_1 = C_1^{\perp}$ with respect to this duality. Note that this code is not linear over \mathbb{F}_4 as a field, nor would ω be a self-orthogonal element over the field. For the duality given by χ_2 , we have that the codes $\{0, 1\}$, $\{0, \omega\}$, $\{0, 1 + \omega\}$ are all linear codes over the additive group and satisfy $C = C^{\perp}$. Note that in all of these cases, the usual MacWilliams relations do not apply since the codes are not linear over the field \mathbb{F}_4 . For the duality given by χ_2 , the dual code $C_1^{\perp} = \{0, 1 + \omega\}$. In this example, the complete weight enumerator of their duals is different. We shall see that if the codes are in fact linear over the ring, the MacWilliams relations will give that the weight enumerators of both orthogonals, in this case, would have to be equal (even if the orthogonals themselves were not equal).

To find MacWilliams relations for these codes, we will need the following two well known lemmas.

Let H be a subgroup of G and let $(\widehat{G} : H) = \{\pi \in \widehat{G} \mid \pi|_H = 1\}$.

Lemma 3.1 (Poisson summation formula) *Let G be a finite group and H a subgroup of G . Let f be a function from G to a complex algebra. For every $a \in G$,*

$$\sum_{x \in H} f(a + x) = \frac{1}{|(\widehat{G} : H)|} \sum_{\pi \in (\widehat{G} : H)} \pi(-a) \widehat{f}(\pi). \quad (3.5)$$

Lemma 3.2 *Suppose $f_i : G \rightarrow A$ are functions, $i = 1, 2, \dots, n$, and A a complex algebra. Let $f : G^n \rightarrow A$ be given by*

$$f(x_1, \dots, x_n) = \prod_{i=1}^n f_i(x_i). \quad (3.6)$$

Then $\widehat{f} = \prod \widehat{f}_i$; i.e. if $\pi = (\pi_1, \dots, \pi_n)$ in $\widehat{G}^n = \prod_{i=1}^n \widehat{G}$, then $\widehat{f}(\pi) = \prod_{i=1}^n \widehat{f}_i(\pi_i)$.

Let $f_i(c_i) = x_{c_i}$ and $f(x) = \prod_{i=1}^n f_i$. Then apply the previous two lemmas, which gives that for a subgroup H of G ,

$$\sum_{x \in H} f(x) = \frac{1}{|(\widehat{G} : H)|} \sum_{\pi \in (\widehat{G} : H)} \widehat{f}(\pi). \quad (3.7)$$

Then noting that $\widehat{f}(\pi) = \sum_{x \in G} \pi(x) f(x)$ gives that the action of the matrix T on the weight enumerator gives us the MacWilliams relations, where T is indexed by the elements of the group and is defined as $T_{\alpha_i, \alpha_j} = \chi_{\alpha_i}(\alpha_j)$. For a vector \mathbf{v} we let $T \cdot \mathbf{v} = (T \mathbf{v}^t)^t$.

For an element $a \in G$, let $[a]$ denote the equivalence class formed under the relation where $a \equiv a'$ if and only if $a = a'$ or $a^{-1} = (a')$, where a^{-1} is the inverse with respect to the operation of the group. Construct the matrix S indexed by (G / \equiv) where $S_{[a], [b]} = T_{a,b} + T_{a,-b}$. Let s' be the number of equivalence classes. Now we can state the MacWilliams relations for groups.

Theorem 3.1 *Let C be a code over G and let $|G| = s$, with weight enumerator $cwe_C(x_0, x_1, \dots, x_{s-1})$. Then, the complete weight enumerator of the orthogonal is given by*

$$cwe_{C^\perp} = \frac{1}{|C|} cwe_C(T \cdot (x_0, x_1, \dots, x_{s-1})), \quad (3.8)$$

$$swe_{C^\perp} = \frac{1}{|C|} swe_C(S \cdot (x_0, x_1, \dots, x_{s'-1})), \quad (3.9)$$

and

$$W_{C^\perp} = \frac{1}{|C|} W_C(x + (s-1)y, x-y). \quad (3.10)$$

Proof The first equation follows from the discussion above. The second equation follows easily from specializing the variables. To get the Hamming weight enumerator, notice that specializing the variables gives

$$\sum_{\alpha \in G} \chi_\alpha(\beta) x_\beta = x + \left(\sum_{\alpha \neq 0} \chi_\alpha(\beta) \right) y, \quad (3.11)$$

where 0 is the identity of the group. If $\beta = 0$, then $\sum_{\alpha \neq 0} \chi_\alpha(\beta) = s-1$. If $\beta \neq 0$ then $\sum_{\alpha \neq 0} \chi_\alpha(\beta) = -1$. \square

