APPLICATIONS OF FINITE FROBENIUS RINGS TO THE FOUNDATIONS OF ALGEBRAIC CODING THEORY

JAY A. WOOD

Abstract. This article addresses some foundational issues that arise in the study of linear codes defined over finite rings. Linear coding theory is particularly well-behaved over finite Frobenius rings. This follows from the fact that the character module of a finite ring is free if and only if the ring is Frobenius.

Key Words: Frobenius ring, generating character, linear code, extension theorem, MacWilliams identities.

2010 *Mathematics Subject Classification*: Primary 16P10, 94B05; Secondary 16D50, 16L60.

1. Introduction

At the center of coding theory lies a very practical problem: how to ensure the integrity of a message being transmitted over a noisy channel? Even children are aware of this problem: the game of "telephone" has one child whisper a sentence to a second child, who in turn whispers it to a third child, and the whispering continues. The last child says the sentence out loud. Usually the children burst out laughing, because the final sentence bears little resemblance to the original.

Using electronic devices, messages are transmitted over many different noisy channels: copper wires, fiber optic cables, saving to storage devices, and radio, cell phone, and deep-space communications. In all cases, it is desirable that the message being received is the same as the message being sent. The standard approach to error-correction is to incorporate redundancy in a cleverly designed way (encoding), so that transmission errors can be efficiently detected and corrected (decoding).

Mathematics has played an essential role in coding theory, with the seminal work of Claude Shannon [27] leading the way. Many constructions of encoding and decoding schemes make strong use of algebra and combinatorics, with linear algebra over finite fields often playing a prominent part. The rich interplay of ideas from multiple areas has led to discoveries that are of independent mathematical interest.

This article addresses some of the topics that lie at the mathematical foundations of algebraic coding theory, specifically topics related to linear codes defined over finite rings. This article is not an encyclopedic survey; the mathematical questions addressed are ones in which the author has been actively involved and are ones that apply to broad classes of finite rings, not just to specific examples.

Prepared for the 44th Symposium on Rings and Representation Theory Japan, 2011.

Supported in part by a sabbatical leave from Western Michigan University.

This paper is in final form and no version of it will be submitted for publication elsewhere.

The topics covered are ring-theoretic analogs of results that go back to one of the early leaders of the field, Florence Jessie MacWilliams (1917–1990). MacWilliams worked for many years at Bell Labs, and she received her doctorate from Harvard University in 1962, under the direction of Andrew Gleason [22]. She is the co-author, with Neil Sloane, of the most famous textbook on coding theory [23].

Two of the topics discussed in this article are found in the doctoral dissertation of MacWilliams [22]. One topic is the famous MacWilliams identities, which relate the Hamming weight enumerator of a linear code to that of its dual code. The MacWilliams identities have wide application, especially in the study of self-dual codes (linear codes that equal their dual code). The MacWilliams identities are discussed in Section 4, and some interesting aspects of self-dual codes due originally to Gleason are discussed in Section 6.

The other topic to be discussed, also found in MacWilliams's dissertation, is the MacWilliams extension theorem. This theorem is not as well known as the MacWilliams identities, but it underlies the notion of equivalence of linear codes. It is easy to show that a monomial transformation defines an isomorphism between linear codes that preserves the Hamming weight. What is not so obvious is the converse: whether every isomorphism between linear codes that preserves the Hamming weight must extend to a monomial transformation. MacWilliams proves that this is indeed the case over finite fields. The MacWilliams extension theorem is a coding-theoretic analog of the extension theorems for isometries of bilinear forms and quadratic forms due to Witt [30] and Arf [1].

This article describes, in large part, how these two results, the MacWilliams identities and the MacWilliams extension theorem, generalize to linear codes defined over finite rings. The punch line is that both theorems are valid for linear codes defined over finite Frobenius rings. Moreover, Frobenius rings are the largest class of finite rings over which the extension theorem is valid.

Why finite Frobenius rings? Over finite fields, both the MacWilliams identities and the MacWilliams extension theorem have proofs that make use of character theory. In particular, finite fields $\mathbb{F}$ have the simple, but crucial, properties that their characters $\widehat{\mathbb{F}}$ form a vector space over $\mathbb{F}$ and $\widehat{\mathbb{F}} \cong \mathbb{F}$ as vector spaces. The same proofs will work over a finite ring R, provided R has the same crucial property that $\widehat{R} \cong R$ as one-sided modules. It turns out that finite Frobenius rings are exactly characterized by this property ([14, Theorem 1] and, independently, [31, Theorem 3.10]). The character theory of finite Frobenius rings is discussed in Section 2, and the extension theorem is discussed in Section 5. Some standard terminology from algebraic coding theory is discussed in Section 3.

While much of this article is drawn from earlier works, especially [31] and [33], some of the treatment of generating characters for Frobenius rings in Section 2 has not appeared before. The new results are marked with a dagger (†).

Acknowledgments. I thank the organizers of the 44th Symposium on Rings and Representation Theory Japan, 2011, especially Professor Kunio Yamagata, for inviting me to address the symposium and prepare this article, and for their generous support. I thank Professor Yun Fan for suggesting subsection 2.4 and Steven T. Dougherty for bringing the problem of the form of a generating character to my attention (answered by Corollary 15). I also thank M. Klemm, H. L. Claasen, and R. W. Goldbach for their early work

on generating characters, which helped me develop my approach to the subject. Finally, I thank my wife Elizabeth S. Moore for her encouragement and support.

2. Finite Frobenius Rings

In an effort to make this article somewhat self-contained, both for ring-theorists and coding-theorists, I include some background material on finite Frobenius rings. The goal of this section is to show that finite Frobenius rings are characterized by having free character modules. Useful references for this material are Lam's books [19] and [20].

All rings will be associative with 1, and all modules will be unitary. While left modules will appear most often, there are comparable results for right modules. Almost all of the rings used in this article will be finite, so that some definitions that are more broadly applicable may be simplified in the finite context.

2.1. **Definitions.** Given a finite ring R, its (Jacobson) *radical* $\operatorname{rad}(R)$ is the intersection of all the maximal left ideals of R; $\operatorname{rad}(R)$ is itself a two-sided ideal of R. A left R-module is *simple* if it has no nonzero proper submodules. Given a left R-module M, its *socle* $\operatorname{soc}(M)$ is the sum of all the simple submodules of M. A ring R has a left socle $\operatorname{soc}({}_RR)$ and a right socle $\operatorname{soc}(R_R)$ (from viewing R as a left R-module or as a right R-module); both socles are two-sided ideals, but they may not be equal. (They are equal if R is semiprime, which, for finite rings, is equivalent to being semisimple.)

Let R be a finite ring. Then the quotient ring $R/\operatorname{rad}(R)$ is semi-simple and is isomorphic to a direct sum of matrix rings over finite fields (Wedderburn-Artin):

$$R/\operatorname{rad}(R) \cong \bigoplus_{i=1}^{k} M_{m_i}(\mathbb{F}_{q_i}), \tag{2.1}$$

where each q_i is a prime power; $\mathbb{F}_q$ denotes a finite field of order q, q a prime power, and $M_m(\mathbb{F}_q)$ denotes the ring of $m \times m$ matrices over $\mathbb{F}_q$.

Definition 1 ([19, Theorem 16.14])**.** A finite ring R is *Frobenius* if ${}_R(R/\operatorname{rad}(R)) \cong \operatorname{soc}({}_RR)$ and $(R/\operatorname{rad}(R))_R \cong \operatorname{soc}(R_R)$.

This definition applies more generally to Artinian rings. It is a theorem of Honold [15, Theorem 2] that, for finite rings, only one of the isomorphisms (left or right) is needed.

Each of the matrix rings $M_{m_i}(\mathbb{F}_{q_i})$ in (2.1) has a simple left module $T_i := M_{m_i\times 1}(\mathbb{F}_{q_i})$, consisting of all $m_i \times 1$ matrices over $\mathbb{F}_{q_i}$, under left matrix multiplication. From (2.1) it follows that, as left R-modules, we have an isomorphism

$${}_R(R/\operatorname{rad}(R)) \cong \bigoplus_{i=1}^{k} m_iT_i. \tag{2.2}$$

It is known that the T_i, $i = 1, \ldots, k$, form a complete list of simple left R-modules, up to isomorphism.

Because the left socle of an R-module is a sum of simple left R-modules, it can be expressed as a sum of the T_i. In particular, the left socle of R itself admits such an expression:

$$\operatorname{soc}({}_R R) \cong \bigoplus_{i=1}^{k} s_i T_i, \tag{2.3}$$

for some nonnegative integers $s_1, \ldots, s_k$. Thus a finite ring is Frobenius if and only if $m_i = s_i$ for all $i = 1, \ldots, k$.

2.2. **Characters.** Let G be a finite abelian group. In this article, a *character* is a group homomorphism $\varpi : G \to \mathbb{Q}/\mathbb{Z}$. The set of all characters of G forms a group called the *character group* $\widehat{G} := \operatorname{Hom}_{\mathbb{Z}}(G, \mathbb{Q}/\mathbb{Z})$. It is well-known that $|\widehat{G}| = |G|$. (Characters with values in the multiplicative group of nonzero complex numbers can be obtained by composing with the complex exponential function $a \mapsto \exp(2\pi i a)$, $a \in \mathbb{Q}/\mathbb{Z}$; this multiplicative form of characters will be needed in later sections.)

If R is a finite ring and A is a finite left R-module, then $\widehat{A}$ consists of the characters of the additive group of A; $\widehat{A}$ is naturally a right R-module via the scalar multiplication $(\varpi r)(a) := \varpi(ra)$, for $\varpi \in \widehat{A}$, $r \in R$, and $a \in A$. The module $\widehat{A}$ will be called the *character module* of A. Similarly, if B is a right R-module, then $\widehat{B}$ is naturally a left R-module.

Example 2. Let $\mathbb{F}_p$ be a finite field of prime order. Define $\vartheta_p : \mathbb{F}_p \to \mathbb{Q}/\mathbb{Z}$ by $\vartheta_p(a) = a/p$, where we view $\mathbb{F}_p$ as $\mathbb{Z}/p\mathbb{Z}$. Then ϑ_p is a character of $\mathbb{F}_p$, and every other character ϖ of $\mathbb{F}_p$ has the form $\varpi = a\vartheta_p$, for some $a \in \mathbb{F}_p$ (because $\widehat{\mathbb{F}}_p$ is a one-dimensional vector space over $\mathbb{F}_p$).

