A CODING-THEORETIC CHARACTERIZATION OF FINITE FROBENIUS RINGS

JAY A. WOOD

Abstract. In this paper we show that finite rings for which the extension theorem of MacWilliams is valid for Hamming weight must necessarily be Frobenius. This result makes use of a strategy of Dinh and López-Permouth.

1. Introduction

This paper is a sequel to [20]. That paper made the case that finite Frobenius rings are the most appropriate rings for coding theory because two fundamental theorems of MacWilliams, known over finite fields, hold over finite Frobenius rings. One of those fundamental theorems, the MacWilliams identities, is known to hold in the very general setting of additive codes [4]. The other fundamental theorem of MacWilliams, known as either the MacWilliams equivalence theorem or the MacWilliams extension theorem, characterizes the form of code automorphisms for the Hamming weight. In [20, Theorem 6.3], it was shown that the MacWilliams extension theorem holds over finite Frobenius rings. The main result in this paper (Theorem 2.5) is the converse—if the MacWilliams extension theorem holds over a finite ring, then the ring must be Frobenius. This is further evidence that finite Frobenius rings are the most appropriate rings for coding theory.

This paper draws on two recent developments. One is the development of the theory of linear codes defined over modules, i.e., codes with an alphabet that is a module A over some finite ring R. Early work was done by Kurakin et al. [11] with R commutative. More recently, Greferath et al. [8] further developed the theory over any finite ring.

The other development is work by Greferath and Schmidt [9], as well as work by Dinh and López-Permouth [6], on the search for counterexamples to the MacWilliams extension theorem over non-Frobenius

Date: February 28, 2006.

1991 *Mathematics Subject Classification.* Primary 94B05.

Key words and phrases. Finite Frobenius rings, Hamming weight, equivalence theorem, extension theorem, virtual codes.

rings. Greferath and Schmidt [9] found the first example of a quasi-Frobenius, but not Frobenius, ring over which the extension theorem fails. Dinh and López-Permouth [6] made a systematic study of conditions necessary for the extension theorem to hold, and they laid out a strategy to prove the converse of the extension theorem.

This paper pursues the strategy of Dinh and López-Permouth. The basic outline of the strategy has three points. (1) If a finite ring is not Frobenius, show that its socle contains a copy of a particular type of module defined over a matrix ring. (2) Show that counter-examples to the extension theorem exist in the context of linear codes defined over this particular matrix module. (3) Show that the counter-examples over the matrix module pull back to give counter-examples over the original ring. Points (1) and (3) were already carried out in [6]. Point (2) is the main technical contribution of this paper (Theorem 4.2).

The form of the counter-examples in Theorem 4.2 is derived from a detailed analysis of modules over matrix rings. Crucial to this analysis is a formulation of the extension theorem in terms of so-called virtual codes [22]. However, the counter-examples are presented in a form that does not require familiarity with virtual codes.

This paper has two main parts. The first part consists of Sections 2–5. Section 2 reviews definitions and presents the statement of the main result, Theorem 2.5, that a finite ring for which the extension theorem holds is necessarily Frobenius. Sections 3–5 then discuss, in turn, the three points in the strategy of Dinh and López-Permouth outlined above. Readers interested in the counter-examples may proceed directly to Theorem 4.2.

The second part of the paper consists of Sections 6 and 7. Section 6 formulates the extension theorem in terms of virtual codes, so that the extension theorem holds if and only if a particular mapping W is injective (see (6.2)). In Section 7, the mapping W of (6.2) is analyzed in great detail for matrix modules. This analysis, together with some computer calculations, results in the form of the counter-examples in Theorem 4.2. The second part of the paper is not needed in order to understand the first part.

Acknowledgments. The author acknowledges with pleasure his intellectual debt to the work of Dinh and López-Permouth [6] and the work of Greferath et al. [8]. The author also thanks E. S. Moore for unwavering support.

2. Preliminaries and statement of main theorem

Fix a finite ring R with 1. A *left* (resp., *right*) *linear code* of length n over R is a left (resp., right) R-submodule $C \subset R^n$. For the rest of this paper, left linear codes will be used and will be referred to simply as *linear codes*. There is a parallel theory for right linear codes.

Denote the group of units of the ring R by $\mathcal{U}(R)$. A *monomial transformation* of R^n is an R-linear homomorphism $f : R^n \to R^n$ of the form

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

where π is a permutation of $\{1, 2, \ldots, n\}$ and $u_1, \ldots, u_n \in \mathcal{U}(R)$. Two linear codes $C, C' \subset R^n$ are *equivalent* if there exists a monomial transformation $f : R^n \to R^n$ with $f(C) = C'$.

Given $x = (x_1, \ldots, x_n) \in R^n$, the *Hamming weight* $\mathrm{wt}(x)$ equals the number of non-zero components of x. That is,

$$\mathrm{wt}(x) = |\{i : x_i \neq 0\}|.$$

The following proposition and corollary are well-known ([20, Props. 6.1 and 6.2]).

Proposition 2.1. *An R-linear automorphism $f : R^n \to R^n$ preserves Hamming weight* (*i.e.,* $\mathrm{wt}(f(x)) = \mathrm{wt}(x)$*, for all* $x \in R^n$) *if and only if f is a monomial transformation.*

Corollary 2.2. *If $C, C' \subset R^n$ are equivalent codes, then there exists an R-linear isomorphism $f : C \to C'$ that preserves Hamming weight.*

This entire paper is devoted to understanding the converse of Corollary 2.2.

Definition 2.3. A finite ring R has the *extension property* (EP) for Hamming weight if:

For any linear code $C \subset R^n$ and any injective R-linear homomorphism $f : C \to R^n$ preserving Hamming weight (i.e., $\mathrm{wt}(f(x)) = \mathrm{wt}(x)$, for all $x \in C$), it follows that f extends to a monomial transformation $f : R^n \to R^n$.

