TÜBİTAK

Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2017) 41: 1313 – 1322

doi:10.3906/mat-1606-95

Examples of self-dual codes over some sub-Hopf algebras of the Steenrod algebra

Tane VERGİLİ*, İsmet KARACA
Department of Mathematics, Ege University, İzmir, Turkey

Received: 21.06.2016 • **Accepted/Published Online:** 19.12.2016 • **Final Version:** 28.09.2017

Abstract: Codes over the finite sub-Hopf algebras $A(n)$ of the (mod 2) Steenrod algebra $\mathcal{A}$ were studied by Dougherty and Vergili. In this paper we study some Euclidean and Hermitian self-dual codes over $A(n)$ by considering Milnor basis elements.

Key words: Hopf algebra, Steenrod algebra, self-dual codes

1. Introduction

The elements of the (mod 2) Steenrod algebra $\mathcal{A}$ are natural transformations between cohomology groups of topological spaces and useful tools for computing the homotopy groups of n-spheres. The finite subalgebras are determined by the profile functions h given in (4); each profile function constructs only one subalgebra [5]. Considering the function $h(t)$ given in equation (5), we construct the subalgebras $A(n)$ of $\mathcal{A}$ for all $n \geq 0$. These subalgebras are nested, i.e. $A(n)$ is contained in $A(m)$ if $n < m$, and their union is the entire algebra. Further, $A(n)$ is a noncommutative Frobenius ring, and so the MacWilliams theorems hold and one can study codes over $A(n)$ [8]. Dougherty and Vergili [2] studied the codes in $A(n)$ by considering the Z-base system over $A(n)$, which can be extended to the whole algebra $\mathcal{A}$ [10]. In this paper, we study codes over $A(n)$ by changing the base system. We use the Milnor basis, which is constructed in $\mathcal{A}$, compatible with $A(n)$, and provides a product formula for two Milnor basis elements. We examine a Euclidean and Hermitian self-dual code over $A(1)$ and show the generalization of that code to $A(n)$ is also a Euclidean and Hermitian self-dual.

2. Definitions and notations

2.1. The Steenrod algebra $\mathcal{A}$

The (mod 2) Steenrod algebra $\mathcal{A}$ is the free associative graded algebra generated by the following group homomorphisms (called square operations)

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

between the cohomology groups of topological spaces X for $i,k \geq 0$. The axiomatic properties of these squares are as follows [7]:

*Correspondence: tane.vergili@ege.edu.tr
2010 *AMS Mathematics Subject Classification:* 16L60, 16W30, 55S10, 94B05

1. The square Sq^0 is an identity homomorphism and if $i<k$, then $\mathrm{Sq}^k=0$.

2. If $k=i$, then $\mathrm{Sq}^k(x)=x^2$ for all $x\in H^i(X;\mathbb{Z}_2)$, where $x^2=x\cup x$ and $\cup$ is the cup product of the cohomology ring $H^*(X;\mathbb{Z}_2):=\bigoplus_{n\geq 0}H^n(X;\mathbb{Z}_2)$.

3. The Cartan formula for evaluating a Steenrod square on the cup product of cohomology classes x and y:

$$\mathrm{Sq}^k(x\cup y)=\sum_{k=k_1+k_2}\mathrm{Sq}^{k_1}(x)\cup\mathrm{Sq}^{k_2}(y).$$

4. All relations in the Steenrod algebra are generated by the set of Adem relations: for $k<2j$,

$$\mathrm{Sq}^k\mathrm{Sq}^j=\sum_{i=0}^{\lfloor\frac{k}{2}\rfloor}\left(\begin{array}{c} j-i-1\\ k-2i\end{array}\right)Sq^{k+j-i}Sq^i,$$

where $\lfloor\frac{k}{2}\rfloor$ denotes the greatest integer less than or equal to $\frac{k}{2}$ and the binomial coefficients are taken modulo 2.

Here k is called the *grading* of the square and the grading of the composition $\mathrm{Sq}^{i_1}\dots\mathrm{Sq}^{i_n}$ is $i_1+\dots+i_n$. For abbreviation, we use $\mathrm{Sq}^{i_1,\dots,i_n}$ for $\mathrm{Sq}^{i_1}\dots\mathrm{Sq}^{i_n}$.

