J. Algebra Comb. Discrete Appl.
4(2) • 141–154

Received: 16 June 2015
Accepted: 18 February 2016

Journal of Algebra Combinatorics Discrete Structures and Applications

Codes and the Steenrod algebra

Research Article

Steven T. Dougherty, Tane Vergili

Abstract: We study codes over the finite sub Hopf algebras of the Steenrod algebra. We define three dualities for codes over these rings, namely the Eulidean duality, the Hermitian duality and a duality based on the underlying additive group structure. We study self-dual codes, namely codes equal to their orthogonal, with respect to all three dualities.

2010 MSC: 11T71, 94B05

Keywords: Self-dual codes, Non-commutative rings, Steenrod algebra

1. Introduction

Codes over commutative rings have received a great deal of attention since the discovery in the early 1990s that certain non-linear binary codes were in fact the images under a Gray map of codes over $\mathbb{Z}_4$. Very little work has been done yet on codes over non-commutative rings. In [11], J. Wood gave foundational results for codes over commutative and non-commutative rings. Specifically, he showed that Frobenius rings were the class of rings for which it was natural to study codes since both MacWilliams theorems hold in this case. In [4], Dougherty and Leroy described some general theorems about self-dual codes over non-commutative rings with respect to the Euclidean inner-product. In this work, we shall study codes over a family of non-commutative Frobenius rings that are of great importance in the study of algebraic topology. Namely, we study codes over the finite sub Hopf algebras of the Steenrod algebra.

We take a broader approach to duality in that we consider both the Euclidean and Hermitian inner-products as well as duality based on the underlying additive group structure. We consider linear codes as well as additive codes. Namely, linear codes are when the code is a submodule of the ambient space and additive codes are when they are simply a subgroup of the ambient space in terms of the additive operation.

Steven T. Dougherty (Corresponding Author); Department of Mathematics, University of Scranton, Scranton, PA 18510, USA (email: prof.steven.dougherty@gmail.com).
Tane Vergili; Department of Mathematics, Ege University, 35100 Izmir, Turkey (email: tanevergili@gmail.com).

2. Definitions and notations

2.1. Steenrod algebra

In this paper, we shall use as our coding alphabet, the Steenrod algebra at the prime 2. We assume throughout the paper that all computations in the Steenrod algebra and in the sub Hopf algebra are done with the assumption that the prime is 2. For a complete topological discussion about the Steenrod algebra see [10]. We shall now give an algebraic description of these algebras. We start our description by defining the Steenrod squaring operations Sq^k. By convention we have that $Sq^0 = 1$ and Sq^k is assigned grading k. The Steenrod algebra A is the free associative graded algebra generated by Sq^k over the field $\mathbb{F}_2$ subject to the following relations:

$$Sq^k Sq^j = \sum_{0 \leq i \leq \lfloor \frac{k}{2} \rfloor} \binom{j-i-1}{k-2i} Sq^{j+k-i} Sq^i \tag{1}$$

for $0 < k < 2j$. These relations are known as the Adem relations.

The Steenrod squares Sq^k are group homomorphisms

$$Sq^k : H^i(X; \mathbb{Z}_2) \longrightarrow H^{i+k}(X; \mathbb{Z}_2)$$

between the cohomology groups of a topological space X, for $k, i \geq 0$ satisfying the following (see [10] for a complete description):

1. The square Sq^0 is an identity and if $i < k$, then $Sq^k = 0$.
2. If $k = i$, then $Sq^k x = x^2$ for all $x \in H^i(X; \mathbb{Z}_2)$.
3. The square $Sq^k(x \cup y) = \sum_{k=k_1+k_2} Sq^{k_1}(x) \cup Sq^{k_2}(y)$, where the operation $\cup$ is the cup product of the cohomology ring $H^*(X; \mathbb{Z}_2) := \bigoplus_{n \geq 0} H^n(X; \mathbb{Z}_2)$ and $x, y \in H^*(X; \mathbb{Z}_2)$.

By utilizing $\mathbb{Z}_2$ as the coefficient group of the cohomology group, no sign problems occur.

The grading of the Steenrod square Sq^k is k and for the monomial formed as the composition of the Steenrod squares, $Sq^{k_1} Sq^{k_2} \cdots Sq^{k_i}$, is $k_1 + k_2 + \ldots + k_i$. Formally, the Steenrod algebra A is the graded associative algebra generated over the finite field $\mathbb{F}_2$ by the Steenrod squares subject to the Adem relations and the identity homomorphism Sq^0. The operations Sq^0 and Sq^{2^k}, $k \geq 0$, constitute a system of multiplicative generators for A, see [9] for a complete description.

The Steenrod algebra has a Hopf algebraic structure (see [7]) and is the union of the finite sub Hopf algebras $A(n)$, for $n \geq 0$, where $A(n)$ is generated by the squares Sq^{2^j} for $0 \leq j \leq n$ and Sq^0. Note that $A(n) \subseteq A(n+1)$ for all $n \geq 0$.

R. Wood [13] has defined the *atomic squares* which are of the form $Sq^{2^s(2^t-1)}$ where $s \geq 0$, $t > 0$ are integers such that $s + t \leq n + 1$, to form a Z base system for the $A(n)$ which can be extended to the whole algebra.

The Z base system for $A(n)$ is constructed as follows: Let

$$X_n = Sq^{1 \cdot 2^n} Sq^{3 \cdot 2^{n-1}} Sq^{7 \cdot 2^{n-2}} \cdots Sq^{2^{n+1}-1}$$

and define

$$Z_n := X_n X_{n-1} \cdots X_1 X_0.$$

For instance,

$$Z_1 = Sq^2Sq^3Sq^1,$$

$$Z_2 = Sq^4Sq^6Sq^7Sq^2Sq^3Sq^1,$$

$$\text{and } Z_3 = Sq^8Sq^{12}Sq^{14}Sq^{15}Sq^4Sq^6Sq^7Sq^2Sq^3Sq^1.$$

The element Z_n is the top element for $A(n)$ in terms of the grading. The set of $2^{(n+1)(n+2)/2}$ monomials obtained by selecting all subsets of atomic factors in Z_n, in the given order, is an additive basis for $A(n)$ (see [13]). We note that the product of the top element in $A(i)$ and the top element in $A(j)$ is 0 in the Steenrod Algebra, that is $Z_iZ_j = 0$, for all i, j, since it exceeds the maximum grading in $A(n)$ where $n = max\{i, j\}$. See [T. Vergili, I. Karaca, A note on the new basis in the mod 2 Steenrod algebra, in preparation, 2016] for a description of the basis of the Steenrod algebra. All computations done in this paper for the Steenrod algebra where performed using the computational tool given in [6]. Throughout the paper, we shall denote Sq^aSq^b by $Sq^{a,b}$ for convenience.

