AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **54** (2012), Pages 115–126

On θ-cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$

Taher Abualrub

Department of Mathematics & Statistics
American University of Sharjah
Sharjah
United Arab Emirates
abualrub@aus.edu

Nuh Aydin

Department of Mathematics
Kenyon College
Gambier, Ohio
U.S.A.
aydinn@kenyon.edu

Padmapani Seneviratne

Department of Mathematics & Statistics
American University of Sharjah
Sharjah
United Arab Emirates
pseneviratne@aus.edu

Abstract

In this paper we study θ-cyclic codes over the ring $R = \mathbb{F}_2 + v\mathbb{F}_2 = \{0, 1, v, v+1\}$ where $v^2 = v$. This is the only ring of order four that is not a field and has a non-trivial ring automorphism. We describe generator polynomials of θ-cyclic codes defined over this ring. We also describe the generator polynomials of the duals of free θ-cyclic codes with respect to Euclidean and Hermitian inner products. Finally, we give examples of optimal self-dual codes with respect to the Euclidean and Hermitian inner products.

1 Introduction

Linear and cyclic codes have been studied for the last sixty years. Different methods and different approaches have been applied to produce certain types of codes with good parameters and properties. Recently, Boucher et al. in [5], and Abualrub et al. in [1] studied an interesting class of linear codes. In [5], Geiselmann and Ulmer introduced the class of θ-cyclic (skew cyclic) codes that generalizes the concept of cyclic codes and uses a non-commutative polynomial ring, called a skew polynomial ring, to construct these types of codes. Abualrub et al., in [1], generalized the concept of skew cyclic codes to skew quasi-cyclic codes. In both cases a number of new codes over GF(4) with better parameters than the previously best known codes were produced. A further generalization was given in [4] where constacyclic codes over Galois rings are studied.

After GF(4) it would be natural to consider θ-cyclic codes over the ring $\mathbb{Z}_4$. However, θ-cyclic codes depend on a ring automorphism and $\mathbb{Z}_4$ has only the trivial automorphism. There are two other commutative rings of order four: $R = \mathbb{F}_2 + v\mathbb{F}_2 = \{0, 1, v, v+1\}$ where $v^2 = v$, and $S = \mathbb{F}_2 + u\mathbb{F}_2 = \{0, 1, u, u+1\}$ where $u^2 = 0$, as in [8]. Like $\mathbb{Z}_4$, the ring S only has the identity automorphism. So, over the rings S and $\mathbb{Z}_4$, there do not exist any θ-cyclic codes that are different from the ordinary cyclic codes.

The ring R, on the other hand, has a non-trivial ring automorphism. If we let $\theta(0) = 0,\ \theta(1) = 1,\ \theta(v) = v+1,\ \theta(v+1) = v$, then θ is a ring automorphism that is different from the identity. Therefore, it would be interesting to consider θ-cyclic codes over R. It is worth mentioning that the ring $R = \mathbb{F}_2 + v\mathbb{F}_2 = \{0, 1, v, v+1\}$ is isomorphic to the ring $\mathbb{F}_2 \times \mathbb{F}_2$ via $0 \to (0,0), 1 \to (1,1), v \to (1,0), v+1 \to (0,1)$, i.e. $a + bv \to (a+b, a)$.

The rest of the paper is organized as follows. Section 2 gives a brief description of the skew polynomial ring $R[x;\theta]$ and the definition of θ-cyclic codes. We show that $R_n = R[x;\theta]/\left(x^n - 1\right)$ can be considered as a left $R[x;\theta]$-module and hence θ-cyclic codes are left submodules of R_n. In Section 3, we describe generators of these codes. In Section 4, we define Euclidean and Hermitian dual codes and find the generator polynomials for the dual code of a free θ-cyclic code. We give tables of optimal self-dual codes in Section 5.

2 The Skew Polynomial Ring $R[x;\theta]$

In this section we construct the non-commutative ring $R[x;\theta]$. The structure of this non commutative ring depends on the elements of the commutative ring $R = \mathbb{F}_2 + v\mathbb{F}_2 = \{0, 1, v, v+1\}$, where $v^2 = v$ and the automorphism θ on R, defined by $\theta(0) = 0,\ \theta(1) = 1,\ \theta(v) = v+1,\ \theta(v+1) = v$. Note that $\theta^2(a) = \theta(\theta(a)) = a$ for all $a \in R$. This implies that θ is a ring automorphism of order 2.