Thus, the converse of Corollary 2.2 holds precisely when the ring R has EP for Hamming weight. A more general formulation of EP appears in [22, p. 1011]. A ring satisfying EP has also been called a MacWilliams ring [5], [6].

The main result of [20] follows. The definition of a Frobenius ring will be reviewed in Section 3.

Theorem 2.4 ([20], Theorem 6.3)**.** *Every finite Frobenius ring has the extension property for Hamming weight.*

The main result of this paper is the converse of Theorem 2.4. The proof appears in Section 5.

Theorem 2.5. *Every finite ring that has the extension property for Hamming weight is Frobenius.*

Historical Remark 2.6. MacWilliams proved that every finite field has the extension property for Hamming weight [14], [15]. Other proofs of this result can be found in [3] and [18]. As noted above, every finite Frobenius ring has the extension property. The original, character-theoretic proof is in [20], while a combinatorial proof is in [9].

Extension theorems analogous to Theorem 2.4 have been proved for symmetrized weight compositions and general weight functions. Every finite field has the extension property for symmetrized weight compositions [7], and this result generalizes to finite Frobenius rings [19]. The paper [21] presents sufficient conditions on a weight function w in order that a finite Frobenius ring have the extension property for w.

Theorem 2.4 has been generalized to the context of linear codes defined over modules (to be defined in Section 4). Greferath, Nechaev, and Wisbauer show in [8] that every finite ring R has a Frobenius bimodule $\widehat{R}$ (its character bimodule) and that codes over $\widehat{R}$ have the extension property for Hamming weight. When R is a Frobenius ring, $\widehat{R}$ is isomorphic to R as one-sided modules, so that Theorem 2.4 is a special case of the result in [8].

Partial converses to Theorem 2.4, i.e., special cases of Theorem 2.5, are known. Finite commutative rings with EP for Hamming weight are Frobenius [20, Theorem 6.4]. Greferath and Schmidt [9] presented the first example of a quasi-Frobenius, but not Frobenius, ring for which the extension property for Hamming weight fails. Dinh and López-Permouth have proven several special cases of Theorem 2.5. In [5, Theorem 4.5], they show that any finite ring that is a direct sum of local rings or homogeneous semilocal rings and that has EP for Hamming weight must be Frobenius. In [6, Theorem 7], Dinh and López-Permouth show that any finite, basic ring that has EP for Hamming weight must be Frobenius.

In order to prove this last result for basic rings, Dinh and López-Permouth prove another theorem [6, Theorem 6] that reduces the converse of Theorem 2.4 (i.e., the proof of Theorem 2.5) to a non-extension problem for codes defined over certain matrix modules. A detailed examination of this non-extension problem will be presented in Section 4, and the argument of Dinh and López-Permouth provides the basic strategy behind the proof of Theorem 2.5 in Section 5.

3. Finite Frobenius rings

There are many equivalent definitions of Frobenius rings (see, for example, Lam [12], Nakayama's original papers [16], [17], and, in the finite case, Greferath and Schmidt [9], Honold [10], as well as [20]. In this paper, it will be useful to use both Nakayama's original definition and the characterization of finite Frobenius rings due to Honold. Much of the following exposition is taken from [20, Section 1].

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

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

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 ${}_R R$. To summarize, we write, as left R-modules,

$$ {}_R R \cong \oplus \mu_i Re_i. \tag{3.1} $$

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* $\operatorname{Soc}(Re_{i,j})$ 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 (3.1) 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 [17, p. 8] refer to (3.1). An Artinian ring R is *quasi-Frobenius* (QF) if there exists a permutation σ of $\{1, 2, \ldots, n\}$ such that

$$ T(Re_i) \cong \operatorname{Soc}(Re_{\sigma(i)}) \quad \text{and} \quad \operatorname{Soc}(e_i R) \cong T(e_{\sigma(i)} R). \tag{3.2} $$

The ring is *Frobenius* if, in addition, $\mu_{\sigma(i)} = \mu_i$. Note, in particular, that $\operatorname{Soc}(Re_i)$ is irreducible in a QF ring; this is the real content hidden in (3.2).

It follows from (3.2) and $\mu_{\sigma(i)} = \mu_i$ that $R/\operatorname{Rad}(R) \cong \operatorname{Soc}(R)$ both as left R-modules and as right R-modules. The main result of Honold in [10] is that, for finite rings, being Frobenius is equivalent to $R/\operatorname{Rad}(R) \cong \operatorname{Soc}(R)$ either as left R-modules or as right R-modules.

If R is a finite ring, then, as rings

$$R/\operatorname{Rad}(R) \cong M_{\mu_1}(\mathbb{F}_{q_1}) \oplus \cdots \oplus M_{\mu_n}(\mathbb{F}_{q_n}), \tag{3.3}$$

where $M_\mu(\mathbb{F}_q)$ is the ring of all $\mu \times \mu$ matrices over the finite field $\mathbb{F}_q$ of q elements. Indeed, being semisimple, $R/\operatorname{Rad}(R)$ is a direct sum of full matrix rings over division rings by a theorem of Wedderburn. Since R is finite, the division rings must also be finite, hence commutative by another theorem of Wedderburn.

As a left R-module, we then have that

$$_R\left(R/\operatorname{Rad}(R)\right) \cong \mu_1 T_1 \oplus \cdots \oplus \mu_n T_n,$$

where $T_i \cong Re_i/\operatorname{Rad}(R)e_i$ is the pullback to R via (3.3) of the "birth-certificate" left $M_{\mu_i}(\mathbb{F}_{q_i})$-module $M_{\mu_i,1}(\mathbb{F}_{q_i})$ of all $\mu_i \times 1$ matrices over $\mathbb{F}_{q_i}$. The irreducible left R-modules T_i, $i = 1, 2, \ldots, n$, form the complete list of all irreducible left R-modules.

The following theorem is implicit in the exposition following Remark 4 of [6].

