# FOUNDATIONS OF LINEAR CODES DEFINED OVER FINITE MODULES: THE EXTENSION THEOREM AND THE MACWILLIAMS IDENTITIES*

—

## BASED ON LECTURES FOR THE CIMPA-UNESCO-TÜBİTAK SUMMER SCHOOL

Jay A. Wood

*Department of Mathematics*
*Western Michigan University*
*1903 W. Michigan Ave.*
*Kalamazoo, MI 49008–5248, USA*
*E-mail: jay.wood@wmich.edu*
*http://homepages.wmich.edu/∼jwood*

This paper discusses the foundations of the theory of linear codes defined over finite modules. Two topics are examined in depth: the extension theorem and the MacWilliams identities. Both of these topics were studied originally by MacWilliams in the context of linear codes defined over finite fields.

*Keywords*: Frobenius ring, Frobenius bimodule, Hamming weight, equivalence theorem, extension theorem, parameterized codes, virtual codes, linear codes over modules, dual codes, weight enumerators, MacWilliams identities

## 1. Introduction

A summer school on Codes over Rings was held August 18–29, 2008, at the Middle East Technical University, Ankara, Turkey. The summer school was sponsored by CIMPA, UNESCO, and TÜBİTAK. It was a great honor for me to be invited to give a series of lectures at the summer school, and I thank the organizers (Marcus Greferath, Ferruh Özbudak, and Patrick Solé) and the sponsors (CIMPA, UNESCO, and TÜBİTAK, together with the Department of Mathematics and the Institute of Applied Mathematics of the Middle East Technical University) for their invitation and support.

*This paper is in final form and no version of it will be submitted for publication elsewhere.

The occasion proved to be an ideal opportunity for me to bring together in one place a number of results related to the extension theorem and the MacWilliams identities. The study of both of these topics began with work of MacWilliams in the early 1960s. The famous identities (the "MacWilliams identities") relating the Hamming weight enumerators of a linear code and its dual code appeared in the doctoral dissertation of MacWilliams.[36,37] The work of MacWilliams on the extension theorem is not as well known, but it underlies the notion of equivalence of linear codes that is central to algebraic coding theory.

The extension theorem shows that two ways of defining equivalence for linear codes are actually the same. One definition is an "extrinsic" definition: two linear codes in $\mathbb{F}_q^n$ are equivalent if there exists a monomial transformation of $\mathbb{F}_q^n$ taking one code to the other. The other definition is an "intrinsic" definition: two linear codes in $\mathbb{F}_q^n$ are equivalent if there exists a linear isomorphism between the codes that preserves Hamming weight. It is easy to see that codes that are equivalent in the extrinsic sense are also equivalent in the intrinsic sense. Indeed, any monomial transformation preserves Hamming weight, so the restriction of the monomial transformation to the codes provides the necessary linear isomorphism that preserves Hamming weight.

The converse amounts to an extension problem. Given a linear isomorphism between two linear codes in $\mathbb{F}_q^n$ that preserves Hamming weight, is it possible to extend the mapping to a monomial transformation of all of $\mathbb{F}_q^n$? MacWilliams proved that this was always possible (Refs. 36 and 35), and thus the two definitions of equivalence are actually the same. This result goes by several names: the "equivalence theorem" of MacWilliams or the "extension theorem" of MacWilliams. I will use the second name.

While there had been some early work on linear codes defined over finite rings (for example, Refs. 2, 5, 6, 45, 46, and 51), there was an explosion of interest in codes over rings following the publication of the famous $\mathbb{Z}_4$ paper.[25]

My interest in the extension problem began on April 28, 1992, when Vera Pless suggested that I re-visit the work of MacWilliams on that topic. This eventually led to a character-theoretic proof of the extension theorem for Hamming weight over finite fields in joint work with Thann Ward.[50] When Ref. 25 appeared, I started working on generalizing the character-theoretic proof of Ref. 50 to the setting of linear codes defined over finite commutative rings and equipped with the Hamming weight. On November 13, 1994, at an AMS meeting, Neil Sloane suggested that I also allow for

non-commutative rings. This work eventually led to Ref. 53, in which the extension theorem was proved for linear codes over finite Frobenius rings with the Hamming weight. In the same paper, a partial converse was proved: if $R$ is a finite commutative ring such that the extension theorem holds with respect to the Hamming weight, then $R$ is in fact Frobenius.

Other authors proved similar extension results.[12,20,22] Dinh and López-Permouth[15,16] proved more general partial converses and provided a strategy for proving the converse in full generality. A proof of the full converse, i.e., if the extension theorem holds for linear codes over a finite ring with respect to Hamming weight, then the ring is necessarily Frobenius, appeared in Ref. 57.

Crucial in the strategy of Dinh and López-Permouth and the work of Ref. 57 is the use of linear codes defined over finite modules. Nechaev and his collaborators[30] defined linear codes in that level of generality, and the study of linear codes over modules matured with an important paper of Greferath, Nechaev, and Wisbauer.[21]

In this paper, many of the results outlined above are consolidated into a unified treatment of the extension problem for linear codes defined over finite modules. In particular, this paper establishes necessary and sufficient conditions on a finite module in order that the extension theorem with respect to Hamming weight hold for linear codes defined over that module.

The MacWilliams identities are very well known. The exposition here is geared primarily towards understanding the features one should expect in a well-behaved dual code. These features, valid for linear codes defined over a finite field, are summarized in what I refer to as a "model theorem," Theorem 10.1. This model theorem is first generalized to additive codes defined over a finite abelian group, a theorem due essentially to Delsarte.[14] The exposition then turns to linear codes defined over a finite ring or over a finite module and to the extra hypotheses needed in order that the model theorem still hold. This exposition was strongly influenced by the desire to understand the interplay between dual codes defined by using a $\mathbb{Q}/\mathbb{Z}$-valued biadditive form and dual codes defined by using a bilinear form with values in the ground ring. I became aware of this interplay from the book by Nebe, Rains, and Sloane (Ref. 39, Remark 1.8.5).

While this paper is not entirely self-contained, I have included several short sections of background material in an attempt to keep prerequisites to a minimum. A number of the results in this paper have not appeared previously in print, and these results are marked with a dagger (†) in the text.

## 2. Characters

We begin by discussing characters of finite abelian groups and of finite rings.

Throughout this section $G$ is a finite abelian group under addition. A *character* of $G$ is a group homomorphism $\pi : G \to \mathbb{C}^\times$, where $\mathbb{C}^\times$ is the multiplicative group of nonzero complex numbers.

More generally, one could allow $G$ to be a commutative topological group, and define characters to be the continuous group homomorphisms $\pi : G \to \mathbb{C}^\times$. By endowing a finite abelian group with the discrete topology, every function from $G$ is continuous, and we recover the original definition. The character theory for locally compact, separable, abelian groups was developed by Pontryagin.[42,43]

### 2.1. *Basic results*

Denote by $\widehat{G} = \mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{C}^\times)$ set of all characters of $G$; $\widehat{G}$ is a finite abelian group under pointwise multiplication of functions: $(\pi\theta)(x) := \pi(x)\theta(x)$, for $x \in G$. The identity element of the group $\widehat{G}$ is the *principal character* $\pi_0 = 1$, with $\pi_0(x) = 1$ for all $x \in G$.

Let $F(G, \mathbb{C}) = \{f : G \to \mathbb{C}\}$ be the set of all functions from $G$ to the complex numbers $\mathbb{C}$; $F(G, \mathbb{C})$ is a vector space over the complex numbers of dimension $|G|$. For $f_1, f_2 \in F(G, \mathbb{C})$, define

$$\langle f_1, f_2 \rangle = \frac{1}{|G|} \sum_{x \in G} f_1(x) \bar{f}_2(x). \tag{1}$$

Then $\langle \cdot, \cdot \rangle$ is a positive definite Hermitian inner product on $F(G, \mathbb{C})$.

The following statement of basic results is left as an exercise for the reader (see, for example, Refs. 44 or 48).

**Proposition 2.1.** *Let $G$ be a finite abelian group, with character group $\widehat{G}$. Then:*

*(1) $\widehat{G}$ is isomorphic to $G$, but not naturally so;*
*(2) $G$ is naturally isomorphic to the double character group $(\widehat{G})\widehat{\ }$;*
*(3) $|\widehat{G}| = |G|$;*
*(4) $(G_1 \times G_2)\widehat{\ } \cong \widehat{G}_1 \times \widehat{G}_2$, for finite abelian groups $G_1, G_2$;*
*(5)* $\sum_{x \in G} \pi(x) = \begin{cases} |G|, & \pi = 1, \\ 0, & \pi \neq 1; \end{cases}$
*(6)* $\sum_{\pi \in \widehat{G}} \pi(x) = \begin{cases} |G|, & x = 0, \\ 0, & x \neq 0; \end{cases}$

*(7) The characters of $G$ form an orthonormal basis of $F(G, \mathbb{C})$ with respect to the inner product $\langle , \rangle$.*

### 2.2. *Additive form of characters*

It will sometimes be convenient to view the character group $\widehat{G}$ additively. Given a finite abelian group $G$, define its *dual abelian group* by $\mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{Q}/\mathbb{Z})$. The dual abelian group is written additively, and its identity element is written 0, which is the zero homomorphism from $G$ to $\mathbb{Q}/\mathbb{Z}$. The complex exponential function defines a group homomorphism $\mathbb{Q}/\mathbb{Z} \to \mathbb{C}^\times$, $x \mapsto \exp(2\pi i x)$, which is injective and whose image is the subgroup of elements of finite order in $\mathbb{C}^\times$. The complex exponential in turn induces a group homomorphism

$$\mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{Q}/\mathbb{Z}) \to \widehat{G} = \mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{C}^\times). \tag{2}$$

When $G$ is finite, the mapping in Eq. (2) is an isomorphism.

Because there will be situations where it is convenient to write characters multiplicatively and other situations where it is convenient to write characters additively, we adopt the following convention.

**Convention 2.1.** Characters written in multiplicative form, i.e., characters viewed as elements of $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{C}^\times)$ will be denoted by the "standard" Greek letters $\pi$, $\theta$, $\phi$, and $\rho$. Characters written in additive form, i.e., characters viewed as elements of $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z})$, will be denoted by the corresponding "variant" Greek letters $\varpi$, $\vartheta$, $\varphi$, and $\varrho$, so that $\pi = \exp(2\pi i \varpi)$, $\theta = \exp(2\pi i \vartheta)$, etc.

The ability to write characters additively will become very useful when $G$ has the additional structure of (the underlying abelian group of) a module over a ring (Subsection 2.3).

We warn the reader that in the last several results in Proposition 2.1, the sums (or linear independence) take place in (or over) the complex numbers. These results must be written with the characters in multiplicative form.

Let $H \subset G$ be a subgroup, and define the *annihilator* $(\widehat{G} : H) = \{\varpi \in \widehat{G} : \varpi(h) = 0, \text{ for all } h \in H\}$. Then $(\widehat{G} : H)$ is isomorphic to the character group of $G/H$, so that $|(\widehat{G} : H)| = |G|/|H|$.

**Proposition 2.2.** *Let $H$ be a subgroup of $G$ with the property that $H \subset \ker \varpi$ for all characters $\varpi \in \widehat{G}$. Then $H = 0$.*

**Proof.** The hypothesis implies that $(\widehat{G} : H) = \widehat{G}$. Calculating $|H| = 1$, we conclude that $H = 0$. □

### 2.3. *Character modules*

If the finite abelian group $G$ is the additive group of a module $M$ over a ring $R$, then the character group $\widehat{M}$ inherits an $R$-module structure. In this process, sides get reversed; i.e., if $M$ is a left $R$-module, then $\widehat{M}$ is a right $R$-module, and vice versa.

Explicitly, if $M$ is a left $R$-module, then the right $R$-module structure of $\widehat{M}$ is defined by

$$(\varpi r)(m) := \varpi(rm), \quad \varpi \in \widehat{M}, r \in R, m \in M.$$

Similarly, if $M$ is a right $R$-module, then the left $R$-module structure of $\widehat{M}$ is given by

$$(r\varpi)(m) := \varpi(mr), \quad \varpi \in \widehat{M}, r \in R, m \in M.$$

**Remark 2.1.** When $\widehat{M}$ is written in multiplicative form, one may see the scalar multiplication for the module structure written in exponential form (for example, in Ref. 53 and in the proof of Theorem 5.1):

$$\pi^r(m) := \pi(rm), \quad \pi \in \widehat{M}, r \in R, m \in M,$$

when $M$ is a left $R$-module and $\widehat{M}$ is a right $R$-module, and

$${}^r\pi(m) := \pi(mr), \quad \pi \in \widehat{M}, r \in R, m \in M,$$

when $M$ is a right $R$-module and $\widehat{M}$ is a left $R$-module. The reader will verify such formulas as $(\pi^r)^s = \pi^{rs}$.

**Lemma 2.1.** *Let $R$ be a finite ring, with $\widehat{R}$ its character bimodule. If $r\widehat{R} = 0$ (resp., $\widehat{R}r = 0$), then $r = 0$.*

**Proof.** Suppose $r\widehat{R} = 0$. For any $\varpi \in \widehat{R}$ and $x \in R$, we have $0 = r\varpi(x) = \varpi(xr)$. Thus $Rr \subset \ker \varpi$, for all $\varpi \in \widehat{R}$. By Proposition 2.2, $Rr = 0$, so that $r = 0$. □

## 3. Finite rings

Throughout this section $R$ will be a finite associative ring with 1. References for this section include Refs. 31 and 32.

### 3.1. *Basic definitions*

The (*Jacobson*) *radical* $\mathrm{rad}(R)$ of a finite ring $R$ is the intersection of all the maximal left ideals of $R$. The radical is also the intersection of all the maximal right ideals of $R$, and the radical is a two-sided ideal of $R$.

A nonzero module over $R$ is *simple* if it has no nontrivial submodules. Given any left $R$-module $M$, the *socle* $\mathrm{soc}(M)$ is the sum of all the simple submodules of $M$.

**Convention 3.1.** If $f : M_1 \to M_2$ is a homomorphism of left $R$-modules, then the inputs to $f$ will be written on the left. Thus, if $x \in M_1$, then $xf \in M_2$. The scalar multiplication property of a left module homomorphism is expressed as $(rx)f = r(xf)$, for $r \in R$, $x \in M_1$.

### 3.2. *Structure of finite rings*

If $R$ is a finite ring, then, as rings

$$R/\operatorname{rad}(R) \cong M_{\mu_1}(\mathbb{F}_{q_1}) \oplus \cdots \oplus M_{\mu_n}(\mathbb{F}_{q_n}), \tag{3}$$

for some nonnegative integers $n, \mu_1, \ldots, \mu_n$ and prime powers $q_1, \ldots, q_n$, where $M_m(\mathbb{F}_q)$ is the ring of all $m \times m$ matrices over the finite field $\mathbb{F}_q$ of $q$ elements. Indeed, being semisimple, $R/\operatorname{rad}(R)$ is a direct sum of full matrix rings over division rings by a theorem of Wedderburn-Artin (Ref. 32, Theorem 3.5). Since $R$ is finite, the division rings must also be finite, hence commutative by another theorem of Wedderburn (Ref. 32, Theorem 13.1).

Recall that the matrix ring $M_m(\mathbb{F})$ has a standard representation on the $M_m(\mathbb{F})$-module $M_{m,1}(\mathbb{F})$ of all $m \times 1$ matrices over $\mathbb{F}_q$, via matrix multiplication. As a left module over itself,

$${}_{M_m(\mathbb{F})}M_m(\mathbb{F}) \cong mM_{m,1}(\mathbb{F}).$$

Consequently, as a left $R$-module, it follows from Eq. (3) that

$${}_R\,(R/\operatorname{rad}(R)) \cong \mu_1 T_1 \oplus \cdots \oplus \mu_n T_n, \tag{4}$$

where $T_i$ denotes the pullback to $R$ via Eq. (3) of the standard left $M_{\mu_i}(\mathbb{F}_{q_i})$-module $M_{\mu_i,1}(\mathbb{F}_{q_i})$ of all $\mu_i \times 1$ matrices over $\mathbb{F}_{q_i}$. The simple left $R$-modules $T_i$, $i = 1, 2, \ldots, n$, form the complete list of all simple left $R$-modules, up to isomorphism.

### 3.3. *Duality*

We provide a few key properties of character modules.

Given a finite left (right) $R$-module $M$, recall that the character module $\widehat{M} = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ is a right (left) $R$-module.

A left module $M$ over a ring $R$ is *injective* if, for every pair of left $R$-modules $B_1 \subset B_2$ and every $R$-linear mapping $f : B_1 \to M$, the mapping $f$ extends to an $R$-linear mapping $\tilde{f} : B_2 \to M$.

The next several propositions are exercises for the reader (cf. Ref. 53, Sections 2–3, and the references therein).

**Proposition 3.1.** *The mapping* $\widehat{\ }$ *taking* $M$ *to* $\widehat{M}$ *is a contravariant functor from the category of finitely-generated left* (*right*) $R$*-modules to the category of finitely-generated right* (*left*) $R$*-modules.*

**Lemma 3.1.** *The abelian group* $\mathbb{Q}/\mathbb{Z}$ *is divisible; i.e.,* $m(\mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$ *for all nonzero integers* $m$*. Moreover,* $\mathbb{Q}/\mathbb{Z}$ *is an injective* $\mathbb{Z}$*-module.*

**Proof.** See Ref. 13, 57.5. □

**Proposition 3.2.** *The functor* $\widehat{\ }$ *is an exact functor; i.e.,* $\widehat{\ }$ *takes short exact sequences of modules to short exact sequences of modules.*

**Proof.** Use $\mathbb{Q}/\mathbb{Z}$ injective. □

**Corollary 3.1.** *When* $M = R$ *itself,* $\widehat{R}$ *is an injective* $R$*-module.*

**Proof.** An exact functor takes projective modules, in particular, free modules, to injective modules. □

**Proposition 3.3.** *Let* $M_R$ *be any finite right* $R$*-module. Then*

$$(\widehat{M} : M \operatorname{rad}(R)) = \operatorname{soc}(\widehat{M});$$

*in particular,*

$$(M/M \operatorname{rad}(R))\widehat{\ } \cong \operatorname{soc}(\widehat{M}).$$

**Proof.** Being an exact functor, the character functor takes direct sums to direct sums and simple modules to simple modules.

Begin with the short exact sequence

$$0 \to M \operatorname{rad}(R) \to M \to M/M \operatorname{rad}(R) \to 0.$$

Now apply the character functor, yielding the short exact sequence

$$0 \to (\widehat{M} : M \operatorname{rad}(R)) \to \widehat{M} \to (M \operatorname{rad}(R))\widehat{\ } \to 0.$$

Because $M/M \operatorname{rad}(R)$ is a finite sum of simple modules, the same is true of $(M/M \operatorname{rad}(R))\widehat{\ } \cong (\widehat{M} : M \operatorname{rad}(R))$. Thus $(\widehat{M} : M \operatorname{rad}(R)) \subset \operatorname{soc}(\widehat{M})$.

For the converse, note that $\operatorname{rad}(R) \operatorname{soc}(\widehat{M}) = 0$, since the radical annihilates simple modules (Ref. 13, Exercise 25.4). This implies that $\operatorname{soc}(\widehat{M}) \subset (\widehat{M} : M \operatorname{rad}(R))$, and equality holds.

For the second claim, use $(\widehat{M} : M \operatorname{rad}(R)) \cong (M/M \operatorname{rad}(R))\widehat{\ }$. □

## 4. Möbius functions of posets

### 4.1. *Basic definitions*

In this subsection, we review some of the basic definitions of partially ordered sets and their Möbius functions. A reference for this material (and much more) is Ref. 47.

Suppose that $(P, \leq)$ is a *partially ordered set*, i.e., $\leq$ is a reflexive, antisymmetric, and transitive relation on $P$. A partially ordered set is also called a *poset*, for short. Assume that, for every $x, y \in P$, the *interval* $\{t \in P : x \leq t \leq y\}$ is finite. Then the *Möbius function* $\mu : P \times P \to \mathbb{Q}$ is defined by the conditions: $\mu(x, x) = 1$, $\mu(x, y) = 0$ if $x \not\leq y$, and

$$\mu(x, y) = -\sum_{x \leq t < y} \mu(x, t), \quad \text{if } x < y. \tag{5}$$

This definition is usually applied recursively. First, $\mu(x, x) = 1$ for any $x \in P$. Then $\mu(x, y) = -1$ for those $y \in P$ with $x < y$, but with no $t \in P$ satisfying $x < t < y$. At the next stage, consider $y \in P$ that are two "steps" from $x$, i.e., there exists $t \in P$ with $x < t < y$, but there do not exist $u, v \in P$ with $x < u < v < y$. In that case, $\mu(x, y) = -1 + n$, where $n$ equals the number of $t \in P$ with $x < t < y$. This process (a generalization of inclusion-exclusion) continues for longer chains of inclusions $x < t_1 < t_2 < \cdots < y$. Observe that Eq. (5) can be re-written as

$$\sum_{x \leq t \leq y} \mu(x, t) = 0, \quad \text{if } x < y. \tag{6}$$

The partial order and the Möbius function induce transformations on the space of rational (or real, or complex) valued functions on $P$, as follows. Define two transformations $\Sigma, \Delta : F(P, \mathbb{Q}) \to F(P, \mathbb{Q})$ by:

$$(\Sigma f)(x) = \sum_{y \leq x} f(y), \qquad x \in P,$$

$$(\Delta g)(y) = \sum_{x \leq y} g(x)\mu(x, y), \qquad y \in P.$$

The reader will check that $\Sigma$ and $\Delta$ are inverses. (This is the *Möbius inversion formula*; see Ref. 47, §3.7, for details.)

### 4.2. *Examples*

We give several examples. Example 4.3 will be used in Subsection 9.1, and Example 4.4 will be used in the proof of Theorem 6.3.

**Example 4.1.** Let $P$ be the set of positive integers. For $a, b \in P$, define $a \leq b$ if $a$ divides $b$ in the integers. Then $\mu(1, a)$ is the standard Möbius function of elementary number theory. See Ref. 47, Examples 3.1.1c and 3.8.4, for details.

**Example 4.2.** Let $R$ be a finite ring and $M$ a finite left module over $R$. Let $P$ be the set of all left $R$-submodules of $M$. Then $P$ is a poset under set inclusion $\subseteq$.

**Example 4.3.** Again, let $R$ be a finite ring and $M$ a finite left module over $R$. Let $P$ be the set of all principal left $R$-submodules of $M$, i.e., submodules with one generator. Then $P$ again is a poset under set inclusion. This poset and the previous one were used, for example, by Greferath and his collaborators[20–22] in their work on the extension theorem with respect to the homogeneous weight (see Subsection 9.1).

**Example 4.4.** As a special case, let $\mathbb{F}_q$ be a finite field of order $q$ and $V$ a finite-dimensional vector space over $\mathbb{F}_q$. Let $P = \mathcal{L}(V)$ be the set of all linear subspaces of $V$. Then $\mathcal{L}(V)$ is a poset under set inclusion. Compare Ref. 47, Example 3.1.1e.

A formula for the Möbius function for $\mathcal{L}(V)$ of Example 4.4 was determined in Ref. 24, (2.7). To describe it, we include a brief description of $q$-binomial coefficients and the Cauchy binomial theorem. The reader may consult Ref. 47, Example 3.10.2 and Exercise 3.45, as well.

The *q-binomial coefficient* (or *Gaussian coefficient*, *Gaussian number* or *Gaussian polynomial*) is defined as

$$\begin{bmatrix} k \\ l \end{bmatrix}_q = \frac{(1-q^k)(1-q^{k-1})\cdots(1-q^{k-l+1})}{(1-q^l)(1-q^{l-1})\cdots(1-q)}.$$

The following lemmas are well-known (see such sources as Ref. 1, Chapter 3, and Ref. 33, Chapter 24]). The first counts the number of row reduced echelon matrices over $\mathbb{F}_q$ (and hence the number of linear subspaces of a finite-dimensional vector space over $\mathbb{F}_q$), and the second is the Cauchy binomial theorem.