Definition 1 *Define the skew polynomial ring $R[x;\theta]$ as the set of polynomials over*

R where the addition is the usual polynomial addition and the multiplication, which we denote by $*$, is defined by the basic rule

$$(ax^i) * (bx^j) = a\theta^i(b)x^{i+j}$$

and the distributive and the associative laws.

Note that this multiplication is not commutative. For example, $x * vx = \theta(v)x^2 = (v+1)x^2$, and $vx * x = v\theta(1)x^2 = vx^2$. Therefore, when an ideal of $R[x;\theta]$ is considered, one should specify whether it is a right ideal or a left ideal. In the rest of the article, when we talk about ideals of $R[x;\theta]$ we always mean left ideals and we use the notation $(p(x))$ to denote the (left) ideal generated by $p(x)$.

Definition 2 *Consider the ring $R = \mathbb{F}_2 + v\mathbb{F}_2 = \{0, 1, v, v+1\}$ where $v^2 = v$ and the automorphism θ defined as above. A subset C of R^n is called a θ-cyclic code of length n if*

1. *C is an R-submodule of R^n and*
2. *if*
$$c = (c_0, c_1, \ldots, c_{n-1}) \in C$$
then
$$T_\theta(c) = (\theta(c_{n-1}), \theta(c_0), \ldots, \theta(c_{n-2})) \in C.$$

Let $R_n = R[x;\theta]/(x^n - 1)$ denote the quotient ring of $R[x;\theta]$ by the (left) ideal $(x^n - 1)$, and let $f(x) \in R_n$ and $r(x) \in R[x;\theta]$. Define multiplication from left as:

$$r(x) * (f(x) + (x^n - 1)) = r(x) * f(x) + (x^n - 1) \text{ for any } r(x) \in R[x;\theta]. \quad (1)$$

This is a well-defined multiplication of the elements of R_n by the elements of $R[x;\theta]$. With this definition we have the following theorem

Theorem 1 *R_n is a left $R[x;\theta]$-module where multiplication is defined as in Equation 1.*

Proof. The proof is similar to the proof of Theorem 9 in [9]. ∎

Under this representation of R_n, we can identify each element $(c_0, c_1, \ldots, c_{n-1})$ in R^n, by the polynomial

$$f(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1} \text{ in } R_n.$$

This relationship between R_n and R^n will give us the following theorem.

Theorem 2 *A code C in R_n is a θ-cyclic code if and only if C is a left $R[x;\theta]$-submodule of the left $R[x;\theta]$-module R_n.*

Proof. See Theorem 10 in [9]. ∎

Lemma 1 *If n is even, and $(x^n - 1) = g(x) * h(x)$ in $R[x;\theta]$, then $(x^n - 1) = g(x) * h(x) = h(x) * g(x)$.*

Proof. See Lemma 8 in [6]. ∎

3 Generators for θ-Cyclic Codes

Theorem 3 *Let C be a θ-cyclic code in $R_n = R[x;\theta]/(x^n - 1)$, $C \neq \{0\}$. Let $f(x)$ be a polynomial of minimal degree in C (among non-zero polynomials) and suppose $f(x)$ is monic. Then $C = (f(x)) = \{r(x)f(x) | r(x) \in R_n\}$, where $f(x)$ is a right divisor of $x^n - 1$. Moreover, C is a free code of dimension $k = n - \deg(f(x))$ with a basis $\{f(x), x * f(x), x^2 * f(x), \ldots, x^{k-1} * f(x)\}$.*

Proof. Let $c(x) \in C$. Then by the left division algorithm, there exist polynomials $q(x)$ and $r(x)$ such that $c(x) = q(x) * f(x) + r(x)$, where $r(x) = 0$ or $\deg(r(x)) < \deg(f(x))$. Since C is linear, $r(x) = c(x) - q(x) * f(x) \in C$. Since $f(x)$ is of minimal degree, we have $r(x) = 0$, so $c(x) = q(x) * f(x)$ and $C = (f(x))$.

