An Overview on Skew Constacyclic Codes and their Subclass of LCD Codes

Aicha Batoul, Delphine Boucher, Ranya D Boulanouar

An overview on skew constacyclic codes and their subclass of LCD codes.

Aicha Batoul [*], Delphine Boucher [†] and Ranya D.Boulanouar [‡]

Abstract

This paper is about a first characterization of LCD skew constacyclic codes and some constructions of LCD skew cyclic and skew negacyclic codes over $\mathbb{F}_{p^2}$.

Keywords Skew polynomial rings, skew constacyclic codes, LCD codes, MDS codes

1 Introduction

One of the most active and important research areas in noncommutative algebra is the investigation of skew polynomial rings. Recently they have been successfully applied in many areas and specially in coding theory. The principal motivation for studying codes in this setting is that polynomials in skew polynomials rings exhibit many factorizations and hence there are many more ideals in a skew polynomial ring than in the commutative case. The research on codes in this setting has resulted in the discovery of many new codes with better Hamming minimum distances than any previously linear code with the same parameters. Some of them were given in [3, 4, 5, 6, 7, 8].

On the other hand, constacyclic codes over finite fields is an important class of linear codes as it includes the well-known family of cyclic codes. They also have many practical applications as they can be efficiently encoded using simple shift registers. Further, they have a rich algebraic structure which can be used for efficient error detection and correction.

Linear complementary dual (LCD) codes, were introduced by Massey [17]. They provide an optimum linear coding solution for the two-user binary adder channel, and in [18] it was shown that asymptotically good LCD codes exist. Since then, several authors have studied these codes ([9, 12, 14, 15, 23]). But until now just a few works have been done on LCD codes in the noncommutative case.

This article is organized as follows. In Section 2, some preliminaries are given about skew constacyclic codes over finite fields and skew polynomial rings. In Section 3, conditions for the equivalency between skew constacyclic codes, skew cyclic codes and skew negacyclic codes are provided. We give examples of skew cyclic codes which are not equivalent to any skew negacyclic codes in the case when the length is even. In Section 4, the notion of LCD skew constacyclic codes is introduced and we give some characterizations of their skew generator polynomials. Section 5 focuses on the construction and enumeration of LCD skew cyclic and negacyclic codes over $\mathbb{F}_{p^2}$. If p is odd, the Euclidean LCD θ-cyclic codes of length $2p^s$ and dimension p^s over $\mathbb{F}_{p^2}$ are all Hermitian LCD codes. All MDS LCD skew codes of length ≤ 16 over $\mathbb{F}_{p^2}$ for $p \in \{3, 5, 7\}$ are obtained and the results are presented in tables.

[*]Faculty of Mathematics, University of Science and Technology Houari Boumedienne (USTHB) 16111 Bab Ezzouar, Algiers, Algeria

[†]Univ Rennes, CNRS, IRMAR - UMR 6625, F-35000 Rennes, France

[‡]Faculty of Mathematics, University of Science and Technology Houari Boumedienne (USTHB) 16111 Bab Ezzouar, Algiers, Algeria

2 Preliminaries

Let q be a prime power, $\mathbb{F}_q$ a finite field and θ an automorphism of $\mathbb{F}_q$. We define the skew polynomial ring R as

$$R = \mathbb{F}_q[x;\theta] = \{a_0 + a_1x + \ldots + a_{n-1}x^{n-1} \mid a_i \in \mathbb{F}_q \text{ and } n \in \mathbb{N}\}$$

under usual addition of polynomials and where multiplication is defined using the rule $\forall a \in \mathbb{F}_q, x \cdot a = \theta(a)x$. The ring R is noncommutative unless θ is the identity automorphism on $\mathbb{F}_q$. According to [20], an element $f \in R$ is central if and only if f is in $\mathbb{F}_q^{\theta}[x^{\mu}]$ where μ is the order of the automorphism θ and $\mathbb{F}_q^{\theta}$ is the fixed field of θ. The two-sided ideals of R are generated by elements having the form $(c_0 + c_1x^{\mu} + \ldots + c_nx^{n\mu})x^l$, where l is an integer. Central elements of R are the generators of two-sided ideals in R [6]. The ring R is Euclidean on the right : the division on the right is defined as follows. Let f and g be in R with $f \neq 0$. Then there exist unique skew polynomials q and r such that

$$g = q \cdot f + r \quad deg(r) < deg(f).$$

If $r = 0$ then f is a right divisor of g in R ([20]). There exists greatest common right divisors (gcrd) and least common left multiples (lclm). The ring R is also Euclidean on the left : there exist a division on the left, greatest common left divisors (gcld) as well as least common right multiples (lcrm).

