TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 354, Number 3, Pages 1007–1026
S 0002-9947(01)02905-1
Article electronically published on October 26, 2001

THE STRUCTURE OF LINEAR CODES OF CONSTANT WEIGHT

JAY A. WOOD

Abstract. In this paper we determine completely the structure of linear codes over $\mathbb{Z}/N\mathbb{Z}$ of constant weight. Namely, we determine exactly which modules underlie linear codes of constant weight, and we describe the coordinate functionals involved. The weight functions considered are: Hamming weight, Lee weight, two forms of Euclidean weight, and pre-homogeneous weights. We prove a general uniqueness theorem for virtual linear codes of constant weight. Existence is settled on a case by case basis.

1. Introduction

This paper classifies the structure of linear codes of constant weight over $\mathbb{Z}/(N) = \mathbb{Z}/N\mathbb{Z}$. A linear code having constant weight means that every nonzero codeword has the same weight. Hamming, Lee, and Euclidean weights are all examined.

The classification specifies which modules over $\mathbb{Z}/(N)$ underlie linear codes of constant weight, and it specifies what the coordinate functionals need to be (up to an appropriate notion of equivalence).

The classification in this paper reproves the classical result about linear codes of constant Hamming weight over a finite field (see [3], for example). Let G be a $k \times (q^k - 1)/(q-1)$ matrix over $\mathbb{F}_q$ whose columns consist of one nonzero vector from each one-dimensional subspace of $\mathbb{F}_q^k$. Then G generates a linear code of constant Hamming weight, and every other k-dimensional constant Hamming weight code is a replication of this one, up to equivalence and zero columns.

The classification also reproves a recent theorem of Carlet [5] on linear codes of constant Lee weight over $\mathbb{Z}/(2^\beta)$. In fact, the desire to reprove Carlet's result using the techniques of [12] gave birth to this paper.

There are a few surprises. While constant Hamming weight codes exist in all dimensions over finite fields, they almost never exist over the $\mathbb{Z}/(N)$'s that are not fields. Constant Lee or Euclidean weight codes exist for any module over $\mathbb{Z}/(2^\beta)$, but are comparatively rare over the $\mathbb{Z}/(N)$'s that have odd prime factors in N.

The structure of the proof is simple. There is the question of existence (given a module M over $\mathbb{Z}/(N)$, does it underlie a linear code of constant weight?), and there is the question of uniqueness (in how many ways can this occur, up to equivalence?).

Received by the editors January 15, 2001.
2000 *Mathematics Subject Classification.* Primary 94B05.
Key words and phrases. Constant weight codes, Lee weight, Euclidean weight, extension theorem, orbital codes, virtual codes.
Partially supported by Purdue University Calumet Scholarly Research Awards. Some results were announced in [17] and [18]. Theorem 10.3 first appeared in [15].

We first prove a strong uniqueness theorem, Corollary 5.2, in the context of what we call virtual codes. Viewing linear codes from the linear functional viewpoint of [1], a linear code is a pair (M, η), where M is a module over R and $\eta : M^\sharp \to \mathbb{N}$ is a multiplicity function. Here, $M^\sharp = \mathrm{Hom}_R(M, R)$ is the linear dual of M, and η is keeping track of repeated columns in a generator matrix. Virtual codes, akin to virtual representations in representation theory, are pairs (M, η), where now $\eta : M^\sharp \to \mathbb{Q}$. The strong uniqueness theorem says that, for any M, there is a one-dimensional rational solution space of η's that correspond to constant weight codes. Only those η with values in $\mathbb{N}$ correspond to linear codes in the classical sense.

Armed with the uniqueness theorem, here is how the proof proceeds. Existence: guess what η should be and verify that it has constant weight. By the uniqueness theorem, η must be a basis for the solution space. If η has both positive and negative values, there is no classical solution. If η has all nonnegative values, clearing denominators leads to a classical solution η'.

Uniqueness: we are interested in the integral points of the one-dimensional rational solution space. The classical solution η' has nonnegative integral values. By dividing by the gcd of those values, we obtain a minimal integral solution η_0. Every other integral point in the solution space must be an integral multiple of η_0. Thus we see that constant weight codes, if they exist at all, must be replications of a minimal length model.

The proof of the uniqueness theorem depends on the extension theorem for weight preserving homomorphisms ([16], for example). Since the extension theorem is not known in general for all of the examples covered in this paper, many results include an extension property as part of their hypotheses. The existence results given do not depend on the extension theorem.

Here is a short guide to the contents of this paper. In Section 2 we discuss our ground rings R and modules over them. We also describe our (M, η) definition of linear codes. In Section 3 we introduce weight functions, the extension property, and viewing codes in terms of function spaces. Many examples are then introduced.

In Sections 4 and 5 we introduce virtual codes and prove the strong uniqueness theorem. Sections 6–10 are concerned with existence: the basic strategy, followed by detailed verifications for Hamming, Lee, and Euclidean weights. An appendix discusses orbital codes and another Euclidean weight that falls slightly outside the main thrust of the paper.

2. Linear Codes over Finite Rings

Notational Conventions. In this paper, any ring denoted by R will be assumed to be a finite commutative ring with 1. The ideal generated by $r \in R$ will be denoted by (r). Any R-module M will be assumed to be finitely generated and unital, i.e., $1 \in R$ acts as the identity. The linear dual of M is denoted $M^\sharp := \mathrm{Hom}_R(M, R)$. The elements of $M^\sharp$ are the *linear functionals* on M. Integer residue rings are denoted $\mathbb{Z}/(N) := \mathbb{Z}/N\mathbb{Z}$. The natural numbers $\mathbb{N}$ will contain 0. The number of elements in a finite set S is $|S|$.

We will study weight functions on two classes of rings R: the integer residue rings $\mathbb{Z}/(N)$ and (finite commutative) chain rings. Finite fields, $\mathbb{Z}/(p^l)$ for p prime, and Galois rings are all examples of chain rings. A *Galois ring* $R = GR(p^n, r)$ is a Galois extension of $\mathbb{Z}/(p^n)$ of degree r. By [10, Corollary 15.5], $GR(p^n, r) \cong$

$\mathbb{Z}/(p^n)[X]/(f)$, where f is a monic polynomial in $\mathbb{Z}/(p^n)[X]$ of degree r whose reduction in $\mathbb{Z}/(p)[X]$ is irreducible.

Chain rings are local rings R whose maximal ideal $\mathfrak{m}$ is principal, say $\mathfrak{m} = (m)$. It follows that every ideal in R is principal and of the form $\mathfrak{m}^j = (m^j)$, for some j. The ideals form a chain

$$R = (m^0) \supset (m) \supset (m^2) \supset \cdots \supset (m^{\beta-1}) \supset (m^\beta) = 0, \tag{2.1}$$

where $m^\beta = 0$, but $m^{\beta-1} \neq 0$.

Observe that $R/\mathfrak{m} \cong \mathbb{F}_q$, a finite field. The class of m^j is a basis of $(m^j)/(m^{j+1})$ as an $R/\mathfrak{m}$-vector space. It follows that

$$|(m^j)| = q|(m^{j+1})| = q^{\beta-j}. \tag{2.2}$$

For more details on chain rings, see [10, pp. 339ff] or [13, Lemma 13].

When R is a chain ring, as in (2.1), every module M over R admits a decreasing filtration

$$M \supset mM \supset m^2M \supset \cdots \supset m^{\gamma-1}M \supset m^\gamma M = 0, \tag{2.3}$$

for some $\gamma \leq \beta$, as well as a direct sum decomposition

$$M \cong \bigoplus_{j=1}^{\beta} \left(R/(m^j)\right)^{k_j}. \tag{2.4}$$

From (2.2), we see that

$$|M| = q^{\sum_{j=1}^{\beta} jk_j}. \tag{2.5}$$

If $k_\beta = 0$, then M is the pullback of a module defined over $R/(m^{\beta-1})$. To avoid this degeneracy, we will assume that $k_\beta \geq 1$. In that case, $\gamma = \beta$ in (2.3).

When $R = \mathbb{Z}/(N)$, with prime factorization

$$N = p_1^{\beta_1} \dots p_l^{\beta_l}, \tag{2.6}$$

every module M over R has a direct sum decomposition

$$M \cong \bigoplus_{i=1}^{l} \bigoplus_{j=1}^{\beta_i} \left(\mathbb{Z}/(p_i^j)\right)^{k_{i,j}}, \tag{2.7}$$

for appropriate non-negative integers $k_{i,j}$. Observe that

$$|M| = \prod_{i=1}^{l} p_i^{\sum_{j=1}^{\beta_i} jk_{i,j}}.$$

To avoid the situation where M is actually a pullback of a module defined over a quotient ring of R, we assume that, for all i,

$$k_{i,\beta_i} \geq 1. \tag{2.8}$$

There will be occasions where the prime number 2 will occur explicitly in (2.6). In that case $2 = p_0$ with exponent β_0 and integers $k_{0,j}$ in (2.7).