Milnor [6] established that $\mathcal{A}$ is a Hopf algebra and finite dimensional vector space in each grading (we say in algebraic topology that the algebra is of finite type) and so the dual algebra $\mathcal{A}^*$ is also a Hopf algebra. Thus if we know what the dual algebra is, then the base system of dual algebra will help us to determine the base system of the Steenrod algebra.

Define the elements ξ_i in $\mathcal{A}^*$ by the dual of $\mathrm{Sq}^{2^{i-1},2^{i-2},\dots,1}$ in $\mathcal{A}$. Note that the degree of ξ_i is equal to the degree of $\mathrm{Sq}^{2^{i-1},2^{i-2},\dots,1}$, which is 2^i-1. Then the dual algebra $\mathcal{A}^*$ is a polynomial algebra $\mathbb{Z}_2[\xi_1,\xi_2,\dots]$. The dual to the monomial basis is a basis for the Steenrod algebra known as the *Milnor basis*. Denote the correspondence of $\xi_1^{r_1}\xi_2^{r_2}\dots\xi_n^{r_n}$ by $\mathrm{Sq}(r_1,r_2,\dots,r_n)$. Formally, $\mathcal{A}$ is a graded vector space over $\mathbb{Z}_2$ with the basis of all symbols $\mathrm{Sq}(r_1,r_2,\dots)$, where each $r_i\geq 0$ and all but a finite number of r_i's is zero. Note that $\mathrm{Sq}(0,0,\dots)$ is the identity and $\mathrm{Sq}(k)=\mathrm{Sq}^k$.

The Milnor basis is nice because it allows us to calculate the composition of the Steenrod operations in terms of Milnor basis elements again [6]. The product on $\mathcal{A}$ has the following expression in terms of the Milnor basis:

$$\mathrm{Sq}(r_1,r_2,\dots).\mathrm{Sq}(s_1,s_2,\dots)=\sum_X\beta(X)\mathrm{Sq}(t_1,t_2,\dots),\tag{1}$$

where the sum ranges over all matrices X of the form

$$X=\left\|\begin{array}{cccc} * & x_{01} & x_{02} & \dots\\ x_{10} & x_{11} & \dots & \\ x_{20} & \vdots & & \\ \vdots & & & \end{array}\right\|$$

such that

$$\sum_i x_{ij} = s_j, \quad \sum_j 2^j x_{ij} = r_i \quad t_k = \sum_{i+j=k} x_{ij}$$

and

$$\beta(X) = \prod_k \frac{(x_{k0} + ... + x_{0k})!}{x_{k0}!...x_{0k}!} \pmod 2.$$

Example 2.1 *Consider the Milnor product of* $\mathrm{Sq}(1,3,2).\mathrm{Sq}(2,0,1)$. *There are four matrices satisfying the desired conditions:*

$X_1 =$

		2	0	1
	*	2	0	1
1	1	0	0	0
3	3	0	0	0
2	2	0	0	0

$X_2 =$

		2	0	1
	*	1	0	1
1	1	0	0	0
3	3	0	0	0
2	0	1	0	0

$X_3 =$

		2	0	1
	*	1	0	1
1	1	0	0	0
3	1	1	0	0
2	2	0	0	0

$X_4 =$

		2	0	1
	*	0	0	1
1	1	0	0	0
3	1	1	0	0
2	0	1	0	0

For the matrix X_1, $t_i = 3$ *for all* $1 \leq i \leq 3$, $t_j = 0$ *for all* $j \geq 4$ *and*

$$\beta(X_1) = \frac{3!}{2!1!}\frac{3!}{3!}\frac{3!}{2!1!} = 1 \pmod 2.$$

For the matrix X_2, $t_1 = 2$, $t_2 = 3$, $t_3 = 1$, $t_4 = 1$, $t_j = 0$ *for all* $j \geq 5$ *and*

$$\beta(X_2) = \frac{2!}{1!1!}\frac{3!}{3!}\frac{1!}{1!}\frac{1!}{1!} = 0 \pmod 2.$$

