DUALITY FOR MODULES OVER FINITE RINGS AND APPLICATIONS TO CODING THEORY

JAY A. WOOD

In memory of Edward F. Assmus, Jr.

ABSTRACT. This paper sets a foundation for the study of linear codes over finite rings. The finite Frobenius rings are singled out as the most appropriate for coding theoretic purposes because two classical theorems of MacWilliams, the extension theorem and the MacWilliams identities, generalize from finite fields to finite Frobenius rings. It is over Frobenius rings that certain key identifications can be made between the ring and its complex characters.

INTRODUCTION

Since the appearance of [8] and [19], using linear codes over $\mathbb{Z}/4\mathbb{Z}$ to explain the duality between the non-linear binary Kerdock and Preparata codes, there has been a revival of interest in codes defined over finite rings. This paper examines the foundations of algebraic coding theory over finite rings and singles out the finite Frobenius rings as the most appropriate rings for coding theory.

Why are Frobenius rings appropriate for coding theory? Because two classical theorems of MacWilliams—the extension theorem and the MacWilliams identities—generalize to the case of finite Frobenius rings. The extension theorem of MacWilliams ([26], [27]) deals with the notion of equivalence of codes. Two codes are equivalent if there is a monomial transformation taking one to the other. This extrinsic description has an intrinsic formulation: if two linear codes are isomorphic as abstract vector spaces via an isomorphism which preserves Hamming weight, then this isomorphism extends to a monomial transformation. This

1991 *Mathematics Subject Classification.* Primary: 94B05, 16L60, 16P10.

Key words and phrases. Characters, Frobenius rings, Morita duality, equivalence, MacWilliams identities.

Partially supported by NSA grants MDA904-91-H-0029, MDA904-94-H-2025, and MDA904-96-1-0067, and by Purdue University Calumet Scholarly Research Awards.

 The article first appeared in the *American Journal of Mathematics*, **121** (1999), 555–575.

is the extension theorem of MacWilliams. It is the analogue of the theorems of Witt [40] and Arf [3] on the extension of isometries for non-degenerate bilinear and quadratic forms.

There are other proofs of the extension theorem for Hamming weight over finite fields: [7], [39]. In the latter, Ward and the author use an argument based on the linear independence of complex characters. It is this character theoretic argument which generalizes to Frobenius rings, because Frobenius rings allow for certain key identifications between a ring and its character module. Klemm [22] and Claasen and Goldbach [9] provided initial ideas in this direction. Hirano [20] and Xue [44] have independently arrived at results similar to those given here.

For other types of weight functions, extension theorems still hold. For the case of symmetrized weight compositions over finite fields, see [17]; over finite Frobenius rings, see [41]. For homogeneous weight functions over $\mathbb{Z}/m\mathbb{Z}$, see [11], and for general weight functions over finite commutative chain rings, see [42] and [43].

The MacWilliams identities relate the weight enumerator of a code to that of its dual code. The most common proof of the MacWilliams identities is Gleason's proof using the Poisson summation formula for Fourier transforms ([4, §1.12], [25, Chapter 5]). Klemm [23] proved the identities for finite commutative Frobenius rings, and Delsarte [13] proved them for additive codes. The results here encompass those of Klemm and Delsarte. Nechaev [33], [34] has results similar to ours. Gleason's argument extends to finite Frobenius rings because, once again, a key identification can be made: this time, between the dual code and the character theoretic annihilator.

Because of the importance of characters in our proofs, we treat character theory as a duality functor and place it in the context of Morita duality. We thank the referee for this idea.

Here is a brief outline of the paper. Sections 1–3 discuss quasi-Frobenius and Frobenius rings, duality functors, and Morita duality. Section 4 summarizes some key identifications for Frobenius rings that are needed for coding theory. The reader interested primarily in the coding theoretic results may wish to begin with Section 4. Section 5 contains a technical result on partial orderings.

The coding theory begins in earnest in Section 6 with a review of essential definitions and a proof of the extension theorem. In Section 7 the orthogonals associated to a duality functor are discussed and another key identification for Frobenius rings is established. The MacWilliams identities are proved in Section 8, and essential results about characters are summarized in Appendix A.

Acknowledgments. I thank: Dave Benson for suggesting the form of Theorem 3.10 and for numerous examples, Vic Camillo for introducing me to the ideas behind Proposition 5.1, Ed Assmus for extensive discussions and guidance, and the referee for placing this work in the context of Morita duality and other helpful suggestions. In addition, I am grateful for advice, suggestions, and references from D. D. Anderson, R. R. Bruner, G. D. Forney, I. Herzog, Th. Honold, W. C. Huffman, R. G. Larson, J. L. Massey, H. F. Mattson, M. May SJ, A. A. Nechaev, N. J. A. Sloane, S. Valdes-Leon, and H. N. Ward. Finally, I thank Vera Pless for originally suggesting a re-examination of MacWilliams' work on the extension problem.

Conventions. All rings are assumed to be associative with $1 \neq 0$. All units are assumed to be two-sided. In finite rings, one-sided units are necessarily two-sided. In any module, the unit element of the base ring is assumed to act as the identity. We denote the ring of integers modulo m by $\mathbb{Z}/(m)$ and the number of elements in a finite set S by $|S|$.

1. Quasi-Frobenius rings

We review Nakayama's definitions [32] of quasi-Frobenius and Frobenius rings. We assume the reader is familiar with standard terms from ring theory: idempotents, projective, injective, irreducible, and indecomposable modules, etc., as found in [2], [5], or [12].

Let R be an Artinian ring. As a left R-module, R admits a *principal decomposition*

$$ {}_RR = Re_{1,1} \oplus \cdots \oplus Re_{1,\mu_1} \oplus \cdots \oplus Re_{n,1} \oplus \cdots \oplus Re_{n,\mu_n}, $$

where the $e_{i,j}$ are primitive orthogonal idempotents, with $1 = \sum e_{i,j}$. The indexing is chosen so that $Re_{i,j} \cong Re_{k,l}$ if and only if $i = k$. Setting $e_i = e_{i,1}$, $Re_1, \ldots, Re_n$ represent the distinct isomorphism classes of principal indecomposable left R-modules, and μ_i is the multiplicity of the isomorphism type of Re_i in ${}_RR$. To summarize, we write, as left R-modules,

$$ {}_RR \cong \oplus \mu_i Re_i. \tag{1.1} $$

Each principal indecomposable $Re_{i,j}$ has a unique irreducible "top quotient" $T(Re_{i,j}) = Re_{i,j}/\operatorname{Rad}(R)e_{i,j}$. The *socle* $S(Re_{i,j})$ is the left submodule generated by the irreducible left submodules of $Re_{i,j}$.

There are right module counterparts to the above. In fact, if e, f are primitive idempotents, then $Re \cong Rf$ if and only if $eR \cong fR$. Thus

the right module counterpart to (1.1) is $R_R \cong \oplus \mu_i e_i R$. In particular, the idempotents e_i and the multiplicities μ_i are the same in both decompositions.

The following definitions [32, II, p. 8] refer to (1.1). An Artinian ring R is *quasi-Frobenius* (QF) if there exists a permutation σ of $\{1, 2, \ldots, n\}$ such that

$$T(Re_i) \cong S(Re_{\sigma(i)}) \quad \text{and} \quad S(e_i R) \cong T(e_{\sigma(i)} R). \tag{1.2}$$

The ring is *Frobenius* if, in addition, $\mu_{\sigma(i)} = \mu_i$. The ring is *weakly symmetric* if $\sigma =$ the identity, i.e., if $T(Re_i) \cong S(Re_i)$ for all i. Note, in particular, that $S(Re_i)$ is irreducible in a QF ring; this is the real content hidden in (1.2).

Remark 1.1. If R is a finite-dimensional algebra over a field, there are also notions of QF and Frobenius algebras [12, Definition 61.1]. Such algebras are QF and Frobenius, respectively, as rings [32, I, Lemma 2].

