Self-dual skew codes and factorization of skew polynomials

Delphine Boucher, Félix Ulmer

Self-dual skew codes and factorization of skew polynomials

D. Boucher and F. Ulmer*

July 19, 2012

Abstract

In previous work the authors generalized cyclic codes to the noncommutative polynomial setting and used this approach to construct new self-dual codes over $\mathbb{F}_4$. According to this previous result, such a self-dual code must be θ-constacyclic, i.e. the generator polynomial is a right divisor of some noncommutative polynomial $X^n - a$. The first result of the paper is that such a self-dual code must be θ-cyclic or θ-negacyclic, i.e. $a = \pm 1$. For codes of length 2^s the noncommutative polynomial approach produced surprisingly poor results. We give an explanation of the length 2^s phenomena by showing that in this case the generating skew polynomial has some unique factorization properties. We also construct self-dual skew codes using least common left multiples of noncommutative polynomials and use this to obtain a new $[78, 39, 19]_4$ self-dual code.

1 Introduction

In [2], self-dual skew codes with good minimum distances were obtained. However, like for cyclic codes ([7]), there is a phenomena in lengths which are a power of 2. For the lengths $4, 8, 16, 32$ and 64 there are only three self-dual skew codes, while otherwise there is a large number of self-dual codes

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

which increases with the length (cf. [3]). The authors conjectured in [4] that for any s there are only three self-dual skew codes of length 2^s.

The aim of this paper is to use the factorization of skew polynomials for studying self-dual skew codes. This allows to prove the above conjecture and to give an iterative construction of self-dual skew codes using least common multiples.

The material is organized as follows.

The section 2 is devoted to some generalities about skew codes ([2]) and self-dual skew codes ([4]).

In section 3 it is proven that for all nonnegative s, there are $2^{2^{s-1}+1}-1$ θ-cyclic codes of length 2^s and dimension 2^{s-1} over $\mathbb{F}_4$ but that among them only three are self-dual for $s > 1$. This gives an answer to Conjecture 1 of [4].

In section 4, we give a construction of self-dual module θ-codes which is based on the factorization and least common right multiples (lcrm) of skew polynomials. An example of a $[78, 39, 19]_4$ self-dual code is given.

2 Self-dual skew codes over a finite field

Starting from the finite field $\mathbb{F}_q$ and an automorphism θ of $\mathbb{F}_q$, a ring structure is defined in [8] on the set:

$$R = \mathbb{F}_q[X;\theta] \;=\; \{a_n X^n + \ldots + a_1 X + a_0 \,|\, a_i \in \mathbb{F}_q \text{ and } n \in \mathbb{N}\}\,.$$

The addition in R is defined to be the usual addition of polynomials and the multiplication is defined by the basic rule $X \cdot a = \theta(a)\, X$ $(a \in \mathbb{F}_q)$ and extended to all elements of R by associativity and distributivity. The ring R is called a skew polynomial ring and its elements are skew polynomials. It is a left and right euclidean ring whose left and right ideals are principal. Left and right gcd (gcrd) and lcm (lclm) exist in R and can be computed using the left and right euclidean algorithm ([5], Section 2).

Following [3] we define linear codes using the skew polynomial ring R.

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

Let us now recall that the **euclidean dual** or **dual** of a linear code C of length n over $\mathbb{F}_q$ can be defined with the **euclidean scalar product** :

$$\forall x, y \in \mathbb{F}_q^n, < x, y >= \sum_{i=1}^{n} x_i y_i$$

as $C^{\perp} = \{x \in \mathbb{F}_q^n, \forall y \in C, < x, y >= 0\}$. A linear code C over $\mathbb{F}_q$ is **euclidean self-dual** or **self-dual** if $C = C^{\perp}$.

To characterize self-dual module θ-codes, we need to define the skew reciprocal polynomial of a skew polynomial (definition 3 of [4]) and also the left monic skew reciprocal polynomial.

Definition 2 *The* **skew reciprocal polynomial** *of* $h = \sum_{i=0}^{m} h_i \, X^i \in R$ *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* $h^{*_\ell} := (1/\theta^m(h_0)) \cdot h^*$.

Since θ is an automorphism, the map $*\colon R \to R$ 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, then $g = h^{*_\ell}$.

