Anti-isomorphisms, character modules and self-dual codes over non-commutative rings

Jay A. Wood

Department of Mathematics,
Western Michigan University,
1903 W. Michigan Avenue,
Kalamazoo, MI 49008–5248, USA
E-mail: jay.wood@wmich.edu

Abstract: This paper is dedicated to Vera Pless. It is an elaboration on ideas of Nebe, Rains and Sloane: by assuming the existence of an anti-isomorphism on a finite ring and by assuming a module alphabet has a well-behaved duality, one is able to study self-dual codes defined over alphabets that are modules over a non-commutative ring. Various examples are discussed.

Keywords: anti-isomorphisms; bi-additive forms; character modules; dual codes; MacWilliams identities; skew-polynomial rings; group rings; Steenrod algebra; self-dual codes.

Reference to this paper should be made as follows: Wood, J.A. (2010), 'Anti-isomorphisms, character modules and self-dual codes over non-commutative rings', *Int. J. Information and Coding Theory*, Vol. 1, No. 4, pp.429–444.

Biographical notes: Jay A. Wood received his AB in Mathematics from the University of Notre Dame and his MA and PhD in Mathematics from the University of California, Berkeley. Currently, he is a Professor of Mathematics at Western Michigan University.

1 Tribute to Vera Pless

I first met Vera Pless on 12 October 1987 at the University of Wisconsin. She was visiting Madison at the time, and I was in town to give a talk. We had shared some correspondence prior to this, because I had discovered that a problem I had been pursuing, which originated in differential geometry and algebraic topology, turned out to be equivalent to classifying the doubly-even self-dual binary codes up to code equivalence. Vera very graciously provided me with copies of some of her papers on the classification of these codes, and I went on to study the relationships between self-dual codes and certain structures in algebraic topology.

When I relocated to the midwest in 1990, Vera very kindly invited me to speak in her UIC seminar on several occasions. On one such occasion, 28 April 1992, Vera suggested that I reexamine the work of MacWilliams on code equivalence. Inspired by Vera's interest, and by subsequent collaboration with Thann Ward, I spent much of the next 17 years developing an understanding of code equivalence and the MacWilliams identities for linear codes defined over finite rings and finite modules, with a special emphasis on the role of

Frobenius rings. I doubt that I would have worked on these topics if Vera had not suggested them. So, I can truthfully say: "Vera, I owe it all to you. Thank you!"

I find it fitting that this paper allows me to return to the topic of my first correspondence with Vera: self-dual codes, with some examples coming from algebraic topology.

2 Introduction

My goal in this paper is to clarify the assumptions that lead to a good theory of self-dual codes over non-commutative rings. This paper was inspired by, and is an elaboration of portions of, the book by Nebe et al. (2006). Virtually all of the content of Sections 3 and 4 can be found, explicitly or implicitly, in Nebe et al. (2006). The material in those sections has been organised in a manner similar to the latter portions of Wood (2009), in which a detailed examination of duality and the MacWilliams identities took place.

In Wood (2009), the dual of a left linear code is a right linear code, and vice versa. While the theory works well, the change of sides makes it difficult for a code to be self-dual. This problem is addressed in Nebe et al. (2006), and in Section 3 the approach of Nebe et al. (2006) is condensed into three properties (Definition 1): that the ring R admit an anti-isomorphism ε; that the alphabet A, a finite left R-module, admit an anti-isomorphism ψ to its character module $\widehat{A}$; and that ψ have a close relation to its own dual map. These properties are equivalent to the existence of a bi-additive form $\beta : A \times A \to \mathbb{Q}/\mathbb{Z}$, with certain additional properties. The form β plays a major role in Nebe et al. (2006), and the same is true here.

In Section 4, it is shown (Theorem 2) that the three properties of Definition 1 imply that left dual codes of left linear codes exist and have all the good properties one would expect of a dual code. In subsequent sections, the paper addresses each of the three properties in turn. In some cases, general theorems can be proved concerning when the property holds. In all cases, several examples (including a group ring and a finite subalgebra of the Steenrod algebra) are explored in detail.

3 Anti-isomorphisms and character modules

Let R be a finite ring with 1. We allow R to be non-commutative. Let A be a finite left R-module, which will serve as the alphabet for linear codes over R. A left *R-linear code* over A of length n is a left R-submodule $C \subset A^n$. (There is a parallel theory for right linear codes.) An important special case is when the alphabet A is the ring R itself, viewed as a left R-module.

In most treatments of the MacWilliams identities, the dual code $C^\perp$ would be a right R-module. Over a non-commutative ring, this change of sides would make it very difficult for a code to be self-dual, that is, satisfy $C = C^\perp$. (But not impossible: in a finite chain ring, every one-sided ideal is actually two-sided.) Nebe et al. (2006) address this problem by assuming some additional structure on R and A so that one can view the dual code $C^\perp$ as a left R-module. To that end, we follow Nebe et al. (2006) and introduce several definitions.

An *anti-isomorphism* $\varepsilon\colon R \to R$ of a ring R is an isomorphism of abelian groups with the property that $\varepsilon(rs) = \varepsilon(s)\varepsilon(r)$ for all $r, s \in R$. An anti-isomorphism ε defines an isomorphism $R \cong R^{\text{op}}$ between the ring R and its opposite ring R^{op}. If ε is an anti-isomorphism of R, then so is its inverse ε^{-1}. An *involution* is an anti-isomorphism $\varepsilon : R \to R$ such that ε^2 is the identity; that is, $\varepsilon^{-1} = \varepsilon$.

Let ${}_R\mathcal{F}$ (resp., $\mathcal{F}_R$) denote the category of finitely generated left (resp., right) R-modules and R-module homomorphisms. Then, an anti-isomorphism $\varepsilon\colon R \to R$ induces covariant functors $\varepsilon\colon {}_R\mathcal{F} \rightleftharpoons \mathcal{F}_R$ as follows. If M is a left R-module, define $\varepsilon(M)$ to be the same abelian group as M with right scalar multiplication defined by $mr = \varepsilon(r)m$, for $m \in M$, $r \in R$, where $\varepsilon(r)m$ uses the left scalar multiplication of M. Similarly, if N is a right R-module, then $\varepsilon(N)$ has left scalar multiplication defined by $rn = n\varepsilon(r)$, for $n \in N$, $r \in R$. One verifies that a homomorphism $f\colon M_1 \to M_2$ of left R-modules is also a homomorphism $\varepsilon(M_1) \to \varepsilon(M_2)$ of right R-modules.

Character modules will be important in our discussion, so we provide a short summary of them next. The *character functor* $\widehat{\ }\colon {}_R\mathcal{F} \rightleftharpoons \mathcal{F}_R$ is a contravariant functor that associates to every finite left (resp., right) R-module M its character module $\widehat{M} = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$, which is a finite right (resp., left) R-module. (In this paper, the additive form of characters will be used. By composing with the exponential map: $\mathbb{Q}/\mathbb{Z} \to \mathbb{C}^\times$, $x \mapsto \exp(2\pi i x)$, $x \in \mathbb{Q}/\mathbb{Z}$, one recovers the multiplicative form of characters. The modules involved are isomorphic.) When M is a left R-module, the right module structure of $\widehat{M}$ is given by $(\varpi r)(m) = \varpi(rm)$, for $\varpi \in \widehat{M}$, $r \in R$ and $m \in M$.