**Lemma 4.1.** *The q-binomial coefficient* $\left[\begin{smallmatrix} k \\ l \end{smallmatrix}\right]_q$ *counts the number of row* (*or column*) *reduced echelon matrices of length* $k$ *over* $\mathbb{F}_q$ *of rank* $l$ (*i.e., row reduced echelon matrices of size* $l \times k$ *of rank* $l$*, or column reduced echelon matrices of size* $k \times l$ *of rank* $l$). *The number* $\left[\begin{smallmatrix} k \\ l \end{smallmatrix}\right]_q$ *is also the number of linear subspaces of dimension* $l$ *inside a vector space of dimension* $k$ *over* $\mathbb{F}_q$.

**Lemma 4.2.** *The Cauchy binomial theorem:*

$$\prod_{i=0}^{k-1}\left(1+xq^i\right)=\sum_{j=0}^{k}\begin{bmatrix}k\\ j\end{bmatrix}_q q^{\binom{j}{2}}x^j.$$

**Proposition 4.1.** *Let $V$ be a finite-dimensional vector space over the finite field $\mathbb{F}_q$. Then the Möbius function $\mu$ for $\mathcal{L}(V)$ satisfies*

$$\mu(0,W)=(-1)^{\dim W}q^{\binom{\dim W}{2}},$$

*for any linear subspace $W\subset V$.*

**Proof.** Notice that $\binom{0}{2}=\binom{1}{2}=0$. We prove the result by induction on $\dim W$. When $\dim W=0$, then $W=0$, and $\mu(0,0)=1=(-1)^0q^{\binom{0}{2}}$ follows from the definition of $\mu$.

Assume that the result holds for all dimensions $<k$; we prove the result for $W$ with $\dim W=k$. By the definition of $\mu$,

$$\mu(0,W)=-\sum_{\substack{U\subset W\\ U\neq W}}\mu(0,U).$$

By the induction hypothesis, the equation above transforms to

$$\mu(0,W)=-\sum_{\substack{U\subset W\\ U\neq W}}(-1)^{\dim U}q^{\binom{\dim U}{2}}=-\sum_{l=0}^{k-1}(-1)^l q^{\binom{l}{2}}\begin{bmatrix}k\\ l\end{bmatrix}_q,$$

where $\dim U=l$. By comparing with the Cauchy binomial theorem for $x=-1$, we conclude that $\mu(0,W)$ has the desired form. □

**Remark 4.1.** More generally, one can show that

$$\mu(W_1,W_2)=(-1)^c\,q^{\binom{c}{2}},$$

where $c=\dim W_2-\dim W_1$.

## 5. Linear codes over modules; sufficient conditions for the extension theorem

### 5.1. *Basic definitions*

Let $R$ be a finite ring with 1, and let $A$ be a finite left $R$-module. The module $A$ will serve as the *alphabet* for the linear codes we discuss. We begin with several standard definitions. Please remember the convention that inputs to homomorphisms of left $R$-modules are written on the left.

A *linear code* of length $n$ over the alphabet $A$ is a left $R$-submodule $C \subset A^n$. The idea of using a module $A$ as the alphabet for linear codes goes back to Ref. 30.

A *monomial transformation* of $A^n$ is an $R$-linear automorphism $T$ of $A^n$ of the form

$$(a_1, \ldots, a_n)T = (a_{\sigma(1)}\tau_1, \ldots, a_{\sigma(n)}\tau_n), \quad (a_1, \ldots, a_n) \in A^n, \tag{7}$$

where $\sigma$ is a permutation of $\{1, 2, \ldots, n\}$ and $\tau_1, \ldots, \tau_n \in \mathrm{Aut}(A)$ are automorphisms of $A$ (being written on the right, as is $T$). If the automophisms $\tau_i$ are constrained to lie in some subgroup $G \subset \mathrm{Aut}(A)$, we say that $T$ is a *$G$-monomial transformation* of $A^n$.

A *weight* on the alphabet $A$ is any function $w : A \to \mathbb{Q}$ with the property that $w(0) = 0$. Any such weight extends to a weight $w : A^n \to \mathbb{Q}$ by $w(a_1, \ldots, a_n) = \sum w(a_i)$.

Given a weight $w : A \to \mathbb{Q}$, define the left and right *symmetry groups* of $w$ by:

$$G_l := \{u \in \mathcal{U}(R) : w(ua) = w(a), \text{ for all } a \in A\}, \tag{8}$$

$$G_r := \{\tau \in \mathrm{Aut}(A) : w(a\tau) = w(a), \text{ for all } a \in A\}. \tag{9}$$

Here, $\mathcal{U}(R)$ denotes the group of units of the ring $R$.

Given a weight $w : A \to \mathbb{Q}$, we say that a function $f : A^n \to A^n$ *preserves* $w$ if $w(xf) = w(x)$, for all $x \in A^n$. Observe that a $G_r$-monomial transformation preserves $w$.

Assume that the alphabet $A$ is equipped with a weight $w$, whose symmetry groups are $G_l$ and $G_r$. Suppose that $C_1, C_2 \subset A^n$ are two linear codes of length $n$ over the alphabet $A$. If there exists a $G_r$-monomial transformation $T$ of $A^n$ such that $C_1T = C_2$ (in which case we say that $C_1$ and $C_2$ are *$G_r$-monomially equivalent*), then the restriction $T : C_1 \to C_2$ is an $R$-linear isomorphism that preserves the weight $w$. We describe the converse as a property—the extension property.

**Definition 5.1.** The alphabet $A$ has the *extension property* (EP) with respect to the weight $w$ if the following condition holds:

For any two linear codes $C_1, C_2 \subset A^n$, if $f : C_1 \to C_2$ is an $R$-linear isomorphism that preserves the weight $w$, then $f$ extends to a $G_r$-monomial transformation of $A^n$.

### 5.2. *The character module as alphabet: the case of Hamming weight*

Any alphabet $A$ can be equipped with the *Hamming* weight $\mathrm{wt} : A \to \mathbb{Q}$, where $\mathrm{wt}(0) = 0$ and $\mathrm{wt}(a) = 1$ for all nonzero $a \in A$. For $x = (x_1, \ldots, x_n) \in A^n$, observe that $\mathrm{wt}(x)$ equals the number of nonzero entries of the vector $x$. The symmetry groups of the Hamming weight are as large as possible: $G_l = \mathcal{U}(R)$, $G_r = \mathrm{Aut}(A)$.

An important class of alphabets for which the extension property holds with respect to Hamming weight is the class of Frobenius bimodules of finite rings. This result is due to Greferath, Nechaev, and Wisbauer,[21] and we will provide below a proof similar to the one for Frobenius rings, Ref. 53, Theorem 6.3 (which, in turn, generalized a proof over finite fields in Ref. 50, Theorem 1). This result provides the backbone for the proof of Theorem 5.2.

A *Frobenius bimodule* $A = {}_RA_R$ is an $(R, R)$-bimodule such that ${}_RA \cong {}_R\widehat{R}$ and $A_R \cong \widehat{R}_R$. Of course, the character bimodule ${}_R\widehat{R}_R$ is a Frobenius bimodule, but a Frobenius bimodule need not be isomorphic, as a bimodule, to ${}_R\widehat{R}_R$.

**Theorem 5.1 (Ref. 21, Theorem 4.5).** *Let $R$ be a finite ring and $A$ be a Frobenius bimodule over $R$. Then $A$ has the extension property with respect to Hamming weight.*

Before we begin the proof, we prove several preliminary results about the structure of $\widehat{A}$, the character bimodule of a Frobenius bimodule $A$.

**Lemma 5.1.** *If $A$ is a Frobenius bimodule, then its character bimodule $\widehat{A}$ satisfies*

$$ {}_R\widehat{A} \cong {}_RR \quad \textit{and} \quad \widehat{A}_R \cong R_R. $$

**Proof.** Dualize the definition of Frobenius bimodule. □

Given that ${}_R\widehat{A} \cong {}_RR$ and $\widehat{A}_R \cong R_R$ for a Frobenius bimodule $A$, we say that a character $\varrho \in \widehat{A}$ is a *left generator* (resp., *right generator*) for $\widehat{A}$ if $\bullet\varrho : {}_RR \to {}_R\widehat{A}$, $r \mapsto r\varrho$ (resp., $\varrho\bullet : R_R \to \widehat{A}_R$, $r \mapsto \varrho r$) is an isomorphism.

The next lemma is a rephrasing of the definition of a generator.

**Lemma 5.2.** *Given a character $\varrho \in \widehat{A}$, if $\ker \varrho \subset A$ contains no nonzero left (resp., right) $R$-submodule of $A$, then $\varrho$ is a left generator (resp., right generator) of $\widehat{A}$.*

**Proof.** We will prove the contrapositive of the left case, with the right case being similar. If $\varrho \in \widehat{A}$ is not a left generator, then the map $\bullet\varrho : {}_R R \to {}_R\widehat{A}$, $r \mapsto r\varrho$, is not an isomorphism. Because $R$ and $A$ are finite and $|\widehat{A}| = |R|$, $\bullet\varrho$ not being an isomorphism implies that $\bullet\varrho$ is not injective. Thus $\ker(\bullet\varrho) \neq 0$.

Take any nonzero $r \in \ker(\bullet\varrho)$. This means that $0 = (r\varrho)(a) = \varrho(ar)$ for all $a \in A$. Thus the left $R$-submodule $Ar$ of $A$ satisfies $Ar \subset \ker\varrho$. Because $r \neq 0$, the module $Ar \neq 0$, by Lemma 2.1. □

The final lemma reverses the sides.

**Lemma 5.3.** *If $\varrho$ is a left generator (resp., right generator) for $\widehat{A}$, then $\ker\varrho$ contains no nonzero right (resp., left) $R$-submodule of $A$.*

**Proof.** We prove the left generator case. The other case follows by a symmetric argument.

Suppose $\varrho$ is a left generator of $\widehat{A}$, and suppose $B_R \subset A_R$ is a right submodule such that $B \subset \ker\varrho$. Take any character $\varpi \in \widehat{A}$. Because $\varrho$ is a left generator of $\widehat{A}$, $\varpi = s\varrho$ for some $s \in R$. For any $b \in B$, we calculate that $\varpi(b) = (s\varrho)(b) = \varrho(bs) = 0$, since $B$ is a right submodule and $B \subset \ker\varrho$. Thus $B \subset \ker\varpi$, for all $\varpi \in \widehat{A}$. By Proposition 2.2, $B = 0$. □

**Corollary 5.1.** *Suppose $A$ is a Frobenius bimodule. Then a character $\varrho \in \widehat{A}$ is a left generator for $\widehat{A}$ if and only if it is a right generator for $\widehat{A}$.*

**Proof.** This follows immediately from Lemmas 5.2 and 5.3. □

**(†) Proof of Theorem 5.1, following [53, Theorem 6.3].**

Before presenting the details, here is an outline of the proof. We assume that two linear codes $C_1, C_2 \subset A^n$ are isomorphic via a linear isomorphism $f : C_1 \to C_2$ such that $f$ preserves Hamming weight, $\mathrm{wt}(xf) = \mathrm{wt}(x)$, for all $x \in C_1$. We can express the Hamming weights $\mathrm{wt}(xf) = \mathrm{wt}(x)$ as sums involving the coordinate functionals of the codes composed with characters on the alphabet $A$. The resulting equation is an equation of sums of characters on $C_1$. The linear independence of characters (together with some careful bookkeeping) allows us to match up terms, thereby constructing the desired monomial transformation extending $f$. We now turn to the details.

Let $M = {}_R M$ be the common underlying module of the isomorphic codes $C_1, C_2 \subset A^n$. Let the two embeddings of $M$ into $A^n$ be given by coordinate functionals $\lambda_1, \ldots, \lambda_n$ (for $C_1$) and $\nu_1, \ldots, \nu_n$ (for $C_2$) in $\mathrm{Hom}_R(M, A)$. (Because $M$ is a left module, the coordinate functionals will

be written on the right: $x\lambda \in A$, for $x \in M$ and $\lambda \in \mathrm{Hom}_R(M, A)$. Linearity is then expressed by $(rm)\lambda = r(m\lambda)$. The right $R$-module structure on $A$ induces a right $R$-module structure on $\mathrm{Hom}_R(M, A)$.)

Because Hamming weight is preserved, Proposition 2.1 implies that

$$\sum_{i=1}^{n} \sum_{\pi \in \widehat{A}} \pi(x\lambda_i) = \sum_{j=1}^{n} \sum_{\theta \in \widehat{A}} \theta(x\nu_j), \quad x \in M. \tag{10}$$

Please remember our notational convention that $\pi, \theta$ are characters in multiplicative form.

Let $\varrho$ be a left generator of $\widehat{A}$. Remember that $\rho = \exp(2\pi i \varrho)$ is the multiplicative form of $\varrho$. We can re-write Eq. (10) as

$$\sum_{i=1}^{n} \sum_{r \in R} {}^{r}\rho(x\lambda_i) = \sum_{j=1}^{n} \sum_{s \in R} {}^{s}\rho(x\nu_j), \quad x \in M.$$

Using the $R$-module structures on $\widehat{A}$ and $\mathrm{Hom}_R(M, A)$, we have

$$\sum_{i=1}^{n} \sum_{r \in R} \rho(x\lambda_i r) = \sum_{j=1}^{n} \sum_{s \in R} \rho(x\nu_j s), \quad x \in M. \tag{11}$$

This is an equation of characters on $M$.

The right $R$-module $\mathrm{Hom}_R(M, A)$ admits a reflexive, transitive relation $\preceq$ defined by $\lambda \preceq \nu$ when $\lambda = \nu r$ for some $r \in R$. It follows from a result of Bass, Ref. 4, Lemma 6.4, that $\lambda \preceq \nu$ and $\nu \preceq \lambda$ imply $\lambda = \nu u$ for some $u \in \mathcal{U}(R)$. Then $\preceq$ induces a partial ordering on the set of right $\mathcal{U}(R)$-orbits in $\mathrm{Hom}_R(M, A)$.

Among the finite number of elements $\lambda_1, \ldots, \lambda_n$, $\nu_1, \ldots, \nu_n$ of (the set of right $\mathcal{U}(R)$-orbits in) $\mathrm{Hom}_R(M, A)$, choose one that is maximal for the partial order $\preceq$. Without loss of generality, call this maximal element $\lambda_1$. Now consider the term $\rho(x\lambda_1)$, i.e., $r = 1$, on the left side of Eq. (11). By the linear independence of characters on $M$, there exists an index $j = \sigma(1)$ and element $s \in R$ with $\rho(x\lambda_1) = \rho(x\nu_j s)$ for all $x \in M$. This implies that $\mathrm{im}(\lambda_1 - \nu_j s) \subset \ker \varrho$. Observe that $\mathrm{im}(\lambda_1 - \nu_j s)$ is a left $R$-submodule of $A$. Because $\varrho$ is a left generator for $\widehat{A}$, Lemma 5.2 implies $\mathrm{im}(\lambda_1 - \nu_j s) = 0$, so that $\lambda_1 = \nu_j s$. This implies that $\lambda_1 \preceq \nu_j$. But $\lambda_1$ was chosen to be a maximal element under $\preceq$, so that $\lambda_1$ and $\nu_j$ are in the same right $\mathcal{U}(R)$-orbit, i.e., $\lambda_1 = \nu_j u_1$ for some unit $u_1$ in $R$.

Re-indexing ($s = u_1 r$) shows that

$$\sum_{r \in R} \rho(x\lambda_1 r) = \sum_{r \in R} \rho(x\nu_j u_1 r) = \sum_{s \in R} \rho(x\nu_j s), \quad x \in M,$$

thereby allowing us to reduce by one the size of the outer summations in Eq. (11). Proceeding by induction, we produce a permutation $\sigma$ and units $u_1, \ldots, u_n$ in $R$ with $\lambda_i = \nu_{\sigma(i)} u_i$, as desired. □

### 5.3. *Sufficient conditions: the case of Hamming weight*

Before stating sufficient conditions for the alphabet $A$ to have the extension property with respect to the Hamming weight wt, we provide one more definition from module theory.

A left module $M$ over a ring $R$ is *pseudo-injective* if, for every left $R$-submodule $B \subset M$ and every injective $R$-linear mapping $f : B \to M$, the mapping $f$ extends to an $R$-linear mapping $\tilde{f} : M \to M$.

Observe that the definition of pseudo-injectivity is very close to that of the extension property for linear codes of length 1. In fact, these two concepts are equivalent, as the following result of Dinh and López-Permouth demonstrates.

**Proposition 5.1 (Ref. 15, Proposition 3.2).** *The alphabet $A$ has the extension property for linear codes of length* 1 *with respect to Hamming weight (i.e., if $C_1, C_2 \subset A$ and if $f : C_1 \to C_2$ is an $R$-linear isomorphism that preserves the Hamming weight* wt*, then $f$ extends to an automorphism of $A$) if and only if the alphabet $A$ is a pseudo-injective $R$-module.*

**Proof, following Ref. 15.** Observe that if an $R$-linear mapping $f$ preserves the Hamming weight wt, then $f$ is injective. Thus, the extension property for length one codes is equivalent to saying that every injective map $f : B \to A$ of a submodule $B \subset A$ extends to an automorphism of $A$. It is evident that this property implies that the module $A$ is pseudo-injective.

For the converse, suppose that $A$ is pseudo-injective. Let $B \subset A$ be a submodule and let $f : B \to A$ be an injective $R$-linear homomorphism. We must show that $f$ extends to an automorphism of $A$.

Case 1: when $\mathrm{soc}(B) = \mathrm{soc}(A)$. Because $A$ is pseudo-injective, $f$ extends to an $R$-linear homomorphism $\tilde{f} : A \to A$. Consider the submodule $\ker(\tilde{f}) \subset A$. Observe that $\mathrm{soc}(\ker(\tilde{f})) \subset \mathrm{soc}(A) = \mathrm{soc}(B) \subset B$. But $\ker(\tilde{f}) \cap B = \ker(f) = 0$, since $f$ is injective. Thus $\mathrm{soc}(\ker(\tilde{f})) = 0$, so that $\ker(\tilde{f}) = 0$ as well.

Case 2: when $\mathrm{soc}(B) \neq \mathrm{soc}(A)$. There exists a submodule $M \subset \mathrm{soc}(A)$ so that $\mathrm{soc}(B) \oplus M = \mathrm{soc}(A)$. Observe that $\mathrm{soc}(B) \cap M = 0$ and that $\mathrm{soc}(B \oplus M) = \mathrm{soc}(A)$. We now show that $f$ extends injectively to $B \oplus M$. Notice that $\mathrm{soc}(B)f$ is properly contained in $\mathrm{soc}(A)$, so there exists a submodule

$N \subset \mathrm{soc}(A)$ with $\mathrm{soc}(B)f \oplus N = \mathrm{soc}(A)$. Putting these together, we see that $\mathrm{soc}(B) \oplus M = \mathrm{soc}(A) = \mathrm{soc}(B)f \oplus N$ and $\mathrm{soc}(B) \cong \mathrm{soc}(B)f$. This implies that $M \cong N$, since $\mathrm{soc}(A)$ is a semi-simple module. Let $g : M \to N$ be any isomorphism. Extend $f : B \to A$ to $h : B \oplus M \to A$ by $(b+m)h = bf + mg$. One verifies that $h$ is injective. Because $\mathrm{soc}(B \oplus M) = \mathrm{soc}(A)$, case 1 implies that $h$ (and hence $f$) extends to an automorphism of $A$. □

The other condition that arises in the statement of the extension theorem is $\mathrm{soc}(A)$ being a *cyclic* module, i.e., there is a surjective $R$-linear homomorphism $R \to \mathrm{soc}(A)$.

Because $\mathrm{soc}(A)$ is a sum of simple $R$-modules, we can write

$$\mathrm{soc}(A) \cong s_1 T_1 \oplus \cdots \oplus s_n T_n, \tag{12}$$

where the $T_i$ are the simple $R$-modules from Eq. (4) of Subsection 3.2.

**Proposition 5.2.** *The socle* $\mathrm{soc}(A)$ *is a cyclic module if and only if* $s_i \leq \mu_i$*, for* $i = 1, 2, \ldots, n$*, where the* $\mu_i$ *are defined in Eq.* (3) *of Subsection 3.2.*

**Proof.** This is an exercise for the reader. □

**Proposition 5.3.** *The socle* $\mathrm{soc}(A)$ *is a cyclic module if and only if* $A$ *can be embedded into* ${}_R\widehat{R}$*.*

**Proof.** There is a right module counterpart to Eq. (4) of Subsection 3.2, yielding simple right $R$-modules $S_1, \ldots, S_n$ that are the counterparts to the simple left $R$-modules $T_1, \ldots, T_n$. A calculation shows that $\widehat{S}_i \cong T_i$. By applying Proposition 3.3 to $R_R$, it then follows that

$$\mathrm{soc}({}_R\widehat{R}) \cong ((R/\operatorname{rad}(R))_R)\widehat{\ } \cong \mu_1 T_1 \oplus \cdots \oplus \mu_n T_n.$$

If $A \subset {}_R\widehat{R}$, then $\mathrm{soc}(A) \subset \mathrm{soc}({}_R\widehat{R})$. But this implies that $s_i \leq \mu_i$ for all $i$, so that $\mathrm{soc}(A)$ is cyclic by Proposition 5.2.

Conversely, if $\mathrm{soc}(A)$ is cyclic, then $\mathrm{soc}(A)$ can be embedded in $\mathrm{soc}({}_R\widehat{R})$, via some homomorphism $f$. View $f : \mathrm{soc}(A) \to {}_R\widehat{R}$. Because the character module of a ring is always an injective module (Corollary 3.1), the homomorphism $f$ extends to a homomorphism $F : A \to {}_R\widehat{R}$. It remains to show that $F$ is injective.

Observe that $\mathrm{soc}(\ker F) = \ker F \cap \mathrm{soc}(A) = \ker f = 0$, because $f$ is injective. Because $\mathrm{soc}(\ker F) = 0$, we conclude that $\ker F = 0$, and $F$ is injective. □

**Theorem 5.2 (†).** *An alphabet $A$ has the extension property with respect to Hamming weight if:*

*(1) $A$ is pseudo-injective, and*
*(2)* $\mathrm{soc}(A)$ *is cyclic.*

**Proof.** Let $C_1, C_2 \subset A^n$ be two $R$-linear codes, and suppose $f : C_1 \to C_2$ is an $R$-linear isomorphism that preserves Hamming weight. By virtue of the hypothesis that $\mathrm{soc}(A)$ is cyclic, Proposition 5.3 implies that $A$ embeds in ${}_R\widehat{R}$. Using this embedding, we may view $C_1, C_2 \subset \widehat{R}^n$ as $R$-linear codes over the alphabet ${}_R\widehat{R}$. Note that the Hamming weights of elements of $C_1, C_2$ remain the same, whether they are viewed as codes over $A$ or as codes over $\widehat{R}$.

With the standard Frobenius bimodule structure on $\widehat{R}$, Theorem 5.1 implies that the isomorphism $f : C_1 \to C_2$ extends to a monomial transformation $F : \widehat{R}^n \to \widehat{R}^n$. Explicitly,

$$(x_1, \ldots, x_n)F = (x_{\sigma(1)}u_1, \ldots, x_{\sigma(n)}u_n), \quad (x_1, \ldots, x_n) \in \widehat{R}^n,$$

where $\sigma$ is a permutation of $\{1, 2, \ldots, n\}$ and $u_i \in \mathcal{U}(R) = \mathrm{Aut}({}_R\widehat{R})$. Remember that $C_1F = C_2$.

Let $P$ (resp., $D$) be the permutation (resp., diagonal) portion of the monomial transformation $F$; i.e.,

$$(x_1, \ldots, x_n)P = (x_{\sigma(1)}, \ldots, x_{\sigma(n)}), \quad (x_1, \ldots, x_n) \in \widehat{R}^n,$$
$$(x_1, \ldots, x_n)D = (x_1u_1, \ldots, x_nu_n), \quad (x_1, \ldots, x_n) \in \widehat{R}^n.$$

Then $xF = xPD$ for $x \in \widehat{R}^n$.

