The extension theorem for Lee and Euclidean weight codes over integer residue rings

Serhii Dyshko

The Extension Theorem for Lee and Euclidean weight codes over integer residue rings

Serhii Dyshko
s.v.dyshko@gmail.com

Abstract

The Extension Theorem is proved for the Lee and Euclidean weights over the integer residue ring $\mathbb{Z}_m$, for $m \geq 2$.

This is a post-peer-review, pre-copyedit version of an article published in Designs, Codes and Cryptography. The final authenticated version is available online at: http://dx.doi.org/10.1007%2Fs10623-018-0521-2

1 Introduction

In the classical theory of error-correcting codes a linear code is defined as a subspace of a finite-dimensional vector space over a finite field alphabet equipped with the Hamming weight. MacWilliams proved in [15] her famous Extension Theorem which states that each linear Hamming isometry of a linear code extends to a monomial map, that is, every linear map that preserves the Hamming weight on the code acts by permutation of coordinates and multiplication of coordinates by nonzero scalars from the field.

Linear codes over ring alphabets became popular after the paper [10], in which the authors prove that certain well-known nonlinear binary codes, such as Kerdock and Preparata codes, can be very simply constructed as binary images under the Gray map of linear codes over $\mathbb{Z}_4$.

Of particular interest for us is the ring $\mathbb{Z}_m$ of integers modulo m, $m \geq 2$, equipped with different weight functions. Like in the case of linear codes over a finite field alphabet, it is an interesting problem to determine if an analogue of the MacWilliams Extension Theorem holds for linear codes over $\mathbb{Z}_m$ for different weights. Some known results and facts about the extension properties of such codes are listed below.

One of the results of [20] implies that the extension property holds for $\mathbb{Z}_m$ equipped with the Hamming weight. In [9] it was mentioned that the extension property holds for the homogeneous weight, defined in [3]. In [7] there were characterized all weights on $\mathbb{Z}_m$ with the maximum symmetry group for which the extension theorem holds. Some interesting examples of weights on $\mathbb{Z}_m$ for which the extension property does not hold are observed in [1] and [21].

In this paper we are interested in the Lee and Euclidean weights on $\mathbb{Z}_m$ and their extension properties. The Lee weight first appeared in [14] and was later studied in [17]. It is defined as follows: putting the ordered elements $0, \ldots, m-1$ of $\mathbb{Z}_m$ evenly distributed on the circle, the Lee weight of an element is the distance on the circle from the element to zero. See Definition 3 for more details. The Euclidean weight is defined

as a square of the Lee weight, see Definition 4. Both weights carry the same symmetry group.

The symmetry group of the Lee weight in general is small compared to the maximum possible symmetry group of a weight on $\mathbb{Z}_m$. Hence the mentioned known results on the extension property do not apply in this case. However, as it was pointed out by one of the referees, in [4] the authors proved a weaker version of the extension theorem for the so-called "egalitarian" weight on $\mathbb{Z}_m$: every linear weight preserving map extends to a monomial map (not necessarily weight preserving). This weight has no assumptions on its symmetry group. For the case $m = 2^k$ the Lee weight is egalitarian, which means that every Lee weight preserving linear map on a code extends to a monomial map, not necessarily Lee weight preserving.

Originally, the difficulty of the extension problem for the Lee weight was pointed out by Wood in [21]. Later, in [22] *Wood conjectured that the extension property holds for the alphabet $\mathbb{Z}_m$ equipped with the Lee weight for every integer $m \geq 2$*, however, the conjecture remained unproved till now. In [2] Barra proved the conjecture for primes of the form $m = 4p + 1$, where p is prime. He also checked the validity of Wood's conjecture for the first 2000 prime m. In [12] Langevin and Wood proved the conjecture for $m = 2^k$, $m = 3^k$, where k is a positive integer, and for primes of the special form $m = 2p + 1$, where p is a prime. Such prime p is called a Sophie Germain prime and the number $2p + 1$ associated with p is called a safe prime. In [5] we resolved the case of all prime m. A work in preparation [13] describes a solution of the problem for the case when m is a power of prime. However, its approach does not seem to work for other integers.

The papers [5] and [12] also consider the extension problem for the Euclidean weight. It is proved that for the mentioned values of m, that is, primes and powers of 2 and 3, the extension property holds for the Euclidean weight as well.

In this paper we give a proof of the conjecture for all integers $m \geq 2$. The original idea of Wood in [21] is to reduce the extension problem for the alphabet $\mathbb{Z}_m$ equipped with some weight to a calculation of the determinant of a special square matrix. Every entry of the matrix is equal to the weight of some element in $\mathbb{Z}_m$. His determinant criterion is the main tool in all the papers [2, 5, 12] related to the conjecture. Our approach is "dual" — we calculate the determinant of a square matrix with entries equal to the discrete Fourier transform of the Lee weight calculated for elements in $\mathbb{Z}_m$. The approach allows us to formulate the dual determinant criterion for arbitrary weight on $\mathbb{Z}_m$, see Proposition 1, and finally prove the Extension Theorem for the Lee weight on $\mathbb{Z}_m$, see Theorem 1. We also improve the existing results for the Euclidean weight by proving the extension theorem for all $m \geq 2$ using our determinant criterion, see Theorem 2 and Remark 2.

2 Preliminaries

Let m be a positive integer. We represent the ring $\mathbb{Z}_m$ in the usual way as a set of integers,

$$\mathbb{Z}_m := \{0, \ldots, m-1\}.$$

The ring $\mathbb{Z}_m$ is a commutative ring with identity. Denote the group of units of $\mathbb{Z}_m$ as $\mathbb{Z}_m^*$ and represent it as the set,

$$\mathbb{Z}_m^* := \{x \in \mathbb{Z}_m \mid (x, m) = 1\}.$$

A *weight* ω on the alphabet $\mathbb{Z}_m$ is a map $\mathbb{Z}_m \to \mathbb{C}$. Some authors require a weight ω to be nonnegative, to satisfy the condition $\omega(0) = 0$, or to satisfy the triangle inequality. In this paper we do not require any of these.

Let n be a positive integer. For an element $\vec{x} \in \mathbb{Z}_m^n$ we define its weight as,

$$\omega(\vec{x}) := \sum_{i=1}^{n} \omega(x_i).$$

For a weight $\omega : \mathbb{Z}_m \to \mathbb{C}$ we define its *symmetry group*,

$$G(\omega) := \left\{ h \in \mathbb{Z}_m^* \mid \forall x \in \mathbb{Z}_m,\ \omega(hx) = \omega(x) \right\}.$$

For example, the symmetry group of the Hamming weight on $\mathbb{Z}_m$ is $\mathbb{Z}_m^*$.

Definition 1. Let G be a subgroup of $\mathbb{Z}_m^*$. A map $f : \mathbb{Z}_m^n \to \mathbb{Z}_m^n$ is called *G-monomial* if there exist a permutation $\pi \in \mathfrak{S}_n$ and elements $g_1, \ldots, g_n \in G$ such that for every $\vec{x} \in \mathbb{Z}_m^n$,

$$f(x_1, \ldots, x_n) = (g_1 x_{\pi(1)}, \ldots, g_n x_{\pi(n)}).$$

It is true that for every $\vec{x} \in \mathbb{Z}_m^n$ and each $G(\omega)$-monomial map f, $\omega(f(\vec{x})) = \omega(\vec{x})$. That is, $G(\omega)$-monomial maps preserve the weight ω. The converse is not always true.