Lemma 1: *Given an anti-isomorphism ε on a finite ring R, the functors ε and $\widehat{\ }$ commute. That is, for any finite R-module M,*

$$\widehat{\varepsilon(M)} = \varepsilon(\widehat{M}).$$

Proof: When M is a left R-module, both $\varepsilon(M)$ and $\widehat{M}$ are right R-modules, and $\widehat{\varepsilon(M)}$ and $\varepsilon(\widehat{M})$ are both left R-modules. For a character $\varpi : M \to \mathbb{Q}/\mathbb{Z}$, left multiplication by $r \in R$ in $\widehat{\varepsilon(M)}$ means, for $m \in M$, $(r\varpi)(m) = \varpi(mr)$, where the right multiplication is that of $\varepsilon(M)$. Left multiplication in $\varepsilon(\widehat{M})$ means $(r\varpi)(m) = (\varpi\varepsilon(r))(m)$. The two left multiplications agree because $\varpi(mr) = \varpi(\varepsilon(r)m) = (\varpi\varepsilon(r))(m)$, using the right module structures of $\varepsilon(M)$ and $\widehat{M}$. □

Suppose the finite ring R admits an anti-isomorphism ε. Even though the functors ε and $\widehat{\ }$ commute, the functors cannot be the same. Indeed, the functor $\varepsilon\colon {}_R\mathcal{F} \rightleftharpoons \mathcal{F}_R$ is covariant, while the character functor $\widehat{\ }\colon {}_R\mathcal{F} \rightleftharpoons \mathcal{F}_R$ is contravariant. However, modules where the functors agree will be important.

To that end, suppose M is a finite left R-module such that $\psi\colon \varepsilon(M) \to \widehat{M}$ is an isomorphism of right R-modules. For every $y \in M$, $\psi(y)$ is a character on M. We denote the value of this character on a point $x \in M$ by $\psi(y)(x)$. Then, ψ being a homomorphism means

$$\psi(\varepsilon(r)y)(x) = \psi(yr)(x) = (\psi(y)r)(x) = \psi(y)(rx) \tag{1}$$

for $r \in R$ and $x, y \in M$.

By applying the character functor to the isomorphism $\psi : \varepsilon(M) \to \widehat{M}$ and using that the double character module of M is naturally isomorphic to M itself, we obtain $\widehat{\psi}\colon M \to \widehat{\varepsilon(M)} = \varepsilon(\widehat{M})$. Applying ε^{-1}, we have an isomorphism $\widehat{\psi}\colon \varepsilon^{-1}(M) \to \widehat{M}$. From the definition of $\widehat{\psi}$, we have the relation

$$\widehat{\psi}(x)(y) = \psi(y)(x), \quad x, y \in M \tag{2}$$

Proposition 1: *Suppose a finite ring R admits an anti-isomorphism ε and that a finite left R-module M admits an isomorphism $\psi\colon \varepsilon(M) \to \widehat{M}$. Then, $\varepsilon(M) \cong \varepsilon^{-1}(M)$; that is, $\varepsilon^2(M) \cong M$.*

Proof: The composition $\widehat{\psi}^{-1}\psi : \varepsilon(M) \to \widehat{M} \to \varepsilon^{-1}(M)$ is an isomorphism. □

Definition 1: *The following is a list of properties that a finite ring R may possess.*

P1: *The ring R admits an anti-isomorphism ε.*

P2: *The ring R admits an anti-isomorphism ε and a finite left R-module A, such that $\varepsilon(A)$ is isomorphic to $\widehat{A}$, via some isomorphism $\psi : \varepsilon(A) \to \widehat{A}$.*

P3: *The ring R satisfies P2, and, in addition, the isomorphism ψ in P2 satisfies $\widehat{\psi} = \psi e$, for some unit $e \in R$.*

The condition in $P3$ means that there exists a unit $e \in R$ such that $\widehat{\psi}(x) = \psi(x)e \in \widehat{A}$, for all $x \in A$, where $\psi(x)e$ uses the right module structure of $\widehat{A}$. This leads to the following relations:

$$\psi(x)(ey) = (\psi(x)e)(y) = \widehat{\psi}(x)(y) = \psi(y)(x), \quad x, y \in A \tag{3}$$

For the rest of this section, we assume that a finite ring R and a finite left R-module A satisfy P1–P3, with anti-isomorphism ε and right module isomorphism $\psi : \varepsilon(A) \to \widehat{A}$. In this case, observe that $\psi : A \to \varepsilon^{-1}(\widehat{A})$ is a left module isomorphism.

We will now associate to $\psi : \varepsilon(A) \to \widehat{A}$ a bi-additive form, in the spirit of Nebe et al. (2006). First, define $\beta : A \times A \to \mathbb{Q}/\mathbb{Z}$ by $\beta(a, b) = \psi(b)(a)$, for $a, b \in A$. Then, extend β to $\beta : A^n \times A^n \to \mathbb{Q}/\mathbb{Z}$ by

$$\beta(x, y) = \sum_{i=1}^{n} \beta(x_i, y_i) = \sum_{i=1}^{n} \psi(y_i)(x_i) \tag{4}$$

for $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in A^n$. Remember that the notation $\psi(y_i)(x_i)$ means to evaluate the character $\psi(y_i)$ of A on the element $x_i \in A$. The result is an element of $\mathbb{Q}/\mathbb{Z}$. One then sums these elements of $\mathbb{Q}/\mathbb{Z}$.

Theorem 1: *Assume properties P1–P3. The form β of Equation (4) satisfies:*

1 *The form β is bi-additive; i.e., $\beta(x + z, y) = \beta(x, y) + \beta(z, y)$ and $\beta(x, y + z) = \beta(x, y) + \beta(x, z)$, for all $x, y, z \in A^n$.*

2 *The form β is non-degenerate. That is, if $\beta(A^n, y) = 0$, then $y = 0$; and if $\beta(x, A^n) = 0$, then $x = 0$.*

3 *The form satisfies $\beta(rx, y) = \beta(x, \varepsilon(r)y)$, for all $r \in R$, $x, y \in A^n$.*

4 *There exists a unit $e \in R$ so that $\beta(x, y) = \beta(ey, x)$, for all $x, y \in A^n$.*

Conversely, assume property P1 and that there exists a form $\beta : A \times A \to \mathbb{Q}/\mathbb{Z}$ satisfying the properties above. If one defines $\psi : A \to \widehat{A}$ by $\psi(b)(a) = \beta(a, b)$, for $a, b \in A$, then ψ satisfies P2–P3.

Proof: The first part of the bi-additivity of β follows from the definition of character; the second from ψ being an additive homomorphism. The non-degeneracy of β follows from a similar non-degeneracy property of characters. The scalar multiplication property follows from ψ being a homomorphism of right R-modules and the definitions of the right module structures on $\widehat{A}$ and $\varepsilon(A)$; compare with Equation (1). The symmetry property follows from $P3$; compare with Equation (3).

The converse is an exercise for the reader. □

4 Dual codes and the MacWilliams identities

We first recall several well-known definitions. We assume that R is a finite ring with 1 and that A is a finite left R-module. An *additive code* over A of length n is an additive subgroup $C \subset A^n$. Recall that a left *linear code* is a left R-submodule of A^n. Every linear code is an additive code, but not conversely. The *Hamming weight* wt on A is a function $\mathrm{wt}\colon A \to \mathbb{Q}$ defined by $\mathrm{wt}(0) = 0$ and $\mathrm{wt}(a) = 1$ for $a \neq 0$. The Hamming weight extends to a function $\mathrm{wt}\colon A^n \to \mathbb{Q}$ by $\mathrm{wt}(a_1, \dots, a_n) = \sum_{i=1}^{n} \mathrm{wt}(a_i)$. The *Hamming weight enumerator* of an additive code $C \subset A^n$ is the polynomial $W_C(X, Y) \in \mathbb{C}[X, Y]$ defined by

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

Assume that a finite ring R and a finite left R-module A satisfy $P1$–$P3$, with anti-isomorphism ε and right module isomorphism $\psi : \varepsilon(A) \to \widehat{A}$. The isomorphism ψ extends to a right module isomorphism $\psi : \varepsilon(A^n) \to \widehat{A}^n$.

