

## CODE EQUIVALENCE CHARACTERIZES FINITE FROBENIUS RINGS

JAY A. WOOD

(Communicated by Martin Lorenz)

**ABSTRACT.** In this paper we show that finite rings for which the code equivalence 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

A left linear code over a finite ring  $R$  is a left submodule  $C \subset R^n$ . A monomial transformation  $f : R^n \rightarrow R^n$  restricts to a linear isomorphism from  $C$  to its image  $f(C)$  that preserves the Hamming weight.

Conversely, MacWilliams [10], [11] proved that linear codes over a finite field have the following *extension property*: if  $f : C_1 \rightarrow C_2$  is a linear isomorphism between linear codes  $C_1, C_2 \subset R^n$  ( $R$  a finite field, here) and  $f$  preserves the Hamming weight, then  $f$  extends to a monomial transformation of  $R^n$ .

Linear codes over a finite Frobenius ring also have the extension property [16]. Following a strategy of Dinh and López-Permouth [4], the main result of this paper is that finite Frobenius rings are characterized by the extension property. That is, if the extension property holds for linear codes over a finite ring  $R$ , then  $R$  is a finite Frobenius ring.

Here is a short guide to the paper. Section 2 reviews definitions and presents the statement of the main result, Theorem 2.3, that a finite ring for which the extension property holds is necessarily Frobenius. Also summarized is the strategy of Dinh and López-Permouth for proving Theorem 2.3. Section 3 reviews the properties of finite Frobenius rings. Section 4 provides the main technical result, Theorem 4.1, needed to carry out the strategy of Dinh and López-Permouth. Section 5 finishes the proof of Theorem 2.3.

*Acknowledgments.* The author acknowledges with pleasure his intellectual debt to the work of Dinh and López-Permouth [4] and the work of Greferath et al. [5]. The author thanks several anonymous referees for their helpful suggestions. The author also thanks E. S. Moore for unwavering support.

---

Received by the editors February 6, 2007.

2000 *Mathematics Subject Classification.* Primary 94B05; Secondary 16D50, 16L60, 16P10.

*Key words and phrases.* Finite Frobenius rings, Hamming weight, equivalence theorem, extension property.

## 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.

A *monomial transformation* of  $R^n$  is an  $R$ -linear homomorphism  $f : R^n \rightarrow R^n$  of the form

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

where  $\pi$  is a permutation of  $\{1, 2, \dots, n\}$  and  $u_1, \dots, u_n$  are units in the ring  $R$ . Two linear codes  $C, C' \subset R^n$  are *equivalent* if there exists a monomial transformation  $f : R^n \rightarrow R^n$  with  $f(C) = C'$ .

Given  $x = (x_1, \dots, x_n) \in R^n$ , the *Hamming weight*  $\text{wt}(x)$  equals the number of nonzero components of  $x$ . That is,

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

It is easy to see that any monomial transformation  $f : R^n \rightarrow R^n$  preserves the Hamming weight; i.e.,  $\text{wt}(f(x)) = \text{wt}(x)$ , for all  $x \in R^n$ . In particular, if  $C, C' \subset R^n$  are equivalent linear codes, then there is an  $R$ -linear isomorphism  $f : C \rightarrow C'$  that preserves the Hamming weight. The next definition addresses the converse of this last statement.

**Definition 2.1.** 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  $f : C \rightarrow R^n$  preserving the Hamming weight (i.e.,  $\text{wt}(f(x)) = \text{wt}(x)$ , for all  $x \in C$ ), it follows that  $f$  extends to a monomial transformation  $f : R^n \rightarrow R^n$ .

A ring satisfying EP has also been called a MacWilliams ring [3], [4].

The main result of [16] follows. The definition of a Frobenius ring will be reviewed in Section 3.

**Theorem 2.2** ([16], 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 2.2. The proof appears in Section 5.

**Theorem 2.3.** *Every finite ring that has the extension property for Hamming weight is Frobenius.*

*Historical Remark 2.4.* MacWilliams proved that every finite field has the extension property for Hamming weight [10], [11]. This is the code equivalence theorem mentioned in the abstract. Other proofs of this result appear in [2] and [15]. As noted in Theorem 2.2, every finite Frobenius ring has the extension property. The original, character-theoretic proof is in [16], while a combinatorial proof is in [6].

