Extension Theorems for Linear Codes over Finite Rings

Jay A. Wood*

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

Abstract. Various forms of the extension problem are discussed for linear codes defined over finite rings. The extension theorem for symmetrized weight compositions over finite Frobenius rings is proved. As a consequence, an extension theorem for weight functions over certain finite commutative rings is also proved. The proofs make use of the linear independence of characters as well as the linear independence of characters averaged over the orbits of a group action.

1 Introduction

Witt [14] and Arf [1] were among the first mathematicians to prove extension theorems in algebra. If V is a finite dimensional vector space over a field and if V is equipped with a non-degenerate quadratic form Q, then for any subspace $W \subset V$, Arf proved that every injective linear transformation $f : W \to V$ which preserves Q extends to a linear automorphism of V which preserves Q.

MacWilliams was the first mathematician to prove an extension theorem in coding theory [9], [10]. If V is a finite dimensional vector space over a finite field, then a choice of basis determines the Hamming weight on V. For any subspace $W \subset V$ and any (injective) linear transformation $f : W \to V$ which preserves Hamming weight, MacWilliams proved that f extends to a linear automorphism of V which preserves Hamming weight; i.e., the extension of f is a monomial transformation. This theorem became the cornerstone of the idea of equivalence of codes.

There have been other proofs of this extension theorem of MacWilliams, for example [3], [6], [13]. Motivated by the increased interest in linear codes defined over finite rings sparked by the famous $\mathbb{Z}/4$-paper [8], the author proved the extension theorem for Hamming weight over finite Frobenius rings [15].

All the results mentioned above deal with the Hamming weight. Other weight functions such as the Lee weight are also important in coding theory. The author's ultimate goal is to prove an extension theorem for weight functions over finite rings in as general a context as possible. In very broad terms, here is

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

what an extension problem is: Suppose we are given a finite ring R and some notion of *weight* w on R^n; regard w as a function defined on R^n. For every submodule C in R^n and every injective linear homomorphism $f : C \to R^n$ which preserves w, *is it the case that f extends to a linear automorphism of R^n which preserves w?* This paper presents extension theorems for symmetrized weight compositions over finite Frobenius rings and for weight functions over certain finite commutative rings, those which are local principal ideal rings.

As was done in [13] and [15], characters will be used to prove the extension theorem for symmetrized weight compositions. In particular, an averaging process will be applied to characters in order to handle any symmetry present. Goldberg [7] has proved this form of the extension theorem over finite fields. His proof used the methods developed in [3].

As an application of this extension theorem for symmetrized weight compositions, we will prove a special case of the extension theorem for weight functions over finite commutative local principal ideal rings. This class of rings includes the finite fields, $\mathbb{Z}/p^n$ for p prime, and Galois rings. In particular, $\mathbb{Z}/4$, the ring investigated in [8], is included. The theorem itself is not the best possible. The author has more general results, but they require additional techniques which are better developed in a separate paper (see [16]). This extension theorem complements the extension theorem for homogeneous weight functions over $\mathbb{Z}/m$ proved by Constantinescu, Heise, and Honold [4]. In addition we state a criterion for solving the extension problem over more general rings. At present, this criterion seems to be too general to be very useful.

2 Hamming Weight

Conventions. All rings R will be finite and associative with 1. We let $\mathcal{U}$ be the group of units of R. Since R is finite, all units in R are necessarily two-sided. The 1-dimensional torus $\mathbf{T}$ is the multiplicative group of unit complex numbers; the complex conjugate of z is $\overline{z}$. We denote by $|S|$ the number of elements in a finite set S. The ring of integers modulo m will be denoted by $\mathbb{Z}/m$.

This section serves the purpose of reviewing notation and summarizing what is known about the extension theorem for the Hamming weight. Refer to [15] for further details.

Let R be a ring and let R^n be the free R-module of rank n consisting of all n-tuples of elements from R. A right *linear code* C is a right submodule of R^n. The *complete weight composition* of an element $x = (x_1, \ldots, x_n) \in R^n$ is a function $n : R^n \times R \to \mathbb{Z}$ given by

$$n_r(x) = |\{i : x_i = r\}|, \quad x \in R^n, \quad r \in R \ . \tag{1}$$

That is, $n_r(x)$ counts the number of components of x which equal the ring element $r \in R$. The *Hamming weight* $\mathrm{wt}(x)$ of $x \in R^n$ is given by $\mathrm{wt}(x) = \sum_{r \neq 0} n_r(x)$; it counts the number of non-zero components of x.