Definition 2. The alphabet $\mathbb{Z}_m$ has *the extension property with respect to the weight* ω if for every positive integer n and for every $\mathbb{Z}_m$-linear code $C \subseteq \mathbb{Z}_m^n$ each $\mathbb{Z}_m$-linear ω-preserving map $f : C \to \mathbb{Z}_m^n$ extends to a $G(\omega)$-monomial map.

2.1 Characters and the Fourier transform

In order to prove our extension criterion we are going to use the character-theoretic approach, first introduced in [19] and generalized in [20, 21, 22]. In this section we recall basic properties of characters and the Fourier transform over finite abelian groups, which can be found in the textbooks [11] and [18].

Consider the abelian group of nonzero complex numbers with respect to multiplication, $(\mathbb{C}^*, \times)$. Let M be a finite abelian group. Denote by

$$\widehat{M} := \mathrm{Hom}(M, \mathbb{C}^*)$$

the *group of characters* of M. The isomorphism $\widehat{M} \cong M$ holds. In fact, the map $M \to \widehat{\widehat{M}}, w \mapsto [\chi \mapsto \chi(w)]$ is a canonical isomorphism of groups. In this paper we identify M and $\widehat{\widehat{M}}$.

The *Fourier transform* of a map $\phi : M \to \mathbb{C}$ is the map $\mathcal{F}(\phi) : \widehat{M} \to \mathbb{C}$ defined as

$$\mathcal{F}(\phi)(\chi) := \sum_{w \in M} \phi(w)\chi(w).$$

The Fourier transform is $\mathbb{C}$-linear and invertible.

Let H be a subgroup of M. Define the *group annihilator* $H^\perp \subseteq \widehat{M}$ as

$$H^\perp := \left\{ \chi \in \widehat{M} \mid \forall w \in H, \chi(w) = 1 \right\}.$$

For all subgroups $H \subseteq M$, $N \subseteq \widehat{M}$,

$$H^{\perp\perp} = H, \quad N^{\perp\perp} = N.$$

Let m be a positive integer and let $\omega : \mathbb{Z}_m \to \mathbb{C}$ be a map. Denote by

$$\theta(x) := \exp\left(2\pi i \frac{x}{m}\right)$$

the canonical additive character of $\mathbb{Z}_m$. We identify the groups $\mathbb{Z}_m$ and $\widehat{\mathbb{Z}_m}$ considering the group isomorphism $\mathbb{Z}_m \to \widehat{\mathbb{Z}_m}, x \mapsto [y \mapsto \theta(xy)]$. Then, the Fourier transform of ω is the map $\mathcal{F}(\omega) : \mathbb{Z}_m \to \mathbb{C}$,

$$\mathcal{F}(\omega)(y) = \sum_{x \in \mathbb{Z}_m} \omega(x)\theta(xy).$$

The map $\mathcal{F}(\omega) : \mathbb{Z}_m \to \mathbb{C}$, denoted $\widehat{\omega}$, is know as the *discrete Fourier transform* of ω. The discrete Fourier transform is also $\mathbb{C}$-linear and the equalities hold, for all $x \in \mathbb{Z}_m$,

$$\widehat{\widehat{\omega}}(x) = m\,\omega(-x)$$

and

$$\sum_{y \in \mathbb{Z}_m} \widehat{\omega}(y) = m\,\omega(0). \tag{1}$$

For all $g \in \mathbb{Z}_m^*$ and all $y \in \mathbb{Z}_m$,

$$\widehat{\omega}(gy) = \sum_{x \in \mathbb{Z}_m} \omega(x)\theta(xgy) = \sum_{x \in \mathbb{Z}_m} \omega(g^{-1}x)\theta(xy) = \widehat{\omega g^{-1}}(y). \tag{2}$$

The symmetry groups of a weight $\omega : \mathbb{Z}_m \to \mathbb{C}$ and its discrete Fourier transform coincide,

$$G(\omega) = G(\widehat{\omega}). \tag{3}$$

Indeed, from eq. (2), $G(\omega) \subseteq G(\widehat{\omega})$ and thus $G(\widehat{\omega}) \subseteq G(\widehat{\widehat{\omega}}) = G(\omega)$.

2.2 Auxiliary map

In this section we introduce an auxiliary map, which plays an important role in the proof of Proposition 1.

Note that every finite abelian group of exponent dividing m is a $\mathbb{Z}_m$-module in a natural way, and this action is the only possible one if the module shall be unital. For the dual group the same holds.

Let M be a finite $\mathbb{Z}_m$-module. Consider a module homomorphism $\sigma \in \mathrm{Hom}(M, \mathbb{Z}_m)$. Denote $a = |\mathrm{im}\,\sigma|$ and $b = \frac{m}{a}$. Since $\mathrm{im}\,\sigma$ is a submodule of $\mathbb{Z}_m$,

$$\mathrm{im}\,\sigma = b\mathbb{Z}_m \cong \mathbb{Z}_a.$$

For the map σ we define the *auxiliary map* $\widetilde{\sigma} : \mathbb{Z}_a \to \widehat{M}$ as, for all $x \in \mathbb{Z}_a$ and all $w \in M$,

$$\widetilde{\sigma}(x)(w) := \theta\left(x\frac{\sigma(w)}{b}\right).$$

It is easy to check that $\widetilde{\sigma}$ is an injective module homomorphism.

Lemma 1. *For every $\sigma \in \mathrm{Hom}(M, \mathbb{Z}_m)$ the equality holds,*

$$(\ker\sigma)^\perp = \mathrm{im}\,\widetilde{\sigma}.$$

Proof. Calculate,

$$\begin{aligned}\ker\sigma &= \{w \in M \mid \sigma(w) = 0\}\\ &= \left\{w \in M \mid \forall x \in \mathbb{Z}_a, \theta\left(x\frac{\sigma(w)}{b}\right) = 1\right\}\\ &= \{w \in M \mid \forall x \in \mathbb{Z}_a, \widetilde{\sigma}(x)(w) = 1\}\\ &= \{w \in M \mid \forall \chi \in \operatorname{im}\widetilde{\sigma}, \chi(w) = 1\} = (\operatorname{im}\widetilde{\sigma})^{\perp}.\end{aligned}$$

Hence, $(\ker\sigma)^{\perp} = (\operatorname{im}\widetilde{\sigma})^{\perp\perp} = \operatorname{im}\widetilde{\sigma}$. □ □

Let $\omega : \mathbb{Z}_m \to \mathbb{C}$ be a map. The map $\omega_a : \mathbb{Z}_a \to \mathbb{C}$, defined as

$$\omega_a(x) := \omega(bx),$$

is the restriction of ω to the submodule $b\mathbb{Z}_m \cong \mathbb{Z}_a$. Note that $\widehat{\omega_a}$ is a map $\mathbb{Z}_a \to \mathbb{C}$.

