J. Algebra Comb. Discrete Appl.
4(2) • 105–113

Received: 12 June 2015
Accepted: 8 February 2016

Journal of Algebra Combinatorics Discrete Structures and Applications

Properties of dual codes defined by nondegenerate forms

Research Article

Steve Szabo, Jay A. Wood

Abstract: Dual codes are defined with respect to non-degenerate sesquilinear or bilinear forms over a finite Frobenius ring. These dual codes have the properties one expects from a dual code: they satisfy a double-dual property, they have cardinality complementary to that of the primal code, and they satisfy the MacWilliams identities for the Hamming weight.

2010 MSC: 94B05, 15A63

Keywords: Frobenius ring, Sesquilinear form, Bilinear form, Dual code, Generating character, MacWilliams identities

1. Introduction and overview

One of the topics discussed in the Mini-cours at the Lens conference in 2015 was dual codes and the MacWilliams identities for linear codes defined over finite rings. In those lectures two notions of duality were used: (1) left and right annihilators defined by the standard dot product and (2) the character-theoretic annihilator. A key idea for proving useful properties of duality, including the cardinality of dual codes and the MacWilliams identities, is to establish an identification between these two notions of annihilators. This can be accomplished over finite Frobenius rings.

As researchers expand their studies of linear codes over finite rings, questions naturally arise concerning the behavior of dual codes defined using more general inner products than just the standard dot product. This paper begins to address these questions.

Our main goal is to prove a "model theorem" that captures the main features of a dual code. Such a model theorem is proved in [7, Sections 10–12], first in the context of character-theoretic annihilators over any ring, and then in the context of the standard dot product over a finite Frobenius ring. The dual code is proved to have a module structure if the code does, to satisfy a double-dual property, to

Steve Szabo; Department of Mathematics and Statistics, Eastern Kentucky University, Richmond, KY 40475 USA (email: steve.szabo@eku.edu).
Jay A. Wood (Corresponding Author); Department of Mathematics, Western Michigan University, Kalamazoo, MI 49008 USA (email: jay.wood@wmich.edu).

http://dx.doi.org/10.13069/jacodesmath.284934

ISSN 2148-838X

have cardinality complementary to that of the code, and to satisfy the MacWilliams identities for the Hamming weight enumerator. In this paper, we show the same results over a finite Frobenius ring for non-degenerate sesquilinear forms (with respect to an anti-automorphism of the ring) and for non-degenerate bilinear forms.

2. Preliminaries

In this section we collect several definitions that will be used throughout the paper.

For a ring A, a subset C of A^n is a **code** of length n over A. If C is an additive subgroup of A^n, then C is an **additive** code over A, and if C is a left (right) A-submodule of A^n, then C is a left (right) **linear code** over A. We will usually state results only for left linear codes, but there are always versions of those results that apply to right linear codes.

If G is a finite abelian group, a **character** of G is a group homomorphism $\pi : G \to \mathbb{C}^\times$, the multiplicative group of nonzero complex numbers. The set of all characters of G is denoted $\widehat{G}$, and $\widehat{G}$ is itself a finite abelian group under pointwise multiplication of functions: $(\pi_1\pi_2)(g) = \pi_1(g)\pi_2(g)$, for $g \in G$. The groups G and $\widehat{G}$ are isomorphic; in particular, $|G| = |\widehat{G}|$.

In particular, the definition of characters applies to the additive groups of finite rings and finite modules. We will always assume that our finite rings have a multiplicative identity 1 and that all modules are unitary. If M is a finite left module over a finite ring A, then $\widehat{M}$ is a right A-module with right scalar multiplication of $\pi \in \widehat{M}$ by $a \in A$ denoted by π^a; $\pi^a(m) = \pi(am)$ for $m \in M$. We use the exponential notation so that the distributive law for the right A-module $\widehat{M}$ (i.e., right scalar multiplication distributing over the "addition" given by pointwise multiplication) reads $(\pi_1\pi_2)^a = \pi_1^a\pi_2^a$. Similarly, if N is a finite right A-module, then $\widehat{N}$ is a left A-module under ${}^a\pi(n) = \pi(na)$ for $a \in A$, $n \in N$, and $\pi \in \widehat{N}$. If B is a finite bimodule over A, then $\widehat{B}$ is also a bimodule over A. In particular, $\widehat{A}$ is a bimodule over A.

