J. Algebra Comb. Discrete Appl.
4(2) • 207–217

Received: 12 June 2015
Accepted: 8 June 2016

Journal of Algebra Combinatorics Discrete Structures and Applications

The extension problem for Lee and Euclidean weights

Research Article

Philippe Langevin, Jay A. Wood

Abstract: The extension problem is solved for the Lee and Euclidean weights over three families of rings of the form $\mathbb{Z}/N\mathbb{Z}$: $N = 2^{\ell+1}$, $N = 3^{\ell+1}$, or $N = p = 2q + 1$ with p and q prime. The extension problem is solved for the Euclidean PSK weight over $\mathbb{Z}/N\mathbb{Z}$ for all N.

2010 MSC: 94B05

Keywords: Extension problem, Lee weight, Euclidean weight, Egalitarian weight

1. Introduction

One of the themes of the Mini-cours at the Lens conference was the extension theorem of MacWilliams. In its original form, this theorem says that any linear isomorphism between linear codes defined over a finite field that preserves the Hamming weight must extend to a monomial transformation. This result has been generalized in several directions, including: for linear codes defined over finite Frobenius rings with respect to the Hamming weight [12] or the homogeneous weight [7]; for linear codes defined over finite Frobenius rings with respect to symmetrized weight compositions [11] (with an improved proof in [2]); for linear codes defined over finite commutative chain rings with respect to any weight function satisfying certain conditions [13, 14]; for linear codes equipped with a weight function having maximal symmetry and satisfying certain conditions, defined over products of finite chain rings [6] or over a finite principal ideal ring [5].

Despite all this progress, there are glaring gaps in our knowledge: does the extension theorem hold for linear codes defined over $\mathbb{Z}/N\mathbb{Z}$ with respect to the Lee weight or the Euclidean weight? In general, we do not know.

The purpose of this paper is to describe what we do know. In [15, Examples 3.7 and 3.9], it was claimed that the extension theorem holds for the Lee and Euclidean weights over the rings $\mathbb{Z}/2^k\mathbb{Z}$, $\mathbb{Z}/3^k\mathbb{Z}$,

Philippe Langevin; Laboratoire IMATH, Université de Toulon, 83957 La Garde Cedex, France (email: langevin@univ-tln.fr).
Jay A. Wood (Corresponding Author); Department of Mathematics, Western Michigan University, 1903 W. Michigan Ave., Kalamazoo, MI 49008–5248 USA (email: jay.wood@wmich.edu).

and $\mathbb{Z}/p\mathbb{Z}$ for a prime p of the form $p = 2q + 1$ with q prime. Proofs of those claims will constitute the bulk of this paper. Barra [1] has proved that the extension theorem holds for the Lee weight over $\mathbb{Z}/p\mathbb{Z}$ for a prime p of the form $p = 4q+1$ with q prime. In [15, Example 3.8], it was claimed that the extension theorem holds for Euclidean PSK weight over the rings $\mathbb{Z}/3^k\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z}$ for a prime p of the form $p = 2q + 1$ with q prime. For this weight, we give a simple proof that works for all $\mathbb{Z}/N\mathbb{Z}$. This proof is similar to the proof in [2, Theorem 6.6] for the homogeneous weight over any finite Frobenius ring.

2. Background

Let $R = \mathbb{Z}/N\mathbb{Z}$ be the ring of integers modulo N. Every element x of R is represented uniquely by an integer a satisfying $-N/2 < a \leq N/2$ with $x \equiv a \bmod N$. The *Lee weight* $w_L(x)$ (resp., *Euclidean weight* $w_E(x)$) of $x \in R$ is the ordinary absolute value $|a|$ (resp., the square $|a|^2$) of the representative a. Alternatively, if one represents $x \in R$ by a unique integer representative b satisfying $0 \leq b < N$ with $x \equiv b \bmod N$, then the Lee weight and the Euclidean weight have the form

$$w_L(x) = \begin{cases} b, & 0 \leq b \leq N/2, \\ N - b, & N/2 \leq b < N; \end{cases}$$

$$w_E(x) = \begin{cases} b^2, & 0 \leq b \leq N/2, \\ (N - b)^2, & N/2 \leq b < N. \end{cases}$$

There is another Euclidean weight, the Euclidean PSK weight w_{PSK}, which is used in phase-shift key modulation. It is defined using the squared Euclidean distance in the complex numbers; for $x \in R$,

$$w_{\mathrm{PSK}}(x) = |\exp(2\pi i x/N) - 1|^2 = 2 - 2\cos(2\pi x/N).$$

Note that all three weights satisfy $w(-x) = w(x)$, for $x \in R$.

The Lee and the Euclidean weights can be extended to real-valued functions (still denoted by w_L, w_E, and w_{PSK}) on the product R^n:

$$\begin{aligned} w_L(x) &= \sum_{i=1}^{n} w_L(x_i), \\ w_E(x) &= \sum_{i=1}^{n} w_E(x_i), \\ w_{\mathrm{PSK}}(x) &= \sum_{i=1}^{n} w_{\mathrm{PSK}}(x_i), \end{aligned}$$

for $x = (x_1, x_2, \ldots, x_n) \in R^n$.

A *monomial transformation* T on R^n is an R-module isomorphism $T : R^n \to R^n$ of the form

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

for $(x_1, x_2, \ldots, x_n) \in R^n$, where $u_1, u_2, \ldots, u_n$ are units of R and σ is a permutation of the set $\{1, 2, \ldots, n\}$. If G is a subgroup of the group of units of R and each $u_i \in G$, we say that T is a *G-monomial transformation*. In the case where $G = \{\pm 1\}$, i.e., each $u_i = \pm 1$, we say that T is a *signed permutation*. The following proposition is now immediate.