Theorem 2.2 has been generalized to the context of linear codes defined over modules (to be defined in Section 4). Greferath, Nechaev, and Wisbauer show in [5] 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 2.2 is a special case of the result in [5].

The conclusion of Theorem 2.3 is already known for several classes of finite rings. Finite commutative rings with EP for Hamming weight are Frobenius [16, Theorem 6.4]. Greferath and Schmidt [6] presented the first example of a quasi-Frobenius, but not Frobenius, ring for which the extension property for Hamming weight fails. In [3, Theorem 4.5], Dinh and López-Permouth 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 [4, Theorem 7], Dinh and López-Permouth show that any finite, basic ring that has EP for Hamming weight must be Frobenius.

*Remark 2.5.* In the course of proving their result on basic rings, Dinh and López-Permouth actually prove more. Their aim in [4, Theorem 6] “is to provide a strategy” for reducing the proof of Theorem 2.3 to a nonextension problem for linear codes defined over certain matrix modules. In more detail, their strategy has three parts. (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 counterexamples to the extension property exist in the context of linear codes defined over this particular matrix module. (3) Show that the counterexamples over the matrix module pull back to give counterexamples over the original ring. Points (1) and (3) were already carried out in [4] and will be summarized for the sake of completeness in Theorem 3.1 and Section 5, respectively. Point (2) is the main technical contribution of this paper (Theorem 4.1).

### 3. FINITE FROBENIUS RINGS

There are many equivalent definitions of Frobenius rings (see, for example, Lam [9], Nakayama’s original papers [12], [13], and, in the finite case, Greferath and Schmidt [6], Honold [7], as well as [16]). In this paper, we will use the characterization of finite Frobenius rings due to Honold. The (left) *socle*  $\text{Soc}(R)$  is the left submodule generated by the irreducible left submodules of  $R$ . Similarly, there is a right socle. Honold [7] showed that, for finite rings, being Frobenius is equivalent to  $R/\text{Rad}(R) \cong \text{Soc}(R)$  either as left  $R$ -modules or as right  $R$ -modules.

If  $R$  is a finite ring, then, as rings,

$$(3.1) \quad R/\text{Rad}(R) \cong M_{\mu_1}(\mathbb{F}_{q_1}) \oplus \cdots \oplus M_{\mu_n}(\mathbb{F}_{q_n}),$$

for some nonnegative integers  $n, \mu_1, \dots, \mu_n$  and prime powers  $q_1, \dots, q_n$ , 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,  $R/\text{Rad}(R)$  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.

Recall that the matrix ring  $M_m(\mathbb{F})$  has a standard representation on the  $M_m(\mathbb{F})$ -module  $M_{m,1}(\mathbb{F})$  of all  $m \times 1$  matrices over  $\mathbb{F}_q$ , via matrix multiplication. As a left module over itself,

$${}_{M_m(\mathbb{F})}M_m(\mathbb{F}) \cong mM_{m,1}(\mathbb{F}).$$

Consequently, as a left  $R$ -module, it follows from (3.1) that

$$(3.2) \quad {}_R(R/\text{Rad}(R)) \cong \mu_1 T_1 \oplus \cdots \oplus \mu_n T_n,$$

where  $T_i$  denotes the pullback to  $R$  via (3.1) of the standard 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  $T_i$ ,  $i = 1, 2, \dots, n$ , form the complete list of all irreducible left  $R$ -modules.

The next result is implicit in the exposition following [4, Remark 4].

**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  $kT_i \subset \text{Soc}({}_R R)$ .*

4. CODES OVER MODULES AND COUNTEREXAMPLES

Several authors have studied linear codes where the alphabet is a module rather than a ring. Kurakin et al. [8] first introduced such codes for alphabets that are modules over a finite commutative ring. Later, Greferath et al. [5] 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 described in Remark 2.5.

