LECTURE NOTES ON DUAL CODES AND THE MACWILLIAMS IDENTITIES
—
FOR THE WORKSHOP ON CODING THEORY AND GEOMETRY OF RATIONAL SURFACES MORELIA, MICHOACÁN, MÉXICO SEPTEMBER 23–26, 2009
—
DRAFT VERSION OF SEPTEMBER 23, 2009

JAY A. WOOD

Abstract. These lecture notes discuss the MacWilliams identities in several contexts: additive codes, linear codes over rings, and linear codes over modules. The last section addresses self-dual codes defined over non-commutative rings. The original study of these topics began with work of MacWilliams in the context of linear codes defined over finite fields, and the last section extends work of Nebe, Rains, and Sloane.

Contents

1991 *Mathematics Subject Classification.* Primary 94B05.

Key words and phrases. Hamming weight, linear codes over modules, dual codes, weight enumerators, MacWilliams identities, Frobenius ring, Frobenius bimodule, involution.

1. Introduction

These lecture notes are in large part a re-ordered subset of the lecture notes I prepared for the summer school on Codes over Rings, held August 18–29, 2008, at the Middle East Technical University, Ankara, Turkey [18]. Except for the last section, they are almost identical to lecture notes used at the International School and Conference on Coding Theory held at CIMAT, Guanajuato, México, in November and December 2008.

The MacWilliams identities are very well known. The exposition here is geared primarily towards understanding the features one should expect in a well-behaved dual code. These features, valid for linear codes defined over a finite field, are summarized in what I refer to as a "model theorem," Theorem 2.1.1. This model theorem is first generalized to additive codes defined over a finite abelian group, a theorem due essentially to Delsarte [4]. The exposition then turns to linear codes defined over a finite ring or over a finite module and to the extra hypotheses needed in order that the model theorem still hold. This exposition was strongly influenced by the desire to understand the interplay between dual codes defined by using a $\mathbb{Q}/\mathbb{Z}$-valued biadditive form and dual codes defined by using a bilinear form with values in the ground ring. I became aware of this interplay from the book [13].

While the material on the MacWilliams identities is mostly self-contained, it is not entirely so. I have included several short sections of background material in an attempt to keep prerequisites to a minimum.

The last section is an outline of recent work on defining self-dual codes in the non-commutative context, extending work of Nebe, Rains, and Sloane in [13]. Greater detail is available in [17].

Acknowledgments. I thank the organizers of the Workshop on Coding Theory and Geometry of Rational Surfaces for the opportunity to present this material. I also thank my wife Elizabeth Moore for her support.

2. A model theorem

In this section we describe a theorem, valid over finite fields, involving linear codes, their dual codes, and the MacWilliams identities between their Hamming weight enumerators. This theorem will serve as a model for subsequent generalizations to additive codes, linear codes over rings or modules, and other weight enumerators.

2.1. **Classical case of finite fields.** We recall without proofs the classical situation of linear codes over finite fields, their dual codes, and the MacWilliams identities between the Hamming weight enumerators of a linear code and its dual code. This material is standard and can be found in [12]. Proofs of generalizations will be provided in subsequent sections.

Let $\mathbb{F}_q$ be a finite field with q elements. Define $\langle \cdot, \cdot \rangle : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ by

$$\langle x, y \rangle = \sum_{j=1}^{n} x_j y_j,$$

for $x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_q^n$. The operations are those of the finite field $\mathbb{F}_q$. The pairing $\langle \cdot, \cdot \rangle$ is a non-degenerate symmetric bilinear form.

A *linear code of length* n is a linear subspace $C \subset \mathbb{F}_q^n$. It is traditional to denote $k = \dim C$. The *dual code* $C^\perp$ is defined by:

$$C^\perp = \{y \in \mathbb{F}_q^n : \langle x, y \rangle = 0, \text{ for all } x \in C\}.$$

The *Hamming weight* $\mathrm{wt} : \mathbb{F}_q \to \mathbb{Q}$ is defined by $\mathrm{wt}(a) = 1$ for $a \neq 0$, and $\mathrm{wt}(0) = 0$. The Hamming weight is extended to a function $\mathrm{wt} : \mathbb{F}_q^n \to \mathbb{Q}$ by

$$\mathrm{wt}(x) = \sum_{j=1}^{n} \mathrm{wt}(x_j), \quad x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n.$$

Then $\mathrm{wt}(x)$ equals the number of non-zero entries of $x \in \mathbb{F}_q^n$.

The *Hamming weight enumerator* of a linear code C is a polynomial $W_C(X, Y)$ in $\mathbb{C}[X, Y]$ defined by

$$W_C(X, Y) = \sum_{x \in C} X^{n-\mathrm{wt}(x)} Y^{\mathrm{wt}(x)} = \sum_{j=0}^{n} A_j X^{n-j} Y^j,$$

where A_j is the number of codewords in C of Hamming weight j.

The following theorem summarizes the essential properties of $C^\perp$ and the Hamming weight enumerator. This theorem will serve as a model for results in later sections.

Theorem 2.1.1. *Suppose C is a linear code of length n over a finite field $\mathbb{F}_q$. The dual code $C^\perp$ satisfies:*

(1) $C^\perp \subset \mathbb{F}_q^n$;
(2) $C^\perp$ *is a linear code of length* n;
(3) $(C^\perp)^\perp = C$;
(4) $\dim C^\perp = n - \dim C$ (*or* $|C| \cdot |C^\perp| = |\mathbb{F}_q^n| = q^n$); *and*

(5) (*the MacWilliams identities,* [10], [11])

$$W_{C^\perp}(X,Y) = \frac{1}{|C|} W_C(X+(q-1)Y, X-Y).$$

2.2. **Plan of attack.** In subsequent sections, Theorem 2.1.1 will be generalized in various ways, first to additive codes, then to linear codes over rings and modules, and finally to other weight enumerators. In order to maintain our focus on the central issue of duality, only the Hamming weight enumerator will be discussed initially.

As we will see in the discussion of additive codes (Section 4), one natural choice for a dual code to a code $C \subset G^n$ will be the character-theoretic annihilator $(\widehat{G}^n : C)$. The drawback of this choice is that the annihilator is not a code in the original ambient space G^n; rather, it is a code in $\widehat{G}^n$. By introducing a nondegenerate biadditive form on G^n (Subsection 4.3), one establishes a choice of identification between G^n and $\widehat{G}^n$. This will remedy the drawback of the dual not being a code in the original ambient space.

At the next stage of generalization, linear codes over rings (Section 5), one must be mindful to ensure that the dual code is again a linear code, that the size of the dual is correct, and that the double dual property is satisfied. The latter requirement will force the ground ring to be quasi-Frobenius. In order that the dual code be linear, the biadditive form needs to be bilinear, yet still provide an identification between R^n and $\widehat{R}^n$. This and the size restriction will place an additional requirement on the ground ring, that it be Frobenius.

For linear codes over a module A, very nice formulations of duality are possible when one allows the dual code to sit in $\widehat{A}^n$ or when one allows the ring to have an involution ε such that $\widehat{A} \cong \varepsilon(A)$. The latter situation is the focus of Section 7.

Once duality has been sorted out, the generalizations to other weight enumerators will be comparatively straight-forward (Section 6).

3. Characters

We begin by discussing characters of finite abelian groups and of finite rings.

Throughout this section G is a finite abelian group under addition. A *character* of G is a group homomorphism $\pi : G \to \mathbb{C}^\times$, where $\mathbb{C}^\times$ is the multiplicative group of nonzero complex numbers.

3.1. **Basic results.** Denote by $\widehat{G} = \mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{C}^\times)$ set of all characters of G; $\widehat{G}$ is a finite abelian group under pointwise multiplication of functions: $(\pi\theta)(x) := \pi(x)\theta(x)$, for $x \in G$. The identity element of the group $\widehat{G}$ is the *principal character* $\pi_0 = 1$, with $\pi_0(x) = 1$ for all $x \in G$.