For the matrix X_3, $t_1 = 2$, $t_2 = 1$, $t_3 = 4$, $t_j = 0$ *for all* $j \geq 4$ *and*

$$\beta(X_3) = \frac{2!}{1!1!}\frac{1!}{1!}\frac{4!}{2!1!1!} = 0 \pmod 2.$$

For the matrix X_4, $t_1 = 1$, $t_2 = 1$, $t_3 = 2$, $t_4 = 1$, $t_j = 0$ *for all* $j \geq 5$ *and*

$$\beta(X_4) = \frac{1!}{1!}\frac{1!}{1!}\frac{2!}{1!1!}\frac{1!}{1!} = 0 \pmod 2.$$

Therefore, $\mathrm{Sq}(1,3,2).\mathrm{Sq}(2,0,1) = \mathrm{Sq}(3,3,3)$.

The conjugation map (involution) [6] in $\mathcal{A}$

$$\tau : \mathcal{A} \longrightarrow \mathcal{A} \tag{2}$$

is defined on the Steenrod squares by [7]

$$\tau(\mathrm{Sq}^k) = \sum_{i=1}^{k} \mathrm{Sq}^i \tau(\mathrm{Sq}^{k-i}). \tag{3}$$

In the literature the conjugation map in $\mathcal{A}$ is denoted by χ but we shall use τ to use the common notation in [2] and to prevent confusion with the fact that the letter χ is used for a generating character of the character module in coding theory.

Let A be a sub-Hopf algebra of $\mathcal{A}$. Then the *profile function* defined by

$$h_A : \{1, 2, \ldots\} \longrightarrow \{0, 1, \ldots, \infty\}$$
$$t \longmapsto h_A(t) = \min\{s \ : \ r_t < 2^s \text{ for all } Sq(r_1, \ldots) \text{ in } A\}.$$

gives us a classification of the basis elements for A. (Note that if no such s exists, we take $h_A(t) = \infty$ [5]). The Milnor basis for A is

$$\{\mathrm{Sq}(r_1, r_2, \ldots) \ : \ r_t < 2^{h_A(t)}\}.$$

Moreover, A is generated as an algebra by the set

$$\{P_t^s \ : \ s < h_A(t)\},$$

where $P_t^s = \mathrm{Sq}(r_1, \ldots)$ is a Milnor basis element in A with $r_i = 0$ unless $i = t$ and $r_t = 2^s$ for $t \geq 1$ and $s \geq 0$.

In contrast, every function

$$h : \{1, 2, \ldots\} \longrightarrow \{0, 1, \ldots, \infty\} \tag{4}$$

satisfying

$$h(u) \leq v + h(u + v) \quad \text{or} \quad h(v) \leq h(u + v), \quad \text{for all } u, v \geq 1$$

is a profile function and generates a sub-Hopf algebra of $\mathcal{A}$ [5]. Now we focus on a special profile function

$$h(t) = \max\{n + 2 - t, 0\} \tag{5}$$

to construct our desired sub-Hopf algebras $A(n)$ of $\mathcal{A}$ for each $n \geq 0$. From this construction $A(n)$ is contained in $A(n + 1)$ for all $n \geq 0$. Thus the Steenrod algebra $\mathcal{A}$ is then the union of an increasing chain of sub-Hopf algebras $A(n)$ [5].

Example 2.2 *By the profile function $h(t)$ given in (5), the basis elements for $A(1)$ are*

$$\mathrm{Sq}(0) = 1, \ \mathrm{Sq}(0, 1), \ \mathrm{Sq}(1, 0), \ \mathrm{Sq}(1, 1), \ \mathrm{Sq}(2, 0), \ \mathrm{Sq}(2, 1), \ \mathrm{Sq}(3, 0), \ \mathrm{Sq}(3, 1).$$

For the proof of Lemma 2.3, we use Gallant's formula for conjugation of the special Milnor basis element P_t^s defined above. Let $R = (0, \ldots, r_1, 0, \ldots, r_2, \ldots)$ be a sequence whose components are zero except possibly for the elements r_i in the (i)-th place and $\mathrm{Sq}(R)$ be a Milnor basis element corresponding to R. Then $\tau(P_t^s)$ is the sum of all Milnor basis elements $Sq(R)$, where the grading of R is $2^s(2^t - 1)$ [3]:

$$\tau(P_t^s) = \sum_{R} \mathrm{Sq}(R). \tag{6}$$

By means of the equation (6), we have the following lemma.

