Weight Functions and the Extension Theorem for Linear Codes over Finite Rings

Jay A. Wood

In memory of Ed Assmus

Abstract. An extension theorem for general weight functions is proved over finite chain rings. The structure of the complex semigroup ring associated to the multiplicative semigroup of the ring plays a prominent role in the proof.

1. Background

In her doctoral dissertation, MacWilliams [**7**], [**8**] proved an equivalence theorem: two linear codes $C_1, C_2 \subset \mathbb{F}^n$ defined over a finite field $\mathbb{F}$ are equivalent up to monomial transformations if and only if there is a linear isomorphism $f : C_1 \to C_2$ which preserves Hamming weight. Bogart, Goldberg, and Gordon [**2**] gave another proof of this theorem, and a character theoretic proof was provided by Ward and the author [**13**].

Following up on the ideas in [**13**], the author has extended the character theoretic techniques to linear codes defined over finite Frobenius rings, first for the Hamming weight [**15**] and then for symmetrized weight compositions [**16**]. In this paper, the author treats general weight functions defined over finite chain rings, i.e., finite commutative local principal ideal rings. Goldberg proved the extension theorem for symmetrized weight compositions over finite fields, [**5**], and Constantinescu, Heise, and Honold have proved an extension theorem for homogeneous weight functions over $\mathbb{Z}/m$, [**4**].

A word on the name of the theorem. MacWilliams' result above is sometimes referred to as "the equivalence theorem of MacWilliams." I have come to prefer

1991 *Mathematics Subject Classification.* Primary 94B05; Secondary 13M05, 16P10, 16S36, 20M25.

Key words and phrases. Semigroup rings, finite Fourier transform, extension theorem.

Partially supported by NSA grants MDA904-94-H-2025 and MDA904-96-1-0067, and by Purdue University Calumet Scholarly Research Awards.

Expanded version of results presented at the Fourth International Conference on Finite Fields and Applications and at the Thirty-Fifth Allerton Conference on Communication, Control, and Computing [**17**]. This paper is in final form and no version of it will be submitted for publication elsewhere.

"the extension theorem of MacWilliams," because of the similarity to the extension theorems of Witt [**14**] and Arf [**1**] for bilinear and quadratic forms. In all these situations there is a fixed ambient space V, usually a finite dimensional vector space over a field. The space V is equipped with an auxiliary function, a weight function in coding theory, a bilinear or quadratic form otherwise. The linear automorphisms of V which preserve the auxiliary function form a group of *linear isometries*, often a classical group in the case of bilinear or quadratic forms, often a group of monomial transformations in coding theory. The *extension theorem* then determines conditions under which any injective linear transformation $f : W \to V$ from a subspace W of V which preserves the auxiliary function must in fact extend to a linear isometry of V itself.

2. Statement of the extension problem

Fix a finite associative ring R with 1. (Later, we will impose additional hypotheses on R, but we will try to be as general as possible for as long as possible.) Let R^n denote the free module consisting of n-tuples of elements from R. A right *linear code* of length n is a right submodule $C \subset R^n$. The *complete weight composition* is the function $c : R \times R^n \to \mathbb{Z}$ given by

$$c_r(x) = |\{i : x_i = r\}|, \quad r \in R, \quad x = (x_1, \ldots, x_n) \in R^n.$$

That is, the complete weight composition counts the number of entries in the n-tuple x which equal a particular element r in R.

Choose complex numbers a_r, $r \neq 0$ in R, and set $a_0 = 0$. Then the *weight function* determined by the a_r's is $w : R^n \to \mathbb{C}$ given by

$$w(x) = \sum_{r \in R} a_r c_r(x), \quad x \in R^n.$$

Since $a_0 = 0$, this sum is the same as the sum over $r \neq 0$.

EXAMPLE 2.1. For any ring R, choosing $a_r = 1$ for all $r \neq 0$ yields the *Hamming weight*.

EXAMPLE 2.2. For $R = \mathbb{Z}/k$, thought of as the integers j satisfying $-k/2 < j \leq k/2$, set $a_j = |j|$. The resulting weight function is then the *Lee weight*. The use of the Lee weight for linear codes over $\mathbb{Z}/4$ and its connections with nonlinear binary codes in [**3**], [**6**] has been an important motivation for the author's work.

EXAMPLE 2.3. The *Euclidean weight* for $R = \mathbb{Z}/k$ has $a_j = |j|^2$.

Notice that the Lee and Euclidean weight functions have some symmetry: $a_{-j} = a_j$. More generally, we define the *symmetry group* of a weight function w by

$$\mathrm{Sym}(w) = \{u \in \mathcal{U} : a_{ur} = a_r, \ r \in R\}.$$

Here $\mathcal{U}$ denotes the group of units in R. Since R is finite, all units are necessarily two-sided. The Lee and Euclidean weights have $\mathrm{Sym}(w) = \{\pm 1\}$.

Let U be a subgroup of $\mathcal{U}$. Multiplication defines a left action of U on the ring R, with each element acting as an additive group automorphism of R; $u \in U$ defines $r \mapsto ur$. We will write $r \approx s$ if $r = us$ for some $u \in U$. We set $\mathrm{orb}(r) = \{s \in R : r \approx s\}$, the *orbit* of $r \in R$ under U. Of course, $r \approx s$ if and only if $\mathrm{orb}(r) = \mathrm{orb}(s)$. Let $U\backslash R$ be the set of U-orbits in R. If $U \subset \mathrm{Sym}(w)$, then $a_r = a_s$ whenever $r \approx s$, and the value of a_r depends only on $\mathrm{orb}(r) \in U\backslash R$.