Let $F(G, \mathbb{C}) = \{f : G \to \mathbb{C}\}$ be the set of all functions from G to the complex numbers $\mathbb{C}$; $F(G, \mathbb{C})$ is a vector space over the complex numbers of dimension $|G|$. For $f_1, f_2 \in F(G, \mathbb{C})$, define

$$\langle f_1, f_2 \rangle = \frac{1}{|G|} \sum_{x \in G} f_1(x) \bar{f}_2(x). \tag{3.1.1}$$

Then $\langle \cdot, \cdot \rangle$ is a positive definite Hermitian inner product on $F(G, \mathbb{C})$.

The following statement of basic results is left as an exercise for the reader (see, for example, [14] or [15]).

Proposition 3.1.1. *Let G be a finite abelian group, with character group $\widehat{G}$. Then:*

(1) *$\widehat{G}$ is isomorphic to G, but not naturally so;*
(2) *G is naturally isomorphic to the double character group $(\widehat{G})\widehat{\ }$;*
(3) *$|\widehat{G}| = |G|$;*
(4) *$(G_1 \times G_2)\widehat{\ } \cong \widehat{G}_1 \times \widehat{G}_2$, for finite abelian groups G_1, G_2;*
(5) $\sum_{x \in G} \pi(x) = \begin{cases} |G|, & \pi = 1, \\ 0, & \pi \neq 1; \end{cases}$
(6) $\sum_{\pi \in \widehat{G}} \pi(x) = \begin{cases} |G|, & x = 0, \\ 0, & x \neq 0; \end{cases}$
(7) *The characters of G form an orthonormal basis of $F(G, \mathbb{C})$ with respect to the inner product $\langle, \rangle$.*

3.2. **Additive form of characters.** It will sometimes be convenient to view the character group $\widehat{G}$ additively. Given a finite abelian group G, define its *dual abelian group* by $\mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{Q}/\mathbb{Z})$. The dual abelian group is written additively, and its identity element is written 0, which is the zero homomorphism from G to $\mathbb{Q}/\mathbb{Z}$. The complex exponential function defines a group homomorphism $\mathbb{Q}/\mathbb{Z} \to \mathbb{C}^\times$, $x \mapsto \exp(2\pi i x)$, which is injective and whose image is the subgroup of elements of finite order in $\mathbb{C}^\times$. The complex exponential in turn induces a group homomorphism

$$\mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{Q}/\mathbb{Z}) \to \widehat{G} = \mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{C}^\times). \tag{3.2.1}$$

When G is finite, the mapping (3.2.1) is an isomorphism.

Because there will be situations where it is convenient to write characters multiplicatively and other situations where it is convenient to write characters additively, we adopt the following convention.

Notational Convention. Characters written in multiplicative form, i.e., characters viewed as elements of $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{C}^\times)$ will be denoted by the "standard" Greek letters π, θ, ϕ, and ρ. Characters written in additive form, i.e., characters viewed as elements of $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z})$, will be denoted by the corresponding "variant" Greek letters ϖ, ϑ, φ, and ϱ, so that $\pi = \exp(2\pi i \varpi)$, $\theta = \exp(2\pi i \vartheta)$, etc.

The ability to write characters additively will become very useful when G has the additional structure of (the underlying abelian group of) a module over a ring (subsection 3.3).

We warn the reader that in the last three items of Proposition 3.1.1, the sums (or linear independence) take place in (or over) the complex numbers. These results must be written with the characters in multiplicative form.

Let $H \subset G$ be a subgroup, and define the *annihilator* $(\widehat{G} : H) = \{\varpi \in \widehat{G} : \varpi(h) = 0, \text{ for all } h \in H\}$. Then $(\widehat{G} : H)$ is isomorphic to the character group of G/H, so that $|(\widehat{G} : H)| = |G|/|H|$.

Proposition 3.2.1. *Let H be a subgroup of G with the property that $H \subset \ker \varpi$ for all characters $\varpi \in \widehat{G}$. Then $H = 0$.*

Proof. The hypothesis implies that $(\widehat{G} : H) = \widehat{G}$. Calculating $|H| = 1$, we conclude that $H = 0$. □

3.3. **Character modules.** If the finite abelian group G is the additive group of a module M over a ring R, then the character group $\widehat{M}$ inherits an R-module structure. In this process, sides get reversed; i.e., if M is a left R-module, then $\widehat{M}$ is a right R-module, and vice versa.

Explicitly, if M is a left R-module, then the right R-module structure of $\widehat{M}$ is defined by

$$(\varpi r)(m) := \varpi(rm), \quad \varpi \in \widehat{M}, r \in R, m \in M.$$

Similarly, if M is a right R-module, then the left R-module structure of $\widehat{M}$ is given by

$$(r\varpi)(m) := \varpi(mr), \quad \varpi \in \widehat{M}, r \in R, m \in M.$$

Remark 3.3.1. When $\widehat{M}$ is written in multiplicative form, one may see the scalar multiplication for the module structure written in exponential form (for example, in [16]):

$$\pi^r(m) := \pi(rm), \quad \pi \in \widehat{M}, r \in R, m \in M,$$

when M is a left R-module and $\widehat{M}$ is a right R-module, and

$${}^r\pi(m) := \pi(mr), \quad \pi \in \widehat{M}, r \in R, m \in M,$$

when M is a right R-module and $\widehat{M}$ is a left R-module. The reader will verify such formulas as $(\pi^r)^s = \pi^{rs}$ and $(\pi\theta)^r = \pi^r\theta^r$.

Lemma 3.3.2. *Let R be a finite ring, with $\widehat{R}$ its character bimodule. If $r\widehat{R} = 0$ (resp., $\widehat{R}r = 0$), then $r = 0$.*

Proof. Suppose $r\widehat{R} = 0$. For any $\varpi \in \widehat{R}$ and $x \in R$, we have $0 = r\varpi(x) = \varpi(xr)$. Thus $Rr \subset \ker \varpi$, for all $\varpi \in \widehat{R}$. By Proposition 3.2.1, $Rr = 0$, so that $r = 0$. □

4. MacWilliams identities for additive codes

In this section we generalize the model Theorem 2.1.1 to additive codes over finite abelian groups. We begin with a review of the Fourier transform and the Poisson summation formula, which will be key tools in proving the MacWilliams identities.

4.1. Fourier transform and Poisson summation formula.

In this subsection we record some of the basic properties of the Fourier transform on a finite abelian group (cf. [15]). We make use of the material in Section 3. The proofs are left as exercises for the reader.

Suppose that G is a finite abelian group and that V is a vector space over the complex numbers. Let $F(G, V) = \{f : G \to V\}$ be the set of all functions from G to V; $F(G, V)$ is vector space over the complex numbers.

The *Fourier transform* $\widehat{\ } : F(G, V) \to F(\widehat{G}, V)$ is defined by

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

Notice that the characters are in multiplicative form. The Fourier transform is a linear transformation with inverse transformation determined by the following relation.

Proposition 4.1.1 (Fourier inversion formula)**.**

$$f(x) = \frac{1}{|G|} \sum_{\pi \in \widehat{G}} \pi(-x) \widehat{f}(\pi), \quad x \in G, \quad f \in F(G, V).$$

Theorem 4.1.2 (Poisson summation formula)**.** *Let H be a subgroup of a finite abelian group G. Then, for any $a \in G$,*

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

In particular, when $a = 0$ *(or* $a \in H$*),*

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

When the vector space V has the additional structure of a commutative complex algebra, we have the following technical result.

Proposition 4.1.3. *Suppose that* $\mathcal{V}$ *is a commutative complex algebra. Suppose that* $f \in F(G^n, \mathcal{V})$ *has the form*

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

where $f_1, \dots, f_n \in F(G, \mathcal{V})$*. Then* $\widehat{f} = \prod \widehat{f}_i$*; i.e., for* $\pi = (\pi_1, \dots, \pi_n) \in \widehat{G^n} \cong \widehat{G}^n$*,*

$$\widehat{f}(\pi) = \prod_{i=1}^{n} \widehat{f}_i(\pi_i).$$

4.2. **Additive codes.** Let $(G, +)$ be a finite abelian group. An *additive code of length* n over G is a subgroup $C \subset G^n$. Hamming weight on G is defined as before, for $a \in G$ and $x = (x_1, \dots, x_n) \in G^n$:

$$\mathrm{wt}(a) = \begin{cases} 1, & a \neq 0, \\ 0, & a = 0; \end{cases} \quad \mathrm{wt}(x) = \sum_{j=1}^{n} \mathrm{wt}(x_j).$$

Thus, $\mathrm{wt}(x)$ is the number of nonzero entries of x.

