

Coding with skew polynomial rings

Delphine Boucher

IRMAR, Université de Rennes 1, Campus de Beaulieu, F-35042 Rennes

Felix Ulmer

IRMAR, Université de Rennes 1, Campus de Beaulieu, F-35042 Rennes

Abstract

In analogy to cyclic codes, we study linear codes over finite fields obtained from left ideals in a quotient ring of a (non commutative) skew polynomial ring. The paper shows how existence and properties of such codes are linked to arithmetic properties of skew polynomials. This class of codes is a generalization of the θ -cyclic codes discussed in (Boucher et al., 2007). However θ -cyclic codes are performant representants of this family and we show that the dual of a θ -cyclic code is still θ -cyclic. Using Groebner bases, we compute all Euclidean and Hermitian self-dual θ -cyclic codes over \mathbf{F}_4 of length less than 40, including a [36, 18, 11] Euclidean self-dual θ -cyclic code which improves the previously best known self-dual code of length 36 over \mathbf{F}_4 .

Key words: cyclic codes, finite rings, skew polynomial rings

Introduction

Let \mathbf{F}_q be a finite field of q elements. A linear $[n, k]$ -code over \mathbf{F}_q is a k -dimensional vector subspace \mathcal{C} of the vector space $V = \mathbf{F}_q^n = \{(a_0, \dots, a_{n-1}) \mid a_i \in \mathbf{F}_q\}$. In the following we use the polynomial representation of the code \mathcal{C} , where we identify code words $(a_0, a_1, \dots, a_{n-1}) \in \mathcal{C}$ with coefficient tuples of polynomials $a_{n-1}X^{n-1} + \dots + a_1X + a_0 \in \mathbf{F}_q[X]$. In the classical case those polynomials can also be seen as elements of a quotient ring $\mathbf{F}_q[X]/(f)$ where f is a polynomial of degree n . In order to generalize the notion of codes associated to ideals, we consider the more general skew polynomial

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

URLs: <http://perso.univ-rennes1.fr/delphine.boucher/> (Delphine Boucher),
<http://perso.univ-rennes1.fr/felix.ulmer/> (Felix Ulmer).

ring of automorphism type which we now define. Starting from the finite field \mathbf{F}_q and an automorphism θ of \mathbf{F}_q one defines a ring structure on the set

$$\mathbf{F}_q[X, \theta] = \{a_{n-1}X^{n-1} + \dots + a_1X + a_0 \mid a_i \in \mathbf{F}_q \text{ and } n \in \mathbf{N}\}.$$

This is the set of formal polynomials where the coefficients are written on the left of the variable X . The addition in $\mathbf{F}_q[X, \theta]$ is defined to be the usual addition of polynomials and the multiplication is defined by the basic rule $Xa = \theta(a)X$ ($a \in \mathbf{F}_q$) and extended to all elements of $\mathbf{F}_q[X, \theta]$ by associativity and distributivity. Those rings are well known (cf. (McDonald, 1974; Ore, 1933)) and, over a finite field, are the most general “polynomial rings” with a commutative field of coefficients where the degree of a product of two elements is the sum of the degrees of the elements.

The ring $\mathbf{F}_q[X, \theta]$ is a left and right Euclidean ring whose left and right ideals are principal (Ore, 1933). Left and right gcd and lcm exist in $\mathbf{F}_q[X, \theta]$ and can be computed using the left and right Euclidean algorithm (Bronstein and Petkovsek, 1994).

According to ((McDonald, 1974), Theorem II.12) or ((Berrick and Keating, 2000), Theorem 3.2.16), the two-sided ideals of $\mathbf{F}_q[X, \theta]$ are generated by elements in $X^t \mathbf{F}_q^\theta[X^m]$, where t is an integer, m is the order of θ and \mathbf{F}_q^θ is the fixed field of θ . The center $Z(\mathbf{F}_q[X, \theta])$ of $\mathbf{F}_q[X, \theta]$ is $\mathbf{F}_q^\theta[X^m]$. In particular a left or right ideal in $\mathbf{F}_q[X, \theta]$ generated by a central element is a two-sided ideal. If I is a two-sided ideal in $\mathbf{F}_q[X, \theta]$ then I is generated by a polynomial f of some degree n in $X^t \mathbf{F}_q^\theta[X^m]$; by the correspondance of ideals, the left ideals in $\mathbf{F}_q[X, \theta]/(f)$ are principal ideals, each generated by a right divisor g of f . To the element $a(X) = a_{n-1}X^{n-1} + \dots + a_1X + a_0$ in $\mathbf{F}_q[X, \theta]/(f)$ we associate the word $a = (a_0, a_1, \dots, a_{n-1}) \in \mathbf{F}_q^n$. The elements $a(X)$ of $\mathbf{F}_q[X, \theta]/(f)$ that belong to a left ideal in $\mathbf{F}_q[X, \theta]/(f)$ generated by a right divisor g of f form a linear $[n, k]$ code in \mathbf{F}_q^n , where $k = n - \deg(g)$. More precisely

Definition 1. Let $f \in \mathbf{F}_q[X, \theta]$ be of degree n . If $I = (f)$ is a two-sided ideal of $\mathbf{F}_q[X, \theta]$, then a θ -code \mathcal{C} consists of code words $a = (a_0, a_1, \dots, a_{n-1})$ that are coefficient tuples of elements $a(X) = a_{n-1}X^{n-1} + \dots + a_1X + a_0$ of a left ideal of $\mathbf{F}_q[X, \theta]/I$. In this case the elements $a(X)$ are left multiples of a right divisor g of f . We will focus on two special cases:

- (1) If $f \in Z(\mathbf{F}_q[X, \theta])$, then we call the θ -code corresponding to the left ideal $(g)/(f)$ a central θ -code.
- (2) If the order of θ divides n and $f = X^n - 1$, then we call the θ -code corresponding to the left ideal $(g)/(X^n - 1)$ a θ -cyclic code.

If $g = g_rX^r + \dots + g_1X + g_0$ divides a polynomial $f \in \mathbf{F}_q[X, \theta]$ of degree n such that (f) is a two-sided ideal, then the generating matrix of the θ -code of type $[n, n - r]$ generated by g is given by

$$G = \begin{pmatrix} g_0 & \dots & g_{r-1} & g_r & 0 & \dots & 0 \\ 0 & \theta(g_0) & \dots & \theta(g_{r-1}) & \theta(g_r) & \dots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & & & & & & \\ 0 & \dots & 0 & \theta^{n-r-1}(g_0) & \dots & \theta^{n-r-1}(g_{r-1}) & \theta^{n-r-1}(g_r) \end{pmatrix}$$

where one reads the polynomial $X^i g(X) = \sum_{j=0}^r \theta^i(g_j) X^j$ on the $(i+1)$ th row for i in $\{0, \dots, n-r-1\}$. Indeed, a code word is represented by a polynomial $m(X)g(X) = \sum_{i=0}^{n-r-1} m_i X^i g(X)$ where $m(X) = \sum_{i=0}^{n-r-1} m_i X^i$.