Next we show that $f(x)$ is a right divisor of $x^n - 1$. By the left division algorithm, $x^n - 1 = q_2(x) * f(x) + r_2(x)$, where $r_2(x) = 0$ or $\deg r_2(x) < \deg f(x)$. Reducing the last equation $\mod x^n - 1$, we get $r_2(x) = -q_2(x) * f(x) \in C$. By the minimality of degree of $f(x)$ we have $r_2(x) = 0$, i.e., $f(x)$ is a right divisor of $x^n - 1$.

The work above shows that the set $B = \{f(x), x * f(x), x^2 * f(x), \ldots, x^{k-1} * f(x)\}$ is a spanning set for C. It is easy to show that B is also linearly independent, hence a basis for C. ∎

Lemma 2 *Let $f(x)$ be a non-monic polynomial in C of minimal degree then $f(x) = vf_1(x)$ or $f(x) = (v+1)f_1(x)$, where $f_1(x)$ is a binary polynomial.*

Proof. Since $f(x)$ is not monic in R_n, the leading coefficient of $f(x)$ is either v or $v + 1$. First assume $f(x) = vx^t + a_{t-1}x^{t-1} + \ldots + a_1x + a_0$. Then $(v+1)f(x) = (v+1)a_{t-1}x^{t-1} + (v+1)a_{t-2}x^{t-2} + \ldots + (v+1)a_1 + (v+1)a_0$, since $(v+1)v = 0$. But minimality of $f(x)$ implies that $(v+1)f(x) = 0$. Hence $f(x) = vf_1(x)$ for some binary polynomial $f_1(x)$. If the leading coefficient of $f(x)$ is $v + 1$ then a similar argument shows that $f(x) = (v+1)f_1(x)$, where $f_1(x)$ is a binary polynomial of degree t. ∎

Left and right division algorithms in a polynomial ring are not applicable unless the divisor polynomial is monic or its leading coefficient is a unit. Because of the structure of the ring R we have the following lemma that gives us a little more freedom in division if the leading coefficient is not a unit.

Lemma 3 *Let $f(x)$ and $g(x)$ be two non-zero, non-monic polynomials in $R[x;\theta]$ with $\deg f(x) \geq \deg g(x)$. Then there are polynomials $q(x)$ and $r(x)$ such that*

$$f(x) = q(x) * g(x) + r(x),$$

where $r(x) = 0$, or $\deg r(x) < \deg g(x)$ or $r(x)$ is a monic polynomial of degree at most the degree of $f(x)$.

Proof. Let $f(x)$ and $g(x)$ be two non-monic polynomials of degrees s and t respectively, with $s \geq t$. We may assume, without loss of generality, that

$$g(x) = vx^t + b_{t-1}x^{t-1} + \ldots b_1 x + b_0.$$

If the leading coefficient of $g(x)$ is $(v+1)$, a similar argument works. Note the following important equation:

$$x^i * v = \begin{cases} vx^i & \text{if } i \text{ is even,} \\ (v+1)\, x^i & \text{if } i \text{ is odd.} \end{cases} \tag{2}$$

We proceed by induction on the $\deg f(x) = s$. Suppose

$$f(x) = a_s x^s + a_{s-1}x^{s-1} + \ldots + a_1 x + a_0.$$

If $s = 0$, then $t = 0$ and $f(x) = a_0$ where $a_0 = v$ or $(v+1)$, and $g(x) = v$. It is clear that there is a constant r such that $a_0 = v + r$, satisfying the required conditions.

Suppose the theorem is true for all polynomials of degree less than s. Consider the polynomial:

$$l(x) = f(x) - x^{s-t} * g(x).$$

From Equation 2 it is clear that $x^{s-t} * vx^t = vx^s$ or $(v+1)\, x^s$. This implies that $l(x)$ is either a polynomial of degree less than degree $f(x)$ or is a monic polynomial of degree s.

If $l(x)$ is a monic polynomial of degree s, then

$$f(x) = x^{s-t} * g(x) + l(x).$$

In this case the proof is complete by taking $q(x) = x^{s-t}$ and $r(x) = l(x)$.

If $\deg l(x) < \deg f(x)$, then by the inductive hypothesis we have

$$l(x) = f(x) - x^{s-t} * g(x) = m(x) * g(x) + r(x),$$

for some polynomials $m(x), r(x)$ where $r(x) = 0$, or $\deg r(x) < \deg g(x)$ or $r(x)$ is a monic polynomial of degree equal to at most the degree of $l(x)$. Arranging the above equation and taking $q(x) = (x^{s-t} + m(x))$, we get:

$$f(x) = q(x) * g(x) + r(x).$$

■

We now consider the case where the θ-cyclic code does not contain any monic polynomials.