Given an additive code $C \subset G^n$, one way to define its dual code is via the character-theoretic annihilator $(\widehat{G}^n : C)$.

As before, the Hamming weight enumerator of an additive code $C \subset G^n$ is:

$$W_C(X, Y) = \sum_{x \in C} X^{n - \mathrm{wt}(x)} Y^{\mathrm{wt}(x)} = \sum_{j=0}^{n} A_j X^{n-j} Y^j,$$

where A_j is the number of codewords of Hamming weight j in C.

The model Theorem 2.1.1 then takes the following form. This result is a variant of a theorem of Delsarte [4].

Theorem 4.2.1. *Suppose* C *is an additive code of length* n *over a finite abelian group* G*. The annihilator* $(\widehat{G}^n : C)$ *satisfies:*

1. $(\widehat{G}^n : C) \subset \widehat{G}^n$*;*
2. $(\widehat{G}^n : C)$ *is an additive code of length* n *in* $\widehat{G}^n$*;*
3. $(G^n : (\widehat{G}^n : C)) = C$*;*
4. $|C| \cdot |(\widehat{G}^n : C)| = |G^n|$*; and*

(5) *the MacWilliams identities hold:*

$$W_{(\widehat{G}^n:C)}(X,Y) = \frac{1}{|C|} W_C(X + (|G|-1)Y, X - Y).$$

The first four properties are clear from the definition of $(\widehat{G}^n : C)$; that $(\widehat{G}^n : C)$ is an additive code in $\widehat{G}^n$ is seen most clearly when characters are written in additive form. For the proof of the MacWilliams identities, we follow Gleason's use of the Poisson summation formula (see [1, §1.12]). To that end, we first lay some groundwork.

Let $\mathcal{V} = \mathbb{C}[X,Y]$, a commutative complex algebra, and let $f_i : G \to \mathbb{C}[X,Y]$ be given by $f_i(x_i) = X^{1-\mathrm{wt}(x_i)} Y^{\mathrm{wt}(x_i)}$, $x_i \in G$. Now define $f : G^n \to \mathbb{C}[X,Y]$ by

$$f(x_1,\ldots,x_n) = \prod_{i=1}^n f_i(x_i) = \prod_{i=1}^n X^{1-\mathrm{wt}(x_i)} Y^{\mathrm{wt}(x_i)} = X^{n-\mathrm{wt}(x)} Y^{\mathrm{wt}(x)},$$

for $x = (x_1,\ldots,x_n) \in G^n$.

Lemma 4.2.2. *For $f_i(x_i) = X^{1-\mathrm{wt}(x_i)} Y^{\mathrm{wt}(x_i)}$, $x_i \in G$, and $\pi_i \in \widehat{G}$,*

$$\widehat{f}_i(\pi_i) = \begin{cases} X + (|G|-1)Y, & \pi_i = 1 \quad (\varpi_i = 0), \\ X - Y, & \pi_i \neq 1 \quad (\varpi_i \neq 0). \end{cases}$$

Thus,

$$\widehat{f}(\pi) = (X + (|G|-1)Y)^{n-\mathrm{wt}(\varpi)} (X - Y)^{\mathrm{wt}(\varpi)},$$

where $\pi = (\pi_1,\ldots,\pi_n) \in \widehat{G^n} = \widehat{G}^n$.

Proof. By the definition of the Fourier transform,

$$\widehat{f}_i(\pi_i) = \sum_{x_i \in G} \pi_i(x_i) f(x_i) = \sum_{x_i \in G} \pi_i(x_i) X^{1-\mathrm{wt}(x_i)} Y^{\mathrm{wt}(x_i)}.$$

Split the sum into the $x_i = 0$ term and the remaining $x_i \neq 0$ terms:

$$\widehat{f}_i(\pi_i) = X + \sum_{x_i \neq 0} \pi_i(x_i) Y.$$

By Proposition 3.1.1, the character sum equals $|G| - 1$ when $\pi_i = 1$ $(\varpi_i = 0)$, while it equals -1 when $\pi_i \neq 1$ $(\varpi_i \neq 0)$. The result for $\widehat{f}_i$ follows. Use Proposition 4.1.3 to obtain the formula for $\widehat{f}$. □

Proof of the MacWilliams identities in Theorem 4.2.1. We use $f(x) = X^{n-\mathrm{wt}(x)} Y^{\mathrm{wt}(x)}$ as defined above. By the Poisson summation formula, Theorem 4.1.2, we have

$$\begin{aligned} W_C(X,Y) &= \sum_{x \in C} f(x) = \frac{1}{|(\widehat{G}^n : C)|} \sum_{\varpi \in (\widehat{G}^n : C)} \widehat{f}(\pi) \\ &= \frac{1}{|(\widehat{G}^n : C)|} \sum_{\varpi \in (\widehat{G}^n : C)} (X + (|G|-1)Y)^{n - \mathrm{wt}(\varpi)} (X - Y)^{\mathrm{wt}(\varpi)} \\ &= \frac{1}{|(\widehat{G}^n : C)|} W_{(\widehat{G}^n : C)}(X + (|G|-1)Y, X - Y). \end{aligned}$$

Interchanging the roles of C and $(\widehat{G}^n : C)$ yields the form of the identities stated in the theorem. □

Remark 4.2.3. In comparing Theorem 4.2.1 with Theorem 2.1.1, the only drawback is that the "dual code" $(\widehat{G}^n : C)$ lives in $\widehat{G}^n$, not G^n. One way to address this deficiency will be the use of biadditive forms in subsection 4.3.

4.3. **Biadditive forms.** Biadditive forms are introduced in order to make identifications between a finite abelian group G and its character group $\widehat{G}$.

Let G, H, and E be abelian groups. A *biadditive form* is a map $\beta : G \times H \to E$ such that $\beta(x, \cdot) : H \to E$ is a homomorphism for all $x \in G$ and $\beta(\cdot, y) : G \to E$ is a homomorphism for all $y \in H$. Observe that β induces two group homomorphisms:

$$\begin{aligned} &\chi : G \to \mathrm{Hom}_{\mathbb{Z}}(H, E), && \chi_x(y) = \beta(x,y), \quad x \in G, y \in H; \\ &\psi : H \to \mathrm{Hom}_{\mathbb{Z}}(G, E), && \psi_y(x) = \beta(x,y), \quad x \in G, y \in H. \end{aligned}$$

The biadditive form β is *nondegenerate* if both maps χ and ψ are injective. Extend β to $\beta : G^n \times H^n \to E$ by

$$\beta(a,b) = \sum_{j=1}^{n} \beta(x_j, y_j), \quad x = (x_1, \ldots, x_n) \in G^n, y = (y_1, \ldots, y_n) \in H^n.$$

If G and H are finite abelian groups and $E = \mathbb{Q}/\mathbb{Z}$, then recall that $\mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{Q}/\mathbb{Z}) \cong \widehat{G}$, so that a nondegenerate biadditive form $\beta : G \times H \to \mathbb{Q}/\mathbb{Z}$ induces two injective homomorphisms, $\chi : G \to \widehat{H}$ and $\psi : H \to \widehat{G}$. Because $|G| = |\widehat{G}|$, we conclude that χ and ψ are isomorphisms, so that $G \cong H$. Thus, there is no loss of generality to have $G = H$, with a nondegenerate biadditive form $\beta : G \times G \to \mathbb{Q}/\mathbb{Z}$. Observe now that $\chi = \psi$ if and only if the form β is symmetric. Equivalently, $\chi_x(y) = \chi_y(x)$ for all $x, y \in G$ if and only if β is symmetric.