Let $C_3 = C_1P \subset A^n \subset \widehat{R}^n$, and observe that $D$ is an $R$-linear isomorphism from $C_3$ to $C_2$ that preserves Hamming weight. We examine the individual components of the diagonal transformation $D$.

For each coordinate $i = 1, 2, \ldots, n$, project $C_3, C_2$ to codes $C_3^{(i)}, C_2^{(i)} \subset A \subset \widehat{R}$. Observe that $xD^{(i)} := xu_i$, $x \in \widehat{R}$, is an $R$-linear isomorphism taking $C_3^{(i)}$ to $C_2^{(i)}$ that preserves Hamming weight. By the hypothesis that the alphabet $A$ is pseudo-injective, Proposition 5.1 implies that $D^{(i)} : C_3^{(i)} \to C_2^{(i)}$ extends to an automorphism $\tau_i \in \mathrm{Aut}(A)$. Using these automorphisms, we build a monomial transformation $F'$ of $A^n$:

$$(x_1, \ldots, x_n)F' = (x_{\sigma(1)}\tau_1, \ldots, x_{\sigma(n)}\tau_n), \quad (x_1, \ldots, x_n) \in A^n,$$

that maps $C_1$ to $C_2$, as desired. □

### 5.4. *Sufficient conditions: the case of rings*

In this subsection we address the case where the alphabet $A$ is the ground ring $R$ itself.

A ring $R$ is a *quasi-Frobenius ring* (Ref. 31, Theorem 15.1) if $R$ is noetherian and self-injective (i.e., injective as a module over itself). A ring $R$ is a *Frobenius ring* (Ref. 31, Theorem 16.14) if

$$\operatorname{soc}({}_R R) \cong {}_R(R/\operatorname{rad}(R)) \quad \text{and} \quad \operatorname{soc}(R_R) \cong (R/\operatorname{rad}(R))_R.$$

In fact, for finite rings, either one of these isomorphisms suffices, by a result of Honold, Ref. 27, Theorem 2.

Another characterization of finite Frobenius rings follows.

**Theorem 5.3 (Ref. 53, Theorem 3.10).** *A finite ring $R$ is Frobenius if and only if ${}_R R_R$ is a Frobenius bimodule. In fact, ${}_R\widehat{R} \cong {}_R R$ if and only if $\widehat{R}_R \cong R_R$.*

The next theorem is now a direct corollary of Theorem 5.1.

**Theorem 5.4 (Ref. 53, Theorem 6.3).** *If $R$ is a finite Frobenius ring, then the alphabet $A = R$ has the extension property with respect to Hamming weight.*

**Remark 5.1.** Theorem 5.4 also follows from Theorem 5.2. For any finite ring $R$, the character module $\widehat{R}$ is injective, hence pseudo-injective. Because ${}_R R \cong {}_R\widehat{R}$, we see that a Frobenius ring is (pseudo-) injective as a left $R$-module. By definition, a Frobenius ring satisfies $\operatorname{soc}({}_R R) \cong {}_R(R/\operatorname{rad}(R))$, so $\operatorname{soc}({}_R R)$ is cyclic, and Theorem 5.2 applies.

### 5.5. *Semi-linear transformations*

The statement of the extension theorem by MacWilliams in Ref. 36 allowed for semi-linear transformations as well as linear ones. In this subsection we will address the semi-linear version of the extension theorem for ring alphabets with respect to Hamming weight. I thank Cary Huffman for bringing this situation to my attention (on November 13, 1994).

Let $R$ and $S$ be finite rings with 1. Assume that $R$ is a subring of $S$, and that the 1 of $R$ is also the 1 of $S$. Denote by $\operatorname{Aut}(S/R)$ the automorphism group of $S$ over $R$:

$$\operatorname{Aut}(S/R) = \{\text{ring automorphisms } \gamma : S \to S : \gamma(r) = r, r \in R\}.$$

Then $\operatorname{Aut}(S/R)$ generalizes the Galois group for field extensions.

Suppose $M_1, M_2, M_3$ are left $S$-modules (hence also left $R$-modules). Then $f : M_1 \to M_2$ is *semi-linear* if $f$ is a homomorphism of abelian groups and there exists $\gamma \in \mathrm{Aut}(S/R)$ such that $(sx)f = \gamma(s)(xf)$, for all $s \in S$, $x \in M_1$. (We still write inputs of $f$ on the left.) Observe that $f$ is linear as a map of $R$-modules. If $f_1 : M_1 \to M_2$ is semi-linear (via $\gamma_1 \in \mathrm{Aut}(S/R)$) and $f_2 : M_2 \to M_3$ is semi-linear (via $\gamma_2$), then the composite $f_1 \circ f_2 : M_1 \to M_3$ is also semi-linear (via $\gamma_2\gamma_1$).

There is also a semi-linear version of monomial transformations over $S^n$. Given an automorphism $\gamma \in \mathrm{Aut}(S/R)$, a *$\gamma$-monomial transformation* of $S^n$ has the form (cf. Eq. (7) of Subsection 5.1)

$$(a_1, \ldots, a_n)T = (\gamma(a_{\sigma(1)})u_1, \ldots, \gamma(a_{\sigma(n)})u_n), \quad (a_1, \ldots, a_n) \in S^n,$$

for some permutation $\sigma$ of $\{1, 2, \ldots, n\}$ and units $u_1, \ldots, u_n$ of $S$. The reader will verify that a $\gamma$-monomial transformation is semi-linear, using $\gamma$ as the automorphism, and that a $\gamma$-monomial transformation preserves Hamming weight on $S^n$.

**Theorem 5.5 (†).** *Let $S$ be a finite Frobenius ring with subring $R$. Then the ring alphabet $A = S$ has the extension property for Hamming weight in the context of semi-linear maps of $S$-modules. That is: suppose $C_1, C_2 \subset S^n$ are left $S$-submodules of $S^n$, and suppose $f : C_1 \to C_2$ is a semi-linear isomorphism (via $\gamma \in \mathrm{Aut}(S/R)$) that preserves Hamming weight, then $f$ extends to a $\gamma$-monomial transformation of $S^n$.*

**Proof.** Because the alphabet $A$ is the ring $S$ itself, any automorphism $\gamma \in \mathrm{Aut}(S/R)$ defines a $\gamma$-monomial transformation $T_\gamma$ of $S^n$:

$$(a_1, \ldots, a_n)T_\gamma = (\gamma(a_1), \ldots, \gamma(a_n)), \quad (a_1, \ldots, a_n) \in S^n.$$

As in the statement of the theorem, we assume $f : C_1 \to C_2$ is a semi-linear isomorphism (with associated automorphism $\gamma$) that preserves Hamming weight. Consider the $\gamma^{-1}$-monomial transformation $T_{\gamma^{-1}}$ of $S^n$, and set $C_3 = (C_2)T_{\gamma^{-1}} \subset S^n$. Let $g : C_1 \to C_3$ be the composite $g = f \circ T_{\gamma^{-1}}$. Being the composite of two semi-linear isomorphisms that preserve Hamming weight, $g$ is also a semi-linear isomorphism that preserves Hamming weight. The automorphism associated to the semi-linear isomorphism $g$ is $\gamma\gamma^{-1}$, which equals the identity. Thus $g : C_1 \to C_3$ is a linear isomorphism of $S$-modules that preserves Hamming weight.

By Theorem 5.4, $g$ extends to a (linear) monomial transformation $T$ of $S^n$. But then $f = g \circ T_\gamma$ extends to $T \circ T_\gamma$, which is a $\gamma$-monomial transformation, as desired. □

## 6. Necessary conditions for the extension theorem

The goal of this section is to prove converses for Theorems 5.4 and 5.2.

### 6.1. *Statement of results*

Here are the statements of the results.

**Theorem 6.1 (Ref. 57, Theorem 2.3).** *Let $R$ be a finite ring. If the alphabet $A = R$ has the extension property with respect to Hamming weight, then $R$ is a Frobenius ring.*

**Theorem 6.2 (†, Ref. 57, Theorem 5.2, in part).** *If the alphabet $A$ has the extension property with respect to Hamming weight, then:*

*(1) $A$ is pseudo-injective, and*
*(2)* $\mathrm{soc}(A)$ *is cyclic.*

The key technical result from which Theorems 6.1 and 6.2 will follow is:

**Theorem 6.3 (Ref. 57, Theorem 4.1).** *Let $R = M_m(\mathbb{F}_q)$ be the ring of all $m \times m$ matrices over a finite field $\mathbb{F}_q$, and let $A = M_{m,k}(\mathbb{F}_q)$ be the left $R$-module of all $m \times k$ matrices over $\mathbb{F}_q$.*

*If $k > m$, then the alphabet $A$ does not have the extension property with respect to Hamming weight.*

*Specifically, if $k > m$, there exist linear codes $C_+, C_- \subset A^N$, $N = \prod_{i=1}^{k-1}(1 + q^i)$, and an $R$-linear isomorphism $f : C_+ \to C_-$ that preserves Hamming weight, yet there is no monomial transformation extending $f$ because the code $C_+$ has an identically zero component while the code $C_-$ does not.*

The proof of Theorem 6.3 will appear in Subsection 6.2 below. The proofs of Theorems 6.1 and 6.2 follow a strategy of Dinh and López-Permouth[16] and will appear in Subsection 6.3. The motivation for the form of Theorem 6.3 will appear in Subsection 7.7.

### 6.2. *Proof of Theorem 6.3*

The proof of Theorem 6.3 presented below makes use of the Möbius function of the poset $\mathcal{L}(V)$ of all linear subspaces of a finite-dimensional vector space $V$ over $\mathbb{F}_q$ (Example 4.4). While this proof has the same structure as the original proof in Ref. 57, Theorem 4.1, the proof of Claim 1 is different and more streamlined.

**(†) Proof of Theorem 6.3, following Ref. 57, Theorem 4.1, in part.** We will construct two linear codes $C_+$ and $C_-$ in $A^N$, $N = \prod_{i=1}^{k-1}(1+q^i)$. The codes will be constructed as the images of two $R$-linear homomorphisms $g_+, g_- : A \to A^N$.

We begin by describing two vectors $v_+, v_-$ in $M_k(\mathbb{F}_q)^N$, i.e., $v_\pm$ will be $N$-tuples of $k \times k$ matrices over $\mathbb{F}_q$. The order of the entries in $v_\pm$ will be irrelevant. The entries of $v_+$ consist of all column reduced echelon matrices $\lambda$ of size $k \times k$ over $\mathbb{F}_q$ of even rank, with the multiplicity of the column reduced echelon matrix $\lambda$ being $q^{\binom{r}{2}}$, where $r = \mathrm{rk}(\lambda)$, the rank of the matrix $\lambda$. In particular, the zero matrix $\lambda = 0$ occurs in $v_+$ with multiplicity one, as $\binom{0}{2} = 0$. The length $L_+$ of $v_+$ is given by

$$L_+ = \sum_{\substack{r=0 \\ r \text{ even}}}^{k} q^{\binom{r}{2}} \begin{bmatrix} k \\ r \end{bmatrix}_q .$$

Similarly, the entries of $v_-$ consist of all column reduced echelon matrices $\lambda$ of odd rank, also with multiplicity $q^{\binom{r}{2}}$, $r = \mathrm{rk}(\lambda)$. (Note that $\binom{1}{2} = 0$.) The length $L_-$ of $v_-$ is given by

$$L_- = \sum_{\substack{r=1 \\ r \text{ odd}}}^{k} q^{\binom{r}{2}} \begin{bmatrix} k \\ r \end{bmatrix}_q .$$

Two applications of Lemma 4.2 with $x = \pm 1$ yield

$$L_+ + L_- = \prod_{i=0}^{k-1}(1+q^i) \quad \text{and} \quad L_+ - L_- = 0.$$

Since the $i = 0$ term in the product above equals 2, we see that

$$L_+ = L_- = \prod_{i=1}^{k-1}(1+q^i) =: N,$$

so that $v_\pm$ have the same length $N$.

Define the $R$-linear homomorphisms $g_\pm : A \to A^N$ by $Xg_\pm = Xv_\pm$, $X \in A$, where $Xv_\pm$ denotes entry-wise matrix multiplication. Define two linear codes $C_\pm \subset A^N$ by $C_\pm = Ag_\pm$.

Claim 1: the Hamming weights of $Xg_\pm$ are equal; i.e., $\mathrm{wt}(Xg_+) = \mathrm{wt}(Xg_-)$, for all $X \in A$.

To show this, we consider $\Delta(X) = \mathrm{wt}(Xg_+) - \mathrm{wt}(Xg_-)$. Then

$$\Delta(X) = \sum_{\substack{r=0 \\ r \text{ even}}}^{k} q^{\binom{r}{2}} \sum_{\substack{\lambda \text{ CRE} \\ \text{rank } r}} \delta(X\lambda) - \sum_{\substack{r=1 \\ r \text{ odd}}}^{k} q^{\binom{r}{2}} \sum_{\substack{\lambda \text{ CRE} \\ \text{rank } r}} \delta(X\lambda),$$

where $\delta(Y) = 1$ if $Y$ is nonzero, and $\delta(Y) = 0$ if $Y = 0$. In the inner summations, $\lambda$ varies over all column reduced echelon (CRE, for short) matrices of size $k \times k$ over $\mathbb{F}_q$ of rank $r$. Thus

$$\Delta(X) = \sum_{r=0}^{k} (-1)^r q^{\binom{r}{2}} \sum_{\substack{\lambda \text{ CRE} \\ \text{rank } r}} \delta(X\lambda).$$

We will view the matrices $X \in A = M_{m,k}(\mathbb{F}_q)$ and $\lambda \in M_k(\mathbb{F}_q)$ as linear transformations of vector spaces over $\mathbb{F}_q$, with inputs written on the right. Thus $\lambda : \mathbb{F}_q^k \to \mathbb{F}_q^k$ and $X : \mathbb{F}_q^k \to \mathbb{F}_q^m$. The column reduced echelon class of $\lambda$ is determined completely by $\operatorname{im}\lambda \subset \mathbb{F}_q^k$; i.e., $\lambda$ is column equivalent to $\nu$ if and only if $\operatorname{im}\lambda = \operatorname{im}\nu$. Thus, varying $\lambda$ over all column reduced echelon classes is the same as varying $\operatorname{im}\lambda$ over all subspaces of $\mathbb{F}_q^k$. Note that $\delta(X\lambda) = 0$ if and only if $X\lambda = 0$ if and only if $\operatorname{im}\lambda \subset \ker X$.

To show $\Delta(X) = 0$, we make use of the Möbius function on $\mathcal{L}(\mathbb{F}_q^k)$ (Example 4.4) and Proposition 4.1. In the sums below, $r = \operatorname{rk}(\lambda)$.

$$\begin{aligned}
\Delta(X) &= \sum_{\lambda \text{ CRE}} (-1)^r q^{\binom{r}{2}} \delta(X\lambda) \\
&= \sum_{\substack{\lambda \text{ CRE} \\ \operatorname{im}\lambda \subset \ker X}} (-1)^r q^{\binom{r}{2}} \delta(X\lambda) + \sum_{\substack{\lambda \text{ CRE} \\ \operatorname{im}\lambda \not\subset \ker X}} (-1)^r q^{\binom{r}{2}} \delta(X\lambda) \\
&= \sum_{\substack{\lambda \text{ CRE} \\ \operatorname{im}\lambda \not\subset \ker X}} (-1)^r q^{\binom{r}{2}} \\
&= \sum_{\lambda \text{ CRE}} (-1)^r q^{\binom{r}{2}} - \sum_{\substack{\lambda \text{ CRE} \\ \operatorname{im}\lambda \subset \ker X}} (-1)^r q^{\binom{r}{2}} \\
&= \sum_{\operatorname{im}\lambda \in \mathcal{L}(\mathbb{F}_q^k)} \mu(0, \operatorname{im}\lambda) - \sum_{\operatorname{im}\lambda \in \mathcal{L}(\ker(X))} \mu(0, \operatorname{im}\lambda) \\
&= 0 - 0 = 0.
\end{aligned}$$

The last line twice uses Eq. (6) of Subsection 4.1. In particular, notice that the hypothesis $k > m$ implies $\dim \ker X \geq 1$. This guarantees that the summation of $\mu(0, \operatorname{im}\lambda)$ over $\operatorname{im}\lambda \in \mathcal{L}(\ker X)$ vanishes, by Eq. (6) of Subsection 4.1. (If $\ker X = 0$, then the sum consists of only one term, $\mu(0,0) = 1$, and $\Delta(X) \neq 0$. This situation occurs when $k \leq m$, and Claim 1 does not hold when $k \leq m$.)

Claim 2: the mapping $f : C_+ \to C_-$ defined by $g_- = g_+ \circ f$ is a well-defined $R$-linear isomorphism that preserves Hamming weight.

Note that the common value

$$\mathrm{wt}(Xg_+) = \mathrm{wt}(Xg_-) = \sum_{\substack{r=1 \\ r \text{ odd}}}^{k} q^{\binom{r}{2}} \sum_{\substack{\lambda \text{ CRE} \\ \text{rank } r}} \delta(X\lambda)$$

is the sum of nonnegative terms. Also, if $X \neq 0$, then not all of the terms $\delta(X\lambda)$ vanish when $\mathrm{rk}(\lambda) = 1$. Thus, for $X \neq 0$, the common value $\mathrm{wt}(Xg_+) = \mathrm{wt}(Xg_-)$ is positive. In particular, for $X \neq 0$, $Xg_+$ and $Xg_-$ are nonzero. Thus, $g_+, g_- : A \to A^N$ are injective $R$-linear homomorphisms. By defining $f : C_+ \to C_-$ via $g_- = g_+ \circ f$, the claim is now apparent.

Claim 3: the mapping $f : C_+ \to C_-$ does not extend to a monomial transformation.

Because the vector $v_+$ contains a zero matrix in one component, that component of $Xg_+$ vanishes for every $X \in A$. On the other hand, no single fixed component of $Xg_-$ vanishes for every $X \in A$. Since monomial transformations preserve identically zero components, the map $f : C_+ \to C_-$ cannot extend to a monomial transformation. □

### 6.3. *The strategy of Dinh and López-Permouth and proofs of necessary conditions*

In this subsection, we prove Theorems 6.1 and 6.2 by following the strategy of Dinh and López-Permouth, Ref. 16, Theorem 6.

The objective of Dinh and López-Permouth in Ref. 16, Theorem 6, "is to provide a strategy" for reducing the proof of Theorem 6.1 to a non-extension problem for linear codes defined over certain matrix modules. Although originally stated for ring alphabets, their ideas, suitably modified, also work for module alphabets. In outline form, their strategy has three parts. (1) If a finite ring is not Frobenius, show that its socle contains a copy of a particular type of module defined over a matrix ring. (2) Show that counter-examples to the extension property exist in the context of linear codes defined over this particular matrix module. (3) Show that the counter-examples over the matrix module pull back to give counter-examples over the original ring. Points (1) and (3) were already carried out in Ref. 16, while point (2) is Theorem 6.3.

The following theorem shows how points (2) and (3) are used, assuming the conclusion of point (1). Recall some notation: the $T_i$ are the simple modules of $R$ given in Eq. (4) of Subsection 3.2; $\mu_i$ is the multiplicity of $T_i$ in $R/\operatorname{rad}(R)$, Eq. (4) of Subsection 3.2; and $s_i$ is the multiplicity of $T_i$ in $\operatorname{soc}(A)$, Eq. (12) of Subsection 5.3.

**Theorem 6.4 (Ref. 57, Theorem 5.2).** *Let $R$ be a finite ring, and assume that the alphabet $A$ has the property that, for some index $i$, the multiplicity $s_i$ of $T_i$ appearing in* $\mathrm{soc}(A)$ *is strictly greater than the multiplicity $\mu_i$ of $T_i$ appearing in $R/\operatorname{rad}(R)$. Then the alphabet $A$ does not have the extension property with respect to Hamming weight.*

**Proof.** By hypothesis, there is an index $i$ such that $s_i > \mu_i$. Of course, $s_i T_i \subset \mathrm{soc}(A) \subset A$. Recall that $T_i$ is the pullback to $R$ of the standard representation $M_{\mu_i,1}(\mathbb{F}_{q_i})$ of $M_{\mu_i}(\mathbb{F}_{q_i})$, so that $s_i T_i$ is the pullback to $R$ of the $M_{\mu_i}(\mathbb{F}_{q_i})$-module $B = M_{\mu_i,s_i}(\mathbb{F}_{q_i})$.

Because $s_i > \mu_i$, Theorem 6.3 implies the existence of linear codes $C_\pm \subset B^N$, with the property that there exists an linear isomorphism $f : C_+ \to C_-$ that preserves Hamming weight, yet $f$ does not extend to a monomial transformation of $B^N$. Note that the codes $C_\pm$ are $M_{\mu_i}(\mathbb{F}_{q_i})$-linear codes over the module $B = M_{\mu_i,s_i}(\mathbb{F}_{q_i})$. The projection mappings $R \to R/\operatorname{rad}(R) \to M_{\mu_i}(\mathbb{F}_{q_i})$ allow us to consider $C_\pm$ as $R$-modules. Since $B$ pulls back to $s_i T_i$, we have $C_\pm \subset (s_i T_i)^N \subset \mathrm{soc}(A)^N \subset A^N$, as $R$-modules. Thus $C_\pm$ are linear codes over $A$.

As in the proof of Theorem 6.3 (claim 3), the fact that $C_+$ has an identically zero component, while $C_-$ does not, implies that there is no monomial transformation of $A^N$ from $C_+$ to $C_-$. Thus, the extension property for Hamming weight over $A$ fails to hold. □

**Proof of Theorem 6.2.** If the alphabet $A$ has the extension property, then $A$ certainly has the extension property for codes of length 1. Since the latter is equivalent to $A$ being pseudo-injective by Proposition 5.1, it follows that $A$ is pseudo-injective.

For the condition on $\mathrm{soc}(A)$, we prove the contrapositive. If $\mathrm{soc}(A)$ is not cyclic, then, by Proposition 5.2, there is an index $i$ with $s_i > \mu_i$. By Theorem 6.4, the alphabet $A$ does not have the extension property. □

**Proof of Theorem 6.1.** By Theorem 6.2, $\mathrm{soc}(R)$ is cyclic. By Proposition 5.3, ${}_R R$ embeds into ${}_R\widehat{R}$. Because $|\widehat{R}| = |R|$, we have an isomorphism ${}_R R \cong {}_R\widehat{R}$. By Theorem 5.3, $R$ is a Frobenius ring.

Alternatively, if $R$ is not Frobenius, one can show that there exists an index $i$ and a value $k > \mu_i$ with $kT_i \subset \mathrm{soc}(R)$ (see the exposition following Ref. 16, Remark 4). Thus $s_i > \mu_i$, and Theorem 6.4 implies that $A = R$ does not have the extension property. □

**Example 6.1.** (Benson, Ref. 53, Example 1.4(ii).) Let $R$ be the ring con-

sisting of all $6 \times 6$ matrices over $\mathbb{F}_q$ of the form $a$ below. The ring $R$ is not Frobenius. As rings, $R/\operatorname{rad}(R) \cong M_2(\mathbb{F}_q) \oplus M_1(\mathbb{F}_q)$.

$$a = \begin{pmatrix} a_1 & 0 & a_2 & 0 & 0 & 0 \\ 0 & a_1 & 0 & a_2 & a_3 & 0 \\ a_4 & 0 & a_5 & 0 & 0 & 0 \\ 0 & a_4 & 0 & a_5 & a_6 & 0 \\ 0 & 0 & 0 & 0 & a_9 & 0 \\ a_7 & 0 & a_8 & 0 & 0 & a_9 \end{pmatrix}.$$

The set $A$ consisting of all matrices of form $a$ with $a_i = 0$ for $i \neq 7, 8$ is a left $R$-module that is isomorphic to the pull-back to $R$ of the $M_1(\mathbb{F}_q)$-module $M_{1,2}(\mathbb{F}_q)$.