Linear codes will be described from the linear functional point of view of [1] (also see [11, §1]), although phrased in a slightly different way. A *linear code* C over R is a pair (M, η), where M is an R-module, the module *underlying* the code, and $\eta : M^\sharp \to \mathbb{N}$ is a *multiplicity function*. The *length* n of the linear code C is $n = \sum_{\lambda \in M^\sharp} \eta(\lambda)$. A linear code is *nondegenerate* if the multiplicity of the zero functional vanishes, i.e., if $\eta(0) = 0$.

A linear code (M,η) determines a linear homomorphism $\phi_\eta : M \to R^n$, $x \mapsto (\lambda(x))_{\lambda\in M^\sharp}$, where the entry $\lambda(x)$ appears $\eta(\lambda)$ times. The image of ϕ_η is a submodule of R^n, and this submodule is a linear code in the classical sense. Note that in defining ϕ_η one must choose an order in which to write down the terms $\lambda(x)$.

We shall usually assume that (M,η) satisfies the *coding axiom*, which states that ϕ_η is injective. By passing to a quotient, $M/\ker\phi_\eta$, the coding axiom holds automatically.

One way to view the definition above is to recall that a linear code is determined by its generator matrix G. The columns of G are given by linear functionals. Up to permutations of coordinate positions (the choice of order in writing down the terms in ϕ_η), the code is determined by the multiplicities of the various columns of G. It is exactly this information that is encoded by the multiplicity function η.

In an analogy with representation theory, we will have occasion to consider *virtual* linear codes. These are pairs (M,η), as above, where we allow η to have values in $\mathbb{Z}$ or $\mathbb{Q}$. That is, we allow linear functionals to occur with negative or rational multiplicities. More details will appear in Section 4.

3. Weight Functions and the Extension Property

In order to define the weight of codewords, we first define a *weight function* w on the ring R by assigning real number weights a_r to every $r \in R$. We assume that $a_0 = 0$ and that $a_r > 0$ for $r \neq 0$. This choice of weight function on R allows us to define a *weight function* $w_\eta : M \to \mathbb{R}$ on any linear code $C = (M,\eta)$:

$$w_\eta(x) = \sum_{\lambda\in M^\sharp} \eta(\lambda)\, a_{\lambda(x)}, \quad x \in M. \tag{3.1}$$

For example, Hamming weight uses $a_r = 1$, for all $r \neq 0$. We say that a linear code C has *constant weight* $L > 0$ if $w_\eta(x) = L$ for all nonzero $x \in M$. Since the zero element $0 \in M$ always has $w_\eta(0) = 0$, we hope the reader will tolerate this slightly misleading terminology.

To capture some of the symmetry of a weight function w, define the *symmetry group* of w to be

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

where $\mathcal{U}(R)$ is the group of units of R. The group $\mathrm{Sym}(w)$ acts on both M and $M^\sharp$ by scalar multiplication, thereby decomposing M and $M^\sharp$ into $\mathrm{Sym}(w)$-orbits. Denote the $\mathrm{Sym}(w)$-orbits of $x \in M$ and $\lambda \in M^\sharp$ by $\mathrm{orb}(x)$ and $\mathrm{orb}(\lambda)$, respectively.

If $f : M' \to M$ is an morphism of R-modules, then the equation $u(\lambda\circ f) = (u\lambda)\circ f$ shows that the induced morphism $f^\sharp : M^\sharp \to M'^\sharp$ takes $\mathrm{Sym}(w)$-orbits on $M^\sharp$ to $\mathrm{Sym}(w)$-orbits on $M'^\sharp$.

Lemma 3.1. *Suppose (M,η) is a linear code over R. If $x, y \in M$ satisfy $y \in \mathrm{orb}(x)$, then $w_\eta(y) = w_\eta(x)$.*

Proof. If $y = ux$ for some $u \in \mathrm{Sym}(w)$, then $a_{\lambda(y)} = a_{u\lambda(x)} = a_{\lambda(x)}$, by the definition of $\mathrm{Sym}(w)$. The result follows immediately. □

Consider a linear code (M,η) over R. For any $\lambda \in M^\sharp$, define

$$\eta_S(\lambda) := \sum_{\mu\in\mathrm{orb}(\lambda)} \eta(\mu). \tag{3.2}$$

Then $\eta_S(\lambda)$ is the total multiplicity of the linear functionals belonging to $\mathrm{orb}(\lambda)$. Clearly, $\eta_S(\lambda) = \eta_S(\mu)$ if $\mu \in \mathrm{orb}(\lambda)$. Note that (3.1) can be rewritten as

$$w_\eta(x) = \sum_{\lambda:\mathrm{rep}} \eta_S(\lambda)\, a_{\lambda(x)}, \quad x \in M, \tag{3.3}$$

where the summation is over one representative λ of each $\mathrm{Sym}(w)$-orbit. As we remarked above, the terms on the right side of (3.3) are independent of the choice of representatives for the $\mathrm{Sym}(w)$-orbits.

Two linear codes $C' = (M, \eta')$, $C = (M, \eta)$, are *scale equivalent* if $\eta'_S = \eta_S$. Let $\mathcal{O}$, $\mathcal{O}^\sharp$ denote the sets of nonzero $\mathrm{Sym}(w)$-orbits on M, $M^\sharp$, respectively. Denote the set of all functions $\mathcal{O}^\sharp \to \mathbb{N}$ by $\mathbb{N}[\mathcal{O}^\sharp]$.

Theorem 3.2. *Fix an R-module M. There is a bijection between the set of all nondegenerate linear codes (M, η), up to scale equivalence, and the function space $\mathbb{N}[\mathcal{O}^\sharp]$.*

Proof. To every code (M, η) we associate the function $\eta_S \in \mathbb{N}[\mathcal{O}^\sharp]$. Scale equivalent codes give rise to the same function η_S.

Conversely, given a function $g \in \mathbb{N}[\mathcal{O}^\sharp]$, we define a code as follows. For every $\mathrm{Sym}(w)$-orbit on $M^\sharp$, choose a representative. Then define $\eta : M^\sharp \to \mathbb{N}$ by

$$\eta(\lambda) = \begin{cases} g(\mathrm{orb}(\lambda)), & \text{if } \lambda \text{ is a chosen representative,} \\ 0, & \text{otherwise.} \end{cases}$$

Then (M, η) is a nondegenerate linear code with $\eta_S = g$. A different choice of representatives for the $\mathrm{Sym}(w)$-orbits results in a scale equivalent code. □

Two linear codes $C' = (M', \eta')$, $C = (M, \eta)$, are *equivalent* if there exists an isomorphism $f : M' \to M$ such that $(M, \eta' \circ f^\sharp)$ and (M, η) are scale equivalent. If C' and C are equivalent, a re-indexing argument shows that $w_{\eta'}(x) = w_\eta(f(x))$ for all $x \in M'$. That is, f induces a weight-preserving isomorphism between the codes. The converse of this statement is discussed next.

Definition EP. A weight function w over a ring R has the *extension property* (EP) if:

For any two linear codes $C' = (M', \eta')$, $C = (M, \eta)$ over R with an isomorphism $f : M' \to M$ satisfying $w_{\eta'}(x) = w_\eta(f(x))$ for all $x \in M'$, it follows that $(M, \eta' \circ f^\sharp)$ and (M, η) are scale equivalent. (Thus C' and C are equivalent via f.)

Remark 3.3. Classically, two linear codes in R^n are equivalent if there is a $\mathrm{Sym}(w)$-monomial transformation on R^n taking one code to the other. ($\mathrm{Sym}(w)$-monomial transformations are those whose units belong to $\mathrm{Sym}(w)$.) In the present definition, multiplication by units in $\mathrm{Sym}(w)$ is handled by scale equivalence. Permutations play a role only when one defines the map $\phi_\eta : M \to R^n$, because one must choose an order in which to write down the terms $\lambda(x)$. Classically, it is the image of ϕ_η that is the code, so that the particular parameterization is not relevant. The isomorphism f allows one to change parameterizations. This is analogous to changing basis within the code, as when one treats classical equivalence via generator matrices.

If EP is satisfied, it follows that every weight-preserving automorphism of R^n is a $\mathrm{Sym}(w)$-monomial transformation.

Theorem 3.4. *Suppose R, w satisfy EP and that M is a fixed R-module. Define a mapping $W : \mathbb{N}[\mathcal{O}^\sharp] \to \mathbb{R}[\mathcal{O}]$, $g \mapsto w_g$, where*

$$w_g(\mathrm{orb}(x)) = \sum_{\lambda:\mathrm{rep}} g(\mathrm{orb}(\lambda))\, a_{\lambda(x)},$$

and the summation is over one representative λ of each $\mathrm{Sym}(w)$-orbit. Then W is injective.