A right linear automorphism $f : R^n \to R^n$ is a right *monomial transformation* if there exist units $u_1, \ldots, u_n \in \mathcal{U}$ and a permutation σ of $\{1, 2, \ldots, n\}$ such that

$$f(x_1, \ldots, x_n) = (u_1 x_{\sigma(1)}, \ldots, u_n x_{\sigma(n)}), \quad (x_1, \ldots, x_n) \in R^n \ . \tag{2}$$

If U is a subgroup of $\mathcal{U}$ and $u_1, \ldots, u_n \in U$, we say that f is a *U-monomial transformation*.

We also make use of some additional structure which is discussed at length in [15]. The *character group* $\widehat{R} = \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{T})$ consists of all *characters* on R, i.e., group homomorphisms from R to $\mathbb{T}$. In fact, $\widehat{R}$ is a bimodule over R, via the scalar multiplications $({}^r\pi)(x) = \pi(xr)$ and $\pi^r(x) = \pi(rx)$. The ring R is a *Frobenius* ring if $\widehat{R}$ is isomorphic to R as one-sided modules. In that case, there exists a *generating character* χ on R with the property that $r \mapsto \chi^r$ is a right linear isomorphism from R to $\widehat{R}$. Examples of Frobenius rings include finite fields, $\mathbb{Z}/m$, and Galois rings. The class of Frobenius rings is closed under forming finite direct sums, under forming matrix rings ($R \rightsquigarrow M_n(R)$), and under forming finite group rings ($R \rightsquigarrow R[G]$). If the ring is also commutative, being Frobenius is equivalent to being quasi-Frobenius (i.e., self-injective) or Gorenstein.

The next theorem summarizes the extension theorem for Hamming weight. The proof is in [15], Theorem 6.1.

Theorem 1. (i) *Suppose $f : R^n \to R^n$ is a right linear automorphism of R^n. Then f preserves* wt*, i.e.,* $\mathrm{wt}(f(x)) = \mathrm{wt}(x)$ *for all $x \in R^n$, if and only if f is a right monomial transformation.*

(ii) *Assume R is Frobenius. Suppose C is a right linear code in R^n and $f : C \to R^n$ is any injective linear homomorphism which preserves* wt*. Then f extends to a right monomial transformation on R^n.*

Observe that the injectivity of f follows from weight preservation. Indeed, the zero vector is the only vector satisfying $\mathrm{wt}(x) = 0$.

Remark 2. In case the ring R is commutative, there is a converse to part (ii) of Theorem 1. That is, if every weight-preserving $f : C \to R^n$ extends to a monomial transformation, then R is necessarily a Frobenius ring ([15], Theorem 6.2).

Consider the non-Frobenius ring $R = \mathbb{F}_2[X, Y]/(X^2, XY, Y^2)$, with $C = (X)$ and $f : C \to R$ given by $f(X) = Y$. This f preserves Hamming weight, but it does not extend to a monomial transformation.

3 Weight Compositions

In this section we discuss the extension problem for symmetrized weight compositions. The extension theorem for symmetrized weight compositions, which we prove in Sect. 5, will be useful in proving the extension theorems for weight functions that occur in later sections.

We will encode symmetry into coding theory by means of a subgroup $U \subset \mathcal{U}$ of the group of units of R; this approach is suggested by [2], pp. 33–34. Left

multiplication by $u \in U$, $r \mapsto ur$, defines a left action of the group U on R; in fact, each $u \in U$ acts as an additive automorphism of R. We write $r \approx s$ if $s = ur$ for some $u \in U$; $\approx$ is an equivalence relation. The *orbit* of r under U is

$$\mathrm{orb}(r) = \{s \in R : s \approx r\} \ .$$

The *symmetrized weight composition* determined by the subgroup U is the function $\mathrm{swc} : R^n \times R \to \mathbb{Z}$ given by

$$\mathrm{swc}_r(x) = \sum_{s \in \mathrm{orb}(r)} n_s(x) \ ;$$

the complete weight composition $n_r(x)$ was defined in (1). If $s \in \mathrm{orb}(r)$, then $\mathrm{swc}_s = \mathrm{swc}_r$. The integers $\mathrm{swc}_r(x)$ are the exponents which appear in symmetrized weight enumerators (e.g., [5], p. 35). We emphasize that the symmetrized weight composition swc depends on the choice of subgroup U.

