Generating Characters of Non-Commutative Frobenius Rings

Steven T. Dougherty*
Department of Mathematics
University of Scranton
Scranton, PA 18518
USA
Arda Kör†
Gebze Technical University
Gebze, Kocaeli, Turkey
André Leroy
Faculté Jean Perrin
Univeristé d'Artois
Lens, France

October 3, 2017

Abstract

We give constructions for the generating character of non-commutative Frobenius rings, which is used in constructing the MacWilliams relations for a given ring. We show how to construct this character directly for any finite Frobenius ring and give examples for various families of Frobenius rings.

1 Introduction

The MacWilliams relations are one of the foundational results of algebraic coding theory. They relate the weight distribution of a code and the weight distribution of its orthogonal.

*The author is grateful to the Univeristé d'Artois where he stayed while this work was completed.
†The author is grateful to the Univeristé d'Artois where she stayed while this work was completed.

These relations were first proven by J. MacWilliams in [8] and [9] for binary codes and this proof naturally extended first to codes over finite fields and then to codes over Frobenius rings in [11]. This result is one of the major reasons why coding theorists generally restrict their alphabets to Frobenius rings. The key element of the MacWilliams relations for Frobenius rings is to find a generating character for the ring. In [6], the technique for finding this generating character when R is commutative was described. In the commutative case, the main tool is the generalized Chinese Remainder Theorem which decomposes arbitrary Frobenius rings into local Frobenius rings. Then a generating character is constructed for local rings and the generating character for the ambient ring is constructed via the Chinese Remainder Theorem. See [4] for a complete description of this technique and for a description of the use of Frobenius rings in algebraic coding theory. For non-commutative rings there is no such decomposition into easily handled subrings, which complicates the situation greatly. In other words, one cannot assume that an arbitrary finite ring has a decomposition into local rings or any other type of ring with an easily constructed generating character. In this work, we shall study the construction of this generating character for non-commutative Frobenius rings. We begin with the necessary definitions both for rings and for codes.

1.1 Rings

For any ring R, we define the Jacobson radical as the intersection of all maximal left ideals in R. It turns out that this is equal to the intersection of all maximal right ideals as well. We denote the Jacobson radical by $J(R)$ and note that it is a two sided ideal. The right socle of a ring R, denoted by $soc(R)$ is the sum of all minimal right ideals. For a complete description of these ideals and for a reference for the results from ring theory see [7].

Let M be a module. A character of M is a homomorphism from the additive group $(M, +)$ to the multiplicative group of nonzero complex numbers. Note that sometimes characters are understood to have images in $\mathbb{Q}/\mathbb{Z}$ but we prefer the image to be the nonzero complex numbers. These maps will also be referred to as "additive maps". For an R module M, let $\widehat{M}$ be the set of characters of M. This set is an abelian group: if $\sigma, \tau \in \widehat{M}$, then we define $(\sigma+\tau)(m)$ to be $\sigma(m)\tau(m)$. Notice that if M_R (respectively ${}_RM$) is a right (respectively left) R-module, then $\widehat{M}$ is left (respectively right) R module via $(r.\varphi)(m) = \varphi(mr)$ (respectively $(\varphi.r)(m) = \varphi(rm)$) where $\varphi \in \widehat{M}$ and $r \in R$.

Throughout the paper, we assume that a ring has a multiplicative unity and that all rings are finite. Rather than providing a definition for Frobenius ring we shall give its characterization as given in Theorem 3.10 in [11]. This states that the following are equivalent for a finite ring R.

- The ring R is a Frobenius ring.
- As a left module, $\widehat{R} \cong {}_RR$.

- As a right module $\widehat{R} \cong R_R$.

Hence, we say that a ring is Frobenius when the second or third condition is met. For a complete description of the classical definition see [3]. Moreover for a Frobenius ring R we have $\mathcal{L}(J) = soc({}_R R) = soc(R_R) = \mathcal{R}(J)$. Note that for non-Frobenius rings this is not necessarily true.

A character χ of a ring R is a right generating character if the mapping $\phi : R \to \widehat{R}$ defined by $\phi(r) = \chi^r$ is an isomorphism of right R modules (where $(\chi^r)(x) = \chi(rx)$ for $r, x \in R$). A character χ of a ring R is a left generating character if the mapping $\phi : R \to \widehat{R}$ defined by $\phi(r) = {}^r\chi$ is an isomorphism of left R modules (where $({}^r\chi)(x) = \chi(xr)$ for $x, r \in R$). Theorem 4.3 in [11] gives that a character χ on R is a left generating character if and only if it is a right generating character. Therefore, throughout this paper we shall restrict ourselves to finding right generating characters and eliminate the adjectives right and left.

The following is Corollary 3.6 in [2].

Lemma 1.1. *[2] Let χ be a character of a finite ring R. Then χ is a right generating character if and only if $ker(\chi)$ contains no non-zero right ideals.*

This lemma gives our most powerful tool in the construction of right generating characters and we shall use it throughout the paper when proving that a given character is in fact a generating character.