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*  $f : A^n \rightarrow A^n$  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  $\pi$  is a permutation of  $\{1, 2, \dots, n\}$  and  $\psi_1, \dots, \psi_n \in \text{Aut}_R(A)$  are automorphisms of  $A$  over  $R$  (being written on the right). Note in the case where  $A = R$  that  $\text{Aut}_R(R)$  equals the group of units of  $R$ , 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  $f : A^n \rightarrow A^n$  with  $f(C) = C'$ .

In the context of codes over modules, the *Hamming weight*  $\text{wt}(a)$  of an element  $a = (a_1, \dots, a_n) \in A^n$  is again the number of nonzero components of  $a$ . It is easy to show that if  $C, C' \subset A^n$  are equivalent linear codes, then there exists an  $R$ -linear isomorphism  $f : C \rightarrow C'$  that preserves the Hamming weight.

The main technical result of the paper follows. It says that the converse of the last statement fails in certain cases.

**Theorem 4.1.** *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  $k > m$ , there exist linear codes  $C_+, C_- \subset A^N$ ,  $N = \prod_{i=1}^{k-1} (1 + q^i)$ , and an  $R$ -linear isomorphism  $f : C_+ \rightarrow C_-$  that preserves the Hamming weight, yet  $C_{\pm}$  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 4.1, 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

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

The following lemmas are well known (see such sources as [1, Chapter 3] and [14, Chapter 24]). The first counts the number of row reduced echelon matrices over  $\mathbb{F}_q$ , and the second is the Cauchy binomial theorem.

**Lemma 4.2.** *The  $q$ -binomial coefficient  $\begin{bmatrix} k \\ l \end{bmatrix}_q$  counts the number of row (or column) reduced echelon matrices of length  $k$  over  $\mathbb{F}_q$  of rank  $l$  (i.e., row reduced echelon matrices of size  $l \times k$  of rank  $l$ , or column reduced echelon matrices of size  $k \times l$  of rank  $l$ ).*

**Lemma 4.3** (Cauchy binomial theorem).

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

*Proof of Theorem 4.1.* 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  $g_+, g_- : A \rightarrow A^N$ .

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 column reduced echelon matrices of size  $k \times k$  over  $\mathbb{F}_q$  of even rank, with the multiplicity of the column reduced echelon matrix being  $q^{\binom{r}{2}}$ , where  $r$  denotes the rank of the matrix. In particular, the zero matrix occurs in  $v_+$  with multiplicity one, as  $\binom{0}{2} = 0$ . The length  $L_+$  of  $v_+$  is given by

$$L_+ = \sum_{\substack{r=0 \\ r \text{ even}}}^k q^{\binom{r}{2}} \begin{bmatrix} k \\ r \end{bmatrix}_q.$$

Similarly, the entries of  $v_-$  will consist of all column reduced 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 4.3 with  $x = \pm 1$  yield

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

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

$$L_+ = L_- = \prod_{i=1}^{k-1} (1 + q^i) =: N,$$

so that  $v_{\pm}$  have the same length  $N$ .

Define the  $R$ -linear homomorphisms  $g_{\pm} : A \rightarrow A^N$  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.,  $\text{wt}(g_+(X)) = \text{wt}(g_-(X))$ , for all  $X \in A$ .

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

$$\Delta(X) = \sum_{\substack{r=0 \\ r \text{ even}}}^k q^{\binom{r}{2}} \sum_{\substack{\lambda \text{ CRE} \\ \text{rank } r}} \delta(X\lambda) - \sum_{\substack{r=1 \\ r \text{ odd}}}^k q^{\binom{r}{2}} \sum_{\substack{\lambda \text{ CRE} \\ \text{rank } r}} \delta(X\lambda),$$

where  $\delta(Y) = 1$  if  $Y$  is nonzero, and  $\delta(Y) = 0$  if  $Y = 0$ . In the inner summations,  $\lambda$  varies over all column reduced echelon (CRE, for short) matrices of size  $k \times k$  over  $\mathbb{F}_q$  of rank  $r$ . Thus

$$\Delta(X) = \sum_{r=0}^k (-1)^r q^{\binom{r}{2}} \sum_{\substack{\lambda \text{ CRE} \\ \text{rank } r}} \delta(X\lambda).$$

Sub-claim: The value of  $\Delta(X)$  depends only on the rank of  $X$ .  
 Suppose  $X$  has rank  $s$ ,  $1 \leq s \leq m$ . 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  $X = PI'_sQ$ .