Lemma 2.3 *Let* $P^0_{n+1} := \mathrm{Sq}(0,\dots,0,1)$ *be a Milnor basis element in* $A(n)$*, where* 1 *occurs in position* $n+1$*. Then* $\tau(P^0_{n+1}) = P^0_{n+1}$*.*

Proof Note that the grading of P^0_{n+1} is $2^{n+1}-1$. Here the only sequence $R=(0,\dots,r_1,0,\dots,r_2,\dots)$ with the grading $2^{n+1}-1$ is $R=(0,\dots,0,1)$ where 1 is in position $n+1$. Hence $\tau(P^0_{n+1}) = \mathrm{Sq}(0,\dots,1) = P^0_{n+1}$. □

2.2. Codes and rings

Let R be a ring with identity and τ be an involution on R. Then a subset C of length m in R^m is called a *code* and a *left (right) linear code* C of length m over R is a left (right) submodule of R^m.

Let $\boldsymbol{v}$, $\boldsymbol{\omega}$ be in R^m. The Euclidean and Hermitian inner-products are defined as

$$[\boldsymbol{v},\boldsymbol{\omega}] = \sum v_i\omega_i. \tag{7}$$

$$[\boldsymbol{v},\boldsymbol{\omega}]_H = \sum v_i\tau(\omega_i) \tag{8}$$

respectively.

For a code C in R^m, *the left (and the right) Euclidean orthogonal of* C is

$$\mathcal{L}(C) = \{\boldsymbol{v}\in R^m \ : \ [\boldsymbol{v},\boldsymbol{\omega}] = 0,\ \forall\boldsymbol{\omega}\in C\}, \tag{9}$$

$$\mathcal{R}(C) = \{\boldsymbol{v}\in R^m \ : \ [\boldsymbol{\omega},\boldsymbol{v}] = 0,\ \forall\boldsymbol{\omega}\in C\} \tag{10}$$

respectively.

Similarly *the left (and the right) Hermitian orthogonal of* C is

$$\mathcal{L}_H(C) = \{\boldsymbol{v}\in R^m \ : \ [\boldsymbol{v},\boldsymbol{\omega}]_H = 0,\ \forall\boldsymbol{\omega}\in C\}, \tag{11}$$

$$\mathcal{R}_H(C) = \{\boldsymbol{v}\in R^m \ : \ [\boldsymbol{\omega},\boldsymbol{v}]_H = 0,\ \forall\boldsymbol{\omega}\in C\} \tag{12}$$

respectively.

It follows easily that $\mathcal{L}(C)$ is always a left linear code and $\mathcal{R}(C)$ is always a right linear code [1]. Moreover, it is shown in [2] that for any code C, $\mathcal{L}_H(C)$ is a left linear code but $\mathcal{R}_H(C)$ is not necessarily right linear.

3. Self-dual codes in $A(n)$

The definition for a self-dual code over a noncommutative ring is as follows:

Definition 3.1 *A linear code* C *is said to be* Euclidean self-dual *if* $C = \mathcal{L}(C)$*.*

Dougherty and Leroy [1] proved that a code C that is equal to $\mathcal{R}(C)$ is also equal to $\mathcal{L}(C)$ and vice versa. Hence for a Euclidean self-dual code C, we have $C = \mathcal{L}(C) = \mathcal{R}(C)$.

Definition 3.2 *A linear code C is said to be* Hermitian self-dual *if* $C = \mathcal{L}_H(C)$.

Note that for a code C over $A(n)$, we have $\mathcal{R}_H(C) = \mathcal{L}_H(C)$ and so a Hermitian self-dual code satisfies $C = \mathcal{L}_H(C) = \mathcal{R}_H(C)$ [2].