In what follows, we consider a positive integer n and a constant λ in $\mathbb{F}_q^*$. We assume that n is a multiple of the order of θ and λ fixed by θ, which means that $x^n - \lambda$ is central.

According to [[6], [10]], a linear code C of length n over $\mathbb{F}_q$ is said to be (θ, λ)**-constacyclic** or **skew** λ**-constacyclic** if it satisfies

$$\forall c \in C, c = (c_0, c_1, \ldots, c_{n-1}) \in C \Rightarrow (\lambda\theta(c_{n-1}), \theta(c_0), \ldots, \theta(c_{n-2})) \in C.$$

Any element of the quotient algebra $R/\langle x^n - \lambda\rangle$ is uniquely represented by a polynomial $\beta_0 + \beta_1x + \ldots + \beta_{n-1}x^{n-1}$ of degree less than n, hence is identified with a word $(\beta_0, \beta_1, \ldots, \beta_{n-1})$ of length n over $\mathbb{F}_q$.

In this way, any skew λ-constacyclic code C of length n over $\mathbb{F}_q$ is identified with exactly one left ideal of the quotient algebra $R/\langle x^n - \lambda\rangle$, which is generated by a right divisor g of $x^n - \lambda$. In that case, g is called a **skew generator polynomial** of C and we will denote $C =< g >_n$.

Note that the skew 1-constacyclic codes are skew cyclic codes and the skew -1-constacyclic codes are skew negacyclic codes.

The **Hamming weight** $wt(y)$ of an n-tuple $y = (y_l, y_2 \ldots y_n) \in \mathbb{F}_q^n$ is the number of nonzero entries in y, that is, $wt(y) =\mid \{i : y_i \neq 0\} \mid$. The **minimum distance** of a linear code C is $\min_{c \in C, c \neq 0} wt(c)$.

A $\mathbb{F}_q$-linear transformation $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is a monomial transformation if there exists a permutation σ of $\{1, 2 \ldots n\}$ and nonzero elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ of $\mathbb{F}_q^n$ such that

$$T(y_1, y_2, \ldots, y_n) = (\alpha_1 y_{\sigma(1)}, \alpha_2 y_{\sigma(2)}, \ldots, \alpha_n y_{\sigma(n)})$$

for all $(y_1, y_2 \ldots y_n) \in \mathbb{F}_q^n$. Two linear codes C_1 and C_2 in $\mathbb{F}_q^n$ are **equivalent** if there exists a monomial transformation $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ taking C_1 to C_2 (i.e. there exists a linear Hamming isometry [16]).

The **Euclidean dual** of a linear code C of length n over $\mathbb{F}_q$ is defined as $C^{\perp} = \{x \in \mathbb{F}_q^n \mid \forall y \in C, < x, y >= 0\}$ where for x, y in $\mathbb{F}_q^n$, $< x, y >:= \sum_{i=1}^n x_iy_i$ is the (Euclidean) scalar product of x and y. A linear code is called an **Eulidean LCD** code if $C \oplus C^{\perp} = \mathbb{F}_q^n$, which is equivalent to $C \cap C^{\perp} = \{0\}$.

Assume that $q = r^2$ is an even power of an arbitrary prime and denote for a in $\mathbb{F}_q$, $\overline{a} = a^r$. The **Hermitian dual** of a linear code C of length n over $\mathbb{F}_q$ is defined as $C^{\perp_H} = \{x \in \mathbb{F}_q^n \mid \forall y \in C, < x, y >_H= 0\}$ where for x, y in $\mathbb{F}_q^n$, $< x, y >_H:= \sum_{i=1}^n x_i\overline{y_i}$ is the (Hermitian) scalar product of x and y. The code C is a **Hermitian LCD** code if $C \cap C^{\perp_H} = \{0\}$.

The **skew reciprocal polynomial** of $g = \Sigma_{i=0}^{k} g_i x^i \in R$ of degree k is $g^* = \Sigma_{i=0}^{k} \theta^i(g_{k-i})x^i$. The left monic skew reciprocal polynomial of g is $g^\natural = (1/\theta^k(g_0))g^*$. If a skew polynomial is equal to its left monic skew reciprocal polynomial, then it is called self-reciprocal.

Consider λ in $(\mathbb{F}_q^\theta)^*$ and C a skew λ-constacyclic code of length n and skew generator polynomial g. According to Theorem 1 of [8], the Euclidean dual $C^\perp$ of C is a skew λ^{-1}-constacyclic code generated by $h^\natural$ where $g \cdot h = h \cdot g = x^n - \lambda$. If $q = r^2$, the Hermitian dual $C^{\perp_H}$ of C is generated by $\overline{h^\natural}$ where for $a(x) = \sum a_i x^i \in R$, $\overline{a(x)} = \sum \overline{a_i} x^i$.