Denote by $(x, y)$ the element of $A$ with $a_7 = x$ and $a_8 = y$ (and other $a_i = 0$). The linear code $C_+ \subset A^{1+q} \subset R^{1+q}$ consists of all vectors of length $1 + q$ of the form having one entry equal to $(0, 0)$ and $q$ entries equal to $(x, y)$. The linear code $C_- \subset A^{1+q} \subset R^{1+q}$ consists of all vectors of length $1 + q$ with entries of the form $(y, 0)$ and $(x + \alpha y, 0)$, with $\alpha$ varying over all $\alpha \in \mathbb{F}_q$. The reader is invited to verify that $C_\pm$ are counter-examples to the extension property.

## 7. Parameterized codes

The purpose of this section is to provide the theoretical foundations that lead to the counter-example in Theorem 6.3. The underlying ideas for ring alphabets go back in part to Ref. 56. These ideas are generalized here to apply to module alphabets as well.

Throughout this section, $R$ is a finite ring with 1 and $A = {}_RA$ is a finite left $R$-module, which will be the alphabet for $R$-linear codes. Fix a weight $w$ on $A$, i.e., a function $w : A \to \mathbb{Q}$ with $w(0) = 0$. As in Eq. (9) of Subsection 5.1, $G_r$ will denote the right symmetry group of $w$.

### 7.1. *Parameterized codes*

In many areas of mathematics one studies objects $X$ and their subobjects $Y \subset X$. Often one way to study the subobjects is to view them as images of morphisms $f : Z \to X$. In coding theory, a linear code is a submodule (subobject) of some ambient space $A^n$, while an encoder is a linear mapping (morphism) from a module of information symbols to the ambient space (whose image is the linear code). Put another way, in terms of generator matrices, the linear code is the row space of a generator matrix, while the

encoder is defined by the generator matrix itself. The parameterized codes defined below are a coordinate-free approach to generator matrices.

**Definition 7.1.** Given a finite left $R$-module $M = {}_RM$, a *parameterized code* of length $n$ is a pair $(M, \lambda)$, where $\lambda : M \to A^n$ is an $R$-linear homomorphism.

Every parameterized code $(M, \lambda)$ gives rise to a linear code $C = \operatorname{im}\lambda = M\lambda \subset A^n$. Of course, different parameterized codes may give rise to the same linear code. Because $\operatorname{Hom}_R(M, A^n) \cong \operatorname{Hom}_R(M, A)^n$, $\lambda \in \operatorname{Hom}_R(M, A^n)$ can be viewed as a list $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_n)$ of linear functionals $\lambda_1, \ldots, \lambda_n \in \operatorname{Hom}_R(M, A)$. These linear functionals are just the *coordinate functionals* of the linear code $C$.

**Example 7.1.** Suppose $R = A = \mathbb{F}_q$ and $M$ is a vector space over $\mathbb{F}_q$ of dimension $k$. If one fixes a basis for the vector space $M$, then any linear functional $\lambda : M \to \mathbb{F}_q$ is determined by its values on the basis of $M$. If one arranges the values of $\lambda_1, \ldots, \lambda_n$ on the basis of $M$ into a $k \times n$ matrix, the resulting matrix is a generator matrix for a $[n, k]$-linear code over $\mathbb{F}_q$.

For a fixed module $M$, let $\mathcal{C}_n(M)$ be the set of all parameterized codes $(M, \lambda)$ of length $n$. For convenience, we define $\mathcal{C}_0(M)$ to be the one-element set consisting of the "empty code" of length 0. One defines an operation of *concatenation* as follows:

$$\mathcal{C}_{n_1}(M) \times \mathcal{C}_{n_2}(M) \to \mathcal{C}_{n_1+n_2}(M),$$
$$((M, \lambda_1), (M, \lambda_2)) \mapsto (M, \lambda_1|\lambda_2).$$

(Here, $\lambda_1$ is a list of $n_1$ elements of $\operatorname{Hom}_R(M, A)$, and $\lambda_2$ is a list of $n_2$ elements of $\operatorname{Hom}_R(M, A)$. Then $\lambda_1|\lambda_2$ is the concatenation of those lists; it has length $n_1 + n_2$.) Set $\mathcal{C}(M) = \coprod_{n\geq 0} \mathcal{C}_n(M)$ equal to the disjoint union of the $\mathcal{C}_n(M)$.

**Example 7.2.** In the context of Example 7.1, concatenation of parameterized codes reduces to concatenation of generator matrices (all defined with respect to the same basis of $M$). A $k \times n_1$ matrix $P$ concatenated with a $k \times n_2$ matrix $Q$ yields a $k \times (n_1 + n_2)$ matrix $(P|Q)$.

**Proposition 7.1.** *The set $\mathcal{C}(M)$ is a monoid (associative semigroup with identity) under concatenation, whose identity is the empty code in $\mathcal{C}_0(M)$.*

**Proof.** Exercise. □

Because the $G_r$-monomial transformations of $A^n$ play an essential role in the extension property, we will now introduce group actions into our discussion of $\mathcal{C}_n(M)$. Let $\mathcal{G}_n$ be the group of $G_r$-monomial transformations of $A^n$. The group $\mathcal{G}_n$ is the semidirect product of the symmetric group $\Sigma_n$ with the product group $(G_r)^n$. The group $\mathcal{G}_n$ acts on $\mathcal{C}_n(M)$ on the right:

$$\mathcal{C}_n(M) \times \mathcal{G}_n \to \mathcal{C}_n(M), \quad (\lambda, T) \mapsto \lambda \circ T,$$

where $\lambda \circ T$ is just the composition of $\lambda : M \to A^n$ with $T : A^n \to A^n$ (viewing function inputs on the left). Let $\overline{\mathcal{C}}_n(M)$ be the orbit space under this group action: $\overline{\mathcal{C}}_n(M) = \mathcal{C}_n(M)/\mathcal{G}_n$. As above, set $\overline{\mathcal{C}}(M) = \coprod_{n \geq 0} \overline{\mathcal{C}}_n(M)$.

**Example 7.3.** In the context of Example 7.1, the action of $\mathcal{G}_n$ means that we allow the $k \times n$ generator matrices to be multiplied on the right by $n \times n$ monomial matrices (with non-zero entries from $G_r$).

**Proposition 7.2.** *Concatenation is a well-defined operation on $\overline{\mathcal{C}}(M)$, making it a commutative monoid.*

**Proof.** Exercise. □

The reader should be aware that a parameterized code $(M, \lambda)$ of length $n$ is different from that same code with a "zero column" added (which is the parameterized code $(M, \lambda|0)$ of length $n+1$). The first is an element of $\mathcal{C}_n(M)$; the second is in $\mathcal{C}_{n+1}(M)$. It will be convenient to identify two parameterized codes that differ in this way, and we turn to that topic next.

To be precise, let $(M, 0) \in \mathcal{C}_1(M)$ be the "zero code" of length 1; i.e., the linear functional $0 \in \mathrm{Hom}_R(M, A)$ is the zero functional, with $x0 = 0$ for all $x \in M$. By concatenating with the zero code, there are injections

$$\mathcal{C}_n(M) \hookrightarrow \mathcal{C}_{n+1}(M), \quad \lambda \mapsto \lambda|0,$$

that are well-defined on the orbit spaces

$$\overline{\mathcal{C}}_n(M) \hookrightarrow \overline{\mathcal{C}}_{n+1}(M).$$

Using these injections to make identifications, we form the identification space $\mathcal{E}(M)$. Two elements of $\overline{\mathcal{C}}(M)$ become identified in $\mathcal{E}(M)$ if they differ by concatenating with zero codes. Thus, elements of $\mathcal{E}(M)$ are represented by parameterized codes with no zero components, up to $G_r$-monomial transformations.

**Example 7.4.** In the context of Example 7.1, the identification space $\mathcal{E}(M)$ treats as equivalent two generator matrices that differ by addition or deletion of zero columns, up to monomial transformations.

**Proposition 7.3.** *Concatenation is also a well-defined operation on $\mathcal{E}(M)$, making it a commutative monoid.*

**Proof.** Exercise. □

**Remark 7.1.** The constructions of $\mathcal{C}(M)$, $\overline{\mathcal{C}}(M)$, and $\mathcal{E}(M)$ can be carried out in the language of category theory (see Ref. 34, III.3). Parameterized codes of length $n$ with alphabet $A$ define a functor $\mathcal{C}_n$ from the category of finite left $R$-modules to the category of sets, via $M \mapsto \mathrm{Hom}_R(M, A^n)$. Then $\mathcal{C}$ is the coproduct of those functors; $\mathcal{C}(M)$ carries the additional structure of a monoid.

Similarly, $\overline{\mathcal{C}}_n$ is a functor from finite $R$-modules to sets, and $\overline{\mathcal{C}}$ is the coproduct of those functors, while $\mathcal{E}$ is the colimit.

### 7.2. *Multiplicity functions*

In this subsection we see how to view parameterized codes in terms of multiplicity functions. The latter are another way to describe codes, similar to using modular representations,[40,41] multisets,[17] or projective systems.[49] Multiplicity functions also draw on the coordinate-free approach[2] to codes.

The abelian group $\mathrm{Hom}_R(M, A)$ of all $R$-linear homomorphisms from $M$ to $A$ admits a right action by the right symmetry group $G_r$ (by post-composition). Denote the orbit space $\mathrm{Hom}_R(M, A)/G_r$ of this action by $\mathcal{O}^\sharp$. If $\lambda \in \mathrm{Hom}_R(M, A)$, we denote its orbit by $\mathrm{orb}(\lambda) \in \mathcal{O}^\sharp$. Let $F(\mathcal{O}^\sharp, \mathbb{N})$ equal the set of functions from $\mathcal{O}^\sharp$ to the natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$. Point-wise addition of functions endows $F(\mathcal{O}^\sharp, \mathbb{N})$ with the structure of a commutative monoid. Define

$$F_0(\mathcal{O}^\sharp, \mathbb{N}) := \{\eta : \mathcal{O}^\sharp \to \mathbb{N} \mid \eta(\mathrm{orb}(0)) = 0\},$$

which is the submonoid of $F(\mathcal{O}^\sharp, \mathbb{N})$ consisting of those multiplicity functions $\eta$ that have multiplicity zero on the $G_r$-orbit of the zero homomorphism in $\mathcal{O}^\sharp$. (Elements of $F_0(\mathcal{O}^\sharp, \mathbb{N})$ will correspond to parameterized codes with no zero components.)

**Theorem 7.1.** *Given a finite left $R$-module $M$,*

*(1) $\overline{\mathcal{C}}(M)$ and $F(\mathcal{O}^\sharp, \mathbb{N})$ are isomorphic as monoids; and*
*(2) $\mathcal{E}(M)$ and $F_0(\mathcal{O}^\sharp, \mathbb{N})$ are isomorphic as monoids.*

**Proof.** Exercise. The multiplicity function counts the number of components of $\lambda : M \to A^n$ that belong to particular $G_r$-orbits. □

**Example 7.5.** In the context of Example 7.1, the multiplicity function counts how many columns of a generator matrix belong to a particular $G_r$-scale class of column vectors. The reader will recognize this as the multiset description of a linear code (up to monomial transformations); see Ref. 17, for example.

### 7.3. *The weight mapping*

In this subsection we describe the function that assigns to every element of a parameterized code its weight. Remember that $w$ is a weight on the alphabet $A$.

Given a parameterized code $(M, \lambda)$, where $\lambda : M \to A^n$, the weight of an element $x \in M$ is $w(x\lambda) = \sum w(x\lambda_i)$, where $\lambda_1, \ldots, \lambda_n$ are the components of $\lambda$. This definition extends to a well-defined map on $\overline{\mathcal{C}}(M)$ and $\mathcal{E}(M)$, because the action of the group $\mathcal{G}_n$ preserves $w$, and because zero components contribute zero to the weight. In terms of multiplicity functions in $F(\mathcal{O}^\sharp, \mathbb{N})$, we get a map of function spaces (with $F(M, \mathbb{Q})$ being the set of functions from $M$ to $\mathbb{Q}$):

$$W : F(\mathcal{O}^\sharp, \mathbb{N}) \to F(M, \mathbb{Q}),$$
$$\eta \mapsto [x \mapsto \sum_{\mathrm{orb}(\lambda) \in \mathcal{O}^\sharp} w(x\lambda)\eta(\lambda)]. \tag{13}$$

**Proposition 7.4.** *The mapping $W : F(\mathcal{O}^\sharp, \mathbb{N}) \to F(M, \mathbb{Q})$:*

*(1) is well-defined;*
*(2) is additive, i.e., $W(\eta_1 + \eta_2) = W(\eta_1) + W(\eta_2)$;*
*(3) satisfies $W(\eta)(0) = 0$, for any $\eta \in F(\mathcal{O}^\sharp, \mathbb{N})$;*
*(4) has image contained in the $G_l$-invariant functions from $M$ to $\mathbb{Q}$, i.e., $W(\eta)(ux) = W(\eta)(x)$ for all $x \in M$, $u \in G_l$.*

**Proof.** Exercise. Recall that the left-symmetry group $G_l$ is defined in Eq. (8) of Subsection 5.1. □

The left-symmetry group $G_l$ acts on $M$ on the left. Denote the orbit space of that action by $\mathcal{O}$. It is easy to see that the set of $G_l$-invariant functions $M \to \mathbb{Q}$ is the same as the set $F(\mathcal{O}, \mathbb{Q})$ of functions $\mathcal{O} \to \mathbb{Q}$; $F(\mathcal{O}, \mathbb{Q})$ is a $\mathbb{Q}$-vector space of dimension $|\mathcal{O}|$. Let $F_0(\mathcal{O}, \mathbb{Q}) \subset F(\mathcal{O}, \mathbb{Q})$ consist of those functions that equal zero on the orbit of the zero element of $M$; $F_0(\mathcal{O}, \mathbb{Q})$ is a vector subspace of $F(\mathcal{O}, \mathbb{Q})$, and $\dim F_0(\mathcal{O}, \mathbb{Q}) = |\mathcal{O}| - 1$. By Proposition 7.4, $W$ maps $F(\mathcal{O}^\sharp, \mathbb{N}) \to F_0(\mathcal{O}, \mathbb{Q})$.

We conclude this subsection by reformulating the extension property in terms of the mapping $W$ restricted to the submonoid $F_0(\mathcal{O}^\sharp, \mathbb{N})$.

**Theorem 7.2.** *For an alphabet $A$, if the mapping $W : F_0(\mathcal{O}^\sharp, \mathbb{N}) \to F_0(\mathcal{O}, \mathbb{Q})$ is injective for every finite $R$-module $M$, then the alphabet $A$ has the extension property with respect to the weight $w$.*

*Moreover, if the weight $w : A \to \mathbb{Q}$ has the property that $w(a) \neq 0$ for every nonzero $a \in A^n$ for any $n$, then the converse holds; i.e., if $A$ has the extension property with respect to the weight $w$, then $W$ is injective for any finite $R$-module $M$.*

**Proof.** Suppose the mapping $W$ is injective for every $M$, and suppose $C_1, C_2 \subset A^n$ are two $R$-linear codes with $f : C_1 \to C_2$ an $R$-linear isomorphism that preserves $w$.

Let $M$ be the $R$-module underlying the linear code $C_1$, and define two parameterized codes by taking $\lambda_1$ to be the inclusion map $C_1 \subset A^n$ and $\lambda_2 = f$. Then $(M, \lambda_1)$ and $(M, \lambda_2)$ are two parameterized codes; their images are $C_1$ and $C_2$, respectively. Let $\eta_1$ and $\eta_2$ be the multiplicity functions associated with $(M, \lambda_1)$ and $(M, \lambda_2)$, respectively. Because $f : C_1 \to C_2$ preserves $w$, it follows that $W(\eta_1) = W(\eta_2)$. Because $W$ is injective, we conclude that $\eta_1 = \eta_2$ as elements of $F_0(\mathcal{O}^\sharp, \mathbb{N})$, which means that there is a $G_r$-monomial transformation $T$ with $\lambda_2 = \lambda_1 \circ T$, as desired.

For the converse, assume that $A$ has the extension property and $w$ has the property that $w(a) \neq 0$ for any nonzero $a \in A^n$. Let $M$ be a finite left $R$-module, and suppose that $\eta_1, \eta_2 \in F_0(\mathcal{O}^\sharp, \mathbb{N})$ satisfy $W(\eta_1) = W(\eta_2)$. The multiplicity functions correspond to parameterized codes $(M, \lambda_1)$ and $(M, \lambda_2)$, respectively. The tricky aspect of the converse is that the homomorphisms $\lambda_1$ and $\lambda_2$ may have kernels.

By the assumed property on $w$, it follows that $w(x\lambda_1) = 0$ if and only if $x\lambda_1 = 0$, $x \in M$, and similarly for $\lambda_2$. Because $W(\eta_1) = W(\eta_2)$, we have that $w(x\lambda_1) = w(x\lambda_2)$ for all $x \in M$. We conclude that $\ker \lambda_1 = \ker \lambda_2$. By passing to the quotient by the common kernel if necessary, we may assume that $\lambda_1$ and $\lambda_2$ are both injective maps.

Let $C_1 = M\lambda_1$ and $C_2 = M\lambda_2$; $C_1$ and $C_2$ are linear codes. Let $f : C_1 \to C_2$ be $\lambda_1^{-1} \circ \lambda_2$. Because $\lambda_1$ and $\lambda_2$ are injective, $f$ is an isomorphism. Because $w(x\lambda_1) = w(x\lambda_2)$ for all $x \in M$, $f$ preserves $w$. By the extension property, there is a $G_r$-monomial transformation taking $C_1$ to $C_2$. But this implies that $\eta_1 = \eta_2$ as elements of $F_0(\mathcal{O}^\sharp, \mathbb{N})$, as desired. □

### 7.4. *Completion over $\mathbb{Q}$: virtual codes*

In this subsection, we formally complete the function space $F_0(\mathcal{O}^\sharp, \mathbb{N})$ to $F_0(\mathcal{O}^\sharp, \mathbb{Q})$.

The mapping $W : F_0(\mathcal{O}^\sharp, \mathbb{N}) \to F_0(\mathcal{O}, \mathbb{Q})$ is an additive map of monoids. We have $F_0(\mathcal{O}^\sharp, \mathbb{N}) \subset F_0(\mathcal{O}^\sharp, \mathbb{Z}) \subset F_0(\mathcal{O}^\sharp, \mathbb{Q})$. Because $F_0(\mathcal{O}^\sharp, \mathbb{Q})$ is a finite-dimensional $\mathbb{Q}$-vector space (of dimension $|\mathcal{O}^\sharp| - 1$), completing $F_0(\mathcal{O}^\sharp, \mathbb{N})$ to $F_0(\mathcal{O}^\sharp, \mathbb{Q})$ will allow us to use the tools of linear algebra in what follows. Elements of $F_0(\mathcal{O}^\sharp, \mathbb{Q})$ will be called *virtual codes*, as in Ref. 56, Section 4.

**Proposition 7.5.** *For any alphabet $A$ and finite $R$-module $M$,*

*(1) the mapping $W : F_0(\mathcal{O}^\sharp, \mathbb{N}) \to F_0(\mathcal{O}, \mathbb{Q})$ extends to a linear transformation $W : F_0(\mathcal{O}^\sharp, \mathbb{Q}) \to F_0(\mathcal{O}, \mathbb{Q})$ of finite-dimensional $\mathbb{Q}$-vector spaces; and*

*(2) the mapping $W : F_0(\mathcal{O}^\sharp, \mathbb{N}) \to F_0(\mathcal{O}, \mathbb{Q})$ is injective if and only if the linear transformation $W : F_0(\mathcal{O}^\sharp, \mathbb{Q}) \to F_0(\mathcal{O}, \mathbb{Q})$ is injective.*

*(3) Theorem 7.2 holds with $W : F_0(\mathcal{O}^\sharp, \mathbb{Q}) \to F_0(\mathcal{O}, \mathbb{Q})$ replacing $W : F_0(\mathcal{O}^\sharp, \mathbb{N}) \to F_0(\mathcal{O}, \mathbb{Q})$.*

**Proof.** In order to prove that $W : F_0(\mathcal{O}^\sharp, \mathbb{Q}) \to F_0(\mathcal{O}, \mathbb{Q})$ is injective, under the assumption that $W : F_0(\mathcal{O}^\sharp, \mathbb{N}) \to F_0(\mathcal{O}, \mathbb{Q})$ is injective, consider $\eta \in F_0(\mathcal{O}^\sharp, \mathbb{Q})$ with $W(\eta) = 0$. Choose a sufficiently large positive integer $K$ to clear the denominators in the values of $\eta$, i.e., $K\eta \in F_0(\mathcal{O}^\sharp, \mathbb{Z})$. Now split out the positive and negative values of $K\eta$, writing $K\eta = \eta_+ - \eta_-$, with both $\eta_+, \eta_- \in F_0(\mathcal{O}^\sharp, \mathbb{N})$. Because $W(\eta) = 0$, it follows that $W(\eta_+) = W(\eta_-)$. Because $W : F_0(\mathcal{O}^\sharp, \mathbb{N}) \to F_0(\mathcal{O}, \mathbb{Q})$ is injective, we conclude that $\eta_+ = \eta_-$, so that $K\eta = 0$, hence $\eta = 0$.

We leave the rest of the proof as an exercise. □

### 7.5. *Matrix representation for W*

The vector spaces $F_0(\mathcal{O}^\sharp, \mathbb{Q})$ and $F_0(\mathcal{O}, \mathbb{Q})$ have natural bases. For any nonzero orbit $\lambda \in \mathcal{O}^\sharp$, define $\delta_\lambda \in F_0(\mathcal{O}^\sharp, \mathbb{Q})$ by

$$\delta_\lambda(\nu) = \begin{cases} 1, & \nu = \lambda, \\ 0, & \nu \neq \lambda. \end{cases}$$

Similarly, for any nonzero orbit $x \in \mathcal{O}$, define $\delta_x \in F_0(\mathcal{O}, \mathbb{Q})$ by

$$\delta_x(y) = \begin{cases} 1, & y = x, \\ 0, & y \neq x. \end{cases}$$

In terms of these bases, the linear transformation $W : F_0(\mathcal{O}^\sharp, \mathbb{Q}) \to F_0(\mathcal{O}, \mathbb{Q})$ is represented by a matrix, also called $W$. We use Eq. (13) of Subsection 7.3 as our guide. Any $\eta \in F_0(\mathcal{O}^\sharp, \mathbb{Q})$ is expressed in terms of the $\delta_\lambda$-basis as

$$\eta = \sum_{\lambda \in \mathcal{O}^\sharp} \eta(\lambda)\delta_\lambda.$$

Similarly, any $h \in F_0(\mathcal{O}, \mathbb{Q})$ is expressed as

$$h = \sum_{x \in \mathcal{O}} h(x)\delta_x.$$

View the coefficients $\eta(\lambda)$ as a column vector indexed by the nonzero elements of $\mathcal{O}^\sharp$, and view the coefficients $h(x)$ as a column vector indexed by the nonzero elements of $\mathcal{O}$. The matrix $W$ representing the mapping $W$ will have size $(|\mathcal{O}| - 1) \times (|\mathcal{O}^\sharp| - 1)$, with rows indexed by the nonzero elements of $\mathcal{O}$ and columns indexed by the nonzero elements of $\mathcal{O}^\sharp$. The entry of the matrix $W$ in row $x$ ($x \in \mathcal{O}$) and column $\lambda$ ($\lambda \in \mathcal{O}^\sharp$) is

$$W_{x,\lambda} = w(x\lambda), \tag{14}$$

i.e., the weight $w(x\lambda)$ of the element $x\lambda \in A$ obtained by evaluating $\lambda$ at $x$. This is well-defined, by the definitions of the symmetry groups. That the matrix $W$ represents the mapping $W$ is exactly the content of Eq. (13) of Subsection 7.3.

### 7.6. *Field case*

In this subsection we examine in detail the mapping $W : F_0(\mathcal{O}^\sharp, \mathbb{Q}) \to F_0(\mathcal{O}, \mathbb{Q})$ when $R = A$ is a finite field.

Let $R = \mathbb{F}_q$ be a finite field of order $q$. Let the alphabet $A = R$ be the field itself, and let $w$ be the Hamming weight wt. Because $\mathbb{F}_q$ is commutative, the left and right symmetry groups are equal, namely $G = \mathbb{F}_q^\times$, the multiplicative group of the field $\mathbb{F}_q$.