Theorem 3.1. *If a finite ring R is not Frobenius, then there exists an i, $1 \leq i \leq n$, and $k > \mu_i$ such that kT_i occurs in the direct sum decomposition of* $\operatorname{Soc}(_RR)$.

Proof. Express $\operatorname{Soc}(_RR)$ as a direct sum of irreducibles:

$$\operatorname{Soc}(_RR) \cong \oplus s_i T_i.$$

Since each $\operatorname{Soc}(Re_i)$ has at least one irreducible component, and there are a total of $\sum \mu_i$ such socles, we must have $\sum s_i \geq \sum \mu_i$.

To prove the contrapositive, we suppose that $s_i \leq \mu_i$ for all $i = 1, 2, \ldots, n$. This first implies that $\sum s_i = \sum \mu_i$, from which it then follows that $s_i = \mu_i$ for ever i. Thus, $\operatorname{Soc}(_RR) \cong {}_R\left(R/\operatorname{Rad}(R)\right)$. By Honold's characterization [10], R is Frobenius. □

4. Codes over modules and counter-examples

Several authors have studied linear codes where the alphabet is a module rather than a ring. Kurakin et al. [11] first introduced such codes for alphabets that are modules over a finite commutative ring. Later, Greferath et al. [8] developed the theory for modules over an arbitrary finite ring. Codes over modules provide exactly the right setting for the strategy of Dinh and López-Permouth that will frame the proof of Theorem 2.5 in Section 5.

Fix a finite ring R and a finite R-module A (for *alphabet*). A *linear code* of length n over the module A is an R-submodule $C \subset A^n$.

In this context, a *monomial transformation* $f : A^n \to A^n$ is an R-linear automorphism of the form

$$f(a_1, \dots, a_n) = (a_{\pi(1)}\psi_1, \dots, a_{\pi(n)}\psi_n), \quad (a_1, \dots, a_n) \in A^n,$$

where π is a permutation of $\{1, 2, \dots, n\}$ and $\psi_1, \dots, \psi_n \in \operatorname{Aut}_R(A)$ are automorphisms of A over R (being written on the right). Note in the case where $A = R$ that $\operatorname{Aut}_R(R) = \mathcal{U}(R)$, acting by right multiplication. Thus, this definition of monomial transformation generalizes the definition given in Section 2.

Two linear codes $C, C' \subset A^n$ are *equivalent* if there exists a monomial transformation $f : A^n \to A^n$ with $f(C) = C'$.

In the context of codes over modules, the *Hamming weight* $\operatorname{wt}(a)$ of an element $a = (a_1, \dots, a_n) \in A^n$ is again the number of nonzero components of a. We record the analog of Corollary 2.2.

Proposition 4.1. *If $C, C' \subset A^n$ are equivalent linear codes, then there exists an R-linear isomorphism $f : C \to C'$ that preserves Hamming weight.*

The main technical result of the paper follows.

Theorem 4.2. *Let $R = M_m(\mathbb{F}_q)$ be the ring of all $m \times m$ matrices over a finite field $\mathbb{F}_q$, and let $A = M_{m,k}(\mathbb{F}_q)$ be the left R-module of all $m \times k$ matrices over $\mathbb{F}_q$.*

If $k > m$, then the converse of Proposition 4.1 fails over A. That is, there exist linear codes $C, C' \subset A^N$, $N = \prod_{i=1}^{k-1}(1+q^i)$, and an R-linear isomorphism $f : C \to C'$ that preserves Hamming weight, yet C and C' are not equivalent because one of the codes has an identically zero component while the other one does not.

Before we begin the proof of Theorem 4.2, we include a brief description of q-binomial coefficients and the Cauchy binomial theorem, which will be used in the proof.

The *q-binomial coefficient* (or *Gaussian coefficient*, *Gaussian number* or *Gaussian polynomial*) is defined as

$$\begin{bmatrix} k \\ l \end{bmatrix}_q = \frac{(1-q^k)(1-q^{k-1})\cdots(1-q^{k-l+1})}{(1-q)(1-q^2)\cdots(1-q^l)}.$$

The following lemmas are well-known (see such sources as [1, Chapter 3] and [13, Chapter 24]). The first counts the number of row echelon matrices over $\mathbb{F}_q$, and the second is the Cauchy binomial theorem.

Lemma 4.3. *The q-binomial coefficient $\left[\begin{smallmatrix} k \\ l \end{smallmatrix}\right]_q$ counts the number of row (or column) echelon matrices of length k over $\mathbb{F}_q$ of rank l (i.e., row echelon matrices of size $l \times k$ of rank l, or column echelon matrices of size $k \times l$ of rank l).*

Lemma 4.4 (Cauchy binomial theorem)**.**

$$\prod_{i=0}^{k-1} \left(1 + xq^i\right) = \sum_{j=0}^{k} \begin{bmatrix} k \\ j \end{bmatrix}_q q^{\binom{j}{2}} x^j.$$

Proof of Theorem 4.2. We will construct two linear codes C_+ and C_- in A^N, $N = \prod_{i=1}^{k-1}(1+q^i)$. The codes will be constructed as the images of two R-linear homomorphisms $g_+, g_- : A \to A^N$.

