Self-dual skew codes and factorization of skew polynomials

Delphine Boucher

IRMAR, CNRS, UMR 6625, Université de Rennes 1, Université européenne de Bretagne,
Campus de Beaulieu, F-35042 Rennes

Felix Ulmer

IRMAR, CNRS, UMR 6625, Université de Rennes 1, Université européenne de Bretagne,
Campus de Beaulieu, F-35042 Rennes

Abstract

The construction of cyclic codes can be generalized to so-called ”module \( \theta \)-codes” using non-commutative polynomials. The product of the generator polynomial \( g \) of a self-dual ”module \( \theta \)-code” and its ”skew reciprocal polynomial” is known to be a noncommutative polynomial of the form \( X^n - a \), reducing the problem of the computation of all such codes to the resolution of a polynomial system where the unknowns are the coefficients of \( g \). We show that \( a \) must be \( \pm 1 \) and that over \( \mathbb{F}_4 \) for \( n = 2^s \) the factorization of the generator \( g \) of a self-dual \( \theta \)-cyclic code has some rigidity properties which explains the small number of self-dual \( \theta \)-cyclic codes with length \( n = 2^s \). In the case \( \theta \) of order two, we present a construction of self-dual codes, based on the least common multiples of noncommutative polynomials, that allows to reduce the computation to polynomial systems of smaller sizes than the original one. We use this approach to construct a \([78, 39, 19]_4 \) self-dual code and a \([52, 26, 17]_9 \) self-dual code which improve the best previously known minimal distances for these lengths.

Keywords: error-correcting codes, finite fields, skew polynomial rings

1. Introduction

For a finite field \( \mathbb{F}_q \) and \( \theta \) an automorphism of \( \mathbb{F}_q \) we consider the ring \( R = \mathbb{F}_q[X; \theta] = \{a_nX^n + \ldots + a_1X + a_0 | a_i \in \mathbb{F}_q \text{ and } n \in \mathbb{N} \} \) where addition is defined to be the usual addition of polynomials and where multiplication is defined by the basic rule \( X \cdot a = \ldots \)

Email addresses: delphine.boucher@univ-rennes1.fr (Delphine Boucher), felix.ulmer@univ-rennes1.fr (Felix Ulmer).

URLs: URL 1 (Delphine Boucher), URL 2 (Felix Ulmer).

Preprint submitted to Elsevier 7 October 2013
\( \theta(a) X \ (a \in \mathbb{F}_q) \), extended to all elements of \( R \) by associativity and distributivity. The noncommutative ring \( R \) is called a skew polynomial ring or Ore ring (cf. Ore (1933b)) and its elements are skew polynomials. It is a left and right Euclidean ring whose left and right ideals are principal. Left and right geds and lcms exist in \( R \) and can be computed using the left and right Euclidean algorithm. Over finite fields skew polynomial rings are also known as linearized polynomials (cf. Ore (1933a); Lidl and Niederreiter (1983)). Following Boucher and Ulmer (2009a) we define module \( \theta \)-codes using the skew polynomial ring \( R \).

**Definition 1.** A module \( \theta \)-code (or module skew code) \( C \) is a left \( R \)-submodule \( Rg/Rf \subset R/Rf \) in the basis \( 1, X, \ldots, X^{n-1} \) where \( g \in R = \mathbb{F}_q[X; \theta] \) and \( f \) is a left multiple of \( g \) in \( R \) of degree \( n \). We denote this code \( C = (g)_{\theta}^n \). If there exists an \( a \in \mathbb{F}_q \setminus \{0\} \) such that \( g \) divides \( X^n - a \) on the right, then the code \( (g)_{\theta}^n \) is \( \theta \)-constacyclic. We will denote it \( (g)_{\theta}^{n,a} \). If \( a = 1 \), the code is \( \theta \)-cyclic and if \( a = -1 \), it is \( \theta \)-negacyclic.

The length of the code is \( n \) and its dimension is \( k = n - \deg(g) \), we say that the code \( C \) is of type \( [n, k]_q \). If the minimal distance of the code is \( d \), then we say that the code \( C \) is of type \( [n, k, d]_q \). As in the commutative case we identify a codeword in the \( \mathbb{F}_q \)-vector space \( R/Rf \) of dimension \( n \) with the list of coefficients of a skew polynomial of degree \( < n \) which is a left multiple of \( g \). The code \( C = Rg/Rf \subset R/Rf \) is the set of left multiples of \( g \) of degree \( < n \) and therefore depends only on \( g \) and \( n \). For \( g = \sum_{i=0}^{n-1} g_i X^i \), the generator matrix of the module \( \theta \)-code \( (g)_{\theta}^n \) is given by

\[
G_{g,n}^\theta = \begin{pmatrix}
g_0 & \cdots & g_{n-k-1} & g_{n-k} & 0 & \cdots & 0 \\
0 & \theta(g_0) & \cdots & \theta(g_{n-k-1}) & \theta(g_{n-k}) & \cdots & 0 \\
0 & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
0 & \cdots & 0 & \theta^{k-1}(g_0) & \cdots & \theta^{k-1}(g_{n-k-1}) & \theta^{k-1}(g_{n-k})
\end{pmatrix}
\]

(1)

showing that distinct generator polynomials correspond to distinct generator matrices.

On the other hand, a skew polynomial \( f \), that can be used to define \( C \) as \( Rg/Rf \), gives informations on the properties of the code. For example, for a \( \theta \)-constacyclic code \( (g)_{\theta}^{n,a} \), where one can choose \( f = X^n - a \), we have

\[ (c_0, \ldots, c_{n-1}) \in (g)_{\theta}^{n,a} \Rightarrow (a \theta(c_{n-1}), \theta(c_0), \ldots, \theta(c_{n-2})) \in (g)_{\theta}^{n,a}. \]

Since \( \mathbb{F}_q[X; \theta] \) is not a unique factorization ring, we obtain much more codes that are \( \theta \)-constacyclic, using the noncommutative approach, than constacyclic codes in the commutative case. Module \( \theta \)-codes are a generalization of Gabidulin codes (cf. Gabidulin (1985)) based on linearized polynomials.

**Example 2.** For \( \mathbb{F}_4 = \mathbb{F}_2(a) \) where \( a^2 + a + 1 = 0 \) and \( \theta \) the Frobenius automorphism \( \alpha \mapsto \alpha^2 \) the skew polynomial \( X^2 + 1 \) admits three distinct decompositions as products of irreducible polynomials in \( \mathbb{F}_4[X; \theta] \)

\[ X^2 + 1 = (X + a^2)(X + a) = (X + a)(X + a^2) = (X + 1)(X + 1) \]

(2)
The polynomials $X^4 + 1, X^6 + 1$ and $X^8 + 1$ admit respectively 15, 90 and 543 distinct decompositions as products of irreducible polynomials in $\mathbb{F}_4[X, \theta]$ (counting the number of factorizations is considered in von zur Gathen et al. (2010)).

In previous work many self-dual module $\theta$-codes with good minimum distances were obtained, sometimes even improving the previously best known minimal distances. However, as in the case of cyclic codes (Jia et al. (2011)), there is a phenomena for the module $\theta$-codes whose lengths are a power of 2. For the lengths 4, 8, 16, 32 and 64 there are only three self-dual module $\theta$-codes over $\mathbb{F}_4$, while otherwise there is a large number of self-dual codes which increases with the length. The authors conjectured that for any $s$ there are only three self-dual module $\theta$-codes of length $2^s$ over $\mathbb{F}_4$ (Boucher and Ulmer (2009a, 2011)). The aim of this paper is to use the factorization properties of skew polynomials to count self-dual module $\theta$-codes of length $2^s$ over $\mathbb{F}_4$ and to construct self-dual module $\theta$-codes when $\theta$ is of order two. The material is organized as follows:

In section 2 we introduce self-dual skew codes and recall the basic properties of such codes. Such a code was known to be $\theta$-constacyclic and we show that it must in fact be $\theta$-cyclic or $\theta$-negacyclic.

In section 3 we prove that for all $s \in \mathbb{N}^*$, there are $2^{2s-1} + 1$ $\theta$-cyclic codes of length $2^s$ and dimension $2^{s-1}$ over $\mathbb{F}_4$ but that for $s > 1$ among them only three are self-dual. This gives an answer to the above conjecture.

In section 4, we give an iterative construction of self-dual module $\theta$-codes by constructing generator polynomials of self-dual module $\theta$-codes as least common left multiples (lclm) of skew polynomials of lower degree. An example of a $[78,39,19]_4$ self-dual code and an example of a $[52,26,17]_4$ self-dual code are given.

2. Self-dual skew codes over a finite field

The (Euclidean) dual of a linear code $C$ of length $n$ over $\mathbb{F}_q$ is defined with the Euclidean scalar product $< x, y > = \sum_{i=1}^n x_i y_i$ in $\mathbb{F}_q^n$ as $C^\perp = \{ x \in \mathbb{F}_q^n \mid \forall y \in C, < x, y > = 0 \}$. A linear code $C$ over $\mathbb{F}_q$ is Euclidean self-dual or self-dual if $C = C^\perp$. To characterize self-dual module $\theta$-codes, we need to define the skew reciprocal polynomial of a skew polynomial (definition 3 of Boucher and Ulmer (2011)) and also the left monic skew reciprocal polynomial.