Lemma 4 *Let C be a θ-cyclic code in $R_n = R[x;\theta]/(x^n-1)$. Suppose that a polynomial of minimal degree in C is not monic, say $f(x) = vf_1(x)$ is a polynomial of minimal degree in C. Moreover, suppose C contains no monic polynomials. Then $C = (vf_1(x))$ where $f_1(x)$ is a monic binary polynomial of lowest degree with $f_1(x) | (x^n-1)$.*

Proof. Suppose C has no monic polynomials and let $f(x) = vf_1(x)$ be a polynomial of least degree in C. Let $c(x) \in C$; then by Lemma 2, there are polynomials $q(x)$, and $r(x)$ such that

$$c(x) = q(x) * f(x) + r(x),$$

where $r(x) = 0$, or $\deg r(x) < \deg f(x)$ or $r(x)$ is a monic polynomial of degree equal to at most the degree of $c(x)$. Since C has no monic polynomials and $f(x)$ is a polynomial of minimal degree in C, $r(x) = 0$. Hence $C = (f(x))$. Since $\mathbb{F}_2$ is a subring of R, factorization of binary polynomials is still valid in the skew polynomial ring $R[x;\theta]$. Hence using the division algorithm we get two unique binary polynomials $Q(x)$ and $R(x)$ such that

$$x^n - 1 = Q(x) * f_1(x) + R(x),$$

where $R(x)$ is a binary polynomial with $R(x) = 0$ or $\deg R(x) < \deg f_1(x) = \deg f(x)$. Write $Q(x) = Q_1(x) + Q_2(x)$ where $Q_1(x)$ consists of all terms with odd powers and $Q_2(x)$ consists of all terms with even powers. Hence

$$\begin{aligned}
x^n - 1 &= (Q_1(x) + Q_2(x)) * f_1(x) + R(x), \\
x^n - 1 &= Q_1(x) * f_1(x) + Q_2(x) * f_1(x) + R(x), \\
v * (x^n - 1) &= v * (Q_1(x) * f_1(x)) + v * (Q_2(x) * f_1(x)) + v * R(x) \\
&= Q_1(x) * (v+1) f_1(x) + (Q_2(x) * vf_1(x)) + v * R(x) \\
&= (Q_1(x) * vf_1(x)) + (Q_2(x) * vf_1(x)) + Q_1(x) * f_1(x) + v * R(x).
\end{aligned}$$

Since $\deg R(x) < \deg f_1(x)$, $Q_1(x) * f_1(x) + v * R(x)$ is a monic polynomial in C, a contradiction. Thus $Q_1(x) * f_1(x) + v * R(x) = 0$. Since $Q_1(x) * f_1(x)$ and $R(x)$ are binary polynomials, $R(x) = 0$ and $f_1(x) | (x^n - 1)$. ∎

Theorem 4 *Let C be a θ-cyclic code in $R_n = R[x;\theta]/(x^n-1)$ that contains some monic polynomials. Suppose that no polynomial $f(x)$ of minimal degree in C is monic. Then $C = (f(x), g(x))$ where $g(x)$ is a polynomial of least degree among monic polynomials in C.*

Proof. Suppose that a polynomial $f(x)$ of minimal degree in C is not monic. Let $g(x)$ be a monic polynomial in C of minimal degree and let $c(x) \in C$. Then by the left division algorithm there are polynomials $q_1(x)$ and $r_1(x)$ such that

$$c(x) = q_1(x) * g(x) + r_1(x) \quad \text{where } r_1(x) = 0 \text{ or } \deg(r_1(x)) < \deg(g(x)).$$