Lemma 2. *For each $\chi \in \widehat{M}$,*

$$\mathcal{F}(\omega\sigma)(\chi) = \begin{cases} |\ker\sigma|\widehat{\omega_a}\left(\widetilde{\sigma}^{-1}(\chi)\right) & , \chi \in \operatorname{im}\widetilde{\sigma};\\ 0 & , \chi \notin \operatorname{im}\widetilde{\sigma}.\end{cases}$$

Proof. For each $\chi \in \operatorname{im}\widetilde{\sigma}$,

$$\begin{aligned}\mathcal{F}(\omega\sigma)(\chi) &= \sum_{w\in M}\omega(\sigma(w))\widetilde{\sigma}(\widetilde{\sigma}^{-1}(\chi))(w)\\ &= \sum_{w\in M}\omega(\sigma(w))\theta\left(\widetilde{\sigma}^{-1}(\chi)\frac{\sigma(w)}{b}\right)\\ &= |\ker\sigma|\sum_{x\in\mathbb{Z}_a}\omega_a(x)\theta\left(\widetilde{\sigma}^{-1}(\chi)x\right)\\ &= |\ker\sigma|\widehat{\omega_a}\left(\widetilde{\sigma}^{-1}(\chi)\right).\end{aligned}$$

Using Lemma 1, for each $\chi \notin \operatorname{im}\widetilde{\sigma} = (\ker\sigma)^{\perp}$ there exists $w_0 \in \ker\sigma$ such that $\chi(w_0) \neq 1$. Then,

$$\begin{aligned}\mathcal{F}(\omega\sigma)(\chi) &= \sum_{w+w_0\in M}\omega(\sigma(w+w_0))\chi(w+w_0)\\ &= \sum_{w\in M}\omega(\sigma(w))\chi(w)\chi(w_0)\\ &= \chi(w_0)\,\mathcal{F}(\omega\sigma)(\chi),\end{aligned}$$

and thus $\mathcal{F}(\omega\sigma)(\chi) = 0$. □ □

3 Determinant criterion

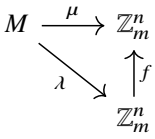
Let $m \geq 2$ and n be positive integers. Let $C \subseteq \mathbb{Z}_m^n$ be a $\mathbb{Z}_m$-linear code and let $f \in \operatorname{Hom}(C, \mathbb{Z}_m^n)$. Let M be a $\mathbb{Z}_m$-module isomorphic to C, called a *message set*. Following [19], let $\lambda \in \operatorname{Hom}(M, \mathbb{Z}_m^n)$ be *an encoding map of C*, i.e., an injective map such that $\operatorname{im}\lambda = C$, in the form

$$\lambda = (\lambda_1, \ldots, \lambda_n),$$

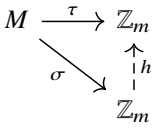
where $\lambda_i \in \mathrm{Hom}(M, \mathbb{Z}_m)$ is a projection on the ith coordinate, for $i \in \{1, \ldots, n\}$. Define the map $\mu \in \mathrm{Hom}(M, \mathbb{Z}_m^n)$,

$$\mu := f\lambda,$$

and the corresponding projections $\mu_i \in \mathrm{Hom}(M, \mathbb{Z}_m)$, for $i \in \{1, \ldots, n\}$.



Lemma 3. *Let σ, τ be two maps in* $\mathrm{Hom}(M, \mathbb{Z}_m)$ *and denote* $a = |\mathrm{im}\,\sigma|$. *If* $\ker\sigma = \ker\tau$, *then* $\mathrm{im}\,\sigma = \mathrm{im}\,\tau$ *and there exists unique* $h \in \mathbb{Z}_a^*$ *such that* $\tau = h\sigma$.



Proof. Since the kernels are equal, consider two canonical injective homomorphisms $\overline{\sigma}, \overline{\tau} : M/\ker\sigma \to \mathbb{Z}_m$. Note that $\mathrm{im}\,\sigma = \mathrm{im}\,\overline{\sigma}$ and $\mathrm{im}\,\sigma \cong M/\ker\sigma$. The cardinalities of the submodules $\mathrm{im}\,\sigma$ and $\mathrm{im}\,\tau$ of $\mathbb{Z}_m$ are equal, hence $\mathrm{im}\,\sigma = \mathrm{im}\,\tau$. The map $\overline{\tau}\overline{\sigma}^{-1}$ is an automorphism of $\mathrm{im}\,\sigma \cong \mathbb{Z}_a$ and thus there exists unique $h \in \mathbb{Z}_a^*$ such that $\overline{\tau}\overline{\sigma}^{-1}(x) = hx$ for all $x \in \mathrm{im}\,\sigma$. For every $w \in M$, $\tau(w) = \overline{\tau}(\overline{w}) = h\overline{\sigma}(\overline{w}) = h\sigma(w)$, where $\overline{w} = w + \ker\sigma$, $\overline{w} \in M/\ker\sigma$. □ □

For a map $\omega : \mathbb{Z}_m \to \mathbb{C}$ define the square matrix over $\mathbb{C}$,

$$W(\omega) := \left(\omega\left(g^{-1}h\right)\right)_{g,h \in \mathbb{Z}_m^*/G(\omega)}.$$

The matrix is well-defined.

Remark 1. Matrices of this and similar forms naturally appear in earlier studies of the extension problem, as for example in [6] and [21]. Also, they were used in more recent works [8] and [12]. In the mentioned papers the extension property for a weight ω was derived by proving that $\det W(\omega)$ is nonzero. In the next proposition we prove a similar determinant criterion but in terms of the discrete Fourier transform of the weight.

Let a be a positive divisor of m. Recall that $G(\omega)$ is a symmetry group of the weight $\omega : \mathbb{Z}_m \to \mathbb{C}$ and recall that $\omega_a(x) = \omega\left(\frac{m}{a}x\right)$. Consider the symmetry group

$$G(\omega_a) = \left\{h \in \mathbb{Z}_a^* \mid \forall x \in \mathbb{Z}_a,\ \omega_a(hx) = \omega_a(x)\right\}$$

of the weight $\omega_a : \mathbb{Z}_a \to \mathbb{C}$.

Proposition 1. *Let $\omega : \mathbb{Z}_m \to \mathbb{C}$ be a weight. If for all positive $a|m$, $a \neq 1$, the matrix $W(\widehat{\omega_a})$ is invertible,*

$$\det W(\widehat{\omega_a}) \neq 0,$$

and the map

$$G(\omega) \to G(\omega_a), g \mapsto g \bmod a,$$

is onto, then $\mathbb{Z}_m$ has the extension property with respect to the weight ω.

Proof. Let $C \subseteq \mathbb{Z}_m^n$ be a linear code and let $f : C \to \mathbb{Z}_m^n$ be a linear ω-preserving map. The map f is ω-preserving if and only if $\omega\lambda = \omega\mu$, i.e.,

$$\sum_{i=1}^{n} \omega\lambda_i = \sum_{j=1}^{n} \omega\mu_j,$$

as functions $M \to \mathbb{C}$. Calculating the Fourier transform of both sides we get the following dual equality of functions on $\widehat{M}$,

$$\sum_{i=1}^{n} \mathcal{F}(\omega\lambda_i) = \sum_{j=1}^{n} \mathcal{F}(\omega\mu_j).$$

We split the rest of the proof of the proposition into four parts.

Part 1. Among all the submodules $\operatorname{im}\widetilde{\lambda_i}$, $\operatorname{im}\widetilde{\mu_j}$ of $\widehat{M}$, for $i, j \in \{1, \ldots, n\}$, choose one maximal with respect to inclusion and let $\sigma \in \operatorname{Hom}(M, \mathbb{Z}_m)$ denote the map that corresponds to the chosen module. As in Section 2.2, we denote $a = |\operatorname{im}\sigma|$.

If $\operatorname{im}\widetilde{\sigma}$ is the zero submodule, then $\sigma = \lambda_i = \mu_j = 0$ for all $i, j \in \{1, \ldots, n\}$ and thus $C = \{0\}$ and f is the zero map, which extends to a $G(\omega)$-monomial map. We assume that $\operatorname{im}\widetilde{\sigma}$ is a non-zero submodule and thus $a \neq 1$.

By analogy with the group of units $\mathcal{U}(\mathbb{Z}_m) = \mathbb{Z}_m^*$, for a $\mathbb{Z}_m$-module N let $\mathcal{U}(N)$ denote the set of elements that generate the module,

$$\mathcal{U}(N) := \{x \in N \mid \langle x \rangle = N\}.$$

If N is not cyclic, then $\mathcal{U}(N) = \emptyset$. Note that the module $\operatorname{im}\widetilde{\sigma}$ is cyclic as a homomorphic image of a cyclic module. We want to restrict the obtained equality of the Fourier transforms to the non-empty set $\mathcal{U}(\operatorname{im}\widetilde{\sigma})$.