In [1], it is stated that all self-dual codes of length 1 are two-sided ideals contained in the Jacobson radical of the ring. Since the Steenrod algebra $\mathcal{A}$ is a prime ring [4], the Jacobson radical of the Steenrod algebra is trivial and hence no self-dual code of length 1 exists in $\mathcal{A}$.

For a ring R with identity, we define the submodule $R[a] := \{ra \ : \ r \in R\}$.

Example 3.3 *[9] Take the submodule $C = A(1)[\mathrm{Sq}(0,1)]$ of $A(1)$. Considering the Milnor product of the Milnor basis elements for $A(1)$ and $\mathrm{Sq}(0,1)$, we get*

$$\mathrm{Sq}(0).\mathrm{Sq}(0,1) = \mathrm{Sq}(0,1), \quad \mathrm{Sq}(0,1).\mathrm{Sq}(0,1) = 0, \quad \mathrm{Sq}(1,0).\mathrm{Sq}(0,1) = \mathrm{Sq}(1,1),$$
$$\mathrm{Sq}(1,1).\mathrm{Sq}(0,1) = 0, \quad \mathrm{Sq}(2,0).\mathrm{Sq}(0,1) = \mathrm{Sq}(2,1), \quad \mathrm{Sq}(2,1).\mathrm{Sq}(0,1) = 0,$$
$$\mathrm{Sq}(3,0).\mathrm{Sq}(0,1) = \mathrm{Sq}(3,1), \quad \mathrm{Sq}(3,1).\mathrm{Sq}(0,1) = 0.$$

Hence the submodule C is spanned by these elements and contains their $\mathbb{Z}_2$ linear sums:

$$C =< \mathrm{Sq}(0,1), \mathrm{Sq}(1,1), \mathrm{Sq}(2,1), \mathrm{Sq}(3,1) > .$$

Then C is a Euclidean and a Hermitian self-dual code in $A(1)$, i.e. $\mathcal{R}(C) = C = \mathcal{R}_H(C)$.

The Example 3.3 can be generalized for the self-dual codes in $A(n)$ for $n \geq 1$. Consider the Milnor basis element $\mathrm{Sq}(0,\ldots,0,1)$, where 1 is in position $n+1$. The following two lemmas are needed for the proofs of Theorem 3.6 and Theorem 3.7.

Lemma 3.4 *Let $\mathrm{Sq}(0,\ldots,0,1)$ be a Milnor basis element where 1 is in position $n+1$. Then*

$$\mathrm{Sq}(r_1, r_2, \ldots, r_n).\mathrm{Sq}(0,\ldots,0,1) = \mathrm{Sq}(r_1, r_2, \ldots, r_n, 1),$$

where $\mathrm{Sq}(r_1, r_2, \ldots, r_n)$ is in $A(n)$ for all $n \geq 1$.

Proof To make the number of entries of the given basis elements equal, consider $\mathrm{Sq}(r_1, r_2, \ldots, r_n)$ as $\mathrm{Sq}(r_1, r_2, \ldots, r_n, 0)$. Then there is only one matrix X satisfying the desired conditions:

X=

		0	0	$\cdots$	0	1
	$*$	0	0	$\ldots$	0	1
r_1	r_1	0	0	$\ldots$	0	0
r_2	r_2	0	0	$\ldots$	0	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
r_n	r_n	0	0	$\ldots$	0	0
0	0	0	0	$\ldots$	0	0

Here for the matrix X, $t_i = r_i$ for $1 \leq i \leq n$, $t_{n+1} = 1$ and

$$\beta(X) = \prod \frac{r_i!}{r_i!} \frac{1!}{1!} = 1 \pmod 2.$$

Hence $\mathrm{Sq}(r_1, r_2, \ldots, r_n).\mathrm{Sq}(0, \ldots, 0, 1) = \mathrm{Sq}(r_1, r_2, \ldots, r_n, 1)$. □

Lemma 3.5 *Consider the Milnor basis* $\mathrm{Sq}(0, \ldots, 0, 1)$, *where* 1 *is in position* $n+1$. *Then*

$$\mathrm{Sq}(r_1, r_2, \ldots, r_n, 1).\mathrm{Sq}(0, 0, \ldots, 0, 1) = 0$$

for all Milnor basis elements $\mathrm{Sq}(r_1, \ldots, r_n, 1)$ *in* $A(n)$.