Definition 3. The skew reciprocal polynomial of $h = \sum_{i=0}^n h_i X^i \in R$ of degree $m$ is $h^* = \sum_{i=0}^m X^{m-i} \cdot h_i = \sum_{i=0}^m \theta^i(h_{m-i}) X^i$. The left monic skew reciprocal polynomial of $h$ is $h^* := (1/\theta^n(h_0)) \cdot h^*$.

Since $\theta$ is an automorphism, the map $\ast : R \to R$ given by $h \mapsto h^*$ is a bijection. In particular for any $g \in R$ there exists a unique $h \in R$ such that $g = h^*$ and, if $g$ is monic, such that $g = h^2$. In order to describe some properties of the skew reciprocal polynomial we will use the morphism of rings $\Theta : R \to R$ given by $\sum_{i=0}^n a_i X^i \mapsto \sum_{i=0}^n \theta(a_i) X^i$.

Lemma 4 (Boucher and Ulmer (2011), Lemma 1). Let $f$ and $g$ be skew polynomials in $R$. Then

1. $(fg)^* = \Theta^k(g^*) f^*$, where $k = \deg(f)$.
2. $(f^*)^* = \Theta^n(f)$, where $n = \deg(f)$.
A module $\theta$-code of length $n = 2k$ which is self-dual is known to be $\theta$-constacyclic, i.e. its generator polynomial $g$ of degree $k$ divides on the right $X^n - a$ for some $a$ in $\mathbb{F}_q \setminus \{0\}$ (Corollary 1 of Boucher and Ulmer (2011)). Furthermore the dual of $(g)^{h\theta}$ is generated by the polynomial $h^2$ where $h$ satisfies simultaneously $\Theta^n(h) \cdot g = X^n - a$ and $g \cdot h = X^n - \theta^{-k}(a)$ (Theorem 1 of Boucher and Ulmer (2011)). The following proposition improves those previous results:

**Proposition 5.** A self-dual module $\theta$-code is either $\theta$-cyclic or $\theta$-negacyclic.

**Proof.** If $n = 2k$ and $C = (g)^h_\theta$ is a self-dual module $\theta$-code, then $C$ is necessarily $\theta$-constacyclic with a generator polynomial $g$ dividing $X^n - a$ on the right in $R$ with $a \in \mathbb{F}_q \setminus \{0\}$ (Boucher and Ulmer (2011), Corollary 1). Consider $h \in R$ of degree $k$ such that $\Theta^n(h) \cdot g = X^n - a$. From Lemma 4, we obtain $\Theta^{k-n}(g)h^* = -a(X^n - \frac{1}{a})$, or equivalently $\frac{1}{a} \Theta^{k-n}(g)h^* = X^n - \frac{1}{a}$. Therefore $h^2 = \frac{1}{a} \Theta^{k-n}(g)$ divides $X^n - \frac{1}{a}$ on the right. Furthermore from (Boucher and Ulmer (2011), Theorem 1), the dual of $C = (g)^h_\theta$ is generated by $h^2$. Since $C$ is a self-dual module $\theta$-code, from the uniqueness of its monic generator polynomial, we have $g = h^2$. Therefore $g$ divides the right the polynomial $(X^n - a) - (X^n - \frac{1}{a}) = a - \frac{1}{a}$ of degree less than $g$ which must be zero and we obtain $a^2 = 1$. □

Combining this result with (Boucher and Ulmer (2011), Theorem 1) we obtain:

**Corollary 6.** A module $\theta$-code $(g)^h_\theta$ with $g \in \mathbb{F}_q[X; \theta]$ of degree $k$ is self-dual if and only if there exists $h \in R$ such that $g = h^2$ and

$$h^2h = X^{2k} - \varepsilon$$

with $\varepsilon \in \{-1, 1\}.$

3. **Self-dual module $\theta$-codes of length $2^n$ over $\mathbb{F}_4$.**

We keep the notation $R = \mathbb{F}_q[X; \theta]$ and we denote $(\mathbb{F}_q)^{\theta}$ the fixed field of $\theta$. The properties of the ring $R$ used in this paper can for example be found in Jacobson (1943) Chapter 3 and Giesbrecht (1998); Ore (1933b). The center $Z(R)$ of $R$ is the commutative polynomial subring $(\mathbb{F}_q)^{\theta}[X^{\theta}]$ in the variable $Y = X^{\theta}$ where $|\theta|$ is the order of $\theta$. We denote $Z(R)$ also $(\mathbb{F}_q)^{\theta}[Y]$. According to (Jacobson (1943), p. 38,39), a left ideal is bounded if it contains a two-sided ideal. Following this definition we call an element $h \in R$ bounded if the left ideal $Rh$ it generates is bounded and the monic generator $f$ of the maximal two-sided ideal contained in $Rh$ is the bound of $h$. In the ring $R$ all elements are bounded. The two sided ideals in $R$ are the ideals of the form $(X^m f)$, where $f \in Z(R)$, and the set of two-sided ideals is closed under multiplication. A bound $f$ is an irreducible bound if the two-sided ideal $(f) \subset R$ is maximal. A bound with a nonzero constant term belongs to the center $Z(R) = (\mathbb{F}_q)^{\theta}[Y]$ of $R$ and is an irreducible bound if and only if $f(Y) \in (\mathbb{F}_q)^{\theta}[Y]$ is an irreducible (commutative) polynomial (Jacobson (1943), Chap. 3, Th. 12).

**Theorem 7.** (Ore (1933b); Jacobson (1943), Chap. 3, Th. 5) Let $R = \mathbb{F}_q[X; \theta]$. If $h_1 h_2 \cdots h_n$ and $g_1 g_2 \cdots g_m$ are two decompositions into irreducible factors of $h \in R$, then $m = n$ and there exists a permutation $\sigma \in S_n$ such that the $R$-modules $R/h_i R$ and $R/g_{\sigma(i)} R$ are isomorphic. In particular the degrees of the irreducible factors of $h$ are unique up to permutation.
The noncommutative ring \( R \) is not a unique factorization ring and there can be more distinct monic factors than in the commutative case as shown in the example below. An important difference is that those monic factors can not always be permuted.

**Definition 8.** (Jacobson (1943), Chap. 3) \( h \in R \) is **lclm-decomposable**\(^1\) if \( h \) is the least common left multiple of skew polynomials of degree strictly less than \( h \), i.e. \( h = \text{lclm}(h_1, h_2) \) where \( h_i \in R \) and \( \text{deg}(h_i) < \text{deg}(h) \). The polynomial \( h \in R \) is **lclm-indecomposable** if \( h \) is not lclm-decomposable.

**Example 9.** Consider \( \mathbb{F}_4 = \mathbb{F}_2(\alpha) \) where \( \alpha^2 + \alpha + 1 = 0 \) and \( \theta \) the Frobenius automorphism \( \alpha \mapsto \alpha^2 \). Two factors of a central polynomial always commute in \( \mathbb{F}_4[X; \theta] \):

\[
X^2 + 1 = (X + \alpha^2)(X + \alpha) = (X + \alpha)(X + \alpha^2) = (X + 1)(X + 1).
\]

(4)

Since the polynomial \( X^2 + 1 \) is right divisible by both \( X + \alpha \) and by \( X + 1 \), it must be the lcm of \( X + \alpha \) and \( X + 1 \) which is unique up to nonzero constants. In \( \mathbb{F}_4[X; \theta] \) we have \( g_1 = (X + \alpha)(X + 1) = X^2 + \alpha^2 X + \alpha \neq X^2 + aX + a = (X + 1)(X + \alpha) = g_2 \). One can verify that the polynomials \( g_1 \) and \( g_2 \) have no further irreducible right or left monic factor, showing that those two polynomials are not the lcm of irreducible right factors and that in the nonunique factorization ring \( R \) some factorizations can still be unique in the sense that the unique irreducible monic factors can only be written in a unique order.

The next theorem gives a first characterization of those skew polynomials in \( R \) which do have a **unique factorization** into irreducible monic skew polynomials:

**Theorem 10.** (Jacobson (1943), Chap. 3, Th. 21 and 24) Let \( R = \mathbb{F}_q[X; \theta] \) and \( m \in \mathbb{N}^* \).

1. A monic polynomial \( h \) in \( R \) has a unique factorization into irreducible monic polynomials (in the sense that the unique irreducible monic factors can only be written in a unique order) if and only if \( h \) is lclm-indecomposable.
2. If \( h_1, h_2, \ldots, h_m \) are monic irreducible polynomials of \( R \) having the same irreducible bound \( f \in \mathbb{Z}(R) \), then the product \( h = h_1 h_2 \cdots h_m \) is an lclm-indecomposable monic polynomial in \( R \) if and only if the bound of \( h \) is \( f^m \).

Since the bound of a skew polynomial \( h \in R \) can be computed using linear algebra (Jacobson (1943); Giesbrecht (1998); Boucher and Ulmer (2009b)), the above result is an efficient test to verify if \( h \) is lclm-indecomposable. In the following however, we search for a method to construct lclm-indecomposable polynomials directly.