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, for  $X = PI'_sQ$ , we have  $\Delta(X) = \Delta(I'_sQ)$ .

The expression for  $\Delta(I'_sQ)$  contains the inner summation

$$\sum_{\substack{\lambda \text{ CRE} \\ \text{rank } r}} \delta(I'_sQ\lambda).$$

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

$$\sum_{\substack{\lambda \text{ CRE} \\ \text{rank } r}} \delta(I'_sQ\lambda) = \sum_{\substack{\lambda' \text{ CRE} \\ \text{rank } r}} \delta(I'_s\lambda'Q') = \sum_{\substack{\lambda' \text{ CRE} \\ \text{rank } r}} \delta(I'_s\lambda').$$

Note that  $Q'$  depends on  $\lambda$ , but, being invertible, it does not affect the value of  $\delta$ . 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  $\lambda$  is a column reduced 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  $\lambda$  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  $\lambda$  are zero. But  $\lambda$  is a column reduced echelon matrix of rank  $r$ , so there are  $\begin{bmatrix} k-s \\ r \end{bmatrix}_q$  such column reduced echelon matrices of rank  $r$  whose first  $s$  rows are zero. Note that this number vanishes when  $r > k - s$ .

In the summation

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

there are  $\begin{bmatrix} k \\ r \end{bmatrix}_q$  terms,  $\begin{bmatrix} k-s \\ r \end{bmatrix}_q$  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 4.3, 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  $\begin{bmatrix} k-s \\ r \end{bmatrix}_q$  is nontrivial. If  $k \leq m$ , one can show that  $\Delta(I'_k) = -1$ .)

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

Note that the common value

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

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

Claim 3: The linear codes  $C_{\pm}$  are not equivalent.

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

### 5. PROOF OF MAIN THEOREM

In this section, we prove Theorem 2.3 by following the strategy of Dinh and López-Permouth outlined in Remark 2.5.

*Proof of Theorem 2.3.* 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  $kT_i \subset \text{Soc}(R) \subset R$ . Recall that  $T_i$  is the pullback to  $R$  of the standard 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 nonequivalent linear codes  $C_{\pm} \subset A^N$ , as in Theorem 4.1. Note that the nonequivalence 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  $R \rightarrow R/\text{Rad}(R) \rightarrow M_{\mu_i}(\mathbb{F}_{q_i})$  allow us to consider  $C_{\pm}$  as  $R$ -modules. Since  $A$  pulls back to  $kT_i$ , we have  $C_{\pm} \subset (kT_i)^N \subset \text{Soc}(R)^N \subset R^N$ , as  $R$ -modules. Thus  $C_{\pm}$  are linear codes over  $R$ .

As in the proof of Theorem 4.1 (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.  $\square$

**Example 5.1** (Benson, [16], Example 1.4(ii)). Let  $R$  be the ring consisting of all  $6 \times 6$  matrices over  $\mathbb{F}_q$  of the form  $a$  below. The ring  $R$  is not Frobenius. As rings,  $R/\text{Rad}(R) \cong M_2(\mathbb{F}_q) \oplus M_1(\mathbb{F}_q)$ .

$$a = \begin{pmatrix} a_1 & 0 & a_2 & 0 & 0 & 0 \\ 0 & a_1 & 0 & a_2 & a_3 & 0 \\ a_4 & 0 & a_5 & 0 & 0 & 0 \\ 0 & a_4 & 0 & a_5 & a_6 & 0 \\ 0 & 0 & 0 & 0 & a_9 & 0 \\ a_7 & 0 & a_8 & 0 & 0 & a_9 \end{pmatrix}.$$

The set  $A$  consisting of all matrices of the form  $a$  with  $a_i = 0$  for  $i \neq 7, 8$  is a left  $R$ -module that is isomorphic to the pullback to  $R$  of the  $M_1(\mathbb{F}_q)$ -module  $M_{1,2}(\mathbb{F}_q)$ .