In order to describe some properties of the skew reciprocal polynomial we need the following morphism of rings already used in [4]:

$$\begin{array}{rcl} \Theta\colon R & \to & R \\ \sum_{i=0}^{n} a_i X^i & \mapsto & \sum_{i=0}^{n} \theta(a_i) X^i \end{array}$$

Lemma 1 ([4]) *Let* $f \in R$ *be a skew polynomial of degree* n *such that* $f = hg$, *where* h *and* g *are skew polynomials of degrees* k *and* $n - k$. *Then*

1. $f^* = \Theta^k(g^*)h^*$
2. $(f^*)^* = \Theta^n(f)$.

In [4], it is established that a module θ-code which is self-dual is necessarily θ-constacyclic (Corollary 1 of [4]). In this case its generator polynomial g divides on the right $X^n - a$ for some a in $\mathbb{F}_q \setminus \{0\}$ where $n = 2k$ is the length of the code. Furthermore the dual of $(g)_n^{\theta,a}$ is generated by the polynomial h^{*_ℓ} where h is defined by the two equivalent following equalities :

$$\Theta^n(h) \cdot g = X^n - a \Leftrightarrow g \cdot h = X^n - \theta^{-k}(a).$$

The following proposition improves Corollary 1 of [4] :

Proposition 1 *A self-dual module θ-code is either θ-cyclic or θ-negacyclic.*

Proof: If $C = (g)_n^\theta$ is a self-dual module θ-code, then C is necessarily θ-constacyclic ([4], Corollary 1). Let a be in $\mathbb{F}_q \setminus \{0\}$ such that g divides $X^n - a$ on the right in R. Consider $h \in R$ such that $\Theta^n(h) \cdot g = X^n - a$. From Lemma 1, we obtain $\frac{-1}{a}\Theta^{k-n}(g^*)h^* = X^n - \frac{1}{a}$, showing that $h^{*\ell} = \frac{1}{\theta^k(h_0)}h^*$ divides $X^n - \frac{1}{a}$ on the right. Since $C = (g)_n^\theta$ is a self-dual module θ-code we must have $g = h^{*\ell}$ ([4], Theorem 1). So g divides on the right the polynomial $(X^n - a) - (X^n - \frac{1}{a}) = a - \frac{1}{a}$ of degree less than g. Therefore $a^2 = 1$.

□

Combining this result with ([4], Theorem 1) we obtain:

Corollary 1 *A module θ-code $(g)_{2k}^\theta$ with $g \in \mathbb{F}_q[X;\theta]$ of degree k is self-dual if and only if $g = h^{*\ell}$ and h satisfies*

$$h^{*\ell}h = X^{2k} - \varepsilon \text{ with } \varepsilon \in \{-1, 1\}. \tag{1}$$

3 Self-dual module θ-codes of length 2^s 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 θ. The properties of the ring R used in this paper can be found in [5, 6]. The **center** $Z(R)$ **of** R is is the commutative polynomial subring $(\mathbb{F}_q)^\theta[X^{|\theta|}]$ in the variable $Y = X^{|\theta|}$ where $|\theta|$ is the order of θ. We denote $Z(R)$ also $(\mathbb{F}_q)^\theta[Y]$. Following [6] we call an element of a ring bounded if the left ideal it generates contains a two-sided ideal. In the ring R all elements are bounded. The monic generator f of the maximal two-sided ideal contained in Rf is **the bound of** f. The generators of two-sided ideals in R are the elements of the form $X^m f$ where $f \in Z(R)$. The two-sided ideals are closed under multiplication, a bound f is an **irreducible bound** if the two-sided ideal (f) is maximal. A bound f with a nonzero constant term belongs to $Z(R) = (\mathbb{F}_q)^\theta[Y]$ and is an irreducible bound if and only if $f(Y) \in (\mathbb{F}_q)^\theta[Y]$ is an irreducible (commutative) polynomial ([6], Chap. 3, Th. 12).

Definition 3 *([6], 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.*

[1] In [6] the term decomposable is used

$h = lclm(h_1, h_2)$ *where* $h_i \in R$ *and* $\deg(h_i) < \deg(h)$. *The polynomial* $h \in R$ *is* **lclm-indecomposable** *if* h *is not lclm-decomposable.*

Theorem 1 *([6], Chap. 3, Th. 5 or [5], Th. 1.3) 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.