Assume $\mathcal{U}(\operatorname{im}\widetilde{\sigma}) \cap \operatorname{im}\widetilde{\lambda_i} \neq \emptyset$ for some $i \in \{1, \ldots, n\}$. Obviously, $\operatorname{im}\widetilde{\sigma} \subseteq \operatorname{im}\widetilde{\lambda_i}$. Since the image $\operatorname{im}\widetilde{\sigma}$ is maximal with respect to inclusion, for all $i \in \{1, \ldots, n\}$, $\operatorname{im}\widetilde{\sigma} \not\subset \operatorname{im}\widetilde{\lambda_i}$. Therefore $\operatorname{im}\widetilde{\sigma} = \operatorname{im}\widetilde{\lambda_i}$. From Lemma 1, $\ker\sigma = \ker\lambda_i$.

According to Lemma 2, the map $\mathcal{F}(\omega\lambda_i)$ has its support in the set $\operatorname{im}\widetilde{\lambda_i}$. Hence, if $\ker\sigma \neq \ker\lambda_i$, then $\mathcal{U}(\operatorname{im}\widetilde{\sigma}) \cap \operatorname{im}\widetilde{\lambda_i} = \emptyset$ and thus $\mathcal{F}(\omega\lambda_i) = 0$ on $\mathcal{U}(\operatorname{im}\widetilde{\sigma})$. In the same way, if $\ker\sigma \neq \ker\mu_j$, for some $j \in \{1, \ldots, n\}$, then $\mathcal{F}(\omega\mu_j) = 0$ on $\mathcal{U}(\operatorname{im}\widetilde{\sigma})$.

Let us denote $I = \{i \mid \ker\sigma = \ker\lambda_i\}$ and $J = \{j \mid \ker\sigma = \ker\mu_j\}$. At least one of the sets I or J is nonempty. The restriction of the dual equality to $\mathcal{U}(\operatorname{im}\widetilde{\sigma})$ gives us the following,

$$\sum_{i \in I} \mathcal{F}(\omega\lambda_i) = \sum_{j \in J} \mathcal{F}(\omega\mu_j).$$

Part 2. We transform this equality of functions on $\widehat{M}$ to an equivalent equality of functions on $\mathbb{Z}_a$.

Since $\ker\lambda_i = \ker\mu_j = \ker\sigma$, for $i \in I$ and $j \in J$, from Lemma 3, there exist unique $g_i, h_j \in \mathbb{Z}_a^*$ such that $\lambda_i = g_i\sigma$ and $\mu_j = h_j\sigma$. And the equality becomes,

$$\sum_{i \in I} \mathcal{F}(\omega g_i\sigma) = \sum_{j \in J} \mathcal{F}(\omega h_j\sigma).$$

We get, moving the terms to the left hand side of the equality and changing the summation over all $g \in \mathbb{Z}_a^*$,

$$\sum_{g \in \mathbb{Z}_a^*} x_g \, \mathcal{F}(\omega g\sigma) = 0$$

on $\mathcal{U}(\operatorname{im}\widetilde{\sigma})$, where

$$x_g := |\{i \in I \mid g\sigma = \lambda_i\}| - |\{j \in J \mid g\sigma = \mu_j\}|.$$

From Lemma 2, $\mathcal{F}(\omega g\sigma) = |\ker\sigma|\widehat{\omega_a g}\widetilde{\sigma}^{-1}$ on $\mathcal{U}(\operatorname{im}\widetilde{\sigma})$, and we get

$$|\ker\sigma|\left(\sum_{g\in\mathbb{Z}_a^*} x_g\widehat{\omega_a g}\right)\widetilde{\sigma}^{-1} = 0$$

on $\mathcal{U}(\operatorname{im}\widetilde{\sigma})$. Since $\widetilde{\sigma}$ is injective,

$$\sum_{g\in\mathbb{Z}_a^*} x_g\widehat{\omega_a g} = 0,$$

on $\mathcal{U}(\mathbb{Z}_a) = \mathbb{Z}_a^*$.

Part 3. We simplify the obtained equality using the symmetries of the map ω_a. Using eq. (2), for all $h \in \mathbb{Z}_a^*$,

$$\sum_{g\in\mathbb{Z}_a^*} x_g\widehat{\omega_a}(g^{-1}h) = 0.$$

Group together equal terms considering the action of the group $G(\omega_a) \overset{(3)}{=} G(\widehat{\omega_a})$,

$$\sum_{g\in\mathbb{Z}_a^*/G(\omega_a)}\left(\sum_{t\in G(\omega_a)} x_{tg}\right)\widehat{\omega_a}(g^{-1}h) = 0,$$

for all $h \in \mathbb{Z}_a^*/G(\omega_a)$. Since the matrix $W(\widehat{\omega_a})$ is invertible, for each $g \in \mathbb{Z}_a^*/G(\omega_a)$,

$$\sum_{t\in G(\omega_a)} x_{tg} = 0.$$

Part 4. From this equality we are going to deduce the conditions on the encoding maps $\lambda_i, i \in I$, and $\mu_j, j \in J$. Rewriting it,

$$\sum_{t\in G(\omega_a)} |\{i \in I \mid tg\sigma = \lambda_i\}| = \sum_{t\in G(\omega_a)} |\{j \in J \mid tg\sigma = \mu_i\}|,$$

or the same, using Lemma 3,

$$|\{i \in I \mid \exists t \in G(\omega_a),\ tg\sigma = \lambda_i\}| = |\{j \in J \mid \exists t \in G(\omega_a),\ tg\sigma = \mu_i\}|,$$

for all $g \in \mathbb{Z}_a^*/G(\omega_a)$. Therefore, there exist a bijection $\pi : I \to J$ and $t_i \in G(\omega_a)$, for $i \in I$, such that $\lambda_i = t_i\mu_{\pi(i)}$.

From the second assumption of the statement, for each $i \in I$ there exists $t_i' \in G(\omega)$ such that $t_i' y = t_i y$, for all $y \in \operatorname{im}\sigma \cong \mathbb{Z}_a$, and thus $\lambda_i = t_i'\mu_{\pi(i)}$.

Since for all $t \in G(\omega)$, for all $i \in I$ and all $j \in J$, $\omega t\lambda_i = \omega\lambda_i$ and $\omega t\mu_j = \omega\mu_j$, the equality

$$\sum_{i\in I}\omega\lambda_i = \sum_{j\in J}\omega\mu_j$$

holds on the whole module M. Subtract the obtained equality from the first equality of the proof. We get

$$\sum_{i\in\{1,\dots,n\}\setminus I}\omega\lambda_i = \sum_{j\in\{1,\dots,n\}\setminus J}\omega\mu_j.$$

Repeat for this equality all the steps starting from the beginning of the proof.

Finally, we come up with a permutation $\pi \in \mathfrak{S}_n$ and maps $t'_i \in G(\omega)$ such that for all $i \in \{1,\dots,n\}$, $\lambda_i = t'_i \mu_{\pi(i)}$. Therefore, f extends to a $G(\omega)$-monomial map. □ □

To illustrate our determinant criterion we give yet another proof of the extension theorem for the Hamming weight on $\mathbb{Z}_m$.