Let $M$ be a finite $R$-module; i.e., $M$ is a finite dimensional vector space over $\mathbb{F}_q$. Let $\dim M = k$. The nonzero elements of the orbit space $\mathcal{O} = M/G = M/\mathbb{F}_q^\times$ form the projective space associated to the vector space $M$ (the set of one-dimensional subspaces of $M$). Similarly, the nonzero elements of the orbit space $\mathcal{O}^\sharp = \mathrm{Hom}_{\mathbb{F}_q}(M, \mathbb{F}_q)/\mathbb{F}_q^\times$ form the projective space associated with the dual vector space $\mathrm{Hom}_{\mathbb{F}_q}(M, \mathbb{F}_q)$. Notice that the numbers of nonzero elements in $\mathcal{O}$ and $\mathcal{O}^\sharp$ are the same, namely, $(q^k - 1)/(q - 1)$. Thus the $\mathbb{Q}$-vector spaces $F_0(\mathcal{O}^\sharp, \mathbb{Q})$ and $F_0(\mathcal{O}, \mathbb{Q})$ both have dimension $(q^k - 1)/(q - 1)$.

The matrix $W$ of Eq. (14) of Subsection 7.5 is just the all-one matrix minus the incidence pairing between the two projective spaces. This matrix is known to be invertible, so this provides another proof of the extension property for linear codes over finite fields with respect to Hamming weight. In fact, this is exactly the approach used by MacWilliams in her dissertation,[36] by Bogart, et al.,[7] and by Greferath.[20]

### 7.7. *Matrix module case*

In this subsection we provide the background behind Theorem 6.3.

Let $R = M_m(\mathbb{F}_q)$ be the ring of all $m \times m$ matrices over a finite field $\mathbb{F}_q$, and let the alphabet $A = M_{m,k}(\mathbb{F}_q)$ be the left $R$-module of all $m \times k$ matrices over $\mathbb{F}_q$. Let $w$ be the Hamming weight wt on $A$. Then the symmetry groups are $G_l = \mathcal{U}(R) = GL(m, \mathbb{F}_q)$ and $G_r = \mathrm{Aut}(_RA) = GL(k, \mathbb{F}_q)$.

Let $M$ be any finite left $R$-module. Because $R = M_m(\mathbb{F}_q)$ is a simple ring, $M \cong M_{m,l}(\mathbb{F}_q)$ for some $l$. It follows that $\mathrm{Hom}_R(M, A) \cong M_{l,k}(\mathbb{F}_q)$, acting by right matrix multiplication on elements of $M$.

The elements of the orbit space $\mathcal{O} = G_l \backslash M = GL(m, \mathbb{F}_q) \backslash M_{m,l}(\mathbb{F}_q)$ are repesented uniquely by the row reduced echelon matrices of size $m \times l$. Similarly, the elements of the orbit space $\mathcal{O}^\sharp = \mathrm{Hom}_R(M, A)/G_r = M_{l,k}(\mathbb{F}_q)/GL(k, \mathbb{F}_q)$ are uniquely represented by the column reduced echelon matrices of size $l \times k$.

Because the matrix transpose interchanges row reduced echelon matrices and column reduced echelon matrices, we see that

- $|\mathcal{O}|$ equals the number of row reduced echelon matrices of size $m \times l$, while
- $|\mathcal{O}^\sharp|$ equals the number of row reduced echelon matrices of size $k \times l$.

If $k > m$, then $|\mathcal{O}^\sharp| > |\mathcal{O}|$.

Remember that $W : F_0(\mathcal{O}^\sharp, \mathbb{Q}) \to F_0(\mathcal{O}, \mathbb{Q})$ is a linear transformation of $\mathbb{Q}$-vector spaces, Also remember that $\dim F_0(\mathcal{O}, \mathbb{Q}) = |\mathcal{O}| - 1$, while $\dim F_0(\mathcal{O}^\sharp, \mathbb{Q}) = |\mathcal{O}^\sharp| - 1$. If $k > m$, then $\dim F_0(\mathcal{O}^\sharp, \mathbb{Q}) > \dim F_0(\mathcal{O}, \mathbb{Q})$, so that $\ker W \neq 0$, and $W$ cannot be injective.

When $k = m + 1$, $\dim F_0(\mathcal{O}^\sharp, \mathbb{Q}) = 1 + \dim F_0(\mathcal{O}, \mathbb{Q})$, so $\dim \ker W \geq 1$. The exact form of an element of $\ker W$ (as in Theorem 6.3) was discovered by doing several computer-assisted computations for small values of $q, m, k$ and guessing the pattern. Once the pattern was guessed, the proof of Theorem 6.3 verified the correctness of the guess.

## 8. Symmetrized weight compositions

In this section, we discuss the extension property for symmetrized weight compositions, following the ideas in Ref. 52. Once again, ideas originally developed for ring alphabets have been generalized to module alphabets.

### 8.1. *Definitions*

Let $R$ be a finite ring with 1, and let $A$ be a finite left $R$-module which will serve as the alphabet for $R$-linear codes. Fix a subgroup $G_r \subset \mathrm{Aut}(A)$ of the automorphism group of $A$.

The subgroup $G_r \subset \mathrm{Aut}(A)$ defines an equivalence relation $\sim$ on $A$, via the right group action of $G_r$ on $A$: $a \sim a'$ if $a = a'\tau$, for some $\tau \in G_r$. Denote the orbit space of this group action by $A/G_r$.

**Definition 8.1.** The *symmetrized weight composition* defined by the subgroup $G_r \subset \mathrm{Aut}(A)$ is a function $\mathrm{swc} : A^n \times A/G_r \to \mathbb{N}$ defined by

$$\mathrm{swc}_a(x) = |\{i : x_i \sim a\}|, \quad x = (x_1, \ldots, x_n) \in A^n, \quad a \in A/G_r.$$

Recall that a $G_r$-monomial transformation $T$ of $A^n$ has the form

$$(x_1, \ldots, x_n)T = (x_{\sigma(1)}\tau_1, \ldots, x_{\sigma(n)}\tau_n), \quad (x_1, \ldots, x_n) \in A^n,$$

for some permutation $\sigma$ of $\{1, 2, \ldots, n\}$ and automorphisms $\tau_1, \ldots, \tau_n \in G_r$; see Eq. (7) of Subsection 5.1. Observe that a $G_r$-monomial transformation $T$ of $A^n$ preserves swc; i.e., $\mathrm{swc}_a(xT) = \mathrm{swc}_a(x)$, for all $a \in A/G_r$ and $x \in A^n$.

**Definition 8.2.** The alphabet $A$ has the *extension property* with respect to swc if the following condition holds: for any two $R$-linear codes $C_1, C_2 \subset A^n$, if $f : C_1 \to C_2$ is an $R$-linear isomorphism that preserves swc, then $f$ extends to a $G_r$-monomial transformation of $A^n$.

### 8.2. *Averaged characters*

In this subsection, we adapt the results on averaged characters of Ref. 52, Section 4, to the context of a module alphabet.

The right action of $G_r \subset \mathrm{Aut}(A)$ on $A$ induces a left action on the function space $F(A, \mathbb{C})$ of $\mathbb{C}$-valued functions on $A$:

$$(\tau f)(a) = f(a\tau), \quad a \in A, \quad \tau \in G_r.$$

Write $g \sim f$ if $g = \tau f$ for some $\tau \in G_r$. The fixed points of this action are the $G_r$-invariant functions on $A$:

$$F^{G_r}(A, \mathbb{C}) = \{f \in F(A, \mathbb{C}) : f(a\tau) = f(a), a \in A, \tau \in G_r\}.$$

Define a projection $P : F(A, \mathbb{C}) \to F^{G_r}(A, \mathbb{C})$ by averaging over the orbits of the $G_r$-action. For $f \in F(A, \mathbb{C})$ and $a \in A$,

$$(Pf)(a) = \frac{1}{|G_r|} \sum_{\tau \in G_r} (\tau f)(a) = \frac{1}{|G_r|} \sum_{\tau \in G_r} f(a\tau).$$

**Proposition 8.1.** *The map $P$ has the following properties.*

*(1) The map $P$ is a linear projection; i.e., $P \circ P = P$.*
*(2) If $g \sim f$, then $Pg = Pf$.*
*(3) Suppose $\pi, \theta$ are two characters on $A$. Then $\theta \sim \pi$ if and only if $P\theta = P\pi$.*
*(4) Discarding duplicates, the distinct $P\pi$'s form an orthogonal system in $F^{G_r}(A, \mathbb{C})$. In particular, the distinct $P\pi$'s are linearly independent in $F^{G_r}(A, \mathbb{C})$.*

**Proof.** The first result is an exercise for the reader. The second result follows from a reindexing argument. For the third result, if $P\pi_1 = P\pi_2$, then

$$\sum_{\tau_1 \in G_r} \tau_1\pi_1 = \sum_{\tau_2 \in G_r} \tau_2\pi_2.$$

The functions $\tau_1\pi_1$ and $\tau_2\pi_2$ are all characters on $A$. By linear independence of characters, $\pi_2 = \tau\pi_1$ for some $\tau \in G_r$.

The fourth result makes use of the inner product $\langle \cdot, \cdot \rangle$ of Eq. (1) of Subsection 2.1. Suppose $P\theta \neq P\pi$. Then

$$|G_r|^2 \langle P\theta, P\pi \rangle = \langle \sum_{\tau_1 \in G_r} \tau_1\theta, \sum_{\tau_2 \in G_r} \tau_2\pi \rangle = \sum_{\tau_1, \tau_2} \langle \tau_1\theta, \tau_2\pi \rangle.$$

But each $\langle \tau_1\theta, \tau_2\pi \rangle = 0$ by Proposition 2.1. The distinct $P\pi$'s actually form a basis for $F^{G_r}(A, \mathbb{C})$, but we will not need this fact. □

### 8.3. *Extension property for Frobenius bimodules*

In this subsection we prove that the extension property with respect to swc holds for any Frobenius bimodule $A$. This result was first proved for finite fields in Ref. 19, p. 364, and for Frobenius rings in Ref. 52, Theorem 9.

**Theorem 8.1 (†).** *Let $A$ be a Frobenius bimodule over a finite ring $R$, and suppose $A$ is equipped with a symmetrized weight composition* swc*. Then $A$ has the extension property with respect to* swc*.*

**Proof.** Suppose $C_1, C_2 \subset A^n$ are two $R$-linear codes and that $f : C_1 \to C_2$ is an $R$-linear isomorphism that preserves swc. Let $M$ be the $R$-module underlying the code $C_1$ and let $\lambda : M \to A^n$ be the inclusion $C_1 \subset A^n$. Set $\nu = \lambda \circ f : M \to A^n$. Because $f$ preserves swc, it follows that $\mathrm{swc}_a(x\lambda) = \mathrm{swc}_a(x\nu)$ for all $a \in A/G_r$ and $x \in M$.

Express $\lambda, \nu : M \to A^n$ in terms of components: $\lambda = (\lambda_1, \ldots, \lambda_n)$, $\nu = (\nu_1, \ldots, \nu_n)$, where $\lambda_i, \nu_j \in \mathrm{Hom}_R(M, A)$. For $a \in A/G_r$, $x \in M$,

$$\mathrm{swc}_a(x\lambda) = \frac{1}{|\widehat{A}|} \sum_{i=1}^{n} \sum_{b \sim a} \sum_{\pi \in \widehat{A}} \pi(x\lambda_i - b) = \frac{1}{|\widehat{A}|} \sum_{i=1}^{n} \sum_{b \sim a} \sum_{\pi \in \widehat{A}} \pi(x\lambda_i)\bar{\pi}(b),$$

by Proposition 2.1. The invariance of swc, i.e., $\mathrm{swc}_a(x\lambda) = \mathrm{swc}_a(x\nu)$, becomes

$$\sum_{\pi \in \widehat{A}} \left( \sum_{i=1}^{n} \pi(x\lambda_i) \right) (P\bar{\pi})(a) = \sum_{\pi \in \widehat{A}} \left( \sum_{j=1}^{n} \pi(x\nu_j) \right) (P\bar{\pi})(a), \qquad (15)$$

for $a \in A/G_r$ and $x \in M$.

For a fixed $x \in M$, Eq. (15) is an equation of complex linear combinations of averaged characters (as functions of $a$). By linear independence of averaged characters, we equate corresponding coefficients. Remember that $\psi \sim \pi$ if and only if $P\psi = P\pi$. Thus

$$\sum_{i=1}^{n} \sum_{\theta \sim \pi} \theta(x\lambda_i) = \sum_{j=1}^{n} \sum_{\phi \sim \pi} \phi(x\nu_j), \quad x \in M. \qquad (16)$$

Note that Eq. (16) is an equation of characters on $M$, and that we have one such equation for each $P\pi$, $\pi \in \widehat{A}$.

We now use the hypothesis that $A$ is a Frobenius bimodule: $\widehat{A}$ has a generating character $\varrho$. Consider Eq. (16) for $\pi = \rho$, and take $i = 1$ and $\theta = \rho$ on the left side. By linear independence of characters on $M$, there exists $\phi \sim \rho$ and index $j$ such that $\rho(x\lambda_1) = \phi(x\nu_j)$ for all $x \in M$. As $\phi \sim \rho$, there exists $\tau_1 \in G_r$ such that $\phi = \tau_1\rho$. Thus $\rho(x\lambda_1) = \rho(x\nu_j\tau_1)$ for all $x \in M$. By Lemma 5.2, $\lambda_1 = \nu_j\tau_1$.

A reindexing argument shows that

$$\sum_{\theta \sim \rho} \theta(x\lambda_1) = \sum_{\phi \sim \rho} \phi(x\nu_j), \quad x \in M.$$

This allows us to reduce by one the size of the outer summation in Eq. (16) (still with $\pi = \rho$). Proceeding by induction, we obtain a $G_r$-monomial transformation $T$ of $A^n$ with $\lambda = \nu T$, as desired. □

**Remark 8.1.** Naturally, one would like to mimic the ideas in the proof of Theorem 5.2 to extend Theorem 8.1 to more general alphabets, but I have not been successful in doing so.

## 9. General weight functions

In this section, we describe what is known about the extension property for weight functions more general than the Hamming weight.

### 9.1. *Homogeneous weight*

The homogeneous weight was first introduced by Constantinescu in her Ph.D. dissertation[10] and was developed in subsequent papers by a number of authors.[11,12,20–22,26] The extension property with respect to homogeneous weight has been proved directly in these papers using techniques involving the combinatorial structure of the principal submodules of the alphabet and its associated Möbius function (as in Example 4.3). In the future, the homogeneous weight may well turn out to be more important than the Hamming weight for general alphabets.

The goal of this subsection is modest: to show that homogeneous weight is preserved if and only if Hamming weight is preserved. It then follows that an alphabet has the extension property with respect to homogenous weight if and only if it has the extension property with respect to Hamming weight. This result goes back to Greferath and Schmidt[22] for ring alphabets. We follow the treatment for module alphabets in Ref. 21, Section 4, but we omit proofs.

As usual, let $R$ be a finite ring with 1, and let $A$ be a finite left $R$-module, which will be the alphabet for $R$-linear codes. For convenience, let $\mathcal{U} = \mathcal{U}(R)$ denote the group of units of $R$.

**Definition 9.1.** A weight $w : A \to \mathbb{Q}$ is *pre-homogeneous* if

(1) the left symmetry group $G_l$ equals $\mathcal{U}$; and
(2) there exists a rational number $\gamma$ such that

$$\sum_{b \in Ra} w(b) = \gamma |Ra|, \quad \text{all nonzero } a \in A.$$

A weight $w$ is *homogeneous* if, in addition:

$$\sum_{b\in B} w(b) = \gamma|B|, \quad \text{all nonzero submodules } B \subset A.$$

Let $P = \{Ra : a \in A\}$ be the poset of all principal left submodules of $A$, as in Example 4.3. Let $\mu$ be the Möbius function for $P$.

**Theorem 9.1 (Ref. 21, Theorem 4.2).** *Every alphabet $A$ admits a pre-homogeneous weight $w$, and every such pre-homogeneous weight has the form*

$$w(a) = \gamma\left(1 - \frac{\mu(0, Ra)}{|\mathcal{U}a|}\right), \quad a \in A,$$

*for some nonzero $\gamma \in \mathbb{Q}$.*

We call $\gamma$ the *average weight* of $w$.

**Proposition 9.1 (Ref. 21, Proposition 4.1).** *An alphabet $A$ admits a homogeneous weight $w$ if and only if* $\mathrm{soc}(A)$ *is cyclic.*

Let $F^{\mathcal{U}}(A, \mathbb{Q})$ be the space of $\mathcal{U}$-invariant $\mathbb{Q}$-valued functions on $A$; i.e., those functions $f : A \to \mathbb{Q}$ satisfying $f(ua) = f(a)$ for all $a \in A$ and $u \in \mathcal{U}$. Define $\Sigma : F^{\mathcal{U}}(A, \mathbb{Q}) \to F^{\mathcal{U}}(A, \mathbb{Q})$ by

$$(\Sigma f)(a) = \frac{1}{|Ra|}\sum_{b\in Ra} f(b), \quad f \in F^{\mathcal{U}}(A, \mathbb{Q}), \quad a \in A.$$

Observe that the pre-homogeneous condition implies that the Hamming weight wt satisfies $\gamma\,\mathrm{wt} = \Sigma w$, where $w$ is a pre-homogeneous weight with average weight $\gamma$.

Also define the *kernel* $K : A \times A \to \mathbb{Q}$ by

$$K(a, b) = \frac{|Ra|}{|\mathcal{U}a|}\frac{|Rb|}{|\mathcal{U}b|}\,\mu(Ra, Rb), \quad a, b \in A,$$

where, as above, $\mu$ is the Möbius function for $P = \{Ra : a \in A\}$. Finally, we use the kernel $K$ to define $\Delta : F^{\mathcal{U}}(A, \mathbb{Q}) \to F^{\mathcal{U}}(A, \mathbb{Q})$ by

$$(\Delta g)(a) = \frac{1}{|Ra|}\sum_{b\in Ra} g(b)K(b, a), \quad g \in F^{\mathcal{U}}(A, \mathbb{Q}), \quad a \in A.$$

**Theorem 9.2 (Ref. 21, Theorem 4.4).** *The endomorphisms*

$$\Sigma, \Delta : F^{\mathcal{U}}(A, \mathbb{Q}) \to F^{\mathcal{U}}(A, \mathbb{Q})$$

*are inverses.*

Functions $f_1, f_2, \ldots, f_n \in F^{\mathcal{U}}(A, \mathbb{Q})$, determine a function $f : A^n \to \mathbb{Q}$ by

$$f(a_1, \ldots, a_n) = \sum_{i=1}^{n} f_i(a_i).$$

Then $\Sigma$ and $\Delta$ commute with this construction (Ref. 21, Proposition 4.2):

$$(\Sigma f)(a_1, \ldots, a_n) = \sum_{i=1}^{n} (\Sigma f_i)(a_i),$$
$$(\Delta f)(a_1, \ldots, a_n) = \sum_{i=1}^{n} (\Delta f_i)(a_i).$$

It follows that Hamming weight and a pre-homogeneous weight $w$ satisfy $\gamma \,\mathrm{wt} = \Sigma w$ on all on $A^n$. Because $\Delta$ inverts $\Sigma$, we have the next corollary.

**Corollary 9.1.** *For linear codes $C_1, C_2 \subset A^n$, a linear homomorphism $f : C_1 \to C_2$ preserves the Hamming weight* wt *if and only if $f$ preserves a pre-homogeneous weight $w$.*

This corollary allows all extension properties proven for homogeneous weights to apply to Hamming weight, and vice versa. Note that one of the conditions for the extension property to hold for Hamming weight, $\mathrm{soc}(A)$ being cyclic, is exactly the condition needed for a pre-homogeneous weight to be homogeneous.

### 9.2. *A sufficient condition*

In this subsection we describe a sufficient condition for the extension theorem to hold with respect to a general weight function over a Frobenius bimodule, generalizing Ref. 54, Theorem 3.1.

Let $R$ be a finite ring with 1 and $A$ be a Frobenius bimodule over $R$. Let $w$ be a weight on the alphabet $A$, so that $w : A \to \mathbb{Q}$ with $w(0) = 0$. Then there are left and right symmetry groups $G_l, G_r$, as in Eqs. (8) and (9) of Subsection 5.1. The right symmetry group $G_r \subset \mathrm{Aut}(A)$ defines a symmetrized weight composition swc, as in Definition 8.1.

**Lemma 9.1.** *Suppose $\lambda : M \to A^n$ is a parameterized code, then*

$$w(x\lambda) = \sum_{a \in A/G_r} w(a) \,\mathrm{swc}_a(x\lambda), \quad x \in M.$$

**Proof.** For any $x \in M$,

$$\begin{aligned} w(x\lambda) &= \sum_{i=1}^{n} w(x\lambda_i) = \sum_{a\in A} w(a)|\{i : x\lambda_i = a\}| \\ &= \sum_{a\in A/G_r} \sum_{b\sim a} w(b)|\{i : x\lambda_i = b\}| \\ &= \sum_{a\in A/G_r} w(a) \sum_{b\sim a} |\{i : x\lambda_i = b\}| = \sum_{a\in A/G_r} w(a)\,\mathrm{swc}_a(x\lambda), \end{aligned}$$

where we used the fact that $w(b) = w(a)$ if $b \sim a$. □

We now utilize the left module structure of $M$.

**Corollary 9.2.** *For $s \in R$,*

$$w(sx\lambda) = \sum_{a\in A/G_r} w(sa)\,\mathrm{swc}_a(x\lambda), \quad x \in M.$$

**Proof.** Repeat the argument of Lemma 9.1 using the fact that

$$w(sx\lambda) = \sum_{i=1}^{n} w(sx\lambda_i) = \sum_{a\in A} w(sa)|\{i : x\lambda_i = a\}|.$$

□

Let $F_0^{G_l}(R,\mathbb{C}) = \{f : R \to \mathbb{C} \mid f(0) = 0 \text{ and } f(us) = f(s), u \in G_l, s \in R\}$ be the complex vector space of $G_l$-invariant functions on $R$ that vanish at 0. Similarly, let $F_0^{G_r}(A,\mathbb{C}) = \{f : A \to \mathbb{C} \mid f(0) = 0 \text{ and } f(a\phi) = f(a), a \in A, \phi \in G_r\}$ be the complex vector space of $G_r$-invariant functions on $A$ that vanish at 0. Define a linear transformation $W : F_0^{G_r}(A,\mathbb{C}) \to F_0^{G_l}(R,\mathbb{C})$ by $(Wf)(s) = \sum_{a\in A} w(sa)f(a)$ for $f \in F_0^{G_r}(A,\mathbb{C})$ and $s \in R$.

**Theorem 9.3 (†).** *If $W : F_0^{G_r}(A,\mathbb{C}) \to F_0^{G_l}(R,\mathbb{C})$ is injective, then the Frobenius bimodule $A$ has the extension property with respect to $w$.*

**Proof.** Suppose $C_1, C_2 \subset A^n$ are two $R$-linear codes, and suppose $f : C_1 \to C_2$ is an $R$-linear isomorphism that preserves the weight $w$. As usual, let $M$ equal the module underlying the code $C_1$, with $\lambda : M \to A^n$ being the inclusion of $C_1 \subset A^n$.