Let $\mathbb{F}_q$ be a finite field with $q = p^\ell$ for some prime p. Let $\operatorname{tr}_{q/p} : \mathbb{F}_q \to \mathbb{F}_p$ be the trace. Define $\vartheta_q : \mathbb{F}_q \to \mathbb{Q}/\mathbb{Z}$ by $\vartheta_q = \vartheta_p \circ \operatorname{tr}_{q/p}$. Then ϑ_q is a character of $\mathbb{F}_q$, and every other character ϖ of $\mathbb{F}_q$ has the form $\varpi = a\vartheta_q$, for some $a \in \mathbb{F}_q$.

Example 3. Let $R = M_m(\mathbb{F}_q)$ be the ring of $m \times m$ matrices over a finite field $\mathbb{F}_q$, and let $A = M_{m\times k}(\mathbb{F}_q)$ be the left R-module consisting of all $m \times k$ matrices over $\mathbb{F}_q$. Then $\widehat{A} \cong M_{k\times m}(\mathbb{F}_q)$ as right R-modules. Indeed, given a matrix $Q \in M_{k\times m}(\mathbb{F}_q)$, define a character ϖ_Q of A by $\varpi_Q(P) = \vartheta_q(\operatorname{tr}(QP))$, for $P \in A$, where tr is the matrix trace and ϑ_q is the character of $\mathbb{F}_q$ defined in Example 2. The map $M_{k\times m}(\mathbb{F}_q) \to \widehat{A}$, $Q \mapsto \varpi_Q$ is the desired isomorphism.

Given a short exact sequence of finite left R-modules $0 \to A \to B \to C \to 0$, there is an induced short exact sequence of right R-modules

$$0 \to \widehat{C} \to \widehat{B} \to \widehat{A} \to 0. \tag{2.4}$$

In particular, if we define the *annihilator* $(\widehat{B} : A) := \{\varpi \in \widehat{B} : \varpi(A) = 0\}$, then

$$(\widehat{B} : A) \cong \widehat{C} \quad \text{and} \quad |(\widehat{B} : A)| = |C| = |B|/|A|. \tag{2.5}$$

2.3. **Generating Characters.** In the special case that $A = R$, R is both a left and a right R-module. A character $\varpi \in \widehat{R}$ induces both a left and a right homomorphism $R \to \widehat{R}$ ($r \mapsto r\varpi$ is a left homomorphism, while $r \mapsto \varpi r$ is a right homomorphism). The character ϖ is called a left (resp., right) *generating character* if $r \mapsto r\varpi$ (resp., $r \mapsto \varpi r$) is a module isomorphism. In this situation, the character ϖ generates the left (resp., right)

R-module $\widehat{R}$. Because $|\widehat{R}| = |R|$, one of these homomorphisms is an isomorphism if and only if it is injective if and only if it is surjective.

Remark 4. The phrase *generating character* ("erzeugenden Charakter") is due to Klemm [17]. Claasen and Goldbach [6] used the adjective *admissible* to describe the same phenomenon, although their use of left and right is the reverse of ours.

The theorem below relates generating characters and finite Frobenius rings. While the theorem is over ten years old, we will give a new proof.

Theorem 5 ([14, Theorem 1], [31, Theorem 3.10])**.** *Let R be a finite ring. Then the following are equivalent:*

(1) *R is Frobenius;*
(2) *R admits a left generating character, i.e., $\widehat{R}$ is a free left R-module;*
(3) *R admits a right generating character, i.e., $\widehat{R}$ is a free right R-module.*

Moreover, when these conditions are satisfied, every left generating character is also a right generating character, and vice versa.

Example 6. Here are several examples of finite Frobenius rings and generating characters (when easy to describe).

(1) Finite field $\mathbb{F}_q$ with generating character ϑ_q of Example 2. Note that ϑ_p is injective, but that for $q > p$, $\ker \vartheta_q = \ker \mathrm{tr}_{q/p}$ is a nonzero $\mathbb{F}_p$-linear subspace of $\mathbb{F}_q$. However, $\ker \vartheta_q$ is not an $\mathbb{F}_q$-linear subspace. (Compare with Proposition 7 below.)
(2) Integer residue ring $\mathbb{Z}/n\mathbb{Z}$ with generating character ϑ_n defined by $\vartheta_n(a) = a/n$, for $a \in \mathbb{Z}/n\mathbb{Z}$.
(3) Finite chain ring R; i.e., a finite ring all of whose left ideals form a chain under inclusion. See Corollary 15 for information about a generating character.
(4) If $R_1, \ldots, R_n$ are Frobenius with generating characters $\varrho_1, \ldots, \varrho_n$, then their direct sum $R = \oplus R_i$ is Frobenius with generating character $\varrho = \sum \varrho_i$. Conversely, if $R = \oplus R_i$ is Frobenius with generating character ϱ, then each R_i is Frobenius, with generating character $\varrho_i = \varrho \circ \iota_i$, where $\iota_i : R_i \to R$ is the inclusion; $\varrho = \sum \varrho_i$.
(5) If R is Frobenius with generating character ϱ, then the matrix ring $M_m(R)$ is Frobenius with generating character $\varrho \circ \mathrm{tr}$, where tr is the matrix trace.
(6) If R is Frobenius with generating character ϱ and G is any finite group, then the group ring $R[G]$ is Frobenius with generating character $\varrho \circ \mathrm{pr}_e$, where $\mathrm{pr}_e : R[G] \to R$ is the projection that associates to every element $a = \sum a_g g \in R[G]$ the coefficient a_e of the identity element of G.

In preparation for the proof of Theorem 5, we prove several propositions concerning generating characters.

Proposition 7 ([6, Corollary 3.6])**.** *Let R be a finite ring. A character ϖ of R is a left (resp., right) generating character if and only if $\ker \varpi$ contains no nonzero left (resp., right) ideal of R.*

Proof. By the definition and $|\widehat{R}| = |R|$, ϖ is a left generating character if and only if the homomorphism $f : R \to \widehat{R}$, $r \mapsto r\varpi$, is injective. Then $r \in \ker f$ if and only if the

principal ideal $Rr \subset \ker \varpi$. Thus, $\ker f = 0$ if and only if $\ker \varpi$ contains no nonzero left ideals. The proof for right generating characters is similar. □

Proposition 8 ([31, Theorem 4.3])**.** *A character ϱ of a finite ring R is a left generating character if and only if it is a right generating character.*

Proof. Suppose ϱ is a left generating character, and suppose that $I \subset \ker \varrho$ is a right ideal. Then for every $r \in R$, $Ir \subset \ker \varrho$, so that $I \subset \ker(r\varrho)$, for all $r \in R$. But every character of R is of the form $r\varrho$, because ϱ is a left generating character. Thus the annihilator $(\widehat{R} : I) = \widehat{R}$, and it follows from (2.5) that $I = 0$. By Proposition 7, ϱ is a right generating character. □

Proposition 9 ([33, Proposition 3.3])**.** *Let A be a finite left R-module. Then* $\operatorname{soc}(\widehat{A}) \cong (A/\operatorname{rad}(R)A)\widehat{\ }$.

Proof. There is a short exact sequence of left R-modules

$$0 \to \operatorname{rad}(R)A \to A \to A/\operatorname{rad}(R)A \to 0.$$

Taking character modules, as in (2.4), yields

$$0 \to (A/\operatorname{rad}(R)A)\widehat{\ } \to \widehat{A} \to (\operatorname{rad}(R)A)\widehat{\ } \to 0.$$

Because $A/\operatorname{rad}(R)A$ is a sum of simple modules, the same is true for $(A/\operatorname{rad}(R)A)\widehat{\ } \cong (\widehat{A} : \operatorname{rad}(R)A)$. Thus $(\widehat{A} : \operatorname{rad}(R)A) \subset \operatorname{soc}(\widehat{A})$.

Conversely, $\operatorname{soc}(\widehat{A}) \operatorname{rad}(R) = 0$, because the radical annihilates simple modules [7, Exercise 25.4]. Thus $\operatorname{soc}(\widehat{A}) \subset (\widehat{A} : \operatorname{rad}(R)A)$, and we have the equality $\operatorname{soc}(\widehat{A}) = (\widehat{A} : \operatorname{rad}(R)A)$. Now remember that $(\widehat{A} : \operatorname{rad}(R)A) \cong (A/\operatorname{rad}(R)A)\widehat{\ }$. □

Using Proposition 7 as a model, we extend the definition of a generating character to modules. Let A be a finite left (resp., right) R-module. A character ϖ of A is a *generating character* of A if $\ker \varpi$ contains no nonzero left (resp., right) R-submodules of A.

Lemma 10 (†)**.** *Let A be a finite left R-module, and let $B \subset A$ be a submodule. If A admits a left generating character, then B admits a left generating character.*

Proof. Simply restrict a generating character of A to B. Any submodule of B inside the kernel of the restriction will also be a submodule of A inside the kernel of the original generating character. □

Lemma 11 (†)**.** *Let R be any finite ring. Define $\varrho : \widehat{R} \to \mathbb{Q}/\mathbb{Z}$ by $\varrho(\varpi) = \varpi(1)$, evaluation at $1 \in R$, for $\varpi \in \widehat{R}$. Then ϱ is a left and right generating character of $\widehat{R}$.*

Proof. Suppose $\varpi_0 \neq 0$ has the property that $R\varpi_0 \subset \ker \varrho$. This means that for every $r \in R$, $0 = \varrho(r\varpi_0) = (r\varpi_0)(1) = \varpi_0(r)$, so that $\varpi_0 = 0$. Thus ϱ is a left generating character by definition. Similarly for ϱ being a right generating character. □

Proposition 12 (†)**.** *Let A be a finite left R-module. Then A admits a left generating character if and only if A can be embedded in $\widehat{R}$.*

Proof. If A embeds in $\widehat{R}$, then A admits a generating character, by Lemmas 10 and 11.