Denote by  $(x, y)$  the element of  $A$  with  $a_7 = x$  and  $a_8 = y$  (and other  $a_i = 0$ ). The linear code  $C_+ \subset A^{1+q} \subset R^{1+q}$  consists of all vectors of length  $1 + q$  of the form having one entry equal to  $(0, 0)$  and  $q$  entries equal to  $(x, y)$ . The linear code  $C_- \subset A^{1+q} \subset R^{1+q}$  consists of all vectors of length  $1 + q$  with entries of the form  $(y, 0)$  and  $(x + \alpha y, 0)$ , with  $\alpha$  varying over all  $\alpha \in \mathbb{F}_q$ . The reader is invited to verify that  $C_\pm$  are counterexamples to the extension property.

The final theorem is a sharpening of [4, Theorem 6] as it applies to linear codes defined over modules. The proof is the same as for Theorem 2.3.

**Theorem 5.2.** *Let  $R$  be a finite ring with notation as in (3.2), and let  $A$  be a left  $R$ -module. If there exists an index  $i$  and a multiplicity  $k > \mu_i$  so that  $kT_i \subset \text{Soc}(A) \subset A$ , then the extension property for Hamming weight fails for linear codes over the module  $A$ .*

#### REFERENCES

1. G. E. Andrews, *The theory of partitions*, Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1976. MR0557013 (58:27738)
2. 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. MR0479646 (57:19067)
3. H. Q. Dinh and S. R. López-Permouth, *On the equivalence of codes over finite rings*, Appl. Algebra Engrg. Comm. Comput. **15** (2004), no. 1, 37–50. MR2142429 (2006d:94097)
4. ———, *On the equivalence of codes over rings and modules*, Finite Fields Appl. **10** (2004), no. 4, 615–625. MR2094161 (2005g:94098)
5. M. Greferath, A. Nechaev, and R. Wisbauer, *Finite quasi-Frobenius modules and linear codes*, J. Algebra Appl. **3** (2004), no. 3, 247–272. MR2096449 (2005g:94099)
6. M. Greferath and S. E. Schmidt, *Finite-ring combinatorics and MacWilliams' equivalence theorem*, J. Combin. Theory Ser. A **92** (2000), no. 1, 17–28. MR1783936 (2001j:94045)
7. T. Honold, *Characterization of finite Frobenius rings*, Arch. Math. (Basel) **76** (2001), no. 6, 406–415. MR1831096 (2002b:16033)
8. 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), Lecture Notes in Comput. Sci., vol. 1719, Springer, Berlin, 1999, pp. 365–391. MR1846512 (2002h:94092)
9. T. Y. Lam, *Lectures on modules and rings*, Graduate Texts in Mathematics, vol. 189, Springer-Verlag, New York, 1999. MR1653294 (99i:16001)
10. F. J. MacWilliams, *Error-correcting codes for multiple-level transmission*, Bell System Tech. J. **40** (1961), 281–308. MR0141541 (25:4945)
11. ———, *Combinatorial properties of elementary abelian groups*, Ph.D. thesis, Radcliffe College, Cambridge, Mass., 1962.
12. T. Nakayama, *On Frobeniusean algebras, I*, Annals of Math. (2) **40** (1939), 611–633. MR0000016 (1:3a)
13. ———, *On Frobeniusean algebras, II*, Annals of Math. (2) **42** (1941), 1–21. MR0004237 (2:344b)
14. J. H. van Lint and R. M. Wilson, *A course in combinatorics*, Cambridge University Press, Cambridge, 1992. MR1207813 (94g:05003)
15. H. N. Ward and J. A. Wood, *Characters and the equivalence of codes*, J. Combin. Theory Ser. A **73** (1996), no. 2, 348–352. MR1370137 (96i:94028)
16. J. A. Wood, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math. **121** (1999), no. 3, 555–575. MR1738408 (2001d:94033)

DEPARTMENT OF MATHEMATICS, WESTERN MICHIGAN UNIVERSITY, 1903 W. MICHIGAN AVE., KALAMAZOO, MICHIGAN 49008–5248

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

*URL:* <http://homepages.wmich.edu/~jwood>