The subgroup U determines a *symmetrized weight composition* swc by

$$\mathrm{swc}_t(x) = |\{i : x_i \approx t\}| = \sum_{r \in \mathrm{orb}(t)} c_r(x).$$

Note that $\mathrm{swc}_s(x) = \mathrm{swc}_t(x)$ if $\mathrm{orb}(s) = \mathrm{orb}(t)$. Provided $U \subset \mathrm{Sym}(w)$, the weight function w can be written as

$$w(x) = \sum_{t \in U \backslash R} a_t \, \mathrm{swc}_t(x), \quad x \in R^n. \tag{2.1}$$

Let us now consider the linear automorphisms of R^n which preserve one of our auxiliary functions: either a weight function w or a symmetrized weight composition swc. A right linear transformation $f : R^n \to R^n$ is a right *monomial transformation* if there exist a permutation σ of $\{1, 2, \ldots, n\}$ and units $u_1, u_2, \ldots, u_n$ in R such that

$$f(x_1, x_2, \ldots, x_n) = (u_1 x_{\sigma(1)}, u_2 x_{\sigma(2)}, \ldots, u_n x_{\sigma(n)}),$$

for $(x_1, x_2, \ldots, x_n) \in R^n$. If, in addition, the units $u_1, \ldots, u_n$ lie in a subgroup $U \subset \mathcal{U}$ of the group of units of R, we say that f is a right *U-monomial transformation*. It is easy to verify that the right U-monomial transformations form a group under composition; the group is isomorphic to the n-fold wreath product of U.

In [**16**, Proposition 2, Theorem 9], the author proved the next two results about automorphisms which preserve a symmetrized weight composition; the second result is the extension theorem for symmetrized weight compositions over finite Frobenius rings. The definition of a Frobenius ring is somewhat technical (see [**11**] or [**15**]); for finite rings it is equivalent to the character module $\widehat{R} = \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{T})$ being free as a one-sided R-module. Here, $\mathbb{T}$ is the multiplicative group of unit complex numbers.

PROPOSITION 2.4. *Let $f : R^n \to R^n$ be a right linear automorphism. Then f preserves* swc, *i.e.,* $\mathrm{swc}_t(f(x)) = \mathrm{swc}_t(x)$, *for all $t \in U \backslash R$, $x \in R^n$, if and only if f is a right U-monomial transformation.*

THEOREM 2.5. *Suppose R is a finite Frobenius ring, and suppose U is a subgroup of the group of units in R. If $C \subset R^n$ is a right linear code and $f : C \to R^n$ is an injective right linear homomorphism which preserves the symmetrized weight composition* swc, *then f extends to a right U-monomial transformation of R^n.*

The corresponding results for a weight function w are the main items discussed in this paper. For the counterpart of Proposition 2.4, we must assume that the linear automorphism is already a monomial transformation. This result was also proved in [**16**, Proposition 10].

PROPOSITION 2.6. *Suppose a weight function w has symmetry group* $\mathrm{Sym}(w)$. *Then a right monomial transformation on R^n preserves w if and only if it is a* $\mathrm{Sym}(w)$*-monomial transformation.*

The following states the extension problem for weight functions over finite Frobenius rings, the counterpart to Theorem 2.5.

EXTENSION PROBLEM. *Suppose R is a finite Frobenius ring and that w is a weight function with symmetry group* $\mathrm{Sym}(w)$. *Determine conditions on the weight function w in order that every injective right linear homomorphism $f : C \to R^n$*

which preserves w, $C \subset R^n$ a right linear code, extends to a right monomial transformation on R^n which preserves w, i.e., a right $\mathrm{Sym}(w)$*-monomial transformation on R^n.*

COROLLARY 2.7. *Suppose w is a weight function with symmetry group* $\mathrm{Sym}(w)$ *for which the extension problem is solvable. Then the group of right linear automorphisms of R^n which preserve w is exactly the group of right* $\mathrm{Sym}(w)$*-monomial transformations.*

PROOF. Simply take $C = R^n$. □

3. Reducing to the weight composition case

In this section we describe two approaches to solving the extension problem for weight functions. Both approaches reduce the extension problem to the weight composition case covered by Theorem 2.5.

Suppose that $C \subset R^n$ is a right linear code with $f : C \to R^n$ a right linear homomorphism which preserves a weight function w. We assume that w has symmetry group $\mathrm{Sym}(w)$.

We utilize linearity: both the code C as well as $f : C \to R^n$ are right linear. What happens if we replace x by xs? We will discuss two ways of answering this question.

First approach. Notice that w can be written in the form

$$w(x) = \sum_{i=1}^{n} a_{x_i}.$$

This allows us to conclude that

$$w(xs) = \sum_{i=1}^{n} a_{x_i s} = \sum_{r \in R} a_{rs}\, c_r(x). \tag{3.1}$$

Let U be a subgroup of $\mathrm{Sym}(w)$. Recall that $r \approx t$ if $r = ut$ for some $u \in U$. Since $U \subset \mathrm{Sym}(w)$, if $r \approx t$, then $a_{rs} = a_{uts} = a_{ts}$. This allows us to rewrite (3.1) as

$$w(xs) = \sum_{t \in U\backslash R} \mathrm{swc}_t(x)\, a_{ts}. \tag{3.2}$$

Let $\mathcal{A}$ be the matrix of size $(|U\backslash R| - 1) \times (|R| - 1)$ whose (t, s) entry is a_{ts}. (We restrict $t \in U\backslash R$ and $s \in R$ to be non-zero, since $a_0 = 0$.) This leads to a very general version of the extension theorem.