We begin by describing two vectors v_+, v_- in $M_k(\mathbb{F}_q)^N$, i.e., $v_\pm$ will be N-tuples of $k \times k$ matrices over $\mathbb{F}_q$. The order of the entries in $v_\pm$ will be irrelevant. The entries of v_+ will consist of all (nonzero) column echelon matrices of size $k \times k$ over $\mathbb{F}_q$ of even rank, with the multiplicity of the column echelon matrix being $q^{\binom{r}{2}}$, where r denotes the rank of the matrix. The length L_+ of v_+ is given by

$$L_+ = \sum_{\substack{r=1 \\ r \text{ even}}}^{k} q^{\binom{r}{2}} \begin{bmatrix} k \\ r \end{bmatrix}_q .$$

Similarly, the entries of v_- will consist of all column echelon matrices of odd rank, also with multiplicity $q^{\binom{r}{2}}$. (Note that $\binom{1}{2} = 0$.) The length L_- of v_- is given by

$$L_- = \sum_{\substack{r=1 \\ r \text{ odd}}}^{k} q^{\binom{r}{2}} \begin{bmatrix} k \\ r \end{bmatrix}_q .$$

Two applications of Lemma 4.4 with $x = \pm 1$, remembering to account for the $j = 0$ term, yield

$$L_+ + L_- = -1 + \prod_{i=0}^{k-1}(1 + q^i) \quad \text{and} \quad L_+ - L_- = -1.$$

Since the $i = 0$ term in the product equals 2, we see that

$$L_- = \prod_{i=1}^{k-1}(1 + q^i) = N \quad \text{and} \quad L_+ = L_- - 1.$$

Pad the shorter vector v_+ with a zero matrix in order that $v_\pm$ have the same length $L_- = N$.

Define the R-linear homomorphisms $g_\pm : A \to A^N$ by $g_\pm(X) = Xv_\pm$, $X \in A$, where $Xv_\pm$ denotes entry-wise matrix multiplication. Define two linear codes $C_\pm \subset A^N$ by $C_\pm = g_\pm(A)$.

Claim 1: the Hamming weights of $g_\pm(X)$ are equal; i.e., $\operatorname{wt}(g_+(X)) = \operatorname{wt}(g_-(X))$, for all $X \in A$.

To show this, we consider $\Delta(X) = \operatorname{wt}(g_+(X)) - \operatorname{wt}(g_-(X))$. Observe that

$$\Delta(X) = \sum_{\substack{r=1 \\ r \text{ even}}}^{k} q^{\binom{r}{2}} \sum_{\substack{\lambda \text{ col ech} \\ \text{rank } r}} \delta(X\lambda) - \sum_{\substack{r=1 \\ r \text{ odd}}}^{k} q^{\binom{r}{2}} \sum_{\substack{\lambda \text{ col ech} \\ \text{rank } r}} \delta(X\lambda),$$

where $\delta(Y) = 1$ if Y is nonzero, and $\delta(Y) = 0$ if $Y = 0$. In the inner summations, λ varies over all column echelon matrices of size $k \times k$ over $\mathbb{F}_q$ of rank r. The above expression can be re-written as

$$\Delta(X) = \sum_{r=1}^{k} (-1)^r q^{\binom{r}{2}} \sum_{\substack{\lambda \text{ col ech} \\ \text{rank } r}} \delta(X\lambda).$$

Sub-claim: The value of $\Delta(X)$ depends only on the rank of X.

Suppose X has rank s, $1 \le s \le m$. Then

$$X = P \begin{pmatrix} I_s & 0 \\ 0 & 0 \end{pmatrix} Q,$$

for some $P \in GL(m, \mathbb{F}_q)$ and $Q \in GL(k, \mathbb{F}_q)$. For convenience, we denote the middle factor by I_s', so that $X = PI_s'Q$.

For any $Y \in A$, $P \in GL(m, \mathbb{F}_q)$, and $Q \in GL(k, \mathbb{F}_q)$, observe that $\delta(PY) = \delta(Y)$ and $\delta(YQ) = \delta(Y)$, because P and Q are invertible. Thus, $\Delta(X) = \Delta(I_s'Q)$.

The expression for $\Delta(I_s'Q)$ contains the inner summation

$$\sum_{\substack{\lambda \text{ col ech} \\ \text{rank } r}} \delta(I_s'Q\lambda).$$

Note that as λ varies over the column echelon matrices of a fixed rank r, $Q\lambda$ varies over the column echelon equivalence classes of rank r. Thus, by a re-indexing argument, we have

$$\sum_{\substack{\lambda \text{ col ech} \\ \text{rank } r}} \delta(I_s'Q\lambda) = \sum_{\substack{\lambda' \text{ col ech} \\ \text{rank } r}} \delta(I_s'\lambda'Q') = \sum_{\substack{\lambda' \text{ col ech} \\ \text{rank } r}} \delta(I_s'\lambda').$$

Note that Q' depends on λ, but, being invertible, it does not affect the value of δ. It is now apparent that $\Delta(X) = \Delta(I_s')$, as (sub-)claimed.

To prove the original claim, we still need to show that $\Delta(I_s') = 0$ for all s. To this end, we examine $\delta(I_s'\lambda)$ in detail, where λ is a column echelon matrix of rank r and size $k \times k$. The rows of the product $I'_s\lambda$ consist of the first s rows of λ followed by $k-s$ rows of zeros. The value $\delta(I'_s\lambda) = 0$ when $I'_s\lambda = 0$. This happens when the first s rows of λ are zero. But λ is a column echelon matrix of rank r, so there $\left[\begin{smallmatrix} k-s \\ r \end{smallmatrix}\right]_q$ such column echelon matrices of rank r whose first s rows are zero. Note that this number vanishes when $r > k-s$.

In the summation

$$\sum_{\substack{\lambda \text{ col ech} \\ \text{rank } r}} \delta(I'_s\lambda)$$

there are $\left[\begin{smallmatrix} k \\ r \end{smallmatrix}\right]_q$ terms, $\left[\begin{smallmatrix} k-s \\ r \end{smallmatrix}\right]_q$ of which are zero and the rest equal 1. Thus

$$\Delta(I'_s) = \sum_{r=1}^{k} (-1)^r q^{\binom{r}{2}} \left\{ \begin{bmatrix} k \\ r \end{bmatrix}_q - \begin{bmatrix} k-s \\ r \end{bmatrix}_q \right\}.$$

By two applications of Lemma 4.4, one shows that $\Delta(I'_s) = 0$, for all s, and hence $\Delta(X) = 0$ for all $X \in A$, as claimed. (Note that the hypothesis $k > m$ guarantees that the summation involving $\left[\begin{smallmatrix} k-s \\ r \end{smallmatrix}\right]_q$ is nontrivial. If $k \leq m$, one can show that $\Delta(I'_k) = -1$.)

