The Extension Theorem with Respect to Symmetrized Weight Compositions

Noha ElGarem, Nefertiti Megahed, and Jay A. Wood

Abstract We will say that an alphabet A satisfies the extension property with respect to a weight w if every linear isomorphism between two linear codes in A^n that preserves w extends to a monomial transformation of A^n. In the 1960s MacWilliams proved that finite fields have the extension property with respect to Hamming weight. It is known that a module A has the extension property with respect to Hamming weight or a homogeneous weight if and only if A is pseudo-injective and embeds into $\hat{R}$. The main theorem presented in this paper gives a sufficient condition for an alphabet to have the extension property with respect to symmetrized weight compositions. It has already been proven that a Frobenius bimodule has the extension property with respect to symmetrized weight compositions. This result follows from the main theorem.

Keywords Linear codes over finite modules • Extension theorem • Symmetrized weight composition

1 Introduction

In the 1960s Florence Jessie MacWilliams proved in her doctoral dissertation [13] that two linear codes over a finite field are isometric if and only if they are monomially equivalent. Two linear codes of the same length are said to be isometric if there is a linear injective map from one to the other that preserves Hamming weight. In other words, two linear codes $C_1, C_2 \subset \mathbb{F}_q^n$ are isometric if there is a linear injective map $f : C_1 \to C_2$ such that $wt(f(c)) = wt(c)$ for every $c \in C_1$, where wt denotes the Hamming weight on $\mathbb{F}_q$. The codes are said to be monomially equivalent if there is a monomial transformation, or an $n \times n$ monomial matrix M, such that $C_2 = C_1 M$. Because monomial equivalence implies the existence of an

N. ElGarem (✉) • N. Megahed
Cairo University, Giza 12613, Egypt
e-mail: n_garem@aucegypt.edu; nefertiti@sci.cu.edu.eg

J.A. Wood
Western Michigan University, 1903 W Michigan Ave, Kalamazoo, MI 49008, USA
e-mail: jay.wood@wmich.edu

R. Pinto et al. (eds.), *Coding Theory and Applications*, CIM Series in Mathematical Sciences 3, DOI 10.1007/978-3-319-17296-5_18

isometry, what MacWilliams proved for codes over finite fields is that any isometry can be extended to a monomial transformation. MacWilliams also proved a semi-linear version of this extension theorem. In 1996, a character theoretic proof of MacWilliams' result appeared in [14].

The publication of [12] rekindled the interest of researchers in codes over finite rings and the question arose, which types of rings satisfy MacWilliams' Extension Theorem? In [17], the character theoretic proof of [14] was generalized to prove that finite Frobenius rings satisfy the Extension Theorem with respect to Hamming weight. In [4] Dinh and López-Permouth proved some partial converses and provided a strategy to prove the full converse. The strategy led to a proof of the full converse in [18] for linear codes over finite rings with the Hamming weight.

In 1997, Constantinescu and Heise introduced a new weight on finite rings [2], namely, the homogeneous weight. The authors of [3] used combinatorial methods to prove the extension theorem for homogeneous weights over the ring $\mathbb{Z}_m$. Following their lead, Greferath and Schmidt proved that every Hamming weight isometry is a homogeneous weight isometry and vice versa, thereby translating all results on the Extension Theorem for Hamming weight to homogeneous weights and vice versa [11]. Greferath, Nechaev, and Wisbauer proved the Extension Theorem for Hamming and homogeneous weights over Frobenius bimodules in [10].

More general weight functions were considered next, specifically bi-invariant weight functions. A weight w on a ring R is said to be bi-invariant if $w(ux) = w(x) = w(xu)$ for every x in R and every unit u in R. The extension theorem was proved for bi-invariant weights in the case of finite chain rings in [6], in the case of $\mathbb{Z}_m$ in [7], in the case of finite direct products of finite chain rings in [9], in the case of matrix rings over finite fields in [19], and in the case of principal ideal rings, necessary and sufficient conditions were found for bi-invariant weights to satisfy the extension theorem in [8].