For an additive code $C \subset G^n$, the character-theoretic annihilator $(\widehat{G}^n : C) \subset \widehat{G}^n$ corresponds, under the isomorphisms χ, ψ, to the annihilators determined by β:

$$l(C) := \{y \in G^n : \beta(y, x) = 0, \text{ for all } x \in C\} \qquad \text{(under } \chi),$$
$$r(C) := \{z \in G^n : \beta(x, z) = 0, \text{ for all } x \in C\} \qquad \text{(under } \psi).$$

Observe that $l(r(C)) = C$ and $r(l(C)) = C$. Of course, if β is symmetric, then $l(C) = r(C)$. To summarize:

Proposition 4.3.1. *Suppose G is a finite abelian group and $\beta : G \times G \to \mathbb{Q}/\mathbb{Z}$ is a nondegenerate biadditive form. The annihilators $l(C)$ and $r(C)$ of an additive code $C \subset G^n$ satisfy*

(1) *$l(C), r(C) \subset G^n$;*
(2) *$l(C), r(C)$ are additive codes of length n in G^n;*
(3) *$l(r(C)) = C$ and $r(l(C)) = C$;*
(4) *$|C| \cdot |l(C)| = |C| \cdot |r(C)| = |G^n|$; and*
(5) *the MacWilliams identities hold:*

$$W_{l(C)}(X, Y) = \frac{1}{|C|} W_C(X + (|G| - 1)Y, X - Y) = W_{r(C)}(X, Y).$$

If β is symmetric, then $l(C) = r(C)$. Moreover, for any finite abelian group G, there exists a nondegenerate, symmetric biadditive form $\beta : G \times G \to \mathbb{Q}/\mathbb{Z}$.

5. Duality for modules

In this section we discuss dual codes and the MacWilliams identities in the context of linear codes defined over a finite ring or, even more generally, over a finite module over a finite ring.

5.1. **Linear codes.** Fix a finite ring R with 1. The ring R may not be commutative. Also fix a finite left R-module A, which will serve as the alphabet for R-linear codes. A left *R-linear code* of length n over the alphabet A is a left R-submodule $C \subset A^n$. An important special case is when the alphabet A equals R itself.

Remember that the character group $\widehat{A}$ of A admits a right R-module structure via $\varpi r(a) = \varpi(ra)$, for $r \in R$, $a \in A$, and $\varpi \in \widehat{A}$.

For an R-linear code $C \subset A^n$, the character-theoretic annihilator $(\widehat{A}^n : C) = \{\varpi \in \widehat{A}^n : \varpi(C) = 0\}$ is a right submodule of $\widehat{A}^n$.

Proposition 5.1.1. *The annihilator $(\widehat{A}^n : C)$ of an R-linear code $C \subset A^n$ satisfies*

(1) *$(\widehat{A}^n : C) \subset \widehat{A}^n$;*

(2) $(\widehat{A}^n : C)$ *is a right* R*-linear code of length* n *in* $\widehat{A}^n$*;*
(3) $(A^n : (\widehat{A}^n : C)) = C$*;*
(4) $|C| \cdot |(\widehat{A}^n : C)| = |A^n|$*; and*
(5) *the MacWilliams identities hold:*

$$W_{(\widehat{A}^n : C)}(X, Y) = \frac{1}{|C|} W_C(X + (|A| - 1)Y, X - Y).$$

The only drawback is that the annihilator $(\widehat{A}^n : C)$ is not a code over the original alphabet A. As was the case for additive codes, one way to remedy this drawback is to use nondegenerate bilinear forms. We will introduce bilinear forms in a very general context and then be more specific as we proceeed.

5.2. **Bilinear forms.** Let R and S be finite rings with 1, A a finite left R-module, B a finite right S-module, and E a finite (R, S)-bimodule. In this context, a *bilinear form* is a map $\beta : A \times B \to E$ such that $\beta(a, \cdot) : B \to E$ is a right S-module homomorphism for all $a \in A$ and $\beta(\cdot, b) : A \to E$ is a left R-module homomorphism for all $b \in B$. Observe that β induces two module homomorphisms:

$$\begin{aligned} \chi &: A \to \mathrm{Hom}_S(B, E), \qquad && \chi_a(b) = \beta(a, b), \quad a \in A, b \in B; \\ \psi &: B \to \mathrm{Hom}_R(A, E), \qquad && \psi_b(a) = \beta(a, b), \quad a \in A, b \in B. \end{aligned}$$

The bilinear form β is *nondegenerate* if both maps ϕ and ψ are injective. Extend β to $\beta : A^n \times B^n \to E$ by

$$\beta(a, b) = \sum_{j=1}^{n} \beta(a_j, b_j), \quad a = (a_1, \ldots, a_n) \in A^n, b = (b_1, \ldots, b_n) \in B^n.$$

For subsets $P \subset A^n$ and $Q \subset B^n$ we define annihilators:

$$\begin{aligned} l(Q) &= \{a \in A^n : \beta(a, q) = 0, \text{ for all } q \in Q\}, \\ r(P) &= \{b \in B^n : \beta(p, b) = 0, \text{ for all } p \in P\}. \end{aligned}$$

Observe that $l(Q)$ is a left submodule of A^n and $r(P)$ is a right submodule of B^n. Also observe that $Q \subset r(l(Q))$ and $P \subset l(r(P))$, for $P \subset A^n$ and $Q \subset B^n$.

An important special case is the following example.

Example 5.2.1. Let $R = S$ and let $A = {}_RR$, $B = R_R$ and $E = {}_RR_R$. Define $\beta : R \times R \to R$ by $\beta(a, b) = ab$, where $ab \in R$ is the product in the ring R. Because R has a unit element, β is a nondegenerate bilinear form.

As above, if $P \subset R^n$, then $l(P)$ is a left submodule of R^n and $r(P)$ is a right submodule of R^n. Moreover, if P is also a left (resp., right) submodule of R^n, then $l(P)$ (resp., $r(P)$) is a sub-bimodule of R^n.

Comparing with the model Theorem 2.1.1, the annihilator $r(C)$ of a left linear code $C \subset R^n$ will indeed be a right linear code in R^n. However, we will need to be concerned about two other of the items in Theorem 2.1.1: the double annihilator property and the size property. In the next several subsections we examine these properties in more detail.

5.3. **A crash course on finite quasi-Frobenius and Frobenius rings.** References for this subsection include [8] and [9].

Let R be a finite associative ring with 1. The (*Jacobson*) *radical* $\operatorname{rad}(R)$ of a finite ring R is the intersection of all the maximal left ideals of R. The radical is also the intersection of all the maximal right ideals of R, and the radical is a two-sided ideal of R.

A nonzero module over R is *simple* if it has no nontrivial submodules. Given any left R-module M, the *socle* $\operatorname{soc}(M)$ is the sum of all the simple submodules of M.

A finite ring R is *quasi-Frobenius* (*QF*) if R is self-injective, i.e., injective as a left (right) module over itself. Equivalently ([8, Theorem 15.1]), R is QF if its ideals satisfy the following double annihilator property: for every left ideal $I \subset R$, $l(r(I)) = I$, and for every right ideal $J \subset R$, $r(l(J)) = J$.

A finite ring R is *Frobenius* if $R/\operatorname{rad}(R) \cong \operatorname{soc}(R)$ as left or as right modules. This version of the definition is based on a theorem of Honold, [6, Theorem 2]. Equivalently ([16, Theorem 3.10]), a finite ring R is Frobenius if and only if its character module $\widehat{R}$ is isomorphic to R as left or as right modules over R.

5.4. **The double annihilator property.** Continue to assume the conditions in Example 5.2.1, i.e., $\beta : R^n \times R^n \to R$ is the standard dot product given by

$$\beta(a, b) = \sum_{i=1}^{n} a_i b_i,$$

for $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n) \in R^n$, where $a_i b_i$ is the product in the ring R.