By hypothesis, $w(x\lambda f) = w(x\lambda)$ for all $x \in M$. In particular, if $s \in R$, then $sx \in M$ for any $x \in M$. Thus, $w(sx\lambda f) = w(sx\lambda)$ for all $x \in M$ and $s \in R$. By Corollary 9.2, this implies that

$$\sum_{a\in A} w(sa)\,\mathrm{swc}_a(x\lambda f) = \sum_{a\in A} w(sa)\,\mathrm{swc}_a(x\lambda), \tag{17}$$

for all $s \in R$ and $x \in M$. For a fixed value of $x \in M$, $\mathrm{swc}_a(x\lambda)$ and $\mathrm{swc}_a(x\lambda f)$ are elements of $F_0^{G_r}(A, \mathbb{C})$, and Eq. (17) says that the values of $W$ on these elements are equal. By the injectivity of $W$, we conclude that $\mathrm{swc}_a(x\lambda f) = \mathrm{swc}_a(x\lambda)$, for all $a \in A$ and $x \in M$. But this means that $f : C_1 \to C_2$ preserves swc. The result now follows from Theorem 8.1. □

**Remark 9.1.** A more concrete way to express Theorem 9.3 is to consider a matrix $W$, whose rows are parameterized by the nonzero elements of $G_l\backslash R$, whose columns are parameterized by the nonzero elements of $A/G_r$, and whose entry $W_{s,a}$, $s \in G_l\backslash R$, $a \in A/G_r$, is $w(sa)$, the weight of the element $sa \in A$. This is well-defined, because of the actions of the symmetry groups. The injectivity condition is that the matrix not annihilate any nonzero column vector (whose entries would be parameterized by $a \in A/G_r$).

### 9.3. *Chain rings*

In this subsection we discuss maximally symmetric weights on finite chain rings.

A finite ring $R$ is a left *chain ring* if its left ideals form a chain under set inclusion. By a result of Clark and Drake, Ref. 9, Lemma 1, a finite left chain ring is also a right chain ring. Moreover, in a finite chain ring the radical $\mathfrak{m} = \mathrm{rad}(R)$ is a maximal ideal, and all the ideals are two-sided and of the form $\mathfrak{m}^i = Rm^i = m^iR$, for some (any) $m \in \mathfrak{m} \setminus \mathfrak{m}^2$. Let $e$ be the smallest positive integer such that $\mathfrak{m}^e = 0$. Denoting by $\mathcal{U}$ the group of units $\mathcal{U}(R)$, note that $\mathfrak{m}^i \setminus \mathfrak{m}^{i+1} = \mathcal{U}m^i = m^i\mathcal{U}$.

A finite chain ring $R$ is Frobenius because $R/\mathfrak{m} \cong \mathfrak{m}^{e-1} = \mathrm{soc}(R)$. Let $A = R$, so that $R$ is a Frobenius bimodule, and let $w : R \to \mathbb{Q}$ be a weight on $R$. Assume that $w$ has maximal symmetry, i.e., that $G_l = G_r = \mathcal{U}$. (In fact, $G_l = \mathcal{U}$ if and only if $G_r = \mathcal{U}$, because $\mathfrak{m}^i \setminus \mathfrak{m}^{i+1} = \mathcal{U}m^i = m^i\mathcal{U}$.) Then the weight $w$ is completely determined by its values $w_i := w(m^i)$, $i = 0, 1, \ldots, e-1$.

According to Remark 9.1, the matrix representing $W$ in Theorem 9.3 has the form

$$W_{i,j} = w(m^i m^j) = w(m^{i+j}) = w_{i+j}, \quad 0 \le i, j \le e-1.$$

Since $m^e = 0$, $w_{i+j} = 0$ for $i + j \ge e$. It is then easy to calculate that $\det(W) = \pm w_{e-1}^e$. As long as $w_{e-1} = w(m^{e-1}) \neq 0$, $W$ is injective, and $R$ has the extension property with respect to $w$. We summarize this discussion in the following theorem, a special case of Ref. 54, Theorem 7.3.

**Theorem 9.4.** *Suppose $R$ is a finite chain ring, with* $\mathrm{rad}(R) = Rm = mR$. *Suppose $w : R \to \mathbb{Q}$ is a weight on $A = R$ such that $G_l = G_r = \mathcal{U}(R)$. Then $w$ is determined by its values $w_i = w(m^i)$, $i = 0, 1, \ldots, e-1$. Moreover, $R$ has the extension property with respect to $w$ if and only if $w_{e-1} = w(m^{e-1}) \neq 0$.*

**Remark 9.2.** When the weight $w$ has less symmetry, the conditions needed in order for the extension property to hold with respect to $w$ can become very complicated. In the commutative case, the determinant $\det(W)$ admits a factorization into linear expressions involving the characters of the group of units $\mathcal{U}(R)$. See Refs. 54, Theorem 7.3, and 55, Theorem 7, for details.

### 9.4. *Matrix rings*

In this subsection we consider weights on the matrix ring $M_n(\mathbb{F}_q)$ having maximal symmetry.

Let $R = M_n(\mathbb{F}_q)$ be the ring of $n \times n$ matrices over the finite field $\mathbb{F}_q$. Let the alphabet $A$ be the ring $R$ itself, and suppose that $w : R \to \mathbb{Q}$ is a weight on $R$ having maximal symmetry. That is, we assume that $G_l = G_r = \mathcal{U}(R) = GL_n(\mathbb{F}_q)$. The ring $R$ is Frobenius, Ref. 53, Example 4.4, so that $R$ is a Frobenius bimodule.

**Proposition 9.2.** *Let $R = A = M_n(\mathbb{F}_q)$, and suppose $w : R \to \mathbb{Q}$ is a weight having maximal symmetry. Then $w(X)$ depends only on the rank* $\mathrm{rk}(X)$ *of the matrix $X \in M_n(\mathbb{F}_q)$. That is, if* $\mathrm{rk}(X) = \mathrm{rk}(Y)$, *$X, Y \in M_n(\mathbb{F}_q)$, then $w(X) = w(Y)$.*

**Proof.** By using elementary row and column operations, every $X \in M_n(\mathbb{F}_q)$ satisfies $PXQ = I'_s$, for some $P, Q \in GL_n(\mathbb{F}_q)$ and integer $s$, where

$$I'_s = \begin{pmatrix} I_s & 0 \\ 0 & 0 \end{pmatrix}.$$

The result now follows from the symmetry assumptions on $w$. □

Consequently, the weight $w$ is completely determined by $n$ values $w_s := w(I'_s)$, $s = 1, 2, \ldots, n$. (Remember that $w(0) = 0$ is part of the definition of weight.) Every matrix $X$ having $\mathrm{rk}(X) = s$ satisfies $w(X) = w_s$.

**Theorem 9.5 (†).** *Let $R = A = M_n(\mathbb{F}_q)$. Suppose $w : R \to \mathbb{Q}$ is a weight having maximal symmetry, and denote by $w_s$ the value of $w$ on an element*

*of $R$ of rank $s$. Then $R$ has the extension property with respect to the weight $w$ if the following quantities $w'_s$ are all non-zero, for $s = 1, 2, \ldots, n$:*

$$w'_s := \sum_{i=1}^{s} (-1)^i q^{\binom{i}{2}} \begin{bmatrix} s \\ i \end{bmatrix}_q w_i.$$

Theorem 9.5 will follow as a corollary of Theorem 9.6, which describes the determinant of the matrix representing $W$ in Theorem 9.3. To prepare for Theorem 9.6, we need to describe the orbit spaces $G_l \backslash R$ and $R/G_r$ of Remark 9.1.

Remember that we are assuming that $w$ has maximal symmetry, so that $G_l = G_r = GL_n(\mathbb{F}_q)$. Then $G_l \backslash R$ is in one-to-one correspondence with the set of row reduced echelon matrices, while $R/G_r$ is in one-to-one correspondence with the set of column reduced echelon matrices. The matrix representing $W$ in Theorem 9.3 thus has rows parameterized by the nonzero row reduced echelon matrices and columns parameterized by the nonzero column reduced echelon matrices. The entry of $W$ in position $(P, Q)$ is $w_s$, where $s = \mathrm{rk}(PQ)$.

It will be useful to view the matrix representing $W$ in another way. To that end, the elements of $R = M_n(\mathbb{F}_q)$ define linear transformations $\mathbb{F}_q^n \to \mathbb{F}_q^n$ via (left) matrix multiplication on column vectors. Two elements of $R$ are in the same left $G_l$-orbit if and only if they have the same kernel as linear transformations. Similarly, two elements of $R$ are in the same right $G_r$-orbit if and only if they have the same image as linear transformations. So, another way to parameterize the matrix representing $W$ is this: parameterize rows and columns by nonzero linear subspaces of $\mathbb{F}_q^n$. The row parameterized by a nonzero subspace $U$ will correspond to the $G_l$-orbit of linear transformations with kernel equal to $U^\perp$ (under the standard dot product on $\mathbb{F}_q^n$). The column parameterized by a nonzero subspace $V$ will correspond to the $G_r$-orbit of linear transformations with image equal to $V$. The entry of $W$ in position $(U, V)$ is then $w_s$, where $s = \dim V - \dim(U^\perp \cap V)$, as the reader will verify.

**Theorem 9.6 (†).** *In the notation given above, the determinant of the matrix representing $W$ is*

$$\det W = C \prod_{s=1}^{n} (w'_s)^{\begin{bmatrix} n \\ s \end{bmatrix}_q} = C \prod_{s=1}^{n} \left( \sum_{i=1}^{s} (-1)^i q^{\binom{i}{2}} \begin{bmatrix} s \\ i \end{bmatrix}_q w_i \right)^{\begin{bmatrix} n \\ s \end{bmatrix}_q},$$

*where $C$ is a nonzero constant.*

**Proof.** Define another matrix $P$ whose rows and columns are parameterized by the nonzero linear subspaces of $\mathbb{F}_q^n$ by

$$P_{U,V} = \begin{cases} (-1)^{\dim U} q^{\binom{\dim U}{2}}, & U \subset V, \\ 0, & U \not\subset V. \end{cases}$$

If we order the nonzero linear subspaces in such a way that the dimensions are (say) nonincreasing, then the matrix $P$ is lower-triangular, with diagonal entries

$$P_{U,U} = (-1)^{\dim U} q^{\binom{\dim U}{2}}.$$

Thus, the matrix $P$ has $\det P \neq 0$ and is invertible over $\mathbb{Q}$.

A somewhat laborious computation shows that the matrix $WP$ has a block upper-triangular form. The block matrices on the diagonal have the form $w'_s Q_s$, $s = 1, 2, \ldots, n$, where, as above,

$$w'_s := \sum_{i=1}^{s} (-1)^i q^{\binom{i}{2}} \begin{bmatrix} s \\ i \end{bmatrix}_q w_i,$$

and $Q_s$ is a square matrix of size $\begin{bmatrix} n \\ s \end{bmatrix}_q$, parameterized by the linear subspaces of dimension $s$ in $\mathbb{F}_q^n$. The entries of the matrix $Q_s$ are given by

$$(Q_s)_{U,V} = \begin{cases} 1, & U^\perp \cap V = 0, \\ 0, & U^\perp \cap V \neq 0. \end{cases}$$

Provided that we can show that $\det Q_s$ is nonzero, the formula for $\det W$ follows. We show that $\det Q_s \neq 0$ in Lemma 9.2. □

**Lemma 9.2.** *In the notation above,* $\det Q_s \neq 0$ *for* $s = 1, 2, \ldots, n$.

**Proof.** We make use of the fact that we already know that $R = M_n(\mathbb{F}_q)$, a Frobenius ring, has the extension property with respect to Hamming weight wt, by Theorem 5.4.

To be more precise, let $R = M_n(\mathbb{F}_q)$ and let the alphabet ${}_R A = {}_R R$ be the ring itself. Using Hamming weight wt on $A = R$, the symmetry groups are $G_l = G_r = \mathcal{U}(R) = GL_n(\mathbb{F}_q)$. Because Hamming weight has the property that $\mathrm{wt}(a) \neq 0$ for every nonzero $a \in A^n$, Theorem 7.2 implies that the mapping $W : F_0(\mathcal{O}^\sharp, \mathbb{N}) \to F_0(\mathcal{O}, \mathbb{Q})$ is injective for every finite $R$-module $M$. When ${}_R M = {}_R R$ is the ring itself, the matrix representing $W : F_0(\mathcal{O}^\sharp, \mathbb{N}) \to F_0(\mathcal{O}, \mathbb{Q})$ is, by Eq. (14) of Subsection 7.5, the same as the matrix of Remark 9.1, using Hamming weight wt. As a consequence,

the matrix $W$ of Theorem 9.6 is invertible, *provided one is using Hamming weight* wt.

In the case of Hamming weight, where $w_1 = w_2 = \cdots = w_n = 1$, a computation using the Cauchy binomial theorem shows that $w'_1 = w'_2 = \cdots = w'_n = 1$, as well. As a consequence, if we repeat the argument in the proof of Theorem 9.6 in the case of Hamming weight, we see that $WP$ is a block upper-triangular matrix, with the matrices $Q_s$ on the diagonal. Because $P$ is invertible in general and $W$ is invertible for Hamming weight, as shown above, we conclude that the matrices $Q_s$ are also invertible. □

**Remark 9.3.** I would expect that there is a direct proof that the matrices $Q_s$ are invertible, but I was unable to locate one.

## 10. The MacWilliams identities: A model theorem

In the next several sections, we turn our attention to the MacWilliams identities on weight enumerators.

In this section we describe a theorem, valid over finite fields, involving linear codes, their dual codes, and the MacWilliams identities between their Hamming weight enumerators. This theorem will serve as a model for subsequent generalizations to additive codes, linear codes over rings or modules, and other weight enumerators.

### 10.1. *Classical case of finite fields*

We recall without proofs the classical situation of linear codes over finite fields, their dual codes, and the MacWilliams identities between the Hamming weight enumerators of a linear code and its dual code. This material is standard.[38] Proofs of generalizations will be provided in subsequent sections.

Let $\mathbb{F}_q$ be a finite field with $q$ elements. Define $\langle \cdot, \cdot \rangle : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ by

$$\langle x, y \rangle = \sum_{j=1}^{n} x_j y_j,$$

for $x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_q^n$. The operations are those of the finite field $\mathbb{F}_q$. The pairing $\langle \cdot, \cdot \rangle$ is a non-degenerate symmetric bilinear form.

A *linear code of length* $n$ is a linear subspace $C \subset \mathbb{F}_q^n$. It is traditional to denote $k = \dim C$. The *dual code* $C^\perp$ is defined by:

$$C^\perp = \{y \in \mathbb{F}_q^n : \langle x, y \rangle = 0, \text{ for all } x \in C\}.$$

As usual, the *Hamming weight* $\mathrm{wt} : \mathbb{F}_q \to \mathbb{Q}$ is defined by $\mathrm{wt}(a) = 1$ for $a \neq 0$, and $\mathrm{wt}(0) = 0$. The Hamming weight is extended to a function $\mathrm{wt} : \mathbb{F}_q^n \to \mathbb{Q}$ by

$$\mathrm{wt}(x) = \sum_{j=1}^{n} \mathrm{wt}(x_j), \quad x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n.$$

Then $\mathrm{wt}(x)$ equals the number of non-zero entries of $x \in \mathbb{F}_q^n$.

The *Hamming weight enumerator* of a linear code $C$ is a polynomial $W_C(X, Y)$ in $\mathbb{C}[X, Y]$ defined by

$$W_C(X, Y) = \sum_{x \in C} X^{n - \mathrm{wt}(x)} Y^{\mathrm{wt}(x)} = \sum_{j=0}^{n} A_j X^{n-j} Y^j,$$

where $A_j$ is the number of codewords in $C$ of Hamming weight $j$.

The following theorem summarizes the essential properties of $C^\perp$ and the Hamming weight enumerator. This theorem will serve as a model for results in later sections.

**Theorem 10.1.** *Suppose $C$ is a linear code of length $n$ over a finite field $\mathbb{F}_q$. The dual code $C^\perp$ satisfies:*

*(1)* $C^\perp \subset \mathbb{F}_q^n$;
*(2)* $C^\perp$ *is a linear code of length* $n$;
*(3)* $(C^\perp)^\perp = C$;
*(4)* $\dim C^\perp = n - \dim C$ *(or* $|C| \cdot |C^\perp| = |\mathbb{F}_q^n| = q^n$*); and*
*(5) (the MacWilliams identities*[36,37]*)*

$$W_{C^\perp}(X, Y) = \frac{1}{|C|} W_C(X + (q-1)Y, X - Y).$$

### 10.2. *Plan of attack*

In subsequent sections, Theorem 10.1 will be generalized in various ways, first to additive codes, then to linear codes over rings and modules, and finally to other weight enumerators. In order to maintain our focus on the central issue of duality, only the Hamming weight enumerator will be discussed initially.

As we will see in the discussion of additive codes (Section 11), one natural choice for a dual code to a code $C \subset G^n$ will be the character-theoretic annihilator $(\widehat{G}^n : C)$. The drawback of this choice is that the annihilator is not a code in the original ambient space $G^n$; rather, it is a code in $\widehat{G}^n$. By introducing a nondegenerate biadditive form on $G^n$ (Subsection 11.3), one

establishes a choice of identification between $G^n$ and $\widehat{G}^n$. This will remedy the drawback of the dual not being a code in the original ambient space.

At the next stage of generalization, linear codes over rings (Section 12), one must be mindful to ensure that the dual code is again a linear code, that the size of the dual is correct, and that the double dual property is satisfied. The latter requirement will force the ground ring to be quasi-Frobenius. In order that the dual code be linear, the biadditive form needs to be bilinear, yet still provide an identification between $R^n$ and $\widehat{R}^n$. This and the size restriction will place an additional requirement on the ground ring, that it be Frobenius.

Once duality has been sorted out, the generalizations to other weight enumerators will be comparatively straight-forward (Section 13).

## 11. MacWilliams identities for additive codes

In this section we generalize the model Theorem 10.1 to additive codes over finite abelian groups. We begin with a review of the Fourier transform and the Poisson summation formula, which will be key tools in proving the MacWilliams identities.

### 11.1. *Fourier transform and Poisson summation formula*

In this subsection we record some of the basic properties of the Fourier transform on a finite abelian group (cf. Ref. 48). We make use of the material in Section 2. The proofs are left as exercises for the reader.

Suppose that $G$ is a finite abelian group and that $V$ is a vector space over the complex numbers. Let $F(G,V) = \{f : G \to V\}$ be the set of all functions from $G$ to $V$; $F(G,V)$ is vector space over the complex numbers.

The *Fourier transform* $\hat{}\ : F(G,V) \to F(\widehat{G},V)$ is defined by

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

Notice that the characters are in multiplicative form. The Fourier transform is a linear transformation with inverse transformation determined by the following relation.

**Proposition 11.1 (Fourier inversion formula).**

$$f(x) = \frac{1}{|G|} \sum_{\pi \in \widehat{G}} \pi(-x) \hat{f}(\pi), \quad x \in G, \quad f \in F(G,V).$$

**Theorem 11.1 (Poisson summation formula).** *Let $H$ be a subgroup of a finite abelian group $G$. Then, for any $a \in G$,*

$$\sum_{x \in H} f(a+x) = \frac{1}{|(\widehat{G} : H)|} \sum_{\pi \in (\widehat{G}:H)} \pi(-a)\hat{f}(\pi).$$

*In particular, when $a = 0$ (or $a \in H$),*

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

In fact, the Poisson summation formula is a special case of a more general result that we will now describe. This more general result will be used in Theorem 13.2 when we discuss a degenerate case of the MacWilliams identities.

Let $G_1$ and $G_2$ be finite abelian groups, and suppose $\tau : G_1 \to \widehat{G}_2$ is a group homomorphism. Then $\tau$ induces a homomorphism $\hat{\tau} : G_2 \cong (\widehat{G}_2)\widehat{\ } \to \widehat{G}_1$ by $(\hat{\tau}(y))(x) = (\tau(x))(y)$, for $x \in G_1$, $y \in G_2$.

**Theorem 11.2 (†).** *Let $G_1, G_2$ be finite abelian groups, and let $\tau : G_1 \to \widehat{G}_2$ be a homomorphism. Assume $K \subset G_1$ is a subgroup and $a \in G_1$. Then for any function $f : G_2 \to V$, $V$ a complex vector space,*

$$\sum_{x \in K} \hat{f}(\tau(a+x)) = |K| \sum_{y \in \hat{\tau}^{-1}(\widehat{G}_1:K)} (\hat{\tau}(y))(a) f(y).$$

*In particular, when $a = 0$ (or $a \in K$),*

$$\sum_{x \in K} \hat{f}(\tau(x)) = |K| \sum_{y \in \hat{\tau}^{-1}(\widehat{G}_1:K)} f(y).$$

To recover the Poisson summation formula in the subgroup case of $H \subset G$, take $G_1 = \widehat{G}$, $G_2 = G$, $\tau : \widehat{G} \to \widehat{G}$ equal to the identity, and $K = (\widehat{G} : H) \subset G_1$. Observe that $\hat{\tau}^{-1}(\widehat{G}_1 : K) = H$.

When the vector space $V$ has the additional structure of a complex algebra, we have the following technical result.

**Proposition 11.2.** *Suppose that $\mathcal{V}$ is a complex algebra. Suppose that $f \in F(G^n, \mathcal{V})$ has the form*

$$f(x_1, \ldots, x_n) = \prod_{i=1}^{n} f_i(x_i),$$

*where* $f_1, \ldots, f_n \in F(G, \mathcal{V})$. *Then* $\hat{f} = \prod \hat{f}_i$; *i.e., for* $\pi = (\pi_1, \ldots, \pi_n) \in \widehat{G^n} \cong \widehat{G}^n$,

$$\hat{f}(\pi) = \prod_{i=1}^{n} \hat{f}_i(\pi_i).$$

### 11.2. *Additive codes*

Let $(G, +)$ be a finite abelian group. An *additive code of length* $n$ over $G$ is a subgroup $C \subset G^n$. Hamming weight on $G$ is defined as before, for $a \in G$ and $x = (x_1, \ldots, x_n) \in G^n$:

$$\mathrm{wt}(a) = \begin{cases} 1, & a \neq 0, \\ 0, & a = 0; \end{cases} \qquad \mathrm{wt}(x) = \sum_{j=1}^{n} \mathrm{wt}(x_j).$$

Thus, $\mathrm{wt}(x)$ is the number of nonzero entries of $x$.

Given an additive code $C \subset G^n$, one way to define its dual code is via the character-theoretic annihilator $(\widehat{G}^n : C)$.

As before, the Hamming weight enumerator of an additive code $C \subset G^n$ is:

$$W_C(X, Y) = \sum_{x \in C} X^{n - \mathrm{wt}(x)} Y^{\mathrm{wt}(x)} = \sum_{j=0}^{n} A_j X^{n-j} Y^j,$$

where $A_j$ is the number of codewords of Hamming weight $j$ in $C$.

The model Theorem 10.1 then takes the following form. This result is a variant of a theorem of Delsarte.[14]

**Theorem 11.3.** *Suppose* $C$ *is an additive code of length* $n$ *over a finite abelian group* $G$. *The annihilator* $(\widehat{G}^n : C)$ *satisfies:*

*(1)* $(\widehat{G}^n : C) \subset \widehat{G}^n$;
*(2)* $(\widehat{G}^n : C)$ *is an additive code of length* $n$ *in* $\widehat{G}^n$;
*(3)* $(G^n : (\widehat{G}^n : C)) = C$;
*(4)* $|C| \cdot |(\widehat{G}^n : C)| = |G^n|$; *and*
*(5) the MacWilliams identities hold:*

$$W_{(\widehat{G}^n : C)}(X, Y) = \frac{1}{|C|} W_C(X + (|G| - 1)Y, X - Y).$$

The first four properties are clear from the definition of $(\widehat{G}^n : C)$; that $(\widehat{G}^n : C)$ is an additive code in $\widehat{G}^n$ is seen most clearly when characters are written in additive form. For the proof of the MacWilliams identities, we

follow Gleason's use of the Poisson summation formula (see Ref. 3, §1.12). To that end, we first lay some groundwork.