2.2. Codes and rings

A code C of length m over a ring R is a subset of R^m. If the code is a left module then we say that C is left linear and if C is a right module then we say that C is right linear.

Suppose R is a finite ring. Let $\widehat{M}$ denote the character module $Hom_{\mathbb{Z}}(M, \mathbb{C})$ where M is a module. The following are equivalent for finite rings, see [11]:

- R is a Frobenius ring.
- As a left module, $\widehat{R} \cong_R R$.
- As a right module $\widehat{R} \cong R_R$.

It is well known that $A(n)$ is a Frobenius ring for all n, see [11] for example. Next, we shall define an involution of the Steenrod algebra which also applies to the sub Hopf Algebras.

Define the map $\tau : A \to A$ by

$$\tau(Sq^0) = Sq^0, \text{ and } \tau(Sq^k) = \sum_{i=1}^{k} Sq^i\tau(Sq^{k-i}). \tag{2}$$

The map τ can be restricted to $A(n)$ in a natural way as long as $Sq^k \in A(n)$. It is well known that τ is an anti-isomorphism, that is, τ is additive and $\tau(ab) = \tau(b)\tau(a)$ and that τ^2 is the identity map. We note that τ is often written as χ in the literature, see [7], [14] and [10] for example, but we shall use χ as a generating character of the character module as is standard and use τ for this anti-isomorphism.

2.3. Orthogonals

We shall now describe inner-products which can be used in $A(n)^m$. In classical coding theory, the Euclidean inner-product is the standard inner-product. However, it is often the case that the Hermitian inner-product is used for specific applications. For example, it is used when self-dual codes over finite rings are used to construct Complex and Quaternionic lattices, see [3] and [2] for example.

Define the two following inner-products. The Euclidean inner-product is defined as

$$[\mathbf{v}, \mathbf{w}] = \sum v_iw_i. \tag{3}$$

The Hermitian inner-product is defined as

$$[\mathbf{v}, \mathbf{w}]_H = \sum v_i\tau(w_i). \tag{4}$$

Let C be a code then the left Euclidean orthogonal is

$$\mathcal{L}(C) = \{\mathbf{v} \mid [\mathbf{v}, \mathbf{w}] = 0, \ \forall \mathbf{w} \in C\} \tag{5}$$

and the right Euclidean orthogonal is

$$\mathcal{R}(C) = \{\mathbf{v} \mid [\mathbf{w}, \mathbf{v}] = 0, \ \forall \mathbf{w} \in C\}. \tag{6}$$

Let C be a code then left Hermitian orthogonal is

$$\mathcal{L}_H(C) = \{\mathbf{v} \mid [\mathbf{v}, \mathbf{w}]_H = 0, \ \forall \mathbf{w} \in C\} \tag{7}$$

and the right Hermitian orthogonal is

$$\mathcal{R}_H(C) = \{\mathbf{v} \mid [\mathbf{w}, \mathbf{v}]_H = 0, \ \forall \mathbf{w} \in C\}. \tag{8}$$

In [4], is shown that $\mathcal{L}(C)$ is a left linear code and $\mathcal{R}(C)$ is a right linear code. Of course, left linearity does not imply right linearity nor does right linearity imply left linearity.

We note that the notion of Hermitian and Euclidean duality are not identical. For example, let $a_1 = a_2 = Sq^{2,1}$. Then $a_1 a_2 = Sq^{2,3,1}$ but $a_1 \tau(a_2) = Sq^{2,1} Sq^3 = 0$. So $a_2 \in \mathcal{R}_H(A(1)[a_1])$ but $a_2 \notin \mathcal{R}(A(1)[a_1])$.

Theorem 2.1. *Let C be a code over $A(n)$ then $\mathcal{L}_H(C)$ is a left linear code.*

Proof. Let C be a code over $A(n)$. Let $\mathbf{v}, \mathbf{w} \in \mathcal{L}_H(C)$. Then

$$[a\mathbf{v} + c\mathbf{w}, \mathbf{u}]_H = \sum (av_i + cw_i)\tau(u_i) = a \sum v_i \tau(u_i) + c \sum w_i \tau(u_i) = 0 + 0 = 0.$$

Hence $a\mathbf{v} + c\mathbf{w} \in \mathcal{L}_H(C)$ and it is a left linear code. □

Unlike in the Euclidean case, $\mathcal{R}(C)$ is not necessarily right linear, since

$$[\mathbf{u}, \mathbf{v}a + \mathbf{w}c]_H = \sum u_i(\tau(v_i a + w_i c)) = \sum u_i \tau(a)\tau(v_i) + \sum u_i \tau(c)\tau(w_i)$$

which may or may not be 0. However, we do have the following theorem, which again is unlike the Euclidean case.

Theorem 2.2. *Let C be a code over $A(n)$. Then $\mathcal{L}_H(C) = \mathcal{R}_H(C)$.*

Proof. Let $\mathbf{w} \in \mathcal{L}_H(C)$. Then $[\mathbf{w}, \mathbf{v}]_H = 0$ for all $\mathbf{v} \in C$. This implies that $\sum w_i \tau(v_i) = 0$ which gives $\tau(\sum w_i \tau(v_i)) = \tau(0) = 0$. Then, we have $\sum \tau(\tau(v_i))\tau(w_i) = 0$ and finally $\sum v_i \tau(w_i) = 0$. This gives that $\mathbf{w} \in \mathcal{R}_H(C)$.

Let $\mathbf{w} \in \mathcal{R}_H(C)$. Then $[\mathbf{v}, \mathbf{w}]_H = 0$ for all $\mathbf{v} \in C$. This implies that $\sum v_i \tau(w_i) = 0$ which gives $\tau(\sum v_i \tau(w_i)) = \tau(0) = 0$. Then we have $\sum \tau(\tau(w_i))\tau(v_i) = 0$ and finally $\sum w_i \tau(v_i) = 0$. This gives that $\mathbf{w} \in \mathcal{L}_H(C)$. □

Example 2.3. *Consider the two sided ideal $A(1)[Sq^{3,1}] = \langle Sq^{3,1}, Sq^{2,3,1} \rangle$ in $A(1)$. Then we have that $\mathcal{R}_H(A(1)[Sq^{3,1}]) = \langle Sq^1, Sq^3, Sq^{2,1}, Sq^{2,3}, Sq^{3,1}, Sq^{2,3,1} \rangle = \mathcal{L}_H(A(1)[Sq^{3,1}])$ is also a two sided ideal in $A(1)$.*

Since the left and right Hermitian orthogonals are equal this gives that $\mathcal{R}_H(C)$ is left linear but it may not be right linear.