The two following lemma will be useful later.

Lemma 1. *[5, Lemma 4] Consider h and g in R. Then $(h \cdot g)^* = \Theta^{\deg(h)}(g^*) \cdot h^*$, where $t = \deg(h)$ and $\Theta : R \mapsto R$ is given by $\Sigma_{i=0}^{k} a_i x^i \mapsto \Sigma_{i=0}^{k} \theta(a_i) x^i$.*

Lemma 2 (Theorem 6.3.7 of [10])**.** *Consider C_1 and C_2 two skew λ-constacyclic code of length n over $\mathbb{F}_q$ with skew generator polynomials g_1 and g_2, then:*

1. *$C_1 \cap C_2$ is a skew λ-constacyclic code of length n generated by $\mathrm{lclm}(g_1, g_2)$.*
2. *$C_1 + C_2$ is a skew λ-constacyclic code of length n generated by $\mathrm{gcrd}(g_1, g_2)$.*

3 The equivalency between skew λ-constacyclic codes, skew cyclic codes and skew negacyclic codes

Let q be a prime power, $\mathbb{F}_q$ a finite field and θ an automorphism of $\mathbb{F}_q$. Consider λ in $\mathbb{F}_q^*$ which is fixed by θ. We assume that n is a multiple of the order of θ. For i in $\mathbb{N}^*$ and α element of $\mathbb{F}_q$ the i^{th} norm is defined as

$$N_i(\alpha) = \alpha\theta(\alpha) \cdots \theta^{i-1}(\alpha).$$

In this section, we provide conditions on the existence of an isomorphism between skew λ-constacyclic codes, skew cyclic codes and skew negacyclic codes. We start with the following useful lemma.

Lemma 3. *Consider an element α of $\mathbb{F}_q^*$. The application*

$$\begin{aligned} \phi_\alpha \ : \ R &\longrightarrow R \\ f(x) &\longmapsto f(\alpha x) \end{aligned}$$

is a morphism. Furthermore for all i in $\mathbb{N}$, $\phi_\alpha(x^i) = N_i(\alpha)x^i$.

Theorem 1.

- *If $\mathbb{F}_q^*$ contains an element α where $\lambda = N_n(\alpha^{-1})$ then the skew λ-constacyclic codes of length n over $\mathbb{F}_q$ are equivalent to the skew cyclic codes of length n over $\mathbb{F}_q$.*
- *If $\mathbb{F}_q^*$ contains an element α where $\lambda = -N_n(\alpha^{-1})$ then the skew λ-constacyclic codes of length n over $\mathbb{F}_q$ are equivalent to the skew negacyclic codes of length n over $\mathbb{F}_q$.*

Proof. Consider α in $\mathbb{F}_q^*$ such that $\lambda = N_n(\alpha^{-1})$. Define

$$\begin{aligned} \Phi_\alpha \ : \ R/\langle x^n - 1\rangle &\longrightarrow R/\langle x^n - \lambda\rangle \\ f(x) &\longmapsto f(\alpha x) \end{aligned}$$

Let us prove that the application Φ_α is an isomorphism who preserves the Hamming weight:

- The application Φ_α is well-defined: consider $f(x)$ and $g(x)$ in R such that $x^n - 1$ divides on the right $f(x) - g(x)$. There exists h in R such that $f(x) - g(x) = h(x) \cdot (x^n - 1)$. By Lemma 3,

  $$f(\alpha x) - g(\alpha x) = \phi_\alpha(h(x)) \cdot \phi_\alpha(x^n - 1) = \phi_\alpha(h(x)) \cdot (N_n(\alpha)x^n - 1) = \phi_\alpha(h(x)) \cdot N_n(\alpha) \cdot (x^n - \lambda).$$

  Therefore, $x^n - \lambda$ divides on the right $f(\alpha x) - g(\alpha x)$.

  In the same way one can prove that the application is injective (and therefore surjective).

- The application Φ_α is a morphism: consider $f(x) = \sum_{i=0}^{n-1} a_i x^i$ and $g(x) = \sum_{i=0}^{n-1} b_i x^i$ in $R/\langle x^n - 1\rangle$

  $$f(x)\cdot g(x) = \sum_{j=0}^{n-1}\left(\sum_{i=0}^{j} a_i\theta^i(b_{j-i}) + \sum_{i=j+1}^{n-1} a_i\theta^i(b_{n-i+j})\right)x^j$$

  because $x^{j+n} = x^j$ in $R/\langle x^n - 1\rangle$.