Conversely, let ϱ be a generating character of A. We use ϱ to define $f : A \to \widehat{R}$, as follows. For $a \in A$, define $f(a) \in \widehat{R}$ by $f(a)(r) = \varrho(ra)$, $r \in R$. It is easy to check that $f(a)$ is indeed in $\widehat{R}$, i.e., that $f(a)$ is a character of R. It is also easy to verify that f is a left R-module homomorphism from A to $\widehat{R}$. If $a \in \ker f$, then $\varrho(ra) = 0$ for all $r \in R$. Thus the left R-submodule $Ra \subset \ker \varrho$. Because ϱ is a generating character, we conclude that $Ra = 0$. Thus $a = 0$, and f is injective. □

When $A = R$, Proposition 12 is consistent with the definition of a generating character of a ring. Indeed, if R embeds into $\widehat{R}$, then R and $\widehat{R}$ are isomorphic as one-sided modules, because they have the same number of elements.

Theorem 13 (†)**.** *Let $R = M_m(\mathbb{F}_q)$ be the ring of $m \times m$ matrices over a finite field $\mathbb{F}_q$. Let $A = M_{m\times k}(\mathbb{F}_q)$ be the left R-module of all $m \times k$ matrices over $\mathbb{F}_q$. Then A admits a left generating character if and only if $m \geq k$.*

Proof. If $m \geq k$, then, by appending $m - k$ columns of zeros, A can be embedded inside R as a left ideal. By Example 3 and Lemma 10, A admits a generating character.

Conversely, suppose $m < k$. We will show that no character of A is a generating character of A. To that end, let ϖ be any character of A. By Example 3, ϖ has the form ϖ_Q for some $k \times m$ matrix Q over $\mathbb{F}_q$. Because $k > m$, the rows of Q are linearly dependent over $\mathbb{F}_q$. Let P be any nonzero matrix over $\mathbb{F}_q$ of size $m \times k$ such that $PQ = 0$. Such a P exists because the rows of Q are linearly dependent: use the coefficients of a nonzero dependency relation as the entries for a row of P. We claim that the nonzero left submodule of A generated by P is contained in $\ker \varpi_Q$. Indeed, for any $B \in R$, $\varpi_Q(BP) = \vartheta_q(\mathrm{tr}(Q(BP))) = \vartheta_q(\mathrm{tr}((BP)Q)) = \vartheta_q(\mathrm{tr}(B(PQ))) = 0$, using $PQ = 0$ and the well-known property $\mathrm{tr}(BC) = \mathrm{tr}(CB)$ of the matrix trace. Thus, no character of A is a generating character. □

Proposition 14 (†)**.** *Suppose A is a finite left R-module. Then A admits a left generating character if and only if* $\mathrm{soc}(A)$ *admits a left generating character.*

Proof. If A admits a generating character, then so does $\mathrm{soc}(A)$, by Lemma 10.

Conversely, suppose $\mathrm{soc}(A)$ admits a generating character ϑ. Utilizing the short exact sequence (2.4), let ϱ be any extension of ϑ to a character of A . We claim that ϱ is a generating character of A. To that end, suppose B is a submodule of A such that $B \subset \ker \varrho$. Then $\mathrm{soc}(B) \subset \mathrm{soc}(A) \cap \ker \varrho = \mathrm{soc}(A) \cap \ker \vartheta$, because ϱ is an extension of ϑ. But ϑ is a generating character of $\mathrm{soc}(A)$, so $\mathrm{soc}(B) = 0$. Since B is a finite module, we conclude that $B = 0$. Thus ϱ is a generating character of A. □

Corollary 15 (†)**.** *Let A be a finite left R-module. Suppose* $\mathrm{soc}(A)$ *admits a left generating character ϑ. Then any extension of ϑ to a character of A is a left generating character of A.*

We now (finally) turn to the proof of Theorem 5.

(†) *Proof of Theorem 5.* Statements (2) and (3) are equivalent by Proposition 8. We next show that (3) implies (1).

By Example 3, the right R-module $(R/\operatorname{rad}(R))_R$ equals the character module of the left R-module ${}_R(R/\operatorname{rad}(R))$. By Proposition 9 applied to the left R-module $A = {}_RR$, we have $({}_R(R/\operatorname{rad}(R)))\widehat{\ } \cong \operatorname{soc}(\widehat{R}_R) \cong \operatorname{soc}(R_R)$, because $\widehat{R}$ is assumed to be right free. We thus have an isomorphism $(R/\operatorname{rad}(R))_R \cong \operatorname{soc}(R_R)$ of right R-modules. One can either repeat the argument for a left isomorphism (using (2)) or appeal to the theorem of Honold [15, Theorem 2] mentioned after Definition 1.

Now assume (1). Referring to (2.1), we see that R being Frobenius implies that $\operatorname{soc}(R)$ is a sum of matrix modules of the form $M_{m_i}(\mathbb{F}_{q_i})$. By Theorem 13 and summing, $\operatorname{soc}(R)$ admits a left generating character. By Propositions 7 and 14, R itself admits a left generating character. Thus (2) holds. □

2.4. **Frobenius Algebras.** In this subsection I want to point out the similarity between a general (not necessarily finite) Frobenius algebra and a finite Frobenius ring. I thank Professor Yun Fan for suggesting this short exposition.

Definition 16. A finite-dimensional algebra A over a field F is a *Frobenius algebra* if there exists a linear functional $\lambda : A \to F$ such that $\ker\lambda$ contains no nonzero left ideals of A.

It is apparent that the structure functional λ plays a role for a Frobenius algebra comparable to that played by a left generating character ϱ of a finite Frobenius ring. As one might expect, the connection between λ and ϱ is even stronger when one considers a finite Frobenius algebra. Recall that every finite field $\mathbb{F}_q$ admits a generating character ϑ_q, by Example 2.

Theorem 17 (†)**.** *Let R be a Frobenius algebra over a finite field $\mathbb{F}_q$, with structure functional $\lambda : R \to \mathbb{F}_q$. Then R is a finite Frobenius ring with left generating character $\varrho = \vartheta_q \circ \lambda$.*

Conversely, suppose R is a finite-dimensional algebra over a finite field $\mathbb{F}_q$ and that R is a Frobenius ring with generating character ϱ. Then R is a Frobenius algebra, and there exists a structure functional $\lambda : R \to \mathbb{F}_q$ such that $\varrho = \vartheta_q \circ \lambda$.

Proof. Both $R^* := \operatorname{Hom}_{\mathbb{F}_q}(R, \mathbb{F}_q)$ and $\widehat{R} = \operatorname{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})$ are (R,R)-bimodules satisfying $|R^*| = |\widehat{R}| = |R|$. A generating character ϑ_q of $\mathbb{F}_q$ induces a bimodule homomorphism $f : R^* \to \widehat{R}$ via $\lambda \mapsto \vartheta_q \circ \lambda$. We claim that f is injective. To that end, suppose $\lambda \in \ker f$. Then $\vartheta_q \circ \lambda = 0$, so that $\lambda(R) \subset \ker\vartheta_q$. Note that $\lambda(R)$ is an $\mathbb{F}_q$-vector subspace contained in $\ker\vartheta_q \subset \mathbb{F}_q$. Because ϑ_q is a generating character of $\mathbb{F}_q$, $\lambda(R) = 0$, by Proposition 7. Thus $\lambda = 0$, and f is injective. Because $|R^*| = |\widehat{R}|$, f is in fact a bimodule isomorphism.

We next claim that the structure functionals in R^* correspond under f to the generating characters in $\widehat{R}$. That is, if $\varpi = f(\lambda)$, where $\lambda \in R^*$ and $\varpi \in \widehat{R}$, then λ satisfies the condition that $\ker\lambda$ contains no nonzero left ideals of R if and only if ϖ is a generating character of R (i.e., $\ker\varpi$ contains no nonzero left ideals of R).

Suppose ϖ is a generating character of R, and suppose that I is a left ideal of R with $I \subset \ker\lambda$. Since $\varpi = \vartheta_q \circ \lambda$, we also have $I \subset \ker\varpi$. Because ϖ is a generating character, Proposition 7 implies $I = 0$, as desired.

Conversely, suppose λ satisfies the condition that $\ker\lambda$ contains no nonzero left ideals of R, and suppose that I is a left ideal of R with $I \subset \ker\varpi$. Then $\lambda(I)$ is an $\mathbb{F}_q$-linear

subspace inside $\ker \vartheta_q \subset \mathbb{F}_q$. Because ϑ_q is a generating character of $\mathbb{F}_q$, we have $\lambda(I) = 0$, i.e., $I \subset \ker \lambda$. By the condition on λ, we conclude that $I = 0$, as desired. □

Remark 18. The proof of Theorem 17 shows the equivalence of the Morita duality functors $*$ and $\widehat{\ }$ when R is a finite-dimensional algebra over a finite field $\mathbb{F}$ (cf., [31, Remark 3.12]). For a finite R-module M, observe that $M^* := \mathrm{Hom}_{\mathbb{F}}(M, \mathbb{F}) \cong \mathrm{Hom}_R(M, R^*)$ and $\widehat{M} = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}_R(M, \widehat{R})$.

3. The Language of Algebraic Coding Theory

3.1. **Background on Error-Correcting Codes.** Error-correcting codes provide a way to protect messages from corruption during transmission (or storage). This is accomplished by adding redundancies in such a way that, with high probability, the original message can be recovered from the received message.

Let us be a little more precise. Let I be a finite set (of "information") which will be the possible messages that can be transmitted. An example: numbers from 0 to 63 representing gray scales of a photograph. Let A be another finite set (the "alphabet"); $A = \{0, 1\}$ is a typical example. An *encoding* of the information set I is an injection $f : I \to A^n$ for some n. The image $f(I)$ is a *code* in A^n.

For a given message $x \in I$, the string $f(x)$ is transmitted across a channel (which could be copper wire, fiber optic cable, saving to a storage device, or transmission by radio or cell phone). During the transmission process, some of the entries in the string $f(x)$ might be corrupted, so that the string $y \in A^n$ that is received may be different from the string $f(x)$ that was originally sent.

The challenge is this: for a given channel, to choose an encoding f in such a way that it is possible, with high probability, to recover the original message x knowing only the corrupted received message y (and the method of encoding). The process of recovering x is called *decoding*.

The seminal theorem that launched the field of coding theory is due to Claude Shannon [27]. Paraphrasing, it says: up to a limit determined by the channel, it is always possible to find an encoding which will decode with as high a probability as one desires, provided one takes the encoding length n sufficiently large. Shannon's proof is not constructive; it does not build an encoding, nor does it describe how to decode. Much of the research in coding theory since Shannon's theorem has been devoted to finding good codes and developing decoding algorithms for them. Good references for background on coding theory are [16] and [23].