Let $\mathcal{V} = \mathbb{C}[X, Y]$, a commutative complex algebra, and let $f_i : G \to \mathbb{C}[X, Y]$ be given by $f_i(x_i) = X^{1-\mathrm{wt}(x_i)}Y^{\mathrm{wt}(x_i)}$, $x_i \in G$. Now define $f : G^n \to \mathbb{C}[X, Y]$ by

$$f(x_1, \ldots, x_n) = \prod_{i=1}^{n} f_i(x_i) = \prod_{i=1}^{n} X^{1-\mathrm{wt}(x_i)}Y^{\mathrm{wt}(x_i)} = X^{n-\mathrm{wt}(x)}Y^{\mathrm{wt}(x)},$$

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

**Lemma 11.1.** *For $f_i(x_i) = X^{1-\mathrm{wt}(x_i)}Y^{\mathrm{wt}(x_i)}$, $x_i \in G$, and $\pi_i \in \widehat{G}$,*

$$\hat{f}_i(\pi_i) = \begin{cases} X + (|G| - 1)Y, & \pi_i = 1 \quad (\varpi_i = 0), \\ X - Y, & \pi_i \neq 1 \quad (\varpi_i \neq 0). \end{cases}$$

*Thus,*

$$\hat{f}(\pi) = (X + (|G| - 1)Y)^{n-\mathrm{wt}(\varpi)}(X - Y)^{\mathrm{wt}(\varpi)},$$

*where $\pi = (\pi_1, \ldots, \pi_n) \in \widehat{G^n} = \widehat{G}^n$.*

**Proof.** By the definition of the Fourier transform,

$$\hat{f}_i(\pi_i) = \sum_{x_i \in G} \pi_i(x_i) f_i(x_i) = \sum_{x_i \in G} \pi_i(x_i) X^{1-\mathrm{wt}(x_i)}Y^{\mathrm{wt}(x_i)}.$$

Split the sum into the $x_i = 0$ term and the remaining $x_i \neq 0$ terms:

$$\hat{f}_i(\pi_i) = X + \sum_{x_i \neq 0} \pi_i(x_i) Y.$$

By Proposition 2.1, the character sum equals $|G| - 1$ when $\pi_i = 1$ ($\varpi_i = 0$), while it equals $-1$ when $\pi_i \neq 1$ ($\varpi_i \neq 0$). The result for $\hat{f}_i$ follows. Use Proposition 11.2 to obtain the formula for $\hat{f}$. □

**Proof of the MacWilliams identities in Theorem 11.3.** We use $f(x) = X^{n-\mathrm{wt}(x)}Y^{\mathrm{wt}(x)}$ as defined above. By the Poisson summation formula, Theorem 11.1, we have

$$\begin{aligned} W_C(X, Y) &= \sum_{x \in C} f(x) = \frac{1}{|(\widehat{G}^n : C)|} \sum_{\varpi \in (\widehat{G}^n : C)} \hat{f}(\pi) \\ &= \frac{1}{|(\widehat{G}^n : C)|} \sum_{\varpi \in (\widehat{G}^n : C)} (X + (|G| - 1)Y)^{n-\mathrm{wt}(\varpi)}(X - Y)^{\mathrm{wt}(\varpi)} \\ &= \frac{1}{|(\widehat{G}^n : C)|} W_{(\widehat{G}^n : C)}(X + (|G| - 1)Y, X - Y). \end{aligned}$$

Interchanging the roles of $C$ and $(\widehat{G}^n : C)$ yields the form of the identities stated in the theorem. □

**Remark 11.1.** In comparing Theorem 11.3 with Theorem 10.1, the only drawback is that the "dual code" $(\widehat{G}^n : C)$ lives in $\widehat{G}^n$, not $G^n$. One way to address this deficiency will be the use of biadditive forms in Subsection 11.3.

### 11.3. *Biadditive forms*

Biadditive forms are introduced in order to make identifications between a finite abelian group $G$ and its character group $\widehat{G}$.

Let $G$, $H$, and $E$ be abelian groups. A *biadditive form* is a map $\beta : G \times H \to E$ such that $\beta(x, \cdot) : H \to E$ is a homomorphism for all $x \in G$ and $\beta(\cdot, y) : G \to E$ is a homomorphism for all $y \in H$. Observe that $\beta$ induces two group homomorphisms:

$$\begin{aligned} &\chi : G \to \mathrm{Hom}_{\mathbb{Z}}(H, E), && \chi_x(y) = \beta(x, y), \quad x \in G, y \in H; \\ &\psi : H \to \mathrm{Hom}_{\mathbb{Z}}(G, E), && \psi_y(x) = \beta(x, y), \quad x \in G, y \in H. \end{aligned}$$

The biadditive form $\beta$ is *nondegenerate* if both maps $\chi$ and $\psi$ are injective. Extend $\beta$ to $\beta : G^n \times H^n \to E$ by

$$\beta(a, b) = \sum_{j=1}^{n} \beta(x_j, y_j), \quad x = (x_1, \ldots, x_n) \in G^n, y = (y_1, \ldots, y_n) \in H^n.$$

If $G$ and $H$ are finite abelian groups and $E = \mathbb{Q}/\mathbb{Z}$, then recall that $\mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{Q}/\mathbb{Z}) \cong \widehat{G}$, so that a nondegenerate biadditive form $\beta : G \times H \to \mathbb{Q}/\mathbb{Z}$ induces two injective homomorphisms, $\chi : G \to \widehat{H}$ and $\psi : H \to \widehat{G}$. Because $|G| = |\widehat{G}|$, we conclude that $\chi$ and $\psi$ are isomorphisms, so that $G \cong H$. Thus, there is no loss of generality to have $G = H$, with a nondegenerate biadditive form $\beta : G \times G \to \mathbb{Q}/\mathbb{Z}$. Observe now that $\chi = \psi$ if and only if the form $\beta$ is symmetric. Equivalently, $\chi_x(y) = \chi_y(x)$ for all $x, y \in G$ if and only if $\beta$ is symmetric.

For an additive code $C \subset G^n$, the character-theoretic annihilator $(\widehat{G}^n : C) \subset \widehat{G}^n$ corresponds, under the isomorphisms $\chi, \psi$, to the annihilators determined by $\beta$:

$$\begin{aligned} l(C) &:= \{y \in G^n : \beta(y, x) = 0, \text{ for all } x \in C\} && \text{(under } \chi), \\ r(C) &:= \{z \in G^n : \beta(x, z) = 0, \text{ for all } x \in C\} && \text{(under } \psi). \end{aligned}$$

Observe that $l(r(C)) = C$ and $r(l(C)) = C$. Of course, if $\beta$ is symmetric, then $l(C) = r(C)$. To summarize:

**Proposition 11.3.** *Suppose $G$ is a finite abelian group and $\beta : G \times G \to \mathbb{Q}/\mathbb{Z}$ is a nondegenerate biadditive form. The annihilators $l(C)$ and $r(C)$ of an additive code $C \subset G^n$ satisfy*

*(1) $l(C), r(C) \subset G^n$;*
*(2) $l(C), r(C)$ are additive codes of length $n$ in $G^n$;*
*(3) $l(r(C)) = C$ and $r(l(C)) = C$;*
*(4) $|C| \cdot |l(C)| = |C| \cdot |r(C)| = |G^n|$; and*
*(5) the MacWilliams identities hold:*

$$W_{l(C)}(X, Y) = \frac{1}{|C|} W_C(X + (|G| - 1)Y, X - Y) = W_{r(C)}(X, Y).$$

*If $\beta$ is symmetric, then $l(C) = r(C)$. Moreover, for any finite abelian group $G$, there exists a nondegenerate, symmetric biadditive form $\beta : G \times G \to \mathbb{Q}/\mathbb{Z}$.*

## 12. Duality for modules

In this section we discuss dual codes and the MacWilliams identities in the context of linear codes defined over a finite ring or, even more generally, over a finite module over a finite ring.

### 12.1. *Linear codes*

Fix a finite ring $R$ with 1. The ring $R$ may not be commutative. Also fix a finite left $R$-module $A$, which will serve as the alphabet for $R$-linear codes. Remember from Subsection 5.1 that a left *$R$-linear code* of length $n$ over the alphabet $A$ is a left $R$-submodule $C \subset A^n$. An important special case is when the alphabet $A$ equals $R$ itself.

Remember that the character group $\widehat{A}$ of $A$ admits a right $R$-module structure via $\varpi r(a) = \varpi(ra)$, for $r \in R$, $a \in A$, and $\varpi \in \widehat{A}$.

For an $R$-linear code $C \subset A^n$, the character-theoretic annihilator $(\widehat{A}^n : C) = \{\varpi \in \widehat{A}^n : \varpi(C) = 0\}$ is a right submodule of $\widehat{A}^n$.

**Proposition 12.1.** *The annihilator $(\widehat{A}^n : C)$ of an $R$-linear code $C \subset A^n$ satisfies*

*(1) $(\widehat{A}^n : C) \subset \widehat{A}^n$;*
*(2) $(\widehat{A}^n : C)$ is a right $R$-linear code of length $n$ in $\widehat{A}^n$;*
*(3) $(A^n : (\widehat{A}^n : C)) = C$;*
*(4) $|C| \cdot |(\widehat{A}^n : C)| = |A^n|$; and*

*(5) the MacWilliams identities hold:*

$$W_{(\widehat{A}^n:C)}(X,Y) = \frac{1}{|C|} W_C(X + (|A|-1)Y, X - Y).$$

The only drawback is that the annihilator $(\widehat{A}^n : C)$ is not a code over the original alphabet $A$. As was the case for additive codes, one way to remedy this drawback is to use nondegenerate bilinear forms. We will introduce bilinear forms in a very general context and then be more specific as we proceeed.

### 12.2. *Bilinear forms*

Let $R$ and $S$ be finite rings with 1, $A$ a finite left $R$-module, $B$ a finite right $S$-module, and $E$ a finite $(R,S)$-bimodule. In this context, a *bilinear form* is a map $\beta : A \times B \to E$ such that $\beta(a,\cdot) : B \to E$ is a right $S$-module homomorphism for all $a \in A$ and $\beta(\cdot,b) : A \to E$ is a left $R$-module homomorphism for all $b \in B$. Observe that $\beta$ induces two module homomorphisms:

$$\chi : A \to \mathrm{Hom}_S(B,E), \qquad \chi_a(b) = \beta(a,b), \quad a \in A, b \in B;$$
$$\psi : B \to \mathrm{Hom}_R(A,E), \qquad \psi_b(a) = \beta(a,b), \quad a \in A, b \in B.$$

The bilinear form $\beta$ is *nondegenerate* if both maps $\phi$ and $\psi$ are injective. Extend $\beta$ to $\beta : A^n \times B^n \to E$ by

$$\beta(a,b) = \sum_{j=1}^{n} \beta(a_j, b_j), \quad a = (a_1, \ldots, a_n) \in A^n, b = (b_1, \ldots, b_n) \in B^n.$$

For subsets $P \subset A^n$ and $Q \subset B^n$ we define annihilators:

$$l(Q) = \{a \in A^n : \beta(a,q) = 0, \text{ for all } q \in Q\},$$
$$r(P) = \{b \in B^n : \beta(p,b) = 0, \text{ for all } p \in P\}.$$

Observe that $l(Q)$ is a left submodule of $A^n$ and $r(P)$ is a right submodule of $B^n$. Also observe that $Q \subset r(l(Q))$ and $P \subset l(r(P))$, for $P \subset A^n$ and $Q \subset B^n$.

An important special case is the following example.

**Example 12.1.** Let $R = S$ and let $A = {}_RR$, $B = R_R$ and $E = {}_RR_R$. Define $\beta : R \times R \to R$ by $\beta(a,b) = ab$, where $ab \in R$ is the product in the ring $R$. Because $R$ has a unit element, $\beta$ is a nondegenerate bilinear form.

As above, if $P \subset R^n$, then $l(P)$ is a left submodule of $R^n$ and $r(P)$ is a right submodule of $R^n$. Moreover, if $P$ is also a left (resp., right) submodule of $R^n$, then $l(P)$ (resp., $r(P)$) is a sub-bimodule of $R^n$.

Comparing with the model Theorem 10.1, the annihilator $r(C)$ of a left linear code $C \subset R^n$ will indeed be a right linear code in $R^n$. However, we will need to be concerned about two other of the items in Theorem 10.1: the double annihilator property and the size property. In the next two subsections we examine these properties in more detail.

### 12.3. *The double annihilator property*

Continue to assume the conditions in Example 12.1, i.e., $\beta : R^n \times R^n \to R$ is the standard dot product given by

$$\beta(a, b) = \sum_{i=1}^{n} a_i b_i,$$

for $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n) \in R^n$, where $a_i b_i$ is the product in the ring $R$.

**Proposition 12.2.** *When $\beta : R^n \times R^n \to R$ is the standard dot product, the annihilators $l(D)$, $r(C)$ satisfy:*

*(1) If $C \subset R^n$ is a left submodule, then $C \subset l(r(C))$.*
*(2) If $D \subset R^n$ is a right submodule, then $D \subset r(l(D))$.*
*(3) Equality holds for all submodules $C$ and $D$ if and only if $R$ is a quasi-Frobenius ring.*

**Proof.** The first two containments are true even if $C$, $D$ are merely subsets of $R^n$. Now consider the last statement. In the case where $n = 1$, equality would mean that $C = l(r(C))$ and $D = r(l(D))$ for every left ideal $C$ and right ideal $D$ of $R$. In some texts, for example Ref. 13, Definition 58.5, this is the definition of a quasi-Frobenius ring. In Ref. 31, Theorem 15.1, the double annihilator condition is one of four equivalent conditions that serve to define a quasi-Frobenius ring.

For $n > 1$, the double annihilator condition holds over a quasi-Frobenius ring by a theorem of Hall, Ref. 23, Theorem 5.2. □

### 12.4. *The size condition*

We continue to assume that $\beta : R^n \times R^n \to R$ is the standard dot product over a finite ring $R$. Motivated by the previous subsection, we now assume that $R$ is a quasi-Frobenius ring as well.

First, the bad news.

**Theorem 12.1 (†).** *If $R$ is a quasi-Frobenius ring, but not a Frobenius ring, there exists a left ideal $I \subset R$ with $|I| \cdot |r(I)| < |R|$, and there exists a right ideal $J \subset R$ with $|J| \cdot |l(J)| < |R|$.*

**Proof.** As in the alternative proof of Theorem 6.1, if $R$ is not Frobenius, there exists an index $i$ and a value $k > \mu_i$ with $kT_i \subset \mathrm{soc}(R)$. The notation is as in Eq. (4) of Subsection 3.2. We set $I = T_i$, a simple left ideal of $R$. Because $T_i$ is the pullback to $R$ of the left $M_{\mu_i}(\mathbb{F}_{q_i})$-module $M_{\mu_i,1}(\mathbb{F}_{q_i})$, we have $|I| = q_i^{\mu_i}$. We now wish to understand $r(I)$.

Because $I = T_i$ is a simple module, it is generated by any non-zero element in $I$. Let $x \in I$ be a nonzero element, so that $I = Rx$. Consider $f_x : R \to R$ given by left multiplication by $x$: $f_x(r) = xr$, $r \in R$. Then $f_x$ is a homomorphism of right $R$-modules, and $r(I) = \ker(f_x)$, because $I = Rx$. It follows that $|r(I)| = |\ker(f_x)| = |R|/|\mathrm{im}\, f_x| = |R|/|xR|$.

As above, $kT_i \subset \mathrm{soc}(R)$. There is no loss of generality in assuming that $k$ is the largest integer with this property. As above, we can view $kT_i$ as the pullback to $R$ of the left $M_{\mu_i}(\mathbb{F}_{q_i})$-module $M_{\mu_i,k}(\mathbb{F}_{q_i})$. But this matrix module is also a right module over $S := M_k(\mathbb{F}_{q_i})$. Right multiplication by a matrix $B \in S$ defines a homomorphism $g_B : kT_i \to kT_i$ of left $R$-modules.

Because $R$ is a quasi-Frobenius ring, it is in particular self-injective. Thus the homomorphism $g_B : kT_i \to kT_i \subset R$ of left $R$-modules extends to a left endomorphism $g'_B : R \to R$. Because $R$ is a ring with 1, every left endomorphism of $R$ is given by right multiplication by an element of $R$. In particular, we have $xS \subset xR$ for any $x \in kT_i$.

Now we compute. Without loss of generality, we assume that $I$ represents the first column of $kT_i \cong M_{\mu_i,k}(\mathbb{F}_{q_i})$, and we take the nonzero element $x \in I$ to be the element with a 1 in the first row and first column and zeroes elsewhere. As above, $|Rx| = |I| = q_i^{\mu_i}$. Inside $M_{\mu_i,k}(\mathbb{F}_{q_i})$, $xS$ consists of all $\mu_i \times k$ matrices with zeroes everywhere in rows $2, \ldots, \mu_i$ (the entries in the first row are arbitrary). Thus $|xS| = q_i^k$. Because $xS \subset xR$, we have $|xS| \leq |xR|$.

Thus, $|r(I)| = |R|/|xR| \leq |R|/|xS| = |R|/q_i^k$, so that $|I| \cdot |r(I)| \leq |R|\, q_i^{\mu_i - k}$. Because $k > \mu_i$, we see that $|I| \cdot |r(I)| < |R|$, as claimed.

The statement for right ideals follows from left-right symmetry. □

**Corollary 12.1.** *The MacWilliams identites cannnot hold over a non-Frobenius ring $R$ using the standard dot product and $l(C)$ and $r(C)$ as the notions of dual codes.*

**Proof.** Consider the meaning of the MacWilliams identities for linear codes

of length 1, i.e., when the linear code $C \subset R$ is a left ideal. Clearly, $W_C(X,Y) = X + (|C|-1)Y$.

Then, the right side of the MacWilliams identities becomes

$$\begin{aligned}\frac{1}{|C|}W_C(X+(|R|-1)Y, X-Y) &\\ &= \frac{1}{|C|}(X+(|R|-1)Y+(|C|-1)(X-Y))\\ &= X+\left(\frac{|R|}{|C|}-1\right)Y.\end{aligned}$$

This latter equals the Hamming weight enumerator for $r(C)$ (or $l(C)$) if and only if $|C|\cdot|r(C)| = |R|$ (or $|C|\cdot|l(C)| = |R|$), which contradicts Theorem 12.1. □

### 12.5. *Generating characters*

For the good news, let us return to the general situation of a nondegenerate $\beta : {}_RA \times B_S \to {}_RE_S$. In the following theorem, there will be two forms, $\beta$ and $\beta'$. The annihilators with respect to $\beta$ will be denoted $r(C)$ and $l(D)$; the annihilators with respect to $\beta'$ will be denoted $r'(C)$ and $l'(D)$.

**Theorem 12.2 (†).** *Suppose $\beta : {}_RA \times B_S \to {}_RE_S$ is a nondegenerate bilinear form. Suppose there exists a character $\varrho : E \to \mathbb{Q}/\mathbb{Z}$ with the property that* $\ker\varrho$ *contains no nonzero left or right submodules.*

*Let $\beta' : A \times B \to \mathbb{Q}/\mathbb{Z}$ be given by $\beta' = \varrho\circ\beta$. Then*

*(1) $\beta'$ is a nondegenerate biadditive form on abelian groups;*
*(2) if $C \subset A^n$ is a left submodule, then $r(C) = r'(C)$;*
*(3) if $D \subset B^n$ is a right submodule, then $l(D) = l'(D)$;*
*(4) $l(r(C)) = C$ for left submodules $C \subset A^n$, and $r(l(D)) = D$ for right submodules $D \subset B^n$;*
*(5) $|C|\cdot|r(C)| = |A^n|$ and $|D|\cdot|l(D)| = |B^n|$;*
*(6) the MacWilliams identities hold for submodules using $r(C)$ and $l(D)$ as the notions of dual codes:*

$$W_{r(C)}(X,Y) = \frac{1}{|C|}W_C(X+(|A|-1)Y, X-Y),$$
$$W_{l(D)}(X,Y) = \frac{1}{|D|}W_D(X+(|B|-1)Y, X-Y).$$

**Proof.** In order to show that $\beta'$ is nondegenerate, suppose that $b \in B$ has the property that $\beta'(A,b) = 0$. We need to show that $b = 0$.

Let $\psi_b : A \to E$ be given by $\psi_b(a) = \beta(a, b)$, $a \in A$; $\psi_b$ is a homomorphism of left $R$-modules. By the hypothesis on $b$ and the definition of $\beta'$, we see that $\varrho(\psi_b(A)) = 0$; i.e., $\psi_b(A) \subset \ker \varrho$. But $\psi_b(A)$ is a left $R$-submodule of $E$, so the hypothesis on $\varrho$ implies that $\psi_b(A) = 0$. Because $\beta$ was assumed to be nondegenerate, we conclude that $b = 0$. A similar argument proves the nondegeneracy of $\beta'$ in the other variable.

If $C \subset A^n$ is a left $R$-submodule, then $\beta' = \varrho \circ \beta$ implies $r(C) \subset r'(C)$. Now suppose that $b \in r'(C)$, i.e., that $\beta'(C, b) = 0$. This implies that $\psi_b(C) = \beta(C, b) \subset \ker \varrho$. But $\psi_b(C)$ is a left $R$-submodule of $E$, so the hypothesis on $\varrho$ again implies that $\psi_b(C) = 0$. Thus $b \in r(C)$, and $r(C) = r'(C)$. The proof for $l(D)$ is similar.

The remaining items now follow from Proposition 11.3. It follows from the discussion in Subsection 11.3 that $A$ and $B$ are isomorphic *as abelian groups*. □

**Remark 12.1.** As mentioned in the Introduction, my interest in understanding the interplay between the annihilators $l(D)$, $r(C)$ defined with respect to a bilinear form $\beta$ and the annihilators $l'(D)$, $r'(C)$ defined with respect to a biadditive form $\beta'$ stems from the work of Nebe, Rains, and Sloane,[39] especially their Remark 1.8.5.

We will call a character $\varrho$ satisfying the hypothesis of Theorem 12.2 a *generating character*.

**Corollary 12.2.** *Over any finite ring $R$, the MacWilliams identities hold in the setting of a nondegenerate bilinear form $\beta : {}_RA \times B_R \to E$, where $E$ is a Frobenius bimodule.*

**Proof.** It follows from Lemmas 5.2 and 5.3 that a Frobenius bimodule admits a generating character. □

**Theorem 12.3.** *A finite ring is Frobenius if and only if it admits a generating character $\varrho$.*

**Proof.** This is a restatement of Theorem 5.3. □

**Corollary 12.3.** *Over a Frobenius ring $R$, the MacWilliams identities hold in the setting of a nondegenerate bilinear form $\beta : {}_RA \times B_R \to {}_RR_R$.*

To conclude this subsection we illustrate Corollary 12.2 by showing a natural pairing $\beta : {}_RA \times B_R \to \widehat{R}$ when $B = \widehat{A}$.

**Lemma 12.1 (Ref. 53, Remark 3.3).** *Let $M$ be a finite $R$-module. Then*

$$\widehat{M} \cong \mathrm{Hom}_R(M, \widehat{R}).$$

**Proof.** Writing characters in additive form, the definition of the module structure on $\widehat{M}$, i.e., $(\varpi r)(m) = \varpi(rm)$, for $\varpi \in \widehat{M}$, $m \in M$, $r \in R$, shows how $\varpi \in \widehat{M}$ defines an element in $\mathrm{Hom}_R(M, \widehat{R})$. The reader will check that this is an isomorphism. □

**Theorem 12.4 (†).** *Let $A$ be a finite left $R$-module, and let $B = \widehat{A} \cong \mathrm{Hom}_R(A, \widehat{R})$. The natural evaluation map*

$$\beta : A \times B \cong A \times \mathrm{Hom}_R(A, \widehat{R}) \to \widehat{R},$$

*is a nondegenerate bilinear form with values in a Frobenius bimodule. The MacWilliams identities hold in this setting.*

**Proof.** The form $\beta$ is nondegenerate because for every $a \in A$ there exists a character $\varpi \in \widehat{A}$ with $\varpi(a) \neq 0$. (This is the double dual property of characters: $G \cong (\widehat{G})\widehat{\ }$, from Proposition 2.1.) Corollary 12.2 implies that the MacWilliams identities hold. □

**Remark 12.2.** Assume that the ring $R$ admits an involution $\varepsilon$, i.e., an isomorphism $R \to R$ of abelian groups of order 2 with $\varepsilon(rs) = \varepsilon(s)\varepsilon(r)$, all $r, s \in R$. Also assume that the left $R$-module $A$ has the property that $\widehat{A} \cong A^{\varepsilon}$, where $A^{\varepsilon}$ is the abelian group $A$ considered as a right $R$-module by $xr = \varepsilon(r)x$, $x \in A$, $r \in R$. For a left linear code $C \subset A^n$, the right annihilator $r(C) \subset \widehat{A}^n$ defined via $\beta$ in Theorem 12.4 can be viewed as a left linear code $r(C)^{\varepsilon} \subset A^n$ by using the involution $\varepsilon$. This approach, due to Nebe, Rains, and Sloane,[39] allows one to study self-dual codes in the non-commutative setting.