Proof. First observe that the terms on the right side of the expression for w_g do not depend on the choice of representatives for the $\mathrm{Sym}(w)$-orbits, nor does the right side depend upon the choice of representative for $\mathrm{orb}(x)$. Cf. (3.3) and Lemma 3.1.

Take any $g, h \in \mathbb{N}[\mathcal{O}^\sharp]$ with $W(g) = W(h)$. Let (M, η_g), (M, η_h) be linear codes corresponding to g, h as in Theorem 3.2. Then $W(g) = w_g$ is just the weight function of the code (M, η_g), as in (3.3). The equality $W(g) = W(h)$ means that $f = \mathrm{id}_M$ is a weight-preserving isomorphism from (M, η_g) to (M, η_h). By EP, these two codes are scale equivalent. But that implies $g = h$, as desired. □

We conclude this section with various examples of weight functions, their symmetry groups, and information about whether EP holds.

Example 3.5. Hamming weight. Over any ring R, set $a_r = 1$ for $r \neq 0$; $a_0 = 0$. The symmetry group $\mathrm{Sym}(w) = \mathcal{U}(R)$, the full group of units of R.

EP holds over finite fields ([2], [8], [9], [12]). EP holds over any finite Frobenius ring ([14, Theorem 6.3]). A *Frobenius ring* is a finite (not necessarily commutative) ring R such that $R/\mathrm{Rad}(R) \cong \mathrm{Socle}(R)$ as one-sided R-modules. Examples include finite fields, integer residue rings $\mathbb{Z}/(N)$, Galois rings, and chain rings [13, Lemma 13].

Example 3.6. Pre-homogeneous weights [6]. A weight function $w : R \to \mathbb{R}$ is *pre-homogeneous* if $a_0 = 0$ and there exists a constant $c > 0$ such that for $r \neq 0$,

$$\sum_{s \in (r)} a_s = c|(r)|.$$

Thus the average weight over principal ideals is the constant c.

For example, let R be a chain ring with $m^\beta = 0$, as in (2.1), and $R/(m) = \mathbb{F}_q$. Set

$$a_r = \begin{cases} q-1, & r \in R \setminus (m^{\beta-1}), \\ q, & r \in (m^{\beta-1}) \setminus (0), \\ 0, & r = 0. \end{cases}$$

The average weight on ideals is $c = q - 1$. Here, $\mathrm{Sym}(w) = \mathcal{U}(R)$.

Generally, if w is pre-homogeneous and $\mathrm{Sym}(w) = \mathcal{U}(R)$, i.e., if w is a *homogeneous* weight in the language of [6], then EP holds (over $\mathbb{Z}/(N)$, by [6]; for general chain rings by [16, Corollary 7.2]). If $\mathrm{Sym}(w) \neq \mathcal{U}(R)$, there is no information about EP.

Example 3.7. Lee weight on $R = \mathbb{Z}/(N)$. Choose representatives in the range $-N/2 < r \leq N/2$, and set $a_r = |r|$. It follows that $\mathrm{Sym}(w) = \{\pm 1\}$. When $N = 2^\beta$, Lee weight is pre-homogeneous with average weight $c = 2^{\beta-2}$.

EP has been numerically verified for $N \leq 256$ (MAPLE computations of the author which verify the sufficient condition of [16, Theorem 3.1]). EP holds for

rings of the form $\mathbb{Z}/(2^\beta)$, $\mathbb{Z}/(3^\beta)$, and for finite fields $\mathbb{F}_p$ with $p = 2q + 1$, q prime. (Work in preparation.) We conjecture that EP holds for all N.

Example 3.8. Euclidean PSK weight on $R = \mathbb{Z}/(N)$. Set

$$a_r = |\exp(2\pi ir/N) - 1|^2 = 2 - 2\cos(2\pi r/N).$$

Then $\mathrm{Sym}(w_{\mathrm{PSK}}) = \{\pm 1\}$. This Euclidean weight is pre-homogeneous with average weight $c = 2$.

EP has the same status and conjecture as for Lee weight, except it is unknown for general $\mathbb{Z}/(2^\beta)$.

Example 3.9. Euclidean AM weight on $R = \mathbb{Z}/(N)$. Set $a_r = |r|^2$, where representatives lie in the range $-N/2 < r \le N/2$. Same as for Lee weight, $\mathrm{Sym}(w_{\mathrm{AM}}) = \{\pm 1\}$.

Same status and conjecture for EP as for Lee weight.

Remark 3.10. The two previous examples reflect the fact that in the literature there are two different notions of Euclidean weight on the rings $\mathbb{Z}/(N)$. In the first notion, which arises in phase-shift key modulation, one embeds $\mathbb{Z}/(N)$ into $\mathbb{C}$ as the Nth roots of unity and measures distance using the squared Euclidean distance inherited from $\mathbb{C}$. When $N = 4$, w_{PSK} equals twice the Lee weight, [7, §IIC].

The second notion of Euclidean weight, which arises in amplitude modulation, is of interest because of the quotient map $\mathbb{Z} \to \mathbb{Z}/(N)$. Codes over $\mathbb{Z}/(N)$ pull back to lattices, and the minimum norm of vectors in the lattice is related to the minimum w_{AM}-weight of the code; see [4, §I].

4. Virtual Codes

We saw in Theorem 3.2 that linear codes, up to scale equivalence, are described by functions $\mathcal{O}^\sharp \to \mathbb{N}$. The function space $\mathbb{N}[\mathcal{O}^\sharp]$ is a semiring which we will embed into a ring, following similar ideas in representation theory, K-theory, Grothendieck groups, etc. We could use $\mathbb{Z}[\mathcal{O}^\sharp]$, but we find it more convenient to use $\mathbb{Q}[\mathcal{O}^\sharp]$, so as to utilize the power of linear algebra over a field. These considerations motivate the following definition.

A *virtual linear code* over a ring R is a pair (M, η), where M is an R-module and $\eta : M^\sharp \to \mathbb{Q}$ is a multiplicity function. Linear codes where η takes values in $\mathbb{N}$ will be called *classical* linear codes. The *weight* of an element $x \in M$ is defined exactly as before; see (3.1).

The definitions of nondegenerate, scale equivalence, and equivalence carry over verbatim from their classical counterparts. For reference, we state the virtual version of Theorem 3.2.

Theorem 4.1. *Suppose M is a fixed R-module. Then there is a bijection between the set of nondegenerate virtual linear codes (M, η), up to scale equivalence, and the function space $\mathbb{Q}[\mathcal{O}^\sharp]$.*

5. A Uniqueness Theorem

In this section we use Theorem 3.4 to prove an isomorphism theorem for virtual linear codes with rational weights. In turn, we obtain a uniqueness theorem for virtual linear codes of constant weight.

Theorem 5.1. *Assume R, w satisfy EP and that $a_r \in \mathbb{Q}$ in* (3.1)*. Fix an R-module M. Then the mapping*

$$W : \mathbb{Q}[\mathcal{O}^\sharp] \to \mathbb{Q}[\mathcal{O}],$$

defined as in Theorem 3.4*, is an isomorphism of $\mathbb{Q}$-vector spaces.*

Proof. The rationality of the a_r guarantees that $w_g \in \mathbb{Q}[\mathcal{O}] \subset \mathbb{R}[\mathcal{O}]$.

Since $\mathrm{Sym}(w)$ acts by scalar multiplication, the vector spaces $\mathbb{Q}[\mathcal{O}]$, $\mathbb{Q}[\mathcal{O}^\sharp]$ have the same finite dimension. Since W is linear, it suffices to show that W is injective.

Take any $g, h \in \mathbb{Q}[\mathcal{O}^\sharp]$ with $W(g) = W(h)$. By clearing denominators in all the values of g, h, we see that there is a positive integer B such that $Bg, Bh \in \mathbb{Z}[\mathcal{O}^\sharp]$. By adding a sufficiently large integer D to all the values of Bg, Bh, we obtain $Bg + D, Bh + D \in \mathbb{N}[\mathcal{O}^\sharp]$. Since $W(Bg + D) = W(Bh + D)$ follows from $W(g) = W(h)$, Theorem 3.4 implies that $Bg + D = Bh + D$. Thus $g = h$. □

Corollary 5.2. *Assume the conditions of Theorem* 5.1*, and fix an R-module M. Then the set of scale equivalence classes of nondegenerate virtual linear codes (M, η) of constant weight over R forms a one-dimensional subspace of $\mathbb{Q}[\mathcal{O}^\sharp]$.*

Proof. Nondegenerate constant weight codes correspond to the constant functions in $\mathbb{Q}[\mathcal{O}]$. □

Theorem 5.3. *Assume the conditions of Theorem* 5.1*. Suppose (M, η') and (M, η) both have constant weight and that they are equivalent via $f \in \mathrm{Aut}(M)$. Then they are scale equivalent. Thus, for linear codes of constant weight, scale equivalence classes are the same as equivalence classes.*

Proof. Observe that $w_{\eta' \circ f^\sharp}(x) = w_{\eta'}(f^{-1}(x)) = w_{\eta'}(x)$, since (M, η') has constant weight. By hypothesis, $(M, \eta' \circ f^\sharp)$ is scale equivalent to (M, η), so that $w_{\eta' \circ f^\sharp} = w_\eta$. Thus $w_{\eta'} = w_\eta$, and (M, η'), (M, η) are scale equivalent. □

We now interpret Corollary 5.2 in classical terms. Given a linear code $C = (M, \eta)$, the d-fold *replication* of C is the linear code $dC = (M, d\eta)$, i.e., every multiplicity $\eta(\lambda)$ is multiplied by a factor of d. In classical coding terminology, we repeat d times each column of a generator matrix for C.