3.2. **Algebraic Coding Theory.** Researchers have more tools at their disposal in constructing codes if they assume that the alphabet A and the codes $C \subset A^n$ are equipped with algebraic structures. The first important case is to assume that A is a finite field and that $C \subset A^n$ is a linear subspace.

Definition 19. Let $\mathbb{F}$ be a finite field. A *linear code* of length n over $\mathbb{F}$ is a linear subspace $C \subset \mathbb{F}^n$. The dimension of the linear code is traditionally denoted by $k = \dim_{\mathbb{F}} C$.

Given two vectors $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in \mathbb{F}^n$, their *Hamming distance* $d(x, y) = |\{i : x_i \neq y_i\}|$ is the number of positions where the vectors differ. The *Hamming*

weight $\mathrm{wt}(x) = d(x,0)$ of a vector $x \in \mathbb{F}^n$ equals the number of positions where the vector is nonzero. Note that $d(x,y) = \mathrm{wt}(x-y)$; d is symmetric and satisfies the triangle inequality. The *minimum distance* of a code $C \subset \mathbb{F}^n$ is the smallest value d_C of $d(x,y)$ for $x \neq y$, $x, y \in C$. When C is a linear code, d_C equals the smallest value of $\mathrm{wt}(x)$ for $x \neq 0$, $x \in C$.

The minimum distance of a code C is a measure of the code's error-correcting capability. Let $B(x,r) = \{y \in \mathbb{F}^n : d(x,y) \leq r\}$ be the ball in $\mathbb{F}^n$ centered at x of radius r. Set $r_0 = [(d_C - 1)/2]$, the greatest integer less than or equal to $(d_C - 1)/2$. Then all the balls $B(x, r_0)$ for $x \in C$ are disjoint. Suppose $x \in C$ is transmitted and $y \in \mathbb{F}^n$ is received. Decode y to the nearest element in the code C (and flip a coin if there is a tie). If at most r_0 entries of x are corrupted in the transmission, then this method always decodes correctly. We say that C corrects r_0 errors. The larger d_C is, the more errors that can be corrected.

3.3. **Weight Enumerators.** It is useful to keep track of the weights of all the elements of a code C. The *Hamming weight enumerator* $W_C(X,Y)$ is a polynomial (generating function) defined by

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

where A_i is the number of elements of weight i in C. Only the zero vector has weight 0. In a linear code, $A_0 = 1$, and $A_i = 0$ for $0 < i < d_C$.

Define an $\mathbb{F}$-valued inner product on $\mathbb{F}^n$ by

$$x \cdot y = \sum_{i=1}^{n} x_i y_i, \quad x = (x_1, \ldots, x_n), \quad y = (y_1, \ldots, y_n) \in \mathbb{F}^n.$$

Associated to every linear code $C \subset \mathbb{F}^n$ is its *dual code* $C^\perp$:

$$C^\perp = \{y \in \mathbb{F}^n : x \cdot y = 0, x \in C\}.$$

If $k = \dim C$, then $\dim C^\perp = n - k$.

One of the most famous results in algebraic coding theory relates the Hamming weight enumerator of a linear code C to that of its dual code $C^\perp$: the MacWilliams identities, which is the subject of Section 4.

Theorem 20 (MacWilliams Identities)**.** *Let C be a linear code in $\mathbb{F}_q^n$. Then*

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

Of special interest are self-dual codes. A linear code C is *self-orthogonal* if $C \subset C^\perp$; C is *self-dual* if $C = C^\perp$. Note that a self-dual code C of length n and dimension k satisfies $n = 2k$, so that n must be even.

3.4. **Linear Codes over Rings.** While there had been some early work on linear codes defined over the rings $\mathbb{Z}/k\mathbb{Z}$, a major breakthrough came in 1994 with the paper [13]. (There was similar, independent work in [25].) It had been noticed that there were two families of nonlinear binary codes that behaved as if they were duals; their weight enumerators satisfied the MacWilliams identities. This phenomenon was explained in [13]. The authors discovered two families of linear codes over $\mathbb{Z}/4\mathbb{Z}$ that are duals of each other and, therefore, their weight enumerators satisfy the MacWilliams identities. In addition, by using a so-called *Gray map* $g : \mathbb{Z}/4\mathbb{Z} \to \mathbb{F}_2^2$ defined by $g(0) = 00$, $g(1) = 01$, $g(2) = 11$, and $g(3) = 10$ (g is not a homomorphism), the authors showed that the two families of linear codes over $\mathbb{Z}/4\mathbb{Z}$ are mapped to the original families of nonlinear codes over $\mathbb{F}_2$. The paper [13] launched an interest in linear codes defined over rings that continues to this day.

Definition 21. Let R be a finite ring. A left (right) *linear code* C of length n over R is a left (right) R-submodule $C \subset R^n$.

It will be useful in Section 5 to be even more general and to define linear codes over modules. These ideas were introduced first by Nechaev and his colloborators [18].

Definition 22. Let R be a finite ring, and let A (for *alphabet*) be a finite left R-module. A left *linear code* C over A of length n is a left R-submodule $C \subset A^n$.

The Hamming weight is defined in the same way as for fields. For $x = (x_1, \ldots, x_n) \in R^n$ (or A^n), define $\mathrm{wt}(x) = |\{i : x_i \neq 0\}|$, the number of nonzero entries in the vector x.

4. The MacWilliams Identities

In this section, we present a proof of the MacWilliams identities that is valid over any finite Frobenius ring. The proof, which dates to [31, Theorem 8.3], is essentially the same as one due to Gleason found in [3, §1.12]. While the MacWilliams identities hold in even more general settings (see the later sections in [33], for example), the setting of linear codes over a finite Frobenius ring will show clearly the role of characters in the proof.

Let R be a finite ring. As we did earlier for fields, we define a *dot product* on R^n by

$$x \cdot y = \sum_{i=1}^{n} x_i y_i, \quad x = (x_1, \ldots, x_n), \quad y = (y_1, \ldots, y_n) \in R^n.$$

For a left linear code $C \subset R^n$, define the *right annihilator* $r(C)$ by $r(C) = \{y \in R^n : x \cdot y = 0, x \in C\}$. The right annihilator will play the role of the dual code $C^\perp$. (Because R may be non-commutative, one must choose between a left and a right annihilator.) The Hamming weight enumerator $W_C(X, Y)$ of a left linear code C is defined exactly as for fields.

Theorem 23 (MacWilliams Identities)**.** *Let R be a finite Frobenius ring, and let $C \subset R^n$ be a left linear code. Then*

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

4.1. **Fourier Transform.** Gleason's proof of the MacWilliams identities uses the Fourier transform and the Poisson summation formula, which we describe in this subsection. Let $(G, +)$ be a finite abelian group.

Throughout this section, we will use the multiplicative form of characters; that is, characters are group homomorphisms $\pi : (G, +) \to (\mathbb{C}^\times, \cdot)$ from a finite abelian group to the multiplicative group of nonzero complex numbers. The set $\widehat{G}$ of all characters of G forms an abelian group under pointwise multiplication. The following list of properties of characters is well-known and presented without proof (see [26] or [28]).

Lemma 24. *Characters of a finite abelian group G satisfy the following properties.*

(1) $|\widehat{G}| = |G|$;
(2) $(G_1 \times G_2)\widehat{\ } \cong \widehat{G}_1 \times \widehat{G}_2$;
(3) $\sum_{x \in G} \pi(x) = \begin{cases} |G|, & \pi = 1, \\ 0, & \pi \neq 1; \end{cases}$
(4) $\sum_{\pi \in \widehat{G}} \pi(x) = \begin{cases} |G|, & x = 0, \\ 0, & x \neq 0; \end{cases}$
(5) *The characters form a linearly independent subset of the vector space of complex-valued functions on G. (In fact, the characters form a basis.)* □

Let V be a vector space over the complex numbers. For any function $f : G \to V$, define its *Fourier transform* $\hat{f} : \widehat{G} \to V$ by

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

Given a subgroup $H \subset G$, define the *annihilator* $(\widehat{G} : H) = \{\pi \in \widehat{G} : \pi(H) = 1\}$. As we saw in (2.5), $|(\widehat{G} : H)| = |G|/|H|$.

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. The proof is an exercise.

Proposition 25 (Poisson Summation Formula)**.** *Let $H \subset G$ be a subgroup, and let $f : G \to V$ be any function from G to a complex vector space V. Then*

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

The next technical result describes the Fourier transform of a function that is the product of functions of one variable. Again, the proof is an exercise for the reader.

Lemma 26. *Suppose V is a commutative algebra over the complex numbers, and suppose $f_i : G \to V$, $i = 1, \ldots, n$, are functions from G to V. Let $f : G^n \to V$ be defined by $f(x_1, \ldots, x_n) = \prod_{i=1}^n f_i(x_i)$. Then*

$$\hat{f}(\pi_1, \ldots, \pi_n) = \prod_{i=1}^n \hat{f}_i(\pi_i).$$

4.2. **Gleason's Proof.**

Proof of Theorem 23. Given a left linear code $C \subset R^n$, we apply the Poisson summation formula with $G = R^n$, $H = C$, and $V = \mathbb{C}[X, Y]$, the polynomial ring over $\mathbb{C}$ in two indeterminates. Define $f_i : R \to \mathbb{C}[X, Y]$ by $f_i(x_i) = X^{1-\mathrm{wt}(x_i)}Y^{\mathrm{wt}(x_i)}$, $x_i \in R$, where $\mathrm{wt}(r) = 0$ for $r = 0$, and $\mathrm{wt}(r) = 1$ for $r \neq 0$ in R. Let $f : R^n \to \mathbb{C}[X, Y]$ be the product of the f_i; i.e.,

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

where $x = (x_1, \ldots, x_n) \in R^n$. We recognize that $\sum_{x \in H} f(x)$, the left side of the Poisson summation formula, is simply the Hamming weight enumerator $W_C(X, Y)$.