Given an additive code $C \subset A^n$, the character-theoretic *annihilator* of C is

$$\big(\widehat{A}^n : C\big) = \big\{\varpi \in \widehat{A}^n : \varpi(C) = 0\big\}$$

Note that $(\widehat{A}^n : C)$ is an additive subgroup of $\widehat{A}^n$ and that $|C|\big|(\widehat{A}^n : C)\big| = \big|A^n\big|$ (see Terras, 1999). Define the *dual code* $C^\perp$ by

$$C^\perp = \psi^{-1}\big(\widehat{A}^n : C\big)$$

Note that the dual code $C^\perp$ is an additive code in A^n. We say that C is *self-orthogonal* if $C \subset C^\perp$ and *self-dual* if $C = C^\perp$.

Theorem 2: *Assume that a finite ring R and a finite left R-module A satisfy P1–P3, with anti-isomorphism ε and right module isomorphism $\psi\colon \varepsilon(A) \to \widehat{A}$. Let β be the form associated to ψ via Equation (4). Then:*

1 *For any additive code $C \subset A^n$, $C^\perp = \{y \in A^n : \beta(C, y) = 0\}$.*

2 *For any additive code $C \subset A^n$, $|C||C^\perp| = |A^n|$.*

3 *For any additive code $C \subset A^n$, the MacWilliams identities are satisfied:*

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

4 *If $C \subset A^n$ is a left linear code, then so is $C^\perp$.*

5 *For any left linear code $C \subset A^n$, $C = (C^\perp)^\perp$.*

Proof: By the definition of $C^\perp$,

$$C^\perp = \psi^{-1}\big(\widehat{A}^n : C\big) = \big\{y \in A^n : \psi(y)(C) = 0\big\} = \big\{y \in A^n : \beta(C, y) = 0\big\}$$

The size condition on $C^\perp$ follows from the size condition on $(\widehat{A}^n : C)$ and ψ being an isomorphism. The standard proof of the MacWilliams identities using the Poisson summation formula applies (see Wood, 2009 or other standard sources for details).

Suppose C is a left linear code. In this case, the character-theoretic annihilator $(\widehat{A}^n : C)$ is a right R-submodule of $\widehat{A}^n$. Because ψ is a right isomorphism (by $P2$), $C^\perp = \psi^{-1}(\widehat{A}^n : C)$ is a right R-submodule of $\varepsilon(A^n)$, that is, a left R-submodule of A^n.

The double dual statement uses $P3$ in an essential way. We first show that $C \subset (C^{\perp})^{\perp}$. To that end, suppose $x \in C$ and $y \in C^{\perp}$. In order that $x \in (C^{\perp})^{\perp}$, we must show that $\beta(y, x) = 0$. But $\beta(y, x) = \beta(ex, y) = \beta(x, \varepsilon(e)y) = 0$, since $\varepsilon(e)y \in C^{\perp}$ because $C^{\perp}$ is a left R-submodule. Note that in this derivation, Theorem 1 was used twice, using properties that follow from $P2$ and $P3$. Once we know that $C \subset (C^{\perp})^{\perp}$, equality follows from the size condition (applied to C and $C^{\perp}$). □

Remark 1: Because of the property $\beta(x, y) = \beta(ey, x)$, which uses $P3$, $C^{\perp}$ is also equal to $\{x \in A^n : \beta(x, C) = 0\}$, provided the code C is linear. (The assumption of C being linear is not needed if $e = 1$.)

Remark 2: Although we do not include it here, the MacWilliams identities are also valid for the complete weight enumerator (see Nebe et al., 2006; Wood, 2009 for details).

5 Property P1–examples

In this section, we provide a number of examples of finite rings that satisfy Property $P1$, that is, rings that admit an anti-isomorphism ε. Because Frobenius rings will play a prominent role in Section 6, we also mention whether the examples are Frobenius rings (see Lam, 1999; Wood, 1999, 2009 for more information about Frobenius rings). Verifications will be left to the reader or to cited references.

Example 1: The first example is a non-example, that is, an example of a finite ring that does not admit an anti-isomorphism. Let R be the ring

$$R = \begin{pmatrix} \mathbb{Z}/2^k\mathbb{Z} & \mathbb{Z}/2\mathbb{Z} \\ 0 & \mathbb{Z}/2\mathbb{Z} \end{pmatrix}$$

where $k \geq 2$. One can show that the left and right annihilators of the set of nilpotent elements are different, which would contradict the existence of an anti-isomorphism. This example is due to H.W. Lenstra Jr. and details can be found in Lam (2003, Ex. 1.22B). This ring is not Frobenius.

Example 2: If R is a finite commutative ring, then any ring isomorphism, in particular the identity isomorphism, is an anti-isomorphism. Some finite commutative rings (such as finite fields and Galois rings) are Frobenius; others are not.

Example 3: The product of rings satisfying $P1$ is another ring satisfying $P1$. That is, if finite rings $R_1, \ldots, R_n$ admit anti-isomorphisms $\varepsilon_1, \ldots, \varepsilon_n$, respectively, then $R = R_1 \times \cdots \times R_n$ admits the anti-isomorphism $\varepsilon = \varepsilon_1 \times \cdots \times \varepsilon_n$. If every ε_i is an involution, then so is ε. The product R is Frobenius if and only if each R_i is Frobenius.

Example 4: Suppose a finite ring S satisfies $P1$ with anti-isomorphism ϵ, and suppose G is a finite group. Then, the group ring $R = S[G]$ satisfies $P1$ with anti-isomorphism ε given by

$$\varepsilon\left(\sum_{g \in G} s_g g\right) = \sum_{g \in G} \epsilon\left(s_g\right) g^{-1}$$

If ϵ is an involution, then so is ε (see Lam, 2003, Ex. 6.10 for details). If S is Frobenius, then so is $S[G]$.

Example 5: Suppose a finite ring S satisfies $P1$ with anti-isomorphism ϵ. Then, the matrix ring $R = M_n(S)$ satisfies $P1$ with anti-isomorphism ε given by

$$\varepsilon(M) = (\epsilon(M))^T, \quad M \in M_n(S);$$

that is, $\varepsilon(M)$ is the transpose of the matrix obtained from M by taking ϵ of each entry. If ϵ is an involution, then so is ε (for details see Lam, 2003, Ex. 1.22). If S is Frobenius, so is $M_n(S)$.

Example 6: Suppose a finite ring S satisfies $P1$ with anti-isomorphism ϵ. Then, the upper triangular matrix ring $U_n(S)$ and the lower triangular matrix ring $L_n(S)$ satisfy $P1$ with anti-isomorphism ε given by:

$$\varepsilon(M)_{i,j} = \epsilon\big(M_{n+1-j,n+1-i}\big), \quad M \in U_n(S), L_n(S);$$

that is, the (i, j)-entry of $\varepsilon(M)$ is ϵ of the $(n+1-j, n+1-i)$-entry of M. If ϵ is an involution, then so is ε (see Lam, 2003, Ex. 1.22 for more details). For $n \geq 2$, the rings $U_n(S)$ and $L_n(S)$ are not Frobenius.

Example 7: This example involves certain finite quotients of skew polynomial rings. Let $\mathbb{F}_q$ be a finite field of characteristic p and order $q = p^f$. Suppose σ is an automorphism of the field $\mathbb{F}_q$. (Then σ necessarily fixes the prime subfield $\mathbb{F}_p \subset \mathbb{F}_q$.) Define the skew-polynomial ring $\mathbb{F}_q[X;\sigma]$, as an abelian group, to be the polynomials in X over $\mathbb{F}_q$, but with the ring multiplication determined by the relation

$$Xa = \sigma(a)X, \quad a \in \mathbb{F}_q$$

If σ is not the identity automorphism, then $\mathbb{F}_q[X;\sigma]$ is a non-commutative ring. It is known that one-sided division algorithms are valid in $\mathbb{F}_q[X;\sigma]$, and thus that every left (resp., right) ideal is principal. The left principal ideal $R(X^{l+1})$ generated by X^{l+1} is in fact a two-sided ideal; we will denote that two-sided ideal by (X^{l+1}).