  As $\Phi_\alpha(x^j) = N_j(\alpha)x^j$, one gets

  $$\Phi_\alpha(f(x)\cdot g(x)) = \sum_{j=0}^{n-1}\left(\sum_{i=0}^{j} a_i\theta^i(b_{j-i}) + \sum_{i=j+1}^{n-1} a_i\theta^i(b_{n-i+j})\right)N_j(\alpha)x^j$$

  Furthermore,

  $\Phi_\alpha(f(x))\cdot\Phi_\alpha(g(x)) =$

  $$\sum_{j=0}^{n-1}\left(\sum_{i=0}^{j} a_i N_i(\alpha)\theta^i(b_{j-i}N_{j-i}(\alpha))\right)x^j + \sum_{j=0}^{n-1}\left(\sum_{i=j+1}^{n-1} a_i N_i(\alpha)\theta^i(b_{n-i+j}N_{n+j-i}(\alpha))\right)x^{j+n}$$

  As $x^{j+n} = x^j\cdot(x^n-\lambda) + x^j\lambda = \theta^j(\lambda)x^j$ in $R/\langle x^n-\lambda\rangle$,

  $\Phi_\alpha(f(x))\cdot\Phi_\alpha(g(x)) =$

  $$\sum_{j=0}^{n-1}\left(\sum_{i=0}^{j} a_i\theta^i(b_{j-i})N_i(\alpha)\theta^i(N_{j-i}(\alpha)) + \sum_{i=j+1}^{n-1} a_i\theta^i(b_{n-i+j})N_i(\alpha)\theta^i(N_{n+j-i}(\alpha))\theta^j(\lambda)\right)x^j$$

  Furthermore $N_i(\alpha)\theta^i(N_{j-i}(\alpha)) = N_j(\alpha)$ and $N_i(\alpha)\theta^i(N_{n+j-i}(\alpha))\theta^j(\lambda) = N_{j+n}(\alpha)/(\theta^j(N_n(\alpha))) = N_j(\alpha)$.

  Therefore

  $$\Phi_\alpha(f(x))\cdot\Phi_\alpha(g(x)) = \sum_{j=0}^{n-1}\left(\sum_{i=0}^{j} a_i\theta^i(b_{j-i}) + \sum_{i=j+1}^{n-1} a_i\theta^i(b_{n-i+j})\right)N_j(\alpha)x^j = \Phi_\alpha(f(x)\cdot g(x)).$$

- Φ_α preserves the Hamming weight:

  Consider $c(x) = \sum_{i=0}^{n-1} a_i x^i$, then $\Phi_\alpha(c(x)) = \sum_{i=0}^{n-1} a_i N_i(\alpha)x^i$.

  $\forall i \in \{0,\ldots,n-1\}, a_iN_i(\alpha) = 0 \Leftrightarrow a_i = 0$ (because $\mathbb{F}_q$ integral domain), therefore $wt(c(x)) = wt(\Phi_\alpha(c(x)))$.

□

Example 1. *For $\mathbb{F}_{2^4} = \mathbb{F}_2(w)$ where $w^4 = w+1$, θ is the automorphism of $\mathbb{F}_{2^4}$ given by $a \mapsto a^{2^2}$ and $\mathbb{F}_{2^4}^\theta = \mathbb{F}_4 = \{0, 1, w^5, w^{10}\}$.*

We have 33 skew cyclic codes of length 4 over $\mathbb{F}_{16}$,we give some of them:

$$\begin{aligned} x^4 - 1 &= (x^2 + w^{13}x + w^9)(x^2 + w^{13}x + w^6) \\ &= (x + w^{12})(x^3 + w^3x^2 + x + w^3) \end{aligned}$$

All of the [4]-th roots of w^5 are $\{w^2, w^5, w^8, w^{11}, w^{14}\}$.

All of the [4]-th roots of w^{10} are $\{w, w^4, w^7, w^{10}, w^{13}\}$.

The table 1 below gives examples of skew w^5-constacyclic codes of length 4 over $\mathbb{F}_{16}$ who are equivalent to the skew cyclic code $C = \langle x^2 + w^{13}x + w^6\rangle$ of length 4 over $\mathbb{F}_{16}$.

The table 2 below gives examples of skew w^{10}-constacyclic codes of length 4 over $\mathbb{F}_{16}$ who are equivalent to the skew cyclic code $C = \langle x^3 + w^3x^2 + x + w^3\rangle$ of length 4 over $\mathbb{F}_{16}$.

In the following, we give a relationship between skew cyclic codes and skew negacyclic codes.