1.2 Codes

A code over a Frobenius ring R of length n is a subset of R^n. It is said to be a left linear code if it is a left submodule of ${}_R R^n$ and it is said to be a right linear code if it is a right submodule of R^n_R. The ambient space R^n has an inner-product defined by

$$[\mathbf{v}, \mathbf{w}] = \sum v_i w_i.$$

For a code C we define

$$\mathcal{L}(C) = \{\mathbf{v} \mid [\mathbf{v}, \mathbf{w}] = 0, \forall \mathbf{w} \in C\} \tag{1}$$

and

$$\mathcal{R}(C) = \{\mathbf{v} \mid [\mathbf{w}, \mathbf{v}] = 0, \forall \mathbf{w} \in C\}. \tag{2}$$

In [5], it is shown that $\mathcal{L}(C)$ is a left linear code and $\mathcal{R}(C)$ is a right linear code. When the ring is commutative these orthogonals coincide and are denoted by $C^\perp$.

For a code over $R = \{a_0, a_1, \ldots, a_{s-1}\}$, the complete weight enumerator is defined to be the following polynomial in commuting variables:

$$cwe_C(x_{a_0}, x_{a_1}, \ldots, x_{a_{s-1}}) = \sum_{\mathbf{c} \in C} \prod_{i=0}^{s-1} x_{a_i}^{n_i(\mathbf{c})} \tag{3}$$

where there are $n_i(\mathbf{c})$ occurrences of a_i in the vector $\mathbf{c}$.

If χ is a right generating character then $\chi^a(b) = \chi(ab)$, where χ^a is the character corresponding to the element a of R. We use this to define the matrix T. Let T be the $|R|$ by $|R|$ matrix given by:

$$(T)_{a,b} = (\chi(ab)) \tag{4}$$

where a and b are elements in R. It is precisely this matrix T that we use to obtain the MacWilliams relations for a given ring R. We note here that the ordering of the elements is arbitrary and must only match the ordering given in the complete weight enumerator.

If $(x_0, \ldots, x_k)$ is a vector we let $T \cdot (x_0, \ldots, x_k) = (T(x_0, \ldots, x_k)^t)^t$ where M^t is the transpose of the matrix M. The following are the MacWilliams relations as given in Corollary 8.2, [11].

Theorem 1.2. *[11] (Generalized MacWilliams Relations) Let R be a Frobenius ring. If C is a left submodule of R^n, then*

$$cwe_C(x_0, x_1, \ldots, x_k) = \frac{1}{|\mathcal{R}(C)|} cwe_{\mathcal{R}(C)}(T^t \cdot (x_0, x_1, \ldots, x_k)).$$

If C is a right submodule of R^n, then

$$cwe_C(x_0, x_1, \ldots, x_k) = \frac{1}{|\mathcal{L}(C)|} cwe_{\mathcal{L}(C)}(T \cdot (x_0, x_1, \ldots, x_k)).$$

It follows from these relations for Frobenius rings, that if C is a left linear code then $|C||\mathcal{R}(C)| = |R|^n$ and if C is a right linear code then $|C||\mathcal{L}(C)| = |R|^n$. See [3] for a proof of these facts. This implies that if you can find a linear code and its proper orthogonal whose cardinalities do not satisfy this then the ring is not Frobenius. Since ideals are codes of length 1, it is enough to show a left ideal and its right annihilator do not have the product of their cardinalities equal to the size of the ring to show that the ring is not Frobenius.

Example 1. *Consider the ring $R = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{F}_q\}$. Here $|R| = q^3$. Consider the right ideal $I = \{\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \mid x, y \in \mathbb{F}_q\}$. This ideal has cardinality q^2. Its left orthogonal $\mathcal{L}(I) = \{\begin{pmatrix} 0 & d \\ 0 & e \end{pmatrix} \mid d, e \in \mathbb{F}_q\}$ which has cardinality q^2. But $q^2 q^2 \neq q^3$. Hence this ring is not Frobenius. In general, the ring of upper triangular matrices is not Frobenius.*

Example 2. *Consider the non-commutative ring $R = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{F}_2\}$. One might naively assume that the additive map $\chi(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}) = (-1)^{a+b+c}$ would be a generating*

character. However, $\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}\}$ *is a right ideal of* R*. The map* χ *contains this ideal in its kernel, hence* χ *is not a generating character. In fact, this ring is not Frobenius and does not have a generating character.*

The previous example shows that a generating character involves much more than the additive structure of the ring. More to the point, the fact that a ring is Frobenius and has a generating character, in some sense, says that the multiplication of the ring works in a compatible way to the addition in terms of orthogonality. The MacWilliams relations can be defined simply on the additive group structure, where the orthogonality is determined via a character table. The ring is not necessary at all. However, we want the orthogonal as defined by the group's character table to coincide with the orthogonal as defined canonically with the ring. When the ring is Frobenius the coincidence of the two orthogonals occurs, when it is not Frobenius it does not. Namely, the group orthogonal comes from characters alone whereas the ring orthogonality uses the multiplication in the ring.