Claim 2: the mapping $f : C_+ \to C_-$ defined by $g_- = f \circ g_+$ is a well-defined R-linear isomorphism that preserves Hamming weight.

Note that the common value

$$\operatorname{wt}(g_+(X)) = \operatorname{wt}(g_-(X)) = \sum_{\substack{r=1 \\ r \text{ odd}}}^{k} q^{\binom{r}{2}} \sum_{\substack{\lambda \text{ col ech} \\ \text{rank } r}} \delta(X\lambda)$$

is the sum of nonnegative terms. Also, if $X \neq 0$, then not all of the terms $\delta(X\lambda)$ vanish when $\operatorname{rk}(\lambda) = 1$. Thus, for $X \neq 0$, the common value $\operatorname{wt}(g_+(X)) = \operatorname{wt}(g_-(X))$ is positive. In particular, for $X \neq 0$, $g_+(X)$ and $g_-(X)$ are nonzero. Thus, $g_+, g_- : A \to A^N$ are injective R-linear homomorphisms. By defining $f : C_+ \to C_-$ via $g_- = f \circ g_+$, the claim is now apparent.

Claim 3: the linear codes $C_\pm$ are not equivalent.

Because the vector v_+ was padded with a zero matrix in one component, that component of $g_+(X)$ vanishes for every $X \in A$. On the other hand, no component of $g_-(X)$ vanishes for every $X \in A$. Since monomial transformations preserve identically zero components, C_+ and C_- cannot be equivalent. □

5. Proof of main theorem

In this section, we prove Theorem 2.5 by following the ideas of Dinh and López-Permouth [6, Theorem 6] whose aim, in their words, "is to provide a strategy" for reducing the proof of Theorem 2.5 to the non-extension result of Theorem 4.2.

Proof of Theorem 2.5. To prove the contrapositive, we suppose that the finite ring R is not Frobenius. By Theorem 3.1, there is an index i and a multiplicity $k > \mu_i$ so that $kT_i \subset \operatorname{Soc}(R) \subset R$. Recall that T_i is the pullback to R of the "birth-certificate" representation $M_{\mu_i,1}(\mathbb{F}_{q_i})$ of $M_{\mu_i}(\mathbb{F}_{q_i})$, so that kT_i is the pullback to R of the $M_{\mu_i}(\mathbb{F}_{q_i})$-module $A = M_{\mu_i,k}(\mathbb{F}_{q_i})$.

Because $k > \mu_i$, there are non-equivalent linear codes $C_\pm \subset A^N$, as in Theorem 4.2. Note that the non-equivalence of $C_\pm$ is in the context of $M_{\mu_i}(\mathbb{F}_{q_i})$-linear codes over the module $A = M_{\mu_i,k}(\mathbb{F}_{q_i})$. The projection mappings $R \to R/\operatorname{Rad}(R) \to M_{\mu_i}(\mathbb{F}_{q_i})$ allow us to consider $C_\pm$ as R-modules. Since A pulls back to kT_i, we have $C_\pm \subset (kT_i)^N \subset \operatorname{Soc}(R)^N \subset R^N$, as R-modules. Thus $C_\pm$ are linear codes over R.

As in the proof of Theorem 4.2 (claim 3), the fact that C_+ has an identically zero component, while C_- does not, implies that $C_\pm$ cannot be equivalent as linear codes over R. Thus, the extension property for Hamming weight over R fails to hold. □

The next theorem is a sharpening of [6, Theorem 6] as it applies to linear codes defined over modules. The proof is the same as for Theorem 2.5.

Theorem 5.1. *Let R be a finite ring with principal decomposition* (3.1)*, and let A be a left R-module. If there exists an index i and a multiplicity $k > \mu_i$ so that $kT_i \subset \operatorname{Soc}(A) \subset A$, then the extension property fails for linear codes over the module A with Hamming weight.*

6. Virtual codes

The next two sections provide the theoretical background that led to the counter-examples of Theorem 4.2. This section adapts the concept of virtual codes, originally developed in [22] for linear codes over rings, to the more general context of linear codes over modules. In Section 7, virtual codes will be analyzed in the specific context of linear codes over the module $A = M_{m,k}(\mathbb{F}_q)$ so as to explain the form of the counter-examples in Theorem 4.2.

Let R and S be two finite rings with 1, and let $A = {}_RA_S$ (for *alphabet*) be an (R, S)-bimodule. The most common situation will be $S = \operatorname{End}({}_RA)$, the endomorphism ring of a left R-module A. Linear codes over rings use $R = S$ and alphabet $A = {}_RR_R$.

Let $w : A \to \mathbb{Q}$ be a *weight function* on the alphabet A, with the property $w(0) = 0$. Of most interest in the paper will be $w = \mathrm{wt}$, the Hamming weight, where $\mathrm{wt}(a) = 1$ for nonzero $a \in A$, and $\mathrm{wt}(0) = 0$.

Given the weight function w, we define two *symmetry groups* (left and right):

$$\begin{aligned} G_l &= \{u \in \mathcal{U}(R) : w(ua) = w(a), \text{ for all } a \in A\}, \\ G_r &= \{v \in \mathcal{U}(S) : w(av) = w(a), \text{ for all } a \in A\}. \end{aligned}$$

In the special case of $S = \mathrm{End}_R(A)$ and $w = \mathrm{wt}$, Hamming weight, we have $G_l = \mathcal{U}(R)$ and $G_r = \mathrm{Aut}_R(A)$.

As in [22], we will recast the classical definitions of linear codes and equivalence (in a uniform manner both for codes over rings and codes over modules) into the linear functional point of view of [2]. First, some notation will be introduced; then, the recast definitions will be stated; and finally, the recast definitions will be reconciled with the classical definitions.