Let $R = \mathbb{F}_q[X;\sigma]/(X^{l+1})$, with $l \geq 1$. Then, R is a finite chain ring of order q^{l+1}. Every left (resp., right) ideal is two-sided, and the ideals are

$$(1) \supset (X) \supset \big(X^2\big) \supset \cdots \supset \big(X^l\big) \supset \big(X^{l+1}\big) = 0$$

Also, R is a vector space over $\mathbb{F}_q$ with basis $1, X, X^2, \ldots, X^l$. Just as for $\mathbb{F}_q[X;\sigma]$, if σ is not the identity, then R is non-commutative (as $l \geq 1$). Because R is a chain ring, it is a Frobenius ring.

Theorem 3: *The ring $R = \mathbb{F}_q[X;\sigma]/(X^{l+1})$ admits an anti-isomorphism if and only if the field automorphism σ is an involution; that is, σ^2 is the identity. Moreover, when σ is an involution, R admits an involution.*

Proof: Observe that every element $r \in R$ was a unique representation in the form $r = \sum_{i=0}^{l} r_i X^i$, with $r_i \in \mathbb{F}_q$.

Suppose σ is an involution, so that σ^2 is the identity. We seek to define $\varepsilon : R \to R$ in such a way that $\varepsilon(a) = a$ for $a \in \mathbb{F}_q$ and $\varepsilon(X) = X$. Then, for any $r = \sum_{i=0}^{l} r_i X^i \in R$, we would need to have

$$\varepsilon(r) = \sum_{i=0}^{l} \varepsilon\big(r_i X^i\big) = \sum_{i=0}^{l} \varepsilon(X)^i \varepsilon\big(r_i\big) = \sum_{i=0}^{l} X^i r_i = \sum_{i=0}^{l} \sigma^i\big(r_i\big) X^i$$

Consequently, we *define* $\varepsilon\colon R \to R$ by this formula. Because σ is a field automorphism, ε is a homomorphism of abelian groups. Because σ is an involution, one sees that ε^2 is the identity, so that ε is an isomorphism of abelian groups.

It remains to verify that $\varepsilon(rs) = \varepsilon(s)\varepsilon(r)$, for $r, s \in R$. Write $r = \sum_{i=0}^{l} r_i X^i$ and $s = \sum_{j=0}^{l} s_j X^j$. Calculations show that the coefficient of X^k in $\varepsilon(rs)$ is

$$\sigma^k \left(\sum_{i+j=k} r_i \sigma^i\big(s_j\big) \right) = \sum_{i+j=k} \sigma^k\big(r_i\big)\sigma^{k+i}\big(s_j\big)$$

while the coefficient of X^k in $\varepsilon(s)\varepsilon(r)$ is

$$\sum_{j+i=k} \sigma^j\big(s_j\big)\sigma^{j+i}\big(r_i\big) = \sum_{j+i=k} \sigma^j\big(s_j\big)\sigma^k\big(r_i\big).$$

In these formulas (which take place in $\mathbb{F}_q$), the factors of $\sigma^k(r_i)$ agree. As for the factors involving s_j, observe that $\sigma^{k+i}(s_j) = \sigma^{j+2i}(s_j)$, because $i + j = k$. The latter equals $\sigma^j(s_j)$, because σ^2 is the identity. Thus, ε is an involution.

For the converse, suppose $\varepsilon\colon R \to R$ is an anti-isomorphism. Because anti-isomorphisms map left ideals to right ideals, and vice versa, they map two-sided ideals to two-sided ideals. Because ε is an isomorphism of abelian groups, it must preserve sizes of ideals. We conclude that ε maps each ideal (X^k) to itself. In particular, $\varepsilon(X) \in (X)$, so that $\varepsilon(X) = b_1 X + b_2 X^2 + \cdots + b_l X^l$, for some $b_1, \ldots, b_l \in \mathbb{F}_q$, with $b_1 \neq 0$. (If $b_1 = 0$, then ε would map (X) into (X^2) and sizes of ideals would not be preserved.) Similarly, the expression for $\varepsilon(X^k) = \varepsilon(X)^k$ has lowest degree terms in degree k. (The coefficient of X^k would be $b_1\sigma(b_1)\sigma^2(b_1)\cdots\sigma^{k-1}(b_1)$, which is non-zero.)

Let $\gamma \in \mathbb{F}_q$ be a primitive element of the field $\mathbb{F}_q$; that is, γ is a generator of the multiplicative group of $\mathbb{F}_q$. Then $\varepsilon(\gamma) = \sum_{i=0}^{l} c_i X^i$, for some $c_i \in \mathbb{F}_q$. Observe that $c_0 \neq 0$, lest ε map all of R into (X). Given the expressions for $\varepsilon(\gamma)$ and $\varepsilon(X)$ above, one could write down a formula for $\varepsilon(r)$ for any $r = \sum_{i=0}^{l} r_i X^i \in R$. In such a formula, the constant term of $\varepsilon(r)$ involves only the constant term of $\varepsilon(r_0)$. More specifically, if $r_0 = 0$, then the constant term of $\varepsilon(r)$ is also 0. If $r_0 \neq 0$, then $r_0 = \gamma^t$, for some t. In that case, one calculates that the constant term of $\varepsilon(r)$ is c_0^t (where c_0 is the constant term of $\varepsilon(\gamma)$).

Claim 1: c_0 is a primitive element of $\mathbb{F}_q$. The anti-isomorphism ε is, in particular, surjective. Thus, any non-zero element a of $\mathbb{F}_q$ must appear as the constant term of $\varepsilon(r)$ for some $r \in R$. But that implies that $a = c_0^t$ for some t, which means that c_0 is a primitive element of $\mathbb{F}_q$.

Remember that σ is a field automorphism of $\mathbb{F}_q$ and that $q = p^f$. Then, σ has the form $\sigma(a) = a^{p^g}$, $a \in \mathbb{F}_q$, for some $g = 0, 1, \ldots, f-1$. Observe that the constant term of $\varepsilon(\sigma(\gamma)) = \varepsilon(\gamma^{p^g}) = \varepsilon(\gamma)^{p^g}$ is $c_0^{p^g} = \sigma(c_0)$.

Claim 2: $\sigma^2(c_0) = c_0$. To see this, set $u = X$ and $v = \gamma X^{l-1}$. Then $uv = \sigma(\gamma)X^l$, and a computation shows that $\varepsilon(uv) = \varepsilon(X)^l \varepsilon(\sigma(\gamma)) = \varepsilon(X)^l \sigma(c_0) = \sigma^{l+1}(c_0)\varepsilon(X)^l$.

(We make use of the fact that $X^{l+1} = 0$ in R to simplify expressions.) On the other hand, a similar computation shows that $\varepsilon(v)\varepsilon(u) = \sigma^{l-1}(c_0)\varepsilon(X)^l$. Since the coefficient of X^l in $\varepsilon(X)^l$, namely $b_1\sigma(b_1)\cdots\sigma^{l-1}(b_1)$, is non-zero, we conclude that $\sigma^{l+1}(c_0) = \sigma^{l-1}(c_0)$. Because σ is an automorphism, hence invertible, it follows that $\sigma^2(c_0) = c_0$.