**Corollary 11.** Consider the decomposition \( h = h_1 \cdots h_m \) of \( h \in R \) into irreducible monic polynomials having all the same irreducible bound \( f \) which is reducible in \( R \).

1. If \( h \) is lclm-indecomposable, then \( f \) does not divide \( h \).
2. If \( f \) does not divide \( h \) then no partial product \( h_i h_{i+1} \cdots h_{i+j} \) appearing in \( h = h_1 \cdots h_m \) can be equal to \( f \).

\(^1\) In Jacobson (1943) the term decomposable is used.
Proof. (1) From (Jacobson (1943), Chap. 3, Th. 12) we obtain that the bound of a product divides the product of the bounds. If \( f \) divides \( h \), then the quotient is a product of at most \( m - 2 \) factors, because \( f \) is reducible and therefore the bound of \( h \) divides \( f \) times the bound of the quotient, so it divides \( f^{m-1} \) and the result follows from part (2) of Theorem 10.

(2) If there exists \( i, j \) such that \( f = h_i h_{i+1} \cdots h_{i+j} \) then \( f h_{i+j+1} \cdots h_m \) is a right factor of \( h \). As \( f \) is central, it commutes with \( h_{i+j+1} \cdots h_m \) and therefore \( f \) divides \( h \) on the right.

\hfill \Box

Example 12. We keep the notations of the previous example. The bound of

\[ h = (X + 1)(X + a)(X + 1)(X + a^2)(X + 1)(X + a^2)(X + 1) \]

is \((X^2 + 1)^7\) and therefore the previous theorem shows that this factorization of \( h \) in \( F_4[X; \theta] \) is unique. Corollary 11 implies that the common central bound \( X^2 + 1 \) of the factors of \( h \) does not divide \( h \) and that two irreducible factors \( X + 1, X + a \) and \( X + a^2 \) of \( X^2 + 1 \) which appear together in a decomposition of \( X^2 + 1 \) (like in example 9) never appear next to each other in the decomposition of \( h \).

Our goal is to prove the converse of the above corollary under the assumption that \( \theta \in \text{Aut}(F_q) \) is of order two, as is the case for \( F_4, F_9, F_{25} \) and \( F_{49} \). When \( \theta \) is of order two, then \( X^{2n} \pm 1 \) belongs to the center \( Z(R) \) of \( R \). In this case the bound of any factor of \( X^{2n} \pm 1 \) also belongs to \( Z(R) \) (Jacobson (1943), Chap. 3, Th. 12). Therefore we will now focus on polynomials whose bounds are central polynomials of the form \( f \in (F_q)^\theta[X^{|\theta|}] \).

Lemma 13. Consider \( R = F_q[X; \theta] \) with \( \theta \) of order two.

(1) For \( g = \sum_{i=0}^{m} a_i X^i \in R \) and for \( \overline{g} = \sum_{i=0}^{m} (-1)^i \theta^{i+1}(a_i) X^i \) we have \( g\overline{g} \in Z(R) \). In particular the bound of \( g \) is of degree \( \leq 2 \deg(g) \).

(2) An irreducible bound \( f \in Z(R) \) which is reducible in \( R \), factors as the product of two irreducible polynomials in \( R \) of degree \( \frac{\deg(f)}{2} \).

Proof. (1) For \( l \in \{0, \ldots, 2m\} \), the \( l \)-th coefficient of \( G = g\overline{g} \) is given by \( G_l = \sum_{i+j=l} a_i (-1)^l \theta^{i+1}(a_j) \). If \( l \) is even, then

\[ G_l = \sum_{i+j=l} a_i (-1)^l \theta^{i+1}(a_j) = \sum_{i+j=l} a_i (-1)^l \theta(a_j). \]

As \( \theta^2 = id \), \( \theta(G_l) = \sum_{i+j=l} \theta(a_i)(-1)^i a_j = G_l \). If \( l \) is odd, then

\[ G_l = \sum_{i+j=l} a_i (-1)^l a_j = \sum_{i+j=l, j \text{ even, } i \text{ odd}} a_i a_j - \sum_{i+j=l, i \text{ odd, } j \text{ even}} a_i a_j = 0. \]

So \( G \) belongs to \( (F_q)^\theta[X^2] = Z(R) \).

(2) The irreducible factors of an irreducible bound \( f \) are of the same degree \( d \) (Jacobson (1943), Chap. 3, Corollary of Th. 20 or Theorem 4.3 of Giesbrecht (1998)) and as \( f \) is reducible, \( d \) must be \( \leq \deg(f)/2 \). The first assertion shows that the factors of \( f \) are of degree \( \geq \deg(f)/2 \) so \( d = \deg(f)/2 \).
If the characteristic of $\mathbb{F}_q$ divides the order of $\theta$, then a central bound $f \in (\mathbb{F}_q)^g[X^{\theta}]$ is reducible in the commutative subring $(\mathbb{F}_q)^g[X] \subseteq R$ and therefore reducible in $R$. From Theorem 7 we get that the number of irreducible factors of $f$ is independent of the factorization.

**Definition 14.** Consider $R = \mathbb{F}_q[X; \theta]$ and let $f \in Z(R)$ be an irreducible bound which is reducible in $R$. To each right monic factor $g$ of $f$ corresponds a unique $\theta \in R$ such that $gg = f$ called the complement of $g$ (for $f$).

**Example 15.** Consider $R = \mathbb{F}_q[X; \theta]$ with $\theta$ of order two. If the central bound $f = X^2 + \lambda \in Z(R)$ is reducible in $R$, then its irreducible monic factors are of the form $X + \alpha \in R$. The skew polynomial $X + \bar{\alpha} \in R$ is the complement of $X + \alpha$ if and only if $(X + \bar{\alpha})(X + \alpha) = X^2 + (\bar{\alpha} + \theta(\alpha))X + \bar{\alpha}\alpha = X^2 + \lambda$, which is the case if and only if

$$\bar{\alpha} = \lambda/\alpha \quad \text{and} \quad \theta(\alpha) = -\lambda/\alpha$$  \hspace{1cm} (5)

The following Proposition gives the converse of Corollary 11 when $\theta$ is of order two.

**Proposition 16.** Consider $R = \mathbb{F}_q[X; \theta]$ with $\theta$ of order two, $f \in Z(R)$ and irreducible bound that is reducible over $R$ and $h = h_1 \cdots h_m$ a product of irreducible monic polynomials bounded by $f$. The following assertions are equivalent

(i) $h$ is lclm-decomposable;
(ii) $f$ divides $h$ in $R$;
(iii) there exists $i$ in $\{1, \ldots, m-1\}$ such that $h_{i+1}$ is the complement of $h_i$ for $f$ (a factor $f = h_{i+1}h_i$ must be present in the factorization).

Proof. Corollary 11 shows that (even if $\theta$ has not order two) we always have (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i). In order to prove the implication (i) $\Rightarrow$ (iii) we proceed by induction on $m \geq 2$ (here we will use the fact that $\theta$ is of order two). If $h = h_1h_2$ where $h_1$ and $h_2$ are irreducible monic polynomials with bound $f$, the bound of $h$ divides the product of the bounds of $h_1$ and $h_2$ (Jacobson (1943), Chap. 3, Th. 12), so it divides $f^2$ in the commutative ring $(\mathbb{F}_q)^g[X]$. Assume that $h$ is lclm-decomposable, then according to part (2) of Theorem 10, the bound of $h$ is not $f^2$. As $f$ is irreducible in $(\mathbb{F}_q)^g[X^2]$ the bound of $h$ is equal to $f$ and $h$ divides $f$ on the right. Since $\theta$ is of order two, the irreducible bound $f$ has degree $2\deg(h_1)$ (Lemma 13) so $\deg(h) = \deg(f)$ and $h = f$, which proves that the results holds for $m = 2$.

Suppose now $m > 2$ and that the result holds for $i < m$. Let $h = h_1 \cdots h_m$ be lclm-decomposable where $h_i$ are irreducible monic polynomials with bound $f$. Then, there exist $g_1, \ldots, g_m \in R$ such that $h = g_1 \cdots g_m$ where $(g_1, \ldots, g_m) \neq (h_1, \ldots, h_m)$. If $g_m = h_m$ then $g_1 \cdots g_{m-1} = h_1 \cdots h_{m-1}$ is lclm-decomposable and one concludes using the induction hypothesis. Otherwise $\lclm(g_m, h_m) = \tilde{h}_{m-1}h_m$ divides on the right $h = h_1 \cdots h_m = h_1 \cdots h_{m-1}h_m$. So $h_1 \cdots h_{m-1} = h_1 \cdots h_{m-1}$. If there exist $i$ such that $\tilde{h}_i \neq h_i$, then $h_1 \cdots h_{m-1}$ is lclm-decomposable and one concludes using the induction hypothesis; otherwise $h_{m-1} = \tilde{h}_{m-1}$ and $\lclm(g_m, h_m) = h_{m-1}h_m$ is lclm-decomposable; so using the same argument as for $m = 2$ above, we obtain $h_{m-1}h_m = f$ and the result follows. $\square$
Example 17. We keep the notations of the previous example. Proposition 16 shows that in \( \mathbb{F}_q[X;\theta] \) the polynomials \((X+1)(X+a)(X+1)(X+a^2)(X+1)(X+a^3)(X+1), (X+a)(X+a), (X+a)(X+1), (X+1)(X+a), (X+a^2)(X+a^3), (X+a^2)(X+1) \) and \((X+1)(X+a^3)\) are lcm-indecomposable, i.e. the factorization of each polynomial into monic irreducible polynomials is unique.