Example 1. Let $m \geq 2$ be a positive integer. Consider the Hamming weight $\mathrm{H} : \mathbb{Z}_m \to \{0,1\}$. Calculate,

$$\widehat{\mathrm{H}}(x) = \begin{cases} m-1 & , x = 0; \\ -1 & , x \neq 0. \end{cases}$$

The symmetry group $G(\widehat{\mathrm{H}}) \overset{(3)}{=} G(\mathrm{H})$ coincides with the full group $\mathbb{Z}_m^*$. Since the quotient $\mathbb{Z}_m^*/G(\mathrm{H})$ contains only one class $\{\bar{1}\}$, $\det W(\widehat{\mathrm{H}}) = \widehat{\mathrm{H}}(1) = -1 \neq 0$.

For every positive integer $a \neq 1$ that divides m the weight $\mathrm{H}_a : \mathbb{Z}_a \to \{0,1\}$ is also the Hamming weight and therefore $W(\widehat{\mathrm{H}_a}) \neq 0$. The map $G(\mathrm{H}) = \mathbb{Z}_m^* \to \mathbb{Z}_a^* = G(\mathrm{H}_a), x \mapsto (x \bmod a)$ is onto. From Proposition 1, for each positive integer m the alphabet $\mathbb{Z}_m$ has the extension property with respect to the Hamming weight.

The following two examples show that the assumptions of Proposition 1 are vital for the conclusion to hold.

Example 2. Consider the weight $\omega : \mathbb{Z}_6 \to \mathbb{Z}$ defined in the following table along with its discrete Fourier transform.

x	0	1	2	3	4	5
$\omega(x)$	0	3	2	1	2	3
$\widehat{\omega}(x)$	11	0	−4	−3	−4	0

The map $\widehat{\omega}$ equals zero in both points of the group $G(\widehat{\omega}) = G(\omega) = \mathbb{Z}_6^* = \{1,5\}$. The quotient group is $\mathbb{Z}_6^*/G(\omega) = \{\bar{1}\}$, and therefore the matrix $W(\widehat{\omega})$ is the zero 1×1 matrix with the zero determinant. Nevertheless, the second condition of Proposition 1 is satisfied, since $G(\omega_3) = \{1,2\}$ and $G(\omega_2) = \{1\}$.

The extension property does not hold for $\mathbb{Z}_6$ equipped with the weight ω. Consider the code $C = \mathbb{Z}_6^2$ and the map $f \in \mathrm{Hom}(C, \mathbb{Z}_6^2)$, defined by,

$$\begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix} \overset{f}{\to} \begin{matrix} 2 & 3 \\ 3 & 2 \end{matrix}.$$

The map f preserves the weight ω and does not extend to a $G(\omega)$-monomial map.

Example 3. Consider the weight $\omega : \mathbb{Z}_6 \to \mathbb{Z}$ defined in the following table along with its discrete Fourier transform.

x	0	1	2	3	4	5
$\omega(x)$	0	1	1	1	1	2
$\widehat{\omega}(x)$	6	$\frac{-1-\sqrt{3}i}{2}$	$\frac{-3-\sqrt{3}i}{2}$	−2	$\frac{-3+\sqrt{3}i}{2}$	$\frac{-1+\sqrt{3}i}{2}$

Calculate the groups, $G(\omega) = \{1\} \subset \mathbb{Z}_6^*$, $G(\omega_2) = \{1\} = \mathbb{Z}_2^*$ and $G(\omega_3) = \{1,2\} = \mathbb{Z}_3^*$. Obviously, the second condition of Proposition 1 does not hold for $a = 3$, because $(1 \bmod 3) = 1 \neq 2$ in $\mathbb{Z}_3^*$.

We check that the first condition of Proposition 1 is satisfied for $a = 6$, $a = 3$ and $a = 2$. Calculate the determinant of $W(\widehat{\omega})$,

$$\det W(\widehat{\omega}) = \det \begin{pmatrix} \frac{-1-\sqrt{3}i}{2} & \frac{-1+\sqrt{3}i}{2} \\ \frac{-1+\sqrt{3}i}{2} & \frac{-1-\sqrt{3}i}{2} \end{pmatrix} = \sqrt{3}i \neq 0.$$

For $a = 3$ and $a = 2$, ω_a is the Hamming weight on $\mathbb{Z}_a$, and from Example 1, $\det W(\widehat{\omega_a}) = -1 \neq 0$. Now we consider the code C and the map $f \in \mathrm{Hom}(C, \mathbb{Z}_6^2)$, defined by,

$$1 \quad 2 \xrightarrow{f} 1 \quad 4 \ .$$

The map f preserves the weight ω and does not extend to a $G(\omega)$-monomial map, even though it extends to a $\mathbb{Z}_6^*$-monomial map.

4 Extension theorem for the Lee weight

Definition 3. *The Lee weight* $\mathrm{L} : \mathbb{Z}_m \to \mathbb{N}_0$ is the map defined as follows,

$$\mathrm{L}(x) := \begin{cases} x & , x \leq \frac{m}{2}; \\ m - x & , x > \frac{m}{2}. \end{cases}$$

Our proof of the extension theorem for the Lee weight follows the idea presented in Example 1. However, for the Lee weight the main difficulty is in the calculation of its discrete Fourier transform $\widehat{\mathrm{L}}$ and proving that the matrix $W(\widehat{\mathrm{L}})$ is invertible. Unlike the case of the Hamming weight, the symmetry group $G(\mathrm{L})$ is much smaller, in general, than $\mathbb{Z}_m^*$, and $W(\widehat{\mathrm{L}})$ is no longer a 1×1 square matrix.

Denote $r := \lceil \frac{m}{2} \rceil$ and define the parity indicator $\delta := 1$ if m is even and $\delta := 0$ if m is odd. Since $\mathrm{L}(x) = \mathrm{L}(m - x)$, for $x \in \mathbb{Z}_m$, the Fourier coefficients of L are in $\mathbb{R}$.

Lemma 4. *For each* $x \in \mathbb{Z}_m \setminus \{0\}$,

$$\widehat{\mathrm{L}}(x) = -\left(\frac{\sin r\frac{\pi x}{m}}{\sin \frac{\pi x}{m}} \right)^2 . \tag{4}$$

Proof. Let n be a positive integer and let $\alpha \in \mathbb{R}$. The *Fejér kernel* is the real-valued map defined on $\mathbb{R}$,

$$F_n(\alpha) := \frac{1}{n} \left(\frac{\sin \frac{n}{2}\alpha}{\sin \frac{\alpha}{2}} \right)^2 = 1 + 2 \sum_{k=1}^{n-1} \left(1 - \frac{k}{n} \right) \cos k\alpha.$$

The *Dirichlet kernel* is the map defined as,

$$D_{n-1}(\alpha) := \frac{\sin \frac{2n-1}{2}\alpha}{\sin \frac{\alpha}{2}} = 1 + 2 \sum_{k=1}^{n-1} \cos k\alpha.$$

Combining the equalities for the Fejér kernel and the Dirichlet kernel we get,

$$\sum_{k=1}^{n-1} k \cos k\alpha = \frac{n}{2} \left(D_{n-1}(\alpha) - F_n(\alpha) \right).$$

Put $\alpha = \frac{\pi x}{m} \in (0, \pi)$. Then,

$$\widehat{\mathrm{L}}(x) = \sum_{k=0}^{m-1} \mathrm{L}(k) \cos 2k\alpha = 2 \sum_{k=1}^{r-1} k \cos 2k\alpha + r(-1)^x \delta$$
$$= r \left(D_{r-1}(2\alpha) - F_r(2\alpha) + (-1)^x \delta \right).$$

For the odd $m = 2r - 1$,

$$D_{r-1}(2\alpha) = \frac{\sin(2r-1)\alpha}{\sin \alpha} = \frac{\sin \pi x}{\sin \frac{\pi x}{m}} = 0.$$