Example 1 *For* $\mathbb{F}_4 = \mathbb{F}_2(a)$ *where* $a^2 + a + 1 = 0$ *and* θ *the Frobenius automorphism* $a \mapsto a^2$ *we have in* $\mathbb{F}_4[X;\theta]$ *that* $(X + a)(X + 1) = X^2 + a^2X + a \neq X^2 + aX + a = (X + 1)(X + a)$. *Two factors of a central polynomial always commute:*

$$X^2 + 1 = (X + a^2)(X + a) = (X + a)(X + a^2) = (X + 1)(X + 1). \quad (2)$$

In a nonunique factorization ring R *some factorizations can still be unique. As we will see, in* $\mathbb{F}_4[X;\theta]$ *the polynomials* $(X+a)(X+a)$, $(X+a)(X+1)$, $(X+1)(X+a)$, $(X+a^2)(X+a^2)$, $(X+a^2)(X+1)$ *and* $(X+1)(X+a^2)$ *are lclm-indecomposable, i.e. their factorization into monic irreducible polynomials is unique. In* $\mathbb{F}_4[X;\theta]$ *the bounds* X^2 *and* $X^2 + 1$ *are irreducible bounds.*

The next theorem characterizes the skew polynomials of R which do have a unique factorization into irreducible monic skew polynomials :

Theorem 2 *([6], Chap. 3, Th. 21 and 24) Let* $R = \mathbb{F}_q[X;\theta]$ *and* $m \in \mathbb{N}^*$.

1. *If* $h_1, h_2, \ldots, h_m$ *are monic irreducible polynomials of* R *having the same irreducible bound* $f \in R$, *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.

2. *An lclm-indecomposable monic polynomial in* R *has a unique factorization into irreducible monic polynomials.*

Lemma 2 *Let* $R = \mathbb{F}_q[X;\theta]$. *The lclm-decomposable product* $h_1 h_2$ *of two irreducible polynomials* h_1 *and* h_2 *having both the same irreducible bound* $f \in R$ *is equal to* $f \in R$.

Proof: Otherwise, since the bound of a product divides the products of the bounds ([6], Chap. 3, Th. 12), the bound of h_1h_2 is f^2 and h_1h_2 would be lclm-indecomposable by the above theorem. □

Definition 4 *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 factor g of f corresponds a unique $\overline{g} \in \mathbb{F}_q[X;\theta]$ such that $\overline{g}g = f$ called the* **complement** *of g (for f). The number of distinct irreducible factors $g \in \mathbb{F}_q[X;\theta]$ of f is the* **capacity** *κ of f.*

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

$$\tilde{a} = \lambda/a \quad \text{and} \quad \theta(a) = -\lambda/a \tag{3}$$

In particular $\theta^2(a) = a$. From the previous example we see that the capacity of the central polynomial $X^2 + 1 \in \mathbb{F}_4[X;\theta]$ is $\kappa = 3$.

In the following we will be interested in the case where, as in the previous example, the irreducible factors in R of an irreducible bound f, which is reducible in R, are of degree $\deg(f)/2$.

Lemma 3 *Consider $R = \mathbb{F}_q[X;\theta]$ with $\theta^2 = id$.*

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. *Consider a product $h = h_1 \cdots h_m$ of irreducible monic polynomials having all the same irreducible bound $f \in Z(R)$ which is reducible in R. The following assertions are equivalent :*

   (i) h is lclm-decomposable;

   (ii) h is divisible by f;

   (iii) there exists i in $\{1, \ldots, m-1\}$ such that h_{i+1} is the complement of h_i (for f).

Proof:

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

   If l is even, then $G_l = \sum_{i+j=l} a_i(-1)^{l-i}\theta(a_j) = \sum_{i+j=l} a_i(-1)^i\theta(a_j)$. 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

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

   So G belongs to $(\mathbb{F}_q)^\theta[X^2] = Z(R)$.

2. The irreducible factors of an irreducible bound f are all similar and therefore of the same degree d ([6], Chap. 3, Corollary of Th. 20 or Theorem 4.3 of [5]). The first assertion shows that in our situation this degree d is equal to $deg(f)/2$.

   The implications $(iii) \Rightarrow (ii) \Rightarrow (i)$ are straightforward.