Since $g(x)$ and $c(x)$ are in C and since C is θ-cyclic, we have $r_1(x) \in C$. Since $\deg r_1(x) < \deg g(x)$, either $r_1(x)$ is a non-monic polynomial or $r_1(x) = 0$. If $r_1(x) = 0$ then $c(x) \in (g(x)) \subseteq (f(x), g(x))$. If $r_1(x) \neq 0$, then by Lemma 3 we can find polynomials $q_2(x)$, and $r_2(x)$ such that

$$r_1(x) = q_2(x) * f(x) + r_2(x),$$

where $r_2(x) = 0$, or $\deg(r_2(x)) < \deg(f(x))$, or $r_2(x)$ is a monic polynomial of degree less than or equal to $\deg r_1(x) < \deg g(x)$. Since $f(x)$ is a non-monic polynomial of minimal degree in C and $g(x)$ is a monic polynomial of minimal degree in C, we must have $r_2(x) = 0$. Therefore, we have:

$$\begin{aligned} c(x) &= q_1(x) * g(x) + r_1(x) \\ &= q_1(x) * g(x) + q_2(x) * f(x). \end{aligned}$$

Thus we have $C = (f(x), g(x))$ where $g(x)$ is a monic polynomial of minimal degree in C. ∎

We summarize the results in this section as follows.

Corollary 5 *Let C be a θ-cyclic code in R_n. Then*

1. *If a polynomial $g(x)$ of least degree in C is monic then $C = (g(x))$, where $g(x)$ is a (skew) right divisor of $x^n - 1$.*
2. *If C contains some monic polynomials but no polynomial $f(x)$ of least degree in C is monic then $C = (f(x), g(x))$ where $g(x)$ is a monic polynomial of least degree in C, and $f(x) = vf_1(x)$ or $f(x) = (v + 1)f_1(x)$ for some binary polynomial $f_1(x)$.*
3. *If C does not contain any monic polynomials, then $C = (f(x))$ where $f(x) = vf_1(x)$ or $f(x) = (v + 1)f_1(x)$ and $f_1(x)$ is a binary polynomial that divides $x^n - 1$.*

4 Duals of θ-Cyclic Codes over R

In this section we focus on dual codes over the ring R. First we consider Euclidean and Hermitian inner products and show that if C is a θ-cyclic code over the ring R, then the Euclidean and Hermitian dual codes $C^\perp$ and C^* are also θ-cyclic codes over R. Furthermore, we give the generator polynomials for the dual codes in this section.

Definition 3 *Let $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ be two elements of R^n. The Euclidean inner product in R^n is defined as*

$$\langle x, y \rangle = x_1y_1 + x_2y_2 + \cdots + x_ny_n,$$

and the Hermitian inner product as

$$[x, y] = x_1\theta(y_1) + x_2\theta(y_2) + \cdots + x_n\theta(y_n).$$

Definition 4 *The dual code $C^{\perp}$ with respect to the Euclidean inner product of C is defined as*

$$C^{\perp} = \{x \in R^n \mid \langle x, c\rangle = 0 \ \text{ for all } c \in C\}$$

and the dual code C^* with respect to the Hermitian inner product of C is defined as

$$C^* = \{x \in R^n \mid [x, c] = 0 \ \text{ for all } c \in C\}.$$

C is called Euclidean self dual if $C = C^{\perp}$ and is called Hermitian self dual if $C = C^*$.

Lemma 5 *Let C be a θ-cyclic code of even length n over R. Then $C^{\perp}$ and C^* are also θ-cyclic codes.*

Proof. The proof is based on the fact that if $\langle u, v\rangle = 0$, and $[u, v] = 0$, then $\langle T_\theta(u), T_\theta(v)\rangle = 0$ and $[T_\theta(u), T_\theta(v)] = 0$. This can be verified easily.

Let C be a θ-cyclic code of even length n over R with a generating set (not necessarily a basis) $\{v_1, T_\theta(v_1), \ldots, T_\theta^{n-1}(v_1), v_2, T_\theta(v_2), \ldots\}$ and let $u \in C^{\perp}$ and $w \in C^*$. Then $\langle u, T_\theta^j(v_i)\rangle = 0$ and $[w, T_\theta^j(v_i)] = 0$ for all i, j. It follows that $\langle T_\theta(u), T_\theta^{j+1}(v_i)\rangle = 0$ and $[T_\theta(w), T_\theta^{j+1}(v_i)] = 0$ for all i, j. Since $T_\theta^n(z) = z$, for any $z \in R^n$, where n is even, the result follows. ∎

Theorem 6 *Let $C = (g(x))$ be a θ-cyclic code of even length n and dimension k, where $x^n - 1 = g(x) * h(x)$, and*

$$\begin{aligned} h(x) &= 1 + h_1 x + \ldots + x^k \ \text{ and} \\ g(x) &= 1 + g_1 x + \ldots x^{n-k}. \end{aligned}$$

Let

$$\overline{h(x)} = 1 + \theta(h_{k-1})x + \theta^2(h_{k-2})x^2 + \cdots + \theta^{k-1}(h_1)x^{k-1} + x^k.$$

Then $\overline{h(x)}$ is a right divisor of $x^n - 1$.