For the even $m = 2r$,

$$D_{r-1}(2\alpha) = \frac{\sin(2r-1)\alpha}{\sin \alpha} = \frac{\sin\left(\pi x - \frac{\pi x}{m}\right)}{\sin \frac{\pi x}{m}} = (-1)^{x+1}.$$

Finally, $\widehat{\mathrm{L}}(x) = -rF_r\left(\frac{2\pi x}{m}\right) = -\left(\frac{\sin r\frac{\pi x}{m}}{\sin \frac{\pi x}{m}}\right)^2$. □ □

Lemma 5. *The following inequality holds,*

$$-4\widehat{\mathrm{L}}(1) > \widehat{\mathrm{L}}(0). \tag{5}$$

Proof. From Lemma 4,

$$\widehat{\mathrm{L}}(1) = -\left(\frac{\sin \frac{r\pi}{m}}{\sin \frac{\pi}{m}}\right)^2,$$

and calculate

$$\widehat{\mathrm{L}}(0) = 2 \sum_{k=0}^{r-1} k + r\delta = r(r-1) + r\delta = \frac{m^2 - 1 + \delta}{4}.$$

Recall the well-known trigonometric inequalities, for $\alpha \in (0, \frac{\pi}{2})$,

$$\frac{2}{\pi}\alpha < \sin \alpha < \alpha. \tag{6}$$

Consider the following,

$$-4\widehat{\mathrm{L}}(1) = 4\left(\frac{\sin \frac{r\pi}{m}}{\sin \frac{\pi}{m}}\right)^2 \overset{(6)}{>} 4\left(\frac{\sin \frac{2\pi}{3}}{\frac{\pi}{m}}\right)^2 = \frac{3m^2}{\pi^2} > \frac{m^2}{4} \geq \widehat{\mathrm{L}}(0).$$

□ □

The symmetry group of the Lee weight is equal to $\{1, m-1\}$. To simplify the notations, we denote this group by $\{\pm 1\}$.

Lemma 6. *The matrix $W(\widehat{\mathrm{L}})$ is invertible,*

$$\det W(\widehat{\mathrm{L}}) \neq 0.$$

Proof. From eq. (3), $G(\widehat{\mathrm{L}}) = G(\mathrm{L}) = \{\pm 1\}$. Recall that

$$W(\widehat{\mathrm{L}}) = \left(\widehat{\mathrm{L}}(g^{-1}h)\right)_{g,h\in\mathbb{Z}_m^*/\{\pm 1\}}.$$

If $m = 2$, then $\det W(\widehat{\mathrm{L}}) = \widehat{\mathrm{L}}(1) = -1 \neq 0$, so we assume that $m > 2$.

Each row and column of the matrix $W(\widehat{\mathrm{L}})$ is a permutation of the Fourier coefficients $\widehat{\mathrm{L}}(g)$ calculated for all $g \in \mathbb{Z}_m^*/\{\pm 1\}$. Hence, each row and each column of the matrix contain exactly one element $\widehat{\mathrm{L}}(1)$, which, up to the sign of the determinant, can be relocated on the main diagonal of the matrix by permuting rows or columns.

Let us take the set of class representatives of $\mathbb{Z}_m^*/\{\pm 1\}$ in $\mathbb{Z}_m^*$ to be a subset of $\{1,\ldots,r-1\}$, since $m > 2$.

For the following sum over all $x \in (\mathbb{Z}_m^*/\{\pm 1\}) \setminus \{1\}$ the inequalities hold,

$$\begin{aligned}
\sum_x |\widehat{\mathrm{L}}(x)| &\leq \sum_{x=2}^{r-1} |\widehat{\mathrm{L}}(x)| \\
&\overset{(4)}{=} -\sum_{x=2}^{r-1} \widehat{\mathrm{L}}(x) = -\sum_{x=2}^{r-1} \widehat{\mathrm{L}}(x) + \frac{m}{2}\,\mathrm{L}(0) \\
&\overset{(1)}{=} -\sum_{x=2}^{r-1} \widehat{\mathrm{L}}(x) + \frac{1}{2}\sum_{x=0}^{m-1} \widehat{\mathrm{L}}(x) = \frac{1}{2}\left(\widehat{\mathrm{L}}(0) + 2\widehat{\mathrm{L}}(1) + \widehat{\mathrm{L}}(r)\delta\right) \\
&\overset{(5)}{<} \frac{1}{2}\left(-4\widehat{\mathrm{L}}(1) + 2\widehat{\mathrm{L}}(1)\right) = -\widehat{\mathrm{L}}(1) \\
&\overset{(4)}{=} |\widehat{\mathrm{L}}(1)|.
\end{aligned}$$

From the Levy–Desplanques dominant diagonal criterion, the determinant $\det W(\widehat{\mathrm{L}})$ is nonzero. □ □

Theorem 1. *For every integer $m \geq 2$ the alphabet $\mathbb{Z}_m$ has the extension property with respect to the Lee weight.*

Proof. To prove this theorem we use Proposition 1. Let $a|m$, $a \neq 1$, be a positive integer and denote $b = \frac{m}{a}$. Let ℓ denote the Lee weight on $\mathbb{Z}_a$. For all $x \in \mathbb{Z}_a$, $\mathrm{L}_a(x) = \mathrm{L}(bx) = b\ell(x)$. Since the discrete Fourier transform is $\mathbb{C}$-linear,

$$\det W(\widehat{\mathrm{L}_a}) = b^{|\mathbb{Z}_a^*/\{\pm 1\}|} \cdot \det W(\widehat{\ell}).$$

From Lemma 6, $\det W(\widehat{\ell}) \neq 0$ and hence $\det W(\widehat{\mathrm{L}_a}) \neq 0$. The first condition of Proposition 1 is satisfied thereby. The second condition is satisfied as well, since $\{1, m-1\} \to \{1, a-1\}, g \mapsto (g \bmod a)$ is onto. From Proposition 1 the alphabet $\mathbb{Z}_m$ has the extension property with respect to the Lee weight. □ □

5 Extension theorem for the Euclidean weight

Definition 4. *The Euclidean weight* $\mathrm{E} : \mathbb{Z}_m \to \mathbb{N}_0$ is the map defined as follows,

$$\mathrm{E}(x) := \begin{cases} x^2 & , x \leq \frac{m}{2}; \\ (m-x)^2 & , x > \frac{m}{2}. \end{cases}$$

In other words, $\mathrm{E} = \mathrm{L}^2$.

As in the case with the Lee weight, the proof of the extension theorem for the Euclidean weight depends on the calculation of the Fourier coefficients of $\widehat{\mathrm{E}}$ and the determinant of the matrix $W(\widehat{\mathrm{E}})$. The proof of the fact that $\det W(\widehat{\mathrm{E}})$ is nonzero is slightly more elaborate, though.

As in the previous section, we denote $r = \lceil \frac{m}{2} \rceil$ and the parity indicator $\delta = 1$ if m is even and $\delta = 0$ if m is odd. Since $\mathrm{E}(x) = \mathrm{E}(m - x)$, for $x \in \mathbb{Z}_m$, the Fourier coefficients of E are in $\mathbb{R}$.