Suppose M is a finite left A-module and $\pi \in \widehat{M}$ is a character of M. The right scalar multiplication defines a homomorphism of right A-modules $A \to \widehat{M}$ by $a \mapsto \pi^a$. We say that π is a **generating character** of M if this homomorphism is surjective (so that π generates $\widehat{M}$ as a right A-module). A character $\pi \in \widehat{M}$ of M is a generating character if and only if $\ker \pi \subseteq M$ contains no nonzero left A-submodules [9, dual of Proposition 12].

We will often assume that a finite ring is Frobenius. There are several equivalent definitions of Frobenius rings [4, Theorem 16.14], and we will say that a *finite* ring A is **Frobenius** if there exists a character $\rho \in \widehat{A}$ of A that is a generating character of A, both as a left A-module and as a right A-module. In fact, for a finite ring A, a character $\rho \in \widehat{A}$ is a left generating character of A if and only if ρ is a right generating character of A. See [6, Sections 3 and 4] for more details. For later use, we state two lemmas, the first of which dates from [1].

Lemma 2.1 ([1, Corollary 3.6])**.** *Let A be a finite ring. A character ρ of A is a generating character if and only if* $\ker \rho$ *contains no nonzero one-sided ideals.*

Lemma 2.2. *Let $\rho \in \widehat{A}$ be a generating character of A. For every $a_1 \in A$, there exists $a_2 \in A$ such that ${}^{a_1}\rho = \rho^{a_2}$. Likewise, for every $a_3 \in A$, there exists $a_4 \in A$ such that $\rho^{a_3} = {}^{a_4}\rho$.*

Proof. For any $a_1 \in A$, ${}^{a_1}\rho$ belongs to $\widehat{A}$. But the homomorphism of right A-modules $A \to \widehat{A}$, $a \mapsto \rho^a$, is surjective. Thus there exists $a_2 \in A$ with $\rho^{a_2} = {}^{a_1}\rho$, as desired. The proof of the other case is similar, using the homomorphism $a \mapsto {}^a\rho$ of left A-modules. □

3. Sesquilinear forms

For a ring A, an anti-automorphism σ on A and a left A-module M, a **σ-sesquilinear form** on M is a map $\langle\cdot,\cdot\rangle : M \times M \to A$ such that if $x, y, z \in M$ and $a \in A$, then $\langle x+z, y\rangle = \langle x, y\rangle + \langle z, y\rangle$, $\langle x, y+z\rangle = \langle x, y\rangle + \langle x, z\rangle$, $\langle ax, y\rangle = a\langle x, y\rangle$ and $\langle x, ay\rangle = \langle x, y\rangle\sigma(a)$. In addition, if $\sigma(\langle x, y\rangle) = \langle y, x\rangle$, then the form is called a **σ-hermitian form**. A σ-sesquilinear form with the property that $\langle x, y\rangle = 0 \iff \langle y, x\rangle = 0$ is called **reflexive**. Clearly a σ-hermitian form is reflexive. A σ-sesquilinear form is called **non-degenerate** if $\langle x, y\rangle = 0$ for all $y \in M$ implies $x = 0$ and $\langle y, x\rangle = 0$ for all $y \in M$ implies $x = 0$.

Proposition 3.1. *Let A be a ring and σ be an anti-automorphism on A. Define the map*

$$\langle\cdot,\cdot\rangle : A^k \times A^k \to A, \quad \langle x, y\rangle = \sum_{i=1}^{k} x_i\sigma(y_i),$$

where $x = (x_1, x_2, \ldots, x_k)$, $y = (y_1, y_2, \ldots, y_k) \in A^k$. Then $\langle\cdot,\cdot\rangle$ is a σ-sesquilinear form. Furthermore, $\langle\cdot,\cdot\rangle$ is a σ-hermitian form if and only if σ is involutory.

Moreover, $\langle xa, y\rangle = \left\langle x, y\sigma^{-1}(a)\right\rangle$, for all $x, y \in A^k$ and $a \in A$.

Proof. Clearly, $\langle\cdot,\cdot\rangle$ is a σ-sesquilinear form. Assume $\langle\cdot,\cdot\rangle$ is hermitian. For $a \in A$,

$$a = a\left\langle(1, 0, \ldots, 0), (1, 0, \ldots, 0)\right\rangle = \left\langle(a, 0, \ldots, 0), (1, 0, \ldots, 0)\right\rangle.$$

Since $\langle\cdot,\cdot\rangle$ is hermitian, $\sigma^2(a) = \sigma^2(\langle(a, 0, \ldots, 0), (1, 0, \ldots, 0)\rangle) = a$, showing σ is involutory.