We shall now generalize the MacWilliams relations to the \mathbf{g} -fold joint weight for codes over Frobenius rings.

Definition 3.3 Let G be a finite commutative group and let C_1, \dots, C_g be additive codes over G . The complete joint weight enumerator of genus \mathbf{g} for codes C_1, \dots, C_g of length n is defined as

$$\tilde{\mathfrak{J}}_{C_1, \dots, C_g}(X_{\mathbf{a}} : \mathbf{a} \in G^g) = \sum_{(\mathbf{c}_1, \dots, \mathbf{c}_g) \in C_1 \times \dots \times C_g} \prod_{\mathbf{a} \in G^g} X_{\mathbf{a}}^{n_{\mathbf{a}}(\mathbf{c}_1, \dots, \mathbf{c}_g)},$$

where

$$\mathbf{c}_l = (c_{l1}, \dots, c_{ln}), 1 \leq l \leq g$$

and

$$n_{\mathbf{a}}(\mathbf{c}_1, \dots, \mathbf{c}_g) = |\{m \mid (c_{1m}, \dots, c_{gm}) = \mathbf{a}, 1 \leq m \leq n\}|.$$

Fix a duality T for the group G . The proof of the following is a straightforward computation similar to the proof for the usual MacWilliams relations.

Corollary 3.1 *Let C_1, \dots, C_g be additive codes over a finite group G and let \tilde{C}_l denote either C_l or C_l^\perp . Then*

$$\tilde{\mathfrak{J}}_{\tilde{C}_1, \dots, \tilde{C}_g}(X_{\mathbf{a}}) = \frac{1}{\prod_{l=1}^g |C_l|^{\delta_{\tilde{C}_l}}} \cdot (\otimes_{l=1}^g T^{\delta_{\tilde{C}_l}}) \mathfrak{J}_{C_1, \dots, C_g}(X_{\mathbf{a}}), \quad (3.12)$$

where

$$\delta_{\tilde{C}_l} = \begin{cases} 0 & \text{if } \tilde{C}_l = C_l, \\ 1 & \text{if } \tilde{C}_l = C_l^\perp. \end{cases}$$

3.3 MacWilliams Relations for Codes Over Rings

We can now use the results for codes over groups to produce MacWilliams relations for codes over Frobenius rings.

Lemma 3.3 *Let R be a finite commutative Frobenius ring with $\widehat{R} = \langle \chi \rangle$. Define the following function $F : R^n \rightarrow \widehat{R}^n$ by*

$$F(\mathbf{v}) = \chi_{\mathbf{v}}, \text{ where } \chi_{\mathbf{v}}(\mathbf{w}) = \chi([\mathbf{v}, \mathbf{w}]). \quad (3.13)$$

Proof It is clear that the map is a homomorphism. We have that

$$\ker(F) = \{\mathbf{v} \mid \chi([\mathbf{v}, \mathbf{w}]) = 1 \text{ for all } \mathbf{w} \in R^n\}.$$

Since $e_i = (0, 0, \dots, 0, 1, 0, \dots, 0) \in R^n$, we have that $\ker(F)$ is trivial and therefore F is an injection. Moreover, $|R^n| = |\widehat{R}^n|$, which gives that the map is a bijection and hence an isomorphism. \square

Note that we are heavily using the fact that the ring is Frobenius in the definition of this map since otherwise we would not have a generating character χ to define it in this manner.