The present paper considers the Extension Theorem with respect to another type of weight, namely the symmetrized weight composition over certain module alphabets. The Extension Theorem for symmetrized weight compositions was proved for linear codes over finite fields in [5], over finite Frobenius rings in [15], and over Frobenius bimodule alphabets in [19]. In [1], Barra and Gluesing-Luerssen greatly simplified the proof in [15], and we apply their ideas to the case of certain module alphabets.

The following is a summary of the contents of this paper. Section 2 provides some basic definitions, as well as the Extension Theorems known for module alphabets equipped with Hamming weight. In Sect. 3, we apply some of the ideas of [1] to module alphabets. The main result of this paper (Theorem 13) states that a sufficient condition for an R-module A to satisfy the Extension Theorem with respect to symmetrized weight compositions is that A can be embedded into ${}_R\hat{R}$. This condition implies that a Frobenius bimodule satisfies the Extension Theorem with respect to symmetrized weight compositions.

The Extension Theorem for symmetrized weight compositions over finite Frobenius rings has been used in [15] and [16] to prove extension theorems for more general weight functions. We anticipate proving similar results in future work.

2 Background

Throughout this paper, let R be a finite ring with unity and let A be a finite left R-module; A will serve as the alphabet for linear codes. We will adopt the following convention: when dealing with maps on left R-modules, the input to the map will be written on the left. In other words, if we have a left R-module A and a map f on A, then for $a \in A$, we write af for $f(a)$.

Definition 1 A *linear code* of length n over the alphabet A is a left R-submodule $C \subset A^n$.

Definition 2 A *monomial transformation* of A^n is an R-linear automorphism T of A^n of the form

$$(a_1, \ldots, a_n)T = (a_{\sigma(1)}\tau_1, \ldots, a_{\sigma(n)}\tau_n),$$

where $(a_1, \ldots, a_n) \in A^n$, σ is a permutation of $\{1, 2, \ldots, n\}$ and $\tau_1, \ldots, \tau_n \in \mathrm{Aut}(A)$, the group of automorphisms of the left R-module A. If $\tau_1, \ldots, \tau_n$ all belong to some subgroup G of $\mathrm{Aut}(A)$, we say that T is a G-monomial transformation of A^n.

A weight on an alphabet A is defined to be a rational-valued function $w : A \to \mathbb{Q}$ with $w(0) = 0$. We define the extension property as follows.

Definition 3 Let A be an R-module. We say that the alphabet A *satisfies the extension property with respect to the Hamming weight* if every R-linear isomorphism between two R-linear codes in A^n that preserves Hamming weight extends to a monomial transformation of A^n.

The class of Frobenius bimodules stood out in coding theory as all Frobenius bimodules satisfy the extension property with respect to Hamming weight [10]. A Frobenius bimodule is defined as follows.

Definition 4 Let A be a bimodule over the ring R. We say that A is a *Frobenius bimodule* if ${}_RA \cong_R \hat{R}$ and $A_R \cong \hat{R}_R$, where $\hat{R} = \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{C}^\times)$ is the character module of R.

The following theorem was proved in [17] and [18].

Theorem 5 *Let R be a finite ring and $A = R$. Then R satisfies the extension property with respect to Hamming weight if and only if R is Frobenius.*

Necessary and sufficient conditions for a module alphabet A to satisfy the extension property with respect to Hamming weight were established in [19]. The first condition is that the R-module alphabet A is pseudo-injective, in other words for every R-submodule B of A and every injective R-linear mapping $f : B \to A$, the mapping f extends to an R-linear mapping $\tilde{F} : A \to A$. The second condition that arises is that A have a cyclic socle. The socle of an R-module A is defined to be the sum of all its simple R-submodules. We note that a left R-module A has a cyclic socle if and only if A embeds into $\hat{R}$ ([19], Proposition 5.3).