Proposition 2.1. *Suppose $T : R^n \to R^n$ is a signed permutation. Then T preserves the Lee and Euclidean weights. That is, for every $x \in R^n$, $w_L(T(x)) = w_L(x)$, $w_E(T(x)) = w_E(x)$, and $w_{\mathrm{PSK}}(T(x)) = w_{\mathrm{PSK}}(x)$.*

Conversely, the signed permutations are precisely the linear isometries of R^n with respect to any of the three weights.

Proposition 2.2. *Let w be one of the weights $w_L, w_E, w_{\mathrm{PSK}}$, and suppose $f : R^n \to R^n$ is an R-module homomorphism that preserves w: $w(f(x)) = w(x)$, for all $x \in R^n$. Then f is a signed permutation.*

Proof. Observe that f is injective. Indeed, only the zero vector has weight zero, so if $f(x) = 0$, then $0 = w(f(x)) = w(x)$ implies $x = 0$. Because R^n is a finite set, f is also surjective, hence an R-module isomorphism.

Let $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, with the 1 in position i, $1 \le i \le n$. Then $w(1) = w(e_i) = w(f(e_i))$. But $w(1) = w(-1)$ is the smallest positive value of w on R, so it follows that $f(e_i) = \pm e_j$ for some j, $1 \le j \le n$. Because f is known to be an isomorphism, it follows that f is a signed permutation. □

Again, let w be one of the weights $w_L, w_E, w_{\mathrm{PSK}}$. We say that $R = \mathbb{Z}/N\mathbb{Z}$ has the *extension property* with respect to w if the following property is satisfied for every R-submodule $C \subseteq R^n$ and every R-module homomorphism $f : C \to R^n$: if f preserves w, $w(f(x)) = w(x)$, $x \in C$, then f extends to a signed permutation. That is, there exists a signed permutation T defined on all of R^n such that $T(x) = f(x)$ for $x \in C$. Another way to view the extension property is that every linear w-isometry on C extends to a linear w-isometry on R^n.

The main results of this paper are the following theorems.

Theorem 2.3. *The rings in the following list have the extension property with respect to the Lee weight w_L and the Euclidean weight w_E:*

1. $R = \mathbb{Z}/2^{\ell+1}\mathbb{Z}$, $l \ge 0$;
2. $R = \mathbb{Z}/3^{\ell+1}\mathbb{Z}$, $l \ge 0$;
3. $R = \mathbb{Z}/p\mathbb{Z}$, *with prime p of the form $p = 2q + 1$, q prime.*

Remark 2.4. Barra proved that $R = \mathbb{Z}/p\mathbb{Z}$, with prime p of the form $p = 4q + 1$, q prime, has the extension property with respect to the Lee weight w_L [1].

Remark 2.5. (Added in proof.) After the submission of this paper, the authors, together with Serhii Dyshko, have extended Theorem 2.3, first to the cases $R = \mathbb{Z}/p\mathbb{Z}$ for all primes p [3], and then to the cases $R = \mathbb{Z}/p^{\ell+1}\mathbb{Z}$ for all primes p and $\ell \ge 0$ [P. Langevin, J. A. Wood, The extension theorem for the Lee and Euclidean weights over $\mathbb{Z}/p^k\mathbb{Z}$, in preparation, 2016]. The methods used for the new results are very different from those of Sections 4 and 5 of this paper.

Theorem 2.6. *For any positive integer N, the ring $R = \mathbb{Z}/N\mathbb{Z}$ has the extension property with respect to the Euclidean PSK weight w_{PSK}.*

After an explanation of the method of attack in Section 3 and an analysis of cases in Section 4, the proof of Theorem 2.3 appears in Section 5. The proof of Theorem 2.6 appears in Section 6.

3. Method of attack for Theorem 2.3

In this section we will describe how the proof of Theorem 2.3 reduces to showing that certain Fourier coefficients are nonzero. In both this section and the next, we will use some basic facts from number theory, such as the structure of the group of units for $\mathbb{Z}/N\mathbb{Z}$ and the form of cyclotomic polynomials, which may be found in textbooks such as [10].

There is an extension theorem for general weight functions over a finite Frobenius ring, [13, Theorem 3.1]. The theorem below is the form that this theorem takes in the context of the Lee or the Euclidean weights on the Frobenius ring $R = \mathbb{Z}/N\mathbb{Z}$.

To establish notation, let $R = \mathbb{Z}/N\mathbb{Z}$ and let w be one of w_L, w_E, or w_{PSK} on R. Let $m = \lfloor N/2 \rfloor$ be the largest integer less than or equal to $N/2$. Form an $m \times m$ real matrix $\mathcal{A}_w$ as follows. The entry of $\mathcal{A}_w$ in position (i, j), $1 \le i, j \le m$, equals $w(ij)$, the value of the weight function on the product of i and j in the ring R.

Theorem 3.1 ([13, Theorem 3.1]). *If the matrix $\mathcal{A}_w$ is nonsingular over $\mathbb{C}$, then R has the extension property with respect to w.*

Remark 3.2. In fact, Theorem 3.1 applies to any complex-valued weight w on R that satisfies two properties: $w(0) = 0$ and $\mathrm{Sym}(w) = \{\pm 1\}$. Here, $\mathrm{Sym}(w)$ denotes the *symmetry group* of the weight w:

$$\mathrm{Sym}(w) = \{u \in R : u \text{ is a unit, and } w(ux) = w(x) \text{ for all } x \in R\}.$$

Example 3.3. For $R = \mathbb{Z}/9\mathbb{Z}$, the determinants of the matrices for w_L and w_E are

$$\det \mathcal{A}_L = \det \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \\ 3 & 3 & 0 & 3 \\ 4 & 1 & 3 & 2 \end{bmatrix} = 189,$$

$$\det \mathcal{A}_E = \det \begin{bmatrix} 1 & 4 & 9 & 16 \\ 4 & 16 & 9 & 1 \\ 9 & 9 & 0 & 9 \\ 16 & 1 & 9 & 4 \end{bmatrix} = 45\ 927.$$

Remark 3.4. MAPLE has been used to verify that $R = \mathbb{Z}/N\mathbb{Z}$ has the extension property for w_L and w_E for $N \le 2048$. The smallest singular values of the matrices $\mathcal{A}_L$ and $\mathcal{A}_E$ were calculated and seen to be nonzero. Barra has verified the extension property for w_L over $R = \mathbb{Z}/p\mathbb{Z}$ for the first 2012 primes p [1, p. 44].

