A Characterization of Modules with Cyclic Socle

Ali Assem
Department of Mathematics
aassem@sci.cu.edu.eg

May 5, 2015

Abstract

In 2009, J. Wood [15] proved that Frobenius bimodules have the extension property for symmetrized weight compositions. Later, in [9], it was proved that having a cyclic socle is sufficient for satisfying the property, while the necessity remained an open question.

Here, landing in Midway, the necessity is proved, a module alphabet \( R A \) has the extension property for symmetrized weight compositions built on \( \text{Aut}_R(A) \) is necessarily having a cyclic socle.

Note: All rings are finite with unity, and all modules are finite too. This may be re-emphasized in some statements. The convention for functions is that inputs are to the left.

1 Introduction

A (left) linear code of length \( n \) over a module alphabet \( R A \) is a (left) submodule \( C \subset A^n \). \( A \) has the extension property (EP) for the weight \( w \) if for any \( n \) and any two codes \( C_1, C_2 \subset A^n \), any isomorphism \( f : C_1 \to C_2 \) preserving \( w \) extends to a monomial transformation of \( A^n \). In 1962, MacWilliams [6] proved the Hamming weight EP for linear codes over finite fields; in 1996, H. Ward and J. Wood [11] re-proved this using the linear independence of group characters. This kind of proofs – using characters – led to further generalities. In 1997, J. Wood [12] proved that Frobenius rings have the EP for symmetrized weight compositions (swc), and in his 1999-paper [13], proved that Frobenius rings have the property for Hamming weight. Besides, for the last case, a partial converse was proved: commutative rings satisfying the EP for Hamming weight are necessarily Frobenius.

In 2004, Greferath et al. [7] showed that Frobenius bimodules do have the EP for Hamming weight. In [2], Dinh and López-Permouth suggested a strategy for proving the full converse. The strategy has three parts. (1) If a finite ring is not Frobenius, its socle contains a matrix module of a particular type. (2) Provide a counter-example to the EP in the context of linear codes over this special module. (3) Show that this counter example over the matrix module pulls back to give a counter example over the original ring. Finally, in 2008, J. Wood [14] provided the main technical result for carrying out the strategy, and thereby proving that rings having the EP for Hamming weight are necessarily Frobenius. The proof was easily adapted in [15] (2009) to prove that a module alphabet \( R A \) has the EP for Hamming weight if and only if \( A \) is pseudo-injective with cyclic socle.

On the other lane, in [15], J. Wood proved that Frobenius bimodules have the EP for swc, and in [9] it was shown that having a cyclic socle is sufficient (Theorem 3.4), while the necessity remained an open question. Here, the necessity is proved, making use of a new notion, namely, the annihilator weight, defined in section 4 below.
2 Background in Ring Theory

Let $R$ be a finite ring with unity, denote by $\text{rad} R$ its Jacobson radical, by the Wedderburn-Artin theorem (and Wedderburn’s little theorem) the ring $R/\text{rad} R$ is semi-simple, and (as rings)

$$R/\text{rad} R \cong \bigoplus_{i=1}^{k} M_{\mu_i} (\mathbb{F}_{q_i}),$$

(2.1)

where each $q_i$ is a prime power, $\mathbb{F}_{q_i}$ denotes a finite field of order $q_i$, and $M_{\mu_i} (\mathbb{F}_{q_i})$ denotes the ring of $\mu_i \times \mu_i$ matrices over $\mathbb{F}_{q_i}$.

It follows that, as left $R$-modules,

$$R(R/\text{rad} R) \cong \bigoplus_{i=1}^{k} \mu_i T_i,$$

(2.2)

where $\mu_i$ defined as above.

The next two propositions can be found in [15], page 17.

**Proposition 2.1.** $\text{soc}(A)$ is cyclic if and only if $s_i \leq \mu_i$ for $i = 1, \ldots, k$; $\mu_i$ defined as above.

**Proposition 2.2.** $\text{soc}(A)$ is cyclic if and only if $A$ can be embedded into $\hat{R}$, the character group of $R$ equipped with the standard module structure.

The next theorem (Theorem 4.1, [14]), by J. Wood, was the key to carry out the strategy of Dinh and López-Permouth mentioned in the introduction, actually, it displays a thoughtfully constructed piece-of-art example for the failure of the Hamming weight EP.

**Theorem 2.3.** Let $R = M_m(\mathbb{F}_q)$ and $A = M_m \times k(\mathbb{F}_q)$. 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 Hamming weight, yet there is no monomial transformation extending $f$.

If $\text{soc}(A)$ is not cyclic, then the previous theorem, applied to a certain submodule of $\text{soc}(A)$, gives counter-examples that pull back to give counter-examples for the original module, as the proof of the following theorem shows (a detailed proof is found in [15], Theorem 6.4).

**Theorem 2.4.** (Th. 5.2, [14]). Let $R$ be a finite ring, and let $A$ be a finite 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 $A$. 