Theorem 6 *Let R be a finite ring and A a finite R-module. Then A satisfies the extension property with respect to Hamming weight if and only if A is pseudo-injective and has a cyclic socle.*

3 The Extension Theorem for Symmetrized Weight Compositions

Given a weight w on an alphabet A, define the symmetry group of w as the set of all automorphisms of A that preserve w. Denote the symmetry group by

$$Sym(w) := \{\tau \in \mathrm{Aut}(A) | w(a\tau) = w(a) \text{ for every } a \in A\}.$$

Then for a general weight w, the extension property is defined as follows.

Definition 7 Let A be an alphabet and w a weight on A. Then A has the *extension property with respect to* w if for any two linear codes $C_1, C_2 \subset A^n$, and R-linear isomorphism $f : C_1 \to C_2$ that preserves w, f is extendable to a $Sym(w)$-monomial transformation of A^n.

The symmetry group of a weight w on an alphabet A acts on A on the right so that the orbit of an element a in A is $orb(a) = \{a\tau | \tau \in Sym(w)\}$. The symmetrized weight composition counts the number of entries of $x = (x_1, \ldots, x_n) \in A^n$ that belong to any given orbit of this action.

We now give the formal definition of the symmetrized weight composition.

Definition 8 Let G be a subgroup of the automorphism group of a finite R-module A. Define $\sim$ on A by $a \sim b$ if and only if $a = b\tau$ for some $\tau \in G$. Let A/G denote the orbit space of this action. The *symmetrized weight composition* is a function $\mathrm{swc} : A^n \times A/G \to \mathbb{Q}$ defined by,

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

where $x = (x_1, \ldots, x_n) \in A^n$ and $a \in A/G$.

Note that if $a, b \in A$ are in the same orbit, then $\mathrm{swc}_a = \mathrm{swc}_b$ and so the symmetrized weight composition is well-defined.

Definition 9 The alphabet A has the *extension property with respect to* swc if for any two linear codes $C_1, C_2 \subset A^n$, and R-linear isomorphism $f : C_1 \to C_2$ that preserves swc, f is extendable to a G-monomial transformation of A^n.

We wish to find conditions on the module alphabet A equipped with swc to satisfy the extension property analogous to those found in Theorem 6 for Hamming weight. Theorem 13 gives a sufficient condition and its proof uses some of the ideas found in [1].

In order to prove the main theorem, we need a few results concerning admissible characters. More details can be found in [19] and [20] (where admissible characters were called generating characters).

Definition 10 Let A be a finite left R-module. We say a character $\rho \in \hat{A}$ is *(left) admissible* if $\ker \rho$ contains no nonzero left R-submodules. There is a corresponding notion of right admissible characters for right R-modules.

The proof of the main theorem requires a proposition from [20].

Proposition 11 ([20], Proposition 12) *Let A be a finite left R-module. Then A has an admissible character if and only if A can be embedded in ${}_R\hat{R}$.*

The reader will verify that Frobenius bimodules have admissible characters.

The condition that will appear in the main theorem (Theorem 13) is that the R-module alphabet A can be embedded into $\hat{R}$. As mentioned earlier, this condition is equivalent to the condition that the alphabet A has a cyclic socle due to the following result (Proposition 5.3 in [19]).

Proposition 12 *Let R be a ring and A a left R-module. Then $soc(A)$ is cyclic if and only if A can be embedded into ${}_R\hat{R}$.*

We now state and prove the main theorem.

Theorem 13 *Let A be a finite left R-module equipped with a symmetrized weight composition. If A can be embedded into $\hat{R}$, then A has the extension property with respect to the symmetrized weight composition. In particular, this theorem applies to Frobenius bimodules.*