Note that only the generating polynomial is used to define the θ -code. In the next section we will see that any skew polynomial g occurs as a generating polynomial of a θ -code, but not for any length. We show that the minimal length for g is determined by the degree of the generator of the maximal two-sided ideal contained in the left ideal $(g) \subset \mathbf{F}_q[X, \theta]$. The ideal structure is a valuable tool, since it describes the properties of a θ -code and should therefore be a useful tool for coding and decoding. The Euclidean ring structure of $\mathbf{F}_q[X, \theta]$ allows to decide whether a polynomial represents a code word using division by the generator polynomial of the code and we will see that the factorization in $\mathbf{F}_q[X, \theta]$ gives the parity check matrix of a θ -cyclic code.

Example 2. Since the generator polynomial g of a θ -cyclic code is a right factor of $X^n - 1$, those codes have the following property ((Boucher et al., 2007), Theorem 1)

$$(a_0, a_1, \dots, a_{n-1}) \in \mathcal{C}_\theta \quad \Rightarrow \quad (\theta(a_{n-1}), \theta(a_0), \theta(a_1), \dots, \theta(a_{n-2})) \in \mathcal{C}_\theta.$$

The special class of θ -cyclic codes is introduced in (Gabidulin, 1985) using the ring of *linearized polynomials* and in (Boucher et al., 2007) using the ring of *skew polynomials*.

Consider $\mathbf{F}_{q_0} \subset \mathbf{F}_q$ and θ be the Frobenius automorphism of $\mathbf{F}_q/\mathbf{F}_{q_0}$ defined by $\theta(a) = a^{q_0}$. According to ((McDonald, 1974) theorem II 13), there is a ring isomorphism between the ring $k[X, \theta]$ and the ring of linearized polynomials $k[Y^{q_0}, \circ]$ given by $X \mapsto Y^{q_0}$.

Example 3. Consider $\mathbf{F}_4[X, \theta]$ where θ is the Frobenius automorphism and let us denote α a generator of the multiplicative group of \mathbf{F}_4 . The polynomial $X^2 + \alpha X + 1$ generates a left ideal in a $\mathbf{F}_4[X, \theta]/(X^4 + X^2 + 1)$ which corresponds to a non-cyclic linear code \mathcal{C} of minimum Hamming distance 2. This leads to a $[4, 2, 2]$ code which is a central θ -code but not a θ -cyclic code.

Note that $a(X) = a_0 + a_1 X + a_2 X^2 + a_3 X^3 \in \mathcal{C}$ implies that $X \cdot a(X) \in \mathcal{C}$

$$\begin{aligned} X a(X) &= \theta(a_0)X + \theta(a_1)X^2 + \theta(a_2)X^3 + \theta(a_3)X^4 \\ &= \theta(a_3) + \theta(a_0)X + (\theta(a_1) + \theta(a_3))X^2 + \theta(a_2)X^3 + \theta(a_3)(X^4 + X^2 + 1) \end{aligned}$$

Therefore in $\mathbf{F}_4[X, \theta]/(X^4 + X^2 + 1)$ we have $X a(X) = \theta(a_3) + \theta(a_0)X + (\theta(a_1) + \theta(a_3))X^2 + \theta(a_2)X^3$, showing that

$$(a_0, a_1, a_2, a_3) \in \mathcal{C} \quad \Rightarrow \quad (\theta(a_3), \theta(a_0), \theta(a_1) + \theta(a_3), \theta(a_2)) \in \mathcal{C}.$$

1. Generalities on θ -codes

The following shows that the class of θ -codes is much larger than the class of θ -cyclic codes and extend Gabidulin's codes.

Lemma 4. *Suppose that $f = X^n - 1 \in \mathbf{F}_q[X, \theta]$ generates a two-sided ideal. A θ -cyclic code generated by a monic right divisor g of f of degree $< n - 1$ generates a cyclic code if and only if all coefficients of g are in \mathbf{F}_q^θ , the fixed field of θ in \mathbf{F}_q .*

Proof. Let $g = X^r + \sum_{i=0}^{r-1} g_i X^i$. First note that if all coefficients of g are in \mathbf{F}_q^θ , then the corresponding generating matrix G is the matrix of a cyclic code. If the θ -code \mathcal{C} generated by the left ideal $(g) \subseteq \mathbf{F}_q[X, \theta]/(f)$ is cyclic, then $g \cdot X \in \mathcal{C}$. Since the code is linear, we have in particular $X \cdot g - g \cdot X \in \mathcal{C}$. Therefore

$$(\theta(g_0) - g_0)X + (\theta(g_1) - g_1)X^2 + \dots + (\theta(g_{r-1}) - g_{r-1})X^r$$

is a (constant) left multiple $\lambda \cdot g$ of g . Since g divides f , its constant term is non zero. This shows that $\lambda = 0$ and that the above polynomial $X \cdot g - g \cdot X$ must be zero. Therefore all coefficients g_i of g are invariant under θ and must be in the fixed field \mathbf{F}_q^θ . \square

The following example shows that the class of central θ -codes is larger than the class of θ -cyclic codes.

Example 5. Consider $\mathbf{F}_4[X, \theta]$ where θ is the Frobenius automorphism and let us denote α a generator of the multiplicative group of \mathbf{F}_4 . Considering all right factors of degree 3 of $X^{12} - 1 \in \mathbf{F}_4[X, \theta]$ we construct all $[12, 9]$ θ -cyclic codes and we see that the best Hamming distance of these codes is 2. However, we can construct a $[12, 9, 3]$ central θ -code. For this we note that the central polynomial

$$f = X^{12} + X^{10} + X^8 + X^6 + X^4 + X^2 + 1 \in \mathbf{F}_4[X, \theta]$$

is divisible on the right by $g = X^3 + X^2 + X + \alpha$. The corresponding central θ -code is a $[12, 9, 3]$ code with weight enumerator polynomial

$$\begin{aligned} 1 + 102Y^3 + 651Y^4 + 3000Y^5 + 10416Y^6 + 27156Y^7 + 50943Y^8 + 67224Y^9 \\ + 61248Y^{10} + 33078Y^{11} + 8325Y^{12} \end{aligned}$$

The number of central θ -codes is connected to the number of right factors of a central polynomial.

Example 6. Consider $\mathbf{F}_4[X, \theta]$ where θ is the Frobenius automorphism and let us denote α a generator of \mathbf{F}_4^* . In $\mathbf{F}_4[X, \theta]$ the polynomial $X^4 + X^2 + 1$ has five distinct factorizations in products of irreducible monic polynomials :

$$\begin{aligned} X^4 + X^2 + 1 &= (X^2 + X + 1)(X^2 + X + 1) \\ &= (X^2 + \alpha^2)(X^2 + \alpha) \\ &= (X^2 + \alpha)(X^2 + \alpha^2) \\ &= (X^2 + \alpha^2 X + 1)(X^2 + \alpha^2 X + 1) \\ &= (X^2 + \alpha X + 1)(X^2 + \alpha X + 1) \end{aligned}$$

The ring $\mathbf{F}_2[X]$ generates a commutative subring of $\mathbf{F}_4[X, \theta]$. This explains why the list of all possible decompositions of $f \in Z(\mathbf{F}_4[X, \theta]) = \mathbf{F}_2[X^2]$ into a product of two polynomials always also contains the decompositions in $\mathbf{F}_2[X]$. A decomposition in $\mathbf{F}_2[X]$ has either both factors in $\mathbf{F}_2[X]$ or none.