Claim 3: σ is an involution. This follows immediately from the previous claims. Indeed, σ^2 is a field automorphism that fixes a primitive element of the field. Thus, σ^2 fixes everything; that is, σ^2 equals the identity. □

Remark3: One of the referees points out that there is a more conceptual proof of Theorem 3. Let $R_{\sigma,m}$ denote the ring $\mathbb{F}_q[X;\sigma]/(X^m)$. Then, $R_{\sigma,m}$ is isomorphic to $R_{\tau,n}$ if and only if $\sigma = \tau$ and $m = n$. (In case $m = n = 2$, this is due to Cronheim (1978).) The opposite ring of $R_{\sigma,m}$ is $R_{\sigma^{-1},m}$. Thus, $R_{\sigma,m}$ admits an anti-isomorphism if and only if $R_{\sigma,m}$ is isomorphic to its opposite ring $R_{\sigma^{-1},m}$, which happens if and only if σ is an involution.

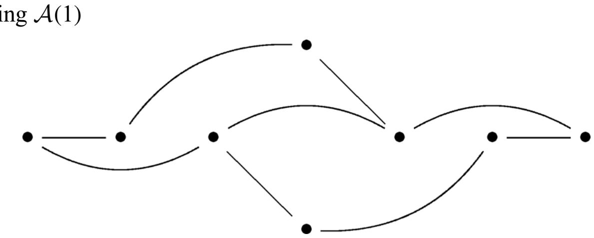
Example 8: Our last example has its origins in algebraic topology, where it appears as a finite sub Hopf algebra of the mod 2 Steenrod algebra. There are many finite sub Hopf algebras in the Steenrod algebra, and the one we present is one of the smallest and simplest. A reference is Whitehead (1978, Chapter VIII).

Define $\mathcal{A}(1)$ to be the $\mathbb{F}_2$-algebra with 1 generated by two elements, traditionally denoted Sq^1 and Sq^2 (examples of Steenrod squares), with relations $\mathrm{Sq}^1\mathrm{Sq}^1 = 0$ and $\mathrm{Sq}^2\mathrm{Sq}^2 = \mathrm{Sq}^1\mathrm{Sq}^2\mathrm{Sq}^1$. Then, it follows that $\mathcal{A}(1)$ has dimension 8 as a vector space over $\mathbb{F}_2$, with vector space basis 1, Sq^1, Sq^2, $\mathrm{Sq}^1\mathrm{Sq}^2$, $\mathrm{Sq}^2\mathrm{Sq}^1$, $\mathrm{Sq}^2\mathrm{Sq}^2 (= \mathrm{Sq}^1\mathrm{Sq}^2\mathrm{Sq}^1)$, $\mathrm{Sq}^2\mathrm{Sq}^1\mathrm{Sq}^2$ and $\mathrm{Sq}^2\mathrm{Sq}^2\mathrm{Sq}^2$. There is an involution on $\mathcal{A}(1)$, traditionally denoted χ, such that $\chi(\mathrm{Sq}^1) = \mathrm{Sq}^1$ and $\chi(\mathrm{Sq}^2) = \mathrm{Sq}^2$. Then $\chi(\mathrm{Sq}^1\mathrm{Sq}^2) = \mathrm{Sq}^2\mathrm{Sq}^1$, $\chi(\mathrm{Sq}^2\mathrm{Sq}^1) = \mathrm{Sq}^1\mathrm{Sq}^2$, and χ fixes the other basis elements. The algebra $\mathcal{A}(1)$ is a graded algebra, with constants having degree 0, Sq^1 having degree 1 and Sq^2 having degree 2.

Figure 1 is a display of the left module structure of $\mathcal{A}(1)$. The basis elements of $\mathcal{A}(1)$ are represented by dots. The dot on the far left is the basis element 1, and the others are arranged rightwards by increasing degree (Sq^1, then Sq^2, etc.; both $\mathrm{Sq}^2\mathrm{Sq}^1$ and $\mathrm{Sq}^1\mathrm{Sq}^2$ have degree three and are stacked vertically). Two basis elements are connected by a straight line segment if left multiplication by Sq^1 of the left endpoint yields the right endpoint. Similarly, two basis elements are connected by an arc if left multiplication by Sq^2 of the left endpoint yields the right endpoint. The involution χ flips the figure top to bottom. The ring $\mathcal{A}(1)$ is a Frobenius ring.

Remark 4: We see from these examples that Property $P1$ is independent of a ring being Frobenius.

Figure 1 The ring $\mathcal{A}(1)$



6 Property P2 and Frobenius rings

In this section, we suppose a finite ring R satisfies property $P1$, with anti-isomorphism ε. We are interested in finding examples of finite left R-modules satisfying property $P2$ with respect to ε; that is, a module A with an isomorphism $\psi : \varepsilon(A) \to \widehat{A}$ of right R-modules.

Theorem 4: *Let R be a ring with anti-isomorphism ε. Then, there exists a finite R-module A satisfying property $P2$ with respect to ε.*

Proof: Both the character functor $A \mapsto \widehat{A}$ and the ε-functor $A \mapsto \varepsilon(A)$ map the set of simple left R-modules bijectively to the set of simple right R-modules. Set A to be the direct sum of (one representative of each isomorphism class of) all the simple left R-modules. Then, both $\widehat{A}$ and $\varepsilon(A)$ are isomorphic to the sum of all the right simple R-modules. □

Lemma 2: *Suppose R satisfies $P1$ with anti-isomorphism ε. Consider the left regular module ${}_RR$. Then $\varepsilon({}_RR) \cong R_R$, as right R-modules.*

Proof: Observe that ε^{-1} provides the desired isomorphism $\varepsilon({}_RR) \to R_R$. □

Theorem 5: *Suppose R is a finite ring that admits an anti-isomorphism ε. Let the left module A be the ring itself: $A = {}_RR$. Then $A = {}_RR$ has property $P2$ with respect to ε, $\varepsilon(A) \cong \widehat{A}$, if and only if the ring R is a finite Frobenius ring.*

Moreover, when R is a finite Frobenius ring with generating character $\varrho\colon R \to \mathbb{Q}/\mathbb{Z}$, an isomorphism $\psi\colon \varepsilon({}_RR) \to \widehat{R}_R$ is given by $\psi(b) = \varrho\varepsilon^{-1}(b)$, the right scalar multiple of $\varrho \in \widehat{R}$ by $\varepsilon^{-1}(b) \in R$. The form $\beta\colon R^n \times R^n \to \mathbb{Q}/\mathbb{Z}$ associated to ψ by Equation (4) is given by

$$\beta(x, y) = \sum_{i=1}^{n} \varrho\big(\varepsilon^{-1}(y_i)x_i\big)$$

for $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in R^n$.

Proof: By Lemma 2, we know that $R_R \cong \varepsilon({}_RR)$. Thus, $A = {}_RR$ satisfies $P2$ if and only if $R_R \cong \varepsilon({}_RR) \cong \widehat{R}_R$. But $R_R \cong \widehat{R}_R$ if and only if R is Frobenius, by Wood (1999, Theorem 3.10).

Assume R is Frobenius, so that $R_R \cong \widehat{R}_R$. This isomorphism implies the existence of a character $\varrho \in \widehat{R}_R$ (called a *generating character*) so that $r \mapsto \varrho r$ is the isomorphism $R_R \to \widehat{R}_R$. By the proof of Lemma 2, we know that ε^{-1} provides an isomorphism $\varepsilon({}_RR) \to R_R$. Thus, $\psi(b) = \varrho\varepsilon^{-1}(b)$ is the composition of these isomorphisms $\varepsilon({}_RR) \to R_R \to \widehat{R}_R$. The formula for β now follows from Equation (4). □

Remark 5: Suppose R admits an anti-isomorphism ε, and let $A = R$. One can always define a form $\gamma\colon R^n \times R^n \to R$ by omitting ϱ in the formula for β:

$$\gamma(x, y) = \sum_{i=1}^{n} \varepsilon^{-1}(y_i)x_i$$

for $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in R^n$. One then uses γ to define left and right annihilators to a code $C\colon l(C) = \{y \in R^n : \gamma(y, C) = 0\}$ and $r(C) = \{y \in R^n : \gamma(C, y) = 0\}$. Both $l(C)$ and $r(C)$ are right submodules of R^n. When R is a Frobenius ring, these annihilators are the same as those defined by β (see Wood, 2009, Theorem 12.2). Property $P3$ implies that $l(C) = r(C)$ for left linear codes C.