The example below shows that in general the converse of Corollary 11 does not hold.

Example 18. Consider \( \mathbb{F}_8 = \mathbb{F}_2(b) \) where \( b^3 + b + 1 = 0 \) and \( \theta \) the Frobenius automorphism \( \alpha \mapsto \alpha^2 \) of order three. The skew polynomial \( h = (X+b^4)(X+1) \) is the product of two irreducible skew polynomials bounded by \( f = X^3 + 1 \in \mathbb{F}_2[X^3] = Z(\mathbb{F}_8[X;\theta]) \). Furthermore it is lcm-decomposable as \( h = (X+b^4)(X+1) = (X+b^3)(X+b) = \text{lcm}(X+1, X+b)\), but it is not divisible by \( f \).

Definition 19. Consider \( R = \mathbb{F}_q[X;\theta] \) and let \( f \in Z(R) \) be an irreducible bound which is reducible in \( R \). The number of distinct irreducible monic right factors \( g \in \mathbb{F}_q[X;\theta] \) of \( f \) is the capacity \( \kappa \) of \( f \).

Example 20. Consider \( R = \mathbb{F}_q[X;\theta] \) with \( \theta \) of order two. Example 15 shows that the capacity \( \kappa \) of the bound \( X^2 + \lambda \) is the size of \( \{ a \in \mathbb{F}_q \mid \theta(a)a = -\lambda \} \). In particular, the capacity of the central polynomial \( X^2 + 1 \in \mathbb{F}_4[X;\theta] \) with \( \theta : \alpha \mapsto \alpha^2 = 3 \), while the three irreducible factors of \( X^2 + 1 \) in \( \mathbb{F}_4[X;\theta] \) are given in example 9.

Proposition 21. Let \( R = \mathbb{F}_q[X;\theta] \) with \( \theta \) of order two, \( 1 \leq m \in \mathbb{N} \) and \( f \in Z(R) \) an irreducible bound which is reducible in \( R \) of capacity \( \kappa > 2 \). The number \( A(m) \) of distinct monic right factors \( g \in R \) of degree \( \frac{m \cdot \deg(f)}{2} \) of \( f^m \) is \( (\kappa - 1)^{m+1} - 1 \)/\((\kappa - 2)\).

Proof. According to Lemma 13, the irreducible factors of \( f \) all have the same degree \( \deg(f)/2 \). Therefore the irreducible factors of \( f^m \) are all of degree \( \deg(f)/2 \). If \( g = g_1g_2\cdots g_m \) is a factorization into monic irreducible polynomials with bound \( f \), and \( \overline{g} \) the complement of \( g_i \), then \( f^m = \overline{f}_m\cdots\overline{f}_1g_1g_2\cdots g_m \). Therefore \( g \) is always a divisor of \( f^m \) and we only need to count the different polynomials \( g = g_1g_2\cdots g_m \) whose irreducible monic factors are bounded by \( f \).

1. If \( g \) is divisible by the central bound \( f \in Z(R) \), then \( g = g'f \) where \( g' = g'_1\cdots g'_{m-2} \) and \( g'_i \) of degree \( \deg(f)/2 \) : there are \( A(m-2) \) such polynomials.

2. Proposition 16 shows that \( g \) is not divisible by \( f \) if and only if for all \( i \), \( g_{i+1} \) is not the complement for \( f \) of \( g_i \). There are \( \kappa \) choices for \( g_1 \) and \( \kappa - 1 \) choices for each factor \( g_2, g_3, \ldots, g_m \).

From \( A(0) = 1, A(1) = \kappa \) and \( A(m) = A(m-2) + \kappa(\kappa - 1)^{m-1} \) we get the result by solving the recursion. \( \square \)

Corollary 22. Let \( \theta \) be the Frobenius automorphisms of \( \mathbb{F}_4 \). For \( s \in \mathbb{N} \setminus \{0\} \) there are \( 2^{2^s-1} - 1 \) module \( \theta \)-cyclic codes over \( \mathbb{F}_4 \) of length \( 2^s \) and dimension \( 2^{s-1} \).

Proof. \( X^{2^s} - 1 = (X^2 + 1)^{2^{s-1}} \) in \( \mathbb{F}_4[X;\theta] \), and the capacity of \( X^2 + 1 \) is \( \kappa = 3 \), so according to the previous proposition applied with \( m = 2^{s-1} \), the skew polynomial \( X^{2^s} - 1 \) has \( 2^{2^s-1} - 1 \) monic right factors of degree \( 2^{s-1} \) in \( \mathbb{F}_4[X;\theta] \). \( \square \)
In the proposition and the corollary above the number of \( \theta \)-cyclic codes over \( \mathbb{F}_4 \) of length \( 2^s \) was obtained by counting the number of distinct monic factors with degree \( 2^s-1 \) of \( (X^2 + 1)^{2^{s-1}} = X^{2^s} + 1 \) using the fact that they are products of linear factors. In the same way the number of self-dual \( \theta \)-h also the relation obtained by counting the number of factors \( h \) with degree \( 2^s-1 \) of \( X^{2^s} + 1 \) which satisfy also the relation \( h^2h = X^{2^s} + 1 \) (cf. Corollary 6).

**Proposition 23.** Let \( R = \mathbb{F}_q[X; \theta] \) with \( \theta \) of order two, \( 1 \leq m \in \mathbb{N} \), \( f \in \mathbb{Z}(R) \) an irreducible bound which is reducible in \( R \) and \( h_i \in R \) and \( g_j \in R \) monic irreducible polynomials having all the same bound \( f \). If \( g_m g_{m-1} \cdots g_1 \) is lcm-indecomposable and

\[
f^m = h_1 \cdots h_{m-1} h_m g_m g_{m-1} \cdots g_1 \tag{6}
\]

then \( h_i \) is the complement of \( g_i \) (for \( f \)).

**Proof.** We proceed by induction on \( m \). If \( m = 1 \) the result is trivial. Suppose that the result holds for \( i < m \). The rhs of (6) is clearly divisible by \( f \) and Proposition 16 shows that two consecutive factors in the rhs of (6) must be complements to each other and their product equal to \( f \). We get three cases

1. There are two successive factors which are complements to each other in the decomposition \( g_m g_{m-1} \cdots g_1 \) of \( g \). Since \( g \) is lcm-indecomposable, Corollary 11 shows that this case cannot occur.

2. If \( h_m \) is the complement of \( g_m \), then we can divide both sides of equation (6) by the central polynomial \( h_m g_m = f \) to obtain \( h_1 \cdots h_{m-1} g_{m-1} \cdots g_1 = f^{m-1} \). Since \( g_{m-1} \cdots g_1 \) is lcm-indecomposable, we obtain the result by induction.

3. Otherwise there are two successive factors which are complements to each other in the product \( h_1 \cdots h_{m-1} h_m \) and we prove that this case cannot happen. Namely, consider \( i \) such that \( h_i h_{i+1} = f \). Dividing both sides of (6) by the central polynomial \( f \) gives \( (h_1 \cdots h_{i-1} h_{i+2} h_m g_m) (g_{m-1} \cdots g_1) = f^{m-1} \). Applying the induction hypothesis to \( g_{m-1} \cdots g_1 \) which is lcm-indecomposable, we obtain that \( g_m \) is the complement of \( g_{m-1} \) which is impossible according to Corollary 11 because \( g_m g_{m-1} \cdots g_1 \) is lcm-indecomposable.

\( \square \)

In the following we want to decide in some special cases if a product of linear polynomials \((X + \alpha_1) (X + \alpha_2) \cdots (X + \alpha_m)\) generates a self-dual code. One difficulty is that the skew reciprocal polynomial of a monic polynomial is not always monic: \((X + \alpha)^* = \theta(\alpha) X + 1 = \theta(\alpha) (X + 1/\theta(\alpha))\).