Let C be a linear code in R^n . Let C^\perp be the standard orthogonal for a code over a ring. Let $\mathcal{L}(C)$ be the orthogonal for C as a subgroup of the additive group of R^n with the duality given by the character χ , namely $\chi_a(b) = \chi(ab)$. We have from Lemma 3.3 that $F(C^\perp) = \mathcal{L}(C)$ which together with the group theoretic MacWilliams relations given in Theorem 3.1 gives the following MacWilliams relations for codes over finite commutative Frobenius rings.

Theorem 3.2 *Let C be a linear code over a finite commutative Frobenius ring R . Define $T_{a,b} = \chi(ab)$, where χ is the generating character associated with R . Let S be the matrix indexed by the equivalence classes formed by the relation where $a \equiv a'$ if and only if $a = \pm a'$, and $S_{[a],[b]} = T_{a,b} + T_{a,b'}$. Then we have the following:*

$$cwe_{C^\perp} = \frac{1}{|C|} cwe_C(T \cdot (x_0, x_1, \dots, x_{s-1})), \quad (3.14)$$

$$swe_{C^\perp} = \frac{1}{|C|} swe_C(S \cdot (x_0, x_1, \dots, x_{s'-1})). \quad (3.15)$$

Note that we are not saying that there is a unique way to express the MacWilliams relations since it depends on the generating character which is not unique for a given ring. However, different matrices will still give the same weight enumerator for the orthogonal.

The following was first proven by F.J. MacWilliams in [4, 5]. There it was proven for codes over finite fields. Here we can extend the proof to codes over finite commutative Frobenius rings.

Theorem 3.3 *Let R be a finite commutative Frobenius ring with $|R| = r$. Let C be a linear code over R . Then*

$$W_{C^\perp}(x, y) = \frac{1}{|C|} W_C(x + (r-1)y, x - y). \quad (3.16)$$

Proof The result follows from Theorem 3.2 by taking the matrix T given in that theorem and by adding all non-zero columns. In the first row, adding all non-zero columns gives $(r-1)$ since every element is 1. Then in any other row (since all non-zero elements have the same Hamming weight), we get -1 when summing the columns since $\sum_{b \in R} \chi(ab) = 0$ for all non-zero $a \in R$ and $\chi(a0) = 1$.

Hence, the matrix that gives the MacWilliams relations is:

$$\begin{pmatrix} 1 & (r-1) \\ 1 & -1 \end{pmatrix}, \quad (3.17)$$

and this gives the result. \square

It is unclear where the next corollary first appeared. It is implicit in [9] but does not appear there. However, it is one of the most important consequences of the MacWilliams relations.

Corollary 3.2 *If C is a linear code over a finite commutative Frobenius ring R , with $|R| = r$, then $|C||C^\perp| = |R|^n$.*

Proof Consider Eq. 3.16 and set $x = 1$ and $y = 1$. Then we have

$$|C^\perp| = \frac{1}{|C|} r^n \quad (3.18)$$

which gives $|C||C^\perp| = |R|^n$. □

One of the main uses of this corollary is that if we have a self-orthogonal code C with $|C| = \sqrt{|R|^n}$, then C is self-dual. This corollary can also be used as a tool to show a ring is not Frobenius. Namely, if a ring has an ideal \mathfrak{a} where its orthogonal does not have cardinality $\frac{|R|}{|\mathfrak{a}|}$, then the ring is not Frobenius. We shall show an example where this fails when the ring is not Frobenius.

Example 3.3 Let $R = \mathbb{F}_2[x, y]/(x^2, y^2, xy)$. We can write the elements of R as $R = \{0, 1, x, y, 1+x, 1+y, x+y, 1+x+y\}$.

The maximal ideal is $\mathfrak{m} = \{0, x, y, x+y\}$. Hence, this ideal is a code of length 1. Its orthogonal is $\mathfrak{m}^\perp = \mathfrak{m} = \{0, x, y, x+y\}$. This gives that \mathfrak{m} is a self-dual code of length 1. However $|\mathfrak{m}||\mathfrak{m}^\perp| = 16 \neq |R| = 8$. This implies that there cannot be MacWilliams relations for this ring, since if there were then $|C||C^\perp|$ would have to be $|R|^n$.

The MacWilliams relations are an extremely powerful tool. We shall exhibit one of their classical applications.