Now assume that $R = \mathbb{Z}/N\mathbb{Z}$ is a local ring, so that N equals a prime power; R is then a finite commutative chain ring. We continue to assume that w is one of $w_L, w_E, w_{\mathrm{PSK}}$. In this chain ring context, the determinant $\det \mathcal{A}_w$ can be factored into linear expressions that are Fourier transforms of values of the weight function w, [14, Theorem 7]. We explain this next.

Suppose $R = \mathbb{Z}/p^{\ell+1}\mathbb{Z}$, with p prime. Let $\mathcal{U}$ be the group of units of R. Then $|\mathcal{U}| = \phi(p^{\ell+1}) = p^{\ell}(p-1)$, where ϕ is Euler's totient function. The group $\mathcal{U}$ is cyclic when p is an odd prime. For powers of 2, $\mathcal{U}$ is cyclic for $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$; for $\mathbb{Z}/2^{\ell+1}\mathbb{Z}$, $l \ge 2$, $\mathcal{U}$ is isomorphic to the product of a cyclic group of order 2 times a cyclic group of order $2^{\ell-1}$, with generators for the two cyclic factors being the residue classes of -1 and 5, respectively.

The group $\mathcal{U}$ acts on the ring R by ring multiplication. The orbits have the form $\mathcal{O}_i = \{up^i : u \in \mathcal{U}\}$, $i = 0, 1, \ldots, \ell+1$. The orbit $\mathcal{O}_i$ equals the set-theoretic difference of ideals $(p^i)\backslash(p^{i+1})$, where $(a) = Ra$ denotes the principal ideal generated by $a \in R$. Because $\mathcal{U}$ is abelian, the stabilizer subgroup of a point in an orbit $\mathcal{O}_i$, $i = 0, 1, \ldots, \ell+1$, is independent of the point chosen; the stabilizer subgroup depends only on the orbit. Denote the stabilizer subgroup of a point of $\mathcal{O}_i$ by $\mathcal{U}_i$. Then $\mathcal{U}_i = \{u \in \mathcal{U} : up^i = p^i\}$, and $\mathcal{O}_i$ can be identified with the coset space $\mathcal{U}/\mathcal{U}_i$. The ideal (p^i) has order $|(p^i)| = p^{\ell+1-i}$, $i = 0, 1, \ldots \ell+1$, so that $|\mathcal{O}_i| = p^{\ell+1-i} - p^{\ell-i} = p^{\ell-i}(p-1)$ and $|\mathcal{U}_i| = p^i$.

The group of complex characters (group homomorphisms from $\mathcal{U}$ to the multiplicative group of nonzero complex numbers) of the group $\mathcal{U}$ will be denoted $\widehat{\mathcal{U}}$. A pair $(\pi, \mathcal{O}_i)$ consisting of a character $\pi \in \widehat{\mathcal{U}}$ and a $\mathcal{U}$-orbit $\mathcal{O}_i$ is *admissible* if $\mathcal{U}_i \subseteq \ker \pi$. For $\pi \in \widehat{\mathcal{U}}$, let i_π be the largest integer $j \le \ell$ such that $(\pi, \mathcal{O}_j)$ is admissible. Because $\mathcal{U}_0 = \{1\}$, every pair $(\pi, \mathcal{O}_0)$ is admissible, so that $i_\pi \ge 0$ for all $\pi \in \widehat{\mathcal{U}}$.

Given a subgroup $H \subseteq \mathcal{U}$, the *annihilator* $(\widehat{\mathcal{U}} : H)$ of H in $\widehat{\mathcal{U}}$ is defined by $(\widehat{\mathcal{U}} : H) = \{\pi \in \widehat{\mathcal{U}} : \pi(H) = 1\}$. Let $U = \{\pm 1\} \subseteq \mathcal{U}$. Suppose a character π satisfies (1) $\pi \in (\widehat{\mathcal{U}} : U)$ and (2) $(\pi, \mathcal{O}_i)$ is admissible. For w equal to $w_L, w_E, w_{\mathrm{PSK}}$, we define

$$\check{w}(\pi, i) = \sum_{u \in \mathcal{U}/U\mathcal{U}_i} w(up^i)\pi(u). \tag{1}$$

Observe that this character sum is well-defined.

Here is the factorization of $\det \mathcal{A}_w$, for w equal to $w_L, w_E, w_{\mathrm{PSK}}$.

Theorem 3.5 ([14, Theorem 7]). *Let $R = \mathbb{Z}/p^{\ell+1}\mathbb{Z}$ and $U = \{\pm 1\} \subseteq \mathcal{U}$. For w equal to $w_L, w_E, w_{\mathrm{PSK}}$, there exists a nonzero integer constant C such that*

$$\det \mathcal{A}_w = C \prod_{\pi \in (\widehat{\mathcal{U}}:U)} \breve{w}(\pi, i_\pi)^{1+i_\pi}.$$

Remark 3.6. Theorem 3.5 also holds for any weight w satisfying the conditions in Remark 3.2. Theorem 3.5 can be viewed as a generalization of the factorization of the group determinant given by Dedekind and Frobenius in 1896 [4].