Lemma 7. *For every* $x \in \mathbb{Z}_m \setminus \{0\}$,

$$\widehat{\mathrm{E}}(x) = \begin{cases} (-1)^x \frac{m}{2\sin^2 \frac{\pi x}{m}}, & m \text{ is even;} \\ (-1)^x \frac{m}{2\sin^2 \frac{\pi x}{m}} \cos \frac{\pi x}{m}, & m \text{ is odd.} \end{cases}$$

Proof. Recall that the Dirichlet kernel is the map defined as,

$$D_{n-1}(\alpha) = \frac{\sin \frac{2n-1}{2}\alpha}{\sin \frac{\alpha}{2}} = 1 + 2\sum_{k=1}^{n-1} \cos k\alpha,$$

for $\alpha \in \mathbb{R}$. Let us denote the second derivative,

$$R_c(\beta) := \left(\frac{\sin c\beta}{\sin \beta}\right)''_{\beta\beta} = -\frac{1}{\sin^3 \beta}\left(\sin c\beta \left((c^2+1)\sin^2 \beta - 2\right) + c \sin 2\beta \cos c\beta\right),$$

for $c \in \mathbb{R}, \beta \in \mathbb{R} \setminus \{0\}$. Then

$$\sum_{k=1}^{n-1} k^2 \cos k\alpha = -\frac{1}{2}(D_{n-1}(\alpha))''_{\alpha\alpha} = -\frac{1}{2}\left(\frac{\sin \frac{2n-1}{2}\alpha}{\sin \frac{\alpha}{2}}\right)''_{\alpha\alpha} = -\frac{1}{8}R_{2n-1}\left(\frac{\alpha}{2}\right).$$

Put $\alpha = \frac{\pi x}{m} \in (0, \pi)$ and calculate,

$$\begin{aligned} \widehat{\mathrm{E}}(x) &= \sum_{k=0}^{m-1} E(k) \cos 2k\alpha = 2\sum_{k=1}^{r-1} k^2 \cos 2k\alpha + \delta(-1)^x r^2 \\ &= -\frac{1}{4}R_{2r-1}(\alpha) + \delta(-1)^x \frac{m^2}{4}. \end{aligned}$$

For the even $m = 2r$,

$$\begin{aligned} \sin(2r-1)\alpha &= \sin(2r-1)\frac{\pi x}{2r} = (-1)^{x+1} \sin \frac{\pi x}{2r} = (-1)^{x+1} \sin \alpha, \\ \cos(2r-1)\alpha &= \cos(2r-1)\frac{\pi x}{2r} = (-1)^x \cos \frac{\pi x}{2r} = (-1)^x \cos \alpha, \end{aligned}$$

and hence,

$$\begin{aligned} R_{2r-1}(\alpha) &= -\frac{1}{\sin^3 \alpha}\Big((-1)^{x+1} \sin \alpha \left((4r^2 - 4r + 2)\sin^2 \alpha - 2\right) \\ &\quad + (4r-2)\sin \alpha \cos \alpha (-1)^x \cos \alpha\Big) \\ &= \frac{(-1)^x}{\sin^2 \alpha}\left(\left(4r^2 - (4r-2)\right)\sin^2 \alpha - 2 - (4r-2)\cos^2 \alpha\right) \\ &= \frac{(-1)^x}{\sin^2 \alpha}\left(4r^2 \sin^2 \alpha - 4r\right) \\ &= (-1)^x 4r^2 - \frac{(-1)^x 4r}{\sin^2 \alpha} = (-1)^x m^2 - \frac{(-1)^x 2m}{\sin^2 \alpha}. \end{aligned}$$

For the odd $m = 2r - 1$,

$$\sin(2r-1)\alpha = \sin(2r-1)\frac{\pi x}{2r-1} = 0, \quad \cos(2r-1)\alpha = (-1)^x,$$

and

$$R_{2r-1}(\alpha) = -\frac{1}{\sin^3\alpha}\left((-1)^x(4r-2)\sin\alpha\cos\alpha\right) = -\frac{(-1)^x 2m\cos\alpha}{\sin^2\alpha}.$$

Substituting the obtained values in the expression for $\widehat{\mathrm{E}}$ we get the statement of the lemma. □ □

Lemma 8. *The following inequality holds,*

$$\det W(\widehat{\mathrm{E}}) \neq 0.$$

Proof. The symmetry group of the Euclidean weight E is equal to $\{\pm 1\}$. Recall that

$$W(\widehat{\mathrm{E}}) = \left(\widehat{\mathrm{E}}(g^{-1}h)\right)_{g,h\in\mathbb{Z}_m^*/\{\pm1\}}.$$

If $m = 2$ or $m = 3$, then $\det W(\widehat{\mathrm{E}}) = \widehat{\mathrm{E}}(1) = -1 \neq 0$, so we assume that $m > 3$.

Each row and column of the matrix $W(\widehat{\mathrm{E}})$ is a permutation of the Fourier coefficients $\widehat{\mathrm{E}}(g)$ calculated for all $g \in \mathbb{Z}_m^*/\{\pm1\}$. Hence, each row and each column of the matrix contain exactly one element $\widehat{\mathrm{E}}(1)$, which, up to the sign of the determinant, can be relocated on the main diagonal of the matrix by permuting rows or columns.

Let us take the set of class representatives of $\mathbb{Z}_m^*/\{\pm1\}$ in $\mathbb{Z}_m^*$ to be a subset of $\{1,\dots,r-1\}$, since $m > 3$.

Recall the famous Euler's sum,

$$\sum_{x=1}^{\infty}\frac{1}{x^2} = \frac{\pi^2}{6}. \tag{7}$$

As in the proof of Theorem 1 we are going to bound the sum of the absolute values of the Fourier coefficients $|\widehat{\mathrm{E}}(x)|$ over all $x \in (\mathbb{Z}_m^*/\{\pm1\}) \setminus \{1\}$ by the single value $|\widehat{\mathrm{E}}(1)|$.

Let us bound the Fourier coefficients for even m,

$$|\widehat{\mathrm{E}}(x)| = \frac{m}{2\sin^2\frac{\pi x}{m}} \overset{(6)}{<} \frac{m}{2\left(\frac{2x}{m}\right)^2} = \frac{m^3}{8x^2},$$

$$|\widehat{\mathrm{E}}(1)| = \frac{m}{2\sin^2\frac{\pi}{m}} \overset{(6)}{>} \frac{m}{2\left(\frac{\pi}{m}\right)^2} = \frac{m^3}{2\pi^2}.$$

Since $2 \notin \mathbb{Z}_m^*$, the inequalities for the sum are the following,

$$\sum_x |\widehat{\mathrm{E}}(x)| \leq \sum_{x=3}^{r-1}|\widehat{\mathrm{E}}(x)| < \sum_{x=3}^{\infty}\frac{m^3}{8x^2} \overset{(7)}{=} \frac{m^3}{8}\left(\frac{\pi^2}{6} - 1 - \frac{1}{4}\right) < \frac{m^3}{2\pi^2} < |\widehat{\mathrm{E}}(1)|.$$

We recall the following trigonometric inequality (see [16, Section 3.4.18]), for $\alpha \in (0, \frac{\pi}{2})$,

$$\cos\alpha < \frac{\sin^2\alpha}{\alpha^2}. \tag{8}$$

For odd $m \geq 5$,

$$|\widehat{\mathrm{E}}(x)| = \frac{m \cos \frac{\pi x}{m}}{2 \sin^2 \frac{\pi x}{m}} \overset{(8)}{<} \frac{m}{2\left(\frac{\pi x}{m}\right)^2} = \frac{m^3}{2\pi^2 x^2},$$
$$|\widehat{\mathrm{E}}(1)| = \frac{m \cos \frac{\pi}{m}}{2 \sin^2 \frac{\pi}{m}} \overset{(6)}{>} \frac{m \cos \frac{\pi}{m}}{2\left(\frac{\pi}{m}\right)^2} = \frac{m^3 \cos \frac{\pi}{m}}{2\pi^2}.$$