Example 9: For all of the Frobenius rings appearing in the examples in Section 5 that admit an anti-isomorphism ε, ε and the left module $A = {}_R R$ satisfy $P2$.

Example 10: Let $R = \mathcal{A}(1)$ be the 8-dimensional algebra over $\mathbb{F}_2$ of Example 8; $\mathcal{A}(1)$ is a subalgebra of the mod 2 Steenrod algebra. Algebraic topology provides a rich source of $\mathcal{A}(1)$-modules, because the mod 2 cohomology of any finite CW complex is a finite module over the Steenrod algebra and, hence, by restriction of scalars, a finite module over $\mathcal{A}(1)$ (see Whitehead, 1978, Chapter VIII).

Here is a specific example: the mod 2 cohomology of the real projective space $\mathbb{R}P^n$. It is known that $H^*(\mathbb{R}P^n; \mathbb{F}_2)$ is a truncated polynomial algebra:

$$H^*\big(\mathbb{R}P^n; \mathbb{F}_2\big) \cong \mathbb{F}_2[a]/(a^{n+1}),$$

with $a \in H^1(\mathbb{R}P^n; \mathbb{F}_2)$, $a \neq 0$. The actions of the generators Sq^1, Sq^2 of $\mathcal{A}(1)$ are

$$\mathrm{Sq}^i\big(a^j\big) = \begin{cases} \binom{j}{i} a^{i+j}, & i+j \leq n \\ 0, & i+j > n \end{cases}$$

where the binomial coefficient is calculated mod 2 (see Whitehead, 1978, p.400).

Write $M = H^*(\mathbb{R}P^n; \mathbb{F}_2)$; M is both a left $\mathcal{A}(1)$-module and a vector space over $\mathbb{F}_2$ of dimension $n+1$. A basis of M is $1 = a^0, a, a^2, \ldots, a^n$. Figure 2 displays $H^*(\mathbb{R}P^7; \mathbb{F}_2)$ as an $\mathcal{A}(1)$-module, with the basis elements being represented by dots (and increasing in degree from $a^0 = 1$ on the far left, to a^7 on the far right) and left multiplication by Sq^1 and Sq^2 being displayed using the same conventions as in Figure 1. The character module $\widehat{M}$ is both a right $\mathcal{A}(1)$-module and an $\mathbb{F}_2$-vector space, with dual basis denoted $\varpi_0, \varpi_1, \ldots, \varpi_n$. As characters, $\varpi_i \colon M \to \mathbb{Q}/\mathbb{Z}$ satisfy $\varpi_i(a^j) = (1/2)\delta_{i,j} \in \mathbb{Q}/\mathbb{Z}$, where δ is the Kronecker delta.

One calculates in the right $\mathcal{A}(1)$-module $\widehat{M}$ that

$$\varpi_i \mathrm{Sq}^j = \begin{cases} \binom{i-j}{j} \varpi_{i-j}, & i-j \geq 0 \\ 0, & i-j < 0 \end{cases}$$

Define $\psi \colon M \to \widehat{M}$ by $\psi(a^j) = \varpi_{n-j}$. Then one calculates that

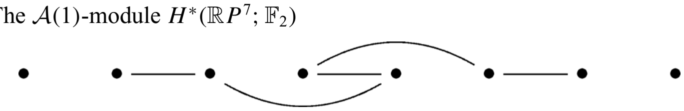
$$\psi\big(a^j \mathrm{Sq}^i\big) = \psi\big(\chi\big(\mathrm{Sq}^i\big)a^j\big) = \psi\big(\mathrm{Sq}^i a^j\big) = \psi\left(\binom{j}{i} a^{i+j}\right) = \binom{j}{i} \varpi_{n-i-j}$$

while

$$\varpi_{n-j} \mathrm{Sq}^i = \binom{n-j-i}{i} \varpi_{n-j-i}$$

The reader will verify that the binomial coefficients agree mod 2 when $n = 4l+3$. Thus, $M = H^*(\mathbb{R}P^n; \mathbb{F}_2)$ satisfies P2 when $n = 4l+3$.

Figure 2 The $\mathcal{A}(1)$-module $H^*(\mathbb{R}P^7; \mathbb{F}_2)$



For $M = H^*(\mathbb{R}P^7; \mathbb{F}_2)$, $\widehat{M}$ has the same display as in Figure 2. The dots represent the basis elements, from ϖ_0 on the far left, to ϖ_7 on the far right. For $\widehat{M}$, right multiplication by Sq^1 and Sq^2 decreases degree and hence moves from right to left.

In general, $M = H^*(\mathbb{R}P^n; \mathbb{F}_2)$ and $\widehat{M}$ have the same displays analogous to Figure 2, but with Sq^1 and Sq^2 going from left to right for M, while going from right to left for $\widehat{M}$. Then M will satisfy $P2$ when its display is left–right symmetric, which happens when $n = 4l+3$.

7 Property *P3* and self-dual codes

In this final section, we discuss property $P3$ and offer some examples of self-dual codes. The investigation of these codes is in its infancy, and all the examples are of length 1. More research will be needed in order to produce better examples.

Remember that a finite Frobenius ring R satisfies $R_R \cong \widehat{R}_R$ (Wood, 1999, Theorem 3.10). Thus, there exists a character $\varrho \in \widehat{R}$ called a *generating character* such that $R_R \to \widehat{R}_R$, $r \mapsto \varrho r$ (right scalar multiplication), is an isomorphism of right R-modules. Such a generating character also provides an isomorphism ${}_RR \to {}_R\widehat{R}$ of left R-modules via left scalar multiplication, $r \mapsto r\varrho$.

Lemma 3: *Suppose R is a Frobenius ring with generating character ϱ. If R satisfies $P1$ with anti-isomorphism ε, then there exists a unit $e \in R$ such that $\varrho \circ \varepsilon = \varrho e$. That is,*

$$\varrho(\varepsilon(r)) = (\varrho e)(r) = \varrho(er), \quad r \in R$$

Proof: We make use of a result of Wood (1999, Lemma 4.1, Theorem 4.3) that says that a character $\varpi \in \widehat{R}$ is a generating character if and only if $\ker \varpi$ contains no non-zero left (resp., right) ideals.

Claim: $\varrho \circ \varepsilon$ is a generating character. Suppose I is a left ideal with $I \subset \ker(\varrho \circ \varepsilon)$. Then, $\varepsilon(I)$ is a right ideal with $\varepsilon(I) \subset \ker \varrho$. Because ϱ is a generating character, $\varepsilon(I) = 0$. But ε is bijective, so $I = 0$, too. Thus, $\ker(\varrho \circ \varepsilon)$ contains no non-zero left ideals, and we conclude that $\varrho \circ \varepsilon$ is a generating character.

Both ϱ and $\varrho \circ \varepsilon$ are generators of $\widehat{R}_R$, so they are scalar multiples of each other. By a result of Bass (1964, Lemma 6.4), they must be unit multiples of each other. Thus, there exists a unit $e \in R$ such that $\varrho \circ \varepsilon = \varrho e$. □

In the statement of the next theorem, we use Theorem 5 and Lemma 3.