Theorem 1.2 ([12, Theorems 58.6 and 58.12])**.** *An Artinian ring R is QF if and only if R is self-injective, i.e., R is injective as a left (right) module over itself.*

Remark 1.3. If an Artinian ring R is also commutative, then $R = \oplus R_i$ is a finite direct sum of local commutative Artinian rings. Let $\mathfrak{m}_i$ be the maximal ideal of R_i, with residue field $k_i = R_i/\mathfrak{m}_i$. The ring R is QF if and only if each R_i is QF. A local ring R_i is QF if and only if its socle $S(R_i)$ is irreducible, in which case $S(R_i) \cong T(R_i) \cong k_i$. Thus, for commutative Artinian rings R, the properties weakly symmetric, Frobenius, and QF coincide, and they are the same as the ring being Gorenstein [16, Proposition 21.5]. Since $S(R_i) = \operatorname{ann}(\mathfrak{m}_i)$, the annihilator of $\mathfrak{m}_i$ in R_i [12, Lemma 58.3], R_i is QF if and only if $\dim_{k_i} \operatorname{ann}(\mathfrak{m}_i) = 1$.

Example 1.4. We invite the reader to verify the following facts.

(i). $R = \mathbb{F}_2[X, Y]/(X^2, XY, Y^2)$ is not QF, [21, Beispiel 1.3].

(ii). If R consists of all 6×6 matrices over $\mathbb{F}_3$ of form a below, then R is QF but not Frobenius. (Dave Benson suggested this example.)

(iii). If R consists of all 4×4 matrices over $\mathbb{F}_3$ of form b below, then R is Frobenius but not weakly symmetric.

$$a = \begin{pmatrix} a_1 & 0 & a_2 & 0 & 0 & 0 \\ 0 & a_1 & 0 & a_2 & a_3 & 0 \\ a_4 & 0 & a_5 & 0 & 0 & 0 \\ 0 & a_4 & 0 & a_5 & a_6 & 0 \\ 0 & 0 & 0 & 0 & a_9 & 0 \\ a_7 & 0 & a_8 & 0 & 0 & a_9 \end{pmatrix}, \quad b = \begin{pmatrix} b_1 & 0 & 0 & 0 \\ 0 & b_1 & b_2 & 0 \\ 0 & 0 & b_4 & 0 \\ b_3 & 0 & 0 & b_4 \end{pmatrix}.$$

2. Duality functors

As preparation for the study of the character functor in Section 3, we review some of Morita's theory of duality for modules. We will work with a single finite ring and finitely generated modules, although Morita's theory works in greater generality. References for this material include Morita's original work [30], as well as [2] and [10].

Let R be any finite ring. Let ${}_R\mathcal{F}$ ($\mathcal{F}_R$) denote the category of finitely generated left (right) R-modules and module homomorphisms. A *duality functor* $\mathcal{D} : {}_R\mathcal{F} \rightleftharpoons \mathcal{F}_R$ between these two categories is a pair of contravariant functors, both denoted by $\mathcal{D}$, with $\mathcal{D}^2$ naturally equivalent to the identity functor. The following theorem summarizes the main results of Morita's theory of duality. (A module U is a *cogenerator* if every finitely generated module M admits an injection $0 \to M \to U^n$ into some power of U. If U is also an injective module, then U is an *injective cogenerator*.)

Theorem 2.1. (i) *Every duality functor $\mathcal{D} : {}_R\mathcal{F} \rightleftharpoons \mathcal{F}_R$ is naturally equivalent to one of the form $\mathcal{D}(M) = \mathrm{Hom}_R(M, U)$, where U is an R-bimodule which is a finitely generated injective cogenerator as both a left and a right module.*

(ii) *Every bimodule U of the type mentioned in* (i) *defines a duality functor via $\mathcal{D}(M) = \mathrm{Hom}_R(M, U)$.*

(iii) *Suppose $\mathcal{D}_1$ and $\mathcal{D}_2$ are duality functors given by bimodules U_1 and U_2. Then $\mathcal{D}_1$ is naturally equivalent to $\mathcal{D}_2$ if and only if U_1 and U_2 are isomorphic as bimodules.*

Proof. In [10] these results are Theorems 5.2, 5.11, and 5.12. □

Example 2.2. Let the bimodule U equal ${}_RR_R$, the ring R considered as a bimodule over itself. Denote the resulting functor by $\mathcal{D} = \sharp$. Then $M^\sharp = \mathrm{Hom}_R(M, R)$ associates to every left (right) module M the right (left) module of all left (right) linear functionals from M to R. The functor $\sharp$ is not always a duality functor, as the next theorem explains.

Theorem 2.3. *The functor $\mathcal{D} = \sharp$ is a duality functor if and only if the ring R is QF.*

Proof. If R is QF, it is self-injective, by Theorem 1.2, and a cogenerator, by [10, Proposition 5.9]. Thus R is an injective cogenerator, and $\mathcal{D} = \sharp$ is a duality functor. The converse is clear. □

Theorem 2.4. *Let R be a finite QF ring with principal decomposition* (1.1). *Let $\mathcal{D} : {}_R\mathcal{F} \rightleftharpoons \mathcal{F}_R$ be any duality functor over R. Then there exists a permutation τ of $\{1, 2, \ldots, n\}$ such that*

$$\mathcal{D}(Re_i) \cong e_{\tau(i)}R, \quad \mathcal{D}(T(Re_i)) \cong S(e_{\tau(i)}R), \quad \mathcal{D}(S(Re_i)) \cong T(e_{\tau(i)}R).$$

Proof. Because the functor $\mathcal{D}$ is contravariant, it takes a projective module, like Re_i, to an injective module. But injective modules over QF rings are projective, so that $\mathcal{D}(Re_i)$ is projective. Since $\mathcal{D}^2 = 1$, it follows that $\mathcal{D}$ of an indecomposable module is again indecomposable. Thus $\mathcal{D}(Re_i)$ is an indecomposable projective right module, and therefore it is isomorphic to some e_jR. By setting $\tau(i) = j$, we have the desired permutation τ.

Theorem 2.1 says that $\mathcal{D} = \mathrm{Hom}_R(-, U)$ for some bimodule U which is injective as left and as right module. That U is injective implies that $\mathcal{D}$ is an exact functor, i.e., it preserves short exact sequences. Since $\mathcal{D}^2 = 1$, it follows that $\mathcal{D}$ of an irreducible module is again irreducible. Together with the contravariance of $\mathcal{D}$, exactness implies that $\mathcal{D}$ carries a composition series of a module M into a composition series of $\mathcal{D}(M)$ in such a way that the successive irreducible quotients of $\mathcal{D}(M)$ are just $\mathcal{D}$ of the irreducible quotients of M, but in the reverse order. Thus, for example, $T(\mathcal{D}(Re_i)) \cong \mathcal{D}(S(Re_i))$. The other claims of the theorem now follow. □

Corollary 2.5. *Let R be a finite QF ring. Then for the duality functor $\mathcal{D} = \sharp$, $\tau = 1$. That is,*

$$(Re_i)^\sharp \cong e_iR, \quad (T(Re_i))^\sharp \cong S(e_iR), \quad (S(Re_i))^\sharp \cong T(e_iR).$$

Proof. This is an easy exercise, [2, Proposition 4.6]. □

3. The character functor and Frobenius rings

Example 3.1. Let R be a finite ring. Following Pontryagin [35], we define a functor $\mathcal{D} = \widehat{\ } : {}_R\mathcal{F} \rightleftharpoons \mathcal{F}_R$ by $\mathcal{D}(M) = \widehat{M}$, the complex characters of the abelian group M. We call $\widehat{M}$ the *character module* associated to M, and we refer the reader to Appendix A for more information.

Because $\widehat{M}$ forms an abelian group under the pointwise multiplication of characters, we choose to write the scalar multiplication on $\widehat{M}$ in exponential form. If M is a left (resp., right) module, then $\widehat{M}$ is a right (resp., left) module via

$$\pi^r(x) = \pi(rx), \quad (\text{resp., } {}^r\pi(x) = \pi(xr),) \quad \pi \in \widehat{M}, r \in R, x \in M.$$

If M is a bimodule, then $\widehat{M}$ is also a bimodule.