THEOREM 3.1. *Suppose R is a finite Frobenius ring with weight function w. If the matrix $\mathcal{A}$ has maximal rank $|U\backslash R| - 1$, then the extension problem is solvable for w. The extension is a U-monomial transformation.*

PROOF. If f preserves w, then the rank condition and (3.2) imply that f preserves swc. Now apply Theorem 2.5. □

REMARK 3.2. If R is a commutative ring, then the value of a_{ts} depends only on the orbits of t and s. In this case, let $\mathcal{A}$ be square of size $|U\backslash R| - 1$ with (t, s) entry a_{ts}, for t, s nonzero elements of $U\backslash R$. The extension problem is solvable if $\det \mathcal{A} \neq 0$.

While this theorem seems very general, it is often difficult to apply. See Section 8 for some examples.

Our second approach, even though it is much less general, leads to conditions which are comparatively easy to verify. This second approach will occupy the remainder of the paper.

Second approach. For convenience, set $\delta_r = \delta_r(x) = c_r(f(x)) - c_r(x)$. Weight preservation says that

$$\sum_{r\neq 0} a_r \delta_r(x) = 0, \quad x \in C.$$

Notice that

$$c_r(xs) = \sum_{q:qs=r} c_q(x).$$

The linearity of C and f allows us to write the weight preservation condition as

$$\sum_{r\neq 0} a_r \left(\sum_{q:qs=r} \delta_q(x) \right) = 0, \quad x \in C, \quad s \in R. \tag{3.3}$$

We write (3.3) in matrix form. Let A be a row vector of length $|R|-1$, with typical entry a_r indexed by $r \neq 0$ in R. Similarly, let Δ be a square matrix of size $|R|-1$ whose rows and columns are indexed by $r, s \neq 0$ in R, with (r,s)-entry equal to $\sum_{q:qs=r} \delta_q(x)$. Thus (3.3) takes the form

$$A\Delta = 0. \tag{3.4}$$

The basic strategy is to exploit the structure of (3.4) in order to conclude that $\sum_{q\in \mathrm{orb}(t)} \delta_q(x) = 0$. Since the latter is equivalent to $\mathrm{swc}_t(f(x)) = \mathrm{swc}_t(x)$, swc is preserved by f, and we may apply Theorem 2.5 to prove the extension theorem. How to go about exploiting the structure of (3.4) is the subject of subsequent sections.

4. Semigroup rings

Let S be a finite semigroup whose operation is written as multiplication. Assume S has both a 0 and a 1 (different). The *complex semigroup ring* $\mathbb{C}[S]$ is then

$$\mathbb{C}[S] = \left\{ \sum_{s\in S} b_s e_s : b_s \in \mathbb{C} \right\},$$

a complex vector space with basis e_s, $s \in S$, whose multiplication is determined by the semigroup multiplication: $e_s e_t = e_{st}$. The one-dimensional subspace spanned by e_0 is a two-sided ideal in $\mathbb{C}[S]$, and its quotient

$$\mathbb{C}_0[S] = \mathbb{C}[S]/(e_0)$$

is called the *reduced* complex semigroup ring associated to S; $\mathbb{C}_0[S]$ has dimension $|S|-1$ over $\mathbb{C}$.

Of particular interest to us is the semigroup we will denote by $S = R^\star$, the multiplicative semigroup of a finite ring. Then $\mathbb{C}_0[R^\star]$ has dimension $|R|-1$. We are interested in the left regular representation of $\mathbb{C}_0[R^\star]$, i.e., $\mathbb{C}_0[R^\star]$ acting on itself by left multiplication. If $b = \sum_{r\neq 0} b_r e_r \in \mathbb{C}_0[R^\star]$, what is the matrix L_b with

respect to the basis $\{e_r\}$ for the linear transformation given by left multiplication by b?

The (r,s)-entry of L_b is the coefficient of e_r in be_s. But

$$be_s = \left(\sum_{q\neq 0} b_q e_q\right) e_s = \sum_{r\neq 0}\left(\sum_{q:qs=r} b_q\right) e_r,$$

so that the (r,s)-entry of L_b is $\sum_{q:qs=r} b_q$. This proves the next proposition.

PROPOSITION 4.1. *In* (3.4)*, i.e., $A\Delta = 0$, which expresses the weight preservation property of a linear homomorphism $f : C \to R^n$, the matrix Δ equals the matrix associated to left multiplication by $\delta = \sum_{r\neq 0} \delta_r(x) e_r$ in the reduced complex semigroup ring $\mathbb{C}_0[R^\star]$.*

To exploit the equation $A\Delta = 0$, we seek a better basis for $\mathbb{C}_0[R^\star]$. The basic idea is that the reduced semigroup ring $B = \mathbb{C}_0[R^\star]$ is an Artinian algebra over $\mathbb{C}$, whereby it admits a direct sum decomposition, as a left module over itself,

$$ {}_B B = \bigoplus V_i, \tag{4.1}$$

where the V_i are indecomposable left B-modules. Each projective indecomposable V_i in turn admits a composition series whose successive quotients are irreducible left B-modules.

By choosing a vector space basis for B over $\mathbb{C}$ which is adapted to the direct sum decomposition and the composition series, the matrix for the left regular representation will take on a block triangular form. If P is the change of basis matrix, expressing the new adapted basis in terms of the old basis of the e_r's, then $P^{-1}\Delta P$ is the matrix for the left regular representation in terms of the new adapted basis; $P^{-1}\Delta P$ is block triangular. Finally, our weight preservation equation, $A\Delta = 0$, can then be written as

$$(AP)(P^{-1}\Delta P) = 0.$$

This decomposition of $\mathbb{C}_0[R^\star]$ can be made very explicit for chain rings, as we shall see in Section 6. The decomposition of $\mathbb{C}_0[R^\star]$ will be expressed in terms of the Fourier transform, to which we turn next.

5. Fourier transform

Since we will make heavy use of the Fourier transform for finite abelian groups, this section establishes notation and records some standard facts.