Other weight enumerators can be defined over specific rings and MacWilliams relations can be found for some of these specialized weight enumerators. In general, by collapsing the elements with an equivalence relation denoted by $\equiv$, we can build a matrix S for the MacWilliams relations by

$$S_{\overline{a},\overline{b}} = \sum_{c \equiv b} T_{a,c}. \tag{5}$$

For this construction to be meaningful, we need

$$\sum_{c \equiv b} T_{a,c} = \sum_{c \equiv b} T_{a',c}$$

if $a \equiv a'$.

Notice that, except for the first row, the rows of the matrix T must sum to 0. Indeed if $a \neq 0$, since χ is a generating character, the ideal aR is not contained in $\ker(\chi)$. Therefore, there exists $b_0 \in R$ such that $\chi(ab_0) \neq 1$. We then have $\chi(ab_0) \sum_{b \in R} \chi(ab) = \sum_{b \in R} \chi(ab_0 + ab) = \sum_{b \in R} \chi(a(b_0 + b)) = \sum_{b \in R} \chi(ab)$. From this we conclude that $\sum_{b \in R} \chi(ab) = 0$, as claimed.

The rows of the matrix S must also sum to 0. For example, the Hamming weight enumerator equates all non-zero elements in the ring. Therefore, there are two equivalence classes, $\overline{0}$ and $\overline{1}$. Then we have that $\sum_{a \in R} \chi(0a) = |R|$ and $\sum_{a \in R} \chi(1a) = 0$. Hence, the matrix S for the MacWilliams relations for the Hamming weight enumerator is given by:

$$\begin{pmatrix} 1 & |R| - 1 \\ 1 & -1 \end{pmatrix}. \tag{6}$$

As a small commutative example, consider the ring $\mathbb{F}_2[x]/\langle x^2\rangle$. Then the matrix T indexed by $0, 1, x, 1+x$ is given by

$$T = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \end{pmatrix}.$$

Equating 1 and $1+x$ you obtain the matrix

$$S = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 0 & -1 \\ 1 & -2 & 1 \end{pmatrix}.$$

However, equating 1 and x would give two different results on the row corresponding to 1 and the row corresponding to x. Hence this is not an acceptable specialization. If the equivalence relation is that two elements are the same if they are equal by left multiplication of a unit then it is a simple matter to see that one can always construct the matrix S. This weight enumerator is known as the symmetrized weight enumerator. We shall denote the matrix S for this weight enumerator by S_1. It is also possible to construct the matrix S, where the equivalence relation is given by two elements a, b are equivalent if $a = \pm b$. This is known as the symmetric weight enumerator. We shall denote the matrix S for this weight enumerator by S_2.

2 Generating Characters

We begin our study of generating characters with the following lemma which appears as Example 4.9 (iii) in Wood's paper [11]. We include the proof since it is constructive and shows how to construct the generating character.

Lemma 2.1. *Let R be a finite Frobenius ring where*

$$R \cong R_1 \times R_2 \times \cdots \times R_s$$

where R_i is Frobenius for all $1 \leq i \leq s$. Let χ_{R_i} be the right generating character for R_i and let $\phi : R \to R_1 \times R_2 \times \cdots \times R_s$ be the isomorphism, with $\phi(a) = (a_1, a_2, \ldots, a_s)$. Define $\chi : R \to \mathbb{C}^*$ by

$$\chi(a) = \prod_{i=1}^{s} \chi_{R_i}(a_i).$$

Then χ is a right generating character of R.

Proof. Assume I is a nonzero right ideal of R. Then I is isomorphic to $I_1 \times I_2 \times \cdots \times I_s$ where I_i is a nonzero right ideal in R_i. Let $a_i \in I_i$ with $\chi_{R_i}(a_i) \neq 1$. We know such an a_i exists since χ_{R_i} is not trivial on any ideal of R_i. Let $a = \phi^{-1}(0, 0, \ldots, a_i, \ldots, 0)$. Then $\chi(a) = 1\chi_{R_i}(a_i) \neq 1$. Hence χ is not trivial on any right ideal I and hence no right ideal is contained in $ker(\chi)$ which gives that χ is a generating character for R. □

Theorem 2.2. *Let R be a finite ring. Let $\theta : soc(R) \to \mathbb{C}^*$ be an additive map such that $\ker(\theta)$ contains no one sided ideals and χ be any additive extension of θ to R. Then χ is a generating character of R and R is a Frobenius ring.*

Proof. Since R is finite any one sided ideal of R contains a minimal one sided ideal. So any extension χ of θ is such that $\ker(\chi)$ does not contain any nonzero one sided ideal. Lemma 1.1 concludes the proof. □

In the next examples, we consider local rings. Here $J(R)$ is the unique maximal ideal and so $\mathcal{R}(J(R)$ is the socle of the ring and is the minimal ideal of the ring.