The following lemma explains why in the above example the two factors in the decomposition of the generator of the two-sided ideal always commute:

Lemma 7. *If $h \cdot g \in Z(\mathbf{F}_q[X, \theta])$, then $h \cdot g = g \cdot h$ in $\mathbf{F}_q[X, \theta]$.*

Proof. Since $h \cdot g \in Z(\mathbf{F}_q[X, \theta])$ we have $h \cdot (g \cdot h) = (h \cdot g) \cdot h = h \cdot (h \cdot g)$. Since $\mathbf{F}_q[X, \theta]$ has no non trivial zero divisors, we can cancel h on the left of both equations. Therefore $h \cdot g = g \cdot h$ in $\mathbf{F}_q[X, \theta]$. \square

Using this commutativity result, we can proceed as in the cyclic case to obtain a parity check polynomial:

Lemma 8. *Let $h \cdot g \in Z(\mathbf{F}_q[X, \theta])$ and denote \mathcal{C} the central θ -code corresponding to the left ideal generated by g in $\mathbf{F}_q[X, \theta]/(h \cdot g)$. Then $a \in \mathcal{C} \Leftrightarrow a(X) \cdot h = 0$ in $\mathbf{F}_q[X, \theta]/(h \cdot g)$.*

Proof. If $a \in \mathcal{C}$, then $a(X) = m \cdot g$. By the above commutativity result we get $a(X) \cdot h = (m \cdot g) \cdot h = m \cdot (h \cdot g) = 0$ in $\mathbf{F}_q[X, \theta]/(h \cdot g)$. Conversely, if $a(X) \cdot h = 0$ in $\mathbf{F}_q[X, \theta]/(h \cdot g)$, then $a(X) \cdot h = f \cdot (h \cdot g) = (f \cdot g) \cdot h$ in $\mathbf{F}_q[X, \theta]$. Since $\mathbf{F}_q[X, \theta]$ is a right cancellation ring we get $a(X) = f \cdot g$, showing that $a \in \mathcal{C}$. \square

The parity check matrix is now obtained from the condition $a \in \mathcal{C} \Leftrightarrow a(X) \cdot h = 0$ in $\mathbf{F}_q[X, \theta]/(h \cdot g)$ (see section 3).

2. The length of a θ -code

We will show that any $g \in \mathbf{F}_q[X, \theta]$ divides a polynomial $f \in \mathbf{F}_q[X, \theta]$ generating a two-sided ideal and therefore is the generating polynomial of some θ -code.

Definition 9. (cf (Jacobson, 1943)) An element $P \in \mathbf{F}_q[X, \theta]$ is bounded if the left ideal (P) contains a two-sided ideal (P^*) . The monic polynomial P^* of minimal degree is the bound of P .

Since P^* generates a two-sided ideal, it must be of the form $(b_0 + b_1 X^m + b_2 X^{2m} + \dots + b_s X^{s \cdot m}) X^t$, where t is an integer, m is the order of θ and $b_i \in \mathbf{F}_q^\theta$ the fixed field of θ . From Theorem 15 in (Jacobson, 1943) we get that all elements of $\mathbf{F}_q[X, \theta]$ are bounded. The discussion before Theorem 15 also shows:

Lemma 10. *Let m be the order of θ and $l = [\mathbf{F}_q : \mathbf{F}_q^\theta]$. If $P \in \mathbf{F}_q[X, \theta]$ is of degree n , then the bound P^* is of degree $\leq m \cdot l \cdot n$.*

Proof. The elements in $\mathbf{F}_q[X, \theta]$ of degree less than n form a \mathbf{F}_q vector space of dimension n and therefore a \mathbf{F}_q^θ vector space of dimension $l \cdot n$. Considering the remainders of the division

$$X^{m \cdot i} = P \cdot Q_i + R_i, \quad i = 0, 1, \dots, l \cdot n,$$

with $\deg(R_i) < n$, there exists a non trivial linear combination $\sum_{i=0}^{l \cdot n} \delta_i R_i = 0$ where $\delta_i \in \mathbf{F}_q^\theta$. This shows that

$$\sum_{i=0}^{l \cdot n} \delta_i X^{m \cdot i} = P \cdot \left(\sum_{i=0}^{l \cdot n} \delta_i Q_i \right).$$

The above polynomial $\sum_{i=0}^{l \cdot n} \delta_i X^{m \cdot i}$ is a bound for P . According to Theorem 12 in (Jacobson, 1943), the bound P^* of P is a divisor of this polynomial. \square

This proves that an element $g \in \mathbf{F}_4[X, \theta]$ of degree r has a bound of degree at most $4r$. The proof of the following stronger result for $\mathbf{F}_4[X, \theta]$ is due to P. Solé :

Lemma 11. *Consider $\mathbf{F}_4[X, \theta]$ where θ is the Frobenius automorphism. The bound of a polynomial of degree r in $\mathbf{F}_4[X, \theta]$ is of degree at most $2r$.*

Proof. Let $g = \sum_{i=0}^r g_i X^i$ and $\tilde{g} = \sum_{i=0}^r \theta^{i+1}(g_i) X^i$. Then $g\tilde{g} = \sum_{k=0}^{2r} a_k X^k$ where $a_{2k+1} = \sum_{i+j=2k+1} g_i g_j = 0$ and $a_{2k} = \sum_{i+j=2k} g_i \theta(g_j) \in \mathbf{F}_2$. So $g\tilde{g} \in \mathbf{F}_2[X^2]$ and the bound of g divides the polynomial $g\tilde{g} \in \mathbf{F}_2[X^2]$ whose degree is $2r$. \square

The existence of θ -codes of type $[n, k]$ for $r = n - k < \frac{n}{2}$ is due to the fact that the degree of the bound of g can be less than $2r$.

Example 12. Consider $\mathbf{F}_4[X, \theta]$ where θ is the Frobenius automorphism and let us denote α a generator of \mathbf{F}_4^* . In $\mathbf{F}_4[X, \theta]$, the polynomial

$$g = X^{12} + X^{11} + \alpha X^{10} + X^9 + \alpha^2 X^8 + X^6 + X^5 + \alpha^2 X^4 + X^2 + X + \alpha^2$$

is a right divisor of $f = X^{14} + X^{12} + X^{10} + 1 \in \mathbf{F}_4[X, \theta]$. Therefore the bound of g is of degree ≤ 14 and $(g)/(f) \subset \mathbf{F}_4[X, \theta]/(f)$ is a θ -code which is a $[14, 2, 11]$ code with the best possible Hamming distance 11.

Two skew polynomials P_1 and P_2 are similar, noted $P_1 \sim P_2$, if the left (or right) $\mathbf{F}_q[X, \theta]$ modules $\mathbf{F}_q[X, \theta]/(P_1)$ and $\mathbf{F}_q[X, \theta]/(P_2)$ are isomorphic. According to (Jacobson, 1943) p.39 the left and right bounds coincide and similar polynomials have the same bound.