Let ${}_RM$ be a finite left R-module. The module M will serve as the abstract R-module underlying a linear code. The left symmetry group G_l acts on M on the left. Let $\mathcal{O}$ be the space of nonzero orbits of G_l acting on M. The orbit of a nonzero element $x \in M$ will be denoted $\mathrm{orb}(x)$. The set of all functions $\omega : \mathcal{O} \to \mathbb{Q}$ will be denoted $\mathbb{Q}[\mathcal{O}]$.

Form the set $\mathrm{Hom}_R(M, A)$ of all left R-linear homomorphisms $\lambda : M \to A$. Because A is a bimodule, $\mathrm{Hom}_R(M, A)$ inherits a right S-module structure. In particular, the right symmetry group G_r acts on $\mathrm{Hom}_R(M, A)$ on the right. Let $\mathcal{O}^\sharp$ be the space of nonzero orbits of G_r acting on $\mathrm{Hom}_R(M, A)$. The orbit of a nonzero element $\lambda \in \mathrm{Hom}_R(M, A)$ will be denoted $\mathrm{orb}(\lambda)$. The set of all functions $\eta : \mathcal{O}^\sharp \to \mathbb{N}$ (nonnegative integers) will be denoted $\mathbb{N}[\mathcal{O}^\sharp]$.

Definition 6.1. A (*left*) *R-linear code C* over the bimodule A is a pair $C = (M, \eta)$, where M is a finite left R-module and $\eta \in \mathbb{N}[\mathcal{O}^\sharp]$ is a *multiplicity function*.

If $f : M \to M'$ is an R-linear homomorphism of R-modules, then there is an induced mapping $f_* : \mathbb{N}[\mathcal{O}^\sharp] \to \mathbb{N}[\mathcal{O}^{\sharp\prime}]$.

Definition 6.2. Two linear codes $C = (M, \eta)$, $C' = (M', \eta')$ are *equivalent* if there exists an R-linear isomorphism $f : M \to M'$ such that $f_*(\eta) = \eta'$.

Given a linear code $C = (M, \eta)$, the *length* n of the code is given by

$$n = \sum_{\lambda \in \mathcal{O}^\sharp} \eta(\lambda),$$

and the *weight* $w_\eta(x)$ of an element $x \in M$ is given by

$$w_\eta(x) = \sum_{\lambda \in \mathcal{O}^\sharp} \eta(\lambda) w(\lambda(x)).$$

In the summations, λ varies over representatives of the nonzero G_r-orbits. The reader will observe that the sums are well-defined. The next lemma follows directly from the definition of the left symmetry group G_l.

Lemma 6.3 ([22], Lemma 3.1)**.** *The weight function $w_\eta : M \to \mathbb{Q}$ is constant on G_l-orbits. That is, if x, x' lie in the same G_l-orbit, then $w_\eta(x) = w_\eta(x')$.*

Define a mapping W that associates to every linear code $C = (M, \eta)$ its weight function $w_\eta : \mathcal{O} \to \mathbb{Q}$. That is, $W : \mathbb{N}[\mathcal{O}^\sharp] \to \mathbb{Q}[\mathcal{O}]$ is defined by $W(\eta) = w_\eta$. Observe that $W(k_1\eta_1 + k_2\eta_2) = k_1 W(\eta_1) + k_2 W(\eta_2)$, for $k_1, k_2 \in \mathbb{N}$ and $\eta_1, \eta_2 \in \mathbb{N}[\mathcal{O}^\sharp]$.

Definition 6.4. The (R, S)-bimodule A has the *extension property* for the weight function w on A if the following holds:

For every finite left R-module M, the mapping

$$W : \mathbb{N}[\mathcal{O}^\sharp] \to \mathbb{Q}[\mathcal{O}], \quad \eta \mapsto w_\eta, \tag{6.1}$$

is injective.

Remark 6.5. To reconcile Definitions 6.1 and 6.2 with their classical counterparts, recall the idea of a generator matrix G for a linear code over a finite field. The rows of G represent a vector space basis for the code. A column of G is then the list of values of a linear functional (a coordinate functional) on that basis. Thus the columns of G determine an ordered list of linear functionals defined on the code.

Given two generator matrices G and G', the codes they represent are equivalent if $G' = PGQ$, where P is any invertible matrix and Q is a monomial matrix. The monomial matrix Q allows one to permute the order of the list of coordinate functionals, as well as multiply the individual coordinate functionals by nonzero scalars. The matrix P allows for a change of vector space basis in the code.

Definition 6.1 has the monomial matrix aspect of equivalence built into the definition of a linear code. The multiplicity function η counts the number of coordinate functionals that are scalar multiples of each other. The scalars are restricted to be elements of G_r in order that scalar multiplication not change the weights of codewords. Because Definition 6.1 never specifies an order for the list of coordinate functionals, the whole issue of permutations of the ordered list is avoided.

Definition 6.2 accounts for the change of basis traditionally provided by the matrix P.

The injectivity of the mapping W in (6.1) of Definition 6.4 is a recasting of Definition 2.3. Indeed, suppose $C \subset R^n$ and $f : C \to R^n$ preserves a weight function w. Let $M = C$ as modules, and let $\eta : \mathcal{O}^\sharp \to \mathbb{N}$ count the multiplicities of the coordinate functionals for $C \subset R^n$. Let η' count the multiplicities of the coordinate functionals arising from $f : C \to R^n$. Because f preserves weight, we have $W(\eta) = W(\eta')$. The injectivity of W under Definition 6.4 is then equivalent to having $\eta = \eta'$ as elements of $\mathbb{N}[\mathcal{O}^\sharp]$, i.e., η and η' being monomially equivalent, as in Definition 2.3.

Please observe that $\eta : \mathcal{O}^\sharp \to \mathbb{N}$ has as domain only nonzero orbits. A value for $\eta(0)$ makes sense: it counts the number of zero columns in a generator matrix. But zero columns play only a passing role in the theory, and the statement of Definition 6.4 is cleaner if $\eta(0)$ is not mentioned.