We now assume that R is equipped with the symmetrized weight composition swc arising from a subgroup $U \subset \mathcal{U}$.

Proposition 3. *Let $f : R^n \to R^n$ be a right linear automorphism. Then f preserves* swc*, i.e.,* $\mathrm{swc}_r(f(x)) = \mathrm{swc}_r(x)$*, for all $x \in R^n$, $r \in R$, if and only if f is a U-monomial transformation.*

Proof. "If": obvious. "Only if": Consider $x = e_i = (0, \ldots, 1, \ldots, 0)$, the vector with a single 1, in position i. Then the preservation of swc forces $f(e_i)$ to have exactly one non-zero component, and this component must be in $\mathrm{orb}(1)$. That means the non-zero component is an element of U. Since f was assumed to be an automorphism, it is now clear that f is a U-monomial transformation. □

Here is the extension problem which we address in Sect. 5.

Extension Problem. *Suppose $C \subset R^n$ is a right linear code and $f : C \to R^n$ is an injective right linear homomorphism which preserves* swc*. Does f extend to a U-monomial transformation on R^n?*

Since $x = 0$ is the only element in R^n for which $\mathrm{swc}_r(x) = 0$ for all $r \in R$, any f which preserves swc is automatically injective.

Remark 4. It is relatively easy to show that an f which preserves swc extends to a $\mathcal{U}$-monomial transformation. Indeed, since f preserves swc, f also preserves the Hamming weight $\mathrm{wt} = \sum_{r \neq 0} \frac{1}{|\mathrm{orb}(r)|} \mathrm{swc}_r$. By Theorem 1, f extends to a $\mathcal{U}$-monomial transformation on R^n.

At this point one is tempted to apply Proposition 3 in order to conclude that f is actually a U-monomial transformation. Alas, while we know that f preserves swc on the linear code C, we do not know that its extension preserves swc on all of R^n.

4 Averaging Characters over Orbits

This section begins by reviewing some facts about characters on finite abelian groups. Then an averaging process is discussed. Proofs of standard results are omitted. The reader is referred to Serre's books, [11], [12], for more details.

Let G be a finite abelian group, written with additive notation. A *character* on G is a group homomorphism $\pi : G \to \mathbf{T}$. The collection $\widehat{G} = \mathrm{Hom}_{\mathbf{Z}}(G, \mathbf{T})$ of all characters on G is itself a finite abelian group under pointwise multiplication. The inverse of $\pi \in \widehat{G}$ is $\overline{\pi}(x) = \overline{\pi(x)}$, the complex conjugate of π. A standard fact that will be used in Sect. 5 is

Lemma 5.

$$\sum_{\pi \in \widehat{G}} \pi(x) = \begin{cases} |G|, & x = 0 \ , \\ 0, & x \neq 0 \ . \end{cases}$$

Let $\mathcal{F} = \{f : G \to \mathbb{C}\}$ be the vector space of all complex-valued functions on G; $\dim_{\mathbb{C}} \mathcal{F} = |G|$. We equip $\mathcal{F}$ with a positive definite hermitian inner product

$$\langle f, g \rangle = \frac{1}{|G|} \sum_{x \in G} f(x)\, \overline{g(x)} \ .$$

Another standard result is

Lemma 6. *The characters of G form an orthonormal basis for $\mathcal{F}$ with respect to $\langle , \rangle$. In particular, the characters are linearly independent.*

We now introduce some symmetry by fixing a subgroup U of the automorphism group of G. View U as acting on G on the left, with an element $u \in U$ being an automorphism $u : x \mapsto ux = u(x)$ of G. Denote the *orbit* of $x \in G$ by

$$\mathrm{orb}(x) = \{ux : u \in U\} \ .$$

The left action of U on G induces a right action of U on $\mathcal{F}$, written $u : f \mapsto f^u$, where $f^u(x) = f(ux)$. The fixed points of this latter action are the U-invariant functions

$$\mathcal{F}^U = \{f \in \mathcal{F} : f(ux) = f(x), u \in U, x \in G\} \ ;$$

the U-invariant functions are constant on any orbit of U. Being a vector subspace of $\mathcal{F}$, $\mathcal{F}^U$ inherits the inner product $\langle , \rangle$. We now define a projection $P : \mathcal{F} \to \mathcal{F}^U$, as follows. For $f \in \mathcal{F}$,

$$\begin{aligned} (Pf)(x) &= \frac{1}{|\mathrm{orb}(x)|} \sum_{y \in \mathrm{orb}(x)} f(y) = \frac{1}{|U|} \sum_{u \in U} f(ux) \\ &= \frac{1}{|U|} \sum_{u \in U} f^u(x) = \frac{1}{|\mathrm{orb}(f)|} \sum_{g \in \mathrm{orb}(f)} g(x) \ . \end{aligned}$$

It is easy to verify that P is indeed a linear projection, i.e., $P \circ P = P$. However, P is not an orthogonal projection.