Theorem 5.4. *Assume the conditions of Theorem* 5.1*. If M underlies a classical linear code of constant weight, then there is a nondegenerate classical linear code (M, η) of constant weight which has minimal length, and it is unique up to equivalence. Any other nondegenerate classical linear code (M, η') of constant weight is a d-fold replication of (M, η), up to equivalence.*

Moreover, if the multiplicity function η of a virtual linear code (M, η) of constant weight attains both positive and negative values, then there is no *classical linear code of constant weight with underlying module M.*

Proof. Let H be the one-dimensional subspace of $\mathbb{Q}[\mathcal{O}^\sharp]$ consisting of virtual linear codes of constant weight. By hypothesis, $H \cap \mathbb{N}[\mathcal{O}^\sharp]$ contains a nonzero element μ. Dividing μ by the gcd of its values yields a nonzero $\eta \in H \cap \mathbb{N}[\mathcal{O}^\sharp]$ of minimal length. Any other element of $H \cap \mathbb{N}[\mathcal{O}^\sharp]$ is an integral multiple of η.

If η attains both positive and negative values, then $H \cap \mathbb{N}[\mathcal{O}^\sharp]$ is zero. □

6. Existence: Basic Strategy

Because of the Corollary 5.2, questions of existence boil down to "guess and check": guess what the answer should be and then check that it is correct. All the guesses are based on extensive calculations—none of which appear in this paper. Instead, we just verify that the guesses are correct.

Underlying the verifications is a simple observation. Suppose $E \subset M^\sharp$ is a submodule of linear functionals and $x \in M$. Then $\check{x} : E \to R$, $\lambda \mapsto \lambda(x)$, is an R-linear homomorphism. Its image $\operatorname{im}\check{x} \subset R$ is an ideal, and every element of $\operatorname{im}\check{x}$ is hit $|\ker\check{x}|$ times. Thus,

$$\sum_{\lambda\in E} a_{\lambda(x)} = |\ker\check{x}| \sum_{r\in\operatorname{im}\check{x}} a_r = \frac{|E|}{|\operatorname{im}\check{x}|} \sum_{r\in\operatorname{im}\check{x}} a_r. \tag{6.1}$$

We then show that expressions built up from sums of this type are independent of the choice of nonzero x. The exact expressions for the sums $\sum_{r\in\operatorname{im}(\check{x})} a_r$ depend heavily upon the particular weight function used.

The existence proofs that follow do not depend on the Extension Property EP. Once questions of existence have been settled, Theorem 5.4 and its proof provide the classification of constant weight codes. Classification statements will not be repeated for every example.

We remind the reader that Theorem 5.4 assumes the validity of EP. Thus the classification of constant weight codes also depends upon EP. If EP is not known, then it must be assumed in order for the classification to be valid. The reader is directed to the examples of Section 3 for information about when EP is known.

7. Pre-homogeneous Weights

Let R be a chain ring equipped with a pre-homogeneous weight function w of average weight c (Example 3.6).

Theorem 7.1. *For any module M over R, set $\eta(\lambda) = 1$ for every nonzero $\lambda \in M^\sharp$. The resulting linear code is classical, with constant weight $c|M|$ and length $|M|-1$.*

Proof. Take any nonzero $x \in M$. Since $a_0 = 0$,

$$w_\eta(x) = \sum_{\lambda\in M^\sharp} a_{\lambda(x)} = \frac{|M^\sharp|}{|\operatorname{im}\check{x}|} \sum_{r\in\operatorname{im}\check{x}} a_r,$$

as in (6.1). But $\operatorname{im}\check{x}$ is a nonzero ideal in R, so that

$$\frac{1}{|\operatorname{im}\check{x}|} \sum_{r\in\operatorname{im}\check{x}} a_r = c$$

is independent of the choice of nonzero x, by the definition of pre-homogeneous weight. Thus the linear code $C = (M, \eta)$ has constant weight $c|M|$ and length $|M|-1$. □

Corollary 7.2. *Let $R = \mathbb{Z}/(N)$ be equipped with the Euclidean PSK weight (Example 3.8). For any module M over R, setting $\eta(\lambda) = 1$ for every nonzero $\lambda \in M^\sharp$ yields a classical linear code of constant weight $2|M|$ and length $|M|-1$.*

Proof. Euclidean PSK weight is pre-homogeneous with $c = 2$. □

The next corollary reproves a result of Carlet [5].

Corollary 7.3 ([5])**.** *Let $R = \mathbb{Z}/(2^\beta)$ be equipped with Lee weight (Example 3.7). For any module M over R, setting $\eta(\lambda) = 1$ for every nonzero $\lambda \in M^\sharp$ yields a classical linear code of constant weight $2^{\beta-2}|M|$ and length $|M| - 1$.*

Proof. On $\mathbb{Z}/(2^\beta)$, Lee weight is pre-homogeneous with $c = 2^{\beta-2}$. □

Corollary 7.4. *Let $R = \mathbb{F}_q$ be a finite field equipped with any weight function w. For any vector space M over $\mathbb{F}_q$, setting $\eta(\lambda) = 1$ for every nonzero $\lambda \in M^\sharp$ yields a classical linear code of constant weight.*

Proof. The weight function w is necessarily pre-homogeneous, since fields have only one nonzero ideal. □

Other weight functions over other rings are not so easy.

8. Hamming Weight

For the case of Hamming weight, we discuss both chain rings and $\mathbb{Z}/(N)$. This will be the first occasion where we use virtual codes.

Theorem 8.1. *Let R be a chain ring with maximal ideal $\mathfrak{m} = (m)$ and $R/\mathfrak{m} \cong \mathbb{F}_q$. Let M be any module over R, as in (2.4). For every nonzero $\lambda \in M^\sharp$, assign multiplicity*

$$\eta(\lambda) = \begin{cases} 1, & \lambda \in M^\sharp \setminus mM^\sharp, \\ 1 - q^{\sum_{j=1}^{\beta} k_j - 1}, & \lambda \in mM^\sharp. \end{cases}$$

Then the resulting virtual linear code has constant Hamming weight $|M|(1 - 1/q)$.

Proof. Consider any nonzero $x \in M$. Since $a_0 = 0$, there is no harm in including $\lambda = 0$ in any summation. Abbreviate $K := \sum_{j=1}^{\beta} k_j$.

$$\begin{aligned} w_\eta(x) &= \sum_{\lambda \in M^\sharp \setminus mM^\sharp} a_{\lambda(x)} + \left(1 - q^{K-1}\right) \sum_{\lambda \in mM^\sharp} a_{\lambda(x)} \\ &= \sum_{\lambda \in M^\sharp} a_{\lambda(x)} - q^{K-1} \sum_{\lambda \in mM^\sharp} a_{\lambda(x)}. \end{aligned}$$

The element x determines a linear map $\check{x} : M^\sharp \to R$ by $\lambda \mapsto \lambda(x)$. The image $\operatorname{im} \check{x}$ is a nonzero ideal in R, say $\operatorname{im} \check{x} = (m^i)$. It now follows that $\operatorname{im}(\check{x}|_{mM^\sharp}) = (m^{i+1})$.

It follows from (2.4) that $|M| = q^K |mM|$. Observe from (2.2) and (2.5) that $|\ker \check{x}| = |M^\sharp|/|\operatorname{im} \check{x}| = q^{\sum jk_j - \beta + i}$, while

$$|\ker(\check{x}|_{mM^\sharp})| = |mM^\sharp|/|(m^{i+1})| = q^{\sum jk_j - K - \beta + i + 1}.$$

Also, $\sum_{r \in (m^i)} a_r = |(m^i)| - 1$.

Then a simple computation shows that

$$\begin{aligned} w_\eta(x) &= |\ker \check{x}| \sum_{r \in (m^i)} a_r - q^{K-1} |\ker(\check{x}|_{mM^\sharp})| \sum_{r \in (m^{i+1})} a_r \\ &= |M|(1 - 1/q) \end{aligned}$$

is independent of x. □

Corollary 8.2. *Suppose R is a chain ring. The only circumstances where a classical linear code over R of constant Hamming weight exists are:*

- *R is a field, or*

- *M is a free module of rank* 1.