Now, assume σ is involutory. For $x, y \in A^k$,

$$\sigma(\langle x, y\rangle) = \sigma(\sum_{i=1}^{k} x_i\sigma(y_i)) = \sum_{i=1}^{k} \sigma(x_i\sigma(y_i)) = \sum_{i=1}^{k} y_i\sigma(x_i) = \langle y, x\rangle,$$

showing $\langle\cdot,\cdot\rangle$ is σ-hermitian. The final identity is a straight-forward verification left for the reader. □

For the rest of the section, let n be a natural number, A be a finite Frobenius ring, ρ be a generating character of A, σ be an anti-automorphism on A, and $\langle\cdot,\cdot\rangle$ be a non-degenerate σ-sesquilinear form on A^n.

For any code (linear or not) $C \subseteq A^n$, the left and right **dual codes** of C, denoted by $l(C)$ and $r(C)$, are

$$l(C) = \{v \in A^n : \langle v, C\rangle = 0\} \text{ and } r(C) = \{v \in A^n : \langle C, v\rangle = 0\},$$

and the left and right **ρ-character dual codes** of C, denoted by $l_\rho(C)$ and $r_\rho(C)$, are

$$l_\rho(C) = \{v \in A^n : \rho(\langle v, C\rangle) = 1\},$$
$$r_\rho(C) = \{v \in A^n : \rho(\langle C, v\rangle) = 1\}.$$

It is immediate that $l(C)$ and $r(C)$ are left A-submodules of A^n, and $l_\rho(C)$ and $r_\rho(C)$ are additive subgroups of A^n.

In fact, $l(C) = l(AC)$ and $r(C) = r(AC)$, where AC is the left A-module generated by C, while $l_\rho(C) = l_\rho(\mathbb{Z}C)$ and $r_\rho(C) = r_\rho(\mathbb{Z}C)$, where $\mathbb{Z}C$ is the additive group generated by C. (It need not be true that $l_\rho(AC) = l_\rho(\mathbb{Z}C)$. Let $A = \mathbb{F}_4$ and $C = \mathbb{F}_2 \subset \mathbb{F}_4$; $C = \mathbb{Z}C$ is an additive subgroup but not an ideal. Of course, $AC = \mathbb{F}_4$, and $l_\rho(C) = \mathbb{F}_2$, while $l_\rho(AC) = \{0\}$.)

As noted earlier, every hermitian form is reflexive; thus $l(C) = r(C)$ when the form is hermitian. When C is a left A-linear code, the following lemma shows that $l_\rho(C)$ and $r_\rho(C)$ are left A-modules as well.

Lemma 3.2. *Let $C \subseteq A^n$ be a left A-linear code over a finite Frobenius ring A. Then $l_\rho(C)$ and $r_\rho(C)$ are left A-modules.*

Proof. We prove the $l_\rho(C)$ case; the $r_\rho(C)$ case is similar. Let $x \in l_\rho(C)$ and $r \in A$. By Lemma 2.2, there exists $s \in A$ with $\rho^r = {}^s\rho$. Then

$$\begin{aligned}\rho(\langle rx, C\rangle) &= \rho(r\langle x, C\rangle) = \rho^r(\langle x, C\rangle) = {}^s\rho(\langle x, C\rangle)\\ &= \rho(\langle x, C\rangle s) = \rho(\langle x, \sigma^{-1}(s)C\rangle) = 1.\end{aligned}$$

□

Lemma 3.3. *Let $C \subseteq A^n$ be a left A-linear code over a finite Frobenius ring A. Then $l(C) = l_\rho(C)$ and $r(C) = r_\rho(C)$.*

Proof. Clearly, $l(C) \subseteq l_\rho(C)$. Let $x \in l_\rho(C)$, so that $\langle x, C\rangle \subseteq \ker\rho$. For $c \in C$ and $a \in A$, $\langle x, c\rangle a = \langle x, \sigma^{-1}(a)c\rangle \in \langle x, C\rangle$, which implies that $\langle x, C\rangle$ is a right ideal. Since ρ is a generating character, Lemma 2.1 implies $\langle x, C\rangle = 0$, showing $x \in l(C)$. Thus, $l_\rho(C) = l(C)$. A similar argument, using $\langle C, x\rangle$ being a left ideal, shows $r_\rho(C) = r(C)$. □