Theorem 3.2. *For any finite ring R, the functor $\mathcal{D} = \widehat{\ } : {}_R\mathcal{F} \rightleftharpoons \mathcal{F}_R$ is a duality functor.*

Proof. Any finitely generated M is actually finite. It is classical that $\mathcal{D}^2(M) \cong M$ naturally, as abelian groups. Then one verifies that this is also a natural isomorphism of modules. □

Remark 3.3. The functor $\mathcal{D} = \widehat{\ }$ is represented by the bimodule $U = \widehat{R}$. Indeed, here is the isomorphism from $\widehat{M}$ to $\mathrm{Hom}_R(M, \widehat{R})$. Take any $\pi \in \widehat{M}$. For $m \in M$, the formula $\pi^r(m) = \pi(rm)$ defines a character of R. Observe that $\widehat{R}$ is always injective, because the torus $\mathbb{T}$ is a divisible group [12, Lemma 57.7].

If R is commutative, $\mathcal{D} = \widehat{\ }$ is the unique duality functor on R [16, Proposition-Definition 21.1].

Example 3.4. Suppose R is a finite dimensional algebra over a finite field $\mathbb{F}$. The functor $\mathcal{D} = {}^* : {}_R\mathcal{F} \rightleftharpoons \mathcal{F}_R$,

$$\mathcal{D}(M) = M^* = \mathrm{Hom}_{\mathbb{F}}(M, \mathbb{F}).$$

is a duality functor with representing bimodule $U = R^*$.

Proposition 3.5. *If R is a finite dimensional algebra over a finite field $\mathbb{F}$, then the functors * and $\widehat{\ }$ are naturally equivalent.*

Proof. We show that $R^* \cong \widehat{R}$ as bimodules and apply Theorem 2.1.

Since $\widehat{\mathbb{F}}$ is a 1-dimensional vector space over $\mathbb{F}$, it has a basis $\chi \in \widehat{\mathbb{F}}$. Define $f : R^* \to \widehat{R}$ by $f(\lambda) = \chi \circ \lambda$ for $\lambda \in R^*$; f is a homomorphism of R-bimodules. Since R is finite, $|R^*| = |R| = |\widehat{R}|$, and it suffices to show that f is injective. Suppose $\lambda \neq 0$. Then, as an $\mathbb{F}$-linear functional $\lambda : R \to \mathbb{F}$, λ is onto $\mathbb{F}$. Since χ is a basis, $f(\lambda) = \chi \circ \lambda$ is non-trivial. □

The next several results will describe how $\mathcal{D} = \widehat{\ }$ transforms a principal decomposition (1.1) of a finite QF ring, as in Theorem 2.4.

Proposition 3.6. *Let R be the simple matrix ring $M_n(\mathbb{F})$, where $\mathbb{F}$ is a finite field. Let M be the irreducible right R-module $M \cong \mathbb{F}^n$, and let N be the irreducible left R-module $N \cong \mathbb{F}^n$. Then*

$$\widehat{M} \cong N \quad \textit{and} \quad \widehat{N} \cong M.$$

Proof. View the elements of M as row vectors, those of N as column vectors. Let χ be a basis of $\widehat{\mathbb{F}}$, as in the proof of Proposition 3.5. The map $N \to \widehat{M}$, $a \mapsto \pi_a$, where $\pi_a(x) = \chi(xa)$, $x \in M$, is an isomorphism of left R-modules. (Here, $xa \in \mathbb{F}$ is the matrix product.) □

Corollary 3.7. *Let R be any finite ring with principal decomposition ${}_RR \cong \oplus \mu_i Re_i$, as in* (1.1)*. Then*

$$(T(Re_i))\widehat{\ } \cong T(e_iR) \quad \textit{and} \quad (T(e_iR))\widehat{\ } \cong T(Re_i).$$

Proof. This is just Proposition 3.6 applied to the Wedderburn decomposition of $R/\operatorname{Rad}(R)$. □

Theorem 3.8. *Let R be a finite QF ring, with ${}_RR \cong \oplus\mu_i Re_i$, as in* (1.1)*, and with permutation σ, as in* (1.2)*. Then*

$$ {}_R(\widehat{R}) \cong \oplus\mu_i Re_{\sigma(i)} \quad \textit{and} \quad (\widehat{R})_R \cong \oplus\mu_i e_{\sigma^{-1}(i)}R. $$

Proof. From Theorem 2.4 we have $(T(Re_i))\widehat{\ } \cong S(e_{\tau(i)}R)$, for some permutation τ. On the other hand, Corollary 3.7 and (1.2) imply that $(T(Re_i))\widehat{\ } \cong T(e_iR) \cong S(e_{\sigma^{-1}(i)}R)$. Thus $S(e_{\tau(i)}R) \cong S(e_{\sigma^{-1}(i)}R)$. But, in QF rings, this isomorphism implies $e_{\tau(i)}R \cong e_{\sigma^{-1}(i)}R$ ([12, Theorem 58.12]). Therefore $\tau = \sigma^{-1}$.

Feeding this back into Theorem 2.4 gives $(e_iR)\widehat{\ } \cong Re_{\sigma(i)}$. Then

$$ {}_R(\widehat{R}) \cong (R_R)\widehat{\ } \cong (\oplus\mu_i e_iR)\widehat{\ } \cong \oplus\mu_i Re_{\sigma(i)}. $$

The proof for $(\widehat{R})_R$ is similar. □

Our next results identify the finite Frobenius rings as those finite rings for which $\widehat{R} \cong R$ as left or right R-modules. We thank Dave Benson for this observation.

Proposition 3.9. *Suppose that R is a finite ring and that $\widehat{R}$ is a free left R-module. Then $\widehat{R} \cong {}_RR$, and R is QF.*

Proof. Since $|\widehat{R}| = |R|$, $\widehat{R}$ has rank one, and $\widehat{R} \cong {}_RR$. Since $\widehat{R}$ is always injective (Remark 3.3), $R \cong \widehat{R}$ is self-injective, hence QF (Theorem 1.2). □

Theorem 3.10. *If R is a finite ring, the following are equivalent.*

(i). *R is a Frobenius ring.*
(ii). *As a left module, $\widehat{R} \cong {}_RR$.*
(iii). *As a right module, $\widehat{R} \cong R_R$.*

Proof. By Proposition 3.9, we may assume that R is QF. The result then follows immediately from the definition of Frobenius rings and Theorem 3.8. See Theorem 4.3 for a direct proof that (ii) is equivalent to (iii). □

Remark 3.11. If R is a finite dimensional algebra over a finite field, $R^* \cong \widehat{R}$ (Proposition 3.5). Thus R is a Frobenius ring if and only if $R^* \cong R$ as one-sided modules. This is the definition of a *Frobenius algebra* [12, Definition 61.1].

Now suppose $\widehat{R} \cong R$ as bimodules. By Theorem 2.1, $\sharp \cong \widehat{\ }$. If R is a finite dimensional algebra, then $R \cong R^*$ as bimodules. This condition is equivalent to R being a *symmetric algebra* [12, Definition 66.1].

For any finite ring, we now define R to be a *symmetric ring* if $\widehat{R} \cong R$ as bimodules. Every symmetric ring is weakly symmetric. Indeed, Corollary 2.5 says $(Re_i)^\sharp \cong e_iR$, while Theorem 3.8 says $(Re_i)\widehat{\ } \cong e_{\sigma^{-1}(i)}R$. Since R is symmetric, $\sharp \cong \widehat{\ }$, forcing $\sigma = 1$, as needed for weakly symmetric.

Nakayama and Nesbitt [31] have an example of a 4-dimensional algebra over $\mathbb{F}_3$ which is weakly symmetric but not symmetric. Thus there are Frobenius rings which are not symmetric. Having $\widehat{R} \cong R$ both as left and as right modules does not imply that $\widehat{R} \cong R$ as bimodules. A left module isomorphism $R \to \widehat{R}$ need not be a homomorphism of right modules.