Lemma 7. *If $g = f^u$ for some $u \in U$, then $Pg = Pf$.*

Proof. Pf is the average of the functions in $\mathrm{orb}(f)$. But $\mathrm{orb}(g) = \mathrm{orb}(f)$, since $g = f^u$. □

Proposition 8. *Suppose π, ψ are two characters on G. Then $\psi = \pi^u$, for some $u \in U$, if and only if $P\psi = P\pi$.*

Proof. The "only if" direction is part of Lemma 7. For the "if" direction, suppose $P\psi = P\pi$. Then

$$\sum_{u \in U} \psi^u = \sum_{v \in U} \pi^v \quad .$$

But all the functions ψ^u, π^v are still characters on G, since U acts as automorphisms of G. The linear independence of characters, Lemma 6, now implies $\psi = \pi^v$, for some $v \in U$. □

As long as we discard duplicates, the $P\pi$'s are linearly independent, too, as we see next.

Theorem 9. *Discarding duplicates, the distinct $P\pi$'s form an orthogonal system in $\mathcal{F}^U$. In particular, they are linearly independent.*

Proof. Suppose $P\psi \neq P\pi$. Then

$$|U|^2 \langle P\psi, P\pi \rangle = \langle \sum_{u \in U} \psi^u, \sum_{v \in U} \pi^v \rangle = \sum_{u,v} \langle \psi^u, \pi^v \rangle \quad .$$

But each $\langle \psi^u, \pi^v \rangle = 0$, by Lemma 6, because ψ^u, π^v are distinct characters. □

Note that $\langle P\pi, P\pi \rangle = 1/|U|$. The distinct $P\pi$ actually form a basis for $\mathcal{F}^U$, but we will not need this fact.

5 Extension Theorem

In this section the extension theorem for symmetrized weight compositions is proved. Strong use is made of the linear independence of characters and of averaged characters.

Let R be a ring, and let U be a subgroup of the group $\mathcal{U}$ of units of R. If we view the additive group of R as a finite abelian group G, then left multiplication by $u \in U$ defines an automorphism of G. Thus we find ourselves in the situation discussed in Sect. 4.

Theorem 10. *Suppose that R is a finite Frobenius ring and that $C \subset R^n$ is a right linear code. Fix a subgroup U of the group of units of R, which gives rise to a symmetrized weight composition* swc. *Then any injective right linear homomorphism $f : C \to R^n$ which preserves* swc *extends to a right U-monomial transformation.*

Proof. View the inclusion $C \subset R^n$ as a right linear homomorphism $\lambda : C \to R^n$; the components of $\lambda = (\lambda_1, \ldots, \lambda_n)$ are right linear functionals on C. Similarly, let $\mu = (\mu_1, \ldots, \mu_n) = f \circ \lambda$. Our goal is to show that $\lambda_i = u_i \mu_{\sigma(i)}$ for some permutation σ of $\{1, 2, \ldots, n\}$ and units $u_1, \ldots, u_n \in U$. The strategy is to write the weight preservation equation $\mathrm{swc}_r(\lambda(x)) = \mathrm{swc}_r(\mu(x))$ as an equation of characters and averaged characters on C.

Lemma 5 implies that

$$n_r(x) = \frac{1}{|R|} \sum_{i=1}^{n} \sum_{\pi \in \widehat{R}} \pi(x_i - r) = \frac{1}{|R|} \sum_{i=1}^{n} \sum_{\pi \in \widehat{R}} \pi(x_i) \overline{\pi}(r) \ .$$

A little manipulation then shows that

$$\mathrm{swc}_r(x) = \frac{|\mathrm{orb}(r)|}{|R|} \sum_{\pi \in \widehat{R}} \left(\sum_{i=1}^{n} \pi(x_i) \right) (P\overline{\pi})(r) \ .$$