In order to be able to use the powerful tools of linear algebra to study the mapping W of (6.1), we must rectify the fact that $\mathbb{N}[\mathcal{O}^\sharp]$ is not a vector space.

Definition 6.6. A *virtual linear code* is a pair $C = (M, \eta)$, where M is a finite left R-module and $\eta \in \mathbb{Q}[\mathcal{O}^\sharp]$ is a *multiplicity function* from $\mathcal{O}^\sharp$ to the rational numbers $\mathbb{Q}$. A linear code whose multiplicity function η takes values in $\mathbb{N}$, i.e., $\eta \in \mathbb{N}[\mathcal{O}^\sharp]$, will be called a *classical linear code.*

The definitions given earlier in this section for weight, equivalence, the mapping W of (6.1), etc., all carry over to virtual codes, with $\mathbb{Q}[\mathcal{O}^\sharp]$ replacing $\mathbb{N}[\mathcal{O}^\sharp]$. In particular, $W : \mathbb{Q}[\mathcal{O}^\sharp] \to \mathbb{Q}[\mathcal{O}]$ is a $\mathbb{Q}$-linear transformation.

Theorem 6.7. *The bimodule A has the extension property for the weight function w on A if, and only if, for every finite left R-module M, the linear transformation*

$$W : \mathbb{Q}[\mathcal{O}^\sharp] \to \mathbb{Q}[\mathcal{O}] \tag{6.2}$$

is injective.

Proof. Since $\mathbb{N}[\mathcal{O}^\sharp] \subset \mathbb{Q}[\mathcal{O}^\sharp]$, $W : \mathbb{Q}[\mathcal{O}^\sharp] \to \mathbb{Q}[\mathcal{O}]$ being injective implies that its restriction to $\mathbb{N}[\mathcal{O}^\sharp]$ will also be injective.

To prove the converse, suppose that η is in the kernel of $W : \mathbb{Q}[\mathcal{O}^\sharp] \to \mathbb{Q}[\mathcal{O}]$. By scalar multiplying by the least common multiple of the denominators of the values of η, we may assume that $\eta \in \mathbb{Z}[\mathcal{O}^\sharp]$. Create the positive part η_+ and the negative part η_- of η as follows:

$$\eta_+(\lambda) = \max\{\eta(\lambda), 0\}, \quad \eta_-(\lambda) = -\min\{\eta(\lambda), 0\}.$$

Then $\eta_\pm \in \mathbb{N}[\mathcal{O}^\sharp]$ and $\eta = \eta_+ - \eta_-$. If η is a nonzero element of $\ker W$, then $\eta_\pm$ are different elements of $\mathbb{N}[\mathcal{O}^\sharp]$ but with $W(\eta_+) = W(\eta_-)$. □

Remark 6.8. Theorems 2.4 and 2.5 say that, for bimodules of the form $A = {}_R R_R$, the extension property for Hamming weight holds if, and only if, R is a Frobenius ring. More generally, for every finite ring R, the character bimodule $A = {}_R \widehat{R}_R$ has the extension property for Hamming weight [8]. This leaves open the question of whether other bimodules have the extension property for Hamming weight. Also open is which bimodules A have the extension property for more general weight functions w.

7. Analysis of matrix modules

We apply the results of Section 6 to the matrix modules of Section 4 in order to explain the form of the counter-examples of Theorem 4.2.

Let $R = M_m(\mathbb{F}_q)$ and $S = M_k(\mathbb{F}_q)$ be the rings of $m \times m$ and $k \times k$ matrices, respectively, over the finite field $\mathbb{F}_q$. Let $A = M_{m,k}(\mathbb{F}_q)$ be the (R,S)-bimodule of $m \times k$ matrices over $\mathbb{F}_q$. The weight function on A will be the Hamming weight wt. The symmetry groups are then $G_l = \mathcal{U}(R) = GL(m, \mathbb{F}_q)$ and $G_r = \mathcal{U}(S) = GL(k, \mathbb{F}_q)$.

Any finite left R-module is isomorphic to $M = M_{m,t}(\mathbb{F}_q)$, for some t. Then the right S-module $\operatorname{Hom}_R(M, A)$ is isomorphic to the right S-module $M_{t,k}(\mathbb{F}_q)$. The set $\mathcal{O}$ of all nonzero left $GL(m, \mathbb{F}_q)$-orbits in $M = M_{m,t}(\mathbb{F}_q)$ is in one-to-one correspondence with the set of all row echelon matrices of size $m \times t$ over $\mathbb{F}_q$. Similarly, the set $\mathcal{O}^\sharp$ of nonzero right $GL(k, \mathbb{F}_q)$-orbits in $\operatorname{Hom}_R(M, A) = M_{t,k}(\mathbb{F}_q)$ is in one-to-one correspondence with the set of all column echelon matrices of size $t \times k$ over $\mathbb{F}_q$ or, by transposing, with the set of all row echelon matrices of size $k \times t$ over $\mathbb{F}_q$.

In Theorem 6.7, the vector space $\mathbb{Q}[\mathcal{O}^\sharp]$ has dimension equal to the cardinality of the set $\mathcal{O}^\sharp$, namely, the number of row echelon matrices of size $k \times t$ over $\mathbb{F}_q$. Similarly, the vector space $\mathbb{Q}[\mathcal{O}]$ has dimension equal to the number of row echelon matrices of size $m \times t$ over $\mathbb{F}_q$. Under the assumption $m < k \le t$ (as in Theorem 4.2), we see that $\dim(\mathbb{Q}[\mathcal{O}^\sharp]) > \dim(\mathbb{Q}[\mathcal{O}])$, so that W must have a nonzero kernel.