Proposition 5.4.1. *The annihilators $l(D)$, $r(C)$ satisfy:*

1. *If $C \subset R^n$ is a left submodule, then $C \subset l(r(C))$.*
2. *If $D \subset R^n$ is a right submodule, then $D \subset r(l(D))$.*

(3) *Equality holds for all C and D if and only if R is a quasi-Frobenius ring.*

Proof. The first two containments are true even if C, D are merely subsets of R^n. Now consider the last statement. In the case where $n = 1$, equality would mean that $C = l(r(C))$ and $D = r(l(D))$ for every left ideal C and right ideal D of R. In some texts, for example [3, Definition 58.5], this is the definition of a quasi-Frobenius ring. In [8, Theorem 15.1], the double annihilator condition is one of four equivalent conditions that serve to define a quasi-Frobenius ring.

For $n > 1$, the double annihilator condition holds over a quasi-Frobenius ring by a theorem of Hall, [5, Theorem 5.2]. □

5.5. **The size condition.** We continue to assume that $\beta : R^n \times R^n \to R$ is the standard dot product over a finite ring R. Motivated by the previous subsection, we now assume that R is a quasi-Frobenius ring as well.

First, the bad news.

Theorem 5.5.1. *If R is a quasi-Frobenius ring, but not a Frobenius ring, there exists a left ideal $I \subset R$ with $|I| \cdot |r(I)| < |R|$, and there exists a right ideal $J \subset R$ with $|J| \cdot |l(J)| < |R|$.*

It turns out that a QF ring that is not Frobenius has a left ideal of the form $M_{m,k}(\mathbb{F}_q)$, with $k > m$. One can then calculate the size of the annihilator and find that it is too small.

Corollary 5.5.2. *The MacWilliams identites cannnot hold over a non-Frobenius ring R using $l(C)$ and $r(C)$ as the notions of dual codes.*

Proof. Consider the meaning of the MacWilliams identities for linear codes of length 1, i.e., when the linear code $C \subset R$ is a left ideal. Clearly, $W_C(X, Y) = X + (|C| - 1)Y$.

Then, the right side of the MacWilliams identities becomes

$$\begin{aligned} &\frac{1}{|C|} W_C(X + (|R| - 1)Y, X - Y) \\ &\qquad\qquad = \frac{1}{|C|}(X + (|R| - 1)Y + (|C| - 1)(X - Y)) \\ &\qquad\qquad = X + \left(\frac{|R|}{|C|} - 1\right) Y. \end{aligned}$$

This latter equals the Hamming weight enumerator for $r(C)$ (or $l(C)$) if and only if $|C| \cdot |r(C)| = |R|$ (or $|C| \cdot |l(C)| = |R|$), which contradicts Theorem 5.5.1. □

5.6. **Generating characters.** For the good news, let us return to the general situation of a nondegenerate $\beta : {}_RA \times B_S \to {}_RE_S$.

Theorem 5.6.1. *Suppose $\beta : {}_RA \times B_S \to {}_RE_S$ is a nondegenerate bilinear form. Suppose there exists a character $\varrho : E \to \mathbb{Q}/\mathbb{Z}$ with the property that $\ker \varrho$ contains no nonzero left or right submodules.*

Let $\beta' : A \times B \to \mathbb{Q}/\mathbb{Z}$ be given by $\beta' = \varrho \circ \beta$. Then

(1) *β' is a nondegenerate biadditive form on abelian groups;*
(2) *if $C \subset A^n$ is a left submodule, then $r(C) = r'(C)$;*
(3) *if $D \subset B^n$ is a right submodule, then $l(D) = l'(D)$;*
(4) *$l(r(C)) = C$ for left submodules $C \subset A^n$, and $r(l(D)) = D$ for right submodules $D \subset B^n$;*
(5) *$|C| \cdot |r(C)| = |A^n|$ and $|D| \cdot |l(D)| = |B^n|$;*
(6) *the MacWilliams identities hold for submodules using $r(C)$ and $l(D)$ as the notions of dual codes:*

$$W_{r(C)}(X,Y) = \frac{1}{|C|} W_C(X + (|A|-1)Y, X - Y),$$
$$W_{l(D)}(X,Y) = \frac{1}{|D|} W_D(X + (|B|-1)Y, X - Y).$$

Proof. In order to show that β' is nondegenerate, suppose that $b \in B$ has the property that $\beta'(A,b) = 0$. We need to show that $b = 0$.

Let $\psi_b : A \to E$ be given by $\psi_b(a) = \beta(a,b)$, $a \in A$; ψ_b is a homomorphism of left R-modules. By the hypothesis on b and the definition of β', we see that $\varrho(\psi_b(A)) = 0$; i.e., $\psi_b(A) \subset \ker \varrho$. But $\psi_b(A)$ is a left R-submodule of E, so the hypothesis on ϱ implies that $\psi_b(A) = 0$. Because β was assumed to be nondegenerate, we conclude that $b = 0$. A similar argument proves the nondegeneracy of β' in the other variable.

If $C \subset A^n$ is a left R-submodule, then $\beta' = \varrho \circ \beta$ implies $r(C) \subset r'(C)$. Now suppose that $b \in r'(C)$, i.e., that $\beta'(C,b) = 0$. This implies that $\psi_b(C) = \beta(C,b) \subset \ker \varrho$. But $\psi_b(C)$ is a left R-submodule of E, so the hypothesis on ϱ again implies that $\psi_b(C) = 0$. Thus $b \in r(C)$, and $r(C) = r'(C)$. The proof for $l(D)$ is similar.

The remaining items now follow from Proposition 4.3.1. It follows from the discussion in subsection 4.3 that A and B are isomorphic *as abelian groups.* □

We will call a character ϱ satisfying the hypothesis of Theorem 5.6.1 a *generating character*. A *Frobenius bimodule* is an (R,R)-bimodule E such that $E \cong \widehat{R}$ both as left R-module and as right R-module.

Corollary 5.6.2. *Over any finite ring R, the MacWilliams identities hold in the setting of a nondegenerate bilinear form $\beta : {}_RA \times B_R \to E$, where E is a Frobenius bimodule.*

Proof. A Frobenius bimodule admits a generating character via $E \cong \widehat{R}$ and evaluating at $1 \in R$. $\square$

Theorem 5.6.3. *A finite ring is Frobenius if and only if it admits a generating character ϱ.*

Proof. This is a restatement of [16, Theorem 3.10], one of our equivalent definitions of a Frobenius ring. $\square$

Corollary 5.6.4. *Over a Frobenius ring R, the MacWilliams identities hold in the setting of a nondegenerate bilinear form $\beta : {}_RA \times B_R \to {}_RR_R$.*

To conclude this subsection we illustrate Corollary 5.6.2 by showing a natural pairing $\beta : {}_RA \times B_R \to \widehat{R}$ when $B = \widehat{A}$.

Lemma 5.6.5 ([16, Remark 3.3])**.** *Let M be a finite R-module. Then*

$$\widehat{M} \cong \operatorname{Hom}_R(M, \widehat{R}).$$

Proof. Writing characters in additive form, the definition of the module structure on $\widehat{M}$, i.e., $(\varpi r)(m) = \varpi(rm)$, for $\varpi \in \widehat{M}$, $m \in M$, $r \in R$, shows how $\varpi \in \widehat{M}$ defines an element in $\operatorname{Hom}_R(M, \widehat{R})$. The reader will check that this is an isomorphism. $\square$

Theorem 5.6.6. *Let A be a finite left R-module, and let $B = \widehat{A} \cong \operatorname{Hom}_R(A, \widehat{R})$. The natural evaluation map*

$$\beta : A \times B \cong A \times \operatorname{Hom}_R(A, \widehat{R}) \to \widehat{R},$$

is a nondegenerate bilinear form with values in a Frobenius bimodule. The MacWilliams identities hold in this setting.

Proof. The form β is nondegenerate because for every $a \in A$ there exists a character $\varpi \in \widehat{A}$ with $\varpi(a) \neq 0$. (This is the double dual property of characters: $G \cong (\widehat{G})\widehat{\ }$, from Proposition 3.1.1.) Corollary 5.6.2 implies that the MacWilliams identities hold. $\square$

Finally, we illustrate Theorem 5.6.6 when some additional hypotheses are satisfied. An *involution* $\varepsilon : R \to R$ is an isomorphism at the level of abelian groups such that $\varepsilon(rs) = \varepsilon(s)\varepsilon(r)$, $r, s \in R$, and $\varepsilon^{-1} = \varepsilon$. If R admits an involution ε, then every left R-module M admits a right R-module structure $\varepsilon(M)$, via $xr = \varepsilon(r)x$, for $r \in R$, $x \in M$. Similarly, every right R-module admits a left R-module structure.