Example 3. *Let $\mathbb{F}_4 = \{0, 1, \omega, 1 + \omega\}$ be the field with 4 elements and $R = \mathbb{F}_4[X, \sigma]/\langle X^2 \rangle$, where σ is the Frobenius map. An element of this ring is of the form $a_0 + a_1 x$ where $x = X + \langle X^2 \rangle$ and $a_0, a_1 \in \mathbb{F}_4$. This ring is a local ring where the maximal ideal is the Jacobson radical with $J(R) = Rx = xR = \{0, 1x, \omega x, (1 + \omega)x\}$. Then $R/J(R) \cong \mathbb{F}_4$. This ideal is the only non-trivial ideal of the ring and in fact $\mathcal{R}(J(R)) = J(R)$ and hence it is a self-dual code of length 1. See [5] for a detailed study of self-dual codes over non-commutative Frobenius rings. The additive structure of $J(R)$ is isomorphic to the additive structure of $\mathbb{F}_4$ which is $\mathbb{F}_2 \times \mathbb{F}_2$. Let τ be the character on $\mathbb{F}_4$ defined by $\tau(\alpha) = (-1)^{b_0+b_1}$ where $\alpha = b_0 + b_1\omega$. Then define θ on the minimal ideal by defining $\theta(\alpha x) = \tau(\alpha)$. We can extend θ to χ where $\chi(a_0 + a_1 x) = \tau(a_0)\tau(a_1)$. Then χ is a generating character of R by Theorem 2.2. In this ring there are 3 nonzero non units, namely $\overline{x} = \{x, \omega x, (1 + \omega)x\}$. This leaves 12 units. Then the matrix S_1 for the symmetrized weight enumerator is indexed by $\overline{0}, \overline{1}, \overline{x}$ and is given by:*

$$\begin{pmatrix} 1 & 12 & 3 \\ 1 & 0 & -1 \\ 1 & -4 & 3 \end{pmatrix}.$$

Since the ring has characteristic 2, the symmetric weight enumerator is equal to the complete weight enumerator so $S_2 = T$.

Example 4. *Let $R = \mathbb{F}_4[X, \sigma]/\langle X^4 \rangle$. As in the above example we let $x = X + \langle X^4 \rangle$. Then $J(R) = Rx = xR$ and $R/J(R) \cong \mathbb{F}_4$. The ring is a local ring as all right ideals are contained in the Jacobson radical. We note that $\mathcal{R}(J(R)) = Rx^3$ which is isomorphic to $\mathbb{F}_4$. Let τ be the character on $\mathbb{F}_4$ defined by $\tau(\alpha) = (-1)^{b_0+b_1}$ where $\alpha = b_0 + b_1\omega$. Then $\theta(\alpha x) = \tau(\alpha)$. Then we extend this to χ to have $\chi(a_0 + a_1 x + a_2 x^2 + a_3 x^3) = \prod_{i=1}^{4} \tau(a_i)$ which is an*

extension of θ. Then χ is a generating character of R by Theorem 2.2. In this ring there are 192 units, and three additional equivalence classes where the equivalence relation is given by left multiplication by a unit. They are $\overline{x}, \overline{x^2}, \overline{x^3}$ with $|\overline{x}| = 48, |\overline{x^2}| = 12, |\overline{x^3}| = 3$. Hence the matrix S_1 is a 5 by 5 matrix which can be computed from the 256 by 256 matrix T. This ring has characteristic 2 so $S_2 = T$.

Example 5. *Let $A = \mathbb{F}_q[x;\sigma]$ where $q > 2$ and σ is an automorphism of $\mathbb{F}_q$ of order 2. Consider $R = \mathbb{F}_q[x;\sigma][y;\sigma']/(Rx^2 + Ry^2)$ where σ' extends σ via $\sigma'(x) = x$. The ring is a local ring with maximal ideal $xR + yR$ which is then the Jacobson radical. The ring has cardinality q^4. The maximal ideal has cardinality q^3. The unique minimal ideal is $(xy)R$ which has cardinality q. Here we can define a character*

$$\chi(a_0 + a_1x + a_2y + a_3xy) = \prod \chi_{\mathbb{F}_q}(a_i).$$

This character is non-trivial on the minimal ideal and hence is a generating character for R. In this case S_2 is not T as in the previous cases. It is a $(\lceil \frac{q}{2} \rceil)^4$ by $(\lceil \frac{q}{2} \rceil)^4$ matrix.

Of course, not all local rings are Frobenius. Consider the finite commutative ring $\mathbb{F}_2[x,y]/\langle x^2, y^2, xy\rangle$. This ring has 8 elements, namely $R = \{0, 1, x, y, 1+x, 1+y, 1+x+y, x+y\}$. The maximal ideal of this ring contains all non-units and is $M = \{0, x, y, x+y\}$. Here $M^\perp = M$, but $4(4) \neq 8$ and so the ring is not Frobenius. It is instructive to point out that if one were to naively take the character of the underlying additive structure of this ring you would have a character defined as follows:

a	0	1	x	y	$x+y$	$1+x$	$1+y$	$1+x+y$
$\chi(a)$	1	-1	-1	-1	1	1	1	-1

(7)

This does not qualify as a generating character because χ is trivial on the ideal $\{0, x+y\}$. Moreover there are three minimal ideals, namely $\{0, x\}$, $\{0, y\}$, $\{0, x+y\}$. For a character to be a generating character, one would need $\chi(x) = \chi(y) = \chi(x+y) = -1$. However, if $\chi(x) = \chi(y) = -1$ then $\chi(x+y)$ would have to be 1, contradicting the earlier statement. This gives an example of why a non-Frobenius ring does not have a generating character and the MacWilliams relations do not apply. In particular, the orthogonal of all three of the minimal ideals would be M if the ring were Frobenius.