Proof. We will give a constructive proof that gives the polynomial $\overline{g(x)}$ such that $x^n - 1 = \overline{h(x)} * \overline{g(x)}$. First note that since n is even, $(x^n - 1) = g(x) * h(x) = h(x) * g(x)$.

If k is odd, let

$$\begin{aligned} \overline{g(x)} = 1 &+ g_{n-k-1}x + \theta\left(g_{n-k-2}\right)x^2 + g_{n-k-3}x^3 + \theta\left(g_{n-k-4}\right)x^4 + \\ &\cdots + g_2 x^{n-k-2} + \theta\left(g_1\right)x^{n-k-1} + x^{n-k}, \end{aligned}$$

and note that

$$\overline{h(x)} = 1 + \theta(k_{k-1})x + h_{k-2}x^2 + \theta(h_{k-3})x^3 + \cdots + \theta(h_2)x^{k-2} + h_1 x^{k-1} + x^k.$$

We claim that $x^n - 1 = \overline{g(x)} * \overline{h(x)}$. If k is even, let

$$\begin{aligned} \overline{g(x)} = 1 &+ \theta\left(g_{n-k-1}\right)x + g_{n-k-2}x^2 + \theta\left(g_{n-k-3}\right)x^3 + g_{n-k-4}x^4 + \ldots \\ &+ \theta\left(g_2\right)x^{n-k-2} + g_1 x^{n-k-1} + x^{n-k}, \end{aligned}$$

and note that

$$\overline{h(x)} = 1 + \theta(k_{k-1})x + h_{k-2}x^2 + \theta(h_{k-3})x^3 + \cdots + h_2x^{k-2} + \theta(h_1)x^{k-1} + x^k.$$

Again we claim that $x^n - 1 = \overline{g(x)} * \overline{h(x)}$. The proof when k is even is similar to the proof when k is odd and in fact the proof depends on comparing the coefficients in $\overline{g(x)} * \overline{h(x)}$ with the coefficients in $x^n - 1 = h(x) * g(x)$. So we will give the proof when k is odd.

Case 1: Suppose i is even and less than k. The coefficient of x^i in $\overline{g(x)} * \overline{h(x)}$ is equal to

$$h_{k-i} + g_{n-k-1}h_{k-i+1} + \theta\left(g_{n-k-2}\right)h_{k-i+2} + g_{n-k-3}h_{k-i+3} + \theta\left(g_{n-k-4}\right)h_{k-i+4} + \cdots + g_{n-k-i+1}h_{k-1} + \theta\left(g_{n-k-i}\right).$$

The coefficient of x^{n-i} in $h(x) * g(x)$ is

$$h_{k-i} + g_{n-k-1}h_{k-i+1} + \theta\left(g_{n-k-2}\right)h_{k-i+2} + g_{n-k-3}h_{k-i+3} + \theta\left(g_{n-k-4}\right)h_{k-i+4} + \cdots + g_{n-k-i+1}h_{k-1} + \theta\left(g_{n-k-i}\right) = 0.$$

Therefore, the coefficient of x^i in $\overline{g(x)} * \overline{h(x)}$ is zero.

Case 2: Suppose i is odd and less than k. The coefficient of x^i in $\overline{g(x)} * \overline{h(x)}$ is equal to

$$\theta\left(h_{k-i}\right) + g_{n-k-1}\theta\left(h_{k-i+1}\right) + \theta\left(g_{n-k-2}\right)\theta\left(h_{k-i+2}\right) + g_{n-k-3}\theta\left(h_{k-i+3}\right) + \theta\left(g_{n-k-4}\right)\theta\left(h_{k-i+4}\right) + \cdots + \theta\left(g_{n-k-i+1}\right)\theta\left(h_{k-1}\right) + g_{n-k-i}. \quad (3)$$