Remark 3.12. The situation where the finite ring R is an algebra over a finite commutative ring K can be handled in a manner similar to the case where K is a field. Define $\mathcal{D} = {}^* : {}_R\mathcal{F} \rightleftharpoons \mathcal{F}_R$ by $M^* = \mathrm{Hom}_K(M, K)$. If we assume that K is Frobenius, which is the same as QF and symmetric for commutative rings, then $\mathcal{D} = {}^*$ is a duality functor and ${}^* \cong \widehat{\ }$.This setting has been discussed by Eilenberg and Nakayama [15] and by Auslander, et al. [5].

4. Generating characters

Let R be a finite ring. A character χ of R is a *right* (*resp., left*) *generating character* if the mapping $\phi : R \to \widehat{R}$, $\phi(r) = \chi^r$ (resp., $\phi(r) = {}^r\chi$) is an isomorphism of right (resp., left) R-modules. From Theorem 3.10, a finite ring is Frobenius if and only if it admits a right or a left generating character.

The phrase *generating character* comes from Klemm [22]. Claasen and Goldbach [9] use the phrase *admissible character*, and their usage of left and right is opposite to ours.

Lemma 4.1 ([9, Corollary 3.6])**.** *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.*

Proof. Because $|\widehat{R}| = |R|$, $\phi : R \to \widehat{R}$, $r \mapsto \chi^r$, is an isomorphism if and only if ϕ is injective. Now $r \in \ker \phi$ if and only if $\chi^r(x) = \chi(rx) = 1$, for all $x \in R$; i.e., if and only if the right ideal $rR \subset \ker \chi$. □

Proposition 4.2. *Suppose R is a finite Frobenius ring, with right generating character χ. Let $M \in \mathcal{F}_R$ be any finitely generated right module. Then the mapping*

$$f : M^\sharp \to \widehat{M}, \quad f(\lambda) = \chi \circ \lambda, \quad \lambda \in M^\sharp$$

is an injective homomorphism of abelian groups.

Proof. It is clear that f is a homomorphism of abelian groups. If $\lambda \in \ker f$, then $\lambda(M)$ is a right ideal contained in $\ker \chi$. By Lemma 4.1, $\lambda(M) = 0$, so that $\lambda = 0$. □

The proof of the next theorem was provided by the referee. It answers directly a question of Claasen and Goldbach, [9, §8].

Theorem 4.3. *Let R be any finite ring. Then a character χ on R is a left generating character if and only if it is a right generating character.*

Proof. Suppose χ is a left generating character and that I is a right ideal contained in $\ker \chi$. Then $I \subset \ker({}^r\chi)$, for all $r \in R$. Since χ is a left generating character, this says that $I \subset \ker \pi$, for all $\pi \in \widehat{R}$. Using annihilators (A.2), this says $(\widehat{R} : I) = \widehat{R}$. Since $|(\widehat{R} : I)| = |\widehat{R}|/|I|$, we have $I = 0$. The result follows from Lemma 4.1 □

Example 4.4. Here are a number of examples of Frobenius rings.

(i). Let $R = \mathbb{F}$, a finite field. A generating character χ on $\mathbb{F}$ is given by $\chi(x) = \xi^{\operatorname{tr} x}$, $x \in \mathbb{F}$, where $\operatorname{tr} : \mathbb{F} \to \mathbb{F}_p$ is the trace map from $\mathbb{F}$ to its prime subfield $\mathbb{F}_p$, and $\xi = \exp(2\pi i/p)$ is a primitive pth root of 1 in $\mathbb{T}$.

(ii). Let $R = \mathbb{Z}/(m)$. Set $\xi = \exp(2\pi i/m)$. Then $\chi(x) = \xi^x$, $x \in \mathbb{Z}/(m)$, is a generating character.

(iii). The finite direct sum of Frobenius rings is Frobenius. If $R_1, \ldots, R_n$ each have right generating characters $\chi_1, \ldots, \chi_n$, then $R = \oplus R_i$ has right generating character $\chi = \prod \chi_i$.

(iv). Suppose R has a right generating character χ_R. Let $S = M_n(R)$ be the ring of $n \times n$ matrices over R. Then $\chi_S(B) = \chi_R(\operatorname{tr} B)$ is a right generating character for S, where $B \in S$ and tr is the classical matrix trace.

(v). Suppose R has a right generating character χ_R. Let G be a finite group, with associated group ring $S = R[G]$. Then

$$\chi_S(\sum_{g \in G} r_g g) = \chi_R(r_e)$$

is a right generating character for S.

(vi). Any Galois ring is Frobenius. A *Galois ring* $R = GR(p^n, r)$ is a Galois extension of $\mathbb{Z}/(p^n)$ of degree r. By [29, Corollary 15.5],

$$GR(p^n, r) \cong \mathbb{Z}/(p^n)[X]/(f),$$

where f is a monic polynomial in $\mathbb{Z}/(p^n)[X]$ of degree r whose reduction in $\mathbb{Z}/(p)[X]$ is irreducible.

Because f is monic, any element a of $R = GR(p^n, r)$ is represented by a unique polynomial $a = \sum_{i=1}^{r} a_i X^{r-i}$, with $a_i \in$

$\mathbb{Z}/(p^n)$. Set $\xi = \exp(2\pi i/p^n)$. Then $\chi(a) = \xi^{a_1}$ is a generating character.

(vii). Any finite dimensional Hopf algebra with an antipode is Frobenius [24, p. 85]. In particular, the various finite subHopf algebras of the mod p Steenrod algebra are Frobenius [28, p. 191].

5. A partial ordering

Suppose M is a left module over a finite ring R. Define an equivalence relation $\approx$ on M by $x \approx y$ if there exists a unit u in R with $y = ux$. Such elements are called *strong associates* [1, Definition 2.1].

Proposition 5.1. *Let M be a left module over a finite ring R. If $x, y \in M$ satisfy $y = ax$, $x = by$ for some $a, b \in R$, then $x \approx y$.*

Proof. Clearly $(1-ba)x = 0$. Now $R = Rba + R(1-ba) = Ra + R(1-ba)$. By [6, Lemma 6.4], $a + R(1 - ba)$ contains a unit. That is, there exists $r \in R$ such that $u = a + r(1 - ba)$ is a unit in R. Then $ux = ax + r(1 - ba)x = ax = y$, as desired. □

On the $\approx$-equivalence classes of M, define $y \leq x$ if $y = ax$ for some $a \in R$. This relation is well-defined, reflexive, and transitive. Proposition 5.1 says that the relation is anti-symmetric.

Theorem 5.2. *The relation $\leq$ on the $\approx$-equivalence classes of a left module M over a finite ring R is a partial ordering.*

6. Coding theory and the extension theorem

Let R be a finite ring, and denote by R^n the free module of rank n consisting of n-tuples of elements from R. An *additive code* [13] is any additive subgroup $H \subset R^n$, while a *right* (*left*) *linear code* is a right (left) submodule $C \subset R^n$. Every linear code is additive. If $1 \in R$ generates R as an abelian group, then the converse is true.

The *complete weight composition* is the function $c : R \times R^n \to \mathbb{Z}$, which for every $r \in R$, $x = (x_1, \ldots, x_n) \in R^n$, assigns the integer

$$c_r(x) = |\{i : x_i = r\}|. \tag{6.1}$$

The *Hamming weight* $\mathrm{wt}(x) = \sum_{r \neq 0} c_r(x)$, the number of non-zero entries of x.

Define a *right* (*left*) *isometry* of R^n to be a right (left) linear automorphism T of R^n which preserves Hamming weights; i.e., $\mathrm{wt}(T(x)) = \mathrm{wt}(x)$ for all $x \in R^n$. A *right monomial transformation* $T : R^n \to R^n$ has the form

$$T(x_1, \ldots, x_n) = (u_1 x_{\sigma(1)}, \ldots, u_n x_{\sigma(n)}),$$

where σ is a permutation of $\{1, 2, \ldots, n\}$, and $u_1, \ldots, u_n$ are units in R. The set of all right monomial transformations of R^n forms a subgroup of the group of right linear automorphisms of R^n.