The weight preservation equation $\mathrm{swc}_r(\lambda(x)) = \mathrm{swc}_r(\mu(x))$, $x \in C$, $r \in R$, can now be written as

$$\sum_{\pi \in \widehat{R}} \left(\sum_{i=1}^{n} \pi(\lambda_i(x)) \right) (P\overline{\pi})(r) = \sum_{\pi \in \widehat{R}} \left(\sum_{j=1}^{n} \pi(\mu_j(x)) \right) (P\overline{\pi})(r) \ , \tag{3}$$

for all $x \in C$, $r \in R$. For fixed $x \in C$, (3) is an equation of U-invariant functions on R. The linear independence of averaged characters, Theorem 9, together with Proposition 8, now implies that for every $\pi \in \widehat{R}$, we have the following equation of characters on C:

$$\sum_{i=1}^{n} \sum_{\psi \in \mathrm{orb}(\pi)} \psi \circ \lambda_i = \sum_{j=1}^{n} \sum_{\phi \in \mathrm{orb}(\pi)} \phi \circ \mu_j \ . \tag{4}$$

Since R is assumed to be a Frobenius ring, it has a generating character χ. In particular, (4) holds for $\pi = \chi$. Considering $i = 1$ and $\psi = \chi$ on the left side of (4), the linear independence of characters on C, Lemma 6, implies the existence of $\phi \in \mathrm{orb}(\chi)$ and $j = \sigma(1)$ such that $\chi \circ \lambda_1 = \phi \circ \mu_{\sigma(1)}$. But $\phi \in \mathrm{orb}(\chi)$ means $\phi = \chi^{u_1}$ for some $u_1 \in U$, so that $\chi \circ \lambda_1 = \chi \circ u_1 \mu_{\sigma(1)}$. An important injectivity property of generating characters ([15], Corollary 4.15) then implies that $\lambda_1 = u_1 \mu_{\sigma(1)}$. A re-indexing argument proves the equality of the corresponding inner sums in (4): $\sum_{\psi \in \mathrm{orb}(\chi)} \psi \circ \lambda_1 = \sum_{\phi \in \mathrm{orb}(\chi)} \phi \circ \mu_{\sigma(1)}$. This allows us to reduce by one the size of the outer sums in (4). We proceed by induction to obtain units $u_1, \ldots, u_n \in U$ and a permutation σ of $\{1, 2, \ldots, n\}$ with $\lambda_i = u_i \mu_{\sigma(i)}$, as desired. □

6 Weight Functions: Generalities

In this section we describe some general properties of weight functions over finite rings.

Let R be a ring. A *weight function* w on R^n is any function $w : R^n \to \mathbb{C}$ of the form

$$w(x) = \sum_{r \in R} a_r n_r(x) \ ,$$

where $a_r \in \mathbb{C}$ and $a_0 = 0$. It is usually the case that the a_r are non-negative real numbers, if not non-negative integers. But one could just as well assume that the a_r belong to some complex vector space or even a torsion-free abelian group. Having $a_r \in \mathbb{C}$ seems to be an appropriate level of generality for this paper.

Examples of weight functions include the *Hamming weight*, which is obtained if $a_r = 1$ for $r \neq 0$. If $\mathbb{Z}/m$ is viewed as the integers satisfying $-m/2 < r \leq m/2$, then the *Lee weight* has $a_r = |r|$. It is evident that the Lee weight has a $\mathbb{Z}/2$-symmetry.

More generally, for any weight function $w = \sum a_r n_r$, let

$$U = \{u \in \mathcal{U} : a_{ur} = a_r, \, r \in R\} \ .$$

We refer to U as the *symmetry group* of the weight function w. View the a_r as a function $a : R \to \mathbb{C}$, i.e., $a \in \mathcal{F}$, as in Sect. 4. Then the symmetry group U is just the stabilizer subgroup of a for the right action of $\mathcal{U}$ on $\mathcal{F}$.

Proposition 11. *Suppose w is a weight function on R^n with symmetry group U, and suppose $f : R^n \to R^n$ is a right monomial transformation of R^n. Then f preserves w if and only if f is a U-monomial transformation.*

Proof. Notice that $w(x)$ can we written as $w(x) = \sum_{i=1}^n a_{x_i}$. Express f in the notation of (2). If f is a U-monomial transformation, then $w(f(x)) = \sum a_{u_i x_{\sigma(i)}} = \sum a_{x_{\sigma(i)}}$, because U is the symmetry group of w and $u_i \in U$. Since σ is a permutation, the last sum equals $\sum a_{x_i} = w(x)$, and f preserves w.