The coefficient of x^{n-i} in $h(x) * g(x)$ is

$$\begin{aligned} & h_{k-i} + h_{k-i+1}\theta\left(g_{n-k-1}\right) + h_{k-i+2}g_{n-k-2} + h_{k-i+3}\theta\left(g_{n-k-3}\right) + \\ & h_{k-i+4}g_{n-k-4} + \cdots + h_{k-1}g_{n-k-i+1} + \theta\left(g_{n-k-i}\right) \quad (4) \\ = \; & 0. \end{aligned}$$

Since θ is an automorphism of order 2, apply θ to (4) to get

$$\theta\left(h_{k-i}\right) + g_{n-k-1}\theta\left(h_{k-i+1}\right) + \theta\left(g_{n-k-2}\right)\theta\left(h_{k-i+2}\right) + g_{n-k-3}\theta\left(h_{k-i+3}\right) + \theta\left(g_{n-k-4}\right)\theta\left(h_{k-i+4}\right) + \ldots + \theta\left(g_{n-k-i+1}\right)\theta\left(h_{k-1}\right) + g_{n-k-i} = 0. \quad (5)$$

Therefore, the coefficient of x^i in $\overline{g(x)} * \overline{h(x)}$ is zero.

Case 3: If i (even or odd) is larger than or equal to k and less than n, then comparing coefficients as in the above cases we see that the coefficient of x^i is always 0. Therefore $x^n - 1 = \overline{g(x)} * \overline{h(x)}$. ∎

Corollary 7 *Let $C = (g(x))$ be a θ-cyclic code of even length n and dimension k, $x^n - 1 = h(x) * g(x)$, and*

$$\begin{aligned} h(x) &= 1 + h_1x + \ldots + x^k \text{ and} \\ g(x) &= 1 + g_1x + \ldots x^{n-k}. \end{aligned}$$

Then the Euclidean dual of C is $C^{\perp} = \left(\overline{h(x)}\right)$, where

$$\overline{h(x)} = 1 + \theta(h_{k-1})x + \theta^2(h_{k-2})x^2 + \cdots + \theta^{k-1}(h_1)x^{k-1} + x^k.$$

Moreover, C has a parity check matrix given by

$$\begin{pmatrix} h_k & \theta(h_{k-1}) & \dots & \theta^k(h_0) & 0 & \dots & 0 \\ 0 & \theta(h_k) & \dots & \dots & \theta^{k+1}(h_0) & \dots & 0 \\ \vdots & \ddots & \ddots & & & \ddots & \vdots \\ 0 & \dots & 0 & \theta^{n-k-1}(h_k) & \theta^{n-k}(h_{k-1}) & \dots & \theta^{n-1}(h_0) \end{pmatrix}.$$

Proof. The proof follows from Theorem 6 ∎

Lemma 6 *Let C be a θ-cyclic code of length n over R with a monic generator $g(x)$ that divides $x^n - 1$, and let $g(x) * h(x) = x^n - 1$, where $h(x) = h_0 + h_1 x + \cdots + h_k x^k$. Then a generator polynomial of C^* is $h^*(x) = \theta(h_k) + \theta^2(h_{k-1})x + \cdots + \theta^{k+1}(h_0)x^k$.*

Proof. The proof is similar to the proof of Theorem 6 ∎

The above discussion about the dual of θ-cyclic codes will yield the following corollary.

Corollary 8 *Let $C = (g(x))$ be a θ-cyclic code of even length n and dimension k. Then*

1. *C is Euclidean self dual if and only if $g(x) = \overline{h(x)}$.*
2. *C is Hermitian self dual if and only if $g(x) = h^*(x)$*

where the notation is as in Theorem 6 and Lemma 6.

5 Examples of Optimal Self-Dual Codes

Self-dual codes and optimal self-dual codes are intensively studied topics in coding theory. In this section we give examples of optimal (in the sense of having largest possible minimum distance among all self-dual codes of given type) θ-cyclic codes that are Euclidean self dual, Euclidean Type IV self dual, or Hermitian Type IV self-dual. They are given in the three tables below. A self-dual code is Type IV if all the Hamming weights are even. We only consider Hamming weights in this paper. Two other weights considered for codes over R are the Lee weight and the Bachoc weight. It is known that the minimum Lee weight of a code over R is the same as its minimum Hamming weight [2]. It is also known that a Euclidean self-dual code of length n over R exists if and only if n is even [8]. Moreover, there are tables of optimal Hermitian self-dual, and Hermitian Type IV self-dual codes of lengths up to 32 in [2]. The minimum distances of optimal Euclidean self-dual codes can be determined from existing tables of binary self-dual codes (e.g. [7]). All of these examples are obtained by a computer search using the computer algebra system Magma [3].