Proof. Since a chain ring is Frobenius, EP holds. The crux of the matter is that the multiplicity

$$\eta(\lambda) = 1 - q^{\sum k_j - 1}$$

is negative once $\sum k_j > 1$. As in (2.4), we work under the assumption that $k_\beta \geq 1$ already. So, there are only two ways for the code to be classical: $\sum k_j = 1$, in which case M is free of rank 1; or the situation where $\eta(\lambda) < 0$, i.e., $\lambda \in mM^\sharp$, never occurs for nonzero λ. That forces $mM^\sharp = 0$. Since $k_\beta \geq 1$, this happens only when R is a field. □

Remark 8.3. Let us examine carefully the case where R is the finite field $\mathbb{F}_q$. Suppose M is a k-dimensional vector space over $\mathbb{F}_q$. Since $\mathrm{Sym}(w) = \mathbb{F}_q^\times$, we see that every nonzero $\mathrm{Sym}(w)$-orbit has $q-1$ elements. Thus $\eta_S(\lambda) = q-1$ for all nonzero λ. The proof of Theorem 5.4 shows that the shortest length code of this dimension has $\eta_S(\lambda) = 1$.

In classical terms, the code has a generator matrix whose columns consist of one representative from each one-dimensional subspace of $\mathbb{F}_q^k$. This reproves a classical result (see [3] or [12, Theorem 4]).

Theorem 8.4. *Let $R = \mathbb{Z}/(N)$, and let M be any module over R. We assume the notation in* (2.6) *and* (2.7)*, in particular that $k_{i,\beta_i} \geq 1$. For every nonzero $\lambda \in M^\sharp$, assign the multiplicity*

$$\eta(\lambda) = \prod_{\substack{i: \\ \lambda \in p_i M^\sharp}} \left(1 - p_i^{\sum_{j=1}^{\beta_i} k_{i,j} - 1}\right).$$

The resulting virtual linear code has constant Hamming weight

$$|M| \prod_{i=1}^{l} (1 - 1/p_i).$$

Proof. By convention, the empty product equals 1. Abbreviate $K_i := \sum_{j=1}^{\beta_i} k_{i,j}$, so that $\eta(\lambda) = \prod (1 - p_i^{K_i - 1})$.

Fix an arbitrary nonzero $x \in M$. Since $a_0 = 0$, there is no harm in including $\lambda = 0$ in summations, so that

$$w_\eta(x) = \sum_{\lambda \in M^\sharp} \eta(\lambda) a_{\lambda(x)}.$$

By an inclusion/exclusion argument, this summation becomes

$$w_\eta(x) = \sum_{t=0}^{l} (-1)^t \sum_{1 \leq i_1 < \cdots < i_t \leq l} p_{i_1}^{K_{i_1} - 1} \cdots p_{i_t}^{K_{i_t} - 1} \sum_{\lambda \in p_{i_1} \cdots p_{i_t} M^\sharp} a_{\lambda(x)}. \tag{8.1}$$

The $t = 0$ term should be interpreted as simply $\sum_{\lambda \in M^\sharp} a_{\lambda(x)}$.

The nonzero element $x \in M$ defines a nonzero linear mapping $\check{x} : M^\sharp \to R$, $\lambda \mapsto \lambda(x)$. By restriction, there are also linear mappings

$$\check{x}_{i_1 \cdots i_t} := \check{x}|_{p_{i_1} \cdots p_{i_t} M^\sharp} : p_{i_1} \cdots p_{i_t} M^\sharp \to R,$$

some of which may be zero. The image $\mathrm{im}(\check{x})$ of $\check{x}$ is an ideal of R, say $\mathrm{im}(\check{x}) = (\nu)$, where $\nu | N$.

Eschewing exceptional cases, the basic argument proceeds as follows. As in (6.1), we consider sums of the form

$$\sum_{\lambda\in p_1\cdots p_t M^\sharp} a_{\lambda(x)} = |\ker(\check{x}_{1\cdots t})| \sum_{r\in \mathrm{im}(\check{x}_{1\cdots t})} a_r, \tag{8.2}$$

where $\mathrm{im}(\check{x}_{1\cdots t}) = (p_1\cdots p_t\nu)$. Now,

$$|\ker(\check{x}_{1\cdots t})| = \frac{|p_1\cdots p_t M^\sharp|}{|\mathrm{im}(\check{x}_{1\cdots t})|}, \qquad |p_1\cdots p_t M^\sharp| = \frac{|M|}{p_1^{K_1}\cdots p_t^{K_t}},$$
$$|\mathrm{im}(\check{x}_{1\cdots t})| = \frac{N}{p_1\cdots p_t\nu}, \qquad \sum_{r\in \mathrm{im}(\check{x}_{1\cdots t})} a_r = |\mathrm{im}(\check{x}_{1\cdots t})| - 1.$$

Simplifying, (8.2) becomes

$$\sum_{\lambda\in p_1\cdots p_t M^\sharp} a_{\lambda(x)} = \frac{|M|}{p_1^{K_1-1}\cdots p_t^{K_t-1}}\left(\frac{1}{p_1\cdots p_t} - \frac{\nu}{N}\right).$$

Remembering to symmetrize indices, we see that (8.1) becomes

$$\begin{aligned} w_\eta(x) &= \sum_{t=0}^{l}(-1)^t \sum_{1\le i_1<\cdots<i_t\le l} |M|\left(\frac{1}{p_{i_1}\cdots p_{i_t}} - \frac{\nu}{N}\right) \\ &= |M|\sum_{t=0}^{l}(-1)^t \sum_{1\le i_1<\cdots<i_t\le l} \frac{1}{p_{i_1}\cdots p_{i_t}} - |M|\frac{\nu}{N}\sum_{t=0}^{l}(-1)^t\binom{l}{t} \\ &= |M|\prod_{i=1}^{l}(1-1/p_i), \end{aligned}$$

which is independent of x. □

Corollary 8.5. *Over $R = \mathbb{Z}/(N)$, an R-module M as in* (2.7) *underlies a classical linear code of constant Hamming weight only in the following circumstances:*

- *$N = p$, a prime, in which case $\eta(\lambda) = 1$ for all nonzero $\lambda \in M^\sharp$, see Remark* 8.3*, or*
- *M is free of rank* 1.

Proof. Since $\mathbb{Z}/(N)$ is Frobenius, EP holds. As usual, we assume that $k_{i,\beta_i} \ge 1$. Thus $\sum_{j=1}^{\beta_i} k_{i,j} - 1 \ge 0$, with equality if and only if $k_{i,\beta_i} = 1$, and $k_{i,j} = 0$ for all $j = 1, 2, \ldots, \beta_i - 1$. Thus, equality holds for all i precisely when M is free of rank 1. In that case,

$$\eta(\lambda) = \begin{cases} 1, & \lambda \notin \bigcup p_i M^\sharp, \\ 0, & \lambda \in \bigcup p_i M^\sharp, \end{cases}$$

which is a classical code.

If M is not free of rank 1, there is some i with $\sum_{j=1}^{\beta_i} k_{i,j} - 1 > 0$. This will provide a negative factor in $\eta(\lambda)$ for any nonzero $\lambda \in p_i M^\sharp$. The only way to avoid this difficulty is for $p_i M^\sharp = 0$ for all i, which occurs only for $N = p$, prime. □

9. Lee Weight

We continue with some of the notation used in Section 8. We work over $R = \mathbb{Z}/(N)$, with prime factorization (2.6). Let M be any module over R, so that (2.7) and (2.8) apply. As in the proof of Theorem 8.4, set $K_i := \sum_{j=1}^{\beta_i} k_{i,j}$; then $K_i \geq 1$.

Theorem 9.1. *Let $R = \mathbb{Z}/(N)$ and M be as above. To every nonzero $\lambda \in M^\sharp$, assign the multiplicity*

$$\eta(\lambda) = \prod_{\substack{p_i \text{ odd:} \\ \lambda \in p_i M^\sharp}} \left(1 - p_i^{K_i - 2}\right).$$

The resulting virtual linear code has constant Lee weight

$$(N/4)|M| \prod_{i=1}^{l} (1 - 1/p_i^2).$$

Proof. By convention, the empty product equals 1.