Example 2.4. *Let C be the code of length 1 over $A(1)$ defined by $A = A(1)[Sq^2 + Sq^{3,1}]$. Then $C = \langle Sq^2 + Sq^{3,1}, Sq^3, Sq^{2,3}, Sq^{3,1} + Sq^{2,3,1}, Sq^{2,3,1} \rangle$. Then $\mathcal{R}_H(C) = \langle Sq^3, Sq^{2,3}, Sq^{2,3,1} \rangle$. We have that $\mathcal{R}_H(C)$ is not right linear since $Sq^3 Sq^1 \notin \mathcal{R}_H(C)$.*

For any ring R let $\mathcal{J}(R)$ denote the Jacobson radical of R, which is defined as the intersection of all maximal left ideals in R.

Theorem 2.5. *Let $A(n)$ be the sub Hopf algebra and let $b_1, b_2, \ldots, b_t$ be the basis elements with $b_1 = Sq^0$ and $b_t = Z_n$. The ring $A(n)$ is a left and right local ring with unique two sided maximal ideal $M(n) = A(n)[b_2, b_3, \ldots, b_t] = \mathcal{J}(A(n))$. We have that $\mathcal{L}(M(n)) = \mathcal{R}(M(n)) = Soc(A(n)) = A(n)[b_t] = \{0, Z_n\}$.*

Proof. We know that $b_t b_i = b_i b_t = 0$ for all i, $1 < i \leq t$. Therefore $A(n)[b_t] = [b_t]A(n) = \{0, Z_n\}$ and $b_t \in \mathcal{L}(I)$ for all left and right ideals $I \subset A(n), I \neq A(n)$. Therefore $\mathcal{R}(\mathcal{L}(I)) = I \subseteq \mathcal{R}(A(n)[b_t])$ and $\mathcal{L}(\mathcal{R}(I)) = I \subseteq \mathcal{L}(A(n)[b_t])$. Then we have that

$$\mathcal{R}(A(n)[b_t]) = \mathcal{L}(A(n)[b_t]) = A(n)[b_2, b_3, \ldots, b_t] = [b_2, b_3, \ldots, b_t]A(n) = M(n).$$

Hence $A(n)[b_t]$ is the unique minimal ideal and its left and right dual is the unique maximal ideal. Therefore $Soc(A(n)) = A(n)[b_t] = \{0, Z_n\}$ and $\mathcal{J}(A(n)) = A(n)[b_2, b_3, \ldots, b_t]$. □

This leads naturally to the following corollary.

Corollary 2.6. *The two sided ideal $\{0, Z_n\}$ is contained in all non-trivial ideals of $A(n)$.*

3. MacWilliams relations

The MacWilliams relations are one of the foundational results of algebraic coding theory. They relate the weight enumerator of a linear code with the weight enumerator of its dual. The critical part of finding specific MacWilliams relations for a code over a ring R is to find a generating character for $\widehat{R}$. Namely, if $\phi : R \to \widehat{R}$ is a right R-module isomorphism then the generating character is $\phi(1)$. A generating character was given for $A(1)$ in [12].

Theorem 3.1. *Let $b_1, \ldots, b_t$ be a basis for $A(n)$ with $b_t = Z_n$. Define $\chi : A(n) \to \mathbb{C}^*$ by*

$$\chi(\sum_{i=1}^{t} a_i b_i) = (-1)^{a_t}, \tag{9}$$

where the $a_i \in \mathbb{F}_2$. Then χ is a generating character of $\widehat{A(n)}$.

Proof. It is immediate that χ is a homomorphism and hence a character of $A(n)$. We know from Corollary 2.6 that $b_t \in I$ for all non-zero left ideals I in $A(n)$. Also we have that $\chi(b_t) = -1$ so χ contains no non-zero ideals in its kernel. By Lemma 3.1 in [11], which states that a character is both a left generating and right generating character if it contains no non-trivial ideals in its kernel, we have that χ is a generating character for $\widehat{A(n)}$. □

Notice that the generating character for $A(n+1)$ is not an extension of the generating character for $A(n)$. We are not claiming that there is a unique generating character. To the contrary, any character whose kernel contains no non-trivial ideal is a generating character. We are simply identifying a useful generating character.

We know that $A(n)$ and $\widehat{A(n)}$ are isomorphic (although not canonically). Let χ_a be the character associated with the element a, then we have that $\chi_a(c) = \chi(ac)$, where χ is the generating character for $\widehat{A(n)}$.

Definition 3.2. *For a code over an alphabet $A = \{a_0, a_1, \ldots, a_{s-1}\}$, the complete weight enumerator is defined as:*

$$cwe_C(x_{a_0}, x_{a_1}, \ldots, x_{a_{s-1}}) = \sum_{\mathbf{c} \in C} \prod_{i=0}^{s-1} x_{a_i}^{n_i(\mathbf{c})} \tag{10}$$

where there are $n_i(\mathbf{c})$ occurrences of a_i in the vector $\mathbf{c}$.

Let T be the $|A(n)|$ by $|A(n)|$ matrix defined by $T_{a,c} = \chi(ac)$. For a matrix M and vector $\mathbf{v}$ we let $M \cdot \mathbf{v} = (M\mathbf{v}^t)^t$ so that the result is a row vector. In [11], Wood establishes the MacWilliams relations for codes over Frobenius rings.