Let G be a finite abelian group. A *character* on G is a group homomorphism $\pi : G \to \mathbb{T}$ from G to the multiplicative group of unit complex numbers. The collection of all characters on G, denoted $\widehat{G}$, is itself a finite abelian group under pointwise multiplication. The inverse π^{-1} of π in $\widehat{G}$ is just the complex conjugate $\bar{\pi}$.

Let $f : G \to \mathbb{C}$ be any complex-valued function on G. The *Fourier transform* of f is $\hat{f} : \widehat{G} \to \mathbb{C}$ given by $\hat{f}(\pi) = \sum_{x\in G} f(x)\pi(x)$.

The statement of the Poisson summation formula depends upon a choice of subgroup $H \subset G$. Define the *annihilator* $(\widehat{G} : H)$ of H in $\widehat{G}$ to be

$$(\widehat{G} : H) = \{\pi \in \widehat{G} : \pi(h) = 1,\, h \in H\}.$$

Then $(\widehat{G} : H) \cong \widehat{G/H}$ and $|(\widehat{G} : H)| = |G|/|H|$. The statement that follows, found in [**12**, §1.10, Theorem 10], generalizes [**9**, Lemma 11, p. 144].

THEOREM 5.1 (Poisson Summation Formula). *For every $x \in G$,*

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

6. Decomposing the semigroup ring

Starting in this section, we concentrate on the case where R is a finite chain ring, i.e., a finite commutative local ring with principal maximal ideal $\mathfrak{m} = Rm$. Our main task is to understand the structure of the reduced semigroup ring $\mathbb{C}_0[R^\star]$. What makes this particularly amenable to attack is the relatively simple ideal structure of the ring R. This and other useful facts are summarized in the next result. The reader may supply the proof or refer to [**16**, Lemma 13].

LEMMA 6.1. *Let $(R, \mathfrak{m})$ be a finite chain ring, with $\mathfrak{m} = Rm$. Then the following hold.*

1. *There exists an $l \geq 0$ such that $\mathfrak{m}^l \neq 0$, but $\mathfrak{m}^{l+j} = 0$ for all $j \geq 1$.*
2. *Each ideal $\mathfrak{m}^i$ is principal with $\mathfrak{m}^i = R(m^i)$.*
3. *Every ideal in R is equal to one of the $\mathfrak{m}^i$, $i = 0, 1, \ldots, l+1$.*
4. *R is Frobenius.*

Examples of these rings include all finite fields, the rings $\mathbb{Z}/p^l$ where p is prime, and the Galois rings $GR(p^l, n)$, [**10**, Chapter XVI].

The full group of units $\mathcal{U}$ acts on R on the left by multiplication. The orbits are $\mathcal{U} = R \setminus \mathfrak{m}$ itself, $\mathfrak{m} \setminus \mathfrak{m}^2, \mathfrak{m}^2 \setminus \mathfrak{m}^3, \ldots, \mathfrak{m}^l \setminus 0$, and 0, where $\setminus$ denotes the set-theoretic difference. Set $\mathcal{O}_0 = \mathcal{U} = R \setminus \mathfrak{m}$, $\mathcal{O}_i = \mathfrak{m}^i \setminus \mathfrak{m}^{i+1}$, and $\mathcal{O}_{l+1} = 0$. Also, set $M_i = |\mathcal{O}_i|$.

Define a relation $\leq$ on R by $y \leq x$ if $y = ax$ for some $a \in R$. The relation $\leq$ is reflexive and transitive, and $x \leq y$, $y \leq x$ implies that x, y lie in the same $\mathcal{U}$-orbit. Thus we see that $\leq$ induces a well-defined partial ordering on the set of $\mathcal{U}$-orbits of R. This works for any finite ring ([**15**]). What is special for R is that $\leq$ is actually a total ordering, with

$$0 = \mathcal{O}_{l+1} \leq \mathcal{O}_l \leq \mathcal{O}_{l-1} \leq \cdots \leq \mathcal{O}_1 \leq \mathcal{O}_0.$$

We now write down a new basis for the reduced semigroup ring $B = \mathbb{C}_0[R^\star]$. For a character π of the group of units $\mathcal{U}$ and an orbit $\mathcal{O}_i$, we say that the pair $(\pi, \mathcal{O}_i)$ is *admissible* if the pointwise stabilizer subgroup $\mathcal{U}_i = \mathrm{Stab}(\mathcal{O}_i)$ of the orbit $\mathcal{O}_i$ is contained in $\ker \pi$. Because R is commutative, $\mathcal{U}_i$ depends only upon the orbit $\mathcal{O}_i$, not on a particular element in the orbit. Note that $\mathcal{U}_i \subset \mathcal{U}_{i+1}$.

Another way to say that the pair $(\pi, \mathcal{O}_i)$ is admissible is that $\pi \in (\widehat{\mathcal{U}} : \mathcal{U}_i)$. Since $|(\widehat{\mathcal{U}} : \mathcal{U}_i)| = |\mathcal{U}|/|\mathcal{U}_i| = |\mathcal{O}_i|$, we see that the number of admissible pairs equals $|R|$. The zero orbit $\mathcal{O}_{l+1}$ has $\mathcal{U}_{l+1} = \mathcal{U}$, so that the trivial character $\pi = 1$ is the only admissible character for $\mathcal{O}_{l+1} = 0$. In dealing with the reduced semigroup ring $\mathbb{C}_0[R^\star]$, the admissible pair $(\pi = 1, \mathcal{O}_{l+1} = 0)$ will be dropped, leaving $|R| - 1 = \dim \mathbb{C}_0[R^\star]$ other admissible pairs.