Example 3.4 Consider the Hamming codes $H(2, r)$ given in Example 1.7. The orthogonal to this code has dimension r and length $2^r - 1$. Since every possible non-zero column is represented in the generator matrix, then the sum of any subset of rows produces a vector with weight 2^{r-1} . This gives that the weight enumerator of $H(2, r)^\perp$ is

$$W_{H(2,r)^\perp} = x^{2^r-1} + x^{2^{r-1}-1} y^{2^r-1}.$$

Then applying the MacWilliams relations gives the weight enumerator of the binary Hamming codes. Namely,

$$W_{H(2,r)} = (x+y)^{2^r-1} + (x+y)^{2^{r-1}-1} (x-y)^{2^r-1}.$$

Corollary 3.3 *Let T be the matrix that gives the MacWilliams relations for a finite commutative Frobenius ring R with $|R| = r$. Then $T^2 = rM$ where M is a monomial matrix corresponding to a permutation of the elements of R .*

Proof For any linear code C we have that $(C^\perp)^\perp = C$. This gives that applying the MacWilliams relations twice will result in the weight enumerator of the original code. This implies that $(\frac{1}{\sqrt{r}}T)(\frac{1}{\sqrt{r}}T)$ must be a monomial matrix. The result follows.

Example 3.5 For \mathbb{Z}_4 , the matrix T which gives the MacWilliams relations is:

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}. \quad (3.19)$$

Then we have

$$T^2 = 4 \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}. \quad (3.20)$$

MacWilliams relations for non-Hamming weight enumerators can also be found. See [2] for the MacWilliams relations for the Rosenbloom-Tsfasman metric.

3.4 A Practical Guide to the MacWilliams Relations

We shall now show how to construct MacWilliams relations for specific rings. As usual with commutative rings and coding theory, one of the most powerful tools is the application of the Chinese Remainder Theorem.

Theorem 3.4 *Let R be a finite commutative Frobenius ring with $R = CRT(R_1, R_2, \dots, R_s)$, where each R_i is a local ring. Let χ_{R_i} be the generating character for R_i . Then the character χ for R defined by*

$$\chi(a) = \prod \chi_{R_i}(a_i), \quad (3.21)$$

where $a = CRT(a_1, a_2, \dots, a_s)$, is a generating character for R .

Proof If χ were not a generating character, then by Theorem 2.4, it would be trivial on an ideal of R . Then there would be an i such that χ_{R_i} is trivial on an ideal of R_i , contradicting that χ_{R_i} is a generating character. Hence, χ is a generating character. \square

This theorem allows us to focus on local rings since we know that any finite commutative ring is isomorphic via the Chinese Remainder Theorem to a product of local rings. With this in mind, let R be a finite local commutative Frobenius ring with maximal ideal \mathfrak{m} . Then it follows that \mathfrak{m}^\perp is the unique minimal ideal of R where \mathfrak{m} is the unique maximal ideal.

Lemma 3.4 *Let R be a finite local commutative Frobenius ring with maximal ideal \mathfrak{m} . If χ is a character of R that is not trivial on \mathfrak{m}^\perp , then χ is a generating character for R .*

Proof We know that \mathfrak{m}^\perp is the unique minimal ideal. This means that \mathfrak{m}^\perp is contained in every non-trivial ideal of R . Hence if χ is non-trivial on \mathfrak{m}^\perp , then it is non-trivial on every ideal of R . This gives that it is a generating character. \square

Lemma 3.4 gives an easy way to find a generating character for any finite local commutative Frobenius ring. Namely, we simply find a character that is not trivial on the unique minimal ideal.

This lemma tells us a lot more about the MacWilliams relations for codes over rings. Namely, there is not a unique way to give the matrix T for a specific Frobenius ring. Rather the MacWilliams relations apply to any linear code over the ring but the matrix T depends on the choice of the generating character which as we see from the previous lemma is not necessarily unique. However, there is still only one matrix that applies the MacWilliams relations for the Hamming weight enumerator. That is, every possible matrix T still collapses to the same matrix for the Hamming weight enumerator.

We shall give some examples of the matrix T , which gives the MacWilliams relations for various rings.