Theorem 3.3. *If C is a left submodule of $A(n)^m$, then*

$$cwe_C(x_0, x_1, \ldots, x_k) = \frac{1}{|\mathcal{R}(C)|} cwe_{\mathcal{R}(C)}(T^t \cdot (x_0, x_1, \ldots, x_k)).$$

If C is a right submodule of $A(n)^m$, then

$$cwe_C(x_0, x_1, \ldots, x_k) = \frac{1}{|\mathcal{L}(C)|} cwe_{\mathcal{L}(C)}(T \cdot (x_0, x_1, \ldots, x_k)).$$

Let T_H be the $|A(n)|$ by $|A(n)|$ matrix with $(T_H)_{a,c} = \chi(a\tau(c))$. We notice that $(T_H)_{a,c}$ is not identical to $T_{a,c}$. Let $a = Sq^3$, $c = Sq^3$. Then $ac = Sq^{2,3,1} = Z_1$ and $a\tau(c) = 0$. Thus $\chi(ac) = -1$ but $\chi(a\tau(c)) = 1$. While $T \neq T^t$ in general, we do have the following for T_H.

Theorem 3.4. *Let $(T_H)_{a,c} = \chi(a\tau(c))$ where χ is the generating character for $\widehat{A(n)}$. Then $T_H = T_H^t$.*

Proof. We note that the anti-isomorphism τ preserves the grading of $A(n)$, so χ defined as $(-1)^{a_t}$ for the element $\sum a_i b_i$ with b_i the basis of $A(n)$, satisfies $\chi(a) = \chi(\tau(a))$.

Then

$$(T_H)_{a,c} = \chi(a\tau(c)) = \chi(\tau(a\tau(c)) = \chi(c\tau(a)) = (T_H)_{c,a}.$$

□

A similar proof to Theorem 3.3 applies to the Hermitian dual although it is not stated in [11]. Namely we have the following.

Theorem 3.5. *If C is a left submodule of $A(n)^m$, then*

$$cwe_C(x_0, x_1, \ldots, x_k) = \frac{1}{|\mathcal{R}_{\mathcal{H}}(C)|} cwe_{\mathcal{R}(C)}(T_H^t \cdot (x_0, x_1, \ldots, x_k)).$$

If C is a right submodule of $A(n)^m$, then

$$cwe_C(x_0, x_1, \ldots, x_k) = \frac{1}{|\mathcal{L}_{\mathcal{H}}(C)|} cwe_{\mathcal{L}(C)}(T_H \cdot (x_0, x_1, \ldots, x_k)).$$

The standard proof, setting $x_i = 1$, gives the following corollary.

Corollary 3.6. *If C is a left linear code over $A(n)$ then $|C||\mathcal{R}_H(C)| = |A(n)|^m$ and if C is a right linear code over $A(n)$ then $|C||\mathcal{L}_H(C)| = |A(n)|^m$.*

Example 3.7. *We continue with Example 2.4. Let C be the code of length 1 over $A(1)$ defined by $A = A(1)[Sq^2 + Sq^{3,1}]$. Then $C = \langle Sq^2 + Sq^{3,1}, Sq^3, Sq^{2,3}, Sq^{3,1} + Sq^{2,3,1}, Sq^{2,3,1}\rangle$. Then $\mathcal{R}_H(C) = \langle Sq^3, Sq^{2,3}, Sq^{2,3,1}\rangle$. Then $|C| = 2^5$ and $|\mathcal{R}_H(C)| = 2^3$ and $2^5 2^3 = |A(1)|$.*

4. Self-dual and Hermitian self-dual codes

Self-dual codes are one of the most widely studied families of codes, for both codes over rings and fields. They have interesting applications to designs, lattices and invariant theory. In a recent text [8] a very broad view of self-dual codes have been given with respect to various dualities and interesting connections to invariant theory have been given. In this section, we shall study self-dual codes over the finite ring $A(n)$. We begin with the definition for a self-dual code over a non-commutative ring.

Definition 4.1. *A linear code C is said to be Euclidean self-dual if $C = \mathcal{L}(C)$.*

It is shown in [4] that a code C that is equal to $\mathcal{L}(C)$ must also be equal to $\mathcal{R}(C)$. This implies that C is both left linear and right linear when it is self-dual. This implies that a self-dual code must be a bimodule.

Definition 4.2. *A linear code C is said to be Hermitian self-dual if $C = \mathcal{L}_H(C)$.*

We know that $\mathcal{L}_H(C) = \mathcal{R}_H(C)$ so a Hermitian self-dual code satisfies $C = \mathcal{L}_H(C) = \mathcal{R}_H(C)$.

We now investigate some results about self-orthogonality and self-duality. In [4] it is shown that if $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s$ are vectors over $A(n)$ such that $[\mathbf{v}_i, \mathbf{v}_j] = 0$ for all i and j, then

$$[\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s]A(n) \subseteq \mathcal{R}(A(n)[\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s]). \tag{11}$$

Notice that we do not necessarily have that $A(n)[\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s] \subseteq \mathcal{R}(A(n)[\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s])$ as we would have for commutative rings. For example, if $a = Sq^1$ and $c = Sq^2$ then $a^2 = 0$ but $(ca)^2 = (ca)(ca) = Sq^{2,3,1} \neq 0$. So the code $A(1)[a] \not\subseteq \mathcal{R}(A(1)[a])$. This means that more must be considered when generating a self-orthogonal code. Specifically, it is shown in [4] that if $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s$ are vectors in R^n, where R is any Frobenius ring, then $[\mathbf{v}_i, \alpha\mathbf{v}_j] = 0$ for all i, j and $\alpha \in R$ if and only if $\langle \mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s \rangle_L$ is a self-orthogonal code.

Theorem 4.3. *There exists Euclidean and Hermitian self-dual codes of length 2 over $A(n)$ for all n.*

Proof. Consider the code $C = A(n)[(Sq^0, Sq^0)]$. Then $\mathbf{v} \in C$ implies that $\mathbf{v} = (a, a)$ which gives $[(a, a), (c, c)] = ac + ac = 0$. Hence it is both left and right self-orthogonal. Then $|C| = |A(n)| = \sqrt{|A(n)|^2}$ and so the code is Euclidean self-dual.

For the Hermitian dual of C, we have $[(a, a), (c, c)]_H = a\tau(c) + a\tau(c) = 0$ and the remainder of the proof is identical. □

Using the standard techniques we have the following corollary.