2.1 Frobenius Algebras

We shall now determine the generating character for Frobenius algebras. For a complete description of Frobenius algebras, see [7]. Let A be a Frobenius $\mathbb{F}_q$ algebra with $q = p^l$. There is a nonsingular bilinear pairing $B : A \times A \to \mathbb{F}_q$ with the associative property. It is known that the functional $\lambda : A \to \mathbb{F}_q$ defined by $\lambda(a) = B(a, 1)$ has a kernel which contains no nonzero right ideals, see page 438 of [7]. This gives that there exists a $\lambda \in Hom_{\mathbb{F}_q}(A, \mathbb{F}_q)$,

such that no right ideal I has $\lambda(I) = \{0\}$. Let tr be the trace map from $\mathbb{F}_q$ to $\mathbb{F}_p$ given by $tr(x) = x + x^p + \cdots + x^{p^{l-1}}$ where $q = p^l$. Define the map $\mu : \mathbb{F}_q \to \mathbb{C}^*$, $\mu(x) = e^{\frac{2\pi i tr(x)}{p}}$, for $x \in \mathbb{F}_q$.

The following theorem also appears in [12]. We shall use the proof to describe the generating characters for finite dimensional Hopf algebras. We include the proof for completeness.

Theorem 2.3. *Let A be a Frobenius $\mathbb{F}_q$-algebra with $q = p^l$. Define a character for A as*

$$\chi(a) = \mu(\lambda(a)) = \mu(B(a, 1)), \qquad \text{for } a \in A. \tag{8}$$

Then χ is a generating character for A.

Proof. Since the map λ is nontrivial on all right ideals of A we have that the map χ is nontrivial on all right ideals of A. Then, by Lemma 1.1, we have that χ is a generating character for the Frobenius algebra A. □

This theorem implies that when the bilinear form is known the generating character follows immediately.

An important particular case of a Frobenius algebra is the case of finite dimensional Hopf algebras. Two prominent examples in this family are the group algebras of a finite group and the envelopping algebra of a Lie algebra. In order to get a generating character for a $\mathbb{F}_p$ finite dimensional Hopf algebra it is enough, according to the previous paragraph, to determine a bilinear pairing from $B : H \times H \longrightarrow \mathbb{F}_p$ which is non-degenerate and associative. This is classical but let us recall that an element $t \in H$ is called a left integral if for every $h \in H$ we have that $ht = \epsilon(h)t$ where $\epsilon : H \longrightarrow \mathbb{F}_p$ is the counity. Now $H^* = Hom(H, \mathbb{F}_p)$ is also a Hopf algebra and if $f \in H^*$ is a left integral it is well known that the map $B : H \times H \longrightarrow \mathbb{F}_p$ defined by $B(x, y) = f(xy)$ is such a pairing.

Let us now analyze the case of a group ring $R = kG$ where k is a finite field and G is a finite group. Let us recall that kG is a Hopf algera with comultiplication, counit and antipode given, for all $g \in G$, by

$$\Delta(g) = g \otimes g, \qquad \epsilon(g) = 1, \qquad S(g) = g^{-1}.$$

In kG, the one dimensional k-space of left (right) integrals is given by $k(\sum_{g \in G} g)$ and in kG^* it is kp_{1_G}, where p_{1_G} is the projection of kG on $k1_G$. The generating character χ of kG is thus given by $\chi(a) = \mu(p_{1_G}(a))$.

2.2 Taft Hopf Algebras

Let us now consider the well-known Taft Hopf algebra T which is neither commutative nor cocommutative. Let $\mathbb{F}_q$ be a finite field with $q = p^l$. For $n \in \mathbb{N}$, such that p does not divide n, we let $\zeta \in \mathbb{F}_q$ be a primitive n^{th}-root of unity. We define $T = \mathbb{F}_q\langle x, g\rangle / I$ where I is the

ideal generated by $x^n, g^n - 1$ and $xg - \zeta gx$. This algebra can be given the structure of a Hopf algebra via:

$$\Delta(x) = x \otimes g + 1 \otimes x, \quad \Delta(g) = g \otimes g \quad \epsilon(g) = 1, \quad \text{and } \epsilon(x) = 0.$$

The antipode S of T is given by $S(g) = g^{-1}$ and $S(x) = -xg^{-1}$. It is known that the left (respectively right) integrals of T is the one dimensional space generated by $\sum_{i=0}^{n-1} g^i x^{n-1}$ (respectively $\sum_{i=0}^{n-1} \zeta^i g^i x^{n-1}$). The Taft algebra T is isomorphic to its dual T^*. The isomorphism of Hopf algebras ψ is given by $\psi(x) = X$ and $\psi(g) = G$ with X and G (notice that G is in fact a ring homomorphism) are defined by

$$X(g^i x^j) = \delta_{1,j} \quad \text{for } 0 \leq i, j \leq n-1 \quad \text{and } G(g) = \zeta^{-1},\ G(x) = 0,$$

where δ is the Kronecker symbol.