Define two maps as follows.

$$\alpha : A^n \to \widehat{A^n}, \quad x \mapsto \alpha_x, \quad \alpha_x(y) = \rho(\langle x, y\rangle), y \in A^n;$$

$$\beta : A^n \to \widehat{A^n}, \quad x \mapsto \beta_x, \quad \beta_x(y) = \rho(\langle y, x\rangle), y \in A^n.$$

Lemma 3.4. *Over a finite Frobenius ring A, the maps α and β are group isomorphisms.*

Proof. We prove the result for α; the proof for β is similar. Then

$$\begin{aligned}\alpha_x(z)\alpha_y(z) &= \rho(\langle x, z\rangle)\rho(\langle y, z\rangle) = \rho(\langle x, z\rangle + \langle y, z\rangle)\\ &= \rho(\langle x + y, z\rangle) = \alpha_{x+y}(z),\end{aligned}$$

for all $x, y, z \in A^n$. So, α is a group homomorphism.

Assume $\alpha_x = \alpha_y$. Then for any $w \in A^n$, $1 = \alpha_x(w)\alpha_{-y}(w) = \rho(\langle x - y, w\rangle)$. Since $\langle x - y, A^n\rangle$ is a right ideal and ρ is a generating character, by Lemma 2.1, $\langle x - y, A^n\rangle = 0$. This implies $x = y$ since $\langle\cdot,\cdot\rangle$ is non-degenerate. So, α is injective and hence bijective. □

For an additive subgroup H of A^n, define

$$(\widehat{A^n} : H) = \{\pi \in \widehat{A^n} : \pi(H) = 1\}.$$

Clearly, $(\widehat{A^n} : H)$ is a subgroup of $\widehat{A^n}$. If $C \subseteq A^n$ is a left (right) linear code, then $(\widehat{A^n} : C)$ is a right (left) A-submodule of $\widehat{A^n}$.

The next lemma follows directly from Lemma 3.4.

Lemma 3.5. *Over a finite Frobenius ring A, there are group isomorphisms $l_\rho(C) \cong (\widehat{A^n} : C)$ and $r_\rho(C) \cong (\widehat{A^n} : C)$.*

Proof. The character dual $l_\rho(C)$ corresponds to $(\widehat{A^n} : C)$ under the isomorphism α, while $r_\rho(C)$ corresponds to $(\widehat{A^n} : C)$ under β. □

Theorem 3.6. *For a left A-linear code $C \subseteq A^n$ over a finite Frobenius ring A,*

$$|C| \cdot |l(C)| = |C| \cdot |r(C)| = |A^n|.$$

Proof. The annihilator $(\widehat{A^n} : C)$ is isomorphic to the character group $(A^n/C)\widehat{}$ of the quotient group A^n/C. Thus $|C| \cdot |(\widehat{A^n} : C)| = |A^n|$. By Lemmas 3.3 and 3.5, the result follows. □

For any code (linear or not) $C \subseteq A^n$, we have $C \subseteq r(l(C))$, $C \subseteq l(r(C))$, $C \subseteq r_\rho(l_\rho(C))$, and $C \subseteq l_\rho(r_\rho(C))$. When C is a left linear code, all these containments are equalities.

Proposition 3.7. *Let $C \subseteq A^n$ be a left A-linear code over a finite Frobenius ring A. Then*

$$\begin{aligned} C &= l(r(C)), & C &= l_\rho(r_\rho(C)), \\ C &= r(l(C)), & C &= r_\rho(l_\rho(C)). \end{aligned}$$

Proof. By using Theorem 3.6, one sees that C and the double annihilators all have the same cardinalities. Thus the containments described above are equalities. □

4. Bilinear forms

This section discusses bilinear forms. Most of the results are similar to those in Section 3, and their proofs are essentially the same. Similar results in the more general setting of bilinear forms with values in a bimodule may be found in [7, Section 12.5]. A very general approach using biadditive forms was initiated in [5]; additional information about that approach appears in [7] and [8].