Proposition 13. *Let m be the order of θ . If the generator g of a θ -code in $\mathbf{F}_q[X, \theta]/(f)$ has factors similar to X , then g is of the form $g = \tilde{g} \cdot X^t$, where \tilde{g} has no factor similar to X . In this case $f = X^{\ell-t} \cdot \tilde{f} \cdot X^t$ where $\ell \geq t$ and $\tilde{f} = b_0 + b_1 X^m + b_2 X^{2m} + \dots + b_s X^{s \cdot m} \in \mathbf{F}_q^\theta[X^m]$, where $b_0 \neq 0$. The polynomial \tilde{f} is a bound for \tilde{g} and the θ -code $(g)/(f)$ can be obtained from $(\tilde{g})/(\tilde{f})$ by adding t zeros to the left of each code word.*

Proof. Polynomials of degree one are irreducible in $\mathbf{F}_q[X, \theta]$. From (Jacobson, 1943; Singer, 1996) we obtain that irreducible skew polynomials P_1 and P_2 are similar if and only if they are of the same degree and there exists a polynomial $U \in \mathbf{F}_q[X, \theta]$ of degree less than $\deg(P_i)$ such that $P_1 U$ is the left lcm of P_2 and U . The polynomial X is only

similar to multiples of itself, since according to the above $(\alpha X + \beta) \sim X$ implies in this case, that there exist u and γ in \mathbf{F}_q such that $(\alpha X + \beta)u = \gamma X$. Therefore the number of irreducible factors similar to X corresponds to the number of factors X in such a decomposition.

From $Xa = \theta(a)X$ we obtain that a factor X can always be moved to become a left or right factor, showing that $g = \tilde{g} \cdot X^t$ and $f = X^{\ell-t} \cdot \tilde{f} \cdot X^t$ where $\ell \geq t$ and $\tilde{f} = b_0 + b_1 X^m + b_2 X^{2m} + \dots + b_s X^{s \cdot m} \in \mathbf{F}_q^\theta[X^m]$, where $b_0 \neq 0$. Since $\mathbf{F}_q[X, \theta]$ is a left and right domain, we obtain that \tilde{g} is a right factor of $X^{\ell-t} \cdot \tilde{f}$. The generating matrix of $(g)/(X^{\ell-t} \cdot f \cdot X^t)$ and $(\tilde{g})/(X^{\ell-t} \cdot \tilde{f})$ differ only by t columns of zeros on the right. In the first case the code words are given by $(\sum_{j=0}^k c_j X^j) \cdot \tilde{g} \cdot X^t$ and in the second by $(\sum_{j=0}^k c_j X^j) \cdot \tilde{g}$. \square

Therefore θ -codes generated by polynomials without constant term are obtained from θ -codes of smaller block length to which zero entries have been added to the right.

There are many factorizations in the non commutative ring $\mathbf{F}_q[X, \theta]$, up to similarity.

Theorem 14 (cf (Jacobson, 1943)). *If $P \in \mathbf{F}_q[X, \theta]$ has two decompositions into irreducible factors*

$$P = P_1 P_2 \cdots P_n = \tilde{P}_1 \tilde{P}_2 \cdots \tilde{P}_m,$$

then $n = m$ and there exists a permutation $\sigma \in S_n$ such that P_i and $\tilde{P}_{\sigma(i)}$ are similar.

Lemma 10 gives a constructive way to compute the bound of a given polynomial. An alternative approach is to note that the bound of a product is a divisor of the product of the bounds of its factors (cf. (Jacobson, 1943), Theorem 12) :

Example 15. In the previous example, the polynomial

$$g = X^{12} + X^{11} + \alpha X^{10} + X^9 + \alpha^2 X^8 + X^6 + X^5 + \alpha^2 X^4 + X^2 + X + \alpha^2$$

factors as $g = (X^4 + X + 1)^2 (X + \alpha) (X + \alpha) (X + 1)^2$. Furthermore the bound of $X + \alpha$ is $X^2 + 1$ whereas $(X^4 + X + 1)^2$ and $(X + 1)^2$ are both polynomials of $\mathbf{F}_2[X^2]$. So one can construct the bound of g as the product $(X^4 + X + 1)^2 (X^2 + 1) (X^2 + 1) (X + 1)^2 = X^{14} + X^{12} + X^{10} + 1$ which is the polynomial f of previous example.

The following table reproduces the best possible Hamming distances for $[n, k]$ θ -codes over $\mathbf{F}_4[X, \theta]$ with $r = n - k \leq \min(n, 10)$ and n an even number ≤ 44 .

As the bound of a polynomial g of degree r is at most of degree $2r$ (lemma 11), every polynomial of degree r generates a θ -code of length $n \geq 2r$. The fact that the bound for g is not needed to generate the corresponding θ -code (only its existence) enables us to make computations with quite large n as long as $r \leq n/2$.

We write C_d if this code is cyclic of Hamming distance d , C_d^θ if the code is θ -cyclic of Hamming distance d and θ_d if the code is a central θ -code of Hamming distance d . If we don't obtain such a code matching the Hamming distance of the best known code in Magma (Bosma et al., 1997) version 2.13 (command `BestKnownLinearCode`), then we indicate the difference in the Hamming distance by a negative number. The notation C_{3s}^θ

means that the code is θ -cyclic of Hamming distance 3 and self-dual.

$n \setminus r$	2	3	4	5	6	7	8	9	10
4	C_{3s}^θ	C_4							
6	C_2	C_4	C_4^θ	C_6					
8	C_2	C_3^θ	C_{4s}^θ	C_5^θ	C_6^θ	C_8			
10	C_2	θ_3	C_4^θ	C_5^θ	C_6^θ	θ_6	θ_8	C_{10}	
12	C_2	θ_3	θ_4	C_4	C_{6s}^θ	C_6^θ	C_7^θ	C_8^θ	C_9^θ
14	C_2	C_3^θ	C_4^θ	C_4	C_5^θ	C_{6s}^θ	C_7^θ	-1	-1
16	C_2	-1	-1	C_4^θ	-1	-1	-1	-1	C_8^θ
18	C_2	-1	θ_3	θ_4	-1	-1	C_6^θ	-1	C_8^θ
20	-1	θ_3	θ_3	θ_4	-1	-1	θ_6	C_7^θ	C_8^θ
22	θ_2	θ_2	θ_3	θ_4	θ_4	θ_5	-1	C_6^θ	C_7^θ

$n \setminus r$	2	3	4	5	6	7	8	9	10
24	C_2^θ	C_2^θ	θ_3	C_4^θ	C_4^θ	-1	-1	C_6^θ	C_7^θ
26	θ_2	θ_2	θ_3	θ_4	θ_4	-1	-1	C_6^θ	-1
28	C_2^θ	C_2^θ	θ_3	C_4^θ	C_4^θ	-1	θ_5	C_6^θ	C_6^θ
30	C_2^θ	C_2^θ	C_3^θ	C_4^θ	C_4^θ	-1	C_5^θ	C_6^θ	C_6^θ
32	C_2^θ	C_2^θ	-1	-1	θ_4	-1	θ_5	C_6^θ	θ_6
34	θ_2	θ_2	-1	-1	θ_4	-1	C_5^θ	C_6^θ	C_6^θ
36	C_2^θ	C_2^θ	-1	-1	θ_4	-1	-1	-1	θ_6
38	θ_2	θ_2	-1	-1	θ_4	-1	-1	-1	θ_6
40	C_2^θ	C_2^θ	-1	-1	θ_4	-1	-1	-1	θ_6
42	C_2^θ	C_2^θ	-1	C_3^θ	C_4^θ	-1	-1	-1	C_6^θ
44	C_2^θ	C_2^θ	-1	θ_3	θ_4	θ_4	-1	-1	-1

The table indicates that, with increasing length, the best θ -codes are no longer all cyclic or θ -cyclic. We note that the best codes given in Magma often have a poor weight distribution and that the θ -codes allow to find codes with a much better distribution.