We first discuss the case where N is odd. Fix an arbitrary nonzero $x \in M$. We will follow the proof of Theorem 8.4 in the Hamming case. In the Lee case, if $\nu | N$, then a computation (or Lemma 10.1) yields

$$\sum_{r \in (\nu)} a_r = (N^2 - \nu^2)/(4\nu).$$

With this modification, (8.2) simplifies to

$$\begin{aligned} \sum_{\lambda \in p_1 \cdots p_t M^\sharp} a_{\lambda(x)} &= \frac{|M|}{p_1^{K_1} \cdots p_t^{K_t}} \, \frac{p_1 \cdots p_t \nu}{N} \, \frac{N^2 - (p_1 \cdots p_t \nu)^2}{4(p_1 \cdots p_t \nu)} \\ &= \frac{|M|}{4N p_1^{K_1 - 2} \cdots p_t^{K_t - 2}} \left(\frac{N^2}{p_1^2 \cdots p_t^2} - \nu^2 \right). \end{aligned}$$

In this Lee context, the counterpart to (8.1) is then

$$\begin{aligned} w_\eta(x) &= \sum_{t=0}^{l} (-1)^t \sum_{1 \leq i_1 < \cdots < i_t \leq l} p_{i_1}^{K_{i_1} - 2} \cdots p_{i_t}^{K_{i_t} - 2} \sum_{\lambda \in p_{i_1} \cdots p_{i_t} M^\sharp} a_{\lambda(x)} \\ &= \frac{|M|}{4N} \sum_{t=0}^{l} (-1)^t \sum_{1 \leq i_1 < \cdots < i_t \leq l} \left(\frac{N^2}{p_{i_1}^2 \cdots p_{i_t}^2} - \nu^2 \right) \qquad (9.1) \\ &= (N/4)|M| \prod_{i=1}^{l} (1 - 1/p_i^2), \end{aligned}$$

which is independent of x.

In the case where N is even, the only difference is the formula for $\sum_{r \in (\nu)} a_r$, where $\nu | N$. Write $N = 2^{\beta_0} p_1^{\beta_1} \cdots p_l^{\beta_l}$, where $\beta_0 > 0$ and $p_1, \ldots, p_l$ are odd primes. Then a computation yields

$$\sum_{r \in (\nu)} a_r = \begin{cases} (N^2 - \nu^2)/(4\nu), & 2^{\beta_0} | \nu, \\ N^2/(4\nu), & 2^{\beta_0} \not| \nu. \end{cases} \qquad (9.2)$$

In the counterpart to (8.2), one needs to sum over $r \in \mathrm{im}(\check{x}_{1 \cdots t}) = (p_1 \cdots p_t \nu)$. Since the p_i are odd primes, their presence does not affect divisibility by 2^{β_0}. Thus

the expressions that appear in the counterpart to (9.1) are consistently of one of the types in (9.2), and the expression simplifies exactly as in (9.1). □

Corollary 9.2. *Over $R = \mathbb{Z}/(N)$, assuming EP, an R-module M underlies a classical linear code of constant Lee weight only in the following circumstances:*

- *$N = p$, a prime, M arbitrary, in which case $\eta(\lambda) = 1$ for all nonzero $\lambda \in M^\sharp$.*
- *$N = 2^{\beta_0}$, M arbitrary, $\eta(\lambda) = 1$: Carlet, [5].*
- *N arbitrary, but M restricted by $K_i \leq 2$, for all $i = 1, 2, \ldots, l$.*

10. Euclidean Weight

In discussing Euclidean weights, remember that the Euclidean PSK weight is pre-homogeneous. The existence of its constant weight codes is covered by Corollary 7.2. Beware that Theorem 5.1 does not apply to Euclidean PSK weight because the weight does not have rational values. Appendix A provides an alternative approach to uniqueness.

In the remainder of this section, we discuss Euclidean AM weight, and we will refer to it simply as Euclidean weight.

We continue to work over $R = \mathbb{Z}/(N)$, with prime factorization $N = 2^{\beta_0} p_1^{\beta_1} \cdots p_l^{\beta_l}$ (the p_i being odd primes). A module M over R has the usual form (2.7), with (2.8). As above, set $K_i := \sum_{j=1}^{\beta_i} k_{i,j}$; $K_i \geq 1$.

For ease of exposition, we will consider several cases, starting with the case where N is odd (i.e., $\beta_0 = 0$).

Lemma 10.1. *Suppose N is odd. When summing over ideals of R, Euclidean weight is proportional to Lee weight.*

Proof. Let $r|N$, with $ur = N$. We calculate $\sum_{s \in (r)} a_s$, for both Lee and Euclidean weights. Exploiting $\pm$-symmetry, we find that

$$\begin{aligned}\sum_{s\in(r)} a_s &= 2 \sum_{t=1}^{(u-1)/2} a_{tr} \\ &= \begin{cases} 2(r + 2r + \cdots + r(u-1)/2) & \text{Lee} \\ 2(r^2 + (2r)^2 + \cdots + (r(u-1)/2)^2) & \text{Euclidean} \end{cases} \\ &= \begin{cases} r(u^2-1)/4 & \text{Lee} \\ (N/3) \cdot r(u^2-1)/4 & \text{Euclidean.} \end{cases} \quad \square \end{aligned}$$

Theorem 10.2. *A virtual linear code over $\mathbb{Z}/(N)$, N odd, has constant Euclidean weight if and only if it has constant Lee weight. For N odd, assuming EP, constant Euclidean weight codes are given by Theorem 9.1 and Corollary 9.2. The weights are multiplied by a factor of $N/3$.*

Proof. The counterpart of (8.2) for Euclidean weight is proportional to that for Lee weight, with a factor of $N/3$. □

We now turn to the cases where N is even ($\beta_0 > 0$). The answers depend on whether N is a power of 2 or not. In either case, we need to filter the module $M^\sharp$ as in (2.3):

$$M^\sharp \supset 2M^\sharp \supset \cdots \supset 2^{\beta_0 - 1} M^\sharp \supset 2^{\beta_0} M^\sharp. \tag{10.1}$$

For nonzero $\lambda \in M^\sharp$, define $\nu(\lambda)$ to be the largest integer $\leq \beta_0$ such that $\lambda \in 2^{\nu(\lambda)}M^\sharp$.

We define some new quantities in terms of the numbers $k_{0,j}$ of (2.8). Set $e_0 = 1$ and

$$e_i = k_{0,1} + 2k_{0,2} + \cdots + (i-1)k_{0,i-1} + i(k_{0,i} + \cdots + k_{0,\beta_0}) - i, \tag{10.2}$$

for $1 \leq i \leq \beta_0$.

Let us now turn to the case where $N = 2^{\beta_0}$ is a power of 2. In this situation, $2^{\beta_0}M^\sharp = 0$ in (10.1), so that $\nu(\lambda) \leq \beta_0 - 1$, for all nonzero $\lambda \in M^\sharp$.

Theorem 10.3 ([15])**.** *Let $R = \mathbb{Z}/(N)$, $N = 2^{\beta_0}$; let M be a module over R, as above. For every nonzero $\lambda \in M^\sharp$, assign the multiplicity*

$$\eta(\lambda) = \sum_{i=0}^{\nu(\lambda)} 2^{e_i}.$$

The resulting linear code is classical and has constant Euclidean weight $2^{2\beta_0-2}|M| = (N^2/4)|M|$ and length

$$n = \frac{|M|}{2^{\beta_0-1}}\left(3 \cdot 2^{\beta_0-1} - 1\right) - \sum_{i=0}^{\beta_0-1} 2^{e_i}.$$

Proof. First note that since we assume $k_{0,\beta_0} \geq 1$, 2^{β_0} divides $|M|$, and n is an integer; see (2.5).

Take any nonzero $x \in M$. Using the definition of $\eta(\lambda)$ and the filtration (10.1),

$$w_\eta(x) = \sum_{\lambda \in M^\sharp} \eta(\lambda) a_{\lambda(x)} = \sum_{j=0}^{\beta_0-1} 2^{e_j} \sum_{\lambda \in 2^j M^\sharp} a_{\lambda(x)}. \tag{10.3}$$

Now consider the linear functional $\check{x} : 2^jM^\sharp \to R$, $\lambda \mapsto \lambda(x)$. Suppose x has order 2^i. If $i \leq j$, the functional $\check{x}$ is zero. When $i > j$, the image $\mathrm{im}(\check{x}) = \check{x}(2^jM^\sharp) = (2^{\beta_0-i+j})$, with $|\mathrm{im}(\check{x})| = 2^{i-j}$. In this case, every $r \in \mathrm{im}(\check{x})$ is hit equally often by $\check{x}$, namely

$$|\ker(\check{x})| = \frac{|2^jM^\sharp|}{|\mathrm{im}(\check{x})|} = 2^{-i+j+\sum_{s=1}^{\beta_0-j} sk_{0,j+s}}$$

times. It is straightforward to show that, for Euclidean weight,

$$3\sum_{r \in (2^c)} a_r = 2^{\beta_0+c-1}\left(2^{2\beta_0-2c-1} + 1\right). \tag{10.4}$$