For a ring A and a two-sided module M over A, a **bilinear form** on M is a map $\langle \cdot, \cdot \rangle : M \times M \to A$ such that if $x, y, z \in M$ and $a \in A$, then $\langle x + z, y\rangle = \langle x, y\rangle + \langle z, y\rangle$, $\langle x, y + z\rangle = \langle x, y\rangle + \langle x, z\rangle$, $\langle ax, y\rangle = a\langle x, y\rangle$, and $\langle x, ya\rangle = \langle x, y\rangle a$. A bilinear form is called **non-degenerate** if $\langle x, y\rangle = 0$ for all $y \in M$ implies $x = 0$ and $\langle y, x\rangle = 0$ for all $y \in M$ implies $x = 0$.

Proposition 4.1. *Let A be a ring. Define the map*

$$\langle \cdot, \cdot \rangle : A^k \times A^k \to A; \quad \langle x, y\rangle = \sum_{i=1}^{k} x_i y_i.$$

Then $\langle \cdot, \cdot \rangle$ is a bilinear form. Moreover, $\langle xa, y\rangle = \langle x, ay\rangle$ for all $x, y \in A^k$ and $a \in A$.

For the rest of the section, let n be a natural number, A be a finite Frobenius ring, ρ be a generating character for A, and $\langle \cdot, \cdot \rangle$ be a non-degenerate bilinear form on A^n.

For any code (linear or not) $C \subseteq A^n$, the left and right **dual codes** of C, denoted by $l(C)$ and $r(C)$, are

$$l(C) = \{v \in A^n : \langle v, C\rangle = 0\} \text{ and } r(C) = \{v \in A^n : \langle C, v\rangle = 0\},$$

and the left and right **ρ-character dual codes** of C, denoted by $l_\rho(C)$ and $r_\rho(C)$, are

$$\begin{aligned} l_\rho(C) &= \{v \in A^n : \rho(\langle v, C\rangle) = 1\}, \\ r_\rho(C) &= \{v \in A^n : \rho(\langle C, v\rangle) = 1\}. \end{aligned}$$

Then $l(C)$ is a left A-submodule and $r(C)$ is a right A-submodule of A^n, while $l_\rho(C)$ and $r_\rho(C)$ are additive subgroups of A^n. In fact, $l(C) = l(CA)$, $r(C) = r(AC)$, $l_\rho(C) = l_\rho(\mathbb{Z}C)$, and $r_\rho(C) = r_\rho(\mathbb{Z}C)$, where CA is the right A-submodule of A^n generated by C.

Lemma 4.2. *Suppose A is a finite Frobenius ring. If $C \subseteq A^n$ is a left A-linear code, then $r_\rho(C)$ is a right A-module. If $C \subseteq A^n$ is a right A-linear code, then $l_\rho(C)$ is a left A-module.*

Proof. See Lemma 3.2. □

Lemma 4.3. *Suppose A is a finite Frobenius ring. If $C \subseteq A^n$ is a left A-linear code, then $r(C) = r_\rho(C)$. If $C \subseteq A^n$ is a right A-linear code, then $l(C) = l_\rho(C)$.*

Proof. See Lemma 3.3. □

Define two maps as follows.

$$\alpha : A^n \to \widehat{A^n}, \quad x \mapsto \alpha_x, \quad \alpha_x(y) = \rho(\langle x, y\rangle), y \in A^n;$$

$$\beta : A^n \to \widehat{A^n}, \quad x \mapsto \beta_x, \quad \beta_x(y) = \rho(\langle y, x\rangle), y \in A^n.$$

Lemma 4.4. *Over a finite Frobenius ring A, the maps α and β are group isomorphisms.*

Proof. See Lemma 3.4. □

The following lemma follows directly from Lemma 4.4.

Lemma 4.5. *Suppose A is a finite Frobenius ring. Let $C \subseteq A^n$ be any code. Then the map α restricts to a group isomorphism $l_\rho(C) \cong (\widehat{A^n} : C)$, while β restricts to a group isomorphism $r_\rho(C) \cong (\widehat{A^n} : C)$.*

Theorem 4.6. *Let A be a finite Frobenius ring. If $C \subseteq A^n$ is a left A-linear code, then $|C|\cdot|r(C)| = |A^n|$. If $C \subseteq A^n$ is a right A-linear code, then $|C| \cdot |l(C)| = |A^n|$.*

Proof. See Theorem 3.6 and Lemma 4.3. □

Just as for sesquilinear forms, for any code (linear or not) $C \subseteq A^n$, we have $C \subseteq r(l(C))$, $C \subseteq l(r(C))$, $C \subseteq r_\rho(l_\rho(C))$, and $C \subseteq l_\rho(r_\rho(C))$. When C is a linear code, appropriate containments are equalities.