**Lemma 24.** Consider \( 0 < m \in \mathbb{N} \) and \( \alpha_1, \alpha_2, \ldots, \alpha_m \) in \( \mathbb{F}_q \setminus \{0\} \). For the skew polynomial \( g = (X + \alpha_1)(X + \alpha_2) \cdots (X + \alpha_m) \in \mathbb{F}_q[X; \theta] \) we have

\[
g^* = \theta^m(\alpha_1 \cdots \alpha_m) \left( X + \frac{\theta^{m-1}(\alpha_1 \cdots \alpha_{m-1})}{\theta^m(\alpha_1 \cdots \alpha_m)} \right) \cdots \left( X + \frac{\theta(\alpha_1)}{\theta^2(\alpha_1 \alpha_2)} \right) \left( X + \frac{1}{\theta(\alpha_1)} \right)
\]

from which we can deduce \( g^\# \) by dividing on the left by \( \theta^m(\alpha_1 \cdots \alpha_m) \).
Proof. We proceed by induction on \( m \). For \( m = 1 \) the result holds. Assume that the result holds for \( k < m \). Lemma 4 shows
\[
((X + \alpha_1) \cdots (X + \alpha_m))^* = \theta^{m-1} ((X + \alpha_m)^*) ((X + \alpha_1) \cdots (X + \alpha_{m-1}))^*
\]
By induction we only need to express \( h = \theta^m ((X + \alpha_m)^*) \theta^{m-1}(\alpha_1 \cdots \alpha_{m-1}) \) as a product of a constant times a monic linear polynomial. By direct computation we obtain
\[
h = \theta^m (\alpha_m) \left( X + \frac{1}{\theta(\alpha_m)} \right) \theta^{m-1}(\alpha_1 \cdots \alpha_{m-1})
= \theta^m (\alpha_1 \cdots \alpha_m) \left( X + \frac{\theta^{m-1}(\alpha_1 \cdots \alpha_{m-1})}{\theta^m(\alpha_1 \cdots \alpha_m)} \right).
\]
The claim now follows by induction. \( \square \)

Proposition 25. Consider \( F_4 = F_2(a) \), \( \theta \) the Frobenius automorphism \( \alpha \mapsto \alpha^2 \) and \( h \in F_4[X; \theta] \) to be monic of degree \( m \in \mathbb{N} \). Then
\[
h^2h = (X^2 + 1)^m
\]
if and only if
\[
h = \begin{cases} (X + 1)^m & \text{if } m \text{ is odd} \\ (X + 1)^{m-1}(X + u), u \in \{1, a, a^2\} & \text{if } m \text{ is even.} \end{cases}
\]

Proof. (\( \Leftarrow \)): If \( m \) is odd, the previous Lemma shows that the skew polynomial \( h = (X + 1)^m \) satisfies (7). Let us assume that \( m \) is even and consider \( h = (X + 1)^{m-1}(X + u) \) with \( u \in F_4 \setminus \{0\} \). From Lemma 4 we obtain
\[
h^* = \Theta((X + u)^*)(X + 1)^{m-1} = u(X + u^2)(X + 1)^{m-1}.
\]
Therefore \( h^2 = (X + u^2)(X + 1)^{m-1} \) and \( hh^2 = (X^2 + 1)^m \). Since \( (X^2 + 1)^m \) is central, this product commutes.

(\( \Rightarrow \)): From (7) and the fact that \( X^2 + 1 \) is reducible over \( F_4[X; \theta] \) we obtain that \( h \) is of the form \( (X + \alpha_1) \cdots (X + \alpha_m) \). Lemma 24 shows that
\[
h^2 = \left( X + \frac{\theta^{m-1}(\alpha_1 \cdots \alpha_{m-1})}{\theta^m(\alpha_1 \cdots \alpha_m)} \right) \cdots \left( X + \frac{\theta(\alpha_1)}{\theta^2(\alpha_1 \alpha_2)} \right) \left( X + \frac{1}{\theta(\alpha_1)} \right).
\]
Since all the factors of \( h \) have the same irreducible bound \( X^2 + 1 \) which is reducible in \( F_4[X; \theta] \) and \( \theta \) is of order two, we can apply Proposition 23 whenever \( h \) is lcim-indecomposable. We proceed by induction on \( m \).

(1) Case \( m = 1 \). We get \( (X + 1/\theta(\alpha_1))(X + \alpha_1) = X^2 + 1 \) showing that \( X + 1/\theta(\alpha_1) \) is the complement of \( X + \alpha_1 \). Using formula (5) we obtain \( 1/\theta(\alpha_1) = 1/\alpha_1 \) and \( \theta(\alpha_1) = 1/\alpha_1 \). Therefore \( \alpha_1^2 + 1 = (\alpha_1 + 1)^2 = 0 \), which implies \( \alpha_1 = 1 \).

(2) Case \( m = 2 \). If \( h = (X + \alpha_1)(X + \alpha_2) \) is lcim-decomposable, then according to Proposition 16, \( h \) is divisible and therefore equal to \( X^2 + 1 = (X + 1)(X + 1) \) and the result follows. If \( h \) is lcim-indecomposable, then Proposition 23 shows that \( X + 1/\theta(\alpha_1) \) is the complement of \( X + \alpha_1 \). Like in the case \( m = 1 \) this implies that \( \alpha_1 = 1 \) and \( h = (X + 1)(X + \alpha_2) \) and the result follows.
(3) Case $m = 3$. If $h = (X + \alpha_1)(X + \alpha_2)(X + \alpha_3)$ is lclm-indecomposable then Proposition 23 shows that for $i = 1, 2, 3, X + \theta^{i-1}(\alpha_1 \cdots \alpha_{i-1})/\theta^i(\alpha_1 \cdots \alpha_i)$ is the complement of $X + \alpha_i$. For $i = 1$, like in the case $m = 1$ we get that $\alpha_2 = 1$, and therefore for $i = 3$ we obtain $(X + \frac{\alpha_2}{\theta(\alpha_2\alpha_3)})(X + \alpha_3) = X^2 + 1$. The constant coefficient of these two polynomials is $\frac{\theta(\alpha_2\alpha_3)}{\theta(\alpha_2\alpha_3)} = 1$, so $\alpha_2\alpha_3 = 1$. We obtain $(X + \alpha_2)(X + \alpha_3) = (X + \alpha_2)(X + 1/\alpha_2) = X^2 + 1$, so $X^2 + 1$ divides $h$, which contradicts the lclm-irreducibility of $h$ (Corollary 11). Therefore $h$ is lclm-decomposable and, according to Proposition 16, $X^2 + 1$ divides $h$. We can write $h = (X + \alpha)(X^2 + 1)$.

Lemma 4 shows that $h^2h = (X^2 + 1)(X + 1/\theta(\alpha))(X + \alpha)(X^2 + 1)$ and after simplifying (7) we obtain $(X + 1/\theta(\alpha))(X + \alpha) = X^2 + 1$. As in the case $m = 1$ this implies that $\alpha = 1$, showing that $h = (X + 1)^3$.

(4) Suppose $m > 3$ and that the result holds for $i < m$. We first show that $h$ must be lclm-decomposable. If $h = (X + \alpha_1) \cdots (X + \alpha_m)$ is lclm-decomposable then Proposition 23 shows that $X + \theta^{m-1}(\alpha_1 \cdots \alpha_{m-1})/\theta^m(\alpha_1 \cdots \alpha_m)$ is the complement of $X + \alpha_m$. Dividing both sides of (7) on the right by $X + \alpha_m$ and on the left by its complement, we obtain that $(X + \alpha_1) \cdots (X + \alpha_{m-1})$ satisfies the induction hypothesis. So $\alpha_1 = \alpha_2 = \cdots = \alpha_{m-2} = 1$ and $(X + \alpha_1)(X + \alpha_2) = X^2 + 1$, which contradicts that $h$ is lclm-decomposable (Corollary 11).

As $h$ is lclm-decomposable $X^2 + 1$ divides $h$, say $h = q(X^2 + 1)$ (Proposition 16). Lemma 4 shows that $h^2h = (X^2 + 1)q^2q(X^2 + 1)$. Therefore $q^2q = (X^2 + 1)^{m-2}$ and we obtain the result for $q$ by induction, which gives also the result for $h = (X^2 + 1)^3$.

We now show that for any integer $s \geq 1$, from the $2^{s−1}+1−1$ module $\theta$-cyclic codes over $\mathbb{F}_4$ of length $2^s$, only 3 are self-dual, which proves Conjecture 1 of Boucher and Ulmer (2011):

**Corollary 26.** Consider $\mathbb{F}_4 = \mathbb{F}_2(a)$, $\theta$ the Frobenius automorphism $\alpha \mapsto \alpha^2$, $s > 1$ an integer and $g \in \mathbb{F}_4[X; \theta]$ monic of degree $2^{s−1}$. The code $(g)_{2^s}$ is self-dual if and only if $g = (X + u)(X + 1)^{2^{s−1}−1}$, where $u \in \{1, a, a^2\}$.