For each admissible pair $(\pi, \mathcal{O}_i)$, $\pi \in (\widehat{\mathcal{U}} : \mathcal{U}_i)$, define an *admissible orbit sum* by

$$s(\pi, \mathcal{O}_i) = \frac{1}{M_i} \sum_{u \in \mathcal{U}/\mathcal{U}_i} \pi(u) e_{um^i} \in \mathbb{C}_0[R^\star].$$

Recall that $M_i = |\mathcal{O}_i|$, and note that $\mathcal{O}_i = \{um^i : u \in \mathcal{U}/\mathcal{U}_i\}$. Also, $\pi(u)$ for $u \in \mathcal{U}/\mathcal{U}_i$ is well-defined, since $\pi \in (\widehat{\mathcal{U}} : \mathcal{U}_i)$. Notice that $(\pi, \mathcal{O}_0)$ is admissible for every $\pi \in \widehat{\mathcal{U}}$, since $\mathcal{U}_0 = \{1\}$.

For any character $\pi \in \widehat{\mathcal{U}}$, let i_π be the largest integer j such that $(\pi, \mathcal{O}_j)$ is admissible. That is, $\mathcal{U}_{i_\pi} \subset \ker \pi$, but $\mathcal{U}_j \not\subset \ker \pi$ for $j > i_\pi$.

PROPOSITION 6.2. *For any element $b = \sum_{r \neq 0} b_r e_r$ in $\mathbb{C}_0[R^\star]$, and for any admissible orbit sum $s(\pi, \mathcal{O}_i)$, their product satisfies the following formula.*

$$b\, s(\pi, \mathcal{O}_i) = \sum_{k=0}^{i_\pi - i} \left(\sum_{u \in \mathcal{U}/\mathcal{U}_k} b_{um^k} \bar{\pi}(u) \right) s(\pi, \mathcal{O}_{i+k}).$$

PROOF. Group the terms of $b = \sum_{r \neq 0} b_r e_r$ into sums over orbits:

$$b = \sum_{k=0}^{l} \sum_{u \in \mathcal{U}/\mathcal{U}_k} b_{um^k} e_{um^k}.$$

Now focus on the product

$$\left(\sum_{u \in \mathcal{U}/\mathcal{U}_k} b_{um^k} e_{um^k} \right) s(\pi, \mathcal{O}_i) = \frac{1}{M_i} \sum_{u \in \mathcal{U}/\mathcal{U}_k} \sum_{v \in \mathcal{U}/\mathcal{U}_i} b_{um^k} \pi(v) e_{uvm^{i+k}}. \tag{6.1}$$

We wish to know the coefficient of $e_{wm^{i+k}}$, where $w \in \mathcal{U}/\mathcal{U}_{i+k}$. This term will arise from $u \in \mathcal{U}/\mathcal{U}_k$, $v \in \mathcal{U}/\mathcal{U}_i$, which satisfy $uv = w$ in $\mathcal{U}/\mathcal{U}_{i+k}$.

For fixed $w \in \mathcal{U}/\mathcal{U}_{i+k}$ and fixed $u \in \mathcal{U}/\mathcal{U}_k$, select one solution $v_0 \in \mathcal{U}/\mathcal{U}_i$ so that $uv_0 = w$. The other solutions $v = v_0 x$ for $uv = w$ are parameterized by elements x in the kernel $\mathcal{U}_{i+k}/\mathcal{U}_i$ of the natural surjection $\mathcal{U}/\mathcal{U}_i \to \mathcal{U}/\mathcal{U}_{i+k}$. In (6.1) there will then be a term of the form

$$\sum_{x \in \mathcal{U}_{i+k}/\mathcal{U}_i} \pi(v_0 x) = \begin{cases} (M_i/M_{i+k})\pi(v_0), & \pi \in (\widehat{\mathcal{U}} : \mathcal{U}_{i+k}), \\ 0, & \pi \notin (\widehat{\mathcal{U}} : \mathcal{U}_{i+k}). \end{cases}$$

When $\pi \in (\widehat{\mathcal{U}} : \mathcal{U}_{i+k})$, the value $\pi(v_0)$ depends only on u, w, in which case $\pi(v_0) = \bar{\pi}(u)\pi(w)$. Then the expression in (6.1) simplifies to

$$\left(\sum_{u \in \mathcal{U}/\mathcal{U}_k} b_{um^k} e_{um^k} \right) s(\pi, \mathcal{O}_i) = \begin{cases} \left(\sum_{u \in \mathcal{U}/\mathcal{U}_k} b_{um^k} \bar{\pi}(u) \right) s(\pi, \mathcal{O}_{i+k}), & \pi \in (\widehat{\mathcal{U}} : \mathcal{U}_{i+k}), \\ 0, & \pi \notin (\widehat{\mathcal{U}} : \mathcal{U}_{i+k}). \end{cases}$$

From this the desired formula follows. □

THEOREM 6.3. *The structure of the Artinian ring $\mathbb{C}_0[R^\star]$ has the following features.*

(1) *The admissible orbit sums $s(\pi, \mathcal{O}_0)$, $\pi \in \widehat{\mathcal{U}}$, are primitive orthogonal idempotents in $\mathbb{C}_0[R^\star]$ whose sum equals 1.*

(2) *For each character $\pi \in \widehat{\mathcal{U}}$, the subspace spanned by the admissible orbit sums $s(\pi, \mathcal{O}_i)$ is the projective indecomposable submodule V_π generated by the idempotent $s(\pi, \mathcal{O}_0)$.*