For the converse, let $e_i = (0, \ldots, 1, \ldots, 0) \in R^n$ have a single 1, in position i. Then, for any $r \in R$, $w(e_i r) = a_r$, while $w(f(e_i r)) = a_{u_i r}$. If f preserves w, then $a_{u_i r} = a_r$ for all $r \in R$. Thus the units u_i from (2) belong to the symmetry group U. □

Extension Problem. *Suppose w is a weight function on R^n with symmetry group U. Let C be an arbitrary right linear code in R^n and let $f : C \to R^n$ be an injective right linear homomorphism which preserves w. What conditions guarantee that any such f extends to a U-monomial transformation of R^n?*

We now make some general comments on reducing the extension problem for weight functions to Theorem 10. As above, suppose R is a ring equipped with a weight function w having symmetry group U. Then U defines a symmetrized weight composition swc. Let $U\backslash R$ denote the set of all U-orbits in R. For any $\mathrm{orb}(r) \in U\backslash R$, the values a_r and $\mathrm{swc}_r(x)$ depend only on the orbit $\mathrm{orb}(r)$, not on the particular representative r. One then calculates that for any $t \in R$, $x \in R^n$,

$$w(xt) = \sum_{\mathrm{orb}(r) \in U\backslash R} a_{rt} \, \mathrm{swc}_r(x) \ .$$

Since $a_0 = 0$, the zero orbit orb(0) can be dropped from the summation.

Let $W = W(x)$ be the row vector of length $|R| - 1$ given by $W_t(x) = w(f(xt)) - w(xt)$ for non-zero $t \in R$. Then f preserves w if and only if $W = 0$ for all x. Similarly, let $\delta = \delta(x)$ be a row vector of length $|U\backslash R| - 1$ with $\delta_r = \mathrm{swc}_r(f(x)) - \mathrm{swc}_r(x)$ for all non-zero orbits $\mathrm{orb}(r) \in U\backslash R$. Clearly f preserves swc if and only if $\delta = 0$ for all x. Finally, let A be the matrix of size $(|U\backslash R| - 1) \times (|R| - 1)$ with $A_{r,t} = a_{rt}$. The calculation above says that $W = \delta A$ for all $x \in R^n$.

Proposition 12. *Suppose the weight function w has the property that the matrix A has maximal rank $|U\backslash R| - 1$. Then every $f : C \to R^n$ which preserves w extends to a U-monomial transformation.*

Proof. Use the equation $W = \delta A$. If f preserves w, then $W = 0$. Now $\delta = 0$, since A has full rank. Thus f preserves swc, and f extends by Theorem 10. □

This very general criterion is of limited usefulness because it is hard to give convenient conditions on the a_r which will imply that A has maximal rank. When the ring R has extra structure, we can sometimes find such conditions, as we will see in Sect. 7.

Remark 13. When the ring R is commutative, we observe that the value of $w(xt)$ depends only on $\mathrm{orb}(t)$. This allows us to throw away repeated columns in the matrix A above. The resulting matrix A' is square of size $|U\backslash R| - 1$. The extension problem for w is then solvable if the matrix A' is invertible.

7 Weight Functions: Specifics

As an application of the extension theorem for symmetrized weight compositions, we solve a special case of the extension problem for weight functions over certain finite commutative rings.

Here are the extra hypotheses we will need. The ring R is assumed to be commutative and local, with unique maximal ideal $\mathfrak{m}$. We assume that $\mathfrak{m}$ is a principal ideal, say $\mathfrak{m} = Rm$. Finally, we assume that R is equipped with a weight function w whose symmetry group U equals $\mathcal{U}$, the full group of units. The author can also solve the cases for arbitrary U, but techniques beyond the scope of this paper are required (see [16]).

Examples of rings satisfying these assumptions include finite fields, $\mathbb{Z}/p^l$ for a prime p, and Galois rings.

Lemma 14. *Let $(R, \mathfrak{m})$ be a commutative local ring. Suppose $\mathfrak{m}$ is a principal ideal, $\mathfrak{m} = Rm$. 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 $\mathfrak{m}^i$, $i = 0, \ldots, l$.*
4. *R is Frobenius.*

Proof. Being finite, the ring R is artinian. Thus the descending chain of ideals $R = \mathfrak{m}^0 \supset \mathfrak{m} \supset \mathfrak{m}^2 \supset \cdots$ eventually stabilizes. Let $\mathfrak{m}^{l+1} = \mathfrak{m}^{l+2}$ be the first time equality holds. Nakayama's Lemma now implies that $\mathfrak{m}^{l+1} = 0$.