Proposition 6.1. *A right linear automorphism T of R^n is an isometry if and only if T is a right monomial transformation.*

Proof. A monomial transformation is clearly an isometry. Conversely, suppose T is an isometry. Apply T to $e_i = (0, \ldots, 1, \ldots 0)$, with a 1 in position i. Since $\mathrm{wt}(T(e_i)) = \mathrm{wt}(e_i) = 1$, $T(e_i) = r_i e_{\sigma(i)}$, for some $r_i \in R$ and index $\sigma(i)$. By hypothesis, T is an automorphism, hence invertible. It follows that the r_i's are units and that σ is a permutation. □

Two right linear codes $C_1, C_2 \subset R^n$ are *equivalent* if there exists a right isometry T on R^n with $T(C_1) = C_2$. We include the next proposition for emphasis.

Proposition 6.2. *Suppose $C_1, C_2 \subset R^n$ are equivalent via the isometry T. Then, regarded as a linear homomorphism $T : C_1 \to C_2$, T is a linear isomorphism from C_1 to C_2 which preserves Hamming weight.*

The converse is the extension theorem, which we prove over finite Frobenius rings.

Theorem 6.3 (Extension theorem)**.** *Let R be a finite Frobenius ring. Suppose $C \subset R^n$ is a right linear code, and suppose $f : C \to R^n$ is a right linear homomorphism which preserves Hamming weight. Then f extends to a right isometry of R^n.*

Proof. Denote by μ the inclusion $C \subset R^n$, and set $\lambda = f \circ \mu$. Then λ, μ are two different embeddings of the finitely generated right R-module C into R^n. Having values in R^n, λ, μ are n-tuples of right linear functionals on C, $\lambda = (\lambda_1, \ldots, \lambda_n)$, $\mu = (\mu_1, \ldots, \mu_n)$.

Since f preserves weights, $\mathrm{wt}(\mu(x)) = \mathrm{wt}(\lambda(x))$, for all $x \in C$. Proposition A.2 implies

$$\sum_{i=1}^{n} \sum_{\pi \in \widehat{R}} \pi(\lambda_i(x)) = \sum_{j=1}^{n} \sum_{\psi \in \widehat{R}} \psi(\mu_j(x)), \quad x \in C. \tag{6.2}$$

Being Frobenius, R admits a generating character χ . Equation (6.2) becomes

$$\sum_{i=1}^{n} \sum_{s \in R} \chi^s \circ \lambda_i = \sum_{j=1}^{n} \sum_{t \in R} \chi^t \circ \mu_j, \tag{6.3}$$

an equation of characters on C. The linear independence of characters, Proposition A.1, will now be applied in a systematic way.

Let $C^\sharp = \mathrm{Hom}_R(C, R)$ be the set of all right linear functionals on C. The left R-module $C^\sharp$ admits a partial ordering $\leq$, as in Theorem 5.2.

From the finite set of linear functionals $S = \{\lambda_1, \ldots, \lambda_n, \mu_1, \ldots, \mu_n\}$, there is at least one which is maximal for S with respect to the partial ordering $\leq$. Without loss of generality, assume λ_1 to be maximal. Then for $s = 1 \in R$ and λ_1 on the left side of (6.3), the linear independence of characters implies the existence of $t \in R$ and $\mu_j = \mu_{\sigma(1)}$ with $\chi^1 \circ \lambda_1 = \chi^t \circ \mu_{\sigma(1)}$.

Proposition 4.2 now implies $\lambda_1 = t\mu_{\sigma(1)}$, so that $\lambda_1 \leq \mu_{\sigma(1)}$. But λ_1 was chosen to be maximal in the set S, hence $\mu_{\sigma(1)} \approx \lambda_1$. Thus, there exists a unit $u_1 \in R$ with $\lambda_1 = u_1\mu_{\sigma(1)}$.

The corresponding inner sums of (6.3) will also be equal; i.e.,

$$\sum_{s\in R} \chi^s \circ \lambda_1 = \sum_{t\in R} \chi^t \circ \mu_{\sigma(1)}.$$

Indeed, $\sum_{s\in R} \chi^s \circ \lambda_1 = \sum_{s\in R} \chi^s \circ u_1\mu_{\sigma(1)} = \sum_{s\in R} \chi^{su_1} \circ \mu_{\sigma(1)}$. Since u_1 is a unit, equality follows by re-indexing.

The equality of these inner sums allows us to reduce by one the size of the outer sums in (6.3). Proceeding by induction, we produce a permutation σ and units $u_1, \ldots, u_n$, with $\lambda_i = u_i\mu_{\sigma(i)}$. This yields a right monomial transformation extending f. □

If the finite ring R is commutative, we can say more: the extension theorem holds over R if and only if R is Frobenius (equals QF over commutative rings by Remark 1.3).

Theorem 6.4. *Suppose R is a finite commutative ring, and suppose that the extension theorem holds over R. I.e., every weight-preserving linear homomorphism $f : C \to R^n$ from a linear code $C \subset R^n$ to R^n extends to an isometry of R^n. Then R is a Frobenius ring.*

Proof. Express the finite commutative ring R as a finite direct sum of local rings, $R = \oplus R_i$. We claim that the extension theorem holds over each R_i. Indeed, for fixed i, suppose C is a linear code in R_i^n and $f_i : C \to R_i^n$ is an R_i-linear homomorphism which preserves Hamming weights. Making use of the projection $R \to R_i$, we can consider everything over the ring R. Then f_i is still a weight-preserving homomorphism (over R, now). Since the extension theorem holds over R, there exists a monomial transformation $T : R^n \to R^n$ extending f_i. Observe that T preserves the $R^n = \oplus R_i^n$ splitting, so that restricting T to the R_i-component produces the necessary monomial transformation over R_i which extends f_i. Thus the extension theorem holds over R_i.

Let x, y be non-zero elements of $\mathrm{ann}(\mathfrak{m}_i)$, where $\mathfrak{m}_i$ is the maximal ideal of R_i and $k_i = R_i/\mathfrak{m}_i$ is the residue field. Consider the code $C = R_i x$, and $f : C \to R_i$ defined by $f(rx) = ry$. Because $x, y \in \mathrm{ann}(\mathfrak{m}_i)$, it follows that f is a well-defined injective linear homomorphism. Since $n = 1$, the injective f preserves Hamming weight. But the extension theorem holds over R_i, so there exists a unit $u \in R_i$ with $y = ux$. Thus x, y are linearly dependent over k_i, and $\dim_{k_i} \mathrm{ann}(\mathfrak{m}_i) = 1$.

By Remark 1.3, each R_i is Frobenius. Then $R = \oplus R_i$ is also Frobenius, by Example 4.4 (iii). □

7. Orthogonals

Every duality functor gives rise to a notion of an orthogonal. For the examples $\sharp$ and $\widehat{\ }$ of duality functors, one can identify the orthogonals with the classically defined notions of dual codes, provided the ring is Frobenius. These identifications will allow us to prove the MacWilliams identities in very general settings in Section 8. Any proofs that are omitted are easy exercises.

As in Section 2, let $\mathcal{D} : {}_R\mathcal{F} \rightleftharpoons \mathcal{F}_R$ be a functor of the form $\mathcal{D}(M) = \mathrm{Hom}_R(M, U)$, where U is a fixed R-bimodule. Fix $M \in {}_R\mathcal{F}$ (resp., $M \in \mathcal{F}_R$). For any submodule $N \subset M$, the *orthogonal* of N in M is

$$N^\circ = \{\lambda \in \mathcal{D}(M) : \lambda(x) = 0, \text{ for all } x \in N\}.$$

Then N° is a submodule of $\mathcal{D}(M) \in \mathcal{F}_R$ (resp., of $\mathcal{D}(M) \in {}_R\mathcal{F}$). It follows that $N \subset N^{\circ\circ}$.