Table 1: Optimal θ-Cyclic codes that are Euclidean Self-Dual

n	d	Generator polynomial
4	2	x^2+1
6	2	x^3+1
8	4	$x^4+(v+1)x^3+x^2+vx+1$
10	2	x^5+1
12	4	$x^6+(v+1)x^5+x^4+x^3+x^2+v*x+1$
14	4	$x^7+x^6+x^5+x^4+x+1$
16	4	$x^8+(v+1)x^5+x^4+vx^3+1$
18	4	$x^9+x^7+vx^6+(v+1)x^5+(v+1)x^4+vx^3+x^2+1$
20	4	$x^{10}+(v+1)x^7+x^6+x^5+x^4+vx^3+1$
22	6	$x^{11}+x^{10}+vx^9+vx^8+vx^7+(v+1)x^6+(v+1)x^5$ $+vx^4+vx^3+vx^2+x+1$
24	8	$x^{12}+x^{11}+vx^{10}+x^9+(v+1)x^7+vx^5+x^3$ $+(v+1)x^2+x+1$

Table 2: Optimal θ-Cyclic codes that are Euclidean Type IV Self-Dual

n	d	Generator polynomial
4	2	x^2+1
6	2	x^3+1
10	2	x^5+1
14	4	$x^7+x^6+x^5+x^4+x+1$

Table 3: Optimal θ-Cyclic codes that are Hermitian Type IV Self-Dual

n	d	Generator polynomial
4	2	x^2+1
6	2	x^3+1
14	4	$x^7+x^6+x^5+x^4+x+1$
16	4	$x^8+x^7+vx^6+x^5+x^3+vx^2+x+1$
18	6	$x^9+x^7+(v+1)x^6+(v+1)x^5+vx^4+vx^3+x^2+1$
22	6	$x^{11}+(v+1)x^{10}+x^7+vx^6+(v+1)x^5+x^4+vx+1$
26	6	$x^{13}+x^{11}+vx^{10}+(v+1)x^9+vx^8+vx^7+(v+1)x^6$ $+(v+1)x^5+vx^4+(v+1)x^3+x^2+1$

Acknowledgments

The authors would like to thank the anonymous referees for their careful reading of the paper and the insightful comments and suggestions.

References

[1] T. Abualrub, A. Ghrayeb, N. Aydin and I. Siap, On the Construction of Skew Quasi-Cyclic Codes, *IEEE Trans. Inform. Theory* 56 no. 2 (2010), 2081–2090.

[2] K. Betsumiya and M. Harada, Optimal Self-Dual Codes over $F_2 \times F_2$ with respect to Hamming Weight, *IEEE Trans. Inform. Theory* 50 No. 2 (2004), 356–358.

[3] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system, I. The user language, *J. Symbolic Comput.* 24 (1997), 235–265.

[4] D. Boucher, P. Solé and F. Ulmer, Skew Constacyclic Codes over Galois Rings, *Advances of Mathematics of Communications* 2 no. 3 (2008), 273–292.

[5] D. Boucher, W. Geiselmann and F. Ulmer, Skew-Cyclic Codes, *Applicable Algebra in Engineering, Communication and Computing* 18, Issue 4 (2007), 379–389.

[6] D. Boucher and F. Ulmer, Coding with skew polynomial rings, *J. Symbolic Computation* 44, Issue 12 (2009), 1644–1656.

[7] J. H. Conway and N. J. A. Sloane, A New Upper Bound on the Minimal Distance of Self-Dual Codes, *IEEE Trans. Inform. Theory* 36 no. 6 (1990), 1319–1333.

[8] S. T. Dougherty, P. Gaborit, M. Harada, A. Munemasa and P. Solé, Type IV Self-Dual Codes Over Rings, *IEEE Trans. Inform. Theory* 45 no. 7 (1999), 2345–2360.

[9] I. Siap, T. Abualrub, N. Aydin and P. Seneviratne, Skew Cyclic Codes of Arbitrary Length, *Int. J. Information and Coding Theory* 2 no. 1 (2011), 10–20.

(Received 4 July 2011; revised 14 June 2012)