   To prove $(i) \Rightarrow (iii)$, we proceed by induction on m. According to Lemma 2, it is true for $m = 2$. Suppose $m > 2$ and that the result holds for $i < m$. Let $h = h_1 \cdots h_m$ be lclm-decomposable where h_i are irreducible 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 $\text{lclm}(g_m, h_m) = \tilde{h}_{m-1}h_m$ divides on the right $h = h_1 \cdots h_m = \tilde{h}_1 \cdots \tilde{h}_{m-1}h_m$. So $h_1 \cdots h_{m-1} = \tilde{h}_1 \cdots \tilde{h}_{m-1}$. 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 $\text{lclm}(g_m, h_m) = h_{m-1}h_m$ is lclm-decomposable; so according to Lemma 2, $h_{m-1}h_m = f$.

□

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

Proof: The irreducible factors of f^m and therefore also of its right factor g are all of degree $\deg(f)/2$. If $g = g_1 g_2 \cdots g_m$ is a factorization into irreducible, and $\overline{g_i}$ the complement of g_i, then $f^m = \overline{g_m} \cdots \overline{g_2}\,\overline{g_1} g_1 g_2 \cdots g_m$. Therefore g is always a divisor of f^m and that we only need to count the different polynomials $g = g_1 g_2 \cdots g_m$.

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. If g is not divisible by f then according to Lemma 3, for all i, g_{i+1} is not the complement of g_i. There are κ 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. □

Corollary 2 *Let s be a nonnegative integer. The number of module θ-cyclic codes over $\mathbb{F}_4$ with length 2^s and dimension 2^{s-1} is $2^{2^{s-1}+1} - 1$.*

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 $2^{2^{s-1}+1} - 1$ monic right factors of degree 2^{s-1} in $\mathbb{F}_4[X;\theta]$. □

Proposition 3 *Let $R = \mathbb{F}_q[X;\theta]$ with $\theta^2 = id$, $1 \leq m \in \mathbb{N}$, $f \in Z(R)$ 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 lclm-indecomposable and $f^m = h_1 \cdots h_{m-1} h_m g_m g_{m-1} \cdots g_1$, then h_i is the complement of g_i.*

Proof: We proceed by induction on m. If $m = 1$ the result is trivial. Suppose that the result holds for $i < m$.

1. If h_m is the complement of g_m, then we can divide both sides 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 lclm-indecomposable, we obtain the result by induction.

2. Otherwise $h_1 \cdots h_{m-1} h_m$ is divisible by f. After simplification we obtain

   $\left(h'_1 \cdots h'_{m-2} h'_{m-3} g_m\right)(g_{m-1} \cdots g_1) = f^{m-1}$. Applying the induction hypothesis we obtain the contradiction that g_m is the complement of g_{m-1} and therefore that f divides $g_m \cdots g_1$. Since $g_{m-1} \cdots g_1$ is lclm-indecomposable, the above lemma shows that this case is not possible.

□

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. The main 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 4 *Consider* $0 < m \in \mathbb{N}$ *and* $\alpha_1, \alpha_2, \ldots, \alpha_m$ *in* $\mathbb{F}_q \setminus \{0\}$. *For* $g = (X+\alpha_1)(X+\alpha_2)\cdots(X+\alpha_m) \in \mathbb{F}_q[X;\theta]$ *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^{*_ℓ} *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 1 shows

$((X+\alpha_1)\cdots(X+\alpha_m))^* = \theta^{m-1}\left((X+\alpha_m)^*\right)\left((X+\alpha_1)\cdots(X+\alpha_{m-1})\right)^*$.
By induction we only need to express $h = \theta^m\left((X+\alpha_m)^*\right)\theta^{m-1}(\alpha_1 \cdots \alpha_{m-1})$ as a product of a constant times a monic linear polynomial. By direct computation we obtain

$$\begin{aligned} h &= \theta^m(\alpha_m)\left(X + \frac{1}{\theta(\alpha_m)}\right)\theta^{m-1}(\alpha_1 \cdots \alpha_{m-1}) \\ &= \theta^m(\alpha_1 \cdots \alpha_m)\left(X + \frac{\theta^{m-1}(\alpha_1 \cdots \alpha_{m-1})}{\theta^m(\alpha_1 \cdots \alpha_m)}\right). \end{aligned}$$