To begin to simplify the right side of the Poisson summation formula, we must calculate $\hat{f}$. By Lemma 26, we first calculate $\hat{f}_i$.

$$\begin{aligned}\hat{f}_i(\pi_i) &= \sum_{a \in R} \pi_i(a) f_i(a) = \sum_{a \in R} \pi_i(a) X^{1-\mathrm{wt}(a)}Y^{\mathrm{wt}(a)} = X + \sum_{a \neq 0} \pi_i(a) Y \\ &= \begin{cases} X + (|R| - 1)Y, & \pi_i = 1, \\ X - Y, & \pi_i \neq 1. \end{cases}\end{aligned}$$

At the end of the first line, one evaluates the case $a = 0$ versus the cases where $a \neq 0$. In going to the second line, one uses Lemma 24. Using Lemma 26, we see that

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

where $\pi = (\pi_1, \ldots, \pi_n) \in \widehat{R}^n$ and $\mathrm{wt}(\pi)$ counts the number of π_i such that $\pi_i \neq 1$.

The last task is to identify the character-theoretic annihilator $(\widehat{G} : H) = (\widehat{R}^n : C)$ with $r(C)$, which is where R being Frobenius enters the picture. Let ρ be a generating character of R. We use ρ to define a homomorphism $\beta : R \to \widehat{R}$. For $r \in R$, the character $\beta(r) \in \widehat{R}$ has the form $\beta(r)(s) = (r\rho)(s) = \rho(sr)$ for $s \in R$. One can verify that $\beta : R \to \widehat{R}$ is an isomorphism of left R-modules. In particular, $\mathrm{wt}(r) = \mathrm{wt}(\beta(r))$.

Extend β to an isomorphism $\beta : R^n \to \widehat{R}^n$ of left R-modules, via $\beta(x)(y) = \rho(y \cdot x)$, for $x, y \in R^n$. Again, $\mathrm{wt}(x) = \mathrm{wt}(\beta(x))$. For $x \in R^n$, when is $\beta(x) \in (\widehat{R}^n : C)$? This occurs when $\beta(x)(C) = 1$; that is, when $\rho(C \cdot x) = 1$. This means that the left ideal $C \cdot x$ of R is contained in $\ker \rho$. Because ρ is a generating character, Proposition 7 implies that $C \cdot x = 0$. Thus $x \in r(C)$. The converse is obvious. Thus $r(C)$ corresponds to $(\widehat{R}^n : C)$ under the isomorphism β.

The right side of the Poisson summation formula now simplifies as follows:

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

as desired. □

5. The Extension Problem

In this section, we will discuss the extension problem, which originated from understanding equivalence of codes. The main result is that a finite ring has the extension property for linear codes with respect to the Hamming weight if and only if the ring is Frobenius.

5.1. **Equivalence of Codes.** When should two linear codes be considered to be the same? That is, what should it mean for two linear codes to be equivalent? There are two (related) approaches to this question: via monomial transformations and via weight-preserving isomorphisms.

Definition 27. Let R be a finite ring. A (left) *monomial transformation* $T : R^n \to R^n$ is a left R-linear homomorphism of the form

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

for some permutation σ of $\{1, 2, \ldots, n\}$ and units $u_1, \ldots, u_n$ of R.

Two left linear codes $C_1, C_2 \subset R^n$ are *equivalent* if there exists a monomial transformation $T : R^n \to R^n$ such that $T(C_1) = C_2$.

Another possible definition of equivalence of linear codes $C_1, C_2 \subset R^n$ is this: there exists an R-linear isomorphism $f : C_1 \to C_2$ that preserves the Hamming weight, i.e., $\mathrm{wt}(f(x)) = \mathrm{wt}(x)$, for all $x \in C_1$. The next lemma shows that equivalence using monomial transformations implies equivalence using a Hamming weight-preserving isomorphism.

Lemma 28. *If $T : R^n \to R^n$ is a monomial transformation, then T preserves the Hamming weight: $\mathrm{wt}(T(x)) = \mathrm{wt}(x)$, for all $x \in R^n$. If linear codes $C_1, C_2 \subset R^n$ are equivalent via a monomial transformation T, then the restriction f of T to C_1 is an R-linear isomorphism $C_1 \to C_2$ that preserves the Hamming weight.*

Proof. For any $r \in R$ and any unit $u \in R$, $r = 0$ if and only if $ru = 0$. The result follows easily from this. □

Does the converse hold? This is an extension problem: given $C_1, C_2 \subset R^n$ and an R-linear isomorphism $f : C_1 \to C_2$ that preserves the Hamming weight, does f extend to a monomial transformation $T : R^n \to R^n$? We will phrase this in terms of a property.

Definition 29. Let R be a finite ring. The ring R has the *extension property* (EP) with respect to the Hamming weight if, whenever two left linear codes $C_1, C_2 \subset R^n$ admit an R-linear isomorphism $f : C_1 \to C_2$ that preserves the Hamming weight, it follows that f extends to a monomial transformation $T : R^n \to R^n$.

Thus, the two notions of equivalence coincide precisely when the ring R satisfies the extension property. Another important theorem of MacWilliams is that finite fields have the extension property [21], [22].

Theorem 30 (MacWilliams)**.** *Finite fields have the extension property with respect to the Hamming weight.*

Other proofs that finite fields have the extension property with respect to the Hamming weight have been given by Bogart, Goldberg, and Gordon [5] and by Ward and Wood [29]. We will not prove the finite field case separately, because it is a special case of the main theorem of this section:

Theorem 31. *Let R be a finite ring. Then R has the extension property with respect to the Hamming weight if and only if R is Frobenius.*

One direction, that finite Frobenius rings have the extension property, first appeared in [31, Theorem 6.3]. The proof (which will be given in subsection 5.2) is based on the linear independence of characters and is modeled on the proof in [29] of the finite field case. A combinatorial proof appears in work of Greferath and Schmidt [12]. More generally yet, Greferath, Nechaev, and Wisbauer have shown that the character module of any finite ring has the extension property for the homogeneous and the Hamming weights [11]. Ideas from this latter paper greatly influenced the work presented in subsection 5.4.

The other direction, that only finite Frobenius rings have the extension property, first appeared in [32]. That paper carried out a strategy due to Dinh and López-Permouth [8]. Additional relevant material appeared in [33].

The rest of this section will be devoted to the proof of Theorem 31.

5.2. **Frobenius is Sufficient.** In this subsection we prove half of Theorem 31, that a finite Frobenius ring has the extension property, following the treatment in [31, Theorem 6.3].

Assume $C_1, C_2 \subset R^n$ are two left linear codes, and assume $f : C_1 \to C_2$ is an R-linear isomorphism that preserves the Hamming weight. We want to show that f extends to a monomial transformation of R^n. The core idea is to express the weight-preservation property of f as an equation of characters of C_1 and to use the linear independence of characters to match up terms.

Let $\mathrm{pr}_1, \ldots, \mathrm{pr}_n : R^n \to R$ be the coordinate projections, so that $\mathrm{pr}_i(x_1, \ldots, x_n) = x_i$, $(x_1, \ldots, x_n) \in R^n$. Let $\lambda_1, \ldots, \lambda_n$ denote the restrictions of $\mathrm{pr}_1, \ldots, \mathrm{pr}_n$ to $C_1 \subset R^n$. Similarly, let $\mu_1, \ldots, \mu_n : C_1 \to R$ be given by $\mu_i = \mathrm{pr}_i \circ f$. Then $\lambda_1, \ldots, \lambda_n, \mu_1, \ldots, \mu_n \in \mathrm{Hom}_R(C_1, R)$ are left R-linear functionals on C_1. It will suffice to prove the existence of a permutation σ of $\{1, \ldots, n\}$ and units $u_1, \ldots, u_n$ of R such that $\mu_i = \lambda_{\sigma(i)} u_i$, for $i = 1, \ldots, n$.

For any $x \in C_1$, the Hamming weight of x is given by $\mathrm{wt}(x) = \sum_{i=1}^n \mathrm{wt}(\lambda_i(x))$, while the Hamming weight of $f(x)$ is given by $\mathrm{wt}(f(x)) = \sum_{i=1}^n \mathrm{wt}(\mu_i(x))$. Because f preserves the Hamming weight, we have

$$\sum_{i=1}^{n} \mathrm{wt}(\lambda_i(x)) = \sum_{i=1}^{n} \mathrm{wt}(\mu_i(x)). \tag{5.1}$$

Using Lemma 24, observe that $1 - \mathrm{wt}(r) = (1/|R|) \sum_{\pi \in \widehat{R}} \pi(r)$, for any $r \in R$. Apply this observation to (5.1) and simplify:

$$\sum_{i=1}^{n} \sum_{\pi \in \widehat{R}} \pi(\lambda_i(x)) = \sum_{i=1}^{n} \sum_{\pi \in \widehat{R}} \pi(\mu_i(x)), \quad x \in C_1. \tag{5.2}$$

Because R is assumed to be Frobenius, R admits a (left) generating character ρ. Every character $\pi \in \widehat{R}$ thus has the form $\pi = a\rho$, for some $a \in R$. Recall that the scalar multiplication means that $\pi(r) = (a\rho)(r) = \rho(ra)$, for $r \in R$. Use this to simplify (5.2) (and use different indices on each side of the resulting equation):

$$\sum_{i=1}^{n} \sum_{a \in R} \rho \circ (\lambda_i a) = \sum_{j=1}^{n} \sum_{b \in R} \rho \circ (\mu_j b). \tag{5.3}$$

This is an equation of characters of C_1. Because characters are linearly independent, we can match up terms from the left and right sides of (5.3). In order to get unit multiples, some care must be taken.

Because C_1 is a left R-module, $\mathrm{Hom}_R(C_1, R)$ is a right R-module. Define a preorder $\preceq$ on $\mathrm{Hom}_R(C_1, R)$ by $\lambda \preceq \mu$ if $\lambda = \mu r$ for some $r \in R$. By a result of Bass [4, Lemma 6.4], $\lambda \preceq \mu$ and $\mu \preceq \lambda$ imply $\mu = \lambda u$ for some unit u of R.