Example 16. The best known $[6, 2, 4]$ code over \mathbf{F}_4 given by Magma 2.13 has weight distribution $1 + 15Y^4$ while the generating polynomial $X^4 + X^3 + \alpha^2 X^2 + X + \alpha$ with bound $X^6 + X^4 + X^2 + 1$ has weight distribution $1 + 3Y^4 + 12Y^5$. The $[12, 7]$ θ -cyclic code generated by $X^5 + \alpha X^4 + \alpha X^2 + \alpha X + \alpha$ has the weight distribution

$$1 + 18Y^4 + 252Y^5 + 672Y^6 + 1548Y^7 + 3285Y^8 + 4212Y^9 \\ + 3816Y^{10} + 2052Y^{11} + 528Y^{12}$$

instead of the distribution of Magma's best code $[12, 7, 4]$ which is

$$1 + 141Y^4 + 459Y^5 + 1215Y^6 + 2895Y^7 + 4230Y^8 + 4209Y^9 + 2541Y^{10} + 693Y^{11}$$

3. Duals of θ -cyclic codes

The θ -cyclic codes have been extensively studied in (Gabidulin, 1985) where the parity check matrix of such a code is given. In this section we derive the parity check matrix from the factorization of $X^n - 1$ in $\mathbf{F}_q[X, \theta]$ and prove (the new result) that the dual of a θ -cyclic code (for the Euclidean product) is a θ -cyclic code.

The following form of a parity check matrix for θ -cyclic codes is given in (Gabidulin, 1985).

Lemma 17. *Suppose that the order of θ divides n . Let $X^n - 1 = h \cdot g \in Z(\mathbf{F}_q[X, \theta])$ and denote \mathcal{C} the θ -cyclic code corresponding to the left ideal generated by g in $\mathbf{F}_q[X, \theta]/(X^n - 1)$. If $g = g_0 + g_1X + \dots + g_rX^r$ and $h = h_0 + h_1X + \dots + h_{n-r}X^{n-r}$, then the following matrix*

$$H = \begin{pmatrix} h_{n-r} & \dots & \theta^{n-r-1}(h_1) & \theta^{n-r}(h_0) & 0 & \dots & 0 \\ 0 & \theta(h_{n-r}) & \dots & \dots & \theta^{n-r+1}(h_0) & \dots & 0 \\ 0 & \ddots & \ddots & & & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \dots & \ddots & 0 \\ 0 & \dots & 0 & \theta^{r-1}(h_{n-r}) & \dots & \theta^{n-2}(h_1) & \theta^{n-1}(h_0) \end{pmatrix}$$

is a parity check matrix for \mathcal{C} .

Proof. Lemma 8 shows that for $a(X) \in \mathcal{C}$ the product $a(X) \cdot h = 0$ in $\mathbf{F}_q[X, \theta]/(X^n - 1)$. Since $\deg(a(X) \cdot h) < n + k$ where $k = n - r$ is the dimension of \mathcal{C} and the degree of h , we deduce that the coefficients of $X^k, X^{k+1}, \dots, X^{n-1}$ in this product must be zero. As, for $l \in \{0, \dots, r - 1\}$, the coefficient of X^{l+k} in $a(X) \cdot h$ is

$$\sum_{i=l}^{l+k} a_i \theta^i (h_{l+k-i})$$

we get that $a(X) \in \mathcal{C}$ implies $H \cdot a^t = 0$. So the code generated by H is in the dual \mathcal{C}^\perp of \mathcal{C} . As the dimension of \mathcal{C}^\perp is $n - \dim(\mathcal{C}) = r$, the number of rows of H , we deduce that H is a generator matrix for the dual of \mathcal{C} . \square

In (Gabidulin, 1985) the parity check matrix of a θ -cyclic code is given, but it is not shown that the dual of θ -cyclic code is θ -cyclic.

Corollary 18. *Suppose that the order of θ divides n . Let $g = \sum_{i=0}^r g_i X^i$ and $h = \sum_{i=0}^{n-r} h_i X^i$ be elements of $\mathbf{F}_q[X, \theta]$ such that $h \cdot g = X^n - 1 \in Z(\mathbf{F}_q[X, \theta])$. The dual of the θ -cyclic code generated by g in $\mathbf{F}_q[X, \theta]/(X^n - 1)$ is the θ -cyclic code generated by*

$$g^\perp = h_{n-r} + \theta(h_{n-r-1})X + \dots + \theta^{n-r}(h_0)X^{n-r}.$$

Proof. The parity check matrix H of the code is a generating matrix for the dual of the code, so we need to show that H is the matrix of a θ -cyclic code. According to the previous result, it amounts to show that $\theta^{n-r}(h_0)X^{n-r} + \dots + \theta(h_{n-r-1})X + h_{n-r}$ is also a divisor of $X^n - 1$. The ring $\mathbf{F}_q[X, \theta]$ is a right Ore domain and therefore has a right skew field of fraction (cf (Cohn, 1971), p. 23). Denote $\mathbf{F}_q(X, \theta)$ the right field of fraction of $\mathbf{F}_q[X, \theta]$ and X^{-1} the inverse of X . We have $aX^{-1} = X^{-1}\theta(a)$. We now consider the ring $R \subset \mathbf{F}_q(X, \theta)$ consisting of the elements $\sum_{i=0}^n X^{-i} a_i$, where the coefficients are on the right and where the multiplication rule is given by $aX^{-1} = X^{-1}\theta(a)$. The ring R is isomorphic to the skew polynomial ring $\mathbf{F}_q[X^{-1}, \theta^{-1}]$. The map

$$\begin{aligned} \varphi: \mathbf{F}_q[X, \theta] &\rightarrow R \subset \mathbf{F}_q(X, \theta) \\ \sum_{i=0}^n a_i X^i &\mapsto \sum_{i=0}^n X^{-i} a_i \end{aligned}$$

is an anti-isomorphism of rings. For $P_1 = \sum_{i=0}^s a_i X^i$ and $P_2 = \sum_{i=0}^t b_i X^i$ we have $\varphi(P_1 + P_2) = \varphi(P_1) + \varphi(P_2)$ and

$$\begin{aligned} \varphi(P_1 P_2) &= \varphi\left(\sum_{k=0}^{s+t} \sum_{i+j=k} a_i X^i b_j X^j\right) = \varphi\left(\sum_{k=0}^{s+t} \sum_{i+j=k} a_i \cdot \theta^i(b_j) X^{i+j}\right) \\ &= \sum_{k=0}^{s+t} X^{-k} \sum_{i+j=k} \theta^i(b_j) \cdot a_i = \sum_{k=0}^{s+t} \sum_{i+j=k} X^{-j} (X^{-i} \theta^i(b_j)) a_i \\ &= \left(\sum_{k=0}^{s+t} \sum_{i+j=k} X^{-j} b_j X^{-i} a_i\right) \\ &= \varphi(P_2) \cdot \varphi(P_1) \end{aligned}$$