Example 3.7. For $R = \mathbb{Z}/9\mathbb{Z}$, the factorizations have the form

$$\begin{aligned}\det \mathcal{A}_w &= 3w(3)^2[w(1) + w(2)\zeta + w(4)\zeta^2][w(1) + w(2)\zeta^2 + w(4)\zeta] \\ &= 3w(3)^2[w(1)^2 - w(1)w(2) - w(1)w(4) \\ &\qquad + w(2)^2 - w(2)w(4) + w(4)^2],\end{aligned}$$

where ζ is a primitive third root of unity in $\mathbb{C}$. Using w_L, w_E, we recover the values of $\det \mathcal{A}_w$ in Example 3.3. For additional details of this computation, see [14, Example 12].

Remark 3.8. In order to prove Theorem 2.3, we will show that $\breve{w}(\pi, i_\pi) \neq 0$ for all $\pi \in (\widehat{\mathcal{U}} : U)$ and then appeal to Theorems 3.1 and 3.5.

To illustrate the type of argument that will be used in the next two sections, consider the factorization of $\det \mathcal{A}_w$ in Example 3.7. Under what conditions could one of the factors vanish? In the example, there are three factors. One possibility is $w(3) = 0$. For the other two factors, make use of the minimal polynomial for ζ over $\mathbb{Q}$, i.e., $\zeta^2 + \zeta + 1 = 0$. Then

$$\begin{aligned}w(1) + w(2)\zeta + w(4)\zeta^2 &= (w(1) - w(4)) + (w(2) - w(4))\zeta, \\ w(1) + w(4)\zeta + w(2)\zeta^2 &= (w(1) - w(2)) + (w(4) - w(2))\zeta.\end{aligned}$$

Both these factors would vanish when $w(1) = w(2) = w(4)$, and, if the values of w are rational numbers, this is the only way in which these factors could vanish. For w_L and w_E, it is easy to see that the factors do not vanish.

4. Analysis of cases

In this section we will analyze the structure of the orbits $\mathcal{O}_i$ and the stabilizer subgroups $\mathcal{U}_i$ that occur in the character sum (1).

The case where $N = 2^{\ell+1}$

Let $R = \mathbb{Z}/2^{\ell+1}\mathbb{Z}$. When $R = \mathbb{Z}/2\mathbb{Z}$ or $R = \mathbb{Z}/4\mathbb{Z}$, the extension property for w_L or w_E follows easily from Theorem 3.1 (also, see Remark 3.4). For the rest of the discussion, we assume $\ell \geq 2$. Then the group of units $\mathcal{U}$ of R is isomorphic to the product of a cyclic group B of order 2 and a cyclic group C of order $2^{\ell-1}$, with B and C generated by the residue classes of -1 and 5, respectively. In particular, $B = U = \{\pm 1\}$.

In Theorem 3.5, it is the characters $\pi \in (\widehat{\mathcal{U}} : U)$, i.e., characters such that $\pi(-1) = 1$, that contribute to the factorization of $\det \mathcal{A}_w$. Since $(\widehat{\mathcal{U}} : U) \cong (\mathcal{U}/U)\widehat{\ }$ and $\mathcal{U} \cong U \times C$, we see that $\mathcal{U}/U \cong C$ is a cyclic group of order $2^{\ell-1}$, and $(\widehat{\mathcal{U}} : U) \cong \widehat{C}$.

The orbits of $\mathcal{U}$ on R have the form

$$\mathcal{O}_i = \{u2^i : u \in \mathcal{U}\}, \quad i = 0, 1, \ldots, \ell + 1,$$

and the stabilizer subgroup of the point $2^i \in \mathcal{O}_i$ is

$$\mathcal{U}_i = \{1 + m2^{\ell+1-i} : 0 \le m < 2^i\}, \quad i = 0, 1, \ldots, \ell.$$

When $i = \ell + 1$, $\mathcal{U}_{\ell+1} = \mathcal{U}$. The stabilizer subgroups satisfy

$$\{1\} = \mathcal{U}_0 \subset \mathcal{U}_1 \subset \cdots \subset \mathcal{U}_l = \mathcal{U}_{\ell+1} = \mathcal{U},$$

and $|\mathcal{U}_i| = 2^i$ (for $0 \le i \le \ell$). Observe that $-1 \in \mathcal{U}_i$ only for $i = \ell$ or $\ell + 1$. Thus, for $i < \ell$, the image of $\mathcal{U}_i$ under the projection $\mathcal{U} \cong U \times C \to C \cong \mathcal{U}/U$ is the unique subgroup in C of order 2^i. In particular, $\mathcal{U}_i$ is cyclic, for $i < \ell$.

Proposition 4.1. *Let $R = \mathbb{Z}/2^{\ell+1}\mathbb{Z}$, $\ell \ge 2$, and $U = \{\pm 1\}$. If $\pi \in (\widehat{\mathcal{U}} : U)$, then $\ker \pi = U\mathcal{U}_{i_\pi}$.*

Proof. Take any $\pi \in (\widehat{\mathcal{U}} : U)$. Under the isomorphism $(\widehat{\mathcal{U}} : U) \cong \widehat{C}$, we can view π as a character on C. From that perspective, $\ker \pi$ is a subgroup E of C of order 2^k, for some $k \le \ell - 1$ (since C is a group of order $2^{\ell-1}$). Note that E is the image of $\mathcal{U}_k$ under the projection $\mathcal{U} \to C$. When we view π as a character on $\mathcal{U}$, we see that $\mathcal{U}_k \subset \ker \pi$, that $\ker \pi \cong U \times E$ (since $\pi \in (\widehat{\mathcal{U}} : U)$), and that $\ker \pi = U\mathcal{U}_k$.