Corollary 4.4. *There exist Euclidean and Hermitian self-dual codes for all even lengths over $A(n)$ for all n.*

Proof. If C and D are self-dual codes (Euclidean or Hermitian) of length m and m' respectively then $C \times D$ is a self-dual code of length $m + m'$. This gives the result. □

Theorem 4.5. *Let C be a binary self-dual code of length m, then reading 1 as Sq^0, we have $A(n)[C]$ is a Euclidean and Hermitian self-dual code.*

Proof. The code C has a basis of vectors $\mathbf{v}_i$ over $\mathbb{F}_2$. We note that m must be even for a binary self-dual code to exist. Then $|A(n)[\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{\frac{m}{2}}]| = |A(n)|^{\frac{m}{2}}$. Then

$$[\sum a_i\mathbf{v}_i, \sum c_j\mathbf{v}_j] = [\sum a_i\mathbf{v}_i, \sum \mathbf{v}_j c_j] = \sum_{i,j} a_i[\mathbf{v}_i, \mathbf{v}_j]c_j = 0, \tag{12}$$

since the elements in the coordinates of v_i commute with all of the elements of $A(n)$. Therefore the code is Euclidean self-dual.

Next consider

$$[\sum a_i\mathbf{v}_i, \sum c_j\mathbf{v}_j]_H = [\sum a_i\mathbf{v}_i, \sum \mathbf{v}_j c_j]_H \sum_{i,j} a_i[\mathbf{v}_i, \mathbf{v}_j]_H c_j = 0, \tag{13}$$

since the Hermitian inner-product and the Euclidean inner-product are identical for vectors with coordinates containing only 0 and Sq^0. □

The key to this result was that 0 and Sq^0 are in the center of the ring. If we take a self-orthogonal code over a subring which is not in the center the proof would not apply and the code over the larger ring generated by the code over the subring may not be self-orthogonal.

Theorem 4.6. *Let C be a non-trivial code of length 1 over $A(n)$. Then $Z_n \in \mathcal{R}(C), Z_n \in \mathcal{L}(C)$ and $Z_n \in \mathcal{R}_H(C) = \mathcal{L}_H(C)$,*

Proof. The codes $\mathcal{L}(C)$, $\mathcal{R}(C)$, and $\mathcal{L}_H(C) = \mathcal{R}_H(C)$ are left linear or right linear regardless if C is linear. Therefore, as non-trivial ideals, $\{0, Z_n\}$ is a subset of all of them by Corollary 2.6. □

Theorem 4.7. *1. Let $C = A(n)[\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s]$ and $C' = A(n+t)[\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s]$, $t > 0$. Then $\mathcal{R}(C) \subseteq \mathcal{R}(C')$ and $\mathcal{R}_H(C) \subseteq \mathcal{R}_H(C')$.*

2. Let $C = [\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s]A(n)$ and $C' = [\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s]A(n+t)$, $t > 0$. Then $\mathcal{L}(C) \subseteq \mathcal{L}(C')$ and $\mathcal{L}_H(C) \subseteq \mathcal{L}_H(C')$.

Proof. We prove only the first item, the second follows similarly. Let $\mathbf{w} \in \mathcal{R}(C)$. Consider the following inner-product:

$$[a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_s\mathbf{v}_s, \mathbf{w}] = a_1[\mathbf{v}_1, \mathbf{w}] + a_2[\mathbf{v}_2, \mathbf{w}] + \cdots + a_s[\mathbf{v}_s, \mathbf{w}] = 0. \tag{14}$$

Therefore $\mathbf{w} \in \mathcal{R}(C')$.

For the second part of the statement, let $\mathbf{w} \in \mathcal{R}_H(C)$. Consider the following inner-product:

$$[a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_s\mathbf{v}_s, \mathbf{w}]_H = a_1[\mathbf{v}_1, \mathbf{w}]_H + a_2[\mathbf{v}_2, \mathbf{w}]_H + \cdots + a_s[\mathbf{v}_s, \mathbf{w}]_H = 0. \tag{15}$$

Therefore $\mathbf{w} \in \mathcal{R}_H(C')$. □

5. Code over $A(n)$ and binary codes

Recall that $A(n)$ has a canonical basis with $2^{\frac{(n+1)(n+2)}{2}}$ elements. Then $|A(n)| = 2^{2^{(\frac{(n+1)(n+2)}{2})}}$. For example, $A(1)$ has 8 basis elements and 2^8 elements. For $A(2)$, the algebra has 2^6 basis elements and 2^{64} elements.

We now fix a basis $b_1, b_2, \ldots, b_t$ for $A(n)$ with $t = 2^{(\frac{(n+1)(n+2)}{2})}$. Let $a \in A(n) = \sum a_i b_i$. Define the map $\Psi : A(n) \to \mathbb{F}_2^t$ by

$$\Psi(a) = \Psi(\sum a_i b_i) = (a_1, a_2, \ldots, a_t). \tag{16}$$

Note that the map Ψ is dependent on the basis $b_1, b_2, \ldots, b_t$ for $A(n)$ and so we keep this ordering of the basis elements throughout the remainder of the paper.

By the definition of addition in $A(n)$ we have that Ψ is an additive map. We extend C to $A(n)^m$ by allowing it to act on each coordinate.

Definition 5.1. *A code C over $A(n)$ is an additive code if for all $\mathbf{v}, \mathbf{w} \in C$, $\mathbf{v} + \mathbf{w} \in C$.*

We see that an additive code is a subgroup of $(A(n))^m$ but it may not be a submodule. That is, a linear code is necessarily additive, but an additive code may not be linear.

Theorem 5.2. *Let C be an additive code over $A(n)$ of length m. Then $\Psi(C)$ is a linear binary code of length $2^{(\frac{(n+1)(n+2)}{2})}m$.*

Proof. We already have that Ψ is an additive map. Then the theorem follows by noting that an additive code over $\mathbb{F}_2$ is linear over $\mathbb{F}_2$. □

Example 5.3. *Let C be the code of length 1 over $A(1)$ defined as $C = A(1)[Sq^{2,1} + Sq^3]$. Then $\Psi(C)$ is the linear binary code generated by*

$$\begin{pmatrix} 0&0&0&1&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&1 \end{pmatrix}.$$

The following theorem has a proof similar to the one of Theorem 5.2.