Remembering that x has order 2^i and using $c = \beta_0 - i + j$ in (10.4), we conclude that

$$3\sum_{\lambda \in 2^j M^\sharp} a_{\lambda(x)} = \begin{cases} 0, & i \leq j, \\ 2^{\sum_{s=1}^{\beta_0-j} sk_{0,j+s}}\left(1 + 2^{-2i+2j+1}\right)2^{2\beta_0-2}, & i > j. \end{cases}$$

This last expression allows us to rewrite (10.3) as

$$3w_\eta(x) = \sum_{j=0}^{i-1} 2^{e_j+\sum_{s=1}^{\beta_0-j} sk_{0,j+s}}\left(1 + 2^{-2i+2j+1}\right)2^{2\beta_0-2}. \tag{10.5}$$

Observe that the complicated exponent in (10.5) simplifies to

$$e_j + \sum_{s=1}^{\beta_0 - j} s k_{0,j+s} = \begin{cases} 1 + \sum_{t=1}^{\beta_0} t k_{0,t}, & j = 0, \\ -j + \sum_{t=1}^{\beta_0} t k_{0,t}, & j > 0. \end{cases}$$

Since $\log_2 |M| = \sum_{t=1}^{\beta_0} t k_{0,t}$ from (2.5), (10.5) simplifies to

$$3w_\eta(x) = 2|M| \left(1 + 2^{-2i+1}\right) 2^{2\beta_0 - 2} + \sum_{j=1}^{i-1} |M| \, 2^{-j} \left(1 + 2^{-2i+2j+1}\right) 2^{2\beta_0 - 2}.$$

By summing the geometric series and simplifying, we obtain the constant weight

$$w_\eta(x) = 2^{2\beta_0 - 2} |M| = (N^2/4)|M|.$$

The value of the length n can be verified by the reader. □

Finally, we consider the general even case where $N = 2^{\beta_0} p_1^{\beta_1} \cdots p_l^{\beta_l}$, $\beta_0 > 0$, $l \geq 1$. Using (10.2), define

$$e'_0 = e_0, \ldots, e'_{\beta_0 - 1} = e_{\beta_0 - 1}, e'_{\beta_0} = e_{\beta_0} + 1.$$

As above, set $K_i = \sum_{j=1}^{\beta_i} k_{i,j}$.

Their proofs being similar to those above, the following results are included without proof.

Theorem 10.4. *Suppose $R = \mathbb{Z}/(N)$, $N = 2^{\beta_0} p_1^{\beta_1} \cdots p_l^{\beta_l}$, $\beta_0 > 0$, $l \geq 1$, M as above. For every nonzero $\lambda \in M^\sharp$, assign the multiplicity*

$$\eta(\lambda) = \left(\sum_{i=0}^{\nu(\lambda)} 2^{e'_i} \right) \prod_{\substack{p_i \text{ odd:} \\ \lambda \in p_i M^\sharp}} \left(1 - p_i^{K_i - 2}\right).$$

The resulting virtual linear code has constant Euclidean weight

$$(N^2/4)|M| \prod_{i=1}^{l} (1 - 1/p_i^2).$$

Corollary 10.5. *Over $R = \mathbb{Z}/(N)$, assuming EP, an R-module M underlies a classical linear code of constant Euclidean weight only in the following circumstances:*

- *$N = p$, a prime, M arbitrary, in which case $\eta(\lambda) = 1$ for all nonzero $\lambda \in M^\sharp$.*
- *$N = 2^{\beta_0}$, M arbitrary: Theorem 10.3.*
- *N arbitrary, but M restricted by $K_i \leq 2$, for all $i = 1, 2, \ldots, l$.*

Appendix A. Orbital Codes

In this appendix, we define orbital codes, both classical and virtual, and show how they give rise to a uniqueness theorem that applies to Euclidean PSK weight. Most proofs are the same as for linear codes, and hence are omitted.

Assume R is a ring equipped with a weight function w that satisfies the Extension Property EP. Let M be a fixed R-module.

Recall from Theorem 3.2 that there is a bijection between the set of nondegenerate linear codes (M, η), up to scale equivalence, and the function space $\mathbb{N}[\mathcal{O}^\sharp]$. The automorphism group $\mathrm{Aut}(M)$ acts on M and on $M^\sharp$, mapping $\mathrm{Sym}(w)$-orbits to $\mathrm{Sym}(w)$-orbits. The next theorem is then evident.

Theorem A.1. *For a fixed R-module M, there is a bijection between the set of nondegenerate linear codes (M,η), up to equivalence, and the space $\mathbb{N}[\mathcal{O}^\sharp]/\operatorname{Aut}(M)$ of $\operatorname{Aut}(M)$-orbits on $\mathbb{N}[\mathcal{O}^\sharp]$.*

A linear code (M,η) is an *orbital code* if $\eta_S(\lambda) = \eta_S(\lambda')$, for all $\lambda, \lambda' \in M^\sharp$ which lie in the same $\operatorname{Aut}(M)$-orbit. (For η_S, see (3.2).) In terms of Theorem A.1, orbital codes correspond to functions in $\mathbb{N}[\mathcal{O}^\sharp]$ that are invariant under the $\operatorname{Aut}(M)$-action. In classical terminology, if λ appears as a column of a generator matrix for an orbital code, then so does every other μ in the $\operatorname{Aut}(M)$-orbit of λ, and with equal multiplicities (columns that are $\operatorname{Sym}(w)$-multiples of each other being counted together).

If we denote by $\mathcal{O}_A$, $\mathcal{O}_A^\sharp$ the sets of nonzero $\operatorname{Aut}(M)$-orbits on M, $M^\sharp$, respectively, we see that the set of $\operatorname{Aut}(M)$-invariant functions in $\mathbb{N}[\mathcal{O}^\sharp]$ is the same as $\mathbb{N}[\mathcal{O}_A^\sharp]$. This proves the next theorem.

Theorem A.2. *For a fixed R-module M, there is a bijection between the set of nondegenerate orbital codes (M,η), up to equivalence, and the function space $\mathbb{N}[\mathcal{O}_A^\sharp]$.*

The relevance of orbital codes in the study of linear codes of constant weight is provided in the next theorem. This result was motivated by Ward's proof of [12, Theorem 4].

Theorem A.3. *Suppose R, w satisfy EP. Let $C = (M,\eta)$ be a nondegenerate linear code of constant weight. Then C is an orbital code.*

Proof. Let $f \in \operatorname{Aut}(M)$ be any automorphism of M. For any nonzero $x \in M$, $f(x) \neq 0$, and so $w_\eta(x) = w_\eta(f(x))$, because C has constant weight. Thus f is a weight-preserving automorphism of (M,η). By EP, $(M, \eta \circ f^\sharp)$ and (M,η) are scale equivalent.

To verify that C is an orbital code, we take any two nonzero $\lambda, \lambda' \in M^\sharp$ and assume that λ' is in the $\operatorname{Aut}(M)$-orbit of λ. Then there exists $f \in \operatorname{Aut}(M)$ with $\lambda' = \lambda \circ f$. Applying the result in the previous paragraph, we have that $(M, \eta \circ f^\sharp)$ and (M,η) are scale equivalent. That is, $\eta_S = \eta_S \circ f^\sharp$. But then $\eta_S(\lambda) = \eta_S(\lambda \circ f) = \eta_S(\lambda')$, as desired. □

Lemma A.4. *Suppose (M,η) is an orbital code. Then w_η is constant on $\operatorname{Aut}(M)$-orbits of M.*

Proof. This is a re-indexing argument. If $y = f(x)$ for some $f \in \operatorname{Aut}(M)$, then, using (3.3),

$$\begin{aligned} w_\eta(y) &= \sum_{\lambda:\mathrm{rep}} \eta_S(\lambda)\, a_{\lambda(y)} = \sum_{\lambda:\mathrm{rep}} \eta_S(\lambda)\, a_{\lambda(f(x))} \\ &= \sum_{\lambda:\mathrm{rep}} \eta_S(\lambda \circ f)\, a_{(\lambda\circ f)(x)} = \sum_{\mu=\lambda\circ f:\mathrm{rep}} \eta_S(\mu)\, a_{\mu(x)} = w_\eta(x), \end{aligned}$$

where we used the definition of orbital code and the fact that, as λ runs over representatives of $\operatorname{Sym}(w)$-orbits, so does $\mu = \lambda \circ f$. □

Given an orbital code (M,η), that is, a function $\eta_S : \mathcal{O}_A^\sharp \to \mathbb{N}$, Lemma A.4 shows that η_S induces a well-defined function $w_\eta : \mathcal{O}_A \to \mathbb{R}$. Denote by $\mathbb{R}[\mathcal{O}_A]$, $\mathbb{N}[\mathcal{O}_A^\sharp]$, the spaces of all functions $\mathcal{O}_A \to \mathbb{R}$, $\mathcal{O}_A^\sharp \to \mathbb{N}$, respectively. We now have the orbital code version of Theorem 3.4.