The claim now follows by induction. □

Proposition 4 *Consider* $\mathbb{F}_4 = \mathbb{F}_2(a)$, θ *the Frobenius automorphism* $a \mapsto a^2$ *and* $h \in \mathbb{F}_4[X;\theta]$ *to be monic of degree* $m \in \mathbb{N}$. *Then* $h^{*_\ell} h = (X^2+1)^m$ *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 $h^{*_\ell}h = (X^2+1)^m$. Let us assume that m is even and consider $h = (X+1)^{m-1}(X+u)$ with $u \in \mathbb{F}_4 \setminus \{0\}$. Then $h^* = \Theta((X+u)^*)(X+1)^{m-1} = u(X+u^2)(X+1)^{m-1}$, which gives $h^{*_\ell} = (X+u^2)(X+1)^{m-1}$ and $hh^{*_\ell} = (X^2+1)^m$. Furthermore this product commutes because $(X^2+1)^m$ is central.
($\Rightarrow$): The polynomial h is of the form $(X+\alpha_1)\cdots(X+\alpha_m)$. We will show by induction that we can choose $\alpha_1 = \cdots = \alpha_m = 1$ for m odd and $\alpha_1 = \cdots = \alpha_{m-1} = 1$ for m even. This will show that h must be one of the above polynomials and prove the claim.

1. For $m = 1$ we get from the lemma that $(X + 1/\theta(\alpha_1))\,(X+\alpha_1) = X^2+1$ or that $X + 1/\theta(\alpha_1)$ is the complement of $X+\alpha_1$. Using formula (3) we obtain $1/\theta(\alpha_1) = 1/\alpha_1$ and $\theta(\alpha_1) = 1/\alpha_1$. Therefore $\alpha_1^2 + 1 = (\alpha_1+1)^2 = 0$ and $\alpha_1 = 1$.

2. For $m = 2$. If $h = (X+\alpha_1)(X+\alpha_2)$ is lclm-decomposable, then h is divisible and therefore equal to to $X^2+1 = (X+1)(X+1)$. If h is lclm-indecomposable, then combining proposition 3 and the previous lemma we obtain that $X + 1/\theta(\alpha_1)$ is the complement of $X+\alpha_1$. Like in the case $m = 1$ this implies that $\alpha_{m-1} = 1$.

3. Suppose $m > 2$ and that the result holds for $i < m$. If X^2+1 divides h, then $h = q(X^2+1)$. Lemma 1 shows that $h^{*_\ell}h = (X^2+1)q^{*_\ell}q(X^2+1)$. Therefore $q^{*_\ell}q = (X^2+1)^{m-2}$ and we obtain the result for q by induction, which gives also the result for $h = (X^2+1)q$. Otherwise $h = (X+\alpha_1)\cdots(X+\alpha_m)$ is lclm-indecomposable (Lemma 3). Combining proposition 3 and the previous lemma we obtain that $X+\theta^{i-1}(\alpha_1\cdots\alpha_{i-1})/\theta^i(\alpha_1\cdots\alpha_i)$ is the complement of $X+\alpha_i$. Dividing $(X^2+1)^m$ on the right by $X+\alpha_m$ and on the left by its complement, we obtain the result by induction for $\alpha_1, \ldots, \alpha_{m-1}$. If m is even we get $\alpha_1 = \ldots = \alpha_{m-1} = 1$ and the result follows. If m is odd we get $\alpha_1 = \ldots = \alpha_{m-2} = 1$. Using $\alpha_1\alpha_2\cdots\alpha_{m-2} = 1$ we get from the above formula that $X + 1/\theta(\alpha_{m-1})$ is the complement of $X+\alpha_{m-1}$. Like in the case $m = 1$ this implies that $\alpha_{m-1} = 1$ and completes the proof.

□

This shows that for any integer $s \geq 1$, from the $2^{2^{s-1}+1} - 1$ θ-cyclic codes over $\mathbb{F}_4$ of length 2^s, only 3 are self-dual and proves Conjecture 1 of [4] :

Corollary 3 *Consider $\mathbb{F}_4 = \mathbb{F}_2(a)$, θ the Frobenius automorphism $a \mapsto a^2$, $s > 1$ an integer and $g \in \mathbb{F}_4[X;\theta]$ monic of degree 2^{s-1}. The code $(g)^\theta_{2^s}$ is self-dual if and only if,*

$$g = (X+u)(X+1)^{2^{s-1}-1},\ u \in \{1, a, a^2\}.$$

Proof: The code $(g)^\theta_{2^s}$ is self-dual if and only if $g = h^{*\ell}$ with $h^{*\ell}h = X^{2^s} - 1$. According to the previous proposition applied with $m = 2^{s-1}$, one gets $h = (X+1)^{2^{s-1}-1}(X+u)$ with $u \in \{1, a, a^2\}$ so according to Lemma 1, $h^* = \Theta(1+u^2X)(X+1)^{2^{s-1}-1}$ and $g = h^{*\ell} = (X+u^2)(X+1)^{2^{s-1}-1}$. □