Proof Suppose $C_1, C_2 \subset A^n$ are two R-linear codes, and $f : C_1 \to C_2$ is an R-linear isomorphism that preserves swc. Let M be the module underlying the two codes C_1, C_2 with $\lambda : M \to A^n$ and $\nu : M \to A^n$, the inclusion maps of C_1 and C_2 into A^n, respectively, and $\nu = \lambda \circ f$ (recall that inputs to functions are written on the left). Suppose $\lambda = (\lambda_1, \ldots, \lambda_n)$ and $\nu = (\nu_1, \ldots, \nu_n)$, where $\lambda_i, \nu_i \in \mathrm{Hom}_R(M, A)$. Since f preserves swc, then $\mathrm{swc}_a(x\lambda) = \mathrm{swc}_a(x\nu)$ for every $a \in A/G$ and every $x \in M$. Following [1], if we fix $x \in M$ then there exists a permutation σ_x of $\{1, \ldots, n\}$ and elements $\phi_{j,x} \in G$ such that $x\lambda_j = x\nu_{\sigma_x(j)}\phi_{j,x}$ for each $j \in \{1, \ldots, n\}$. Let $\psi \in G$, noting that $G \subset \mathrm{Aut}(A)$, then for all j,

$$x\lambda_j\psi = x\nu_{\sigma_x(j)}\phi_{j,x}\psi. \tag{1}$$

Since A can be embedded into $\hat{R}$, it follows from Proposition 11 that A has an admissible character $\rho : A \to \mathbb{C}^\times$. Compose ρ with both sides of Eq. (1) to get

$$(x\lambda_j\psi)\rho = (x\nu_{\sigma_x(j)}\phi_{j,x}\psi)\rho.$$

We can now take the summation of the previous equation over all $j \in \{1, \ldots, n\}$

and all $\psi \in G$ yielding the following,

$$\sum_{j=1}^{n} \sum_{\psi \in G} (x\lambda_j \psi)\rho = \sum_{j=1}^{n} \sum_{\psi \in G} (x\nu_{\sigma_x(j)} \phi_{j,x} \psi)\rho$$
$$= \sum_{k=1}^{n} \sum_{\tau \in G} (x\nu_k \tau)\rho.$$

Since the above equation is true for every $x \in M$, we have the following equation of characters of M,

$$\sum_{j=1}^{n} \sum_{\psi \in G} (\lambda_j \psi)\rho = \sum_{k=1}^{n} \sum_{\tau \in G} (\nu_k \tau)\rho. \tag{2}$$

We can now make use of the fact that characters of M are linearly independent, when considered as complex-valued functions on M. On the left hand side of Eq. (2), fix $j = 1$ and $\psi = id_A$. By the independence of characters it follows that there exists $k_1 \in \{1, \ldots, n\}$ and $\tau_1 \in G$ such that $\lambda_1 \circ \rho = \nu_{k_1}\tau_1 \circ \rho$. Then $im(\lambda_1 - \nu_{k_1}\tau_1) \subset \ker \varrho$. But ρ is an admissible character of A and therefore contains no non-zero submodules. It follows that $im(\lambda_1 - \nu_{k_1}\tau_1) = 0$ and so $\lambda_1 = \nu_{k_1}\tau_1$. Re-indexing (letting $\phi = \tau_1\psi$), shows that

$$\sum_{\psi \in G} (\lambda_1 \psi)\rho = \sum_{\psi \in G} (\nu_{k_1}\tau_1 \psi)\rho = \sum_{\phi \in G} (\nu_{k_1}\phi)\rho.$$

This allows us to reduce the outer summation in Eq. (2) by one. Proceeding by induction, we find a permutation σ and automorphisms $\tau_1, \ldots, \tau_n \in G$ with $\lambda_i = \nu_{\sigma(i)}\tau_i$. □

A natural question to ask is whether the converse of Theorem 13 is true. In other words, if the extension property holds for an R-module alphabet A equipped with a symmetrized weight composition, must A have a cyclic socle? Or equivalently must there be an embedding of A into $\hat{R}$? This remains an open question.