Theorem A.5. *Given a module M, the mapping $W : \mathbb{N}[\mathcal{O}_A^\sharp] \to \mathbb{R}[\mathcal{O}_A]$, $\eta_S \mapsto w_\eta$, is injective.*

Just as in Section 4, one can speak of virtual orbital codes: η is allowed to take values in $\mathbb{Q}$. Theorems 4.1 and 5.1 generalize as follows.

Theorem A.6. *For a fixed R-module M, there is a bijection between the set of nondegenerate virtual orbital codes (M, η), up to equivalence, and the function space $\mathbb{Q}[\mathcal{O}_A^\sharp]$.*

Theorem A.7. *Assume that R, w satisfy EP and that M is a fixed R-module. Also assume that w has the property that $w_\eta(x) \in \mathbb{Q}$ for every $x \in M$ and every orbital code (M, η). Then the mapping*

$$W : \mathbb{Q}[\mathcal{O}_A^\sharp] \to \mathbb{Q}[\mathcal{O}_A], \quad \eta_S \mapsto w_\eta,$$

is an isomorphism of $\mathbb{Q}$-vector spaces.

The orbital analog of Corollary 5.2 is next.

Corollary A.8. *Assume the conditions of Theorem* A.7. *Then the set of equivalence classes of nondegenerate virtual orbital codes (M, η) of constant weight over R forms a one-dimensional subspace of $\mathbb{Q}[\mathcal{O}_A^\sharp]$.*

The classical interpretation of this corollary is clear.

Remark A.9. Let us compare Corollaries 5.2 and A.8. By Theorem A.3, every linear code of constant weight is orbital. By Theorem 5.3, scale equivalence classes of constant weight codes are the same as equivalence classes. Thus the one-dimensional solution spaces of Corollaries 5.2 and A.8 are exactly the same.

Finally, we show that orbital codes for Euclidean PSK weight satisfy the rationality condition of Theorem A.7.

Lemma A.10. *Equip $R = \mathbb{Z}/(N)$ with Euclidean PSK weight, and let (M, η) be a virtual orbital code over R. Then $w_\eta(x) \in \mathbb{Q}$ for all $x \in M$.*

Proof. Because automorphisms of M are linear, $\mathrm{Sym}(w)$-orbits lie entirely within $\mathrm{Aut}(M)$-orbits. For each $\mathrm{Aut}(M)$-orbit, choose a representative λ, and for each $\mathrm{Sym}(w)$-orbit within the $\mathrm{Aut}(M)$-orbit of λ, choose a representative μ_λ. Then from (3.3), we have

$$\begin{aligned} w_\eta(x) &= \sum_{\lambda:\mathrm{rep}} \sum_{\mu_\lambda:\mathrm{rep}} \eta_S(\mu_\lambda)\, a_{\mu_\lambda(x)} \\ &= \sum_{\lambda:\mathrm{rep}} \eta_S(\lambda) \sum_{\mu_\lambda:\mathrm{rep}} a_{\mu_\lambda(x)}. \end{aligned}$$

The summations are over the appropriate representatives only, and we used the definition of orbital code to pull out the factor of $\eta_S(\lambda)$. To prove the lemma, it suffices to show that

$$\sum_{\mu_\lambda:\mathrm{rep}} a_{\mu_\lambda(x)} \in \mathbb{Q},$$

for every $x \in M$ and $\lambda \in M^\sharp$.

Let us be a little more careful in how we pick the μ_λ. Call Λ the $\mathrm{Aut}(M)$-orbit of λ. First pick $\mu_1 \in \Lambda$. For $u \in \mathcal{U} = \mathcal{U}(R)$, the group of units of R, $u\mu_1$ is also in Λ but

is generally in a different $\mathrm{Sym}(w)$-orbit. Use these $u\mu_1$ as representatives of their $\mathrm{Sym}(w)$-orbits. Now pick $\mu_2 \in \Lambda$ outside the $\mathrm{Sym}(w)$-orbits already represented, and repeat the process. It suffices to show for each j that

$$\sum_u a_{u\mu_j(x)} \in \mathbb{Q}. \tag{A.1}$$

Write $\omega = \exp(2\pi i \mu_j(x)/N)$; ω is a primitive nth root of unity in $\mathbb{C}$ for some $n|N$. For $u \in \mathcal{U}$, ω^u is another primitive nth root of unity. Thus $\sum_u \omega^u \in \mathbb{Q}$, since the primitive nth roots of unity are precisely the roots of the nth cyclotomic polynomial. By taking real parts and remembering that $a_r = 2 - 2\cos(2\pi r/N)$, (A.1) now follows. Any duplication in counting can be divided out, and the resulting quantities are still in $\mathbb{Q}$. □

Acknowledgments

The author thanks Purdue University Calumet, the University of Notre Dame, and Western Michigan University for sabbatical support. I thank J. Wolfmann, Ph. Langevin, and the research group GRIM at Université Toulon-Var for their hospitality during the spring of 2000. I also thank H. N. Ward for some key ideas, especially Theorem A.3, G. McNinch for pointing out (2.2), the referee for helping improve the clarity of the paper, and E. S. Moore for many things.

References

[1] E. F. Assmus, Jr. and H. F. Mattson, *Error-correcting codes: An axiomatic approach*, Inform. and Control **6** (1963), 315–330. MR **31:**3251

[2] K. Bogart, D. Goldberg, and J. Gordon, *An elementary proof of the MacWilliams theorem on equivalence of codes*, Inform. and Control **37** (1978), 19–22. MR **57:**19067

[3] A. Bonisoli, *Every equidistant linear code is a sequence of dual Hamming codes*, Ars Combin. **18** (1984), 181–186. MR **87b:**94044

[4] A. Bonnecaze, P. Solé, and A. R. Calderbank, *Quaternary quadratic residue codes and unimodular lattices*, IEEE Trans. Inform. Theory **41** (1995), 366–377. MR **96b:**94027

[5] C. Carlet, *One-weight $\mathbb{Z}_4$-linear codes*, Coding Theory, Cryptography and Related Areas (J. Buchmann, T. Høholdt, H. Stichtenoth, and H. Tapia-Recillas, eds.), Springer, Berlin, 2000, pp. 57–72. MR **2000m:**94034

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

[7] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), 301–319. MR **95k:**94030

[8] F. J. MacWilliams, *Error-correcting codes for multiple-level transmission*, Bell System Tech. J. **40** (1961), 281–308. MR **25:**4945

[9] ———, *Combinatorial properties of elementary abelian groups*, Ph.D. thesis, Radcliffe College, Cambridge, Mass., 1962.

[10] B. R. McDonald, *Finite rings with identity*, Pure and Applied Mathematics, vol. 28, Marcel Dekker, Inc., New York, 1974. MR **50:**7245

[11] H. N. Ward, *An introduction to divisible codes*, Des. Codes Cryptogr. **17** (1999), 73–79. MR **2000j:**94039

[12] H. N. Ward and J. A. Wood, *Characters and the equivalence of codes*, J. Combin. Theory Ser. A **73** (1996), 348–352. MR **96i:**94028

[13] J. A. Wood, *Extension theorems for linear codes over finite rings*, Applied Algebra, Algorithms and Error-Correcting Codes (T. Mora and H. Mattson, eds.), Lecture Notes in Comput. Sci., vol. 1255, Springer-Verlag, Berlin, 1997, pp. 329–340. MR **99h:**94062

[14] ———, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math. **121** (1999), 555–575. MR **2001d:**94033

[15] ———, *Linear codes over $\mathbb{Z}/(2^k)$ of constant Euclidean weight*, Proceedings of the Thirty-Seventh Annual Allerton Conference on Communication, Control, and Computing, University of Illinois, 1999, pp. 895–896.

[16] ———, *Weight functions and the extension theorem for linear codes over finite rings*, Finite fields: Theory, Applications and Algorithms (R. C. Mullin and G. L. Mullen, eds.), Contemp. Math., vol. 225, Amer. Math. Soc., Providence, 1999, pp. 231–243. MR **2000b:**94024

[17] ———, *Understanding linear codes of constant weight using virtual linear codes*, Proceedings of the Thirty-Eighth Annual Allerton Conference on Communication, Control, and Computing, University of Illinois, 2000, pp. 1038–1046.

[18] ———, *The structure of linear codes of constant weight*, Proceedings of the International Workshop on Coding and Cryptography, Paris, INRIA, 2001, pp. 547–556.

Department of Mathematics, Computer Science & Statistics, Purdue University Calumet, Hammond, Indiana 46323, Department of Mathematics, University of Notre Dame, Notre Dame, Indiana 46556, and GRIM, Université Toulon-Var, 83957 La Garde Cedex, France

Current address: Department of Mathematics, Western Michigan University, 1903 W. Michigan Ave., Kalamazoo, Michigan 49008–5248

E-mail address: jay.wood@wmich.edu

URL: http://unix.cc.wmich.edu/jwood