Theorem 7.1 ([2, Theorem 24.5])**.** *Let $\mathcal{D} : {}_R\mathcal{F} \rightleftharpoons \mathcal{F}_R$ be a duality functor. For submodules $N \subset M$, as above, it is always the case that $N^{\circ\circ} = N$.*

Let us turn to the example $\mathcal{D} = \sharp$ for a finite ring R, where Theorem 2.3 generalizes to the following.

Theorem 7.2. *Let R be a finite ring, and let $\mathcal{D} = \sharp$. The following are equivalent.*

(i). *$\mathcal{D} : {}_R\mathcal{F} \rightleftharpoons \mathcal{F}_R$ is a duality functor.*
(ii). *R is a QF ring.*
(iii). *For submodules $M \subset R^n$, $M^{\circ\circ} = M$.*

Proof. That (i) is equivalent to (ii) is Theorem 2.3. By [18, Theorem 5.2], (iii) holds for all n if and only if it holds for $n = 1$. Now, (ii) is equivalent to (iii) for $n = 1$ by [32, II, Theorem 6]. Note that (iii) for $n = 1$ is the definition of QF in [12, Definition 58.5]. □

On R^n define the *standard dot product* by

$$x \cdot y = \sum_{i=1}^{n} x_i y_i,$$

for $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in R^n$. For ease of notation, let $P = R^n$ as a left module and $Q = R^n$ as a right module. For an arbitrary ring, the abelian groups underlying $P^\sharp$ and $Q^\sharp$ are different subgroups of $\mathrm{Hom}_{\mathbb{Z}}(R^n, R)$. Define two linear homomorphisms as follows.

$$\gamma : P \to Q^\sharp, \quad x \mapsto \gamma_x, \quad \gamma_x(y) = x \cdot y,$$
$$\delta : Q \to P^\sharp, \quad x \mapsto \delta_x, \quad \delta_x(y) = y \cdot x.$$

Proposition 7.3. *The homomorphism $\gamma : P \to Q^\sharp$ is an isomorphism of left modules. The homomorphism $\delta : Q \to P^\sharp$ is an isomorphism of right modules.*

We now define ring theoretic analogues of classical dual codes. For any subgroup $H \subset R^n$ define

$$\mathcal{L}(H) = \{x \in R^n : x \cdot h = 0, \text{ for all } h \in H\},$$
$$\mathcal{R}(H) = \{x \in R^n : h \cdot x = 0, \text{ for all } h \in H\}.$$

Then $\mathcal{L}(H)$ is a left submodule of R^n, and $\mathcal{R}(H)$ is a right submodule of R^n.

Proposition 7.4. *If M is a left submodule of P, then $M^\circ \subset P^\sharp$ corresponds to $\mathcal{R}(M)$ under the isomorphism δ. If M is a right submodule of Q, then $M^\circ \subset Q^\sharp$ corresponds to $\mathcal{L}(M)$ under the isomorphism γ.*

Now turn to the example $\mathcal{D} = \widehat{\ }$ over a finite Frobenius ring R with generating character χ. For $M \subset R^n$, it is clear that $M^\circ = (\widehat{R^n} : M)$, the *annihilator* of M in $\widehat{R^n}$ of (A.2).

Define two linear homomorphisms as follows.

$$\alpha : R^n \to \widehat{R^n}, \quad x \mapsto \alpha_x, \quad \alpha_x(y) = \chi(x \cdot y),$$
$$\beta : R^n \to \widehat{R^n}, \quad x \mapsto \beta_x, \quad \beta_x(y) = \chi(y \cdot x).$$

Proposition 7.5. *Suppose R is a finite Frobenius ring with generating character χ. Then the homomorphism α is an isomorphism of right modules, and the homomorphism β is an isomorphism of left modules.*

Let H be any subgroup of R^n. Set

$$A(H) = \{x \in R^n : \chi(x \cdot h) = 1, \text{ for all } h \in H\},$$
$$B(H) = \{x \in R^n : \chi(h \cdot x) = 1, \text{ for all } h \in H\}.$$

If M is a left submodule of R^n, then $A(M)$ is a right submodule of R^n. Similarly, if M is a right submodule of R^n, then $B(M)$ is a left submodule of R^n. It is clear that $\mathcal{L}(H) \subset A(H)$ and $\mathcal{R}(H) \subset B(H)$ for any subgroup $H \subset R^n$.

Proposition 7.6. *Under the isomorphism α, $H^\circ = (\widehat{R^n} : H) \subset \widehat{R^n}$ corresponds to $A(H)$. Under β, H° corresponds to $B(H)$.*

Theorem 7.7. *Suppose R is a finite Frobenius ring with generating character χ. If M is a left submodule of R^n, then $\mathcal{R}(M) = B(M)$. Similarly, if M is a right submodule of R^n, then $\mathcal{L}(M) = A(M)$.*

Proof. As we saw above, $\mathcal{L}(H) \subset A(H)$ and $\mathcal{R}(H) \subset B(H)$, for any subgroup $H \subset R^n$. (Exercise: use Example 1.4 (iii) to show that proper containments can occur.) For a right submodule M of R^n, take any $x \in A(M)$, so that $\chi(x \cdot m) = 1$ for all $m \in M$. In particular, for any $m \in M$, $r \in R$, we have $1 = \chi(x \cdot (mr)) = \chi((x \cdot m)r) = \chi^{x \cdot m}(r)$. Thus the character $\chi^{x \cdot m}$ is trivial. But χ is a generating character, so $x \cdot m = 0$, and $x \in \mathcal{L}(M)$. The proof for left submodules is similar. □

Any finite abelian group G admits the structure of a commutative Frobenius ring. Indeed, as an abelian group, G is isomorphic to a product of $\mathbb{Z}/(n)$'s. But the ring $\mathbb{Z}/(n)$ is Frobenius, as is any product thereof. This allows one to impose a commutative Frobenius ring structure on G. A choice of generating character χ, together with commutativity, defines an isomorphism $\phi : G \to \widehat{G}$, $\phi_x = \chi^x$, with the property that $\phi_x(y) = \phi_y(x)$, for all $x, y \in G$. This allows one to identify $A(H)$ and $B(H)$ with the orthogonals defined by Delsarte in [13].

8. MacWilliams identities

In this section we state several forms of the MacWilliams identities, valid over finite Frobenius rings, relating the weight enumerator of a code to that of its dual code. We follow the well-known technique of Gleason ([4, §1.12], [25, Chap. 5]) and derive the identities from the Poisson summation formula. The reader is referred to Appendix A for information about the Fourier transform and the Poisson summation formula.

Here is the general argument. The Poisson summation formula relates the sum of a function over a subgroup to the sum of its Fourier transform over the annihilator of the subgroup. Taking a weight enumerator as the function in question, Proposition A.5 computes its Fourier transform. The isomorphisms of Proposition 7.6 then identify the annihilators of an additive code with the orthogonals of the

code. For linear codes, the equalities in Theorem 7.7 allow for additional identifications. The MacWilliams identities are the resulting formulas.

We begin with the *complete weight enumerator*, which has the form

$$\mathcal{W}_H(Z) = \sum_{x\in H}\prod_{i=1}^{n} Z_{x_i} = \sum_{x\in H}\prod_{r\in R} Z_r^{c_r(x)},$$

for any additive subgroup $H \subset R^n$. The complete weight composition $c_r(x)$ of x appeared in (6.1). In the notation of Proposition A.5, the algebra A is the complex polynomial algebra $A = \mathbb{C}[Z_r : r \in R]$, with one indeterminate Z_r for each element $r \in R$. We write $Z = (Z_r)_{r\in R}$. The function f has the form $f(x) = \prod_{i=1}^n f_i(x_i)$, with $f_i(x_i) = Z_{x_i}$.