(3) *For each character $\pi \in \widehat{\mathcal{U}}$, let i_π be the largest integer such that $(\pi, \mathcal{O}_{i_\pi})$ is admissible. Then $(\pi, \mathcal{O}_i)$ is admissible for $i \le i_\pi$. Moreover, the subspaces V_π^i spanned by $s(\pi, \mathcal{O}_i), s(\pi, \mathcal{O}_{i+1}), \ldots, s(\pi, \mathcal{O}_{i_\pi})$ are submodules of $\mathbb{C}_0[R^\star]$, with $\dim_{\mathbb{C}} V_\pi^i = i_\pi - i + 1$. The submodules V_π^i form a composition series for V_π:*

$$V_\pi = V_\pi^0 \supset V_\pi^1 \supset \cdots \supset V_\pi^{i_\pi} \supset 0.$$

(4) *The left regular representation for an element $b = \sum_{r \neq 0} b_r e_r \in \mathbb{C}_0[R^\star]$, expressed in terms of the basis of admissible orbit sums, has the block diagonal form*

$$\begin{pmatrix} \ddots & & \\ & N_\pi & \\ & & \ddots \end{pmatrix},$$

where each N_π is lower triangular of size $(i_\pi + 1) \times (i_\pi + 1)$. The matrix N_π has the form

$$N_\pi = \begin{pmatrix} \hat{b}(\bar{\pi}, 0) & 0 & 0 & \cdots & 0 \\ \hat{b}(\bar{\pi}, 1) & \hat{b}(\bar{\pi}, 0) & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ \hat{b}(\bar{\pi}, i_\pi - 1) & \hat{b}(\bar{\pi}, i_\pi - 2) & \cdots & \hat{b}(\bar{\pi}, 0) & 0 \\ \hat{b}(\bar{\pi}, i_\pi) & \hat{b}(\bar{\pi}, i_\pi - 1) & \cdots & \hat{b}(\bar{\pi}, 1) & \hat{b}(\bar{\pi}, 0) \end{pmatrix},$$

where

$$\hat{b}(\bar{\pi}, j) = \sum_{u \in \mathcal{U}/\mathcal{U}_j} b_{um^j} \bar{\pi}(u), \quad j = 0, 1, \ldots, i_\pi.$$

PROOF. With the exception of the idempotents $s(\pi, \mathcal{O}_0)$ being primitive, all these statements follow immediately from the formula in Proposition 6.2 and the orthogonality relations on characters.

Since the idempotents $s(\pi, \mathcal{O}_0)$, $\pi \in \widehat{\mathcal{U}}$, are orthogonal, the Artinian ring $B = \mathbb{C}_0[R^\star]$ splits as a direct sum of rings:

$$B = \bigoplus_{\pi \in \widehat{\mathcal{U}}} Bs(\pi, \mathcal{O}_0).$$

The idempotent $s(\pi, \mathcal{O}_0)$ is primitive if and only if the ring $Bs(\pi, \mathcal{O}_0)$ is local.

Inside $Bs(\pi, \mathcal{O}_0)$ consider the subspace V_π^1; it is clearly an ideal. Every element $x \in Bs(\pi, \mathcal{O}_0)$ has the form $x = x_0 s(\pi, \mathcal{O}_0) + x'$, where $x_0 \in \mathbb{C}$ and $x' \in V_\pi^1$. Standard arguments show that x is a unit in $Bs(\pi, \mathcal{O}_0)$ if and only if $x_0 \neq 0$. Thus x is a unit if and only if $x \notin V_\pi^1$. This implies that $Bs(\pi, \mathcal{O}_0)$ is a local ring with maximal ideal V_π^1, as desired. □

7. Extension theorem

We continue to assume that $(R, \mathfrak{m})$ is a finite chain ring with $\mathfrak{m} = Rm$. We also assume that w is a weight function of the typical form $w(x) = \sum a_r c_r(x)$. In the next result, please be aware that the subgroup U need *not* be a subgroup of $\mathrm{Sym}(w)$, the symmetry group of w.

THEOREM 7.1. *Let U be any subgroup of $\mathcal{U}$. Suppose the weight function w satisfies $\hat{a}(\pi, i_\pi) = \sum_{u \in \mathcal{U}/\mathcal{U}_{i_\pi}} a_{um^{i_\pi}} \pi(u) \neq 0$ for all $\pi \in (\widehat{\mathcal{U}} : U)$. Then for any right linear code $C \subset R^n$, every injective right linear homomorphism $f : C \to R^n$ which preserves w extends to a U-monomial transformation on R^n.*

PROOF. In the general developments described above, the approach is to utilize the weight preservation equation $A\Delta = 0$ in order to show that the symmetrized weight composition determined by U is preserved. The result will then follow from the extension theorem for weight compositions, Theorem 2.5.

We make use of Theorem 6.3 to pick a better basis for $\mathbb{C}_0[R^\star]$: the basis consisting of the admissible orbit sums $s(\pi, \mathcal{O}_j)$, $\pi \in \widehat{\mathcal{U}}$, $j = 0, 1, \ldots, i_\pi$. Then $A\Delta = 0$ implies $(AP)(P^{-1}\Delta P) = 0$, where P is the change of basis matrix whose columns are the coefficients of the new basis elements $s(\pi, \mathcal{O}_j)$ in terms of the old basis elements e_r.

The entries of the row vector AP are simply $\hat{a}(\pi, i)/M_i$, where

$$\hat{a}(\pi, i) = \sum_{u \in \mathcal{U}/\mathcal{U}_i} a_{um^i} \pi(u).$$

The matrix $P^{-1}\Delta P$ is block triangular, as in Therorem 6.3.