Theorem 5.4. *Let C be a linear code over $\mathbb{F}_2$ of length $2^{(\frac{(n+1)(n+2)}{2})}m$. Then $\Psi^{-1}(C)$ is an additive code of length m over $A(n)$.*

Example 5.5. *Let C be the binary Hamming code of length 8. Then $\Psi^{-1}(C)$ is a subgroup of $A(1)$ but not a submodule. For example, the elements $Sq^0 + Sq^1 + Sq^2 + Sq^{2,3,1}$ and $Sq^2 + Sq^3 + Sq^{2,3} + Sq^{2,3,1}$ are both elements of $\Psi^{-1}(C)$ but their product $Sq^2 + Sq^{3,1}$ is not. It is easy to see that this element is not in the code since its corresponding vector in $\mathbb{F}_2^8$ would have Hamming weight 2 whereas the minimum Hamming weight of the length 8 Hamming code is 4.*

We can define an orthogonality relation for additive codes that will correspond to the orthogonality for binary codes. Let $G(n)$ be the additive group of $A(n)$. Order the elements of $G(n)$ by $g_1, g_2, \ldots, g_s$, where $s = 2^{(2^{\frac{(n+1)(n+2)}{2}})}$. Fix a character table TG for $\widehat{G}$ defined by

$$TG_{g_1,g_2} = -1^{[\Psi(g_1),\Psi(g_2)]}, \tag{17}$$

where $[\Psi(g_1), \Psi(g_2)]$ indicates the usual binary inner-product. Then χ_{g_i} corresponds to the row of TG given by $\chi(g_i g_j)$ where j goes from 1 to s.

Definition 5.6. *Let $\mathbf{v}, \mathbf{w} \in A(n)^m$. Define $[\mathbf{v}, \mathbf{w}]_G = \prod \chi_{v_i}(w_i)$.*

We note that the result of this inner-product is either 1 or -1. If C is an additive code over $A(n)$ define the orthogonal to be

$$C^* = \{(c_1, c_2, \ldots, c_m) \mid \prod \chi_{c_i}(v_i) = 1, \text{ for all } (v_1, v_2, \ldots, v_m) \in C\}. \tag{18}$$

Theorem 5.7. *If C is an additive code in $A(n)^m$, then*

$$cwe_C(x_0, x_1, \ldots, x_k) = \frac{1}{|C^*|} cwe_{C^*}(TG \cdot (x_0, x_1, \ldots, x_k)). \tag{19}$$

Proof. It follows from the standard MacWilliams relations for codes over groups. Namely, the matrix TG serves as a duality for the underlying additive group of the ring. □

Theorem 5.8. *Let C be a code over $A(n)$ then $\Psi(C^*) = \Psi(C)^\perp$.*

Proof. Let $\mathbf{v}, \mathbf{w} \in A(n)^m$. The following are equivalent statements:

1. $[\mathbf{v}, \mathbf{w}]_G = 1$
2. $\prod \chi_{v_i}(w_i) = 1$
3. $\prod (-1)^{[\Psi(v_i), \Psi(w_i)]} = 1$
4. $[\Psi(\mathbf{v}), \Psi(\mathbf{w})] = 0$.

This gives that $[\mathbf{v}, \mathbf{w}]_G = 1$ if and only if $[\Psi(\mathbf{v}), \Psi(\mathbf{w})] = 0$. □

The next corollary follows immediately from Theorem 5.8.

Corollary 5.9. *A code C in $(A(n))^m$ is self-dual with respect to the duality TG if and only if $\Psi(C)$ is a binary self-dual code.*

Corollary 5.10. *Self-dual codes exists for all lengths over $A(n)$ with respect to the duality TG.*

Proof. Since $2^{\frac{(n+1)(n+2)}{2}}$ is even, for all $n \geq 0$, there exists binary self-dual codes of all lengths $2^{\frac{(n+1)(n+2)}{2}} m$. Then apply Corollary 5.9. □

Note that we can replace the duality TG with a different duality for the group, which may or may not correspond directly to the binary orthogonality.

6. Codes over the Steenrod algebra

Just as we described codes over $A(n)$ we can extend these ideas to the infinite ring A. This was done in a similar way for codes over the p-adics in [1] and [5]. A code here is a subset of A^m and it is left linear or right linear if it is a left submodule or right submodule of A^m. Similarly, we can define $\mathcal{L}(C)$, $\mathcal{R}(C)$, $\mathcal{L}_H(C)$ and $\mathcal{R}_H(C)$ as in the finite case. We cannot define the group orthogonality since the underlying additive group is infinite and the technique no longer applies. Notice that in this infinite case, we have that $\mathcal{L}_H(C) = \mathcal{R}_H(C)$ as it is in the finite case.

We can now define a projection to $A(n)$. Let C be a code over A, then let

$$C_n = C \cap (A(n))^m. \tag{20}$$

Theorem 6.1. *Let C be a left (right) linear code over A then C_n is a left (right) linear code for all n.*

Proof. Assume C is left linear. Let $\mathbf{v}, \mathbf{w} \in C$ and $a, c \in A(n)$. Then $a\mathbf{v} + c\mathbf{w} \in C$ since C is left linear. Each coordinate of $\mathbf{v}$ and $\mathbf{w}$ is an element of $A(n)$ so $a\mathbf{v} + c\mathbf{w} \in (A(n))^m$ since the ring $A(n)$ is closed under addition and multiplication. Then $a\mathbf{v} + c\mathbf{w} \in C \cap (A(n))^m = C_n$ and C_n is left linear.

The proof in the right linear case is similar. □

In general we have $C_0 \subseteq C_1 \subseteq \cdots \subseteq C$.

Theorem 6.2. *Let C be a code over A.*

- *If $C \subseteq \mathcal{L}(C)$ then $C_n \subseteq \mathcal{L}(C_n)$.*
- *If $C \subseteq \mathcal{R}(C)$ then $C_n \subseteq \mathcal{R}(C_n)$.*
- *If $C \subseteq \mathcal{L}_H(C) = \mathcal{R}_H(C)$ then $C_n \subseteq \mathcal{L}_H(C_n) = \mathcal{R}_H(C)$.*

Proof. We prove the first case and the rest are similar. If $C \subseteq \mathcal{L}(C)$ then $C_n \subseteq C \subseteq \mathcal{L}(C)$ and $C_n \subseteq \mathcal{L}(C) \cap (A(n))^m \subseteq \mathcal{L}(C_n)$. □

In this sense self-orthogonality projects down but self-duality may not. For example, let $C_1 = A(1)(Sq^{2,1} + Sq^3)$, which is self-dual. But $C_0 \cap A(0) = \{0\}$ is not self-dual.

Lemma 6.3. *Let G be a binary matrix in standard form $(I\ |M)$ and let $C = A[G]$. Then $C_n = A(n)[G]$.*

Proof. If $\mathbf{v} \in C \cap (A(n))^m$ then the coefficients of the rows in the linear combination resulting in $\mathbf{v}$ must all be from $A(n)$ since the first part of the matrix is the identity. □

Theorem 6.4. *Let G be a matrix in standard form that generates a self-dual binary code, then $A[G]$ is a self-dual code over A.*

Proof. The proof of Theorem 4.5 shows that the code must be self-orthogonal. However, it does not show self-duality since it uses a cardinality argument.