Theorem 8.1. *Assume R is a finite Frobenius ring, with generating character χ. Assume H is any additive subgroup of R^n. Then*

$$\mathcal{W}_H(Z) = \frac{1}{|B(H)|}\mathcal{W}_{B(H)}\Big(\sum_{s\in R}\chi(sr)Z_s\Big), \tag{8.1}$$

where, on the right side, one replaces Z_r in $\mathcal{W}_{B(H)}(Z)$ by the linear combination $\sum_{s\in R}\chi(sr)Z_s$. Also,

$$\mathcal{W}_H(Z) = \frac{1}{|A(H)|}\mathcal{W}_{A(H)}\Big(\sum_{s\in R}\chi(rs)Z_s\Big). \tag{8.2}$$

Proof. The Fourier transform (A.1) of $f_i(x_i) = Z_{x_i}$ is

$$\hat{f}_i(\pi_i) = \sum_{s\in R}\pi_i(s)Z_s.$$

Under the isomorphism α of Proposition 7.6, $(\widehat{R^n} : H)$ corresponds to $A(H)$, and π_i has the form $\pi_i(s) = \chi(y_i s)$, for some $y = (y_1, \ldots, y_n) \in A(H)$. We then observe that the resulting right hand side of the Poisson summation formula, Theorem A.4, is in the form of the complete weight enumerator after a linear substitution, as claimed in (8.2). The proof of (8.1) uses the isomorphism β instead. □

Defining an $|R| \times |R|$ matrix M by $M_{s,r} = \chi(sr)$, $s, r \in R$, and regarding $Z = (Z_r)$ as a column vector, the identities take the form

$$\mathcal{W}_H(Z) = \frac{1}{|B(H)|}\mathcal{W}_{B(H)}(M^tZ) \quad \text{and} \quad \mathcal{W}_H(Z) = \frac{1}{|A(H)|}\mathcal{W}_{A(H)}(MZ).$$

Corollary 8.2. *If H is a left submodule C, then $B(C) = \mathcal{R}(C)$ and*

$$\mathcal{W}_C(Z) = \frac{1}{|\mathcal{R}(C)|}\mathcal{W}_{\mathcal{R}(C)}(M^tZ).$$

Similarly, if H is a right submodule C, then $A(C) = \mathcal{L}(C)$ and

$$\mathcal{W}_C(Z) = \frac{1}{|\mathcal{L}(C)|}\mathcal{W}_{\mathcal{L}(C)}(MZ).$$

The *Hamming weight enumerator* for an additive subgroup H of R^n is

$$W_H(X,Y) = \sum_{x\in H} X^{n-\mathrm{wt}(x)}Y^{\mathrm{wt}(x)}.$$

The MacWilliams identities for the Hamming weight enumerator are then obtained from Theorem 8.1 by a specialization of variables: $Z_0 = X$, $Z_r = Y$ for $r \neq 0$.

Theorem 8.3. *For a finite Frobenius ring R and an additive subgroup H of R^n,*

$$W_H(X,Y) = \frac{1}{|B(H)|}W_{B(H)}\big(X + (|R|-1)Y, X - Y\big)$$

and

$$W_H(X,Y) = \frac{1}{|A(H)|}W_{A(H)}\big(X + (|R|-1)Y, X - Y\big).$$

When H is a submodule C, there are similar statements involving $\mathcal{R}(C)$ and $\mathcal{L}(C)$.

Finally, we describe symmetrized weight enumerators. Fix a subgroup U of the group of units of R. Let U act on R by left multiplication, and write $r \approx s$ if $r = us$ for some $u \in U$. Then $\approx$ is an equivalence relation, as we saw in Section 5. Let $S = \{s_1, \ldots, s_t\}$ be a set of representatives of the distinct orbits of U. Write $[r]$ for the representative in S of the orbit of r.

For every $s \in S$, let W_s be an indeterminate, and let $A = \mathbb{C}[W_s : s \in S]$ be the resulting complex polynomial algebra. The *symmetrized weight enumerator* of an additive subgroup H of R^n is

$$\mathcal{S}_H(W) = \sum_{x\in H}\prod_{i=1}^{n} W_{[x_i]} = \sum_{x\in H}\prod_{s\in S} W_s^{\mathrm{swc}_s(x)},$$

where $\mathrm{swc}_s(x) = \sum_{r\approx s} c_r(x)$ is the *symmetrized weight composition* of x. One then obtains the MacWilliams identities for the symmetrized weight enumerator from Theorem 8.1 by specializing variables Z_r to $W_{[r]}$. But in order for the specialization to work, we must make a technical assumption that the subgroup U be *central*, that is, $ru = ur$, for all $u \in U$, $r \in R$. If R is itself commutative, this condition is automatically satisfied.

Theorem 8.4. *Assume R is a finite Frobenius ring, that U is a subgroup of the group of units of R, that U is central, and that H is an additive subgroup of R^n. Then*

$$\mathcal{S}_H(W) = \frac{1}{|B(H)|}\mathcal{S}_{B(H)}\left(\sum_{s\in S}\Big(\sum_{r\approx s}\chi(rt)\Big)W_s\right)$$

and

$$\mathcal{S}_H(W) = \frac{1}{|A(H)|}\mathcal{S}_{A(H)}\left(\sum_{s\in S}\Big(\sum_{r\approx s}\chi(tr)\Big)W_s\right).$$

In both cases, the notation means to replace W_t in $\mathcal{S}(W)$ by the indicated linear combinations. When H is a submodule C, there are similar statements involving $\mathcal{R}(C)$ and $\mathcal{L}(C)$.

Remark 8.5. A similar set of identities holds if the subgroup U acts on R by right multiplication. The reader can make the needed adjustments in the definition of $\approx$.

Remark 8.6. These identities also extend to the situation where one uses an inner product on R^n of a slightly more general form. If $^-$ is an (anti)automorphism of R, let $\langle x, y\rangle = \sum x_i\bar{y}_i$ on R^n. By adjusting the definitions of $A(H)$ and $B(H)$, one can deduce MacWilliams identities for the new inner product from those for the standard dot product.

Remark 8.7. Dougherty [14] proved the MacWilliams identities for biweight enumerators over finite Frobenius rings.

Appendix A. Characters and the Fourier transform

For the convenience of the reader we collect together some standard definitions and theorems. There are no proofs. The results on characters are proved, for example, in Serre's books [36] and [37]. The results on the Fourier transform are left as exercises for the reader. The treatment that follows draws heavily on that of Terras in [38].

Let G be a finite abelian group, written additively. Let $\mathbb{T}$ be the multiplicative group of unit complex numbers; $\mathbb{T}$ is a 1-dimensional torus. A *character* of G is a group homomorphism $\pi : G \to \mathbb{T}$. The set of all characters of G forms a group $\widehat{G}$ called the *character group* of G; the group operation is pointwise multiplication of characters. We denote the trivial character by $\pi = 1$. The groups G and $\widehat{G}$ are isomorphic, but not naturally so; G is naturally isomorphic to the double character group $\widehat{\widehat{G}}$. If $G = G_1 \times G_2$ is a product, then so is $\widehat{G}$: $\widehat{G} = \widehat{G}_1 \times \widehat{G}_2$. The product character $\pi = (\pi_1, \pi_2)$ satisfies $\pi(x_1, x_2) = \pi_1(x_1)\pi_2(x_2)$.

Proposition A.1. *As elements of the vector space of all complex-valued functions on G, the characters of G are linearly independent.*

Proposition A.2.

$$\sum_{x\in G}\pi(x)=\begin{cases}|G|, & \pi=1,\\ 0, & \pi\neq 1,\end{cases}\quad \textit{and}\quad \sum_{\pi\in\widehat{G}}\pi(x)=\begin{cases}|G|, & x=0,\\ 0, & x\neq 0.\end{cases}$$

Let A be any vector space over the complex numbers. If $f:G\to A$ is any function, the *Fourier transform* $\hat{f}$ of f is the function $\hat{f}:\widehat{G}\to A$ given by

$$\hat{f}(\pi)=\sum_{x\in G}\pi(x)f(x). \tag{A.1}$$

Proposition A.3 (Fourier inversion formula)**.**

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

For any subgroup $H\subset G$, define the *annihilator* $(\widehat{G}:H)$ of H to be

$$(\widehat{G}:H)=\{\pi\in\widehat{G}:\pi(h)=1 \text{ for all } h\in H\}. \tag{A.2}$$

It follows that $(\widehat{G}:H)$ is isomorphic to the character group $(G/H)\widehat{\ }$ of the quotient group G/H. Thus $|(\widehat{G}:H)|=|G|/|H|$.