Proposition 4.7. *Let A be a finite Frobenius ring. If $C \subseteq A^n$ is a left A-linear code, then*

$$C = l(r(C)), \quad C = l_\rho(r_\rho(C)).$$

If $C \subseteq A^n$ is a right A-linear code, then

$$C = r(l(C)), \quad C = r_\rho(l_\rho(C)).$$

Proof. See Proposition 3.7 and Theorem 4.6. □

Remark 4.8. The double-annihilator property of Proposition 4.7 holds in more general settings. Suppose A is any finite ring with 1, and consider the standard dot product on A^n of Proposition 4.1. Then the results of Proposition 4.7 hold if and only if A is a quasi-Frobenius ring [3]. In fact, the double-annihilator property for ideals (i.e., $n = 1$) is often taken as the definition of a quasi-Frobenus ring.

Remark 4.9. We thank the referee for the observation that the results in the sesquilinear case are special cases of those in the bilinear case. Suppose A is a finite ring with 1 and σ is an anti-automorphism on A. Suppose M is a left A-module equipped with a σ-sesquilinear form $\langle \cdot, \cdot \rangle : M \times M \to A$. Define a right A-module structure on M by $ma = \sigma^{-1}(a)m$, for $m \in M$ and $a \in A$, where the left scalar multiplication is used for $\sigma^{-1}(a)m$. This makes M a two-sided module over A. Moreover, $\langle \cdot, \cdot \rangle$ is now a bilinear form: $\langle x, ya\rangle = \left\langle x, \sigma^{-1}(a)y\right\rangle = \langle x, y\rangle\, \sigma(\sigma^{-1}(a)) = \langle x, y\rangle\, a$, for $x, y \in M$ and $a \in A$.

5. MacWilliams identities

In this section we will prove the MacWilliams identities relating the Hamming weight enumerators of a linear code over a finite Frobenius ring and its dual code with respect to a non-degenerate sesquilinear form or a non-degenerate bilinear form.

Given a finite ring A, the **Hamming weight** of an element $a \in A$ is

$$\mathrm{wt}(a) = \begin{cases} 0, & a = 0, \\ 1, & a \neq 0. \end{cases}$$

We extend wt to apply to vectors $x = (x_1, \ldots, x_n) \in A^n$ by $\mathrm{wt}(x) = \sum_{i=1}^n \mathrm{wt}(x_i)$, where the sum takes place in $\mathbb{Z}$. Thus $\mathrm{wt}(x)$ counts the number of nonzero entries of the vector x. We will also need to define the Hamming weight on $\widehat{A}$: $\mathrm{wt}(\pi) = 0$ when $\pi = 1$ (the trivial character with $\pi(a) = 1$ for all $a \in A$) and $\mathrm{wt}(\pi) = 1$ for $\pi \neq 1$. Then extend to $\widehat{A}^n$ as above.

Given an additive code $C \subseteq A^n$, the **Hamming weight enumerator** $W_C(X, Y)$ of C is the polynomial in $\mathbb{C}[X, Y]$ defined by

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

We quote the MacWilliams identities for additive codes from [7], but the result in this generality goes back to Delsarte [2].

Theorem 5.1 ([7, Theorem 11.3])**.** *Let $C \subseteq A^n$ be an additive code over A. Then the MacWilliams identities hold:*

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

We now state the MacWilliams identities with respect to non-degenerate forms.

Theorem 5.2 (MacWilliams identities)**.** *Suppose A is a finite Frobenius ring. Then*

$$W_D(X, Y) = \frac{1}{|C|} W_C(X + (|A| - 1)Y, X - Y)$$

holds in the following cases:

- *$\langle \cdot, \cdot \rangle$ is a non-degenerate sesquilinear form on A^n, $C \subseteq A^n$ is a left A-linear code, and $D = l(C)$ or $r(C)$;*
- *$\langle \cdot, \cdot \rangle$ is a non-degenerate bilinear form on A^n, $C \subseteq A^n$ is a left A-linear code, and $D = r(C)$;*
- *$\langle \cdot, \cdot \rangle$ is a non-degenerate bilinear form on A^n, $C \subseteq A^n$ is a right A-linear code, and $D = l(C)$.*

Theorem 5.2 will follow from Theorem 5.1 once we prove the next lemma.