It is clear that $m^i \in \mathfrak{m}^i$. On the other hand, any element of $\mathfrak{m}^i$ equals a sum of terms of the form $(r_1 m) \cdots (r_i m) = r m^i \in R(m^i)$. Thus $\mathfrak{m}^i = R(m^i)$.

Any ideal B in R is finite, and each element $b \in B$ defines an integer $i(b)$ such that $b \in \mathfrak{m}^{i(b)}$ but $b \notin \mathfrak{m}^{i(b)+1}$. If we set $i = \min\{i(b) : b \in B\}$, then $B = \mathfrak{m}^i$. Indeed, the containment $B \subset \mathfrak{m}^i$ is clear. For the other containment, let $b \in B$ have $i(b) = i$. Then $b \in \mathfrak{m}^i$, so that $b = r m^i$ for some $r \in R$. If $r \in \mathfrak{m}$, then $b \in \mathfrak{m}^{i+1}$, contradicting $i(b) = i$. Thus $r \in \mathcal{U}$, since $\mathcal{U}$ is the complement of $\mathfrak{m}$ in a local ring. But then $m^i = r^{-1} b \in B$, so that $\mathfrak{m}^i \subset B$.

Being commutative, the ring R is Frobenius if it is quasi-Frobenius. The latter happens if and only if the socle $S(R) = \mathrm{ann}(\mathfrak{m})$ is simple. It is clear that $\mathrm{ann}(\mathfrak{m}) = \mathfrak{m}^l$. Since $\mathfrak{m}^l = R(m^l)$, it follows that $\mathfrak{m}^l$ has dimension 1 as a vector space over the residue field $k = R/\mathfrak{m}$. Thus $\mathfrak{m}^l$ is simple. The reader is referred to [15], Remark 2.4, for more details. □

Before we state our next result, some notation is desirable. Remember that we are assuming $U = \mathcal{U}$. Decompose R into $\mathcal{U}$-orbits, which we denote as $\mathcal{O}_i = \mathrm{orb}(m^i)$, $i = 0, 1, \ldots, l$. Then $\mathcal{O}_0 = \mathcal{U}$ and $\mathcal{O}_{l+1} = \{0\}$. The key computation is isolated as a lemma.

Lemma 15. *Let $C_{i,j} = |\mathcal{O}_i| \,/\, |\mathcal{O}_{i+j}|$. Then, for every $i = 0, 1, \ldots, l$,*

$$\sum_{r \in \mathcal{O}_i} w(rx) = \sum_{j=0}^{l-i} C_{i,j} \left(\sum_{s \in \mathcal{O}_{i+j}} a_s \right) \left(\sum_{t \in \mathcal{O}_j} n_t(x) \right) \quad .$$

Proof. Take any component x_k of x, and set $t = x_k$. Then $t \in \mathcal{O}_j$ for some j. If $j > l - i$, then $rt = 0$ for any $r \in \mathcal{O}_i$. As $a_0 = 0$, this component x_k makes no contribution to $w(rx)$.

Now suppose $j \leq l - i$. Then $rt \in \mathcal{O}_{i+j}$ for any $r \in \mathcal{O}_i$. As r varies over $\mathcal{O}_i$, rt varies over $\mathcal{O}_{i+j}$ with multiplicity $|\mathcal{O}_i| \,/\, |\mathcal{O}_{i+j}| = C_{i,j}$. Thus this component $x_k = t \in \mathcal{O}_j$ contributes a coefficient of $C_{i,j} \left(\sum_{s \in \mathcal{O}_{i+j}} a_s \right)$ to $\sum_{r \in \mathcal{O}_i} w(rx)$, as desired. □

Theorem 16. *Let R be a commutative local ring whose maximal ideal $\mathfrak{m}$ is principal. Suppose the weight function $w(x) = \sum_{r \in R} a_r n_r(x)$ on R^n satisfies $\sum_{r \in \mathcal{O}_l} a_r \neq 0$. Suppose C is a linear code in R^n and $f : C \to R^n$ is an injective linear homomorphism which preserves w. Then f extends to a monomial transformation on R^n. In particular, the extension problem is solved for any w whose symmetry group U equals $\mathcal{U}$.*

Proof. By Lemma 14, the ring R is Frobenius. Let $U = \mathcal{U}$ be the full group of units of R. Observe that $\mathrm{swc}_{m^j}(x) = \sum_{t \in \mathcal{O}_j} n_t(x)$.