Proof Since $\mathrm{Sq}(r_1, r_2, \ldots, r_n, 1)$ is a Milnor basis element in $A(n)$ then all r_i's are less than 2^{n+1} and so the only matrix satisfying the desired conditions for the Milnor product of the given basis elements is

X=

		0	0	$\cdots$	0	1
	$*$	0	0	$\ldots$	0	1
r_1	r_1	0	0	$\ldots$	0	0
r_2	r_2	0	0	$\ldots$	0	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
r_n	r_n	0	0	$\ldots$	0	0
1	1	0	0	$\ldots$	0	0

In this matrix, $t_i = r_i$ for $1 \leq i \leq n$, $t_{n+1} = 2$ and

$$\beta(X) = \prod_{i=1}^{n} \frac{r_i!}{r_i!} \frac{2!}{1!1!} = 0 \pmod 2.$$

Hence $\mathrm{Sq}(r_1, r_2, \ldots, r_n, 1).\mathrm{Sq}(0, \ldots, 0, 1) = 0$. □

The generalizations of Example 3.3 for the Euclidean and the Hermitian self-dual codes in $A(n)$ for $n \geq 1$ are as follows:

Theorem 3.6 *The submodule* $C = A(n)[\mathrm{Sq}(0, \ldots, 0, 1)]$ *in* $A(n)$ *is a Euclidean self-dual code for all* $n \geq 1$.

Proof Note that the sub-Hopf algebra $A(n)$ is spanned by the Milnor basis elements $\mathrm{Sq}(r_1, r_2, \ldots, r_{n+1})$, where

$$r_{n+1} < 2, \quad r_n < 4, \quad \ldots, \quad r_2 < 2^n, \quad r_1 < 2^{n+1}.$$

If $r_{n+1} = 1$, we have

$$\mathrm{Sq}(r_1, \ldots, r_n, 1).\mathrm{Sq}(0, \ldots, 0, 1) = 0$$

by Lemma 3.5 and if $r_{n+1} = 0$, by Lemma 3.4 the product

$$\mathrm{Sq}(r_1, \ldots, r_n, 0).\mathrm{Sq}(0, \ldots, 0, 1) = \mathrm{Sq}(r_1, \ldots, r_n, 1)$$

is again a Milnor basis element for $A(n)$. Thus the submodule C is spanned by all Milnor basis elements of the form

$$\mathrm{Sq}(r_1, r_2, \ldots, r_n, 1)$$

and their $\mathbb{Z}_2$ linear sums. We claim that $C = \mathcal{R}(C)$. Hence we must show that any Milnor basis element for $A(n)$ in C is in $\mathcal{R}(C)$ and vice versa. Let c be a Milnor basis element in C of the form

$$c = \mathrm{Sq}(s_1, s_2, \ldots, s_n, 1).$$

By the product formula given in (1), we have

$$\mathrm{Sq}(r_1, r_2, \ldots, r_n, 1).c = \mathrm{Sq}(r_1, r_2, \ldots, r_n, 1).\mathrm{Sq}(s_1, s_2, \ldots, s_n, 1) = 0,$$

for all Milnor basis element $\mathrm{Sq}(r_1, r_2, \ldots, r_n, 1)$ in C and thus c is in $\mathcal{R}(C)$.