If $k < \ell - 1$, we claim that $k = i_\pi$, i.e., that k is the largest integer j such that $\mathcal{U}_j \subset \ker \pi$. On the one hand, $\ker \pi \cong U \times E$ has order 2^{k+1} but is not cyclic. If $\mathcal{U}_{k+1} \subset \ker \pi$, then $\mathcal{U}_{k+1} = \ker \pi$, because both groups have order 2^{k+1}. But $\mathcal{U}_{k+1}$ is cyclic, forcing $\ker \pi$ to be cyclic as well; contradiction. Thus, if $k < \ell - 1$, we have $i_\pi = k$ and $\ker \pi = U\mathcal{U}_{i_\pi}$.

If $k = \ell - 1$, then $\ker \pi \cong U \times E$ has order 2^ℓ, so that $\ker \pi = \mathcal{U}$ and π is the trivial character. In that case, $i_\pi = \ell$, so that $\ker \pi = \mathcal{U} = \mathcal{U}_\ell = U\mathcal{U}_\ell$. □

The case where $N = 3^{\ell+1}$

We first assume that $N = p^{\ell+1}$, with p an odd prime. We will specialize to $p = 3$ later. Set $R = \mathbb{Z}/p^{\ell+1}\mathbb{Z}$, and let $\mathcal{U}$ be its group of units. The group $\mathcal{U}$ is cyclic of order $p^\ell(p-1)$. Let $U = \{\pm 1\}$; then $\mathcal{U}/U$ is cyclic of order $p^\ell(p-1)/2$.

The orbits of $\mathcal{U}$ on R have the form

$$\mathcal{O}_i = \{up^i : u \in \mathcal{U}\}, \quad i = 0, 1, \ldots, \ell + 1,$$

and the stabilizer subgroup of the point $p^i \in \mathcal{O}_i$ is

$$\mathcal{U}_i = \{1 + mp^{\ell+1-i} : 0 \le m < p^i\}, \quad i = 0, 1, \ldots, \ell.$$

When $i = \ell + 1$, $\mathcal{U}_{\ell+1} = \mathcal{U}$. The stabilizer subgroups satisfy

$$\{1\} = \mathcal{U}_0 \subset \mathcal{U}_1 \subset \cdots \subset \mathcal{U}_\ell \subset \mathcal{U}_{\ell+1} = \mathcal{U},$$

and $|\mathcal{U}_i| = p^i$ (for $0 \le i \le \ell$). Observe that $-1 \in \mathcal{U}_i$ only for $i = \ell + 1$.

Proposition 4.2. *Let $R = \mathbb{Z}/3^{\ell+1}\mathbb{Z}$ and $U = \{\pm 1\}$. If $\pi \in (\widehat{\mathcal{U}} : U)$, then $\ker \pi = U\mathcal{U}_{i_\pi}$.*

Proof. Take any $\pi \in (\widehat{\mathcal{U}} : U)$. Viewing π as a character on $\mathcal{U}/U$, $\ker \pi$ is a subgroup of the cyclic group $\mathcal{U}/U$, which, for a general odd prime p, has order $p^\ell(p-1)/2$. For a general odd prime p, there is not much control on the order of $\ker \pi$. But this proposition assumes that $p = 3$, so that the cyclic group $\mathcal{U}/U$ has order 3^ℓ. Thus $\ker \pi$ is the unique subgroup of order 3^k for some $k \le l$.

Under the projection $\mathcal{U} \to \mathcal{U}/U$, $\mathcal{U}_i$ projects to a subgroup of order 3^i (for $i \le \ell$) because $-1 \notin \mathcal{U}_i$. Thus, when we view π as a character on $\mathcal{U}$, we see that $\mathcal{U}_k \subset \ker \pi$, and $\ker \pi = U\mathcal{U}_k$ has order $2 \cdot 3^k$. Note that $\mathcal{U}_{k+1} \not\subseteq \ker \pi$ by size considerations, so that $i_\pi = k$ and $\ker \pi = U\mathcal{U}_{i_\pi}$. For $i = \ell + 1$, $\ker \pi = \mathcal{U}$, so that $i_\pi = \ell$ and $\ker \pi = U\mathcal{U}_{i_\pi}$. □

The case where $N = p = 2q + 1$, p, q prime

Let $R = \mathbb{Z}/p\mathbb{Z}$, where p is prime and $p = 2q + 1$, with q prime. Then the group of units $\mathcal{U}$ is cyclic of order $p - 1 = 2q$. Set $U = \{\pm 1\}$; then $\mathcal{U}/U$ is cyclic with prime order q.

Because R is a field, the orbit structure of $\mathcal{U}$ acting on R is very simple. There are only two orbits: $\mathcal{O}_0 = \mathcal{U} = R \setminus (0)$ and $\mathcal{O}_1 = (0)$. The stabilizer subgroups of a point are $\mathcal{U}_0 = \{1\}$ and $\mathcal{U}_1 = \mathcal{U}$, respectively.

Proposition 4.3. *Let $R = \mathbb{Z}/p\mathbb{Z}$, with prime p satisfying $p = 2q + 1$, q prime. Set $U = \{\pm 1\}$. If $\pi \in (\widehat{\mathcal{U}} : U)$, then $\ker \pi = U\mathcal{U}_{i_\pi}$.*

Proof. Take any $\pi \in (\widehat{\mathcal{U}} : U)$. Because $\mathcal{U}/U$ has prime order, $\ker \pi$ (viewed as a subgroup of $\mathcal{U}/U$) is either trivial or all of $\mathcal{U}/U$. When viewing π as a character on $\mathcal{U}$, $\ker \pi = U$ or $\ker \pi = \mathcal{U}$. In the first case, $i_\pi = 0$, so that $\ker \pi = U = U\mathcal{U}_0$; in the second case, $i_\pi = 1$, and $\ker \pi = \mathcal{U} = U\mathcal{U}_1$. □

A common corollary

Propositions 4.1, 4.2, and 4.3 all lead to a common corollary.