If $X^n - 1 = h \cdot g$, then

$$\varphi(X^n - 1) = X^{-n} - 1 = \varphi(h \cdot g) = \varphi(g \cdot h) = \left(\sum_{j=0}^{n-r} X^{-j} h_j\right) \left(\sum_{i=0}^r X^{-i} g_i\right)$$

Therefore in the field $\mathbf{F}_q(X, \theta)$ we get

$$\begin{aligned} X^{n-r} (X^{-n} - 1) X^r &= -(X^n - 1) \\ &= (h_{n-r} + \theta(h_{n-r-1})X + \dots + \theta^{n-r}(h_0)X^{n-r}) \cdot \tilde{g} \end{aligned}$$

where $\tilde{g} \in \mathbf{F}_q[X, \theta]$. This shows that $h_{n-r} + \theta(h_{n-r-1})X + \dots + \theta^{n-r}(h_0)X^{n-r}$ divides $X^n - 1$ in $\mathbf{F}_q[X, \theta]$. \square

Example 19. Consider $\mathbf{F}_4[X, \theta]$ where θ is the Frobenius automorphism and let us denote α a generator of \mathbf{F}_4^* . In $\mathbf{F}_4[X, \theta]$, the polynomial $g = X^2 + \alpha X + \alpha^2$ and the polynomial $h = X^2 + \alpha X + \alpha$ satisfy $g h = X^4 - 1$. The polynomial g^\perp is

$$\theta^2(\alpha)X^2 + \theta(\alpha)X + 1 = \alpha X^2 + \alpha^2 X + 1$$

and from $\alpha^2 g^\perp = g$ we get that the code generated by g in $\mathbf{F}_4[X]/(X^4 - 1)$ is Euclidean self-dual.

We now show that the dual of a central θ -code is not necessarily a central θ -code.

Example 20. Let us consider the example of the [12, 9, 3] central θ -code given in section 1. Using Magma, one can compute the generating matrix of the dual code:

$$G^\perp = \begin{pmatrix} 1 & 0 & 0 & \alpha & \alpha & 0 & \alpha^2 & 0 & \alpha^2 & \alpha & 1 & \alpha \\ 0 & 1 & 0 & 1 & \alpha & \alpha^2 & \alpha & \alpha & \alpha & \alpha^2 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & \alpha^2 & 0 & \alpha^2 & 1 & \alpha & 1 & 1 \end{pmatrix}$$

The word $a = (0, \dots, 0, 1) G^\perp$ is represented by the polynomial $a(X) = X^2 + X^3 + \alpha^2 X^5 + \alpha^2 X^7 + X^8 + \alpha X^9 + X^{10} + X^{11} = (1 + X + \alpha^2 X^3 + \alpha^2 X^5 + X^6 + \alpha X^7 + X^8 + X^9) X^2$. As $\theta^2 = Id$, the polynomial $a(X)$ can also be written $a(X) = X^2 g^\perp(X)$ where

$$g^\perp(X) = 1 + X + \alpha^2 X^3 + \alpha^2 X^5 + X^6 + \alpha X^7 + X^8 + X^9$$

The code C^\perp is a $[12, 3]$ code, but the polynomial g^\perp , which is monic of degree 9, is not a right divisor of a central polynomial of degree 12, so the code C^\perp cannot be a central θ -code.

Furthermore, to complete this example, one can compute the bound of the polynomial g^\perp from the following factorization :

$$g^\perp = (X + \alpha^2)(X + \alpha)(X + 1)(X + \alpha)(X + \alpha)(X + 1)(X^3 + X^2 + \alpha X + 1)$$

Indeed the polynomial g^\perp divides to the right the polynomial

$$\tilde{g} = (X^2 + 1)^6 (X^3 + X + 1)^2 = X^{18} + X^{12} + X^8 + X^4 + X^2 + 1$$

whose degree is 18 and one can check that g^\perp divides no factor of \tilde{g} of degree < 18 , so \tilde{g} is the bound of g^\perp .

4. Computation of Euclidean self-dual θ -cyclic codes over \mathbf{F}_4

The generalization to \mathbf{F}_q of the method we now present for \mathbf{F}_4 is straightforward. Our goal is to compute all Euclidean self-dual θ -cyclic codes of length $n \leq 40$ over $\mathbf{F}_4[X, \theta]$ where θ is the Frobenius automorphism. We need to find all skew polynomials g such that $X^n - 1 = h \cdot g$ and such that the θ -cyclic code $C = (g)/(X^n - 1)$ is self-dual. Corollary 18 allows to express the coefficients of the generating polynomial g^\perp of C^\perp in terms of the coefficients of h . For C to be self-dual, g^\perp and g must differ by a constant multiple. This allows to express the coefficients of h in terms of the coefficients of g . Equating the coefficients of $X^n - 1 - (h \cdot g) = 0$ to zero, produces a (commutative) polynomial system of equations over \mathbf{F}_4 for the coefficients of all skew polynomials g for which $C = C^\perp$. All possible generators g of Euclidean self-dual θ -cyclic codes of given length can then be determined by computing a Groebner bases for this polynomial system in Magma.

In order to derive this polynomial system explicitly, suppose that $g = \sum_{i=0}^{r-1} g_i X^i + X^r$ with $g_0 \neq 0$ is the generator polynomial of a self-dual θ -cyclic code with length $n = 2r$. Let $h = X^r + \sum_{i=0}^{r-1} h_i X^i$ such that $gh = X^n - 1$. According to corollary 18, the code C^\perp is generated by $g^\perp = 1 + \sum_{i=1}^r \theta^i(h_{r-i})X^i$. As $C = C^\perp$, g^\perp is a constant multiple of g , namely $g^\perp = \theta^r(h_0)g$. Comparing coefficients of both polynomials, we get

$$\begin{cases} 1 &= \theta^r(h_0) \cdot g_0 \\ \theta^i(h_{r-i}) &= \theta^r(h_0) \cdot g_i, \text{ for } i = 0, \dots, r-1 \end{cases}$$

Since the Frobenius automorphism θ of \mathbf{F}_4 is of order two, we have $\theta = \theta^{-1}$. Using also that $g_0 \neq 0$ and $g_0 \in \mathbf{F}_4$ implies $g_0^{-1} = g_0^2$ we obtain

$$\begin{cases} h_0 &= \theta^r(g_0^2) \\ h_{r-i} &= \theta^i(g_0^2 \cdot g_i), \text{ for } i = 0, \dots, r-1 \end{cases}$$