Among the linear functionals $\lambda_1, \ldots, \lambda_n, \mu_1, \ldots, \mu_n$ (a finite list), choose one that is maximal in the preorder $\preceq$. Without loss of generality, assume μ_1 is maximal in $\preceq$. (This means: if $\mu_1 \preceq \lambda$ for some λ, then $\mu_1 = \lambda u$ for some unit u of R.) In (5.3), consider the term on the right side with $j = 1$ and $b = 1$. By linear independence of characters, there exists i_1, $1 \leq i_1 \leq n$, and $a \in R$ such that $\rho \circ (\lambda_{i_1} a) = \rho \circ \mu_1$. This equation implies that $\mathrm{im}(\mu_1 - \lambda_{i_1} a) \subset \ker \rho$. But $\mathrm{im}(\mu_1 - \lambda_{i_1} a)$ is a left ideal of R, and ρ is a generating character of R. By Proposition 7, $\mathrm{im}(\mu_1 - \lambda_{i_1} a) = 0$, so that $\mu_1 = \lambda_{i_1} a$. This means that $\mu_1 \preceq \lambda_{i_1}$. Because μ_1 was chosen to be maximal, we have $\mu_1 = \lambda_{i_1} u_1$, for some unit u_1 of R. Begin to define a permutation σ by $\sigma(1) = i_1$.

By a reindexing argument, all the terms on the left side of (5.3) with $i = i_1$ match the terms on the right side of (5.3) with $j = 1$. That is, $\sum_{a \in R} \rho \circ (\lambda_{i_1} a) = \sum_{b \in R} \rho \circ (\mu_1 b)$. Subtract these sums from (5.3), thereby reducing the size of the outer summations by one. Proceed by induction, building a permutation σ and finding units $u_1, \ldots, u_n$ of R, as desired.

5.3. **Reformulating the Problem.** The proof that being a finite Frobenius ring is sufficient for having the extension property with respect to the Hamming weight was based on the proof of the extension theorem over finite fields that used the linear independence of characters [29]. In contrast, the proof that Frobenius is necessary will make use of the approach for proving the extension theorem due to Bogart, et al. [5]. This requires a reformulation of the extension problem.

Every left linear code $C \subset R^n$ can be viewed as the image of the inclusion map $C \to R^n$. More generally, every left linear code is the image of an R-linear homomorphism $\Lambda : M \to R^n$, for some finite left R-module M. By composing with the coordinate projections pr_i, the homomorphism Λ can be expressed as an n-tuple $\Lambda = (\lambda_1, \ldots, \lambda_n)$, where each $\lambda_i \in \mathrm{Hom}_R(M, R)$. The λ_i will be called the *coordinate functionals* of the linear code.

Remark 32. It is typical in coding theory to present a linear code $C \subset R^n$ by means of a *generator matrix* G. The matrix G has entries from R, the number of columns of G equals the length n of the code C, and (most importantly) the rows of G generate C as a left submodule of R^n.

The description of a linear code via coordinate functionals is essentially equivalent to that using generator matrices. If one has coordinate functionals $\lambda_1, \ldots, \lambda_n$, then one can produce a generator matrix G by choosing a set $v_1, \ldots, v_k$ of generators for C as a left module over R and taking as the (i,j)-entry of G the value $\lambda_j(v_i)$. Conversely, given a generator matrix, its columns define coordinate functionals. Thus, using coordinate functionals is a "basis-free" approach to generator matrices. This idea goes back to [2].

We are interested in linear codes up to equivalence. For a linear code given by $\Lambda = (\lambda_1, \ldots, \lambda_n) : M \to R^n$, the order of the coordinate functionals $\lambda_1, \ldots, \lambda_n$ is irrelevant, as is replacing any λ_i with $\lambda_i u_i$, for some unit u_i of R. We want to encode this information systematically. Let $\mathcal{U}$ be the group of units of the ring R. The group $\mathcal{U}$ acts on the module $\mathrm{Hom}_R(M,R)$ by right scalar multiplication; let $\mathcal{O}^\sharp$ denote the set of orbits of this action: $\mathcal{O}^\sharp = \mathrm{Hom}_R(M,R)/\mathcal{U}$. Then a linear code $M \to R^n$, up to equivalence, is specified by choosing n elements of $\mathcal{O}^\sharp$ (counting with multiplicities). This choice can be encoded by specifying a function (a *multiplicity function*) $\eta : \mathcal{O}^\sharp \to \mathbb{N}$, the nonnegative integers, where $\eta(\lambda)$ is the number of times λ (or a unit multiple of λ) appears as a coordinate functional. The length n of the linear code is given by $\sum_{\lambda \in \mathcal{O}^\sharp} \eta(\lambda)$.

In summary, linear codes $M \to R^n$ (for fixed M, but any n), up to equivalence, are given by multiplicity functions $\eta : \mathcal{O}^\sharp \to \mathbb{N}$. Denote the set of all such functions by $F(\mathcal{O}^\sharp, \mathbb{N}) = \{\eta : \mathcal{O}^\sharp \to \mathbb{N}\}$, and define $F_0(\mathcal{O}^\sharp, \mathbb{N}) = \{\eta \in F(\mathcal{O}^\sharp, \mathbb{N}) : \eta(0) = 0\}$.

We are also interested in the Hamming weight of codewords and in how to describe the Hamming weight in terms of the multiplicity function η. Fix a multiplicity function $\eta : \mathcal{O}^\sharp \to \mathbb{N}$. Define $W_\eta : M \to \mathbb{N}$ by

$$W_\eta(x) = \sum_{\lambda \in \mathcal{O}^\sharp} \mathrm{wt}(\lambda(x))\, \eta(\lambda), \quad x \in M. \tag{5.4}$$

Then $W_\eta(x)$ equals the Hamming weight of the codeword given by $x \in M$. Notice that $W_\eta(0) = 0$.

Lemma 33. *For $x \in M$ and unit $u \in \mathcal{U}$, $W_\eta(ux) = W_\eta(x)$.*

Proof. This follows immediately from the fact that $\mathrm{wt}(ur) = \mathrm{wt}(r)$ for $r \in R$ and unit $u \in \mathcal{U}$; that is, $ur = 0$ if and only if $r = 0$. □

Because M is a left R-module, the group of units $\mathcal{U}$ acts on M on the left. Let $\mathcal{O}$ denote the set of orbits of this action. Observe that Lemma 33 implies that W_η is a well-defined function from $\mathcal{O}$ to $\mathbb{N}$. Let $F(\mathcal{O}, \mathbb{N})$ denote the set of all functions from $\mathcal{O}$ to $\mathbb{N}$, and define $F_0(\mathcal{O}, \mathbb{N}) = \{w \in F(\mathcal{O}, \mathbb{N}) : w(0) = 0\}$. Now define $W : F(\mathcal{O}^\sharp, \mathbb{N}) \to F_0(\mathcal{O}, \mathbb{N})$ by $\eta \in F(\mathcal{O}^\sharp, \mathbb{N}) \mapsto W_\eta \in F_0(\mathcal{O}, \mathbb{N})$. (Remember that $W_\eta(0) = 0$.) Thus W associates to every linear code, up to equivalence, a listing of the Hamming weights of all the codewords. The discussion to this point (plus a technical argument on the role of the zero functional, which is relegated to subsection 5.5) proves the following reformulation of the extension property.

Theorem 34. *A finite ring R has the extension property with respect to the Hamming weight if and only if the function*

$$W : F_0(\mathcal{O}^\sharp, \mathbb{N}) \to F_0(\mathcal{O}, \mathbb{N}), \quad \eta \mapsto W_\eta,$$

is injective for every finite left R-module M.

Observe that the function spaces $F_0(\mathcal{O}^\sharp, \mathbb{N}), F_0(\mathcal{O}, \mathbb{N})$ are additive monoids and that $W : F_0(\mathcal{O}^\sharp, \mathbb{N}) \to F_0(\mathcal{O}, \mathbb{N})$ is additive, i.e., a monoid homomorphism. If we tensor with the rational numbers $\mathbb{Q}$ (which means we formally allow coordinate functionals to have multiplicities equal to any rational number), it is straight-forward to generalize Theorem 34 to:

Theorem 35. *A finite ring R has the extension property with respect to the Hamming weight if and only if the $\mathbb{Q}$-linear homomorphism*

$$W : F_0(\mathcal{O}^\sharp, \mathbb{Q}) \to F_0(\mathcal{O}, \mathbb{Q}), \quad \eta \mapsto W_\eta,$$

is injective for every finite left R-module M.

Theorem 35 is very convenient because the function spaces $F_0(\mathcal{O}^\sharp, \mathbb{Q}), F_0(\mathcal{O}, \mathbb{Q})$ are $\mathbb{Q}$-vector spaces, and we can use the tools of linear algebra over fields to analyze the linear homomorphism W. In fact, in [5], Bogart et al. prove the extension theorem over finite fields by showing that the matrix representing W is invertible. The form of that matrix is apparent from (5.4). Greferath generalized that approach in [10].

For use in the next subsection, we will need a version of Theorem 35 for linear codes defined over an alphabet A. Let A be a finite left R-module, with automorphism group $\mathrm{Aut}(A)$. A left R-linear code in A^n is given by the image of an R-linear homomorphism $M \to A^n$, for some finite left R-module M. In this case, the coordinate functionals will belong to $\mathrm{Hom}_R(M, A)$. The group $\mathrm{Aut}(A)$ acts on $\mathrm{Hom}_R(M, A)$ on the right; let $\mathcal{O}^\sharp$ denote the set of orbits of this action. A linear code over A, up to equivalence, is again specified by a multiplicity function $\eta \in F(\mathcal{O}^\sharp, \mathbb{N})$.

Just as before, the group of units $\mathcal{U}$ of R acts on the module M on the left, with set $\mathcal{O}$ of orbits. In the same way as above, we formulate the extension property for the alphabet A as:

Theorem 36. *Let A be a finite left R-module. Then A has the extension property with respect to the Hamming weight if and only if the linear homomorphism*

$$W : F_0(\mathcal{O}^\sharp, \mathbb{Q}) \to F_0(\mathcal{O}, \mathbb{Q}), \quad \eta \mapsto W_\eta,$$

is injective for every finite left R-module M.

5.4. **Frobenius is Necessary.** In this subsection we follow a strategy of Dinh and López-Permouth [8] and use Theorem 35 to prove the other direction of Theorem 31; viz., if a finite ring has the extension property with respect to the Hamming weight, then the ring must be Frobenius.

The strategy of Dinh and López-Permouth [8] can be summarized as follows.