For a fixed character π, the block parameterized by π in the matrix equation $(AP)(P^{-1}\Delta P) = 0$ yields the following system of equations:

$$\begin{aligned}
\frac{1}{M_0}\hat{a}(\pi,0)\hat{\delta}(\bar{\pi},0) + \frac{1}{M_1}\hat{a}(\pi,1)\hat{\delta}(\bar{\pi},1) + \cdots + \frac{1}{M_{i_\pi}}\hat{a}(\pi,i_\pi)\hat{\delta}(\bar{\pi},i_\pi) &= 0 \\
\frac{1}{M_1}\hat{a}(\pi,1)\hat{\delta}(\bar{\pi},0) + \cdots + \frac{1}{M_{i_\pi}}\hat{a}(\pi,i_\pi)\hat{\delta}(\bar{\pi},i_\pi - 1) &= 0 \\
\vdots &= \vdots \\
\frac{1}{M_{i_\pi}}\hat{a}(\pi,i_\pi)\hat{\delta}(\bar{\pi},0) &= 0.
\end{aligned}$$

Since we are assuming that $\hat{a}(\pi, i_\pi) \neq 0$ for all $\pi \in (\widehat{\mathcal{U}} : U)$, we see by induction that $\hat{\delta}(\bar{\pi}, j) = 0$ for $\pi \in (\widehat{\mathcal{U}} : U)$ and $j = 0, 1, \ldots, i_\pi$. Note that $(\pi, \mathcal{O}_j)$ being admissible for $\pi \in (\widehat{\mathcal{U}} : U)$ means that $\pi \in (\widehat{\mathcal{U}} : \mathcal{U}_j)$ as well, so that $\pi \in (\widehat{\mathcal{U}} : U \cdot \mathcal{U}_j)$.

We now apply the Poisson summation formula, Theorem 5.1. The difference $\mathrm{swc}_t(f(x)) - \mathrm{swc}_t(x)$ of the symmetrized weight compositions has the form

$$\mathrm{swc}_t(f(x)) - \mathrm{swc}_t(x) = \sum_{r \in \mathrm{orb}(t)} (c_r(f(x)) - c_r(x)) = \sum_{r \in \mathrm{orb}(t)} \delta_r(x).$$

More than just a sum over a U-orbit, it is, in fact, a sum over the coset of t for the subgroup $U/(U \cap \mathcal{U}_t)$ of $\mathcal{U}/\mathcal{U}_t$. (We write $\mathcal{U}_t$ for the stabilizer subgroup of t in $\mathcal{U}$. The $\mathcal{U}$-orbit of t is some $\mathcal{O}_i$. The characters of $\mathcal{U}/\mathcal{U}_t$ are exactly those characters for which $(\pi, \mathcal{O}_i)$ is admissible.) The Poisson summation formula states that coset sums are equal to sums of transforms over annihilators. Since we know that $\hat{\delta}(\bar{\pi}, j) = 0$ for $\pi \in (\widehat{\mathcal{U}} : U)$ and $j = 0, 1, \ldots, i_\pi$, these sums of transforms over annihilators vanish. Thus the symmetrized weight composition is preserved, and the theorem follows from Theorem 2.5. □

COROLLARY 7.2. *Suppose w is any weight function with $a_r > 0$ for $r \neq 0$. Then any weight preserving linear homomorphism on a submodule extends to a monomial transformation.*

PROOF. Taking $U = \mathcal{U}$, we see that the only character in $(\widehat{\mathcal{U}} : U)$ is the trivial character $\pi = 1$. For $\pi = 1$, it is clear that $\hat{a}(\pi, i_\pi) \neq 0$, since it equals a sum of positive a_r's. □

The solution of the extension problem now follows from Theorem 7.1 simply by taking U to be the symmetry group of the weight function w. We record this result next.

THEOREM 7.3 (Extension Theorem). *Let $U = \mathrm{Sym}(w)$, the symmetry group of the weight function w. If $\hat{a}(\pi, i_\pi) = \sum_{u \in \mathcal{U}/\mathcal{U}_{i_\pi}} a_{um^{i_\pi}} \pi(u) \neq 0$ for all $\pi \in (\widehat{\mathcal{U}} : U)$, then the extension problem is solvable for w.*

REMARK 7.4. Suppose we are in the situation of Theorem 7.1, where U is some subgroup of $\mathcal{U}$ and $\hat{a}(\pi, i_\pi) \neq 0$ for all $\pi \in (\widehat{\mathcal{U}} : U)$. Then any $f : C \to R^n$ which preserves w extends to a U-monomial transformation on R^n. Beware that the extension of f need not preserve w on all of R^n (a priori, just on C). But if U is a subgroup of the symmetry group of w, then Proposition 2.6 applies to show that the extension also preserves w on R^n.

8. Examples

We conclude with some examples which illustrate both the uses and the limitations of the theorems of Section 7.

EXAMPLE 8.1. Let $R = \mathbb{Z}/2^{l+1}$. This is a finite chain ring with $\mathfrak{m} = (2)$. If we concentrate on the case where $U = \mathcal{U}$, then only the trivial character $\pi = 1$ arises in $(\widehat{\mathcal{U}} : U)$. For $\pi = 1$, $i_\pi = l$, and $\hat{a}(\pi, i_\pi) = a_{2^l}$. Thus, as long as $a_{2^l} \neq 0$, Theorem 7.1 says that a weight preserving $f : C \to R^n$ extends to a monomial transformation. As in Remark 7.4, the extension may not preserve the weight function on all of R^n.

A similar result holds for $R = \mathbb{Z}/p^{l+1}$ with p prime. The condition on w is that

$$a_{p^l} + a_{2p^l} + \cdots + a_{(p-1)p^l} \neq 0. \tag{8.1}$$

EXAMPLE 8.2. In [**4**], Constantinescu, Heise, and Honold prove an extension theorem for what they call *homogeneous* weight functions on $\mathbb{Z}/m$. For the case where $m = p^{l+1}$ is a prime power, it is a direct consequence of the definition that homogeneous weight functions satisfy (8.1). Thus the extension theorem in [**4**], in the case where $m = p^{l+1}$, also follows from Theorem 7.1.