This leads to the following expression for h

$$h = \theta^r(g_0^2) + \sum_{i=1}^r \theta^{r-i}(g_0^2) \theta^{r-i}(g_{r-i}) X^i$$

Using that $\theta^i(a) = a^{2^i \bmod 3}$, we can replace expressions involving θ^i by powers of g_i of degree ≤ 4 :

$$h = g_0^{(2^{r+1} \bmod 3)} + \sum_{i=1}^r g_0^{(2^{r-i+1} \bmod 3)} g_{r-i}^{(2^{r-i} \bmod 3)} X^i \quad (1)$$

Expanding the skew product

$$(X^n - 1) - (h \cdot g) = 0$$

and using the rule $X^i a = a^{2^i \bmod 3} X^i$, we obtain $2r + 1$ polynomial equations in the coefficients g_i of degree less than 4 in each variable. Since we seek solutions g_i in \mathbf{F}_4 , we add the r equations $g_i^4 - g_i = 0$ to these equations. This leads to a system of $3r + 1$ polynomial equations in r variables of degree ≤ 4 in each variable which we solve using Groebner bases in Magma. Clearly the solution set must be finite. For each polynomial g corresponding to a solution, we compute the linear code which it generates and its minimum Hamming distance.

In the following table (next page), one lists the best Hamming distances of self-dual θ -cyclic codes with length $n \leq 40$. For each n , we give a generator polynomial g of a code with best Hamming distance d . In the fourth column the best known Hamming distance D of linear codes of length n and dimension $n/2$ is given; in the fifth column the previously best known Hamming distance D_s for self-dual codes of length n is given (cf. (Gaborit and Otmani, 2002)). In the two last columns we give the number n_d of θ -cyclic codes with minimum Hamming distance d and the number E_d of classes of codes which are equivalent (by permutation).

We notice that we always reach the best known Hamming distances of self-dual codes over \mathbf{F}_4 except when $n \in \{16, 24, 32\}$ (and we do not give a generator polynomial in these cases). Furthermore, we improve the best known Hamming distance for self-dual codes of length 36 which was 10. Indeed our best self-dual $[36, 18]$ θ -cyclic codes have Hamming distance 11. There are 36 such codes which are classified in three classes of equivalent codes. Here are the generator polynomials of three non equivalent $[36, 18, 11]$ self-dual θ -cyclic codes:

$$\begin{aligned} & X^{18} + X^{16} + \alpha^2 X^{15} + \alpha X^{14} + \alpha^2 X^{13} + X^{12} + \alpha X^{10} + \alpha X^9 + \alpha X^8 + \alpha^2 X^6 + X^5 + \alpha X^4 + \\ & \quad X^3 + \alpha^2 X^2 + \alpha^2, \\ & X^{18} + \alpha X^{17} + \alpha^2 X^{16} + \alpha^2 X^{15} + X^{14} + X^{13} + \alpha^2 X^{12} + X^{10} + \alpha X^9 + \alpha^2 X^8 + X^6 + \alpha^2 X^5 + \\ & \quad \alpha^2 X^4 + X^3 + X^2 + \alpha X + \alpha^2, \\ & X^{18} + \alpha^2 X^{17} + \alpha X^{16} + \alpha^2 X^{15} + \alpha^2 X^{14} + X^{13} + \alpha^2 X^{12} + \alpha^2 X^{11} + \alpha^2 X^{10} + X^8 + X^7 + \\ & \quad X^6 + \alpha^2 X^5 + X^4 + X^3 + \alpha X^2 + X + \alpha^2. \end{aligned}$$

The computation of all the $[36, 18]$ self-dual θ -cyclic codes required the resolution of a system of 55 polynomial equations over \mathbf{F}_4 of degree ≤ 4 in each of the 18 variables. A search for these codes by testing all skew polynomials of degree 18 would be much

more costly. Indeed there are $2^{36} \sim 10^{10}$ skew polynomials of degree 18 and for each such polynomial one would have to use the command `IsSelfDual` of Magma in order to test if the corresponding code is self-dual. The technique using Groebner basis that we used offers a much more efficient tool to get all self-dual codes of a given length. The computation of all the self-dual codes of length ≤ 40 over \mathbf{F}_4 using Magma took a total CPU time of 105804.279 seconds (30 hours) and a memory usage of 1511.38 MB.

n	g	d	D	D_s	n_d	E_d
4	$X^2 + \alpha^2 X + \alpha$	3	3	3	2	1
6	$X^3 + \alpha X^2 + \alpha X + 1$	3	4	3	2	1
8	$X^4 + \alpha^2 X^3 + \alpha^2 X^2 + \alpha^2 X + \alpha$	4	4	4	2	1
10	$X^5 + X^4 + \alpha X^3 + \alpha X^2 + X + 1$	4	5	4	4	1
12	$X^6 + X^5 + \alpha^2 X^4 + X^3 + \alpha X^2 + X + 1$	6	6	6	4	1
14	$X^7 + X^5 + \alpha X^4 + \alpha X^3 + X^2 + 1$	6	7	6	2	1
16	...	4	7	6	2	1
18	$X^9 + \alpha X^6 + X^5 + X^4 + \alpha X^3 + 1$	6	8	6	12	2
20	$X^{10} + \alpha^2 X^9 + \alpha X^8 + X^7 + X^6 + X^4 + X^3 + \alpha^2 X^2 + \alpha X + 1$	8	8	8	8	1
22	$X^{11} + X^8 + X^7 + \alpha X^6 + \alpha X^5 + X^4 + X^3 + 1$	8	8	8	10	1
24	...	7	9	8	16	2
26	$X^{13} + X^{10} + \alpha^2 X^8 + \alpha X^7 + \alpha X^6 + \alpha^2 X^5 + X^3 + 1$	8	10	8	36	3
28	$X^{14} + X^{11} + X^{10} + X^9 + \alpha^2 X^8 + X^7 + \alpha X^6 + X^5 + X^4 + X^3 + 1$	9	11	9	32	4
30	$X^{15} + \alpha X^{12} + X^{11} + \alpha^2 X^{10} + \alpha^2 X^9 + X^8 + X^7 + \alpha^2 X^6 + \alpha^2 X^5 + X^4 + \alpha X^3 + 1$	10	12	10	8	1
32	...	4	10	10	2	1
34	$X^{17} + X^{13} + X^{11} + X^{10} + \alpha X^9 + \alpha X^8 + X^7 + X^6 + X^4 + 1$	10	11	10	96	6
36	(cf. three polynomials above)	11	12	10	36	3
38	$X^{19} + X^{18} + \alpha X^{17} + \alpha X^{15} + X^{14} + \alpha^2 X^{11} + \alpha^2 X^8 + X^5 + \alpha X^4 + \alpha X^2 + X + 1$	11	12	11	36	2
40	$X^{20} + X^{17} + \alpha^2 X^{15} + \alpha X^{14} + \alpha^2 X^{13} + \alpha^2 X^{12} + X^{11} + X^9 + \alpha X^8 + \alpha X^7 + \alpha^2 X^6 + \alpha X^5 + X^3 + 1$	12	12	12	16	1