Theorem 5.6.7. *Let A be a finite left R-module. Suppose that R admits an involution ε such that $\varepsilon(A) \cong \widehat{A}$. Then there exists*

$$\beta : A \times \varepsilon(A) \to \widehat{R},$$

which is a nondegenerate bilinear form with values in a Frobenius bimodule. The MacWilliams identities hold in this setting.

Proof. Just use Theorem 5.6.6 and the isomorphism $\varepsilon(A) \cong \widehat{A}$. □

Because right submodules of $\varepsilon(A)$ correspond to left submodules of A, the involution ε allows one to consider self-dual codes $C \subset A^n$: those for which $\varepsilon(r(C)) = C$. This is the approach taken in [13], and this approach will be addressed in more detail in Section 7.

6. Other weight enumerators

In this section we discuss two other weight enumerators, the full weight enumerator and the complete weight enumerator. In discussing these two weight enumerators, we follow, in part, the treatment of this material in [13]. We also make use of some of the notation introduced by [2], who in turn build on results of [7].

6.1. **Full weight enumerators.** Let G be a finite abelian group. The full weight enumerator of a code $C \subset G^n$ is essentially a copy of the code inside the complex group ring $\mathbb{C}[G^n]$. Recall that the complex group ring $\mathbb{C}[G^n]$ is the set of all formal complex linear combinations of elements of G^n. One way to notate $\mathbb{C}[G^n]$ is to introduce formal symbols e_x for every $x \in G^n$. Then an element of $\mathbb{C}[G^n]$ has the form

$$\sum_{x \in G^n} \alpha_x e_x,$$

where $\alpha_x \in \mathbb{C}$. Addition in $\mathbb{C}[G^n]$ is performed term-wise: $\sum \alpha_x e_x + \sum \beta_x e_x = \sum (\alpha_x + \beta_x) e_x$. Multiplication is as for polynomials, using the rule $e_x e_y = e_{x+y}$, where the latter is the formal symbol associated to the sum $x + y$ in the group G^n.

Let $f : G^n \to \mathbb{C}[G^n]$ be any function from G^n to $\mathbb{C}[G^n]$. In terms of the basis of e_x, $x \in G^n$, the function f has the form

$$f(x) = \sum_{y \in G^n} \mathcal{B}_{x,y} e_y, \quad \mathcal{B}_{x,y} \in \mathbb{C}.$$

The Fourier transform of f is then $\widehat{f} : \widehat{G}^n \to \mathbb{C}[G^n]$,

$$\widehat{f}(\pi) = \sum_{x \in G^n} \pi(x) f(x) = \sum_{y \in G^n} \left(\sum_{x \in G^n} \pi(x) \mathcal{B}_{x,y} \right) e_y.$$

For any subset $C \subset G^n$ and any function $f : G^n \to \mathbb{C}[G^n]$, define the *full weight enumerator of* C *with respect to* f by $\operatorname{fwe}_C(f) = \sum_{x \in C} f(x)$. Then the Poisson summation formula implies

$$\operatorname{fwe}_C(f) = \frac{1}{|(\widehat{G}^n : C)|} \operatorname{fwe}_{(\widehat{G}^n : C)}(\widehat{f}).$$

In the special case where the function f is $e : G^n \to \mathbb{C}[G^n]$, $e(x) = e_x$, the Fourier transform has the form $\widehat{e}(\pi) = \sum_{x \in G^n} \pi(x) e_x$, and we have the following version of the MacWilliams identities for the full weight enumerator (with respect to e).

Theorem 6.1.1. *For any additive code* $C \subset G^n$*, the full weight enumerator satisfies the following MacWilliams identities:*

$$\operatorname{fwe}_C(e) = \frac{1}{|(\widehat{G}^n : C)|} \operatorname{fwe}_{(\widehat{G}^n : C)}(\widehat{e}).$$

When G is equipped with a nondegenerate biadditive form $\beta : G \times G \to \mathbb{Q}/\mathbb{Z}$, we can make use of the identifications of Proposition 4.3.1. Using the notation of subsection 4.3, if we use $\chi : G \to \widehat{G}$, $\chi(x) = \beta(x, -)$, to make identifications, then the Fourier transform of e is

$$\widehat{e}_\chi(x) = \sum_{y \in G^n} \exp(2\pi i \beta(x, y))\, e_y, \quad x \in G^n.$$

The MacWilliams identities then become

$$\operatorname{fwe}_C(e) = \frac{1}{|l(C)|} \operatorname{fwe}_{l(C)}(\widehat{e}_\chi). \tag{6.1.1}$$

Similarly, if one uses instead $\psi : G \to \widehat{G}$, $\psi(x) = \beta(-, x)$, to make identifications, then one has

$$\widehat{e}_\psi(x) = \sum_{y \in G^n} \exp(2\pi i \beta(y, x))\, e_y, \quad x \in G^n.$$

The MacWilliams identities in this case take the form

$$\operatorname{fwe}_C(e) = \frac{1}{|r(C)|} \operatorname{fwe}_{r(C)}(\widehat{e}_\psi).$$

6.2. **Complete weight enumerators.** The complete weight enumerator will be an element of a certain polynomial ring, which we now define. For every $x \in G$, let Z_x be an indeterminate. Form the polynomial ring on these indeterminates: $\mathbb{C}[Z_x : x \in G]$. We will write $\mathbb{C}[(Z_\bullet)]$ for short.

Given a code $C \subset G^n$, the *complete weight enumerator* of C is

$$\mathrm{cwe}_C((Z_\bullet)) = \sum_{x \in C} \prod_{i=1}^{n} Z_{x_i} = \sum_{x \in C} \prod_{y \in G} Z_y^{c_y(x)} \in \mathbb{C}[(Z_\bullet)],$$

where $c_y(x) = |\{i : x_i = y\}|$ counts the number of components of $x \in G^n$ that equal the element $y \in G$.

A linear change of variables can be specified by $Z_x \mapsto \sum_{y \in G} B_{x,y} Z_y$, where B is a matrix of size $|G| \times |G|$ whose rows and columns are parameterized by the elements of G. Such a linear change of variables induces a homomorphism of $\mathbb{C}$-algebras $M_B : \mathbb{C}[(Z_\bullet)] \to \mathbb{C}[(Z_\bullet)]$ via $M_B(Z_x) = \sum_{y \in G} B_{x,y} Z_y$.

We would now like to compare the full weight enumerator with the complete weight enumerator. A $\mathbb{C}$-linear transformation of vector spaces $S : \mathbb{C}[G^n] \to \mathbb{C}[(Z_\bullet)]$ ("specialization") is completely determined by defining $S(e_x) = \prod_{j=1}^{n} Z_{x_j}$, for $x = (x_1, x_2, \ldots, x_n) \in G^n$. In particular, notice that $S(\mathrm{fwe}_C(e)) = \mathrm{cwe}_C((Z_\bullet))$.