The left (respectively right) integrals of T^* is the one dimensional space generated by $\sum_{i=0}^{n-1} G^i X^{n-1}$ (respectively $\sum_{i=0}^{n-1} \zeta^i G^i X^{n-1}$). The generating character χ of T is thus given by $\chi(x) = \mu(\lambda(x)) = \mu(B(x,1)) = \mu(\sum_{i=0}^{n-1} G^i X^{n-1}(x))$.

It is well known that a restricted enveloping k-algebra of a restricted finite dimensional Lie algebra over a field (also called u-algebra) is a Frobenius algebra. For more information about this enveloping algebra $u(L)$ we refer the reader to [10]. If the Lie algebra is $L = \sum_{i=1}^{n} ka_i$, where k is a field of characteristic $p \neq 0$, the restricted enveloping algebra $u(L)$ of L has a k-basis $a_I = a_1^{i_1} \dots a_n^{i_n}$ where $0 \leq i_s < p$. It is shown in [1] that the element $\phi \in u(L)^*$ defined by $\phi(a_I) = 0$ for every subset $I \subset \mathbb{N}^n$, except for $I = p-1$, has $\phi(a_1^{p-1} \cdots a_n^{p-1}) = 1$. We then have that $u(L)^* = \{a\phi \mid a \in u(L)\}$. This shows that ϕ is a generating character over k.

3 The Socle and Generating Characters

Let R be a finite Frobenius ring and let $J(R)$ be the Jacobson radical of R. It is well known that,

$$R/J(R) \cong M_{n_1}(\mathbb{F}_{q_1}) \times M_{n_2}(\mathbb{F}_{q_2}) \times \cdots \times M_{n_s}(\mathbb{F}_{q_s}), \tag{9}$$

where $M_{n_i}(\mathbb{F}_{q_i})$ is the ring of n_i by n_i matrices with entries from the field $\mathbb{F}_{q_i}$ (for more details see [7]). Let us recall that, for $q = p^e$ where p is a prime number, the generating character $\chi_{\mathbb{F}_q}$ of $\mathbb{F}_q$ is defined by $\chi_{\mathbb{F}_q}(a) = e^{\frac{2\pi i t}{p}}$ where, for $a \in \mathbb{F}_q$, $t = tr(a) = a + a^p + \cdots + a^{p^{e-1}} \in \mathbb{F}_p$.

We now define a generating character σ for R/J by

$$\sigma(M_1, M_2, \dots, M_s) = \prod_{i=1}^{s} \chi_{\mathbb{F}_{q_i}}(Tr(M_i)) \tag{10}$$

where, for $M_i \in M_{n_i}(\mathbb{F}_{q_i})$, $Tr(M_i)$ is the trace of the matrix M_i. It is easily seen from Lemma 2.1 that this is a generating character for $M_{n_1}(\mathbb{F}_{q_1}) \times M_{n_2}(\mathbb{F}_{q_2}) \times \cdots \times M_{n_s}(\mathbb{F}_{q_s})$.

Theorem 3.1. *Let R be a finite Frobenius ring. Let χ be any additive extension on*

$$\sigma : soc(R) \to \mathbb{C}^*$$

defined in Equation 10, then χ is a generating character for R.

Proof. Since the ring is Frobenius we have that $R/J(R) \cong soc(R)$. We also have that

$$R/J(R) \cong M_{n_1}(\mathbb{F}_{q_1}) \times M_{n_2}(\mathbb{F}_{q_2}) \times \cdots \times M_{n_s}(\mathbb{F}_{q_s})$$

which gives that

$$soc(R) \cong M_{n_1}(\mathbb{F}_{q_1}) \times M_{n_2}(\mathbb{F}_{q_2}) \times \cdots \times M_{n_s}(\mathbb{F}_{q_s}).$$

Therefore, we can define σ as in Equation 10 on $soc(R)$. Then Theorem 2.2 gives that χ is a generating character. □

Note that this theorem gives the generating character for any finite Frobenius ring. Namely, we explicitly construct the generating character for the socle. Then the additive structure of the ring is a finite abelian additive group. Therefore, it is a trivial matter to extend the map σ to the entire ring additively.

Corollary 3.2. *Let R be a finite local Frobenius ring. Let $\chi_{\mathbb{F}_q}$ be the standard character on the field of order q. Let χ be any additive extension of $\chi_{\mathbb{F}_q} : soc(R) \to \mathbb{C}^*$ to R. Then χ is a generating character for R.*

Proof. The proof is the same as Theorem 3.1, noting that $R/J(R)$ is a finite field of order q if R is a local ring. □