4 Construction of self-dual θ-codes with $\theta^2 = id$

In [7] a characterization of the generator polynomials of (classical) self-dual cyclic codes of length n over $\mathbb{F}_{2^m}$ is given using the factorization of $X^n - 1$ in $\mathbb{F}_{2^m}[X]$. In [2], self-dual θ-cyclic codes over $\mathbb{F}_4$ are constructed by solving polynomial systems satisfied by the coefficients of their generator polynomials. Since the polynomial system becomes increasingly difficult to solve, we propose in this section a construction that allows to construct self-dual codes from suitable smaller degree polynomials.

Proposition 5 *Consider a finite field $\mathbb{F}_q$ of characteristic p, $R = \mathbb{F}_q[X;\theta]$ with $\theta^2 = id$ and $k = p^s \times t$ with $s \in \mathbb{N}^*$ and t an integer not multiple of p. For $h \in R$ of degree k the polynomial $g = h^{*\ell}$ generates a self-dual θ-code over $\mathbb{F}_q$ of length $n = 2k$ if and only if*

1. *$Y^t - \varepsilon = f_1(Y)f_2(Y)\cdots f_m(Y) \in (\mathbb{F}_q)^\theta[Y] = Z(R)$ ($\varepsilon = \pm 1$ and $Y = X^2$), where $f_i(X^2) \in R$ are monic polynomials that are pairwise coprime with the property that $f_i^{*\ell} = f_i$.*
2. *$h_i^{*\ell}h_i = f_i^{p^s}$*
3. *$h = \mathrm{lcrm}(h_1, \ldots, h_m)$*

Proof:

1. ($\Leftarrow$): We have to prove that $h^{*_\ell}h = X^{2tp^s} - \varepsilon$ (Corollary 1). From $h = \mathrm{lcrm}(h_1, \ldots, h_m)$ we obtain that $h = h_i q_i$ with $q_i \in R$. Lemma 1 shows that $h^{*_\ell} = \tilde{q}_i h_i^{*_\ell}$ where $\tilde{q}_i \in R$. Therefore $h^{*_\ell}h = \tilde{q}_i(h_i^{*_\ell}h_i)q_i = \tilde{q}_i(f_i)^{p^s}q_i = \tilde{q}_i q_i (f_i)^{p^s}$ (because $(f_i)^{p^s} \in (\mathbb{F}_q)^\theta[X^2]$ is central), showing that $\mathrm{lclm}((f_1)^{p^s}, \ldots, (f_m)^{p^s})$ is a right divisor of $h^{*_\ell}h$ in R. To prove the claim it remains to show that

$$\mathrm{lclm}((f_1)^{p^s}, \ldots, (f_m)^{p^s}) \;=\; (f_1)^{p^s} \cdots (f_m)^{p^s} = X^n - \varepsilon. \qquad (4)$$

   Comparing degrees we obtain from relation (4) that $h^{*_\ell}h = X^n - \varepsilon$. In order to prove the first equality of relation (4) 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 lclm can be computed in both cases using the extended euclidean algorithm ([5], Section 2), they coincide in both rings. In the commutative ring $Z(R) = (\mathbb{F}_q)^\theta[Y]$ the first equality of relation (4) is a consequence of Gauss Lemma and the claim follows.

2. ($\Rightarrow$): Corollary 1 shows that if $g = h^{*_\ell}$ generates a self-dual θ-code over $\mathbb{F}_q$ of length $n = 2k$, then $h^{*_\ell}h = X^n - \varepsilon = ((X^2)^t - \varepsilon)^{p^s} = (Y^t - \varepsilon)^{p^s}$ (where $Y = X^2$). Since $(Y^t - \varepsilon)^{*_\ell} = Y^t - \varepsilon$, a decomposition $Y^t - \varepsilon = f_1(Y)f_2(Y)\cdots f_m(Y) \in (\mathbb{F}_q)^\theta[Y] = Z(R)$ into pairwise coprime $f_i(Y)$ with $f_i^{*_\ell} = f_i$ must exist in $\mathbb{F}_q[Y]$. We noted above that the division in $Z(R)$ and R coincide in $Z(R)$, so that $(f_i^{p^s})^{*_\ell} = f_i^{p^s}$ are pairwise coprime in $Z(R)$ and R. According to ([5], Theorem 4.1), we have $h^{*_\ell} = \mathrm{lclm}({h_1}^{*_\ell}, \ldots, {h_m}^{*_\ell})$ where ${h_i}^{*_\ell} = \mathrm{gcrd}(f_i^{p^s}, h^{*_\ell})$ are pairwise coprime in R. In particular, according to [8], $\deg(\mathrm{lclm}({h_i}^{*_\ell}, {h_j}^{*_\ell})) = \deg({h_i}^{*_\ell}) + \deg({h_j}^{*_\ell})$ for $i \neq j$ and $\deg(h^{*_\ell}) = \deg(\mathrm{lclm}({h_i}^{*_\ell})) = \sum \deg(h_i^{*_\ell})$.