### 12.6. *A degenerate case*

In the preceding subsections, many of the results have had the form: assume a "nondegeneracy" condition on the ground ring, and then conclude a result valid for *all* submodules. In this subsection we make no assumptions about the ground ring, and instead make hypotheses on the submodules.

The following result is due to Duursma and concerns the double annihilator property. For an $R$-module $M$, define the $R$-linear dual of $M$ by $M^{\sharp} := \mathrm{Hom}_R(M, R)$. The functor $\sharp$ interchanges sides, so that $M^{\sharp}$ is a right

$R$-module when $M$ is a left $R$-module, and vice versa. An $R$-module $M$ is *torsionless* if the natural map $M \to M^{\sharp\sharp}$ is injective. Duursma's theorem is that a linear code $C \subset R^n$ satisfies the double annihilator property if and only if the quotient module $M = R^n/C$ is torsionless. We use the notation from Subsection 12.3.

**Theorem 12.5 (Duursma[18]).** *Suppose $R$ is a finite ring and $C \subset R^n$ is a left linear code. Let $M = R^n/C$ be the quotient module associated to $C$. Then $l(r(C)) = C$ if and only if the quotient module $M$ is torsionless. In that case, the right annihilator $D = r(C)$ satisfies $r(l(D)) = D$, as well.*

*Similarly, when $D \subset R^n$ is a right linear code, $r(l(D)) = D$ if and only if $R^n/D$ is torsionless. In that case, the left annihilator $C = l(D)$ satisfies $l(r(C)) = C$.*

**Proof.** Adapt Ref. 31, Exercise 15.6, to the setting of $C \subset R^n$. □

Over a quasi-Frobenius ring, $R^n/C$ is always torsionless (Ref. 31, Theorem 15.11), so that Proposition 12.2 follows from Theorem 12.5.

## 13. Other weight enumerators

In this section we discuss two other weight enumerators, the full weight enumerator and the complete weight enumerator. In discussing these two weight enumerators, we follow, in part, the treatment of this material by Nebe, Rains, and Sloane.[39] We also make use of some of the notation introduced by Byrne, Greferath, and O'Sullivan,[8] who in turn built on results of Honold and Landjev.[28]

### 13.1. *Full weight enumerators*

Let $G$ be a finite abelian group. The full weight enumerator of a code $C \subset G^n$ is essentially a copy of the code inside the complex group ring $\mathbb{C}[G^n]$. Recall that the complex group ring $\mathbb{C}[G^n]$ is the set of all formal complex linear combinations of elements of $G^n$. One way to notate $\mathbb{C}[G^n]$ is to introduce formal symbols $e_x$ for every $x \in G^n$. Then an element of $\mathbb{C}[G^n]$ has the form

$$\sum_{x \in G^n} \alpha_x e_x,$$

where $\alpha_x \in \mathbb{C}$. Addition in $\mathbb{C}[G^n]$ is performed term-wise: $\sum \alpha_x e_x + \sum \beta_x e_x = \sum (\alpha_x + \beta_x) e_x$. Multiplication is as for polynomials, using the

rule $e_x e_y = e_{x+y}$, where the latter is the formal symbol associated to the sum $x + y$ in the group $G^n$.

Let $f : G^n \to \mathbb{C}[G^n]$ be any function from $G^n$ to $\mathbb{C}[G^n]$. In terms of the basis of $e_x$, $x \in G^n$, the function $f$ has the form

$$f(x) = \sum_{y \in G^n} \mathcal{B}_{x,y} e_y, \quad \mathcal{B}_{x,y} \in \mathbb{C}.$$

The Fourier transform of $f$ is then $\hat{f} : \widehat{G}^n \to \mathbb{C}[G^n]$,

$$\hat{f}(\pi) = \sum_{x \in G^n} \pi(x) f(x) = \sum_{y \in G^n} \left( \sum_{x \in G^n} \pi(x) \mathcal{B}_{x,y} \right) e_y.$$

For any subset $C \subset G^n$ and any function $f : G^n \to \mathbb{C}[G^n]$, define the *full weight enumerator of $C$ with respect to $f$* by $\mathrm{fwe}_C(f) = \sum_{x \in C} f(x)$. Then the Poisson summation formula implies

$$\mathrm{fwe}_C(f) = \frac{1}{|(\widehat{G}^n : C)|} \mathrm{fwe}_{(\widehat{G}^n : C)}(\hat{f}).$$

In the special case where the function $f$ is $e : G^n \to \mathbb{C}[G^n]$, $e(x) = e_x$, the Fourier transform has the form $\hat{e}(\pi) = \sum_{x \in G^n} \pi(x) e_x$, and we have the following version of the MacWilliams identities for the full weight enumerator (with respect to $e$).

**Theorem 13.1.** *For any additive code $C \subset G^n$, the full weight enumerator satisfies the following MacWilliams identities:*

$$\mathrm{fwe}_C(e) = \frac{1}{|(\widehat{G}^n : C)|} \mathrm{fwe}_{(\widehat{G}^n : C)}(\hat{e}).$$

When $G$ is equipped with a nondegenerate biadditive form $\beta : G \times G \to \mathbb{Q}/\mathbb{Z}$, we can make use of the identifications of Proposition 11.3. Using the notation of Subsection 11.3, if we use $\chi : G \to \widehat{G}$, $\chi(x) = \beta(x, -)$, to make identifications, then the Fourier transform of $e$ is

$$\hat{e}_\chi(x) = \sum_{y \in G^n} \exp(2\pi i \beta(x, y))\, e_y, \quad x \in G^n.$$

The MacWilliams identities then become

$$\mathrm{fwe}_C(e) = \frac{1}{|l(C)|} \mathrm{fwe}_{l(C)}(\hat{e}_\chi). \tag{18}$$

Similarly, if one uses instead $\psi : G \to \widehat{G}$, $\psi(x) = \beta(-, x)$, to make identifications, then one has

$$\hat{e}_\psi(x) = \sum_{y \in G^n} \exp(2\pi i \beta(y, x))\, e_y, \quad x \in G^n.$$

The MacWilliams identities in this case take the form

$$\mathrm{fwe}_C(e) = \frac{1}{|r(C)|}\,\mathrm{fwe}_{r(C)}(\hat{e}_\psi). \tag{19}$$

### 13.2. *Complete weight enumerators*

The complete weight enumerator will be an element of a certain polynomial ring, which we now define. For every $x \in G$, let $Z_x$ be an indeterminate. Form the polynomial ring on these indeterminates: $\mathbb{C}[Z_x : x \in G]$. We will write $\mathbb{C}[(Z_\bullet)]$ for short.

Given a code $C \subset G^n$, the *complete weight enumerator* of $C$ is

$$\mathrm{cwe}_C((Z_\bullet)) = \sum_{x\in C}\prod_{i=1}^{n} Z_{x_i} = \sum_{x\in C}\prod_{y\in G} Z_y^{c_y(x)} \in \mathbb{C}[(Z_\bullet)],$$

where $c_y(x) = |\{i : x_i = y\}|$ counts the number of components of $x \in G^n$ that equal the element $y \in G$.

A linear change of variables can be specified by $Z_x \mapsto \sum_{y\in G} B_{x,y}Z_y$, where $B$ is a matrix of size $|G| \times |G|$ whose rows and columns are parameterized by the elements of $G$. Such a linear change of variables induces a homomorphism of $\mathbb{C}$-algebras $M_B : \mathbb{C}[(Z_\bullet)] \to \mathbb{C}[(Z_\bullet)]$ via $M_B(Z_x) = \sum_{y\in G} B_{x,y}Z_y$.

We would now like to compare the full weight enumerator with the complete weight enumerator. A $\mathbb{C}$-linear transformation of vector spaces $S : \mathbb{C}[G^n] \to \mathbb{C}[(Z_\bullet)]$ ("specialization") is completely determined by defining $S(e_x) = \prod_{j=1}^{n} Z_{x_j}$, for $x = (x_1, x_2, \ldots, x_n) \in G^n$. In particular, notice that $S(\mathrm{fwe}_C(e)) = \mathrm{cwe}_C((Z_\bullet))$.

As in the previous subsection, let $G$ be equipped with a nondegenerate biadditive form $\beta : G \times G \to \mathbb{Q}/\mathbb{Z}$, and use $\chi : G \to \widehat{G}$, $\chi(x) = \beta(x, -)$, to make identifications, so that

$$\hat{e}_\chi(x) = \sum_{y\in G^n} \exp(2\pi i\beta(x, y))\, e_y, \quad x \in G^n.$$

For any subgroup $D \subset G^n$, a computation shows that $S(\mathrm{fwe}_D(\hat{e}_\chi)) = M_B(\mathrm{cwe}_D((Z_\bullet)))$, where the matrix $B$ is given by

$$B_{x,y} = \exp(2\pi i\beta(x, y)), \quad x, y \in G. \tag{20}$$

By applying $S : \mathbb{C}[G^n] \to \mathbb{C}[(Z_\bullet)]$ to the MacWilliams identities for the full weight enumerator, Eq. (18) of Subsection 13.1, we obtain the MacWilliams identities for the complete weight enumerator:

$$\mathrm{cwe}_C((Z_\bullet)) = \frac{1}{|l(C)|} M_B(\mathrm{cwe}_{l(C)}((Z_\bullet))). \tag{21}$$

If one uses instead $\psi : G \to \widehat{G}$, $\psi(x) = \beta(-, x)$, to make identifications, then $B$ of Eq. (20) is replaced by its transpose $B^t$, and the MacWilliams identities take the form:

$$\mathrm{cwe}_C((Z_\bullet)) = \frac{1}{|r(C)|} M_{B^t}(\mathrm{cwe}_{r(C)}((Z_\bullet))). \tag{22}$$

Finally, by mapping $Z_0$ to $X$ and mapping all the other $Z_y$, $y \neq 0$, to $Y$, one induces a specialization map from $\mathbb{C}[(Z_\bullet)]$ to $\mathbb{C}[X, Y]$, which takes $\mathrm{cwe}_C((Z_\bullet))$ to the Hamming weight enumerator $W_C(X, Y)$. A computation using Lemma 11.1 shows that $M_B(\mathrm{cwe}_C((Z_\bullet)))$ specializes to $W_C(X+(|G|-1)Y, X-Y)$, where $B$ is given in Eq. (20). In this way, the MacWilliams identities for Hamming weight can be deduced from those for the complete weight enumerator.

**Remark 13.1.** It is possible to define other weight enumerators called *symmetrized weight enumerators*. The MacWilliams identities for these symmetrized weight enumerators (in special situations) first appeared in Ref. 53, Theorem 8.4. More general situations in which the MacWilliams identities hold have been studied by Byrne, Greferath, and O'Sullivan[8] and by Honold and Landjev.[28]

### 13.3. *A degenerate case*

The final result can be viewed as a degenerate version of Theorem 12.2. It has been adapted from a result of Klemm (Ref. 29, Satz 1.2).

**Theorem 13.2.** *Let $R$ be a finite ring, and let $\beta : R^n \times R^n \to R$ be the standard dot product. Suppose $\varrho$ is any character on $R$, $\varrho : R \to \mathbb{Q}/\mathbb{Z}$. Let $\beta' : R^n \times R^n \to \mathbb{Q}/\mathbb{Z}$ be given by $\beta' = \varrho \circ \beta$. For left submodules $C \subset R^n$ and right submodules $D \subset R^n$, the MacWilliams identities hold in the following form:*

$$\mathrm{cwe}_{r'(C)}((Z_\bullet)) = \frac{1}{|C|} M_P(\mathrm{cwe}_C((Z_\bullet))),$$
$$\mathrm{cwe}_{l'(D)}((Z_\bullet)) = \frac{1}{|D|} M_{P^t}(\mathrm{cwe}_D((Z_\bullet))),$$

*where $P$ is the matrix of size $|R| \times |R|$ with rows and columns parameterized by elements of $R$ and $P_{r,s} = \rho(rs)$.*

**Proof.** Use Theorem 11.2 twice, with $\tau = \chi'$ and $\tau = \psi'$, where $\chi' : R^n \to \widehat{R}^n$ is $\chi'_a(b) = \beta'(a, b)$ and $\psi' : R^n \to \widehat{R}^n$ is $\psi'_b(a) = \beta'(a, b)$. □

**Remark 13.2.** In general, $\beta'$ will be degenerate, so the double annihilator condition will not be satisfied. Thus one cannot reverse the roles of $r'(C)$ and $C$ in the theorem.

## Acknowledgments

In addition to repeating my thanks to the organizers and sponsors of the summer school, I want to acknowledge and thank many friends and colleagues who provided encouragement and valuable insights over the years: Dave Benson, Hai Dinh, Iwan Duursma, Marcus Greferath, Thomas Honold, Cary Huffman, T. Y. Lam, Sergio López-Permouth, Gabriele Nebe, Alexandr Nechaev, Vera Pless, Neil Sloane, Thann Ward, and the late Ed Assmus. I thank the referee for a number of valuable suggestions for improving this paper and Ryan Schwiebert for pointing out an error in an earlier form of Lemma 5.2. And, I especially want to thank my wife Elizabeth Moore for her unwavering support.

## References

1. G. E. Andrews, *The theory of partitions*, Encyclopedia of Mathematics and its Applications, vol. 2, Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, Reading, Mass., 1976. MR MR0557013 (58 #27738)
2. E. F. Assmus, Jr. and H. F. Mattson, Jr., *Error-correcting codes: An axiomatic approach*, Inform. and Control **6** (1963), 315–330. MR MR0178997 (31 #3251)
3. ———, *Coding and combinatorics*, SIAM Rev. **16** (1974), 349–388. MR MR0359982 (50 #12432)
4. H. Bass, *$K$-theory and stable algebra*, Inst. Hautes Études Sci. Publ. Math. **22** (1964), 5–60. MR MR0174604 (30 #4805)
5. I. F. Blake, *Codes over certain rings*, Inform. and Control **20** (1972), 396–404. MR MR0323440 (48 #1796)
6. ———, *Codes over integer residue rings*, Inform. and Control **29** (1975), no. 4, 295–300. MR MR0434607 (55 #7572)
7. K. Bogart, D. Goldberg, and J. Gordon, *An elementary proof of the MacWilliams theorem on equivalence of codes*, Inform. and Control **37** (1978), no. 1, 19–22. MR MR0479646 (57 #19067)
8. E. Byrne, M. Greferath, and M. E. O'Sullivan, *The linear programming bound for codes over finite Frobenius rings*, Des. Codes Cryptogr. **42** (2007), no. 3, 289–301. MR MR2298938 (2008c:94053)
9. A. E. Clark and D. A. Drake, *Finite chain rings*, Abh. Math. Sem. Univ. Hamburg **39** (1973), 147–153. MR MR0332875 (48 #11200)
10. I. Constantinescu, *Lineare Codes über Restklassringen ganzer Zahlen und ihre Automorphismen bezüglich einer verallgemeinerten Hamming-Metrik*, Ph.D. thesis, Techniche Universität, München, München, 1995.

11. I. Constantinescu and W. Heise, *A metric for codes over residue class rings of integers*, Problemy Peredachi Informatsii **33** (1997), no. 3, 22–28. MR MR1476368 (99a:94058)
12. I. Constantinescu, W. Heise, and T. 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.
13. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Pure and Applied Mathematics, vol. XI, Interscience Publishers, a division of John Wiley & Sons, New York, London, 1962. MR MR0144979 (26 #2519)
14. P. Delsarte, *Bounds for unrestricted codes, by linear programming*, Philips Res. Rep. **27** (1972), 272–289. MR MR0314545 (47 #3096)
15. H. Q. Dinh and S. R. López-Permouth, *On the equivalence of codes over finite rings*, Appl. Algebra Engrg. Comm. Comput. **15** (2004), no. 1, 37–50. MR MR2142429 (2006d:94097)
16. ———, *On the equivalence of codes over rings and modules*, Finite Fields Appl. **10** (2004), no. 4, 615–625. MR MR2094161 (2005g:94098)
17. S. Dodunekov and J. Simonis, *Codes and projective multisets*, Electron. J. Combin. **5** (1998), no. 1, Research Paper 37, 23 pp. (electronic). MR 99m:94041
18. I. Duursma, *MacWilliams duality for cosets over rings*, preliminary report at AMS meeting, Evanston, IL, October 23, 2004.
19. D. Y. Goldberg, *A generalized weight for linear codes and a Witt-MacWilliams theorem*, J. Combin. Theory Ser. A **29** (1980), no. 3, 363–367. MR MR600600 (82e:94052)
20. M. Greferath, *Orthogonality matrices for modules over finite Frobenius rings and MacWilliams' equivalence theorem*, Finite Fields Appl. **8** (2002), no. 3, 323–331. MR MR1910395 (2003d:94107)
21. M. Greferath, A. Nechaev, and R. Wisbauer, *Finite quasi-Frobenius modules and linear codes*, J. Algebra Appl. **3** (2004), no. 3, 247–272. MR MR2096449 (2005g:94099)
22. M. Greferath and S. E. Schmidt, *Finite-ring combinatorics and MacWilliams's equivalence theorem*, J. Combin. Theory Ser. A **92** (2000), no. 1, 17–28. MR MR1783936 (2001j:94045)
23. M. Hall, *A type of algebraic closure*, Ann. of Math. (2) **40** (1939), no. 2, 360–369. MR MR1503463
24. P. Hall, *The Eulerian functions of a group*, Quart. J. Math. **7** (1936), 134–151.
25. 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.
26. W. Heise, T. Honold, and A. A. Nechaev, *Weighted modules and representations of codes*, Proceedings of the Sixth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT '98) (Pskov, Russia), 1998, pp. 123–129.

27. T. Honold, *Characterization of finite Frobenius rings*, Arch. Math. (Basel) **76** (2001), no. 6, 406–415. MR MR1831096 (2002b:16033)
28. T. Honold and I. Landjev, *MacWilliams identities for linear codes over finite Frobenius rings*, Finite fields and applications (Augsburg, 1999) (D. Jungnickel and H. Niederreiter, eds.), Springer, Berlin, 2001, pp. 276–292. MR MR1849094 (2002i:94066)
29. M. Klemm, *Selbstduale Codes über dem Ring der ganzen Zahlen modulo* 4, Arch. Math. (Basel) **53** (1989), no. 2, 201–207. MR MR1004279 (91a:94031)
30. V. L. Kurakin, A. S. Kuzmin, V. T. Markov, A. V. Mikhalev, and A. A. Nechaev, *Linear codes and polylinear recurrences over finite rings and modules (a survey)*, Applied algebra, algebraic algorithms and error-correcting codes (Honolulu, HI, 1999) (M. Fossorier, H. Imai, S. Lin, and A. Poli, eds.), Lecture Notes in Comput. Sci., vol. 1719, Springer, Berlin, 1999, pp. 365–391. MR MR1846512 (2002h:94092)
31. T. Y. Lam, *Lectures on modules and rings*, Graduate Texts in Mathematics, vol. 189, Springer-Verlag, New York, 1999. MR MR1653294 (99i:16001)
32. ———, *A first course in noncommutative rings*, second ed., Graduate Texts in Mathematics, vol. 131, Springer-Verlag, New York, 2001. MR MR1838439 (2002c:16001)
33. J. H. van Lint and R. M. Wilson, *A course in combinatorics*, Cambridge University Press, Cambridge, 1992. MR MR1207813 (94g:05003)
34. S. Mac Lane, *Categories for the working mathematician*, second ed., Graduate Texts in Mathematics, vol. 5, Springer-Verlag, New York, 1998. MR MR1712872 (2001j:18001)
35. F. J. MacWilliams, *Error-correcting codes for multiple-level transmission*, Bell System Tech. J. **40** (1961), 281–308. MR MR0141541 (25 #4945)
36. ———, *Combinatorial properties of elementary abelian groups*, Ph.D. thesis, Radcliffe College, Cambridge, Mass., 1962.
37. ———, *A theorem on the distribution of weights in a systematic code*, Bell System Tech. J. **42** (1963), 79–94. MR MR0149978 (26 #7462)
38. F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland Publishing Co., Amsterdam, 1977, North-Holland Mathematical Library, Vol. 16. MR MR0465509 (57 #5408a)
39. G. Nebe, E. M. Rains, and N. J. A. Sloane, *Self-dual codes and invariant theory*, Algorithms and Computation in Mathematics, vol. 17, Springer-Verlag, Berlin, 2006. MR MR2209183 (2007d:94066)
40. W. W. Peterson, *Error-correcting codes*, The MIT Press, Cambridge, Mass. 1961.
41. W. W. Peterson and E. J. Weldon, Jr., *Error-correcting codes*, 2 ed., The M.I.T. Press, Cambridge, Mass.-London, 1972. MR 49 #12164
42. L. Pontrjagin, *Topological Groups*, Princeton Mathematical Series, vol. 2, Princeton University Press, Princeton, 1939. MR MR0000265 (1,44e)
43. L. S. Pontryagin, *Selected works*, third ed., Classics of Soviet Mathematics, vol. 2, Gordon & Breach Science Publishers, New York, 1986. MR MR898007 (90a:01106)
44. J.-P. Serre, *Linear representations of finite groups*, Graduate Texts in Math-

ematics, vol. 42, Springer-Verlag, New York, Heidelberg, Berlin, 1977.
45. E. Spiegel, *Codes over $Z_m$*, Inform. and Control **35** (1977), no. 1, 48–51. MR MR0446721 (56 #5045)
46. ———, *Codes over $Z_m$, revisited*, Inform. and Control **37** (1978), no. 1, 100–104. MR MR0479661 (57 #19082)
47. Richard P. Stanley, *Enumerative combinatorics*, The Wadsworth & Brooks/Cole Mathematics Series, vol. I, Wadsworth & Brooks/Cole Advanced Books & Software, Monterey, CA, 1986. MR MR847717 (87j:05003)
48. A. Terras, *Fourier analysis on finite groups and applications*, London Mathematical Society Student Texts, vol. 43, Cambridge University Press, Cambridge, 1999. MR MR1695775 (2000d:11003)
49. M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-geometric codes*, Mathematics and its Applications (Soviet Series), vol. 58, Kluwer Academic Publishers Group, Dordrecht, 1991. MR 93i:94023
50. H. N. Ward and J. A. Wood, *Characters and the equivalence of codes*, J. Combin. Theory Ser. A **73** (1996), no. 2, 348–352. MR MR1370137 (96i:94028)
51. S. K. Wasan, *On codes over $Z_m$*, IEEE Trans. Inform. Theory **28** (1982), no. 1, 117–120. MR MR651113 (83f:94037)
52. J. A. Wood, *Extension theorems for linear codes over finite rings*, Applied algebra, algebraic algorithms and error-correcting codes (Toulouse, 1997) (T. Mora and H. Mattson, eds.), Lecture Notes in Comput. Sci., vol. 1255, Springer, Berlin, 1997, pp. 329–340. MR MR1634126 (99h:94062)
53. ———, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math. **121** (1999), no. 3, 555–575. MR MR1738408 (2001d:94033)
54. ———, *Weight functions and the extension theorem for linear codes over finite rings*, Finite fields: theory, applications, and algorithms (Waterloo, ON, 1997) (R. C. Mullin and G. L. Mullen, eds.), Contemp. Math., vol. 225, Amer. Math. Soc., Providence, RI, 1999, pp. 231–243. MR MR1650644 (2000b:94024)
55. ———, *Factoring the semigroup determinant of a finite chain ring*, Coding Theory, Cryptography and Related Areas (J. Buchmann, T. Høholdt, H. Stichtenoth, and H. Tapia-Recillas, eds.), Springer, Berlin, 2000, pp. 249–259.
56. ———, *The structure of linear codes of constant weight*, Trans. Amer. Math. Soc. **354** (2002), no. 3, 1007–1026. MR MR1867370 (2002k:94042)
57. ———, *Code equivalence characterizes finite Frobenius rings*, Proc. Amer. Math. Soc. **136** (2008), 699–706.