Example 6. *Let $R = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{F}_q\}$. Then we have that $J(R) = \{\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \mid b \in \mathbb{F}_q\}$. This gives that $soc(R) = R/J(R) \cong \mathbb{F}_q \times \mathbb{F}_q$. For $(\alpha, \beta) \in \mathbb{F}_q \times \mathbb{F}_q, \alpha = a_0 + a_1 p + \cdots + a_{e-1}p^{e-1}, \beta = b_0 + b_1 p + \cdots + b_{e-1}p^{e-1}$, $\tau(\alpha, \beta) = \xi_p^{\sum a_i} \xi_p^{\sum b_i} = \xi_p^{\sum a_i + b_i}$. Then $\sigma(\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}) = \xi_p^b$. This then gives the generating character χ on R. For the equivalence relation where $a \equiv b$ if $a = \mu b$ for some unit b we have 6 classes, namely*

$$\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\}, \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\}, \{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\}, \{\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}\}, \{\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\}, \{\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\}.$$

Using these to index the matrix we get that

$$S_1 = \begin{pmatrix} 1 & 2 & 1 & 2 & 1 & 1 \\ 1 & 0 & -1 & 0 & -1 & 1 \\ 1 & 0 & -1 & 0 & -1 & 1 \\ 1 & -2 & 1 & -2 & 1 & 1 \\ 1 & -2 & 1 & -2 & 1 & 1 \\ 1 & 0 & -1 & 0 & -1 & 1 \end{pmatrix}.$$

This ring has characteristic 2 so $S_2 = T$.

Note that if the ring is not Frobenius then this is not possible to apply the theorem since $R/J(R)$ is not necessarily the socle. Therefore, we cannot say that the socle is isomorphic to the direct product of matrix rings and so we cannot define σ on the socle. For example, consider the non-Frobenius ring $R = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, a, b, c \in \mathbb{F}_2\}$. This ring is not Frobenius and therefore does not admit a generating character. However, $R/J(R) \cong \mathbb{F}_2 \times \mathbb{F}_2$ has a (unique) generating character defined via,

$$\sigma((0,0)) = 1, \sigma((0,1)) = \sigma((1,0)) = -1, \sigma((1,1)) = 1.$$

Concretely, $J(R) = \{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\}$ and

$$R/J(R) = \{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\}.$$

However, this is not the socle of the ring and the so the map cannot be extended. For example, if one were to define χ to be as given on $R/J(R)$ and extend it to the whole ring defined by

$$\chi(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}) = -1, \chi(\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}) = 1, \chi(\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}) = 1, \chi(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}) = -1.$$

Then χ would be trivial on the ideal

$$\{\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\}$$

and so would not be a generating character.

4 The Hull of the Jacobson Radical

We have shown the importance of finding an additive map on the socle of the ring that contains no non-trivial ideals. There is an ideal possibly smaller than the socle which can serve a similar purpose. We now describe that ideal.

For R a finite ring and I a left ideal of R, let $\mathcal{H}(I) = I \cap \mathcal{R}(I)$. The notation here is inspired by the use of the hull when using codes to study designs, which is defined to be $C \cap C^{\perp}$.

Theorem 4.1. *Let R be a finite Frobenius ring. Then $\mathcal{H}(J(R))$ is a self-orthogonal two sided ideal with the property that $\mathcal{H}(J(R))^2 = 0$.*

Proof. First, $\mathcal{H}(J(R))$ is the intersection of two sided ideals and is therefore a two sided ideal. Let $a \in \mathcal{H}(J(R))$ then $a \in J(R)$ and $a \in \mathcal{R}(J(R))$ which implies $a^2 = 0$ so that the ideal is self-orthogonal, namely it is contained in its right orthogonal. □

Theorem 4.2. *If R is a local Frobenius ring then $\mathcal{H}(J(R)) = \mathcal{R}(J(R)) = soc(R)$.*

Proof. First since the ring is Frobenius, we have that $\mathcal{R}(J(R)) = soc(R)$. The ideal $J(R)$ is the unique maximal ideal in a local ring R so $\mathcal{R}(J(R))$ must be contained in $J(R)$ which gives the result. □

Theorem 4.3. *Let R be a finite Frobenius ring. If τ is an additive map, $\tau : R \to \mathbb{C}^*$ such that τ is non-trivial on right ideals in $\mathcal{H}(J(R))$, then τ is non-trivial on all right ideals in R.*

Proof. The socle $soc(R)$ is defined as the sum of the minimal right ideals of R. Hence any minimal right ideal must be contained in the right socle. Any minimal right ideal I of R must have an ideal I' which is $I \cap J(R)$, but I is minimal which means $I = I'$. Therefore the ideal is in both $J(R)$ and $\mathcal{R}(J(R)) = soc(R)$. This gives that any minimal right ideal in R is a minimal right ideal in $J(R) \cap \mathcal{R}(J(R)) = \mathcal{H}(J(R))$ which gives the result. □

Theorem 4.4. *Let R be a finite Frobenius ring. If $\mathcal{H}(J(R))$ contains no non-trivial right ideals then any non-trivial additive map τ defined on the additive group of $\mathcal{H}(J(R))$ extended to the additive group of R forms a generating character for R.*

Proof. If $\mathcal{H}(J(R))$ contains no non-trivial right ideals then τ cannot be trivial on a non-trivial right ideal of R. Since the map is defined non-trivially on the additive group of $\mathcal{H}(J(R))$ it does not contain this ideal in its kernel. □