Theorem 6: *Suppose R is a finite Frobenius ring with generating character ϱ. Suppose R satisfies $P1$ with anti-isomorphism ε and $A = {}_RR$ satisfies $P2$ with isomorphism $\psi : \varepsilon({}_RR) \to \widehat{R}_R$ given by $\psi(b) = \varrho\varepsilon^{-1}(b)$ (right scalar multiplication).*

Suppose ε is an involution and that $\varrho \circ \varepsilon = \varrho e$ with unit e being central (i.e. e is in the centre of R; it commutes with every element of R). Then ψ satisfies P3, that is, $\widehat{\psi} = \psi e$.

Proof: Remember that $\widehat{\psi}(a)(b) = \psi(b)(a)$, $a, b \in R$. Because ε is an involution, $\psi(b) = \varrho\varepsilon(b)$. One then computes:

$$\begin{aligned}
\widehat{\psi}(a)(b) &= \psi(b)(a) = (\varrho\varepsilon(b))(a) = \varrho(\varepsilon(b)a) = \varrho(\varepsilon(\varepsilon(a)b)) \\
&= (\varrho \circ \varepsilon)(\varepsilon(a)b) = (\varrho e)(\varepsilon(a)b) = \varrho(e\varepsilon(a)b) = \varrho(\varepsilon(a)eb) \\
&= (\varrho\varepsilon(a))(eb) = \psi(a)(eb) = (\psi(a)e)(b)
\end{aligned}$$

The result now follows. □

We conclude this section with several examples.

Example 11: Let $\mathbb{F}_q$ be a finite field of order $q = p^f$. Then $\mathbb{F}_q$ is a Frobenius ring with generating character ϑ, as follows. Let $\mathrm{tr}\colon \mathbb{F}_q \to \mathbb{F}_p$ be the trace map from $\mathbb{F}_q$ to its prime subfield. If we view elements of $\mathbb{F}_p$ as integers mod p, then $\vartheta(a) = \mathrm{tr}(a)/p \in \mathbb{Q}/\mathbb{Z}$ (see Wood, 1999, Example 4.4(i)).

Let G be a finite group (with identity element e), and let $R = \mathbb{F}_q[G]$ be the group ring of G over $\mathbb{F}_q$. Let $r = \sum_{g \in G} r_g g \in R$, where $r_g \in \mathbb{F}_q$. Define $\varrho \in \widehat{R}$ by $\varrho(r) = \vartheta(r_e)$, where $r_e \in \mathbb{F}_q$ is the coefficient of e in $r \in R$. Then, ϱ is a generating character of R, by Wood (1999, Example 4.4(v)). By Example 4 and Theorem 5, $\beta\colon R \times R \to \mathbb{Q}/\mathbb{Z}$ has the form

$$\beta(r, s) = \varrho\left(\left(\sum_{h \in G} s_h h^{-1}\right)\left(\sum_{g \in G} r_g g\right)\right) = \vartheta\left(\sum_{g \in G} s_g r_g\right)$$

for $r, s \in R$. Thus, $\beta(r, s) = \beta(s, r)$, and $P3$ is satisfied.

Example 12: Let Σ_3 be the symmetric group on three letters; $|\Sigma_3| = 6$. The elements of Σ_3 are denoted $e, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2$, with $\tau^2 = e$, $\sigma^3 = e$ and $\sigma\tau = \tau\sigma^2$. Let $R = \mathbb{F}_2[\Sigma_3]$ be the group algebra of Σ_3 over $\mathbb{F}_2$, and let

$$e_1 = e + \sigma + \sigma^2$$
$$e_2 = e + \sigma + \tau\sigma + \tau\sigma^2$$
$$e_3 = e + \sigma^2 + \tau\sigma + \tau\sigma^2$$

Then e_1, e_2, e_3 are orthogonal idempotents that sum to e, which is the multiplicative identity of R.

The left ideals Re_2 and Re_3 are isomorphic, and they are simple, with dimension 2 over $\mathbb{F}_2$ (other basis elements are τe_2 and τe_3, respectively). The left ideal Re_1 is indecomposable and of dimension 2 over $\mathbb{F}_2$, but it is not simple. It has a 1-dimensional subideal $R(e+\tau)e_1$. The left ideals $C_1 = R(e + \tau)e_1 + Re_2$ and $C_2 = R(e + \tau)e_1 + Re_3$ are examples of self-dual codes in R.

Example 13: Let $R = \mathbb{F}_q[X; \sigma]/(X^{l+1})$. Let ϑ be a generating character for $\mathbb{F}_q$, as in Example 11. Let $r = \sum_{i=0}^{l} r_i X^i \in R$, where $r_i \in \mathbb{F}_q$. Define $\varrho\colon R \to \mathbb{Q}/\mathbb{Z}$ by $\varrho(r) = \vartheta(r_l)$, where r_l is the coefficient of X^l in $r \in R$. Then, ϱ is a generating character of R. Here is the argument. The ring R is a chain ring, so (X^l) is a minimal ideal (and (X^l) is the socle of R). If $\ker \varrho$ were to contain a non-zero ideal, then $(X^l) \subset \ker \varrho$. That is, $\varrho((X^l)) = 0$. But $\varrho(r_l X^l) = \vartheta(r_l)$, which is not identically zero, because ϑ is a generating character of $\mathbb{F}_q$.

Now assume that σ is an involution, so that R admits an involution ε and $A = R$ satisfies $P2$ (by Theorems 3 and 5). Using the ε from Theorem 3 and the structure of R from Example 7, $\beta\colon R \times R \to \mathbb{Q}/\mathbb{Z}$ has the form

$$\beta(r, s) = \varrho(\varepsilon(s)r) = \varrho\left(\left(\sum_{i=0}^{l} \sigma^i(s_i) X^i\right)\left(\sum_{j=0}^{l} r_j X^j\right)\right)$$

$$= \varrho\left(\sum_{i,j}\sigma^i(s_i)\sigma^i(r_j)X^{i+j}\right) = \vartheta\left(\sum_{i+j=l}\sigma^i(s_i)\sigma^i(r_j)\right)$$

$$= \sum_{i+j=l}\vartheta\left(\sigma^i(s_i r_j)\right) = \sum_{i+j=l}\vartheta(s_i r_j)$$

Here, we have used the fact that $\vartheta(\sigma(a)) = \vartheta(a)$ for $a \in \mathbb{F}_q$, because the trace satisfies $\mathrm{tr}(\sigma(a)) = \mathrm{tr}(a)$, $a \in \mathbb{F}_q$. Because the formula above for β is symmetric in r, s, we see that $\beta(r, s) = \beta(s, r)$, and $P3$ is satisfied.

When $l + 1 = 2k$ is even, $C = (X^k)$ is a self-dual code.

Example 14: Let $R = \mathcal{A}(1)$ be the 8-dimensional $\mathbb{F}_2$-algebra of Example 8. Refer to the $\mathbb{F}_2$-vector space basis elements as follows: $b_0 = 1$, $b_1 = \mathrm{Sq}^1$, $b_2 = \mathrm{Sq}^2$, $b_3 = \mathrm{Sq}^1\mathrm{Sq}^2$, $b_{3'} = \mathrm{Sq}^2\mathrm{Sq}^1$, $b_4 = \mathrm{Sq}^2\mathrm{Sq}^2$, $b_5 = \mathrm{Sq}^2\mathrm{Sq}^1\mathrm{Sq}^2$ and $b_6 = \mathrm{Sq}^2\mathrm{Sq}^2\mathrm{Sq}^2$. Set $I = \{0, 1, 2, 3, 3', 4, 5, 6\}$. We will write a typical element of $\mathcal{A}(1)$ as $r = \sum_{i\in I} r_i b_i$, with $r_i \in \mathbb{F}_2$. Let ϑ be a generating character for $\mathbb{F}_2$; if we view elements of $\mathbb{F}_2$ as integers mod 2, then $\vartheta(a) = a/2 \in \mathbb{Q}/\mathbb{Z}$. Define $\varrho \in \widehat{R}$ by $\varrho(r) = \vartheta(r_6)$, where r_6 is the coefficient of b_6 in $r \in \mathcal{A}(1)$. Then, ϱ is a generating character of $\mathcal{A}(1)$. Indeed, the socle of $\mathcal{A}(1)$ is the simple 1-dimensional ideal generated by $b_6 = \mathrm{Sq}^2\mathrm{Sq}^2\mathrm{Sq}^2$, and the argument given in Example 13 applies.