EXAMPLE 8.3. Here is a further illustration of Remark 7.4. Let $R = \mathbb{F}_5$ and take $a_i = i$, for $i = 0, 1, 2, 3, 4$. The symmetry group of w is trivial.

In R^2, let C be the vector subspace spanned by the vector $(1, 4)$, so that

$$C = \{(0,0), (1,4), (2,3), (3,2), (4,1)\}.$$

Every non-zero vector in C has $w(x) = 5$. Thus the linear transformation $f : C \to R^2$ determined by $f(1,4) = (2,3)$ preserves w. Corollary 7.2 says that f extends to a monomial transformation. In fact, f extends to $2I$, i.e., scalar multiplication by 2. But $2I$ does not preserve w on all of R^2.

Now let us try to apply the extension theorem with $U = \{1\}$, the symmetry group of w. The group of units $\mathcal{U}$ is cyclic of order 4, and every character $\pi \in \widehat{\mathcal{U}}$ is admissible. In particular, consider the character π of order 2 in $\mathcal{U}$: $\pi(2^j) = (-1)^j$, for $j = 0, 1, 2, 3$. We then compute that

$$\hat{a}(\pi) = a_1 - a_2 + a_4 - a_3 = 0.$$

Thus the extension theorem does not apply.

It is easy to verify that the group of weight preserving automorphisms on R^2 is precisely the symmetric group Σ_2. Since f is not the restriction of a permutation, f does not extend to a weight preserving automorphism.

EXAMPLE 8.4. Let $R = \mathbb{Z}/8$, with $U = \pm 1$, as for the Lee or Euclidean weight functions. The nonzero U-orbits are $\{1, 7\}$, $\{3, 5\}$, $\{2, 6\}$, and $\{4\}$. We assume $U \subset \mathrm{Sym}(w)$, so that $a_1 = a_7$, etc. Since R is commutative, the matrix $\mathcal{A}$ of Remark 3.2 is:

$$\mathcal{A} = \begin{pmatrix} a_1 & a_3 & a_2 & a_4 \\ a_3 & a_1 & a_2 & a_4 \\ a_2 & a_2 & a_4 & 0 \\ a_4 & a_4 & 0 & 0 \end{pmatrix}.$$

Then $\det \mathcal{A} = 2a_4^3(a_3 - a_1)$. This determinant is clearly nonzero for the Lee and Euclidean weight functions, so Theorem 3.1 implies the extension theorem in this case.

Similarly explicit calculations can be made for other small chain rings, proving the extension theorem in those settings. What is still missing is a uniform approach to the Lee and Euclidean weight functions for all chain rings.

REMARK 8.5. Notice that the factors of $\det \mathcal{A}$ above are exactly the $\hat{a}$'s which occur in Theorem 7.1. This pattern has appeared in all the calculations that the author has performed on various chain rings. For chain rings, we conjecture that $\det \mathcal{A}$ always factors into a product of $\hat{a}$'s, and hence that Theorem 3.1 and Theorem 7.1 are equivalent, provided $U \subset \mathrm{Sym}(w)$.

REMARK 8.6 (Added in proof). For chain rings, the conjecture in Remark 8.5 is true. This result will appear in subsequent work of the author.

References

[1] Č. Arf, *Untersuchungen über quadratische Formen in Körpern der Charakteristik* 2. I., J. Reine Angew. Math. **183** (1941), 148–167.

[2] 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.

[3] A. R. Calderbank, A. R. Hammons, Jr., P. V. Kumar, N. J. A. Sloane, and P. Solé, *A linear construction for certain Kerdock and Preparata codes*, Bull. Amer. Math. Soc. (N. S.) **29** (1993), 218–222.

[4] I. Constantinescu, W. Heise, and Th. Honold, *Monomial extensions of isometries between codes over* $\mathbb{Z}_m$, Proceedings of the Fifth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT '96) (Sozopol, Bulgaria), Unicorn, Shumen, 1996, pp. 98–104.

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

[6] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The* $\mathbb{Z}_4$*-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **IT-40** (1994), 301–319.

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

[8] ———, *Combinatorial problems of elementary abelian groups*, Ph.D. thesis, Radcliffe College, Cambridge, Mass., 1962.
[9] ——— and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland Mathematical Library, vol. 16, North-Holland, Amsterdam, New York, Oxford, 1978.
[10] B. R. McDonald, *Finite rings with identity*, Pure and Applied Mathematics, vol. 28, Marcel Dekker, Inc., New York, 1974.
[11] T. Nakayama, *On Frobeniusean algebras.* I., Ann. of Math. (2) **40** (1939), 611–633; II., **42** (1941), 1–21.
[12] A. Terras, *Fourier analysis on finite groups and applications*, UCSD lecture notes, 1992.
[13] H. N. Ward and J. A. Wood, *Characters and the equivalence of codes*, J. Combin. Theory Ser. A **73** (1996), 348–352.
[14] E. Witt, *Theorie der quadratischen Formen in beliebigen Körpern*, J. Reine Angew. Math. **176** (1937), 31–44.
[15] J. A. Wood, *Duality for modules over finite rings and applications to coding theory*, submitted.
[16] ———, *Extension theorems for linear codes over finite rings*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (T. Mora and H. Mattson, eds.), Springer-Verlag, Berlin, 1997, LNCS 1255, pp. 329–340.
[17] ———, *Semigroup rings and the extension theorem for linear codes*, Proceedings of the Thirty-Fifth Allerton Conference on Communication, Control, and Computing, 1997, to appear.

Department of Mathematics, Computer Science & Statistics, Purdue University Calumet, Hammond, Indiana 46323–2094 USA
E-mail address: wood@calumet.purdue.edu