- Consider the ring \mathbb{Z}_n . The classical Chinese Remainder Theorem gives that $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times \cdots \times \mathbb{Z}_{p_s^{e_s}}$, where the p_i are distinct primes. The ring $\mathbb{Z}_{p_i^{e_i}}$ is a local ring with maximal ideal $\langle p_i \rangle$ and minimal ideal $\langle p_i^{e_i-1} \rangle$. Let $\chi_{\mathbb{Z}_{p_i^{e_i}}}(a) = \eta_i^a$, where η_i is a primitive $p_i^{e_i}$ -th root of unity. Then $\eta_i^{p_i^{e_i-1}} \neq 1$ and so $\chi_{\mathbb{Z}_{p_i^{e_i}}}$ is non-trivial on the minimal ideal and therefore is a generating character. Then $\chi_{\mathbb{Z}_n} = \prod \chi_{\mathbb{Z}_{p_i^{e_i}}}$, which is realized as $\chi_{\mathbb{Z}_n}(a) = \eta^a$ where η is a primitive n -th root of unity.
- Consider the Galois ring $\mathbb{Z}_{p^e}[x]/\langle q(x) \rangle$, where $q(x)$ is an irreducible polynomial over \mathbb{Z}_{p^e} of degree k and p is a prime. Here any element is of the form $a_0 + a_1x + \cdots + a_{k-1}x^{k-1}$. Then

$$\chi(a_0 + a_1x + \cdots + a_{k-1}x^{k-1}) = \xi_{p^e}^{\sum a_i} \quad (3.22)$$

is a generating character for $\mathbb{Z}_{p^e}[\widehat{x}]/\widehat{\langle q(x) \rangle}$ where ξ_{p^e} is a primitive p^e -th root of unity. Of course, when $e = 1$ this gives us the class of finite fields.

- Consider the rings $R_k = \mathbb{F}_2[u_1, u_2, \dots, u_k]$, where $u_i^2 = 0$ and $u_i u_j = u_j u_i$ for all i, j . Then for $A \subseteq \{1, 2, \dots, k\}$ we denote $u_A = \prod_{i \in A} u_i$ and each element can be written as $\sum_{A \subseteq \mathcal{P}(\{1, 2, \dots, k\})} \alpha_A u_A$, where $\alpha_A \in \mathbb{F}_2$. Then

$$\chi \left(\sum_{A \subseteq \mathcal{P}(\{1, 2, \dots, k\})} \alpha_A u_A \right) = -1^{\sum \alpha_A} \quad (3.23)$$

is a generating character for \widehat{R}_k .

- Let R be a finite chain ring with maximal ideal $\langle \gamma \rangle$ where $R/\langle \gamma \rangle$ is isomorphic to \mathbb{F}_q . Let χ_q be the generating character for \mathbb{F}_q . We have that $\langle \gamma^{e-1} \rangle$ is the minimal ideal. Then let χ be defined by

$$\chi(a_0 + a_1\gamma + \cdots + a_{e-1}\gamma^{e-1}) = \prod \chi_q(a_i). \tag{3.24}$$

It follows that χ is not minimal on $\langle \gamma^{e-1} \rangle$ and therefore χ is a generating character for \widehat{R} .

In general, we are interested in determining the generating character of local rings, since by using Theorem 3.4, we can then determine the MacWilliams relations for any finite Frobenius commutative ring. In [7], it is shown that the smallest local Frobenius ring that is not a chain ring has order 16. Hence, the previous discussion gives the MacWilliams relations for all rings of order less than 16. Additionally in [7], the local Frobenius rings of order 16 were classified. In [1], the generating character for all of these rings is given. We give them in Table 3.1. In the table, $\eta = e^{\frac{2\pi i}{8}}$ and $\zeta = e^{\frac{2\pi i}{16}}$.