In the special case where $k = t = m+1$, we have $\dim \mathbb{Q}[\mathcal{O}^\sharp] = 1 + \dim \mathbb{Q}[\mathcal{O}]$, because there is exactly one row echelon matrix of size $(m+1) \times (m+1)$ and rank $m+1$, namely the identity matrix I_{m+1}. After some computer experimentation, one determines the form of the one-dimensional kernel $\ker(W)$ to be

$$\eta(\lambda) = (-1)^r q^{\binom{r}{2}},$$

where $\lambda \in \mathcal{O}^\sharp$ is a column echelon matrix of rank r. The proof of Theorem 4.2 provides the verification that $\eta \in \ker W$. For the more general case of $m < k \leq t$, $\dim \ker W$ will typically be strictly larger than 1. Nonetheless, the η given above is still in $\ker W$. The reader can verify this by making minor adjustments in the proof of Theorem 4.2.

The linear codes $C_\pm$ of Theorem 4.2 arise by using the positive (r even) and negative (r odd) parts of $\eta(\lambda)$, as in the proof of Theorem 6.7.

We summarize this discussion in the next theorem.

Theorem 7.1. *Let $R = M_m(\mathbb{F}_q)$, $S = M_k(\mathbb{F}_q)$, and $A = M_{m,k}(\mathbb{F}_q)$, with Hamming weight. If $m < k$, then A does not satisfy the extension property for Hamming weight.*

Specifically, let $M = M_{m,t}(\mathbb{F}_q)$, with $m < t$. Then $\dim(\mathbb{Q}[\mathcal{O}^\sharp]) > \dim(\mathbb{Q}[\mathcal{O}])$*, and* $\ker W$ *is nonzero. Moreover, if $\eta \in \mathcal{O}^\sharp$ is defined by*

$$\eta(\lambda) = (-1)^r q^{\binom{r}{2}}, \quad \lambda \in \mathcal{O}^\sharp, \quad r = \operatorname{rk} \lambda,$$

then $\eta \in \ker W$.

For completeness, we discuss the cases that fall outside those cases covered by Theorem 7.1, namely $k \leq m$ and $t \leq m < k$.

Proposition 7.2. *Let $R = M_m(\mathbb{F}_q)$, $S = M_k(\mathbb{F}_q)$, and $A = M_{m,k}(\mathbb{F}_q)$, with Hamming weight. If $m \geq k$, then A satisfies the extension property for Hamming weight.*

If $m < k$ and M is the R-module $M = M_{m,t}(\mathbb{F}_q)$, with $t \leq m$, then the associated mapping W of Theorem 6.7 *is injective. That is, when $m < k$, the extension property for codes over A with Hamming weight fails when the underlying module $M = M_{m,t}(\mathbb{F}_q)$ has $m < t$, but the extension property holds when the underlying module $M = M_{m,t}(\mathbb{F}_q)$ has $m \geq t$.*

Proof. (Sketch) When $k \leq m$, the alphabet A is an R-submodule of R itself: $A \subset R$. The extension property for A then follows from the known extension property for R (Theorem 2.4, since R is a Frobenius ring).

In the other case, where $t \leq m < k$, one observes that the mapping W of Theorem 6.7 is the same as the mapping W' associated with the extension problem for the Frobenius ring $R' = M_t(\mathbb{F}_q)$ with underlying module $M' = R'$ itself. Since W' is injective by Theorem 2.4, so is W injective. □

References

[1] G. E. Andrews, *The theory of partitions*, Encyclopedia of Mahematics and its Applications, vol. 2, Addison-Wesley, Reading, Mass., 1976.

[2] E. F. Assmus, Jr. and H. F. Mattson, *Error-correcting codes: An axiomatic approach*, Inform. and Control **6** (1963), 315–330.

[3] 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.

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

[5] H. Q. Dinh and S. R. López-Permouth, *On the equivalence of codes over finite rings*, AAECC **15** (2004), 37–50.

[6] ______, *On the equivalence of codes over rings and modules*, Finite Fields Appl. **10** (2004), 615–625.

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

[8] M. Greferath, A. Nechaev, and R. Wisbauer, *Finite quasi-Frobenius modules and linear codes*, J. Algebra & Appl. **3** (2004), 247–272.

[9] M. Greferath and S. E. Schmidt, *Finite ring combinatorics and MacWilliams's equivalence theorem*, J. Combin. Theory Ser. A **92** (2000), 17–28.

[10] T. Honold, *Characterization of finite Frobenius rings*, Arch. Math. (Basel) **76** (2001), 406–415.

[11] 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 (Survey)*, Proc. 13th Intl. Symp. AAECC-13, Springer, 1999.

[12] T. Y. Lam, *Lectures on modules and rings*, GTM, vol. 189, Springer, New York, 1999.

[13] J. H. van Lint and R. M. Wilson, *A course in combinatorics*, Cambridge University Press, Cambridge, 1992.

[14] F. J. MacWilliams, *Error-correcting codes for multiple-level transmission*, Bell System Tech. J. **40** (1961), 281–308.

[15] ______, *Combinatorial properties of elementary abelian groups*, Ph.D. thesis, Radcliffe College, Cambridge, Mass., 1962.

[16] T. Nakayama, *On Frobeniusean algebras, I*, Annals of Math. (2) **40** (1939), 611–633.

[17] ______, *On Frobeniusean algebras, II*, Annals of Math. (2) **42** (1941), 1–21.

[18] H. N. Ward and J. A. Wood, *Characters and the equivalence of codes*, J. Combin. Theory Ser. A **73** (1996), 348–352.

[19] J. A. Wood, *Extension theorems for linear codes over finite rings*, Applied Algebra, Algorithms and Error-Correcting Codes (T. Mora and H. Mattson, eds.), Lecture Notes in Comput. Sci., vol. 1255, Springer-Verlag, Berlin, 1997, pp. 329–340.

[20] ______, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math. **121** (1999), 555–575.

[21] ______, *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, 1999, pp. 231–243.

[22] ______, *The structure of linear codes of constant weight*, Trans. Amer. Math. Soc. **354** (2002), 1007–1026.

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

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

URL: http://homepages.wmich.edu/∼jwood