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

   - Let δ_i be the degree of $f_i^{p^s}$ and d_i be the degree of h_i. Since $f_i \in Z(R)$, δ_i is even. Applying Lemma 1 to $f_i^{p^s} = q_i h_i^*$ we obtain $(f_i^{p^s})^* = \Theta^{\delta_i - d_i}(h_i^{**})q_i^* = \Theta^{\delta_i - d_i}(\Theta^{d_i}(h_i))q_i^* = \Theta^{\delta_i}(h_i)q_i^* = h_i q_i^*$ (δ_i is even and $\theta^2 = id$). So h_i divides on the left $(f_i^{p^s})^*$. As $(f_i)^{p^s}$ is

central, it is equal to $(f_i^{p^s})^*$ times a constant, so h_i divides on the left $(f_i^{p^s})^{*_\ell} = f_i^{p^s}$.

- Since $h_i^{*_\ell}$ divides h^{*_ℓ} on the right, we also have $h^* = p_i h_i^*$. Using Lemma 1, we obtain $\Theta^k(h) = h^{**} = \Theta^{k-d_i}(h_i^{**})p_i^*$. Therefore $\Theta^k(h) = \Theta^{k-d_i}(\Theta^{d_i}(h_i))p_i^* = \Theta^k(h_i)p_i^*$. Since Θ is a morphism of rings, h_i divides h on the left.

Since $h_i^{*_\ell}$ divides h^{*_ℓ} on the right and h_i divides h on the left, we obtain $h^{*_l}h = \tilde{g}_i h_i^{*_l} h_i g_i$. Since two factors of a decomposition of the central polynomial $h^{*_l}h = \tilde{g}_i h_i^{*_l} h_i g_i$ into two factors commute, $h_i^{*_l}h_i$ divides $h^{*_l}h = X^n - \varepsilon$ on the right. According to Theorem 4.1 of [5], $h_i^{*_\ell}h_i = \mathrm{lclm}(\mathrm{gcrd}(h_i^{*_\ell}h_i, f_j^{p^s}), j = 1, \ldots m)$. We now note that both $h_i^{*_\ell}$ and h_i divide the central polynomial $f_i^{p^s}$, so that the product $h_i^{*_\ell}h_i$ divides $(f_i^{p^s})^2$. For $j \neq i$ we obtain $\mathrm{gcrd}(h_i^{*_\ell}h_i, f_j^{p^s}) = 1$ and $h_i^{*_\ell}h_i = \mathrm{gcrd}(h_i^{*_\ell}h_i, f_i^{p^s})$. In particular, $h_i^{*_\ell}h_i$ divides $f_i^{p^s}$.

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

$$\deg(\mathrm{lclm}(h_i^{*_\ell}h_i)) = \sum_{i=0}^{m} \deg(h_i^{*_\ell}h_i) = 2\sum_{i=0}^{m} \deg(h_i^{*_\ell})$$

$$= 2\deg(h^{*_\ell}) = \sum_{i=0}^{m} \deg(f_i^{p^s}).$$

From $\sum_{i=0}^m \deg(h_i^{*_\ell}h_i) = \sum_{i=0}^m \deg(f_i^{p^s})$ and the fact that $h_i^{*_\ell}h_i$ divides $f_i^{p^s}$, we obtain ${h_i}^{*_\ell}h_i = f_i^{p^s}$.