Assume there exists $\mathbf{v} \in \mathcal{L}(C)$ with $\mathbf{v} \notin C$. Then for some n, we have that $\mathbf{v} \in A(n)^m$. This implies that $C_n = A(n)[G]$, by Lemma 6.3, has an element $\mathbf{v} \in \mathcal{L}(C_n), \mathbf{v} \notin C_n$ which contradicts Theorem 4.5. Therefore the code is self-dual. □

Let G generate a binary self-dual code of length m and let $C = A[G]$. Then C is self-dual and C_n is self-dual for all n. This gives infinite families of self-dual codes for all even lengths.

We shall now investigate some codes over A which we can then project down.

Lemma 6.5. *For all $\alpha \in A$ we have that $Z_1 \alpha Z_1 = 0$.*

Proof. Any α in A can be written as a sum of atomic squares so it is sufficient to prove the result for atomic squares.

- If α is one of the atomic squares in $A(1)$ then the claim is true since Z_1 is the top element of $A(1)$.
- Next, we consider the case for atomic squares with an odd power. Let $\alpha = Sq^{2^t-1}$ for $t \geq 3$ then

$$Sq^1 Sq^{2^t-1} = 0 \tag{21}$$

  since $2^t - 1$ is an odd number and the result follows from the Adem relations. Hence $Z_1 \alpha Z_1 = 0$.
- Next, we consider the case for atomic squares where the power of the atomic square is a power of 2. Let $\alpha = Sq^{2^s}$ for $s \geq 2$. First we multiply Z_1 and α. Note that if k is an even integer then from the Adem relations we have that

$$Sq^1 Sq^k = Sq^{k+1}. \tag{22}$$

  Then we have

$$Z_1 \alpha = Sq^2 Sq^3 Sq^1 Sq^{2^s} = Sq^2 Sq^3 Sq^{2^s+1}. \tag{23}$$

  For $s \geq 2$, $3 < 2(2^s + 1)$, we then apply the Adem relations to $Sq^3 Sq^{2^s+1}$ which gives

$$\begin{aligned} Sq^2 Sq^3 Sq^{2^s+1} &= Sq^2[\sum_{k=0}^{1} \binom{2^s - k}{3 - 2k} Sq^{2^s+4-k} Sq^k] \\ &= Sq^2[\binom{2^s}{3} Sq^{2^s+4} + \binom{2^s - 1}{1} Sq^{2^s+3} Sq^1]. \end{aligned}$$

The first term will be 0 since the binomial coefficient is an even number. Hence $Z_1\alpha = Sq^2Sq^3Sq^{2^s+1} = Sq^2Sq^{2^s+3}Sq^1$. Since $2 < 2(2^s+3)$ for $s \geq 2$, we can apply the Adem relations to $Sq^2Sq^{2^s+3}$, which gives

$$\begin{aligned} Sq^2Sq^{2^s+3}Sq^1 &= [\sum_{k=0}^{1} \binom{2^s+2-k}{2-2k} Sq^{2^s+5-k}Sq^k]Sq^1 \\ &= [\binom{2^s+2}{2} Sq^{2^s+5} + \binom{2^s+1}{0} Sq^{2^s+4}Sq^1]Sq^1 \\ &= Sq^{2^s+5}Sq^1 + Sq^{2^s+4}Sq^1Sq^1 \\ &= Sq^{2^s+5}Sq^1. \end{aligned}$$

Now we have $Z_1\alpha = Sq^{2^s+5}Sq^1$. If we multiply these with Z_1 from the right we have

$$Z_1\alpha Z_1 = Sq^{2^s+5}Sq^1Sq^2Sq^3Sq^1 = Sq^{2^s+5}(Sq^3Sq^3Sq^1) = Sq^{2^s+5}0 = 0. \tag{24}$$

- Next we consider the remaining two cases of atomic squares. Let $\alpha = Sq^{2(2^t-1)}$ where $t \geq 2$. From the Adem relations we have that $Sq^2Sq^3Sq^1 = Sq^5Sq^1$. Then

$$Z_1\alpha = Sq^2Sq^3Sq^1Sq^{2(2^t-1)} = Sq^5Sq^1Sq^{2(2^t-1)} = Sq^5Sq^{2^{t+1}-1}. \tag{25}$$

Since $5 < 2(2^{t+1}-1)$ for $t \geq 2$, we can apply the Adem relations to $Sq^5Sq^{2^{t+1}-1}$ which gives

$$\begin{aligned} Sq^5Sq^{2^{t+1}-1} &= \sum_{k=0}^{2} \binom{2^{t+1}-k-2}{5-2k} Sq^{2^{t+1}+4-k}Sq^k \\ &= \binom{2^{t+1}-2}{5} Sq^{2^{t+1}+4} + \binom{2^{t+1}-3}{3} Sq^{2^{t+1}+3}Sq^1 \\ &+ \binom{2^{t+1}-4}{1} Sq^{2^{t+1}+2}Sq^2 = 0, \end{aligned}$$

since the binomial coefficients are always even numbers. Hence we get $Z_1\alpha = 0$ so $Z_1\alpha Z_1 = 0$.

- We now consider the final case. Let $\alpha = Sq^{2^s(2^t-1)}$ where $s,t \geq 2$. We have that

$$Z_1\alpha = Sq^2Sq^3Sq^1Sq^{2^s(2^t-1)} = Sq^5Sq^1Sq^{2^s(2^t-1)} = Sq^5Sq^{2^s(2^t-1)+1}. \tag{26}$$

Since $5 < 2(2^s(2^t-1)+1)$ for $s,t \geq 0$, we can apply the Adem relations to $Sq^5Sq^{2^s(2^t-1)+1}$ which gives

$$\begin{aligned} Sq^5Sq^{2^s(2^t-1)+1} &= \sum_{k=0}^{2} \binom{2^s(2^t-1)-k}{5-2k} Sq^{2^s(2^t-1)+6-k}Sq^k \\ &= \binom{2^s(2^t-1)}{5} Sq^{2^s(2^t-1)+6} + \binom{2^s(2^t-1)-1}{3} Sq^{2^s(2^t-1)+5}Sq^1 \\ &+ \binom{2^s(2^t-1)-2}{1} Sq^{2^s(2^t-1)+4}Sq^2. \end{aligned}$$

The first and the last term are zero since the binomial coefficients are even. For the second term if the binomial coefficient is 0 then $Z_1\alpha = 0$ and $Z_1\alpha Z_1 = 0$. Otherwise it will be 1 and then $Z_1\alpha = Sq^{2^s(2^t-1)+5}Sq^1$ and then $Z_1\alpha Z_1$ will again be 0 as in the third case when the powers of the atomic squares were a power of 2.