2
3 Symmetrized Weight Compositions

**Definition 3.1.** (Symmetrized Weight Compositions) Let $G$ be a subgroup of the automorphism group $\text{Aut}_R(A)$ of a finite $R$-module $A$. Define an equivalence relation $\sim$ on $A$: $a \sim b$ if $a = b\tau$ for some $\tau \in G$. Let $A/G$ denote the orbit space of this relation. The symmetrized weight composition (swc) built on $G$ is a function $\text{swc} : A^n \times A/G \to \mathbb{Q}$ defined by,

$$\text{swc}(x, a) = |\{i : x_i \sim a\}|,$$

where $x = (x_1, \ldots, x_n) \in A^n$ and $a \in A/G$. Thus, swc counts the number of components in each orbit.

**Definition 3.2.** (Monomial Transformation) Let $G$ be a subgroup of $\text{Aut}_R(A)$, a map $T$ is called a $G$-monomial transformation of $A^n$ if there are some $\sigma \in S_n$ and $\tau_i \in G$ for $i = 1, \ldots, n$, such that

$$(x_1, \ldots, x_n)T = (x_{\sigma(1)}\tau_1, \ldots, x_{\sigma(n)}\tau_n),$$

where $(x_1, \ldots, x_n) \in A^n$.

**Definition 3.3.** (Extension Property) The alphabet $A$ has the extension property (EP) with respect to $\text{swc}$ if for every $n$, and any two linear codes $C_1, C_2 \subset A^n$, any $R$-linear isomorphism $f : C_1 \to C_2$ preserving $\text{swc}$ is extends to a $G$-monomial transformation of $A^n$.

In [12], J.A. Wood proved that Frobenius rings do have the extension property with respect to swc. Later, in [9], it was shown that, more generally, a left $R$-module $A$ has the extension property with respect to swc if it can be embedded in the character group $\hat{R}$ (given the standard module structure).

**Theorem 3.4.** (Th.4.1.3, [8]) Let $A$ be a finite left $R$-module. If $A$ can be embedded into $\hat{R}$ (or equivalently, $\text{soc}(A)$ is cyclic), then $A$ has the extension property with respect to the swc built on any subgroup $G$ of $\text{Aut}_R(A)$. In particular, this theorem applies to Frobenius bimodules.

4 Annihilator Weight

We now define a new notion (the Midway!) on which we’ll depend in the rest of this paper.

**Definition 4.1.** (Annihilator Weight) On $R^n$, define an equivalence relation $\approx$ by $a \approx b$ if $\text{Ann}_a = \text{Ann}_b$, where $a$ and $b$ are any two elements in $A$ and $\text{Ann}_a = \{r \in R | ra = 0\}$ is the annihilator of $a$. Clearly, $\text{Ann}_a$ is a left ideal.

Now, on $A^n$ we can define the annihilator weight $aw$ that counts the number of components in each orbit.

**Remark:** It is easily seen that the EP for Hamming weight implies the EP for swc, and the EP for $aw$ as well.

**Lemma 4.2.** Let $R^n$ be a pseudo-injective module. Then for any two elements $a$ and $b$ in $A$, $a \approx b$ if and only if $a \sim b$ ($\sim$ corresponds to the action of the whole group $\text{Aut}_R(A)$).
Proof. If \( a \sim b \), this means \( a = b\tau \) for some \( \tau \in \text{Aut}_R(A) \), and consequently \( \text{Ann}_a = \text{Ann}_b \).

Conversely, if \( a \approx b \), then we have (as left \( R \)-modules)

\[
Ra \cong R/R/\text{Ann}_a = R/R/\text{Ann}_b \cong Rb,
\]

with \( ra \mapsto r + \text{Ann}_a \mapsto rb \). By Proposition 5.1 in [15], since \( A \) is pseudo-injective, the isomorphism \( Ra \rightarrow Rb \subseteq A \) extends to an automorphism of \( A \) taking \( a \) to \( b \).

\[ \square \]

Corollary 4.3. If \( R \)A is a pseudo-injective module, then the EP with respect to \( \text{swc} \) built on \( \text{Aut}_R(A) \) is equivalent to the EP with respect to \( \text{aw} \).

Theorem 4.4. Let \( R \) be a principal ideal ring, \( R \)A a pseudo-injective module, and let \( C \) be a submodule of \( A^n \) for some \( n \). Then a monomorphism \( f : C \rightarrow A^n \) preserves Hamming weight if and only if it preserves \( \text{swc} \) built on \( \text{Aut}_R(A) \).