Corollary 4.4. *Let $R = \mathbb{Z}/N\mathbb{Z}$, with, respectively, $N = 2^{\ell+1}$, $N = 3^{\ell+1}$, or $N = p = 2q + 1$, with p and q prime. Let $U = \{\pm 1\}$. Let w be w_L or w_E on R. For any $\pi \in (\widehat{\mathcal{U}} : U)$,*

- *the quotient groups $\mathcal{U}/U\mathcal{U}_j$ are cyclic groups of prime power order;*
- *the character π, viewed as a homomorphism $\pi : \mathcal{U}/U\mathcal{U}_{i_\pi} \to \mathbb{C}$, is injective; and*
- *the function $f : \mathcal{U}/U\mathcal{U}_{i_\pi} \to \mathbb{Q}$, $f(u) = w(up^{i_\pi})$, is well-defined and injective. (Here, p is 2, 3, or p, respectively.)*

Proof. The group $\mathcal{U}/U\mathcal{U}_j$ is a quotient of the group $\mathcal{U}/U$, which is cyclic of prime power order (under the hypotheses on N). By Propositions 4.1, 4.2, and 4.3, $\ker \pi = U\mathcal{U}_{i_\pi}$, so that the character π viewed as $\pi : \mathcal{U}/U\mathcal{U}_{i_\pi} \to \mathbb{C}$ is injective. That the function f is well-defined and injective follows from the definition of $\mathcal{U}_{i_\pi}$ and the $\pm$-symmetry of w (i.e., $w(-x) = w(x)$, for $x \in R$). □

5. Proof of Theorem 2.3

The proof of Theorem 2.3 will depend upon understanding the Fourier transform of a function defined on a cyclic group of prime power order. In this section we isolate the necessary lemma that will be used and then prove Theorem 2.3.

Let p be a prime, and suppose G is a cyclic group of order p^k. Let $\gamma \in G$ be a generator of G. Given any function $f : G \to \mathbb{C}$, the *Fourier transform* of f is a function $\hat{f} : \widehat{G} \to \mathbb{C}$, given by

$$\hat{f}(\pi) = \sum_{g \in G} \pi(g) f(g), \quad \pi \in \widehat{G}.$$

Lemma 5.1. *Assume G is a cyclic group of order p^k, p prime. If $\pi \in \widehat{G}$ is injective as a function $\pi : G \to \mathbb{C}$ and $f : G \to \mathbb{Q}$ is any injective function with rational values, then $\hat{f}(\pi) \neq 0$.*

Proof. The image $\xi = \pi(\gamma)$ under π of the generator γ of G is a p^kth root of unity. Because π is assumed to be injective, ξ is a primitive p^kth root of unity. As $g = \gamma^j$ varies over G, the images $\pi(g) = \xi^j$

vary over all the p^kth roots of unity. The Fourier transform of f has the form

$$\hat{f}(\pi) = \sum_{j=0}^{p^k-1} f(\gamma^j)\xi^j. \tag{2}$$

The summation in (2), with $0 \le j < p^k$, can be written as a double summation by making use of the residue class m of j mod p^{k-1}. Write $j = ip^{k-1} + m$, with $0 \le i < p$ and $0 \le m < p^{k-1}$. As a double summation, the Fourier transform is

$$\hat{f}(\pi) = \sum_{i=0}^{p-1} \sum_{m=0}^{p^{k-1}-1} f(\gamma^{ip^{k-1}+m})\xi^{ip^{k-1}+m}. \tag{3}$$

To simplify (3), we make use of the minimal polynomial of ξ over $\mathbb{Q}$. The minimal polynomial of ξ over $\mathbb{Q}$ has degree $\phi(p^k) = p^{k-1}(p-1)$, and the minimal polynomial itself is the cyclotomic polynomial

$$\Phi_{p^k}(x) = x^{(p-1)p^{k-1}} + x^{(p-2)p^{k-1}} + \cdots + x^{p^{k-1}} + 1. \tag{4}$$

In (3), those terms where $i = p-1$ will be replaced by the following expression derived from the minimal polynomial (4):

$$\xi^{(p-1)p^{k-1}+m} = -\sum_{i=0}^{p-2} \xi^{ip^{k-1}+m}. \tag{5}$$

After substituting the expressions from (5) into (3), the form of $\hat{f}(\pi)$ becomes

$$\hat{f}(\pi) = \sum_{i=0}^{p-2} \sum_{m=0}^{p^{k-1}-1} \{f(\gamma^{ip^{k-1}+m}) - f(\gamma^{(p-1)p^{k-1}+m})\}\xi^{ip^{k-1}+m}. \tag{6}$$

Observe from (6) that $\hat{f}(\pi)$, as a polynomial in ξ, has degree $< (p-1)p^{k-1}$, the latter being the degree of the minimal polynomial of ξ over $\mathbb{Q}$. If $\hat{f}(\pi) = 0$, then all the (rational) coefficients of the powers of ξ must vanish. This contradicts f being injective. □

Proof of Theorem 2.3. When $N = 2^{\ell+1}$, $N = 3^{\ell+1}$, or $N = p = 2q+1$, p, q prime, Corollary 4.4 shows that the groups $\mathcal{U}/U\mathcal{U}_j$ are cyclic of prime power order. It also shows that a character $\pi \in (\widehat{\mathcal{U}} : U)$ is injective on $\mathcal{U}/U\mathcal{U}_j$ when $j = i_\pi$. Set $G = \mathcal{U}/U\mathcal{U}_{i_\pi}$, and define $f : G \to \mathbb{Q}$ by $f(u) = w(up^{i_\pi})$, where w is w_L or w_E. This is a well-defined injective function on G.