**Proof.** The code $(g)_{2^s}$ is self-dual if and only if there exists $h \in R$ such that $g = h^2$ and $h^2h = X^{2^{s−1}−1}$. The previous proposition applied with $m = 2^s−1$ shows that $h = (X + 1)^{2^{s−1}−1}(X + u)$ with $u \in \{1, a, a^2\}$. Therefore $h^2 = 4(1 + u^2X)(X + 1)^{2^{s−1}−1}$ and $g = h^2 = (X + u^2)(X + 1)^{2^{s−1}−1}$ (Lemma 4). □

4. **Construction of self-dual $\theta$-codes with $\theta$ of order 2**

Self-dual $\theta$-cyclic codes over $\mathbb{F}_q$ can be constructed by solving polynomial systems satisfied by the coefficients of their generator polynomials, however the polynomial system becomes increasingly difficult to solve (cf. Boucher and Ulmer (2009b)). In Jia et al. (2011) a characterization of the generator polynomials of (classical) self-dual cyclic codes of length $n$ over $\mathbb{F}_{2^n}$ is given using the factorization of $X^n − 1$ in $\mathbb{F}_{2^n}[X]$. In analogy to this result we give now a procedure that allows to construct all self-dual codes from suitable smaller degree polynomials. We start with a technical Lemma (a similar result appears in Jia et al. (2011) page 2245).
Lemma 27. Let $\mathbf{F}_q$ be a finite field, $\theta \in \text{Aut}(\mathbf{F}_q)$, $R = \mathbf{F}_q[X; \theta]$ and $\epsilon \in \{-1, 1\}$. The polynomial $Y^t - \epsilon \in (\mathbf{F}_q)^\theta[Y] = (\mathbf{F}_q)^\theta[Q^\theta] \subset R$ factors in $(\mathbf{F}_q)^\theta[Y]$ into distinct irreducible monic polynomials as

$$Y^t - \epsilon = h_1(Y) \cdots h_s(Y) \left( g_1(Y)g_1^\theta(Y) \right) \left( g_2(Y)g_2^\theta(Y) \right) \cdots \left( g_r(Y)g_r^\theta(Y) \right)$$

where $h_i(Y) = h_i^\theta(Y)$, $g_i(Y) \neq g_i^\theta(Y)$ and $(g_ig_i^\theta)^2 = g_i^2g_i$. Furthermore $Y^t - \epsilon$ factors in $(\mathbf{F}_q)^\theta[Y] = (\mathbf{F}_q)^\theta[X^t]$ as a product $f_1(Y) \cdots f_m(Y)$ of pairwise coprime polynomials of minimal degree such that $f_i^\theta = f_i$.

Proof. Let $g$ be an irreducible monic factor of $Y^t - \epsilon$ such that $g \neq g^\theta$. Assume that $g^\theta$ is reducible in $(\mathbf{F}_q)^\theta[Y]$, then according to Lemma 4, $g = (g^\theta)^r$ is also reducible in $(\mathbf{F}_q)^\theta[Y]$, so $g^\theta$ and therefore $g^2$ are irreducible in $(\mathbf{F}_q)^\theta[Y]$. Furthermore $g^\theta$ divides $(Y^t - \epsilon)^2$ (Lemma 4) therefore $g^2$ divides $(Y^t - \epsilon)^2$. As $(Y^t - \epsilon)^2 = -(Y^t - 1/\epsilon)$ and as $1/\epsilon = \epsilon$, we have $(Y^t - \epsilon)^2 = Y^{2t} - \epsilon$, which shows that $g^2$ divides $Y^{2t} - \epsilon$. This proves the existence of the decomposition (8). For $\lambda$ the constant coefficient of $g$ we obtain $(g^\theta)^2 = (\frac{1}{\lambda^2} \theta)\theta = \frac{1}{\lambda^2} g$. Therefore the monic polynomial $(g^\theta)^2$ is equal to $g$, showing that the irreducible factors appearing in (8) are distinct. A direct computation gives $(gg^\theta)^2 = (g^\theta)^2 = g^2g$ (Lemma 4).

Setting $f_i = h_i$ for $i \in \{1, \ldots, s\}$ and $f_{i+j} = g_jg_i^\theta$ for $j \in \{1, \ldots, r\}$ in (8) we obtain a factorization $f_1(Y)f_2(Y) \cdots f_m(Y)$ of $Y^t - \epsilon$ in $(\mathbf{F}_q)^\theta[Y] = Z(R)$ into pairwise coprime monic polynomials $f_i(Y)$ with $f_i^\theta = f_i$. □

Algorithm 1 Construction of self-dual module $\theta$-codes.

**Input** : $n$, $\mathbf{F}_q$ of characteristic $p$, $\theta \in \text{Aut}(\mathbf{F}_q)$ of order 2, $\epsilon \in \{-1, 1\}$

**Output** : the set of all generator polynomials of self-dual module $\theta$-codes of length $n$ over $\mathbf{F}_q$ which are $\theta$-cyclic if $\epsilon = 1$, $\theta$-negacyclic if $\epsilon = -1$

1: compute $s$ and $t$ such that $n = p^s \times 2 \times t$ with $t \mod p \neq 0$

2: compute a factorization of $Y^t - \epsilon = f_1(Y) \cdots f_m(Y)$ in the commutative ring $(\mathbf{F}_q)^\theta[Y] = (\mathbf{F}_q)^\theta[X^t]$ into pairwise coprime polynomials of minimal degree such that $f_i^\theta = f_i$

3: for $i \in \{1, \ldots, m\}$ do

4: compute the sets $\mathcal{H}_i = \{h_i \in \mathbf{F}_q[X; \theta] \mid h_i^2h_i = (f_i)^{p^s}(X^t)\}$ by solving the corresponding polynomial system whose unknowns are the coefficients of $h_i$. 

5: end for

6: return $\{\text{lcm}(h_1^\theta, \ldots, h_m^\theta) \mid h_i \in \mathcal{H}_i\}$

The following algorithm reduces the computation of $h \in R$ with the property $h^2h = X^{2k} - \epsilon$ (Corollary 6) to the computation in step 4 of the polynomials $h_i$ of smaller degree with the properties $h_i^\theta h_i = (f_i)^{p^s}$. The polynomial system, that has to be solved in step 4 in order to compute $h_i$, contains polynomial equations with less variables than the polynomial system which one would have to solve in order to compute $h$. The computational gain depends on $s$ and on the degrees of the polynomials $f_i$ in the factorization $Y^t - \epsilon = f_1(Y) \cdots f_m(Y)$. The correctness of the algorithm is proven in the next proposition.
Proposition 28. Let $F_q$ be a finite field, $\theta \in \text{Aut}(F_q)$ of order 2, $R = F_q[X;\theta]$ and $k = p^s \times t$ a nonzero integer with $s \in \mathbb{N}$ and $t \in \mathbb{N}$ not multiple of $p$. Let $\varepsilon \in \{-1,1\}$ and $Y^t - \varepsilon = f(Y)f_2(Y) \cdots f_m(Y) \in (F_q)[Y] = (F_q)[X^2] = Z(R)$, where $f_i(Y)$ are monic polynomials that are pairwise coprime with the property that $f_i^2 = f_i$. For $\varepsilon = 1$ (resp. $\varepsilon = -1$) and for $h \in R$ of degree $k$ the polynomial $g = h^{\theta}$ generates a self-dual $\theta$-cyclic (resp. $\theta$-negacyclic) code over $F_q$ of length $n = 2k$ if and only if there exist $h_1, \ldots, h_m \in R$ such that

1. $h_i^*h_i = (f_i)^{p^s}$,
2. $h = \text{lcm}(h_1, \ldots, h_m)$

Proof. (1) ($\Rightarrow$): (the codes obtained are self-dual) According to Corollary 6 we have to show that $h^*h = X^{2n^p} - \varepsilon$. From $h = \text{lcm}(h_1, \ldots, h_m)$ we obtain that $h = h_iq_i$ with $q_i \in R$. Lemma 4 shows that $h^* = \Theta^{\text{deg}(h_i)}(q_i^*)h_i^*$. As $h^*$ (resp. $h_i^*$) is a constant times $h^*$ (resp. $h_i^*$), there exists $q_i \in R$ such that $h^* = q_i^*h_i^*$. Therefore $h^*h = q_i^*(h_i^*h_i)q_i = q_i^*(f_i)^{p^s}q_i = q_iq_i(f_i)^{p^s}$ (because $(f_i)^{p^s} \in (F_q)[X^2]$ is central), showing that $\text{lcm}(f_1)^{p^s} \cdots (f_m)^{p^s}$ is a right divisor of $h^*h$ in $R$. To prove the claim it remains to show that

$$\text{lcm}((f_1)^{p^s} \cdots (f_m)^{p^s}) = (f_1)^{p^s} \cdots (f_m)^{p^s} = X^{n - \varepsilon}.$$  \hspace{1cm} (9)

Comparing degrees we obtain from relation (9) that $h^*h = X^{n - \varepsilon}$. In order to prove the first equality of relation (9) we first show that the least common right multiple of polynomials in $Z(R) \subset R$ coincide when viewed as polynomials either in $R$ or in the commutative polynomial ring $Z(R)$. Both $R$ and $Z(R)$ are euclidean rings and the left and right for $R$ euclidean division has a unique quotient and unique remainder. Therefore a division in $Z(R)$ is also a (left and right) division in $R$. Since the lcm can be computed in both cases using the euclidean algorithm (Ore (1933b), Section 3), they coincide in both rings. In the commutative ring $Z(R) = (F_q)[Y]$ the second equality of relation (9) is a consequence of Gauss Lemma and the claim follows.