Now let c be a Milnor basis element in $\mathcal{R}(C)$ of the form

$$\mathrm{Sq}(s_1, s_2, \ldots, s_n, s_{n+1}).$$

Take any Milnor basis element $\mathrm{Sq}(r_1, r_2, \ldots, r_n, 1)$ in C. Since c is in $\mathcal{R}(C)$, we have

$$\mathrm{Sq}(r_1, r_2, \ldots, r_n, 1).c = \mathrm{Sq}(r_1, r_2, \ldots, r_n, 1).\mathrm{Sq}(s_1, s_2, \ldots, s_n, s_{n+1}) = 0.$$

Note that s_{n+1} is either 1 or 0. However, s_{n+1} cannot be zero since $\mathrm{Sq}(0, \ldots, 0, 1)$ is in C and the product

$$\mathrm{Sq}(0, 0, \ldots, 1).\mathrm{Sq}(s_1, s_2, \cdots, s_n, 0) = \mathrm{Sq}(s_1, s_2, \ldots, s_n, 1)$$

is not zero. Therefore $s_{n+1} = 1$ and this shows that c is in C.

The equality $C = \mathcal{R}(C)$ leads to $C = \mathcal{L}(C)$ and so C is a Euclidean self-dual code in $A(n)$. □

Theorem 3.7 *The submodule $C = A(n)[\mathrm{Sq}(0, \ldots, 0, 1)]$ of $A(n)$ is a Hermitian self-dual code for all $n \geq 1$.*

Proof We know that the submodule C is spanned by all the elements in the Milnor basis in $A(n)$ whose entry in the $(n+1)$th place is 1. We will show that $C = \mathcal{R}_H(C)$ (hence $C = \mathcal{L}_H(C)$). Again we only consider the Milnor basis elements. Let c be a Milnor basis element for $A(n)$ in C of the form

$$c = \mathrm{Sq}(s_1, s_2, \ldots, s_n, 1)$$

By the product formula in (1) and Lemma 3.5, we have

$$\begin{aligned}
\mathrm{Sq}(r_1, r_2, \ldots, r_n, 1).\tau(c) &= \mathrm{Sq}(r_1, r_2, \ldots, r_n, 1).\tau(\mathrm{Sq}(s_1, s_2, \ldots, s_n, 1)) \\
&= \mathrm{Sq}(r_1, r_2, \ldots, r_n, 1).\tau(\mathrm{Sq}(s_1, s_2, \ldots, s_n, 0).\mathrm{Sq}(0, \ldots, 0, 1)) \\
&= \mathrm{Sq}(r_1, r_2, \ldots, r_n, 1).\tau(\mathrm{Sq}(0, \ldots, 0, 1)).\tau(\mathrm{Sq}(s_1, s_2, \ldots, s_n, 0)) \\
&= \mathrm{Sq}(r_1, r_2, \ldots, r_n, 1).\mathrm{Sq}(0, \ldots, 0, 1).\tau(\mathrm{Sq}(s_1, s_2, \ldots, s_n, 0)) \\
&= 0
\end{aligned}$$

and so c is in $\mathcal{R}_H(C)$.

Now let c be a Milnor basis element in $\mathcal{R}_H(C)$ of the form

$$\mathrm{Sq}(s_1, s_2, \ldots, s_n, s_{n+1}).$$

Then

$$\mathrm{Sq}(r_1, r_2, \ldots, r_n, 1).\tau(c) = \mathrm{Sq}(r_1, r_2, \ldots, r_n, 1).\tau(\mathrm{Sq}(s_1, s_2, \ldots, s_n, s_{n+1})) = 0$$

for any Milnor basis element $\mathrm{Sq}(r_1, r_2, \ldots, r_n, 1)$. Here s_{n+1} is either 1 or 0. However, s_{n+1} again cannot be zero. If so, the product

$$\mathrm{Sq}(0, \ldots, 0, 1).\tau(\mathrm{Sq}(s_1, s_2, \ldots, s_n, 0))$$

would be zero but then

$$\tau(\mathrm{Sq}(0, \ldots, 0, 1).\tau(\mathrm{Sq}(s_1, s_2, \ldots, s_n, 0)))$$

and

$$\begin{aligned}\tau(\mathrm{Sq}(0, \ldots, 0, 1).\tau(\mathrm{Sq}(s_1, s_2, \ldots, s_n, 0))) &= \mathrm{Sq}(s_1, s_2, \ldots, s_n, 0).\tau(\mathrm{Sq}(0, \ldots, 0, 1)) \\ &= \mathrm{Sq}(s_1, s_2, \ldots, s_n, 0).\mathrm{Sq}(0, \ldots, 0, 1) \\ &= \mathrm{Sq}(s_1, s_2, \ldots, s_n, 1)\end{aligned}$$

would be zero, which is impossible. Therefore $s_{n+1} = 1$ and this shows that c is in C.