Under the assumptions above, Lemma 5.1 implies that

$$\check{w}(\pi, i_\pi) = \sum_{u \in \mathcal{U}/U\mathcal{U}_{i_\pi}} w(up^{i_\pi})\pi(u) \neq 0$$

(see (1)). Because the $\check{w}(\pi, i_\pi)$ are the factors of $\det \mathcal{A}_w$ in Theorem 3.5, we conclude that $\det \mathcal{A}_w \neq 0$. By Theorem 3.1, the extension property holds in the cases claimed in the statement of the theorem. □

The same arguments show that Theorem 2.3 holds for any *rational*-valued weight satisfying the conditions of Remark 3.2 such that $w(x) = w(y)$ implies $y = \pm x$. Rational weights yield rational coefficients in (6), which are needed to apply the minimal polynomial argument.

Remark 5.2. Consider the case where $R = \mathbb{Z}/p\mathbb{Z}$, with $p = 4q + 1$ and p, q prime, as in Remark 2.4. The group $\mathcal{U}/U$ is cyclic of order $2q$. For any $\pi \in (\widehat{\mathcal{U}} : U)$, $\ker \pi$ (viewed as a subgroup of $\mathcal{U}/U$) will be cyclic of order 1, 2, q, or $2q$. Barra provides separate arguments for each of the four cases. Refer to [1, Theorem 5.28] for the details.

For other values of N, the type of analysis given above quickly becomes very complicated. The group $\mathcal{U}/U$ need not be cyclic, and even in cases (such as N prime) where $\mathcal{U}/U$ is cyclic, it need not have prime power order. The degree and form of the cyclotomic polynomial becomes complicated, and the number of different cases to consider quickly gets out of hand.

6. An egalitarian weight and the proof of Theorem 2.6

Theorem 2.6 will be a special case of a general result valid over any finite module with a cyclic socle, in particular, over any finite Frobenius ring. The treatment here generalizes that for Frobenius bimodules in [18, Section 2.3] and will be rather brisk. Readers wanting more background information are also referred to [16].

We work in the following context. Let R be a finite ring with 1, and let A be a finite unitary left R-module. Suppose χ is an *generating character* for A, i.e., $\chi : A \to \mathbb{C}^\times$ is a homomorphism from the additive group of A to the multiplicative group of nonzero complex numbers that has the property that $\ker \chi$ contains no nonzero left R-submodules. Such a generating character exists if and only if the socle of A is cyclic [17, Proposition 14] (and in the case where $A = R$, a generating character exists if and only if the ring R is Frobenius [12, Theorem 3.10]). It follows that any character π on A is a right scalar multiple of χ; i.e., $\pi = \chi^r$, for some $r \in R$, where $\chi^r(a) = \chi(ra)$ for $a \in A$.

Let G be a subgroup of the automorphism group $GL_R(A)$. We will write elements $g \in GL_R(A)$ as acting on the right of A, so that the preservation of scalar multiplication takes the form $(rx)g = r(xg)$, for $r \in R$, $x \in A$, and $g \in GL_R(A)$.

Define a weight $w_G : A \to \mathbb{C}$ on A by

$$w_G(x) = 1 - \frac{1}{|G|} \sum_{g \in G} \chi(xg), \quad x \in A.$$

A weight w on A is *egalitarian* if there exists a nonzero constant γ such that $\sum_{x \in B} w(b) = \gamma |B|$ for any nonzero left R-submodule $B \subseteq A$.

Proposition 6.1. *The weight w_G has the following properties.*

1. *The value $w_G(0) = 0$.*
2. *The weight w_G is right G-invariant; i.e., $w_G(xg) = w_G(x)$, for all $x \in A$ and $g \in G$.*
3. *The weight w_G is egalitarian with $\gamma = 1$. Moreover, w_G is egalitarian on cosets with $\gamma = 1$; i.e., $\sum_{b \in B} w_G(x_0 + b) = |B|$ for any nonzero left R-submodule $B \subseteq A$ and element $x_0 \in A$.*

Proof. Because $\chi(0) = 1$, the first result is immediate. The right invariance follows immediately by a re-indexing argument. To prove that w_G is egalitarian on cosets, let $x_0 \in A$ and $B \subseteq A$ be a nonzero submodule. We calculate:

$$\begin{aligned} \sum_{b \in B} w_G(x_0 + b) &= \sum_{b \in B} \left(1 - \frac{1}{|G|} \sum_{g \in G} \chi((x_0 + b)g) \right) \\ &= |B| - \frac{1}{|G|} \sum_{g \in G} \chi(x_0 g) \sum_{b \in B} \chi(bg) = |B|, \end{aligned}$$

where we have used the fact that $\sum_{b\in B}\chi(bg)=0$ for any nonzero left submodule B. Indeed, because $\ker\chi$ contains no nonzero left submodules, there exists some $b_0\in B$ with $\chi(b_0g)\neq 1$. By re-indexing $(b=b_0+c)$, we see that $\sum_{b\in B}\chi(bg)=\chi(b_0g)\sum_{c\in B}\chi(cg)$. Thus, $\sum_{b\in B}\chi(bg)=0$. □

Remark 6.2. When $A=R$ and $G=\mathcal{U}(R)$, the group of units of R, the resulting weight $w_{\mathcal{U}(R)}$ is the homogeneous weight on R [9]. The egalitarian property for the homogeneous weight was proved in [8, Theorem 2]. The proof of the next theorem generalizes that for the homogeneous weight found in [2, Theorem 6.6].