□

This does not say that αZ_i is necessarily 0 for all α. For example, $Z_1Sq^4 = Sq^{9,1}$ and $Sq^4Z_1 = Sq^{7,2,1} + Sq^{9,1}$ but $Z_1Sq^4Z_1 = 0$.

Theorem 6.6. *Let $C = A[Z_1, Z_2, \dots]$ and $D = [Z_1, Z_2, \dots]A$. Then C and D are Hermitian self-orthogonal codes.*

Proof. For the left linear code C, we need to show that $[aZ_i, cZ_j]_H = 0$ for all integer $i, j \geq 1$. We have that $[aZ_i, cZ_j]_H = aZ_i\tau(cZ_j) = aZ_i\tau(Z_j)\tau(c) = aZ_iZ_j\tau(c) = a(0)\tau(c) = 0$. This gives that C is Hermitian self-orthogonal.

We note that $Z_i = \gamma Z_1$ and $Z_j = \delta Z_1$ for some $\gamma, \delta \in A(n)$, $n = max\{i, j\}$. For the right linear code D, we need to show that $[Z_ia, Z_jc]_H = 0$ for all integers $i, j \geq 1$. We have that $[Z_ia, Z_jc]_H = Z_ia\tau(Z_jc) = Z_i(a\tau(c))Z_j = \gamma(Z_1(a\tau(c)\delta)Z_1) = 0$ by Lemma 6.5. This gives that D is Hermitian self-orthogonal. □

Similarly, we have the following theorem.

Theorem 6.7. *Let $C = A[Z_1, Z_2, \dots]$ and $D = [Z_1, Z_2, \dots]A$. Then C and D are Euclidean self-orthogonal codes.*

Proof. As in the previous proof, we let $Z_i = \gamma Z_1$ and $Z_j = \delta Z_1$ for some $\gamma, \delta \in A(n)$, $n = max\{i, j\}$.

For the left linear code C we need to show that $[aZ_i, cZ_j] = 0$ for all integers $i, j \geq 1$. We have that $[aZ_i, cZ_j] = aZ_i(cZ_j) = a\gamma Z_1\beta\delta Z_1 = a\gamma(Z_1(\beta\delta)Z_1) = 0$ by Lemma 6.5. This gives that C is Euclidean self-orthogonal.

For the right linear code D, we need to show that $[Z_ia, Z_jc] = 0$ for all integers $i, j \geq 1$. We have that $[Z_ia, Z_jc] = \gamma Z_1a\delta Z_1c = \gamma(Z_1(a\delta)Z_1)c = 0$ by Lemma 6.5. This gives that D is Euclidean self-orthogonal. □

This leads naturally to the following corollary.

Corollary 6.8. *Let $C = A[Z_1, Z_2, \dots]$, $D = [Z_1, Z_2, \dots]A$, $C_n = C \cap (A(n))^m$ and $D_n = D \cap (A(n))^m$ then C_n and D_n are both Euclidean and Hermitian self-orthogonal codes for all n.*

Proof. The results follow directly from Theorem 6.6, Theorem 6.7 and Theorem 6.2. □

The code $C = A[Z_1, Z_2, \dots]$ is not self-dual. If it were then $\mathcal{L}(C)$ would be equal to $\mathcal{R}(C)$. However, $Sq^1Sq^6Z_1 = Sq^{9,3,1} \neq 0$ but $Z_n = \gamma Z_1 = \gamma Sq^2Sq^3Sq^1$ is $Z_nSq^1 = 0$ and $Sq^1 \notin \mathcal{L}(C)$ but $Sq^1 \in \mathcal{R}(C)$. In terms of the Hermitian inner-product, Sq^1 is in both duals but Sq^1 is not in C, hence the code is not Hermitian self-dual. Similar results hold for $D = [Z_1, Z_2, \dots]A$.

References

[1] A. R. Calderbank, N. J. A. Sloane, Modular and $p-$adic cyclic codes, Des. Codes Cryptog. 6(1) (1995) 21–35.

[2] Y. J. Choie, S. T. Dougherty, Codes over Σ_{2m} and Jacobi forms over the quaternions, Appl. Algebra Engrg. Comm. Comput. 15(2) (2004) 129–147.

[3] Y. J. Choie, S. T. Dougherty, Codes over rings, complex lattices and Hermitian modular forms, European J. Combin. 26(2) (2005) 145–165.

[4] S. T. Dougherty, A. Leroy, Euclidean self–dual codes over non–commuatative Frobenius rings, Appl. Alg. Engrg. Comm. Comp. 27 (3) (2016) 185–203.

[5] S. T. Dougherty, Y. H. Park, Codes over the $p-$adic integers, Des. Codes Cryptog. 39(1) (2006) 65–80.

[6] A. Kruckman, https://math.berkeley.edu/∼kruckman/adem/.
[7] J. Milnor, The Steenrod algebra and its dual, Ann. Math. 67(1) (1958) 150–171.
[8] G. Nebe, E. M. Rains, N. J. A. Sloane, Self–Dual Codes and Invariant Theory, Vol. 17, Algorithms and Computation in Mathematics, Springer–Verlag, Berlin, 2006.
[9] J. P. Serre, Cohomologie modulo 2 des complexes d'Eilenberg–Mac–Lane, Comment. Math. Helv. 27(1) (1953) 198–232.
[10] N. E. Steenrod, D. B. A. Epstein, Cohomology Operations, Ann. of Math. Studies, no.50, Princeton University Press, 1962.
[11] J. A. Wood, Duality for modules over finite rings and applications to coding theory, Amer. J. Math. 121(3) (1999) 555–575.
[12] 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.
[13] R. M. W. Wood, A note on bases and relations in the Steenrod algebra, Bull. Lond. Math. Soc. 27(4) (1995) 380–386.
[14] R. M. W. Wood, Problems in the Steenrod algebra, Bull. Lond. Math. Soc. 30(5) (1998) 449–517.