(1) If a finite ring R is not Frobenius, then its left socle contains a left R-module of the form $M_{m\times k}(\mathbb{F}_q)$ with $m < k$, for some q (cf., (2.1) and (2.3)).
(2) Use the matrix module $M_{m\times k}(\mathbb{F}_q)$ as the alphabet A. If $m < k$, show that A does not have the extension property.
(3) Take the counter-examples over A to the extension property, consider them as R-modules, and show that they are also counter-examples to the extension property over R.

The first and last points were already proved in [8]. Here's one way to see the first point. We know from (2.3) that $\mathrm{soc}({}_R R)$ is a sum of matrix modules $M_{m_i \times s_i}(\mathbb{F}_{q_i})$. If $m_i \geq s_i$ for all i, then each of the $M_{m_i \times s_i}(\mathbb{F}_{q_i})$ would admit a generating character, by Theorem 13. By adding these generating characters, one would obtain a generating character for $\mathrm{soc}({}_R R)$ itself. Then, by Proposition 14, R would admit a generating character, and hence would be Frobenius by Theorem 5.

For the third point, consider counter-examples $C_1, C_2 \subset A^n$ to the extension property for the alphabet A with respect to the Hamming weight. Because $A^n \subset \mathrm{soc}({}_R R)^n \subset {}_R R^n$, C_1, C_2 can also be viewed as R-modules via (2.1). The Hamming weight of an element x of A^n equals the Hamming weight of x considered as an element of R^n, because the Hamming weight just depends upon the entries of x being zero or not. In this way, C_1, C_2 will also be counter-examples to the extension property for the alphabet R with respect to the Hamming weight.

Thus, the key step remaining is the second point in the strategy. An explicit construction of counter-examples to the extension property for the alphabet $A = M_{m \times k}(\mathbb{F}_q)$, $m < k$, was given in [32]. Here, we give a short existence proof; more details are available in [32] and [33].

Let $R = M_m(\mathbb{F}_q)$ be the ring of $m \times m$ matrices over $\mathbb{F}_q$. Let $A = M_{m \times k}(\mathbb{F}_q)$, with $m < k$; A is a left R-module. It is clear from Theorem 36 that A will fail to have the extension property with respect to the Hamming weight if we can find a finite left R-module M with $\dim_{\mathbb{Q}} F_0(\mathcal{O}^\sharp, \mathbb{Q}) > \dim_{\mathbb{Q}} F_0(\mathcal{O}, \mathbb{Q})$. It turns out that this inequality will hold for any nonzero M.

Because R is simple, any finite left R-module M has the form $M = M_{m \times \ell}(\mathbb{F}_q)$, for some ℓ. First, let us determine $\mathcal{O}$, which is the set of left $\mathcal{U}$-orbits on M. The group $\mathcal{U}$ is the group of units of R, which is precisely the general linear group $GL_m(\mathbb{F}_q)$. The left orbits of $GL_m(\mathbb{F}_q)$ on $M = M_{m \times \ell}(\mathbb{F}_q)$ are represented by the row reduced echelon matrices[1] over $\mathbb{F}_q$ of size $m \times \ell$.

Now, let us determine $\mathcal{O}^\sharp$, which is the set of right $\mathrm{Aut}(A)$-orbits on $\mathrm{Hom}_R(M, A)$. The automorphism group $\mathrm{Aut}(A)$ equals $GL_k(\mathbb{F}_q)$, acting on $A = M_{m \times k}(\mathbb{F}_q)$ by right matrix multiplication. On the other hand, $\mathrm{Hom}_R(M, A) = M_{\ell \times k}(\mathbb{F}_q)$, again using right matrix multiplication. Thus $\mathcal{O}^\sharp$ consists of the right orbits of $GL_k(\mathbb{F}_q)$ acting on $M_{\ell \times k}(\mathbb{F}_q)$. These orbits are represented by the column reduced echelon matrices over $\mathbb{F}_q$ of size $\ell \times k$.

Because the matrix transpose interchanges row reduced echelon matrices and column reduced echelon matrices, we see that $|\mathcal{O}^\sharp| > |\mathcal{O}|$ if and only if $k > m$ (for any positive ℓ). Finally, notice that $\dim_{\mathbb{Q}} F_0(\mathcal{O}^\sharp, \mathbb{Q}) = |\mathcal{O}^\sharp| - 1$ and $\dim_{\mathbb{Q}} F_0(\mathcal{O}, \mathbb{Q}) = |\mathcal{O}| - 1$. Thus, for any nonzero module M, $\dim_{\mathbb{Q}} F_0(\mathcal{O}^\sharp, \mathbb{Q}) > \dim_{\mathbb{Q}} F_0(\mathcal{O}, \mathbb{Q})$ if and only if $m < k$. Consequently, if $m < k$, then W fails to be injective and A fails to have the extension property with respect to Hamming weight.

5.5. **Technical Remarks.** Here is the technical argument regarding the zero functional needed to justify Theorem 34.

Remark 37. For $\eta \in F(\mathcal{O}^\sharp, \mathbb{N})$, define the *length* of η to be $l(\eta) = \sum_{\lambda \in \mathcal{O}^\sharp} \eta(\lambda)$ and the *essential length* of η to be $l_0(\eta) = \sum_{\lambda \neq 0} \eta(\lambda)$. The length $l(\eta)$ equals the length of the

[1]Prof. Yamagata tells me that the Japanese name for this concept translates literally as "step matrices."

linear code defined by η; the reduced length $l_0(\eta)$ equals the length of the linear code defined by η after any all-zero positions have been removed. (In terms of a generator matrix, one removes all the zero columns.)

Assume the extension property holds with respect to the Hamming weight. This means that if $\eta, \eta' \in F(\mathcal{O}^\sharp, \mathbb{N})$ satisfy $l(\eta) = l(\eta')$ and $W_\eta = W_{\eta'}$, then $\eta = \eta'$. That is, W is injective along the level sets of the length function l. If $l(\eta') < l(\eta)$ and $W_\eta = W_{\eta'}$, then we can append zeros to η' until its length is the same as $l(\eta)$ without changing $W_{\eta'}$. More precisely, define η'' by $\eta''(\lambda) = \eta'(\lambda)$ for $\lambda \neq 0$ and set $\eta''(0) = \eta'(0) + l(\eta) - l(\eta')$. Then $l(\eta'') = l(\eta)$ and $W_{\eta''} = W_\eta$. Then $\eta'' = \eta$, by the extension property. In particular, the reduced lengths are equal: $l_0(\eta) = l_0(\eta') = l_0(\eta'')$.

There is a projection $\mathrm{pr} : F(\mathcal{O}^\sharp, \mathbb{N}) \to F_0(\mathcal{O}^\sharp, \mathbb{N})$ which sets $(\mathrm{pr}\,\eta)(0) = 0$ and leaves the other values unchanged, $(\mathrm{pr}\,\eta)(\lambda) = \eta(\lambda)$, $\lambda \neq 0$. This projection splits the monoid as $F(\mathcal{O}^\sharp, \mathbb{N}) = F_0(\mathcal{O}^\sharp, \mathbb{N}) \oplus \mathbb{N}$. The argument of the previous paragraph shows that if $W_\eta = W_{\eta'}$, then $\mathrm{pr}\,\eta = \mathrm{pr}\,\eta'$ as elements of $F_0(\mathcal{O}^\sharp, \mathbb{N})$.

Conversely, suppose $W : F_0(\mathcal{O}^\sharp, \mathbb{N}) \to F_0(\mathcal{O}, \mathbb{N})$ is injective. Let $\eta, \eta' \in F(\mathcal{O}^\sharp, \mathbb{N})$ satisfy $l(\eta) = l(\eta')$ and $W_\eta = W_{\eta'}$. Because the value of $\eta(0)$ does not affect W_η, we see that $W_{\mathrm{pr}\,\eta} = W_{\mathrm{pr}\,\eta'}$. By assumption, W is injective on $F_0(\mathcal{O}^\sharp, \mathbb{N})$, so that $\mathrm{pr}\,\eta = \mathrm{pr}\,\eta'$. In particular, $l_0(\eta) = l_0(\eta')$. Since $l(\eta) = l(\eta')$, we must also have $\eta(0) = \eta'(0)$, and thus $\eta = \eta'$.

6. Self-Dual Codes

I want to finish this article by touching on a very active research topic: self-dual codes.

As we saw in subsection 3.3, if $C \subset \mathbb{F}^n$ is a linear code of length n over a finite field $\mathbb{F}$, then its dual code $C^\perp$ is defined by $C^\perp = \{y \in \mathbb{F}^n : x \cdot y = 0, x \in C\}$. A linear code C is *self-orthogonal* if $C \subset C^\perp$ and is *self-dual* if $C = C^\perp$. Because $\dim C^\perp = n - \dim C$, a necessary condition for the existence of a self-dual code C over a finite field is that the length n must be even; then $\dim C = n/2$.

The Hamming weight enumerator of a self-dual code appears on both sides of the MacWilliams identities:

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

where C is self-dual over $\mathbb{F}_q$. As $|C| = q^{n/2}$ and the total degree of the polynomial $W_C(X, Y)$ is n, the MacWilliams identities for a self-dual code can be written in the form

$$W_C(X, Y) = W_C\left(\frac{X + (q-1)Y}{\sqrt{q}}, \frac{X - Y}{\sqrt{q}}\right).$$

Every element x of a self-dual code satisfies $x \cdot x = 0$. In the binary case, $q = 2$, notice that $x \cdot x \equiv \mathrm{wt}(x) \bmod 2$. Thus, every element of a binary self-dual code C has even length. This implies that $W_C(X, -Y) = W_C(X, Y)$.

Restrict to the binary case, $q = 2$. Define two complex 2×2 matrices P, Q by

$$P = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}, \quad Q = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Notice that $P^2 = Q^2 = I$. Let $\mathcal{G}$ be the group generated by P and Q (inside $GL_2(\mathbb{C})$). Define an action of $\mathcal{G}$ on the polynomial ring $\mathbb{C}[X, Y]$ by linear substitution: $(fS)(X, Y) = f((X, Y)S)$ for $S \in \mathcal{G}$. The paragraphs above prove the following

Proposition 38. *Let C be a self-dual binary code. Then its Hamming weight enumerator $W_C(X, Y)$ is invariant under the action of the group $\mathcal{G}$. That is, $W_C(X, Y) \in \mathbb{C}[X, Y]^{\mathcal{G}}$, the ring of $\mathcal{G}$-invariant polynomials.*

Much more is true, in fact. Let $C_2 \subset \mathbb{F}_2^2$ be the linear code $C_2 = \{00, 11\}$. Then C_2 is self-dual, and $W_{C_2}(X, Y) = X^2 + Y^2$. Let $E_8 \subset \mathbb{F}_2^8$ be the linear code generated by the rows of the following binary matrix

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

Then E_8 is also self-dual, with $W_{E_8}(X, Y) = X^8 + 14X^4Y^4 + Y^8$.