δ	$g(x)$	d
w^2	$x^2 + w^6x + w$	3
w^5	$x^2 + w^3x + w$	3
w^8	$x^2 + x + w$	3
w^{11}	$x^2 + w^{12}x + w$	3
w^{14}	$x^2 + w^9x + w$	3

Table 1: Some skew w^5-constacyclic codes of length 4 over $\mathbb{F}_{16}$

δ	g(x)	d
w	$x^3 + w^4x^2 + w^5x + w^9$	4
w^4	$x^3 + w^7x^2 + w^5x + w^{12}$	4
w^7	$x^3 + w^{10}x^2 + w^5x + 1$	4
w^{10}	$x^3 + w^{13}x^2 + w^5x + w^3$	4
w^{13}	$x^3 + wx^2 + w^5x + w^6$	4

Table 2: Some skew w^{10}-constacyclic code of length 4 over $\mathbb{F}_{16}$

Corollary 1. *If q is odd and n is an odd integer then the skew cyclic codes of length n over $\mathbb{F}_q$ are equivalent to the skew negacyclic codes of length n over $\mathbb{F}_q$.*

Proof. Consider α in $\mathbb{F}_q^*$ such that $\lambda = N_n(\alpha^{-1}) \neq 1$. As n is odd, $\lambda = -N_n(-\alpha^{-1})$ and we conclude with Theorem 1. □

In the following example, we show that not all a skew cyclic codes of length n over $\mathbb{F}_q$ are equivalent to a skew negacyclic code of length n over $\mathbb{F}_q$, when n is even.

Example 2. *Let $\mathbb{F}_9 = \mathbb{F}_3(w)$ where $w^2 = w + 1$, θ the Frobenius automorphism. Let the skew cyclic code $C = \langle x^3 + x^2 + x + 1\rangle$ over $\mathbb{F}_9$ with parameter $[4, 1, 4]$. There is no skew negacyclic code of length 4 equivalent to C (because there is no skew negacyclic code of length 4 with minimum distance 4).*

In the following we give a case where the skew constacyclic codes are equivalent to the skew cyclic codes using only a relation between the length n, the characteristic of $\mathbb{F}_q$ and the cardinality of $\mathbb{F}_q$. We start with the following useful lemma.

Lemma 4. *[2, Lemma 3.1] Let α be a primitive element of $\mathbb{F}_q$ and $\lambda = \alpha^i$ for $i \leqslant q - 1$. Then the equation $x^s = \lambda$ has a solution in $\mathbb{F}_q$ if and only if $(s, q - 1) \mid i$.*

In the following, we give a similar result of [2, Theorem 3.4] but in the noncommutative case.

Proposition 1. *Assume that θ is the automorphism defined by $a \mapsto a^{p^r}$ and that $([n], q - 1) = 1$ where $[n] := \frac{p^{rn}-1}{p^r-1}$. Then all skew λ-constacyclic codes of length n over $\mathbb{F}_q$ are equivalent to skew cyclic codes of length n over $\mathbb{F}_q$.*

Proof. Let λ in $\mathbb{F}_q^*$ fixed by θ then there exist i such that $\lambda = \alpha^i$. As $([n], q-1) = 1 \mid i$, according to Lemma 4, there exist δ in $\mathbb{F}_q^*$ such that $\lambda = \delta^{[n]}$. Furthermore $N_n(\delta) = \delta^{[n]}$, therefore by Theorem 1 skew λ-constacyclic codes of length n over $\mathbb{F}_q$ are equivalent to skew cyclic codes of length n over $\mathbb{F}_q$. □

When θ is the Frobenius and $\mathbb{F}_q = \mathbb{F}_{p^n}$, θ-cyclic codes of length n are equivalent to θ-negacyclic codes of length n :

Proposition 2. *Assume that θ is the automorphism defined by $a \mapsto a^p$ and that $q = p^n$. Then all skew negacyclic codes of length n over $\mathbb{F}_q$ are equivalent to skew cyclic codes of length n over $\mathbb{F}_q$.*

Proof. According to Theorem 1, it suffices to prove that the equation $N_n(\alpha) = -1$ has a solution in $\mathbb{F}_q^*$. Consider a a primitive element of $\mathbb{F}_q$, then $-1 = a^{\frac{p^n-1}{2}}$, furthermore $(\frac{p^n-1}{p-1}, p^n-1) = \frac{p^n-1}{p-1}$ divides $\frac{p^n-1}{2}$, therefore according to Lemma 4, the equation $N_n(\alpha) = \alpha^{\frac{p^n-1}{p-1}} = -1$ has a solution in $\mathbb{F}_q^*$. □

The previous isometry of Theorem 1 does not preserve the duality as shown in the following example.