Lemma 5.3. *The group isomorphisms α and β of Lemmas 3.4 and 4.4 preserve the Hamming weight.*

Proof. We will prove the result for α; the proof for β is similar. Express $x = (x_1, \ldots, x_n) \in A^n$ as the linear combination $x = \sum_{i=1}^n x_i e_i$, where the e_i are the standard basis of A^n. I.e., e_i is the n-tuple with 1 in position i and 0s elsewhere. Then

$$\begin{aligned} \alpha_x(y) = \rho(\langle x, y \rangle) &= \rho(\sum_{i=1}^n x_i \langle e_i, y \rangle) \\ &= \prod_{i=1}^n \rho(x_i \langle e_i, y \rangle) = \prod_{i=1}^n \rho^{x_i}(\langle e_i, y \rangle) \end{aligned}$$

The lemma is equivalent to showing that $y \mapsto \rho^{x_i}(\langle e_i, y\rangle)$ is the trivial character if and only if $x_i = 0$.

If $x_i = 0$, then certainly $y \mapsto \rho^{x_i}(\langle e_i, y\rangle)$ is trivial. For the converse, suppose $y \mapsto \rho^{x_i}(\langle e_i, y\rangle)$ is trivial. Then $x_i \langle e_i, A^n\rangle \subseteq \ker\rho$. But $x_i \langle e_i, A^n\rangle$ is a right ideal of A, so $x_i \langle e_i, A^n\rangle = 0$ by Lemma 2.2. This means $\langle x_i e_i, A^n\rangle = 0$, so that $x_i e_i = 0$ by the non-degeneracy of the form $\langle \cdot, \cdot\rangle$. Thus $x_i = 0$. □

Proof of Theorem 5.2. By Lemma 5.3, $W_D(X,Y) = W_{(\widehat{A^n}:C)}(X,Y)$ via the weight-preserving isomorphisms α or β. The result then follows from Theorem 5.1. □

6. Summary

In this final section, we collect in one place the main results of the paper, arranged in the same manner as the "model theorem" in [7].

Theorem 6.1. *Let $C \subseteq A^n$ be a left A-linear code over a finite Frobenius ring A. Suppose A^n is equipped with a non-degenerate sesquilinear form. Then*

- *$l(C)$ and $r(C)$ are left A-linear codes in A^n;*
- *$l(r(C)) = C$ and $r(l(C)) = C$;*
- *$|C| \cdot |l(C)| = |A^n|$ and $|C| \cdot |r(C)| = |A^n|$;*
- *the MacWilliams identities hold, for D equaling $l(C)$ or $r(C)$:*

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

Theorem 6.2. *Let $C \subseteq A^n$ be a left A-linear code and $C' \subseteq A^n$ be a right A-linear code over a finite Frobenius ring A. Suppose A^n is equipped with a non-degenerate bilinear form. Then*

- *in A^n, $r(C)$ is a right A-linear code, and $l(C')$ is a left A-linear code;*
- *$l(r(C)) = C$ and $r(l(C')) = C'$;*
- *$|C| \cdot |r(C)| = |A^n|$ and $|C'| \cdot |l(C')| = |A^n|$;*
- *the MacWilliams identities hold:*

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

Acknowledgment: We thank the referee for valuable comments which helped improve the clarity of the paper and which reminded us that we initially forgot to include Proposition 4.7.

References

[1] H. L. Claasen, R. W. Goldbach, A field–like property of finite rings, Indag. Math. (N.S.) 3(1) (1992) 11–26.

[2] P. Delsarte, Bounds for unrestricted codes, by linear programming, Philips Res. Rep. 27 (1972) 272–289.

[3] M. Hall, A type of algebraic closure, Ann. of Math. 40(2) (1939) 360–369.

[4] T. Y. Lam, Lectures on Modules and Rings, Graduate Texts in Mathematics, vol. 189, Springer–Verlag, New York, 1999.

[5] G. Nebe, E. M. Rains, N. J. A. Sloane, Self–Dual Codes and Invariant Theory, Algorithms and Computation in Mathematics, vol. 17, Springer–Verlag, Berlin, 2006.

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

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

[8] J. A. Wood, Anti–isomorphisms, character modules and self–dual codes over non-commutative rings, Int. J. Inf. Coding Theory 1(4) (2010) 429–444.

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