By Example 8, $\beta\colon \mathcal{A}(1) \times \mathcal{A}(1) \to \mathbb{Q}/\mathbb{Z}$ has the form

$$\beta(r, s) = \varrho(\chi(s)r) = \vartheta\left(\sum_{i+j=6} s_i r_j\right)$$

where we agree that $3 + 3' = 6$ (and $3 + 3$ and $3' + 3'$ do not sum to 6). Since the sum above is symmetric in r, s, we have $\beta(r, s) = \beta(s, r)$, and $P3$ is satisfied.

The left ideal $C = \mathcal{A}(1)(\mathrm{Sq}^2\mathrm{Sq}^1 + \mathrm{Sq}^1\mathrm{Sq}^2)$ is a self-dual code. A vector space basis for C is $\mathrm{Sq}^2\mathrm{Sq}^1 + \mathrm{Sq}^1\mathrm{Sq}^2$, $\mathrm{Sq}^2\mathrm{Sq}^2$, $\mathrm{Sq}^2\mathrm{Sq}^1\mathrm{Sq}^2$ and $\mathrm{Sq}^2\mathrm{Sq}^2\mathrm{Sq}^2$. Figures 3 and 4 offer two displays of this code. The filled-in dots are a basis for the code; the open dots are to allow comparison with Figure 1. In Figure 3, the symbol $\oslash$ is used because it is the sum of the elements $\mathrm{Sq}^2\mathrm{Sq}^1$ and $\mathrm{Sq}^1\mathrm{Sq}^2$ that belongs to C. Left multiplication by Sq^1, Sq^2 is represented as in Figure 1.

Figure 3 An $\mathcal{A}(1)$-linear self-dual code in $\mathcal{A}(1)$: first view

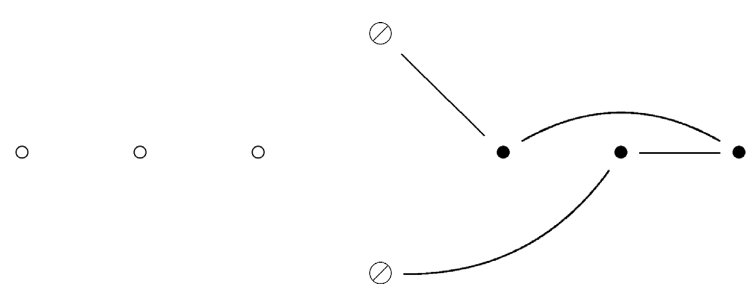


Figure 4 An $\mathcal{A}(1)$-linear self-dual code in $\mathcal{A}(1)$: second view

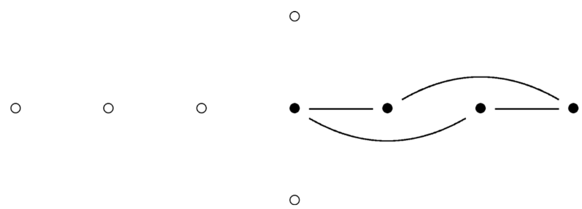


Figure 5 An $\mathcal{A}(1)$-linear self-dual code in $H^*(\mathbb{R}P^7; \mathbb{F}_2)$.

Example 15: Let $R = \mathcal{A}(1)$, as in Example 14. Let $M = H^*(\mathbb{R}P^n; \mathbb{F}_2)$, with $n = 4l + 3$, as in Example 10; M satisfies $P2$. A typical element of M has the form $r = \sum_{i=0}^{n} r_i a^i$, with $r_i \in \mathbb{F}_2$. Using ψ defined in Example 10, $\beta\colon M \times M \to \mathbb{Q}/\mathbb{Z}$ has the form

$$\begin{aligned}\beta(r, s) = \psi(s)(r) &= \left(\sum_{i=0}^{n} s_i \varpi_{n-i}\right)\left(\sum_{j=0}^{n} r_j a^j\right)\\ &= \sum_{i,j} s_i r_j \varpi_{n-i}(a^j) = \vartheta\left(\sum_{i=0}^{n} s_i r_{n-i}\right)\end{aligned}$$

where ϑ is the generating character for $\mathbb{F}_2$. The formula is symmetric in r, s, so $\beta(r, s) = \beta(s, r)$, and $P3$ is satisfied.

The vector subspace C spanned by $a^{2l+2}, a^{2l+3}, \ldots, a^{4l+3}$ has dimension $2l + 2$ and is a left $\mathcal{A}(1)$-submodule of M; C is a self-dual code. Figure 5 displays this self-dual code when $n = 7$. The filled-in dots are a basis for the code (namely a^4, a^5, a^6, a^7); the open dots are to allow comparison with Figure 2. Left multiplication by Sq^1 and Sq^2 is represented as in Figure 2.

Remark 6: The examples in this section have the feature that the rings R are algebras over a finite field $\mathbb{F}_q$, and the R-modules are vector spaces over $\mathbb{F}_q$. Then, R-linear self-dual codes can be viewed as self-dual codes over $\mathbb{F}_q$ with additional symmetry coming from R. One caution: the self-duality over $\mathbb{F}_q$ may involve an inner product β different from the standard dot product. The standard dot product occurs for group rings. An alternating form occurs in the other examples.

Acknowledgements

In addition to thanking Vera Pless once more for her help to me over my career, I gratefully acknowledge the influence of the book Nebe et al. (2006). I thank the two anonymous referees for their valuable comments, T.Y. Lam and Gabriele Nebe for helpful correspondence and conversations, Brian Nienow for his continued interest in my work, and my wife Elizabeth S. Moore for her unfailing support.

References

Bass, H. (1964) 'K-theory and stable algebra', *Institute des Hautes Études Scientique Publications Mathamatiques*, Vol. 22, pp.5–60.

Cronheim, A. (1978) 'Dual numbers, Witt vectors, and Hjelmslev planes', *Geometriae Dedicata*, Vol. 7, No. 3, pp.287–302.

Lam, T.Y. (1999) *Lectures on Modules and Rings*, Vol. 189 of *Graduate Texts in Mathematics*, New York: Springer-Verlag.

Lam, T.Y. (2003) *Exercises in Classical Ring Theory*, Problem Books in Mathematics, (2nd ed.), New York: Springer-Verlag.

Nebe, G., Rains, E.M. and Sloane, N.J.A. (2006) *Self-Dual Codes and Invariant Theory*, Volume 17 of *Algorithms and Computation in Mathematics*. Berlin: Springer-Verlag.

Terras, A. (1999) *Fourier Analysis on Finite Groups and Applications*, Volume 43 of *London Mathematical Society Student Texts*. Cambridge: Cambridge University Press.

Whitehead, G.W. (1978) *Elements of Homotopy Theory*, Volume 61 of *Graduate Texts in Mathematics*. New York: Springer-Verlag.

Wood, J.A. (1999) 'Duality for modules over finite rings and applications to coding theory', *American Journal of Mathematics*, Vol. 121, No. 3, pp.555–575.

Wood, J.A. (2009) 'Foundations of linear codes defined over finite modules: the extension theorem and the MacWilliams identities', in P. Solé, (Ed.), *Codes Over Rings (Ankara, 2008)*. *Series on Coding Theory and Cryptology*, Vol. 6, Singapore: World Scientific, pp.124–190.