Example 3. *Consider $R = \mathbb{F}_9[x;\theta]$ where $\theta : u \mapsto u^3$ and $a \in \mathbb{F}_9$ such that $a^2 = a + 1$. The application*

$$\Phi_a : \begin{cases} R/ < x^2 - 1 > & \to & R/ < x^2 + 1 > \\ x & \mapsto & ax \end{cases}$$

is an isomorphism which preserves the Hamming distance according to Theorem 1 (because $-1 = a^4 = N_2(a)$). However it does not preserve the duality. Namely, consider the skew cyclic code C generated by $g = x + a^2$. As $\Phi_a(g) = ax + a^2 = a(x + a)$, the image D of C by Φ_a is generated by $x + a$. Now we have $(x + a^2) \cdot (x + a^2) = x^2 - 1$, therefore the dual $C^\perp$ of C is generated by $(x + a^2)^\natural = x + 1/a^6 = x + a^2$ (and C is self-dual). The image of $C^\perp$ by Φ_a is generated by $x + a$. Now, we have $(x + a^7) \cdot (x + a) = x^2 + 1$, therefore the dual $D^\perp$ of D is generated by $(x + a^7)^\natural = x + a^3$. We obtain that $D^\perp \neq \Phi_a(C^\perp)$ (and $D = \Phi_a(C)$ is not self-dual whereas C is self-dual).

Lemma 5. *If n is odd and $h \in R$ with degree k, then $\phi_{-1}(h^*) = (-1)^k \phi_{-1}(h)^*$.*

Proof. Consider $h = \sum_{i=0}^k h_i X^i$ with degree k, then $h^* = \sum_{i=0}^k X^{k-i} \cdot h_i$. As ϕ_α is a morphism, one gets

$$\phi_\alpha(h^*) = \sum_{i=0}^{k} N_{k-i}(\alpha) X^{k-i} \cdot h_i.$$

Now the skew reciprocal polynomial of $\phi_\alpha(h) = \sum_{i=0}^k h_i N_i(\alpha) X^i$ is equal to $\phi_\alpha(h)^* = \sum_{i=0}^k X^{k-i} \cdot (h_i N_i(\alpha)) = \sum_{i=0}^k \theta^{k-i}(N_i(\alpha)) X^{k-i} \cdot h_i$ therefore

$$\phi_\alpha(h)^* = N_k(\alpha) \sum_{i=0}^{k} 1/N_{k-i}(\alpha) X^{k-i} \cdot h_i.$$

If $\alpha = -1$, then $N_{k-i}(\alpha)^2 = 1$, therefore $\phi_\alpha(h)^* = (-1)^k \phi_\alpha(h^*)$. □

Proposition 3. *If n is odd and C is a skew cyclic code of length n then the dual of the skew negacyclic code $\Phi_{-1}(C)$ is $\Phi_{-1}(C)^\perp = \Phi_{-1}(C^\perp)$*

Proof. As n is odd, $N_n(-1) = -1$, therefore according to Theorem 1, Φ_{-1} is well defined and is an isometry. Consider C a skew cyclic code $[n, k]$ with generator skew polynomial g and consider h in R such that $x^n - 1 = g \cdot h = h \cdot g$. Then the skew generator polynomial of $D = \Phi_{-1}(C)$ is generated by $G = (-1)^r \Phi_{-1}(g)$ where $r = \deg(g) = n - k$. Furthermore $G \cdot H = H \cdot G = x^n + 1$ where $H = (-1)^{r+1} \Phi_{-1}(h)$. The dual $D^\perp$ of D is generated by H^* and the conclusion follows from Lemma 5. □

In what follows, we will study LCD skew cyclic and skew negacyclic codes. We will mostly concentrate on the case when the length of the code is even and the automorphism θ has order 2.

4 Skew generator polynomials of LCD skew cyclic and negacyclic codes

Like previously, we assume that $\mathbb{F}_q$ is a finite field, θ is an automorphism of $\mathbb{F}_q$ of order μ and n is a multiple of μ. In the following, we give a necessary and sufficient condition for skew λ-constacyclic codes to be LCD codes, when $\lambda^2 = 1$.