Table 3.1 Generating characters for local Frobenius rings of order 16

Ring	Additive structure	Generating character
$\mathbb{F}_{16} \cong \frac{\mathbb{F}_2[x]}{(x^4+x+1)}$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\chi(a + bx + cx^2 + dx^3) = (-1)^{a+b+c+d}$
$\frac{\mathbb{F}_2[x]}{(x^4)}$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\chi(a + bx + cx^2 + dx^3) = (-1)^{a+b+c+d}$
$\frac{\mathbb{F}_4[x]}{(x^2)} \cong \frac{\mathbb{F}_2[u,v]}{(u^2+u+1,v^2)}$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\chi(a + bu + cv + duv) = (-1)^{a+b+c+d}$
$\frac{\mathbb{F}_2[u,v]}{(u^2,v^2)}$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\chi(a + bu + cv + duv) = (-1)^{a+b+c+d}$
$\frac{\mathbb{F}_2[u,v]}{(u^2+v^2,uv)}$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\chi(a + bu + cv + du^2) = (-1)^{a+b+c+d}$
$GR(2^2, 2) \cong \frac{\mathbb{Z}_4[x]}{(x^2+x+1)}$	$\mathbb{Z}_4 \times \mathbb{Z}_4$	$\chi(a + bx) = i^{a+b}$
$\frac{\mathbb{Z}_4[x]}{(x^2-2)}$	$\mathbb{Z}_4 \times \mathbb{Z}_4$	$\chi(a + bx) = i^{a+b}$
$\frac{\mathbb{Z}_4[x]}{(x^2-2x-2)}$	$\mathbb{Z}_4 \times \mathbb{Z}_4$	$\chi(a + bx) = i^{a+b}$
$\frac{\mathbb{Z}_4[x]}{(x^2)}$	$\mathbb{Z}_4 \times \mathbb{Z}_4$	$\chi(a + bx) = i^{a+b}$
$\frac{\mathbb{Z}_4[x]}{(x^2-2x)}$	$\mathbb{Z}_4 \times \mathbb{Z}_4$	$\chi(a + bx) = i^{a+b}$
$\frac{\mathbb{Z}_4[x]}{(x^2-2,2x)}$	$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\chi(a + bx + cx^2) = i^a(-1)^{b+c} = i^{a+2b+2c}$
$\frac{\mathbb{Z}_4[x,y]}{(x^2,xy-2,y^2,2x,2y)}$	$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\chi(a + bx + cy) = i^a(-1)^{b+c} = i^{a+2b+2c}$
$\frac{\mathbb{Z}_4[x,y]}{(x^2-2,xy-2,y^2,2x,2y)}$	$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\chi(a + bx + cy) = i^a(-1)^{b+c} = i^{a+2b+2c}$
$\frac{\mathbb{Z}_8[x,y]}{(x^2-4,2x)}$	$\mathbb{Z}_8 \times \mathbb{Z}_2$	$\chi(a + bx) = \eta^a(-1)^b = \eta^{a+4b}$
\mathbb{Z}_{16}	\mathbb{Z}_{16}	$\chi(a) = \zeta^a$

References

1. Dougherty, S.T., Saltürk, E., Szabo, S.: On codes over local Frobenius rings: generator matrices, generating characters and MacWilliams Identities (to appear)
2. Dougherty, S.T., Skriganov, M.M.: MacWilliams duality and the rosenbloom-tsfasman metric. *Moscow Math. J.* **2**(1), 83–99 (2002)
3. Greferath, M., Schmidt, S.E.: Finite-ring combinatorics and MacWilliams' equivalence theorem. *J. Combin. Theory Ser. A* **92**(1), 17–28 (2000)
4. MacWilliams, F.J.: Combinatorial problems of elementary group theory, Ph.D. thesis, Harvard University (1961)
5. MacWilliams, F.J.: A theorem on the distribution of weights in a systematic code. *Bell Syst. Tech. J.* **42**, 79–94 (1963)
6. MacWilliams, F.J., Sloane, N.J.A.: *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam (1977)
7. Martnez-Moro, E., Szabo, S.: On codes over local Frobenius non-chain rings of order 16, non-commutative rings and their applications. *Contemp. Math.* **634**, 227–241 (2015)
8. Nebe, G., Rains, E.M., Sloane, N.J.A.: *Self-Dual Codes And Invariant Theory, Algorithms and Computation in Mathematics*, 17. Springer, Heidelberg (2006)
9. Wood, J.: Duality for modules over finite rings and applications to coding theory. *Am. J. Math.* **121**(3), 555–575 (1999)