5. Computation of Hermitian self-dual θ -cyclic codes over \mathbf{F}_4

We compute Hermitian self-dual codes over \mathbf{F}_4 using the same techniques as for Euclidean self-dual codes. For $x, y \in \mathbf{F}_q^n$, we replace the Euclidean scalar product over \mathbf{F}_q^n

$$\langle x, y \rangle = \sum_{i=1}^n x_i \cdot y_i$$

with the Hermitian scalar product :

$$\langle x, y \rangle_H = \sum_{i=1}^n x_i \cdot \theta(y_i)$$

Lemma 21. *Suppose that the order m of θ divides $2r$. Let g and $h = \sum_{i=0}^{r-1} h_i X^i$ be elements of $\mathbf{F}_q[X, \theta]$ such that $h \cdot g = X^{2r} - 1$. The Hermitian dual of the θ -cyclic code generated by g in $\mathbf{F}_q[X, \theta]/(X^{2r} - 1)$ is again a θ -cyclic code and is generated by*

$$g^H = \theta^{m-1}(h_r) + \theta^m(h_{r-1})X + \dots + \theta^{m+r-1}(h_0)X^r.$$

Proof. Let c be a code word, then from Lemma 17 we get that for the generator g^\perp of C^\perp and for all $k \in \{0, \dots, r-1\}$

$$\begin{aligned} 0 &= \langle c(X), X^k g^\perp \rangle \\ &= \sum c_{i+k} \cdot \theta^{i+k}(h_{r-i}) \\ &= \sum c_{i+k} \cdot \theta(\theta^{i+m-1+k}(h_{r-i})) \quad (\text{because } \theta^m = Id) \\ &= \langle c(X), X^k g^H \rangle_H \end{aligned}$$

In order to prove that the Hermitian dual is again a θ -cyclic code, we need to show that g^H is a right factor of $X^{2r} - 1$. We consider the application $\phi: \mathbf{F}_4[X, \theta] \rightarrow \mathbf{F}_4[X, \theta]$ defined by $\phi(\sum_{i=0}^n a_i X^i) = \sum_{i=0}^n \theta(a_i) X^i$. To verify that ϕ is a morphism we check that $\phi(Xa) = \phi(\theta(a)X) = \theta^2(a)X = X\theta(a) = \phi(X)\phi(a)$. Using that g^\perp is a right divisor of $X^{2r} - 1$ (cf. Corollary 18) we obtain

$$X^{2r} - 1 = \phi(X^{2r} - 1) = \phi(\tilde{h} \cdot g^\perp) = \phi(\tilde{h}) \cdot \phi(g^\perp).$$

Now the result follows from $\phi^{m-1}(g^\perp) = g^H$. \square

The method is again based on a Gröbner basis computation. Following the same computations as in the previous section, the polynomial h of an Hermitian self-dual code over $\mathbf{F}_4[X, \theta]$ is

$$h = X^r + \sum_{i=1}^{r-1} (\theta^{r-i+1}(g_0^2) \theta^{r-i+1}(g_{r-i}) X^i) + \theta^{r+1}(g_0^2)$$

(we have just shifted the coefficients of (1) by $\theta^{m-1} = \theta$). The relation $X^{2r} - 1 = gh$ gives again a polynomial system of equations that we solve using Groebner bases.

In the following table, one lists the best Hamming distances of Hermitian self-dual θ -cyclic codes with length $n \leq 40$. For each n , we give the best Hamming distance d , the best known Hamming distance D_s for Hermitian self-dual codes of length n (cf. (Gaborit and Otmani, 2002)) and the number E_d of classes of Hermitian self-dual codes which are equivalent (by permutation) with best distance d . When $d = D_s$, we give an exemple of a generator polynomial g of a code with such a distance.

n	g	d	D_s	E_d
4	$X^2 + 1$	2	2	1
6	$X^3 + \alpha^2 X^2 + \alpha X + 1$	4	4	1
8	...	2	4	1
10	$X^5 + X^4 + \alpha^2 X^3 + \alpha X^2 + X + 1$	4	4	2
12	$X^6 + X^5 + \alpha X^4 + \alpha X^2 + X + 1$	4	4	1
14	...	6	8	1
16	...	2	8	1
18	...	6	8	3
20	...	6	8	1
22	$X^{11} + X^8 + X^7 + \alpha^2 X^6 + \alpha X^5 + X^4 + X^3 + 1$	8	8	2
24	...	6	8	2
26	$X^{13} + X^{10} + X^8 + \alpha^2 X^7 + \alpha X^6 + X^5 + X^3 + 1$	8	8-10	5
28	$X^{14} + X^{11} + X^{10} + X^9 + \alpha X^8 +$ $\alpha X^6 + X^5 + X^4 + X^3 + 1$	10	10	2
30	$X^{15} + X^{13} + \alpha^2 X^{12} + \alpha X^{11} + \alpha^2 X^{10} + \alpha X^8 +$ $\alpha^2 X^7 + \alpha X^5 + \alpha^2 X^4 + \alpha X^3 + X^2 + 1$	12	12	1
32	...	2	10-12	1
34	$X^{17} + X^{13} + X^{11} + X^{10} + \alpha^2 X^9 +$ $\alpha X^8 + X^7 + X^6 + X^4 + 1$	10	10-12	14
36	...	10	12-14	6
38	$X^{19} + X^{15} + \alpha^2 X^{14} + X^{13} + \alpha X^{11} +$ $\alpha X^{10} + \alpha^2 X^9 + \alpha^2 X^8 + X^6 + \alpha X^5 + X^4 + 1$	12	12-14	4
40	...	10	12-14	3

References

- Berrick, A., Keating, M., 2000. An introduction to rings and modules. Cambridge Studies in Advanced Mathematics 65, Cambridge University Press.
- Bosma, W., Cannon, J., Playoust, C., 1997. The magma algebra system i: The user language. *Journal of Symbolic Computation* 24, 235–265.
- Boucher, D., Geiselmann, W., Ulmer, F., 2007. Skew cyclic codes. *Applied Algebra in Engineering, Communication and Computing* 18, 379–389.
- Bronstein, M., Petkovsek, M., 1994. On ore rings, linear operators and factorisation. *Programming and Computer Software* 20, 14–18.
- Cohn, P., 1971. Free rings and their relations. Academic Press Inc.
- Gabidulin, E., 1985. Theory of codes with maximum rank distance. *Probl. Peredach. Inform.* 21, 3–16 (in Russian; pp. 1–12 in the English translation).
- Gaborit, P., Otmani, A., 2002. Tables of Euclidian and Hermitian self-dual codes over $GF(4)$.
http://www.unilim.fr/pages_perso/philippe.gaborit/SD/
- Jacobson, N., 1943. The theory of rings. Publication of the AMS.
- McDonald, B., 1974. Finite rings with identity. Marcel Dekker Inc.
- Ore, O., 1933. Theory of non-commutative polynomials. *Ann. of Math.* 34.
- Singer, M., 1996. Testing reducibility of linear differential operators: A group theoretic perspective. *Applied Algebra in Engineering, Communication and Computing* 7, 77–104.