As in the previous subsection, let G be equipped with a nondegenerate biadditive form $\beta : G \times G \to \mathbb{Q}/\mathbb{Z}$, and use $\chi : G \to \widehat{G}$, $\chi(x) = \beta(x, -)$, to make identifications, so that

$$\widehat{e}_\chi(x) = \sum_{y \in G^n} \exp(2\pi i \beta(x,y))\, e_y, \quad x \in G^n.$$

For any subgroup $D \subset G^n$, a computation shows that $S(\mathrm{fwe}_D(\widehat{e}_\chi)) = M_B(\mathrm{cwe}_D((Z_\bullet)))$, where the matrix B is given by

$$B_{x,y} = \exp(2\pi i \beta(x,y)), \quad x, y \in G. \tag{6.2.1}$$

By applying $S : \mathbb{C}[G^n] \to \mathbb{C}[(Z_\bullet)]$ to the MacWilliams identities for the full weight enumerator, (6.1.1), we obtain the MacWilliams identities for the complete weight enumerator:

$$\mathrm{cwe}_C((Z_\bullet)) = \frac{1}{|l(C)|} M_B(\mathrm{cwe}_{l(C)}((Z_\bullet))).$$

If one uses instead $\psi : G \to \widehat{G}$ to make identifications, then B is replaced by its transpose B^t, and the MacWilliams identities take the form:

$$\mathrm{cwe}_C((Z_\bullet)) = \frac{1}{|r(C)|} M_{B^t}(\mathrm{cwe}_{r(C)}((Z_\bullet))).$$

Finally, by mapping Z_0 to X and mapping all the other Z_y, $y \neq 0$, to Y, one induces a specialization map from $\mathbb{C}[(Z_\bullet)]$ to $\mathbb{C}[X, Y]$, which takes $\mathrm{cwe}_C((Z_\bullet))$ to the Hamming weight enumerator $W_C(X, Y)$. A computation using Lemma 4.2.2 shows that $M_B(\mathrm{cwe}_C((Z_\bullet)))$ specializes to $W_C(X + (|G|-1)Y, X - Y)$, where B is given in (6.2.1). In this way, the MacWilliams identities for Hamming weight can be deduced from those for the complete weight enumerator.

Remark 6.2.1. It is possible to define other weight enumerators called *symmetrized weight enumerators*. The MacWilliams identities for these symmetrized weight enumerators (in special situations) first appeared in [16, Theorem 8.4]. More general situations in which the MacWilliams identities hold have been studied in [2] and [7].

7. Self-dual codes in the non-commutative setting

My goal in this section is to clarify the assumptions that lead to a good theory of self-dual codes over non-commutative rings. The section was inspired by, and is an elaboration of portions of, the book by Nebe, Rains, and Sloane [13]. Virtually all of the content of the beginning of this section can be found, explicitly or implicitly, in [13]. This section is a condensed version of the beginning of [17], to which the reader is referred for more details.

7.1. **Anti-isomorphisms and character modules.** Let R be a finite ring with 1. We allow R to be non-commutative. Let A be a finite left R-module, which will serve as the alphabet for linear codes over R. A left *R-linear code* over A of length n is a left R-submodule $C \subset A^n$. (There is a parallel theory for right linear codes.) An important special case is when the alphabet A is the ring R itself, viewed as a left R-module.

In most treatments of the MacWilliams identities, the dual code $C^\perp$ would be a right R-module. Unless the ring R is commutative, this change of sides would make it impossible for a code to be self-dual, i.e., satisfy $C = C^\perp$. Nebe, Rains, and Sloane [13] address this problem by assuming some additional structure on R and A so that one can view the dual code $C^\perp$ as a left R-module. To that end, we follow [13] and introduce several definitions.

An *anti-isomorphism* $\varepsilon : R \to R$ of a ring R is an isomorphism of abelian groups with the property that $\varepsilon(rs) = \varepsilon(s)\varepsilon(r)$ for all $r, s \in R$. An anti-isomorphism ε defines an isomorphism $R \cong R^{op}$ between the ring R and its opposite ring R^{op}. If ε is an anti-isomorphism of R, then so is its inverse ε^{-1}. An *involution* is an anti-isomorphism $\varepsilon : R \to R$ such that ε^2 is the identity; i.e., $\varepsilon^{-1} = \varepsilon$.

Let ${}_R\mathcal{F}$ (resp., $\mathcal{F}_R$) denote the category of finitely-generated left (resp., right) R-modules and R-module homomorphisms. Then an anti-isomorphism $\varepsilon : R \to R$ induces covariant functors $\varepsilon : {}_R\mathcal{F} \rightleftharpoons \mathcal{F}_R$ as follows. If M is a left R-module, define $\varepsilon(M)$ to be the same abelian group as M with right scalar multiplication defined by $mr = \varepsilon(r)m$, for $m \in M$, $r \in R$, where $\varepsilon(r)m$ uses the left scalar multiplication of M. Similarly, if N is a right R-module, then $\varepsilon(N)$ has left scalar multiplication defined by $rn = n\varepsilon(r)$, for $n \in N$, $r \in R$. One verifies that a homomorphism $f : M_1 \to M_2$ of left R-modules is also a homomorphism $\varepsilon(M_1) \to \varepsilon(M_2)$ of right R-modules.

Character modules will be important in our discussion, so we provide a short summary of them next. The *character functor* $\widehat{\ } : {}_R\mathcal{F} \rightleftharpoons \mathcal{F}_R$ is a contravariant functor that associates to every finite left (resp., right) R-module M its character module $\widehat{M} = \operatorname{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$, which is a finite right (resp., left) R-module. (The additive form of characters will be used. By composing with the exponential map: $\mathbb{Q}/\mathbb{Z} \to \mathbb{C}^\times$, $x \mapsto \exp(2\pi i x)$, $x \in \mathbb{Q}/\mathbb{Z}$, one recovers the multiplicative form of characters. The modules involved are isomorphic.) When M is a left R-module, the right module structure of $\widehat{M}$ is given by $(\varpi r)(m) = \varpi(rm)$, for $\varpi \in \widehat{M}$, $r \in R$, and $m \in M$.

Lemma 7.1.1. *Given an anti-isomorphism ε on a finite ring R, the functors ε and $\widehat{\ }$ commute. That is, for any finite R-module M,*

$$\widehat{\varepsilon(M)} = \varepsilon(\widehat{M}).$$

Suppose the finite ring R admits an anti-isomorphism ε. Even though the functors ε and $\widehat{\ }$ commute, the functors cannot be the same. Indeed, the functor $\varepsilon : {}_R\mathcal{F} \rightleftharpoons \mathcal{F}_R$ is covariant, while the character functor $\widehat{\ } : {}_R\mathcal{F} \rightleftharpoons \mathcal{F}_R$ is contravariant. However, modules where the functors agree will be important.

To that end, suppose M is a finite left R-module such that $\psi : \varepsilon(M) \to \widehat{M}$ is an isomorphism of right R-modules. For every $y \in M$, $\psi(y)$ is a character on M. We denote the value of this character on a point $x \in M$ by $\psi(y)(x)$. Then ψ being a homomorphism means

$$\psi(\varepsilon(r)y)(x) = \psi(yr)(x) = (\psi(y)r)(x) = \psi(y)(rx), \tag{7.1.1}$$

for $r \in R$ and $x, y \in M$.

By applying the character functor to the isomorphism $\psi : \varepsilon(M) \to \widehat{M}$ and using that the double character module of M is naturally isomorphic to M itself, we obtain $\widehat{\psi} : M \to \widehat{\varepsilon(M)} = \varepsilon(\widehat{M})$. Applying ε^{-1}, we have an isomorphism $\widehat{\psi} : \varepsilon^{-1}(M) \to \widehat{M}$. From the definition of $\widehat{\psi}$ we have the relation

$$\widehat{\psi}(x)(y) = \psi(y)(x), \quad x, y \in M. \tag{7.1.2}$$

Proposition 7.1.2. *Suppose a finite ring R admits an anti-isomorphism ε and that a finite left R-module M admits an isomorphism $\psi : \varepsilon(M) \to \widehat{M}$. Then $\varepsilon(M) \cong \varepsilon^{-1}(M)$; i.e., $\varepsilon^2(M) \cong M$.*

Definition 7.1.3. The following is a list of properties that a ring R may possess.

- **P1:** The ring R admits an anti-isomorphism ε.
- **P2:** Given an anti-isomorphism ε on R, there exists a finite left R-module A and an isomorphism $\psi : \varepsilon(A) \to \widehat{A}$.
- **P3:** In P2, the isomorphism ψ satisfies $\widehat{\psi} = \psi e$, for some unit $e \in R$.

The condition in P3 means that there exists a unit $e \in R$ such that $\widehat{\psi}(x) = \psi(x)e \in \widehat{A}$, for all $x \in A$, where $\psi(x)e$ uses the right module structure of $\widehat{A}$. This leads to the following relations:

$$\psi(x)(ey) = (\psi(x)e)(y) = \widehat{\psi}(x)(y) = \psi(y)(x), \quad x, y \in A. \tag{7.1.3}$$

For the rest of this section we assume that a finite ring R and a finite left R-module A satisfy P1–P3, with anti-isomorphism ε and right module isomorphism $\psi : \varepsilon(A) \to \widehat{A}$. In this case, observe that $\psi : A \to \varepsilon^{-1}(\widehat{A})$ is a left module isomorphism.