Theorem 2. *Consider $\mathbb{F}_q$ a finite field, θ an automorphism of $\mathbb{F}_q$ of order μ, $R = \mathbb{F}_q[x;\theta]$, n a multiple of μ and $\lambda \in \{-1, 1\}$. Consider a (θ, λ)-constacyclic code C with length n, skew generator polynomial g. Consider h such that $h \cdot g = g \cdot h = x^n - \lambda$.*

1. *C is an Euclidean LCD code if and only if $\mathrm{gcrd}(g, h^\natural) = 1$.*
2. *If q is an even power of a prime number, $q = r^2$, C is an Hermitian LCD code if and only if $\mathrm{gcrd}(g, \overline{h^\natural}) = 1$.*

Proof. As C and $C^\perp$ are two skew λ-constacyclic codes of length n and skew generator polynomials g and $h^\natural$, according to Lemma 2, the skew polynomial $f = \mathrm{lclm}(g, h^\natural)$ is the skew generator polynomial of the skew constacyclic code $C \cap C^\perp$. In particular, as g and $h^\natural$ both divide $x^n - \lambda$, f divides $x^n - \lambda$. Assume that $C \cap C^\perp = \{0\}$, then $x^n - \lambda$ divides f, therefore $x^n - \lambda = f$. According to [22], $\deg(\mathrm{gcrd}(g, h^\natural)) + \deg(\mathrm{lclm}(g, h^\natural)) = \deg(g) + \deg(h^\natural)$, therefore $\deg(\mathrm{gcrd}(g, h^\natural)) = \deg(g) + \deg(h) - \deg(f) = 0$ and $\mathrm{gcrd}(g, h^\natural) = 1$.

Conversely, if $\mathrm{gcrd}(g, h^\natural) = 1$, then $\deg(f) = n$, therefore, as f divides $x^n - \lambda$, $f = x^n - \lambda$, and $C \cap C^\perp = \{0\}$. The same proof holds for Hermitian LCD codes. □

Example 4. *Consider $\mathbb{F}_9 = \mathbb{F}_3(w)$ where $w^2 = w + 1$ and θ the Frobenius automorphism $\theta : a \mapsto a^3$. One has :*

$$x^4 + 1 = (x^2 + w^3x + 1) \cdot (x^2 + w^7x + 1).$$

The skew reciprocal polynomial of x^2+w^3x+1 is x^2+wx+1 and $\mathrm{gcrd}(x^2+w^7x+1, x^2+wx+1) = 1$.

Then by Theorem 2 the skew negacyclic code $C = \langle x^2 + w^7x + 1\rangle$ of length 4 and minimum distance 3 over $\mathbb{F}_9$ is an Euclidean LCD code.

Example 5. *For $\mathbb{F}_9 = \mathbb{F}_3(w)$ where $w^2 = w + 1$ and θ the Frobenius automorphism $\theta : a \mapsto a^3$, one has :*

$$x^6 - 1 = (x^3 + wx^2 + x + 1) \cdot (x^3 + w^7x^2 + x + 2).$$

The skew reciprocal polynomial of $x^3 + wx^2 + x + 1$ is $x^3 + x^2 + w^3x + 1$ and $\mathrm{gcrd}(x^3 + w^7x^2 + x + 2, x^3 + x^2 + wx + 1) = 1$.

Then by Theorem 2 the skew cyclic code $C = \langle x^3 + w^7x^2 + x + 2\rangle$ of length 6 and minimum distance 4 over $\mathbb{F}_9$ is an Hermitian LCD code.

Over a finite field $\mathbb{F}_q$, if a cyclic code C generated by a monic polynomial g is an Euclidean LCD code then $g = g^\natural$. Furthermore if q is coprime with n, then $g = g^\natural$ if and only if C is an Euclidean LCD code ([17], [19]). This comes from the fact that when q is coprime with n then $x^n - 1 = gh = ppcm(g, h)$ is squarefree therefore, if $g = g^\natural$, then g and $h = h^\natural$ are coprime.

The following proposition generalizes this result. We use the notion of similarity (definition 1).

Definition 1 ([22])**.** *Consider a, b in R. a is* **similar** *to b if there exists u in R such that $\mathrm{lclm}(a, u) = b \cdot u$ and $\mathrm{gcrd}(a, u) = 1$.*

Remark 1. *If θ is the identity then a is similar to b if and only if a is equal to b up to a multiple constant.*

Proposition 4. *Consider $\mathbb{F}_q$ a finite field, θ an automorphism of $\mathbb{F}_q$ of order μ, $R = \mathbb{F}_q[x;\theta]$, n a multiple of μ and $\lambda \in \{-1, 1\}$. Consider a (θ, λ)-constacyclic code C with dimension k, length n, skew generator polynomial g. Consider $G = \Theta^k(g^* \cdot \frac{1}{g_0}) = g_0 \cdot \Theta^k(g^\natural \cdot \frac{1}{g_0})$ where g_0 is the constant coefficient of g and h in R such that $g \cdot h = h \cdot g = x^n - \lambda$.*

1. *If C is an Euclidean (resp. Hermitian) LCD code then g is similar to G (resp. $\Theta(G)$).*
2. *Assume that $\mathrm{lclm}(g, h) = x^n - 1$. If $g = G$ (resp. $g = \Theta(G)$) then C is an Euclidean (resp. Hermitian) LCD code.*

Proof. As $h \cdot g = x^n - \lambda$, according to Lemma 1, $x^n - \lambda = g_0 \cdot \Theta^k(g^\natural \cdot \frac{1}{g_0}) \cdot h^\natural = G \cdot h^\natural$. Therefore, as g and $h^\natural$ divide on the right $x^n - \lambda$, $\mathrm{lclm}(g, h^\natural)$ divides $x^n - \lambda$ on the right.