Proof. The “if” part is direct. For the converse, we’ll use that any left ideal \( I \) contains an element \( e_I \) that doesn’t belong to any other left ideal not containing \( I \). Now, if

\[
(c_1, c_2, \ldots, c_n) f = (b_1, b_2, \ldots, b_n),
\]

choose, from \( c_1, c_2, \ldots, c_n; b_1, b_2, \ldots, b_n \), a component with a maximal annihilator \( I \). Act on equation (4.1) by \( e_I \), then the only zero places are those of the components in equation (4.1) with annihilator \( I \), and the preservation of Hamming weight gives the preservation of \( I \)-annihilated components. Omit these components from the list \( c_1, c_2, \ldots, c_n; b_1, b_2, \ldots, b_n \) and choose one with the new maximal, and repeat. This gives that \( f \) preserves \( \text{aw} \) and hence, by Lemma 4.2, \( f \) preserves \( \text{swc} \) built on \( \text{Aut}_R(A) \).

\[ \square \]

Corollary 4.5. If \( RA \) is a module alphabet, then \( A \) has the extension property with respect to \( \text{swc} \) if and only if \( \text{soc}(A) \) is cyclic.

Proof. The “if” part is answered by Theorem 3.4. Now, if \( \text{soc}(A) \) is not cyclic, then by Proposition 2.1 there is an index \( i \) such that \( s_i > \mu_i \), where \( s_i T_i \subset \text{soc}(A) \subset A \). Recall that \( T_i \) is the pullback to \( R \) of the matrix module \( M_{\mu_i}(\mathbb{F}_q)M_{\mu_i \times 1}(\mathbb{F}_q) \), so that \( s_i T_i \) is the pullback to \( R \) of the \( M_{\mu_i}(\mathbb{F}_q) \)-module \( B = M_{\mu_i \times s_i}(\mathbb{F}_q) \). Theorem 2.3 implies the existence of linear codes \( C_+, C_- \subset B^N \), and an isomorphism \( f : C_+ \rightarrow C_- \) that preserves Hamming weight, yet \( f \) does not extend to a monomial transformation of \( B^N \). But the ring \( M_{\mu_i}(\mathbb{F}_q) \) is a principal ideal ring (in fact, more is true, Theorem 3.7, [10]), besides, \( B \) is injective, and then Theorem 4.4 implies that \( f \) preserves \( \text{swc} \) built on \( \text{Aut}_{M_{\mu_i}(\mathbb{F}_q)}(B) \).

Now, a little notice finishes the work. The isomorphism in equation (2.1) and the projection mappings \( R \rightarrow R/\text{rad}R \rightarrow M_{\mu_i}(\mathbb{F}_q) \) allow us to consider the whole situation for \( C_\pm \) as \( R \)-modules. Since \( B \) pulls back to \( s_i T_i \), we have \( C_\pm \subset (s_i T_i)^N \subset \text{soc}(A)^N \subset A^N \), as \( R \)-modules. Thus \( C_\pm \) are linear codes over \( A \) that are isomorphic through an isomorphism preserving \( \text{swc} \) built on \( \text{Aut}_R(s_i T_i) \). Also, any automorphism of \( A \) restricts to an automorphism of \( s_i T_i \), hence the isomorphism preserves \( \text{swc} \) built on \( \text{Aut}_R(A) \). However, this isomorphism does not extend to a monomial transformation of \( A^N \), since, as appears in the proof of Theorem 2.3 (found in [14]), \( C_+ \) has an identically zero component, while \( C_- \) does not.
References

[1] 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. MR MR2142429 (2006d:94097)

[2] 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 MR2094161 (2005g:94098).

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

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

[5] T. Y. Lam, *A First course in noncommutative rings*, second ed., Graduate Texts in Mathematics, vol. 131, Springer-Verlag, New York, 2001. MR MR1838439 (2002c:16001)

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

[7] M. Greferath, A. Nechaev, and R. Wisbauer, *Finite quasi-Frobenius modules and linear codes*, J. Algebra Appl. 3 (2004), no. 3, 247-272. MR MR2096449 (2005g:94099)

[8] N. ElGarem, *Codes over Finite Modules*, Master Thesis - Cairo University, 2014.

[9] N. ElGarem, N. Megahed, and J.A. Wood, The extension Theorem with respect to Symmetrized Weight Compositions, 4th international castle meeting on coding theory and applications, 2014.

[10] Thomas W. Hungerford, *ALGEBRA*, Berlin: Springer-Verlag, 1980.

[11] 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 MR1370137 (96i:94028)

[12] J. A. Wood, *Extension theorems for linear codes over finite rings*, Applied algebra, algebraic algorithms and error-correcting codes (Toulouse, 1997) (T. Mora and H. Mattson, eds.), Lecture Notes in Comput. Sci., vol. 1255, Springer, Berlin, 1997, pp. 329-340. MR MR1634126 (99h:94062)

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

[14] J. A. Wood, *Code equivalence characterizes finite Frobenius rings*, Proc. Amer. Math. Soc. 136 (2008), 699-706.

[15] J. A. Wood, *Foundations of Linear Codes Defined over Finite Modules: The Extension Theorem and MacWilliams Identities*, *Codes over Rings*, Proceedings of the CIMPA Summer School, Ankara, Turkey, 18-29 August 2008, (Patrick Solé) Series on Coding Theory and Cryptology, Vol. 6, World Scientific, Singapore, 2009, p. 124-190.