(2) ($\Rightarrow$): (all self-dual module $\theta$-codes are obtained this way) Corollary 6 shows that if $g = h^{\theta}$ generates a self-dual $\theta$-code over $F_q$ of length $n = 2k$, then $h^*h = X^{n - \varepsilon} = ((X^2)^t - \varepsilon)^{p^s} = (Y^t - \varepsilon)^{p^s}$ (where $Y = X^2$). We noted above that the division in $Z(R)$ and $R$ coincide in $Z(R)$, so that $((f_i)^{p^s})^2 = (f_i)^{p^s}$ are pairwise coprime in $Z(R)$ and $R$. According to (Giesbrecht (1998), Theorem 4.1), we have $h^*h = \text{lcm}(h_1^*, \ldots, h_m^*)$, where $h_i^* = \text{gcd}((f_i)^{p^s}, h)$ are pairwise coprime in $R$. In particular, according to Ore (1933b), $\text{deg}([\text{lcm}(h_1^*, h_2^*)]) = \text{deg}(h_1^*) + \text{deg}(h_2^*)$ for $i \neq j$ and $\text{deg}(h^*) = \text{deg}([\text{lcm}(h_1^*)]) = \sum \text{deg}(h_i^*)$.

We now show that $h_i$ divides $(f_i)^{p^s}$ and $h$ on the left:

- Let $d_i$ be the degree of $(f_i)^{p^s}$ and $d_i$ be the degree of $h_i$. Since $f_i \in Z(R)$, $d_i$ is even. Applying Lemma 4 to $(f_i)^{p^s} = q_ih_i^*$ we obtain $(f_i)^{p^s} = \Theta^{d_i}(h_i^*)q_i = \Theta^{d_i}(\Theta^{d_i}(h_i^*)q_i) = \Theta^{d_i}(h_i^*)q_i = \Theta^{d_i}(h_i^*)q_i = h_i^*q_i$ ($d_i$ is even and $\theta^2 = id$). So $h_i$ divides on the left $((f_i)^{p^s})^*$, As $\theta^2 = id$ is central, it is equal to $(f_i)^{p^s}$ times a constant, so $h_i$ divides on the left $((f_i)^{p^s})^* = (f_i)^{p^s}$.

- Since $h_i^*$ divides $h^*$ on the right, we also have $h^* = p_ih_i^*$. Using Lemma 4, we obtain $\Theta^k(h_i) = h_i^* = \Theta^{k-d_i}(h_i^*)p_i^*$. Therefore $\Theta^k(h_i) = \Theta^{k-d_i}(\Theta^{d_i}(h_i^*))p_i^* = \Theta^k(h_i)p_i^*$.

Since $\Theta$ is a morphism of rings, $h_i$ divides $h$ on the left.
Since $h_i^5$ divides $h^5$ on the right and $h_i$ divides $h$ on the left, we obtain $h^3 h = \tilde{g} h_i^3 h_i$. Since two factors of a decomposition of the central polynomial $h^5 h = \tilde{g} h_i^3 h_i$, into two factors commute, $h_i^3 h_i$ divides $h^5 h = X^n - \varepsilon$ on the right. According to Theorem 4.1 of Giesbrecht (1998), $h_i^3 h_i = \operatorname{lcm}(\gcd(h_i^3 h_i, (f_i)^{p^s})), j = 1, \ldots, m$). We now note that both $h_i^3$ and $h_i$ divide the central polynomial $(f_i)^{p^s}$, so that the product $h_i^3 h_i$ divides $((f_i)^{p^s})^2$. For $j \neq i$ we obtain $\gcd(h_i^3 h_i, (f_j)^{p^s}) = 1$ and $h_i^3 h_i = \gcd(h_i^3 h_i, (f_j)^{p^s})$. In particular, $h_i^3 h_i$ divides $(f_i)^{p^s}$.

For $i \in \{1, \ldots, m\}$ the polynomials $(f_i)^{p^s}$ are pairwise coprime, showing that their divisors $h_i^3 h_i$ are also pairwise coprime. Therefore

$$\operatorname{deg}(\operatorname{lcm}(h_i^3 h_i)) = \sum_{i=1}^{m} \operatorname{deg}(h_i^3 h_i) = 2 \sum_{i=1}^{m} \operatorname{deg}(h_i^3) = 2 \operatorname{deg}(h^3) = \sum_{i=1}^{m} \operatorname{deg}((f_i)^{p^s}).$$

From $\sum_{i=1}^{m} \operatorname{deg}(h_i^3 h_i) = \sum_{i=1}^{m} \operatorname{deg}((f_i)^{p^s})$ and the fact that $h_i^3 h_i$ divides $(f_i)^{p^s}$, we obtain $h_i^3 h_i = (f_i)^{p^s}$. As $h_i$ divides $h$ on the left, $\operatorname{lcm}(h_i, i = 1, \ldots, m)$ also divides $h$ on the left. Since $\gcd(h_i^3, h_i) = 1$ implies $\gcd(h_i, h_j) = 1$ we have $\operatorname{deg}(\operatorname{lcm}(h_i, i = 1, \ldots, m)) = \sum \operatorname{deg}(h_i) = \operatorname{deg}(h)$. Therefore $h = \operatorname{lcm}(h_i, i = 1, \ldots, m).$

\[\Box\]

**Example 29.** Let $F_4 = F_2(a), \theta$ the Frobenius automorphism $a \mapsto a^2$ and $R = F_4[X; \theta]$. In $F_2[Y] = Z(R)$ (where $Y = X^2$), we have $Y^{39} - 1 = f_1(Y) f_2(Y) f_3(Y) f_4(Y)$ where:

- $f_1(Y) = Y + 1$
- $f_2(Y) = Y^2 + Y + 1$
- $f_3(Y) = Y^{12} + Y^{11} + Y^{10} + Y^9 + Y^8 + Y^7 + Y^6 + Y^5 + Y^4 + Y^3 + Y^2 + Y + 1$
- $f_4(Y) = (Y^{12} + Y^{11} + Y^{10} + Y^9 + Y^8 + Y^7 + Y^6 + Y^5 + Y^4 + Y^3 + Y^2 + Y + 1)$

The polynomials $f_i$ are pairwise coprime polynomials satisfying $f_i^5 = f_i$ ($i \in \{1, \ldots, 4\}$). The computational problem is therefore reduced from degree 39 to degree at most 12 which is now in reach of a Gröbner basis computation and allows to compute the four sets $\mathcal{H}_i$. For all $h_i \in \mathcal{H}_i$ we computed all the codes generated by $g = h^3 = \operatorname{lcm}(h_1^3, h_2^3, h_3^3, h_4^3)$. For the skew polynomials

- $h_1 = X + 1$
- $h_2 = X^2 + X + 1$
- $h_3 = X^{12} + a X^{11} + X^{10} + X^8 + a X^6 + a^2 X^4 a^2 X^2 + X + a^2$
- $h_4 = X^{24} + a^2 X^{23} + X^{22} + a X^{20} + X^{19} + a^2 X^{18} + X^{17} + a X^{15} + X^{13} + a^2 X^{12}$
  + $a^2 X^{11} + a X^9 + a^2 X^7 + a^2 X^6 + a^2 X^5 + a^2 X^4 + a X^2 + X + a$

14
we obtain the skew polynomial
\[
g = X^{39} + a^2X^{38} + a^2X^{37} + X^{36} + a^2X^{34} + aX^{33} + aX^{32} + a^2X^{31} + aX^{30} + a^2X^{29} + aX^{26} + aX^{27} + a^2X^{26} + a^2X^{25} + X^{24} + a^2X^{22} + X^{20} + X^{19} + a^2X^{17} + X^{15} + a^2X^{14} + a^2X^{13} + aX^{12} + a^2X^{11} + a^2X^{10} + aX^9 + a^2X^8 + aX^7 + aX^6 + a^2X^5 + X^3 + a^2X^2 + a^2X + 1
\]
which generates a \([78, 39, 19]_4\) self-dual code and therefore improves the best previously known minimal distance from Table 5 in Grassl and Gulliver (2009). Note that the generator matrix \(G_9\) of this code can be easily obtained from the generator polynomial using the formula (1), so that it is straightforward to construct this code and verify in Magma (cf. Bosma et al. (1997)) that its minimum distance is equal to 19.

**Example 30.** Let \(F_9 = F_3(a)\) where \(a^2 - a - 1 = 0, \theta\) the Frobenius automorphism \(\alpha \mapsto \alpha^2\) and \(R = F_9[X; \theta]\). In \(F_3[Y] = Z(R)\) (where \(Y = X^2\)), we have \(Y^{26} + 1 = f_1(Y)f_2(Y)f_3(Y)\) where:

\[
f_1(Y) = Y^2 + 1
\]

\[
f_2(Y) = (Y^6 + 2Y^2 + 1)(Y^6 + Y^4 + 2Y^2 + 1) = Y^{12} + 2Y^{10} + 2Y^8 + 2Y^4 + 2Y^2 + 1
\]

\[
f_3(Y) = (Y^6 + 2Y^4 + 1)(Y^6 + 2Y^4 + Y^2 + 1) = Y^{12} + 2Y^8 + Y^6 + 2Y^4 + 1.
\]
The polynomials \(f_i\) are pairwise coprime polynomials satisfying \(f_i^3 = f_i\) \((i \in \{1, \ldots, 3\})\).

The computational problem is therefore reduced from degree 26 to degree at most 12 which is now in reach of a Gröbner basis computation and allows us to compute the three sets \(\mathcal{H}_i\). For all \(h_i \in \mathcal{H}_i\) we computed the codes generated by \(g = h^i = \text{lcm}(h_1^i, h_2^i, h_3^i)\).