Example 7. *Let us consider the ring $R = \mathbb{F}_2[X]/(X^n)$. We have that $J(R)$ is the ideal generated by $x = X + (X^n)$. The ring R is in fact a local ring and $\mathcal{H}(J(R))$ is the ideal generated by x^{n-1} i.e. $\mathcal{H}(J(R)) = \{0, x^{n-1}\}$ which is a minimal ideal in R. The only additive map τ defined on $\mathcal{H}(J(R))$ is given by $\tau(0) = 1$ and $\tau(x^{n-1}) = -1$.*

The conditions of Theorem 4.4 occur often. For example, for local rings, we have that $\mathcal{H}(J(R))$ is the unique minimal ideal. Then it contains no non-trivial ideals. If $R = M_n(\mathbb{F}_q)$ then $J(R) = \{0\}$ giving that $\mathcal{H}(J(R)) = \{0\}$ and therefore it contains no non-trivial ideals.

Theorem 4.5. *Let R be a finite Frobenius ring and I be any two sided ideal of R. Then $\mathcal{R}(\mathcal{H}(I)) = \mathcal{L}(\mathcal{H}(I)) = I + \mathcal{R}(I)$.*

Proof. We have that since $\mathcal{H}(I) = I \cap \mathcal{R}(I)$ then $I + \mathcal{R}(I) \subseteq \mathcal{R}(\mathcal{H}(I))$. Then

$$|\mathcal{R}(\mathcal{H}(I))| = \frac{|R|}{|\mathcal{H}(I)|} = \frac{|I||\mathcal{R}(I)|}{|\mathcal{H}(I)|} = \frac{|I||\mathcal{L}(I)|}{|\mathcal{H}(I)|} = |\mathcal{L}(\mathcal{H}(I))| = |I + \mathcal{R}(I)|.$$

Then since we have containment and the cardinalities are the same the ideals must be equal. □

In particular, $\mathcal{R}(\mathcal{H}(J(R))) = J(R) + soc(R)$. Notice that we are using heavily that the ring is Frobenius in that we often use that for a left linear code C of length n, we have that $|C||\mathcal{R}(C)| = |R|^n$. In the case of the previous theorems, the codes are of length 1.

Corollary 4.6. *Let R be a finite Frobenius ring. If $J(R) + soc(R)$ is a maximal ideal of R or $J(R) + soc(R) = R$ then any non-trivial additive map τ defined on the additive group of $\mathcal{H}(J(R))$ extended to R forms a generating character for R.*

Proof. If $J(R) + soc(R)$ is a maximal ideal then $\mathcal{R}(\mathcal{H}(J(R)))$ is a maximal ideal and so $\mathcal{H}(J(R))$ is a minimal ideal. If $J(R) + soc(R) = R$ then $\mathcal{H}(J(R)) = \{0\}$. In both cases, the result follows from Theorem 4.4. □

5 Conclusion

Generating characters for finite Frobenius rings are the key to finding the MacWilliams relations for codes over a specific ring. The MacWilliams relations are one of the foundational results of algebraic coding theory. In fact, we only study codes in spaces where the MacWilliams relations exist. In this work, we have shown how to construct a generating character for an arbitrary Frobenius ring and we have given numerous examples of finding generating characters for specific rings. We have also identified another ideal which allows us to find generating characters based on maps from this ideal.

References

[1] A. J. Berkson, The u-algebra over restricted Lie algebra is Frobenius, Proceeding. A. M. S., vol. 15, 1964, 14 - 15.

[2] H. L. Claasen, R. W. Goldbach, A field like property of finite rings, Indag. Math. vol 3, 1992, 11 - 26.

[3] S. T. Dougherty, Foundations of Algebraic Coding Theory, Contemporary Mathematics, vol. 634, 2015, 101 - 136.

[4] S. T. Dougherty, Algebraic Coding Theory over Finite over Finite Commutative Rings, Spinger-Verlag, (2017).

[5] S. T. Dougherty, A. Leroy, Self-dual codes over non-commutative Frobenius rings, Applicable Algebra in Engineering, Communication and Computing, vol. 27, no. 3, 185 - 203.

[6] S. T. Dougherty, E. Saltürk, S. Szabo, Codes over local rings of order 16, Advances in Mathematics of Communication, vol. 10, no. 2, May 2016, 379 - 391.

[7] T. Y. Lam, Lectures on Modules and Rings, Springer-Verlag, 1999.

[8] F. J. MacWilliams, Combinatorial problems of elementary group theory, Ph.D. thesis, Harvard University, 1961.

[9] F. J. MacWilliams, A theorem on the distribution of weights in a systematic code, Bell System Tech. J., vol. 42, 1963, 79 - 94.

[10] S. Montgomery, Hopf algebras and their actions on rings, CBMS, vol. 82, American Mathematical Society, 1993.

[11] J. Wood, Duality for modules over finite rings and applications to coding theory, Amer. J. Math., vol. 121, 1999, 555 - 575.

[12] Wood, J. Applications of finite Frobenius rings to the foundations of algebraic coding theory. Proceedings of the 44th Symposium on Ring Theory and Representation Theory, Symp. Ring Theory Represent. Theory Organ. Comm., Nagoya, 2012, 223 - 245.