Theorem 6.3. *The weight w_G has the extension property. That is, if $C\subseteq A^n$ is a left R-linear code in A^n and $f:C\to A^n$ is an injective homomorphism of R-modules that preserves w_G, $w_G(xf)=w_G(x)$ for all $x\in C$, then f extends to a G-monomial transformation of A^n.*

Proof. Write the components of f as $f=(f_1,f_2,\dots,f_n)$; each $f_i:C\to A$ is a homomorphism of left R-modules. Inputs to f_i are written on the left. Weight preservation and the definition of w_G yield, for all $x\in C$,

$$\sum_{i=1}^{n}\left(1-\frac{1}{|G|}\sum_{g\in G}\chi((xf_i)g)\right)=\sum_{i=1}^{n}\left(1-\frac{1}{|G|}\sum_{g\in G}\chi(x_ig)\right).$$

This simplifies to

$$\sum_{i=1}^{n}\sum_{g\in G}\chi((xf_i)g)=\sum_{i=1}^{n}\sum_{g\in G}\chi(x_ig),\quad x\in C. \tag{7}$$

This is an equation of functions on C, specifically, linear combinations of characters on C. Because characters are linearly independent over the complex numbers, if we set $i=1$ and $g=\mathrm{id}_G$ on the left side of (7), there exist $i=\sigma(1)$ and $g_1\in G$ on the right side so that $\chi(xf_1)=\chi(x_{\sigma(1)}g_1)$ for all $x\in C$. This implies that the image of the module homomorphism $C\to A$, $x\mapsto xf_1-x_{\sigma(1)}g_1$, is contained in $\ker\chi$. But $\ker\chi$ contains no nonzero left submodules, so $xf_1=x_{\sigma(1)}g_1$ for all $x\in C$.

It now follows, by re-indexing, that

$$\sum_{g\in G}\chi(xf_1g)=\sum_{g\in G}\chi(x_{\sigma(1)}g_1g)=\sum_{g\in G}\chi(x_{\sigma(1)}g)$$

for all $x\in C$. This allows us to reduce by one the size of the outer summation in (7) and to proceed by induction to produce a permutation σ of $\{1,2,\dots,n\}$ and elements $g_i\in G$ with $xf_i=x_{\sigma(i)}g_i$ for all $x\in C$ and $i=1,2,\dots,n$. □

Proof of Theorem 2.6. Let $R=\mathbb{Z}/N\mathbb{Z}$, $A=R$, and $G=\{\pm1\}$. A generating character for $\mathbb{Z}/N\mathbb{Z}$ is $\chi(x)=\exp(2\pi ix/N)$, $x\in\mathbb{Z}/N\mathbb{Z}$, where exp is the usual complex exponential function. Then $\chi(x)+\chi(-x)=2\cos(2\pi x/N)$, so that

$$w_G(x)=1-\cos(2\pi x/N),\quad x\in\mathbb{Z}/N\mathbb{Z}.$$

Up to a factor of 2, $w_G(x)$ equals w_{PSK}. □

Acknowledgment: We thank Aleams Barra for renewing our interest in this problem. The second author thanks the Université de Toulon for its support for research visits in 2000 and 2015, when the ideas of this paper were developed and finalized.

References

[1] A. Barra, Equivalence Theorems and the Local-Global Property, ProQuest LLC, PhD thesis University of Kentucky, Ann Arbor, MI, USA, 2012.

[2] A. Barra, H. Gluesing–Luerssen, MacWilliams extension theorems and the local–global property for codes over Frobenius rings, J. Pure Appl. Algebra 219(4) (2015) 703–728.

[3] S. Dyshko, P. Langevin, J. A. Wood, Deux analogues au déterminant de Maillet, C. R. Math. Acad. Sci. Paris 354(7) (2016) 649–652.

[4] F. G. Frobenius, Gesammelte Abhandlungen, Springer–Verlag, Berlin, 1968.

[5] M. Greferath, T. Honold, C. Mc Fadden, J. A. Wood, J. Zumbrägel, MacWilliams' extension theorem for bi-invariant weights over finite principal ideal rings, J. Combin. Theory Ser. A 125 (2014) 177–193.

[6] M. Greferath, C. Mc Fadden, J. Zumbrägel, Characteristics of invariant weights related to code equivalence over rings, Des. Codes Cryptogr. 66(1) (2013) 145–156.

[7] M. Greferath, S. E. Schmidt, Finite–ring combinatorics and MacWilliams' equivalence theorem, J. Combin. Theory Ser. A 92(1) (2000) 17–28.

[8] W. Heise, T. Honold, Homogeneous and egalitarian weights on finite rings, Proceedings of the Seventh International Workshop on Algebraic and Combinatorial Coding Theory (ACCT-2000), Bansko, Bulgaria, 183–188, 2000.

[9] T. Honold, Characterization of finite Frobenius rings, Arch. Math. 76(6) (2001) 406–415.

[10] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990.

[11] J. A. Wood, Extension theorems for linear codes over finite rings, Applied algebra, algebraic algorithms and error–correcting codes (Toulouse, 1997), Lecture Notes in Comput. Sci. 1255 (1997) 329–340.

[12] J. A. Wood, Duality for modules over finite rings and applications to coding theory, Amer. J. Math. 121(3) (1999) 555–575.

[13] J. A. Wood, Weight functions and the extension theorem for linear codes over finite rings, Finite fields: theory, applications, and algorithms (Waterloo, ON, 1997), Contemp. Math. 225 (1999) 231–243.

[14] J. A. Wood, Factoring the semigroup determinant of a finite chain ring, Coding Theory, Cryptography and Related Areas (2000) 249–264.

[15] J. A. Wood, The structure of linear codes of constant weight, Trans. Amer. Math. Soc. 354(3) (2002) 1007–1026.

[16] J. A. Wood, Foundations of linear codes defined over finite modules: the extension theorem and the MacWilliams identities. Codes over rings, 124–190, Ser. Coding Theory Cryptol., 6, World Sci. Publ., Hackensack, NJ, 2009.

[17] J. A. Wood, Applications of finite Frobenius rings to the foundations of algebraic coding theory. Proceedings of the 44th Symposium on Ring Theory and Representation Theory, 223–245, Symp. Ring Theory Represent. Theory Organ. Comm., Nagoya, 2012.

[18] J. A. Wood, Relative one-weight linear codes, Des. Codes Cryptogr. 72(2) (2014) 331–344.