The equality $C = \mathcal{R}_H(C)$ leads to $C = \mathcal{L}_H(C)$ and so C is a Hermitian self-dual code in $A(n)$. □

In [2], it has been shown that Euclidean self-dual codes exist for all even lengths over $A(n)$ for all n. By the existence of self-dual codes over $A(n)$ of length 1, the existence can be generalized to all lengths over $A(n)$.

Corollary 3.8 *There exist Euclidean and Hermitian self-dual codes of all lengths over $A(n)$ for all n.*

Proof The result follows from the fact that $C \times D$ is a self-dual code of length $m + k$ whenever C and D are self-dual codes of length m and k, respectively. □

Now we have a Euclidean self-dual code $C = A(n)[\mathrm{Sq}(0, \cdots, 0, 1)]$ in $A(n)$ so that $A(n)$ is not semiprime since every ideal I in a semiprime ring is idempotent, $I^2 = I$. Moreover, the (mod 2) Steenrod algebra $\mathcal{A}$ is a prime ring [4]. Let $a_1, a_2, \cdots, a_t$ be the Milnor basis of $A(n)$ with $a_1 = \mathrm{Sq}(0)$ and $a_t = \mathrm{Sq}(2^{n+1}-1, 2^n-1, ..., 1)$. Note that $A(n)$ is a local ring [2] with a unique maximal ideal $A(n)[a_2, a_3, \cdots, a_t]$.

Corollary 3.9 *The sub-Hopf algebra $A(n)$ of the Steenrod algebra $\mathcal{A}$ is not prime for all $n \geq 1$.*

Proof A ring R is prime iff the right annihilator of every nonzero right ideal of R is zero. Since a submodule $C = A(n)[\mathrm{Sq}(0, \cdots, 0, 1)]$ has a nonzero right annihilator $\mathcal{R}(C) = \mathcal{L}(C)$, $A(n)$ is not a prime ring. □

Corollary 3.10 *The sub-Hopf algebra $A(n)$ of the Steenrod algebra $\mathcal{A}$ is not simple for all $n \geq 1$.*

Proof Primality of a left Artinian ring is equivalent to being simple. □

Acknowledgements

We would like to thank Professor ST Dougherty for his comments and valuable advice and our anonymous referees for their contributions to our manuscript.

References

[1] Dougherty ST, Leroy A. Self-dual codes over non-commutative Frobenius rings. Appl Algebr Eng Comm 2016; 27: 185-203.

[2] Dougherty ST, Vergili T. Codes and the Steenrod algebra. Journal of Algebra, Combinatorics, Discrete Structures and Applications 2017; 4: 141-154.

[3] Gallant AM. Excess and conjugation in the Steenrod algebra. P Am Math Soc 1979; 76: 161-166.

[4] Kashkarev I. The primality of the Steenrod algebra. Commun Algebra 2009; 37: 1182-1185.

[5] Margolis HR. Spectra and the Steenrod algebra. North-Holland Mathematical Library. Amsterdam, Netherlands: Elsevier, 1983.

[6] Milnor J. The Steenrod algebra and its dual. Ann Math 1958; 67: 150-171.

[7] Steenrod NE, Epstein DBA. Cohomology operations, Annals of Mathematics Studies. Princeton, NJ, USA: Princeton University Press, 1962.

[8] Wood JA. Duality for modules over finite rings and applications to coding theory. Am J Math 1999; 121: 555-575.

[9] Wood JA. Anti-isomorphism, character modules and self-dual codes over non-commutative rings. International Journal of Information and Coding Theory 2010; 1: 429-444.

[10] Wood RMW. A note on basis and relations in the Steenrod algebra. B Lond Math Soc 1995; 27: 380-386.