Theorem 39 (Gleason (1970))**.** *The ring of $\mathcal{G}$-invariant polynomials is generated as an algebra by W_{C_2} and W_{E_8}. That is,*

$$\mathbb{C}[X, Y]^{\mathcal{G}} = \mathbb{C}[X^2 + Y^2, X^8 + 14X^4Y^4 + Y^8].$$

Gleason proved similar statements in several other contexts (doubly-even self-dual binary codes, self-dual ternary codes, Hermitian self-dual quaternary codes) [9]. The results all have this form: for linear codes of a certain *type* (e.g., binary self-dual), their Hamming weight enumerators are invariant under a certain finite matrix group $\mathcal{G}$, and the ring of $\mathcal{G}$-invariant polynomials is generated as an algebra by the weight enumerators of two explicit linear codes of the given type.

Gleason's Theorem has been generalized greatly by Nebe, Rains, and Sloane [24]. Those authors have a general definition of the *type* of a self-dual linear code defined over an alphabet A, where A is a finite left R-module. Associated to every type is a finite group $\mathcal{G}$, called the Clifford-Weil group, and the (complete) weight enumerator of every self-dual linear code of the given type is $\mathcal{G}$-invariant. Finally, the authors show (under certain hypotheses on the ring R) that the ring of all $\mathcal{G}$-invariant polynomials is spanned by weight enumerators of self-dual codes of the given type.

In order to define self-dual codes over non-commutative rings, Nebe, Rains, and Sloane must cope with the difficulty that the dual code of a left linear code C in A^n is a right linear code of the form $(\widehat{A}^n : C) \subset \widehat{A}^n$ (cf., the proof of Theorem 23 in subsection 4.2). This difficulty can be addressed first by assuming that the ring R admits an anti-isomorphism ε, i.e., an isomorphism $\varepsilon : R \to R$ of the additive group, with $\varepsilon(rs) = \varepsilon(s)\varepsilon(r)$, for $r, s \in R$. Then every left (resp., right) R-module M defines a right (resp., left) R-module $\varepsilon(M)$. The additive group of $\varepsilon(M)$ is the same as that of M, and the right scalar multiplication on $\varepsilon(M)$ is $mr := \varepsilon(r)m$, $m \in M$, $r \in R$, where $\varepsilon(r)m$ uses the left scalar multiplication of M. (And similarly for right modules.)

Secondly, in order to identify the character-theoretic annihilator $(\widehat{A}^n : C) \subset \widehat{A}^n$ with a submodule in A^n, Nebe, Rains, and Sloane assume the existence of an isomorphism

$\psi : \varepsilon(A) \to \widehat{A}$. In this way, $C^\perp := \varepsilon^{-1}\psi^{-1}(\widehat{A}^n : C)$ can be viewed as the dual code of C; $C^\perp$ is a left linear code in A^n if C is. With one additional hypothesis on ψ, $C^\perp$ satisfies all the properties one would want from a dual code, such as $(C^\perp)^\perp = C$ and the MacWilliams identities. (See [34] for an exposition.)

There are several questions that arise immediately from the work of Nebe, Rains, and Sloane that may be of interest to ring theorists.

(1) Which finite rings admit anti-isomorphisms? Involutions?
(2) Assume a finite ring R admits an anti-isomorphism ε. Which finite left R-modules A admit an isomorphism $\psi : \varepsilon(A) \to \widehat{A}$?
(3) Even in the absence of complete answers to the preceding, are there good sources of examples?

There are a few results in [34], but much more is needed. Progress on these questions may prove helpful in understanding the limits and the proper setting for the work of Nebe, Rains, and Sloane.

References

[1] Č. Arf, *Untersuchungen über quadratische Formen in Körpern der Charakteristik* 2. *I.*, J. Reine. Angew. Math. **183** (1941), 148–167. MR 0008069 (4,237f)
[2] E. F. Assmus, Jr. and H. F. Mattson, Jr., *Error-correcting codes: An axiomatic approach*, Inform. and Control **6** (1963), 315–330. MR 0178997 (31 #3251)
[3] ———, *Coding and combinatorics*, SIAM Rev. **16** (1974), 349–388. MR 0359982 (50 #12432)
[4] H. Bass, *K-theory and stable algebra*, Inst. Hautes Études Sci. Publ. Math. **22** (1964), 5–60. MR 0174604 (30 #4805)
[5] K. Bogart, D. Goldberg, and J. Gordon, *An elementary proof of the MacWilliams theorem on equivalence of codes*, Inform. and Control **37** (1978), no. 1, 19–22. MR 0479646 (57 #19067)
[6] H. L. Claasen and R. W. Goldbach, *A field-like property of finite rings*, Indag. Math. (N.S.) **3** (1992), no. 1, 11–26. MR 1157515 (93b:16038)
[7] 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 0144979 (26 #2519)
[8] H. Q. Dinh and S. R. López-Permouth, *On the equivalence of codes over rings and modules*, Finite Fields Appl. **10** (2004), no. 4, 615–625. MR 2094161 (2005g:94098)
[9] A. M. Gleason, *Weight polynomials of self-dual codes and the MacWilliams identities*, Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 3, Gauthier-Villars, Paris, 1971, pp. 211–215. MR 0424391 (54 #12354)
[10] M. Greferath, *Orthogonality matrices for modules over finite Frobenius rings and MacWilliams' equivalence theorem*, Finite Fields Appl. **8** (2002), no. 3, 323–331. MR 1910395 (2003d:94107)
[11] M. Greferath, A. Nechaev, and R. Wisbauer, *Finite quasi-Frobenius modules and linear codes*, J. Algebra Appl. **3** (2004), no. 3, 247–272. MR 2096449 (2005g:94099)
[12] M. Greferath and S. E. Schmidt, *Finite-ring combinatorics and MacWilliams's equivalence theorem*, J. Combin. Theory Ser. A **92** (2000), no. 1, 17–28. MR 1783936 (2001j:94045)
[13] 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 **40** (1994), no. 2, 301–319. MR 1294046 (95k:94030)
[14] Y. Hirano, *On admissible rings*, Indag. Math. (N.S.) **8** (1997), no. 1, 55–59. MR 1617802 (99b:16034)
[15] T. Honold, *Characterization of finite Frobenius rings*, Arch. Math. (Basel) **76** (2001), no. 6, 406–415. MR 1831096 (2002b:16033)

[16] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge, 2003. MR 1996953 (2004k:94077)
[17] M. Klemm, *Eine Invarianzgruppe für die vollständige Gewichtsfunktion selbstdualer Codes*, Arch. Math. (Basel) **53** (1989), no. 4, 332–336. MR 1015996 (91a:94032)
[18] V. L. Kurakin, A. S. Kuzmin, V. T. Markov, A. V. Mikhalev, and A. A. Nechaev, *Linear codes and polylinear recurrences over finite rings and modules (a survey)*, Applied algebra, algebraic algorithms and error-correcting codes (Honolulu, HI, 1999) (M. Fossorier, H. Imai, S. Lin, and A. Poli, eds.), Lecture Notes in Comput. Sci., vol. 1719, Springer, Berlin, 1999, pp. 365–391. MR 1846512 (2002h:94092)
[19] T. Y. Lam, *Lectures on modules and rings*, Graduate Texts in Mathematics, vol. 189, Springer-Verlag, New York, 1999. MR 1653294 (99i:16001)
[20] ———, *A first course in noncommutative rings*, second ed., Graduate Texts in Mathematics, vol. 131, Springer-Verlag, New York, 2001. MR 1838439 (2002c:16001)
[21] F. J. MacWilliams, *Error-correcting codes for multiple-level transmission*, Bell System Tech. J. **40** (1961), 281–308. MR 0141541 (25 #4945)
[22] ———, *Combinatorial properties of elementary abelian groups*, Ph.D. thesis, Radcliffe College, Cambridge, Mass., 1962.
[23] 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 0465509 (57 #5408a)
[24] 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 2209183 (2007d:94066)
[25] A. A. Nechaev, *Kerdock code in cyclic form*, Discrete Mathematics and Applications **1** (1991), no. 4, 365–384.
[26] J.-P. Serre, *Linear representations of finite groups*, Springer-Verlag, New York, 1977, Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42. MR 0450380 (56 #8675)
[27] C. E. Shannon, *A mathematical theory of communication*, Bell System Tech. J. **27** (1948), 379–423, 623–656. MR 0026286 (10,133e)
[28] A. Terras, *Fourier analysis on finite groups and applications*, London Mathematical Society Student Texts, vol. 43, Cambridge University Press, Cambridge, 1999. MR 1695775 (2000d:11003)
[29] H. N. Ward and J. A. Wood, *Characters and the equivalence of codes*, J. Combin. Theory Ser. A **73** (1996), no. 2, 348–352. MR 1370137 (96i:94028)
[30] E. Witt, *Theorie der quadratischen Formen in beliebigen Körpern*, J. Reine. Angew. Math. **176** (1937), 31–44.
[31] J. A. Wood, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math. **121** (1999), no. 3, 555–575. MR 1738408 (2001d:94033)
[32] ———, *Code equivalence characterizes finite Frobenius rings*, Proc. Amer. Math. Soc. **136** (2008), no. 2, 699–706. MR 2358511 (2008j:94062)
[33] ———, *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.
[34] ———, *Anti-isomorphisms, character modules and self-dual codes over non-commutative rings*, Int. J. Information and Coding Theory **1** (2010), no. 4, 429–444, Special Issue on Algebraic and Combinatorial Coding Theory: in Honour of the Retirement of Vera Pless. Series 3.

Department of Mathematics
Western Michigan University
1903 W. Michigan Ave.
Kalamazoo, MI 49008–5248 USA
E-mail address: jay.wood@wmich.edu