As h_i divides h on the left, $\mathrm{lcrm}(h_i, i = 1, \ldots, m)$ also divides h on the left. Since $\mathrm{gcrd}(h_i^{*_\ell}, h_j^{*_\ell}) = 1$ implies $\mathrm{gcld}(h_i, h_j) = 1$ we have $\deg(\mathrm{lcrm}(h_i, i = 1, \ldots, m)) = \sum \deg(h_i) = \deg(h)$. Therefore $h = \mathrm{lcrm}(h_i, i = 1, \ldots, m)$.

□

Example 3 *Let $\mathbb{F}_4 = \mathbb{F}_2(a)$, θ the Frobenius automorphism $a \mapsto a^2$ and $R = \mathbb{F}_4[X;\theta]$. In $\mathbb{F}_2[Y] = Z(R)$ (where $Y = X^2$), we have $Y^{39} - 1 =$*

$f_1(Y)f_2(Y)f_3(Y)f_4(Y)$ *where:*

$$\begin{aligned}
f_1(Y) &= Y+1\\
f_2(Y) &= Y^2+Y+1\\
f_3(Y) &= Y^{12}+Y^{11}+Y^{10}+Y^9+Y^8+Y^7+Y^6+Y^5+Y^4+Y^3+Y^2+Y+1\\
f_4(Y) &= (Y^{12}+Y^{11}+Y^{10}+Y^9+Y^5+Y^4+Y^3+Y^2+1)\\
&\quad (Y^{12}+Y^{11}+Y^{10}+Y^9+Y^8+Y^7+Y^6+Y^5+Y^4+Y^3+Y^2+Y+1)
\end{aligned}$$

The polynomials f_i *are pairwise coprime polynomials satisfying* $f_i^{*\ell} = f_i$ *(*$i \in \{1,\ldots,4\}$*).*

The skew polynomials

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

satisfy $h_i^{*\ell}h_i = f_i(= f_i(X^2))$ *(*$i \in \{1,2,3,4\}$*.*

According to Proposition 5 for $h = lcrm(h_1,h_2,h_3,h_4)$ *the skew polynomial* $g = h^{*\ell} = \mathrm{lclm}(h_1^{*\ell},h_2^{*\ell},h_3^{*\ell},h_4^{*\ell})$ *below*

$$X^{39}+a^2X^{38}+a^2X^{37}+X^{36}+a^2X^{34}+aX^{33}+aX^{32}+a^2X^{31}+aX^{30}+a^2X^{29}+a^2X^{28}+$$

$$aX^{27}+a^2X^{26}+a^2X^{25}+X^{24}+a^2X^{22}+X^{20}+X^{19}+a^2X^{17}+X^{15}+a^2X^{14}+a^2X^{13}$$

$$+aX^{12}+a^2X^{11}+a^2X^{10}+aX^9+a^2X^8+aX^7+aX^6+a^2X^5+X^3+a^2X^2+a^2X+1$$

generates a $[78,39]$ *self-dual code over* $\mathbb{F}_4$*. Using the generator matrix of the code (cf. [2, 3]) one can verify in* Magma *(cf. [1]) that its minimum distance is equal to* 19*. Therefore* g *generates a* $[78,39,19]_4$ *self-dual code.*

References

[1] Bosma, W., Cannon, J., Playoust, C., *The magma algebra system: The user language*, Journal of Symbolic Computation 24, 235–265 (1997).

[2] Boucher, D. and Ulmer, F., *Coding with skew polynomial rings*, Journal of Symbolic Computation, 44, 1644–1656 (2009).

[3] Boucher, D. and Ulmer, F., *Codes as modules over skew polynomial rings* Proceedings of the 12th IMA conference on Cryptography and Coding, Lecture Notes in Computer Science, 5921, 38–55 (2009).

[4] Boucher D. and Ulmer F., *A note on the dual codes of module skew codes*, Proceedings of the 13th IMA Conference of Cryptography and Coding, Lecture Notes in Computer Science, 7089, 230–243 (2011).

[5] Giesbrecht, M. *Factoring in skew-polynomial rings over finite fields*, J. Symbolic Comput., 26, 4, 463–486 (1998).

[6] Jacobson, N. *The Theory of Rings* Mathematical Surveys and Monographs, Vol 2, American Mathematical Society, 1943

[7] Jia, S., Ling S., Xing C. *On Self-Dual Cyclic Codes Over Finite Fields*, IEEE Transactions on Information Theory, Vol. 57, No. 4 (2011).

[8] O. Ore, *Theory of Non-Commutative Polynomials*, *Annals of Mathematics*, 2nd Ser, Vol. 34, No. 3. pp 480–508 (1933).