For the skew polynomials
\[
h_1 = X^2 + 2X + 2
\]
\[
h_2 = X^{12} + a^8X^{11} + a^5X^{10} + aX^9 + a^5X^8 + 2X^6 + a^7X^4 + a^7X^3 + a^7X^2 + a^3X + 1
\]
\[
h_3 = X^{12} + aX^{11} + X^{10} + X^8 + aX^6 + a^2X^4 + a^2X^2 + X + a^2
\]
we obtain the skew polynomial
\[
g = X^{26} + 2X^{25} + 2X^{24} + X^{22} + aX^{21} + 2X^{20} + X^{19} + aX^{18} + a^5X^{16} + 2X^{14} + X^{13} + aX^{12} + a^8X^{10} + a^7X^8 + X^7 + X^6 + a^5X^5 + 2X^4 + X^2 + 2X + 2
\]
which generates a \([52, 26]_9\) self-dual code. Note that the generator matrix of this code can be easily obtained from the generator polynomial using the formula (1), so that it is straightforward to construct this code. We verify in Magma (cf. Bosma et al. (1997)) that its minimum distance is 17, which improves the previous best known minimum distance for self-dual codes of this length (table 14 of Grassl and Gulliver (2009)).

The following example illustrates the fact that polynomials \(f_i \in (F_q)^\theta[Y]\) with the property \(f_i^3 = f_i\) can appear at different length \(n\) and that this previous computation can be used again.

**Example 31.** Let \(F_{49} = F_7(a)\) where \(a^2 - a + 3 = 0, \theta\) the Frobenius automorphism \(\alpha \mapsto \alpha^2\) and \(R = F_{49}[X; \theta]\).
The polynomial $Y^4 + 1$ factorizes over $\mathbb{F}_7$ into the product of two irreducible polynomials as $Y^4 + 1 = (Y^2 + 3Y + 1)(Y^2 + 4Y + 1)$, where $(Y^2 + 3Y + 1)^3 = Y^2 + 3Y + 1$, $(Y^2 + 4Y + 1)^2 = Y^2 + 4Y + 1$. The sets $\mathcal{H}_1 = \{ h \in \mathbb{F}_{49}[X;\theta], h^5 h = X^4 + 3X^2 + 1 \}$ and $\mathcal{H}_2 = \{ h \in \mathbb{F}_{49}[X;\theta], h^5 h = X^4 + 4X^2 + 1 \}$ are

\[
\mathcal{H}_1 = \{ X^2 + 4X + 6, X^2 + a^6 X + a^{10}, X^2 + a^{22} X + a^{12}, X^2 + 3X + 6, X^2 + a^{34} X + a^{36}, X^2 + a^{42}, X^2 + a^{46} X + a^{12} \}
\]

\[
\mathcal{H}_2 = \{ X^2 + a^{21} X + a^6, X^2 + a^{45} X + a^6, X^2 + a^{18}, X^2 + X + 6, X^2 + a^{50}, X^2 + a^3 X + a^{42}, X^2 + a^{27} X + a^{42}, X^2 + 6X + 6 \}
\]

and the polynomials $g = \text{lcm}(h_1^5, h_2^5)$ (where $h_i \in \mathcal{H}_i$) generate all the 64 self-dual $\theta$-negacyclic codes $[8,4]$ over $\mathbb{F}_{49}$, among which 20 reach the Singleton Bound 5. The generator polynomial $g$ of four of those codes are belong to $\mathbb{F}_7[X]$ and are therefore negacyclic, i.e. $g$ divides $X^8 + 1$ in $\mathbb{F}_7[X]$. Since codes over $\mathbb{F}_{49}$ are not well classified, we use Theorem 3.4 of Mouaha (1992) to construct self-dual codes over $\mathbb{F}_7$ as 7-ary images $d_B(C)$ of self-dual codes $C$ over $\mathbb{F}_{7^2}$ using the symmetric basis $B = (1, a^3)$. Many good codes over $\mathbb{F}_7^2$ reduce poorly to $\mathbb{F}_p$, but in the present case we obtain four $[16,8,7]$ self-dual codes over $\mathbb{F}_7$ whose generator matrices are

\[
\begin{pmatrix}
5 & 6 & 5 & 2 & 4 & 4 & 4 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
6 & 6 & 2 & 3 & 4 & 0 & 1 & 3 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 6 & 1 & 3 & 5 & 0 & 3 & 3 & 6 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 5 & 5 & 3 & 4 & 6 & 4 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 5 & 6 & 5 & 2 & 4 & 4 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 6 & 6 & 2 & 3 & 4 & 0 & 1 & 3 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 6 & 1 & 3 & 5 & 0 & 3 & 3 & 6 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 5 & 5 & 3 & 4 & 6 & 4 & 0 & 1
\end{pmatrix}
\begin{pmatrix}
1 & 6 & 4 & 3 & 5 & 1 & 3 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
6 & 2 & 3 & 1 & 1 & 4 & 0 & 3 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 2 & 1 & 1 & 4 & 4 & 6 & 3 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 4 & 4 & 6 & 5 & 0 & 3 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 6 & 4 & 3 & 5 & 1 & 3 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 6 & 2 & 3 & 1 & 1 & 4 & 0 & 3 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 2 & 1 & 1 & 4 & 4 & 6 & 3 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 4 & 4 & 6 & 5 & 0 & 3 & 0 & 1
\end{pmatrix}
\]

\[
\begin{pmatrix}
2 & 1 & 2 & 0 & 1 & 5 & 3 & 5 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 2 & 5 & 3 & 5 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 6 & 2 & 0 & 3 & 2 & 5 & 2 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 6 & 2 & 0 & 2 & 1 & 2 & 3 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 2 & 1 & 2 & 0 & 1 & 5 & 3 & 5 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 2 & 5 & 3 & 5 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 6 & 2 & 0 & 3 & 2 & 5 & 2 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 6 & 2 & 0 & 2 & 2 & 1 & 2 & 3 & 0
\end{pmatrix}
\begin{pmatrix}
6 & 1 & 3 & 3 & 0 & 2 & 3 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 5 & 3 & 0 & 2 & 5 & 1 & 2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 5 & 6 & 0 & 4 & 5 & 5 & 2 & 6 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 6 & 6 & 4 & 3 & 5 & 0 & 6 & 3 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 3 & 3 & 0 & 2 & 3 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 5 & 3 & 0 & 2 & 5 & 1 & 2 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 5 & 6 & 0 & 4 & 5 & 5 & 2 & 6 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 6 & 6 & 4 & 3 & 5 & 0 & 6 & 3 & 0
\end{pmatrix}
\]
The weight enumerators of the resulting self-dual codes of length 16 defined over $\mathbb{F}_7$ correspond to four of the five weight enumerators of the self-dual quasi-twisted codes constructed in Gulliver et al. (2007).

- The two polynomials $Y^2 + 3Y + 1$ and $Y^2 + 4Y + 1$ used above also appear in the factorization of $Y^{12} + 1$ into irreducible factors over $\mathbb{F}_7$:


Since $(Y^2 + 2Y + 2)^\sharp = Y^2 + Y + 4$ and $(Y^2 + 5Y + 2)^\sharp = Y^2 + 6Y + 4$, the minimal factorization of $Y^{12} + 1$ into a product of pairwise coprime polynomials $f_i$ over $\mathbb{F}_7$ such that $f_i = f_i^\sharp$ is

$$(Y^2 + 3Y + 1)(Y^2 + 4Y + 1)(Y^4 + 3Y^3 + Y^2 + 3Y + 1)(Y^4 + 4Y^3 + Y^2 + 4Y + 1).$$

In order to obtain all self-dual module $\theta$ codes we only need to construct the two additional sets $\mathcal{H}_3 = \{ h \in \mathbb{F}_{49}[X;\theta], h^5h = X^8 + 3X^6 + X^4 + 3X^2 + 1 \}$ and $\mathcal{H}_4 = \{ h \in \mathbb{F}_{49}[X;\theta], h^3h = X^8 + 4X^6 + X^4 + 4X^2 + 1 \}$. The generator polynomials of the 173056 self-dual $\theta$-negacyclic codes over $\mathbb{F}_{49}$ with length 24 are now given by

$$g = \text{lcm}(h_1^\sharp, h_2^\sharp, h_3^\sharp, h_4^\sharp)$$

where $h_i$ belongs to $\mathcal{H}_i$. The best codes within this set reach the distance 12 (one less than the Singleton bound). The polynomial

$$g = X^{12} + a^{42}X^{11} + a^{33}X^9 + a^2X^8 + a^{13}X^7 + a^6X^6 + a^{31}X^5 + a^{26}X^4 + a^{27}X^3 + a^{44}X^2 + a^{42}X + a^{12}$$

is an example of a generator polynomial for a $[24, 12, 12]_{49}$ self-dual code. The generator matrix $G_{\theta, 24}$ of this code can be easily obtained from the generator polynomial using the formula (1), so that it is straightforward to construct this code and verify in Magma (cf. Bosma et al. (1997)) that its minimum distance is equal to 12.

**Acknowledgements**

We thank the referees for many helpful comments.

**References**


URL http://dx.doi.org/10.3934/amc.2007.1.223


URL http://dx.doi.org/10.1007/BF01294839