Define two row vectors $W = W(x), \delta = \delta(x)$ of length $l+1$ by

$$W_i = \sum_{r \in \mathcal{O}_{l-i}} (w(rf(x)) - w(rx)) \,, \quad \delta_i = \mathrm{swc}_{m^i}(f(x)) - \mathrm{swc}_{m^i}(x) \;\;,$$

for $i = 0, 1, \ldots, l$. Notice the "reverse" ordering on W. Then Lemma 15 says that $W = \delta A$, where A is an upper triangular matrix with $\sum_{s \in \mathcal{O}_l} a_s \neq 0$ on the main diagonal. Since f preserves w, $W = 0$. Then $\delta = 0$, as A is invertible. Thus f preserves swc, and the theorem follows from Theorem 10. □

Observe two things: (i) Even if the symmetry group U of w is not $\mathcal{U}$, f as above still extends to a $\mathcal{U}$-monomial transformation. For $R = \mathbb{Z}/p^l$, this generalizes the extension theorem of [4]; on the other hand, the result in [4] applies to the non-local rings $\mathbb{Z}/m$ as well. (ii) If the a_r are positive real numbers, as is often the case, then the condition $\sum_{r \in \mathcal{O}_l} a_r \neq 0$ is automatic.

Corollary 17. *Let R be a commutative local ring whose maximal ideal $\mathfrak{m}$ is principal. Suppose the weight function $w(x) = \sum_{r \in R} a_r n_r(x)$ on R^n has symmetry group U and satisfies $\sum_{r \in \mathcal{O}_l} a_r \neq 0$. Then a linear automorphism f on R^n preserves w if and only if f is a U-monomial transformation on R^n.*

Proof. The "if" direction is part of Proposition 11. The "only if" direction follows from applying Theorem 16 with $C = R^n$ and then using Proposition 11 once more. □

References

1. Arf, Č.: Untersuchungen über quadratische Formen in Körpern der Charakteristik 2. I. J. Reine Angew. Math. **183** (1941) 148–167
2. Assmus, E. F., Jr., Key, J. D.: *Designs and their codes,* Cambridge: Cambridge University Press, 1992
3. Bogart, K., Goldberg, D., Gordon, J.: An elementary proof of the MacWilliams theorem on equivalence of codes. Inform. and Control **37** (1978) 19–22
4. Constantinescu, I., Heise, W., Honold, T.: 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. Conway, J. H., Sloane, N. J. A.: Self-dual codes over the integers modulo 4. J. Combin. Theory Ser. A **62** (1993) 30–45
6. Filip, P., Heise, W.: Monomial code-isomorphisms. Ann. Disc. Math. **30** (1986) 217–224
7. Goldberg, D. Y.: A generalized weight for linear codes and a Witt-MacWilliams theorem. J. Combin. Theory Ser. A **29** (1980) 363–367
8. Hammons, A. R., Kumar, P. V., Calderbank, A. R., Sloane, N. J. A., Solé, P.: The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. IEEE Trans. Inform. Theory **IT-40** (1994) 301–319
9. MacWilliams, F. J.: Error-correcting codes for multiple-level transmission. Bell System Tech. J. **40** (1961) 281–308

10. MacWilliams, F. J.: Combinatorial problems of elementary abelian groups. Ph.D. dissertation, Radcliffe College, Cambridge, Mass., 1962
11. Serre, J.-P.: *A course in arithmetic.* Grad. Texts in Math. 7, New York: Springer-Verlag, 1973
12. Serre, J.-P.: *Linear representations of finite groups.* Grad. Texts in Math. 42, New York: Springer-Verlag, 1977
13. Ward, H. N., Wood, J. A.: Characters and the equivalence of codes. J. Combin. Theory Ser. A **73** (1996) 348–352
14. Witt, E.: Theorie der quadratischen Formen in beliebigen Körpern. J. Reine Angew. Math. **176** (1937) 31–44
15. Wood, J. A.: Duality for modules over finite rings and applications to coding theory. Submitted, 1996
16. Wood, J. A.: Semigroup rings and the extension theorem for linear codes. To appear in the Proceedings of the Thirty-Fifth Annual Allerton Conference on Communication, Control, and Computing, 1997.