We will now associate to $\psi : \varepsilon(A) \to \widehat{A}$ a bi-additive form, in the spirit of [13]. First define $\beta : A \times A \to \mathbb{Q}/\mathbb{Z}$ by $\beta(a, b) = \psi(b)(a)$, for $a, b \in A$. Then extend β to $\beta : A^n \times A^n \to \mathbb{Q}/\mathbb{Z}$ by

$$\beta(x, y) = \sum_{i=1}^{n} \beta(x_i, y_i) = \sum_{i=1}^{n} \psi(y_i)(x_i), \tag{7.1.4}$$

for $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in A^n$. Remember that the notation $\psi(y_i)(x_i)$ means to evaluate the character $\psi(y_i)$ of A on the element $x_i \in A$. The result is an element of $\mathbb{Q}/\mathbb{Z}$. One then sums these elements of $\mathbb{Q}/\mathbb{Z}$.

Theorem 7.1.4. *Assume properties* P1–P3*. The form β of* (7.1.4) *satisfies:*

1. *The form β is bi-additive; i.e., $\beta(x + z, y) = \beta(x, y) + \beta(z, y)$ and $\beta(x, y + z) = \beta(x, y) + \beta(x, z)$, for all $x, y, z \in A^n$.*
2. *The form β is non-degenerate. That is, if $\beta(A^n, y) = 0$, then $y = 0$; and if $\beta(x, A^n) = 0$, then $x = 0$.*
3. *The form satisfies $\beta(rx, y) = \beta(x, \varepsilon(r)y)$, for all $r \in R$, $x, y \in A^n$.*
4. *There exists a unit $e \in R$ so that $\beta(x, y) = \beta(ey, x)$, for all $x, y \in A^n$.*

Conversely, assume property P1 *and that there exists a form* $\beta : A \times A \to \mathbb{Q}/\mathbb{Z}$ *satisfying the properties above. If one defines* $\psi : A \to \widehat{A}$ *by* $\psi(b)(a) = \beta(a,b)$*, for* $a, b \in A$*, then* ψ *satisfies* P2–P3.

7.2. **The MacWilliams identities.** Given an additive code $C \subset A^n$, the character-theoretic *annihilator* of C is

$$(\widehat{A}^n : C) = \{\varpi \in \widehat{A}^n : \varpi(C) = 0\}.$$

Note that $(\widehat{A}^n : C)$ is an additive subgroup of $\widehat{A}^n$ and that $|C|\,|(\widehat{A}^n : C)| = |A^n|$; see Theorem 4.2.1. Define the *dual code* $C^\perp$ by

$$C^\perp = \psi^{-1}(\widehat{A}^n : C).$$

Note that the dual code $C^\perp$ is an additive code in A^n. We say that C is *self-orthogonal* if $C \subset C^\perp$ and *self-dual* if $C = C^\perp$.

Theorem 7.2.1. *Assume that a finite ring R and a finite left R-module A satisfy* P1–P3*, with anti-isomorphism ε and right module isomorphism $\psi : \varepsilon(A) \to \widehat{A}$. Let β be the form associated to ψ via* (7.1.4)*. Then:*

(1) *For any additive code $C \subset A^n$, $C^\perp = \{y \in A^n : \beta(C, y) = 0\}$.*
(2) *For any additive code $C \subset A^n$, $|C||C^\perp| = |A^n|$.*
(3) *For any additive code $C \subset A^n$, the MacWilliams identities are satisfied:*

$$W_{C^\perp}(X,Y) = \frac{1}{|C|} W_C(X + (|A|-1)Y, X - Y).$$

(4) *If $C \subset A^n$ is a left linear code, then so is $C^\perp$.*
(5) *For any left linear code $C \subset A^n$, $C = (C^\perp)^\perp$.*

Remark 7.2.2. Because of the property $\beta(x,y) = \beta(ey,x)$, which uses P3, $C^\perp$ is also equal to $\{x \in A^n : \beta(x, C) = 0\}$, provided the code C is linear. (The assumption of C being linear is not needed if $e = 1$.)

Remark 7.2.3. Although we do not include it here, the MacWilliams identities are also valid for the complete weight enumerator. See [13] or [18] for details.

References

[1] E. F. Assmus, Jr. and H. F. Mattson, Jr., *Coding and combinatorics*, SIAM Rev. **16** (1974), 349–388. MR MR0359982 (50 #12432)

[2] E. Byrne, M. Greferath, and M. E. O'Sullivan, *The linear programming bound for codes over finite Frobenius rings*, Des. Codes Cryptogr. **42** (2007), no. 3, 289–301. MR MR2298938 (2008c:94053)

[3] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Pure and Applied Mathematics, vol. XI, Interscience Publishers, a division of John Wiley & Sons, New York, London, 1962. MR MR0144979 (26 #2519)

[4] P. Delsarte, *Bounds for unrestricted codes, by linear programming*, Philips Res. Rep. **27** (1972), 272–289. MR MR0314545 (47 #3096)

[5] M. Hall, *A type of algebraic closure*, Ann. of Math. (2) **40** (1939), no. 2, 360–369. MR MR1503463

[6] T. Honold, *Characterization of finite Frobenius rings*, Arch. Math. (Basel) **76** (2001), no. 6, 406–415. MR MR1831096 (2002b:16033)

[7] T. Honold and I. Landjev, *MacWilliams identities for linear codes over finite Frobenius rings*, Finite fields and applications (Augsburg, 1999) (D. Jungnickel and H. Niederreiter, eds.), Springer, Berlin, 2001, pp. 276–292. MR MR1849094 (2002i:94066)

[8] T. Y. Lam, *Lectures on modules and rings*, Graduate Texts in Mathematics, vol. 189, Springer-Verlag, New York, 1999. MR MR1653294 (99i:16001)

[9] ———, *A first course in noncommutative rings*, second ed., Graduate Texts in Mathematics, vol. 131, Springer-Verlag, New York, 2001. MR MR1838439 (2002c:16001)

[10] F. J. MacWilliams, *Combinatorial properties of elementary abelian groups*, Ph.D. thesis, Radcliffe College, Cambridge, Mass., 1962.

[11] ———, *A theorem on the distribution of weights in a systematic code*, Bell System Tech. J. **42** (1963), 79–94. MR MR0149978 (26 #7462)

[12] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland Publishing Co., Amsterdam, 1977, North-Holland Mathematical Library, Vol. 16. MR MR0465509 (57 #5408a)

[13] G. Nebe, E. M. Rains, and N. J. A. Sloane, *Self-dual codes and invariant theory*, Algorithms and Computation in Mathematics, vol. 17, Springer-Verlag, Berlin, 2006. MR MR2209183 (2007d:94066)

[14] J.-P. Serre, *Linear representations of finite groups*, Graduate Texts in Mathematics, vol. 42, Springer-Verlag, New York, Heidelberg, Berlin, 1977.

[15] A. Terras, *Fourier analysis on finite groups and applications*, London Mathematical Society Student Texts, vol. 43, Cambridge University Press, Cambridge, 1999. MR MR1695775 (2000d:11003)

[16] J. A. Wood, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math. **121** (1999), no. 3, 555–575. MR MR1738408 (2001d:94033)

[17] ———, *Anti-isomorphisms, character modules, and self-dual codes over noncommutative rings*, submitted to the Int. J. Information and Coding Theory volume in honor of Vera Pless, 2009.

[18] ———, *Foundations of linear codes defined over finite modules: the extension theorem and the MacWilliams identities*, Codes over rings (Ankara, 2008) (P. Solé, ed.), World Scientific, Singapore, 2009.

Department of Mathematics, Western Michigan University, 1903 W. Michigan Ave., Kalamazoo, MI 49008–5248

E-mail address: `jay.wood@wmich.edu`

URL: `http://homepages.wmich.edu/~jwood`