Theorem A.4 (Poisson summation formula)**.** *For any $a\in G$,*

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

We close with a technical result used in the proof of the MacWilliams identities.

Proposition A.5. *Assume that A is an commutative algebra over the complex numbers. Suppose $f:G^n\to A$ is a product of functions of one variable, i.e.,*

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

where each $f_i:G\to A$.

Then $\hat{f}=\prod\hat{f}_i$, i.e., for $\pi=(\pi_1,\dots,\pi_n)\in\widehat{G^n}$,

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

References

[1] D. D. Anderson and S. Valdes-Leon, Factorization in commutative rings with zero-divisors, *Rocky Mountain J. Math.* **26** (1996), 439–480.

[2] F. W. Anderson and K. R. Fuller, *Rings and categories of modules, Graduate Texts in Math.*, vol. 13, Springer-Verlag, New York, 1974.

[3] Č. Arf, Untersuchungen über quadratische Formen in Körpern der Charakteristik 2. I., *J. Reine Angew. Math.* **183** (1941), 148–167.

[4] E. F. Assmus, Jr. and H. F. Mattson, Jr., Coding and combinatorics, *SIAM Review* **16** (1974), 349–388.

[5] M. Auslander, I. Reiten, and S. Smalø, *Representation theory of Artin algebras*, Cambridge University Press, Cambridge, 1995.

[6] H. Bass, K-theory and stable algebra, *Inst. Hautes Études Sci. Publ. Math.* **22** (1964), 5–60.

[7] K. Bogart, D. Goldberg, and J. Gordon, An elementary proof of the MacWilliams theorem on equivalence of codes, *Inform. and Control* **37** (1978), 19–22.

[8] A. R. Calderbank, A. R. Hammons, Jr., P. V. Kumar, N. J. A. Sloane, and P. Solé, A linear construction for certain Kerdock and Preparata codes, *Bull. Amer. Math. Soc. (N. S.)* **29** (1993), 218–222.

[9] H. L. Claasen and R. W. Goldbach, A field-like property of finite rings, *Indag. Math.* **3** (1992), 11–26.

[10] P. M. Cohn, *Morita equivalence and duality*, Queen Mary College Mathematics Notes, London, 1966.

[11] I. Constantinescu, W. Heise, and Th. Honold, Monomial extensions of isometries between codes over $\mathbb{Z}_m$, *Proceedings of the Fifth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT '96) (Sozopol, Bulgaria)*, Unicorn, Shumen, 1996, pp. 98–104.

[12] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Interscience Publishers, New York, 1962.

[13] P. Delsarte, Bounds for unrestricted codes, by linear programming, *Philips Res. Rpts.* **27** (1972), 272–289.

[14] S. T. Dougherty, Codes and biweight enumerators, University of Scranton preprint, 1996.

[15] S. Eilenberg and T. Nakayama, On the dimension of modules and algebras II (Frobenius algebras and quasi-Frobenius rings), *Nagoya Math. J.* **9** (1955), 1–16.

[16] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry, Graduate Texts in Math.*, vol. 150, Springer-Verlag, New York, 1995.

[17] D. Y. Goldberg, A generalized weight for linear codes and a Witt-MacWilliams theorem, *J. Combin. Theory Ser. A* **29** (1980), 363–367.

[18] M. Hall, A type of algebraic closure, *Ann. of Math.* **40** (1939), 360–369.

[19] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE Trans. Inform. Theory* **IT-40** (1994), 301–319.

[20] Y. Hirano, On admissible rings, *Indag. Math.* **8** (1997), 55–59.

[21] M. Klemm, Über die Identität von MacWilliams für die Gewichtsfunktion von Codes, *Arch. Math. (Basel)* **49** (1987), 400–406.

[22] ———, Eine Invarianzgruppe für die vollständige Gewichtsfunktion selbstdualer Codes, *Arch. Math. (Basel)* **53** (1989), 332–336.
[23] ———, Selbstduale Codes über dem Ring der ganzen Zahlen modulo 4, *Arch. Math. (Basel)* **53** (1989), 201–207.
[24] R. G. Larson and M. E. Sweedler, An associative orthogonal bilinear form for Hopf algebras, *Amer. J. Math.* **91** (1969), 75–94.
[25] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes, North-Holland Mathematical Library*, vol. 16, North-Holland, Amsterdam, New York, Oxford, 1978.
[26] F. J. MacWilliams, Error-correcting codes for multiple-level transmission, *Bell System Tech. J.* **40** (1961), 281–308.
[27] ———, Combinatorial problems of elementary abelian groups, Ph.D. thesis, Radcliffe College, Cambridge, Mass., 1962.
[28] H. R. Margolis, *Spectra and the Steenrod algebra*, North-Holland, Amsterdam, 1983.
[29] B. R. McDonald, *Finite rings with identity, Pure and Applied Mathematics*, vol. 28, Marcel Dekker, Inc., New York, 1974.
[30] K. Morita, Duality for modules and its applications to the theory of rings with minimum condition, *Sci. Rep. Tokyo Kyoiku Daigaku, Sect. A* **6** (1958), 85–142.
[31] T. Nakayama and C. Nesbitt, Note on symmetric algebras, *Ann. of Math.* **39** (1938), 659–668.
[32] T. Nakayama, On Frobeniusean algebras. I., *Ann. of Math.* **40** (1939), 611–633, II., **42** (1941), 1–21.
[33] A. A. Nechaev, Linear codes over modules and over spaces: MacWilliams identities, *Proceedings of the 1996 IEEE Int. Symp. on Inf. Theory and Appl. (Victoria, B.C., Canada)*, September 17–20, 1996.
[34] A. A. Nechaev and A. S. Kuzmin, Formal duality of linearly presentable codes over a Galois field, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (Toulouse, 1997)* (T. Mora and H. Mattson, eds.), *Lecture Notes in Comput. Sci.*, vol. 1255, Springer-Verlag, Berlin, 1997, pp. 263–276.
[35] L. Pontryagin, *Topological groups*, Princeton University Press, Princeton, 1939.
[36] J.-P. Serre, *A course in arithmetic, Graduate Texts in Math.*, vol. 7, Springer-Verlag, New York, 1973.
[37] ———, *Linear representations of finite groups, Graduate Texts in Math.*, vol. 42, Springer-Verlag, New York, 1977.
[38] A. Terras, Fourier analysis on finite groups and applications, UCSD lecture notes, 1992.
[39] H. N. Ward and J. A. Wood, Characters and the equivalence of codes, *J. Combin. Theory Ser. A* **73** (1996), 348–352.
[40] E. Witt, Theorie der quadratischen Formen in beliebigen Körpern, *J. Reine Angew. Math.* **176** (1937), 31–44.
[41] J. A. Wood, Extension theorems for linear codes over finite rings, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (Toulouse, 1997)* (T. Mora and H. Mattson, eds.), *Lecture Notes in Comput. Sci.*, vol. 1255, Springer-Verlag, Berlin, 1997, pp. 329–340.
[42] ———, Semigroup rings and the extension theorem for linear codes, *Proceedings of the Thirty-Fifth Annual Allerton Conference on Communication, Control, and Computing*, University of Illinois, 1997, pp. 163–174.

[43] ———, Weight functions and the extension theorem for linear codes over finite rings, *Finite Fields: Theory, Applications and Algorithms* (R. C. Mullin and G. L. Mullen, eds.), *Contemp. Math.*, vol. 225, Amer. Math. Soc., Providence, RI, 1999, pp. 231–243.
[44] W. Xue, A note on finite local rings, *Indag. Math.* (to appear).

Department of Mathematics, Computer Science & Statistics, Purdue University Calumet, Hammond, IN 46323–2094
E-mail address: wood@calumet.purdue.edu
URL: http://www.calumet.purdue.edu/public/math/wood/