Since $\cos \frac{\pi}{m} > \cos \frac{\pi}{4} = \frac{1}{\sqrt{2}}$, for the sum we get the following bound,

$$\sum_x |\widehat{\mathrm{E}}(x)| \leq \sum_{x=2}^{r-1} |\widehat{\mathrm{E}}(x)| < \sum_{x=2}^{\infty} \frac{m^3}{2\pi^2 x^2} \overset{(7)}{=} \frac{m^3}{2\pi^2}\left(\frac{\pi^2}{6} - 1\right) < \frac{m^3 \cos \frac{\pi}{m}}{2\pi^2} < |\widehat{\mathrm{E}}(1)|.$$

From the Levy–Desplanques dominant diagonal criterion, the determinant of $W(\widehat{\mathrm{E}})$ is nonzero. □ □

Theorem 2. *For every integer $m \geq 2$ the alphabet $\mathbb{Z}_m$ has the extension property with respect to the Euclidean weight.*

Proof. The proof of this theorem repeats the proof of Theorem 1 with minor changes. Let $a|m$, $a \neq 1$, be a positive integer and denote $b = \frac{m}{a}$. Let e denote the Euclidean weight on $\mathbb{Z}_a$. For all $x \in \mathbb{Z}_a$, $\mathrm{E}_a(x) = \mathrm{E}(bx) = b^2 e(x)$. Since the discrete Fourier transform is $\mathbb{C}$-linear,

$$\det W(\widehat{\mathrm{E}_a}) = b^{2|\mathbb{Z}_a^*/\{\pm 1\}|} \cdot \det W(\widehat{e}).$$

From Lemma 8, $\det W(\widehat{e}) \neq 0$ and hence $\det W(\widehat{\mathrm{E}_a}) \neq 0$. The first condition of Proposition 1 is satisfied thereby. The second condition is satisfied as well, since $\{1, m-1\} \to \{1, a-1\}, g \mapsto (g \bmod a)$ is onto. From Proposition 1 the alphabet $\mathbb{Z}_m$ has the extension property with respect to the Euclidean weight. □ □

Remark 2. In [12] there was mentioned another Euclidean weight $\mathrm{E}^{\mathrm{PSK}} : \mathbb{Z}_m \to \mathbb{C}$, which is used in phase-shift key modulation. It is defined using the squared Euclidean distance in the complex numbers, for $x \in \mathbb{Z}_m$,

$$\mathrm{E}^{\mathrm{PSK}}(x) := \left|1 - \exp\left(\frac{2\pi i x}{m}\right)\right|^2 = 2 - 2\cos\frac{2\pi x}{m}.$$

In [12] the authors proved the extension theorem for this weight for all $m \geq 2$. It can also be easily proved using the approach we used for the Lee and Euclidean weights. The main points of our proof follow. First, for all $m \geq 2$, $G(\mathrm{E}^{\mathrm{PSK}}) = \{\pm 1\}$. Second, for all positive $a|m$, $a \neq 1$, the restricted weight $\mathrm{E}_a^{\mathrm{PSK}}$ on $\mathbb{Z}_a$ coincides with $\mathrm{E}^{\mathrm{PSK}}$. And third, for all $m \geq 3$ and all $x \in \mathbb{Z}_m$,

$$\widehat{\mathrm{E}^{\mathrm{PSK}}}(x) = \begin{cases} 2m & , x = 0; \\ -m & , x \in \{\pm 1\}; \\ 0 & , x \notin \{-1, 0, 1\}. \end{cases}$$

The resulting matrix $W(\widehat{\mathrm{E}^{\mathrm{PSK}}})$ is a square diagonal matrix with $-m$ on the main diagonal and zeros elsewhere. The extension property follows from Proposition 1. The details of the proof, which repeats the proofs of Theorem 1 and Theorem 2, are left to the reader.

References

[1] A. Barra. *Equivalence Theorems and the Local-Global Property*. Doctoral dissertation, University of Kentucky, 2012.

[2] A. Barra. MacWilliams Equivalence Theorem for the Lee weight over $\mathbb{Z}_{4p+1}$. *Malaysian Journal of Science*, 34(2):222–226, 2015.

[3] I. Constantinescu and W. Heise. A metric for codes over residue class rings. *Problems of Information Transmission*, 33:208–213, 1997.

[4] I. Constantinescu, W. Heise, and T. Honold. Monomial extensions of isometries between codes over $\mathbb{Z}_m$. In *Proceedings of the 5th International Workshop on Algebraic and Combinatorial Coding Theory (ACCT'96), Unicorn Shumen*, pages 98–104, 1996.

[5] S. Dyshko, P. Langevin, and J. A. Wood. Deux analogues au déterminant de Maillet. *Comptes Rendus Mathematique*, 354(7):649–652, July 2016.

[6] M. Greferath. Orthogonality matrices for modules over finite Frobenius rings and MacWilliams' equivalence theorem. *Finite Fields and Their Applications*, 8(3):323 – 331, 2002.

[7] M. Greferath and T. Honold. Monomial extensions of isometries of linear codes II: invariant weight functions on $\mathbb{Z}_m$. In *Proceedings of the Tenth International Workshop in Algebraic and Combinatorial Coding Theory (ACCT-10), Zvenigorod, Russia*, pages 106–111, 2006.

[8] M. Greferath, T. Honold, C. M. Fadden, J. A. Wood, and J. Zumbrägel. MacWilliams' extension theorem for bi-invariant weights over finite principal ideal rings. *Journal of Combinatorial Theory, Series A*, 125:177–193, 2014.

[9] M. Greferath, A. Nechaev, and R. Wisbauer. Finite quasi-Frobenius modules and linear codes. *Journal of Algebra and Its Applications*, 03(03):247–272, 2004.

[10] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Sole. The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Transactions on Information Theory*, 40(2):301–319, Mar. 1994.

[11] B. Huppert. *Character theory of finite groups*. Number 25 in De Gruyter expositions in mathematics. Walter de Gruyter, Berlin ; New York, 1998.

[12] P. Langevin and J. A. Wood. The extension problem for Lee and Euclidean weights. *Journal of Algebra Combinatorics Discrete Structures and Applications*, 4(2):207–217, 2017.

[13] P. Langevin and J. A. Wood. The extension theorem for the Lee and Euclidean weights over $\mathbb{Z}/p^k\mathbb{Z}$. *to appear in the Journal of Pure and Applied Algebra*, 2018.

[14] C. Lee. Some properties of nonbinary error-correcting codes. *IRE Transactions on Information Theory*, 4(2):77–82, June 1958.

[15] J. MacWilliams. Error-Correcting Codes for Multiple-Level Transmission. *Bell System Technical Journal*, 40(1):281–308, Jan. 1961.

[16] D. S. Mitrinović. *Analytic Inequalities*. Springer Berlin Heidelberg, Berlin, Heidelberg, 1970. DOI: 10.1007/978-3-642-99970-3.

[17] C. Satyanarayana. Lee metric codes over integer residue rings (Corresp.). *IEEE Transactions on Information Theory*, 25(2):250–254, Mar. 1979.

[18] A. Terras. *Fourier Analysis on Finite Groups and Applications*. Cambridge University Press, Mar. 1999.

[19] H. N. Ward and J. A. Wood. Characters and the equivalence of codes. *Journal of Combinatorial Theory, Series A*, 73(2):348 – 352, 1996.

[20] J. A. Wood. Duality for modules over finite rings and applications to coding theory. *American Journal of Mathematics*, 121(3):555–575, 1999.

[21] J. A. Wood. Weight functions and the extension theorem for linear codes over finite rings. *Contemporary Mathematics*, 225:231–243, 1999.

[22] J. A. Wood. The structure of linear codes of constant weight. *Transactions of the American Mathematical Society*, 354(3):1007–1026, 2002.