References

1. Barra, A., Gluesing-Luerssen, H.: MacWilliams extension theorems and the local-global property for codes over rings (2013). arXiv:1307.7159
2. Constantinescu, I., Heise, W.: A metric for codes over residue class rings of integers. Probl. Inf. Trans. **33**(3), 208–213 (1997)
3. Constantinescu, I., Heise, W., Honold, T.: Monomial extensions of isometries between codes over $\mathbb{Z}_m$. In: Proceedings of the Fifth International Workshop on Algebraic and Combinatorial Coding Theory, Sozopol, pp. 98–104. Unicorn, Shumen (1996)

4. Dinh, H.Q., López-Permouth, S.R.: On the equivalence of codes over rings and modules. Finite Fields Appl. **10**(4), 615–625 (2004). doi:10.1016/j.ffa.2004.01.001
5. Goldberg, D.: A generalized weight for linear codes and a Witt-MacWilliams theorem. J. Comb. Theory Ser. A **29**(3), 363–367 (1980)
6. Greferath, M., Honold, T.: On weights allowing for MacWilliams equivalence theorem. In: Proceedings of the Fourth International Workshop on Optimal Codes and Related Topics, Pamporovo, pp. 182–192 (2005)
7. Greferath, M., Honold, T.: Monomial extensions of isometries of linear codes ii: invariant weight functions on $\mathbb{Z}_m$. In: Proceedings of the Tenth International Workshop on Algebraic and Combinatorial Coding Theory, Zvenigorod, pp. 106–111 (2006)
8. Greferath, M., Honold, T., McFadden, C., Wood, J.A., Zumbrägel, J.: MacWilliams' extension theorem for bi-invariant weights over finite principal ideal rings. J. Comb. Theory Ser. A **125**, 177–193 (2014)
9. Greferath, M., McFadden, C., Zumbrägel, J.: Characteristics of invariant weights related to code equivalence over rings. Des. Codes Cryptogr. **66**(1–3), 145–156 (2013)
10. Greferath, M., Nechaev, R., Wisbauer, R.: Finite quasi-Frobenius modules and linear codes. J. Algebra Appl. **3**(3), 247–272 (2004)
11. Greferath, M., Schmidt, S.E.: Finite ring combinatorics and MacWilliams equivalence theorem. J. Comb. Theory Ser. A **92**(1), 17–28 (2000). doi:10.1006/jcta.1999.3033
12. Hammons, A., Kumar, P., Calderbank, A., Sloane, N., Solé, P.: The $\mathbb{Z}_4$ linearity of Kerdock, Preparata, Goethals, and related codes. IEEE Trans. Inf. Theory **40**(2), 301–319 (1994). doi:10.1109/18.312154
13. MacWilliams, F.J.: Combinatorial properties of elementary abelian groups. Ph.D. thesis, Harvard University, Cambridge (1962)
14. Ward, H.N., Wood, J.A.: Characters and the equivalence of codes. J. Comb. Theory Ser. A **73**(2), 348–352 (1996). doi:10.1016/S0097-3165(96)80011-2
15. Wood, J.A.: Extension theorems for linear codes over finite rings. In: Mora, T., Mattson, H. (eds.) Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. Lecture Notes in Computer Science, vol. 1255, pp. 329–340. Springer, Berlin/Heidelberg (1997). doi:10.1007/3-540-63163-1_26
16. Wood, J.A.: Weight functions and the extension theorem for linear codes over finite rings. In: Proceedings of the Fourth International Conference on Finite Fields: Theory, Applications and Algorithms, University of Waterloo, Waterloo (1997)
17. Wood, J.A.: Duality for modules over finite rings and applications to coding theory. Am. J. Math. **121**, 555–575 (1999)
18. Wood, J.A.: Code equivalence characterizes finite Frobenius rings. Proc. Am. Math. Soc. **136**, 699–706 (2008). doi:10.1090/S0002-9939-07-09164-2
19. Wood, J.A.: Foundations of linear codes defined over finite modules: the extension theorem and MacWilliams identities. In: Solé, P. (ed.) CIMPA Summer School, Ankara, 18–29 Aug 2008. Series on Coding Theory and Cryptology, vol. 6, pp. 124–190. World Scientific (2009)
20. Wood, J.A.: Applications of finite Frobenius rings to the foundations of algebraic coding theory. In: Iyama, O. (ed.) 44th Symposium on Ring Theory and Representation Theory, Okayama University, Nagoya, pp. 235–245 (2012)