1. Assume that $\mathrm{gcrd}(g, h^\natural) = 1$, then $\deg(\mathrm{lclm}(g, h^\natural)) = \deg(g) + \deg(h^\natural) = n$, therefore, one has $\mathrm{lclm}(g, h^\natural) = x^n - \lambda = G \cdot h^\natural$, and $\mathrm{lclm}(g, h^\natural) = G \cdot h^\natural$ with $\mathrm{gcrd}(g, h^\natural) = 1$. One can conclude that g is similar to G.

2. Assume that $g = G$. As $x^n - \lambda = g \cdot h = G \cdot h^\natural$, one gets $h = h^\natural$. As $\mathrm{lclm}(g, h) = x^n - 1$, one deduces that $\mathrm{gcrd}(g, h^\natural) = \mathrm{gcrd}(g, h) = 1$, therefore C is an Euclidean LCD code.

□

Example 6. *In Example 4, one has* $g = x^2 + w^7x + 1$ *and* $G = \Theta^2(1 \cdot g^* \cdot \frac{1}{1}) = x^2 + w^3x + 1$, *therefore* $\mathrm{lclm}(g, w^2) = G \cdot w^2 = w^2 \cdot g$ *and* g *is similar to* G.

Example 7. *In Example 5, one has* $g = x^3 + w^7x^2 + x + 2$ *and* $G = \Theta^3(g^*) = x^3 - x^2 + w^3x - 1$. *As* $\mathrm{lclm}(g, x^2 - x + w^7) = \Theta(G) \cdot (x^2 - x + w^7) = x^5 + x^4 + x^3 + wx^2 + w^5x + w^3$ *and* $\mathrm{gcrd}(g, x^2 - x + w^7) = 1$, g *is similar to* $\Theta(G)$.

If θ is the identity, then $G = g_0 g^\natural \frac{1}{g_0} = g^\natural$ and following Remark 1, one gets the already known result recalled above the proposition : if C is an Euclidean LCD code then $g = G = g^\natural$. If g and h are coprime and $g = G = g^\natural$ then C is an Euclidean LCD code.

If θ is not the identity, as seen in the previous example, Euclidean LCD (θ, λ)-constacyclic codes do not necessarily satisfy the equality $g = G$. Furthermore, when $\mathrm{lclm}(g, h) = x^n - 1$, g being similar to G does not imply necessarily the code to be a LCD code :

Example 8. *Consider* $R = \mathbb{F}_4[x; \theta]$ *where* $\mathbb{F}_4 = \mathbb{F}_2(w)$, $g = x^2 + w^2x + w$ *and* $h = x^2 + w^2w + w^2$. *One has* $g \cdot h = h \cdot g = \mathrm{lclm}(g, h) = x^4 - 1$ *and* $G = w(x^2 + x + w^2) \cdot \frac{1}{w} = x^2 + w^2x + w^2$. *The* θ*-cyclic code of length* 4 *generated by* g *is not an Euclidean LCD code because* $\mathrm{gcrd}(g, h^\natural) = g \neq 1$, *however* g *and* G *are similar because* $\mathrm{lclm}(g, x + w) = x^3 + x^2 + x + 1 = G \cdot (x + w)$ *and* $\mathrm{gcrd}(g, x + w) = 1$.

We are now going to characterize the skew generators of LCD skew cyclic and negacyclic codes as least common left multiples of skew polynomials. This will enable to give a construction and an enumeration of LCD skew cyclic and negacyclic codes over $\mathbb{F}_{p^2}$ (section 5). Let us introduce a first notation. We recall that the fixed field of θ is $\mathbb{F}_q^\theta$ and we denote μ the order of θ. For $F(x^\mu) \in \mathbb{F}_q^\theta[x^\mu]$ and b in $\{0, 1\}$, consider the following set :

$$\mathcal{L}^{(b)}_{F(x^\mu)} := \{g \in R \mid g \,\text{monic},\ g \cdot h = F(x^\mu) \text{ and } \mathrm{gcrd}(\Theta^b(h^\natural), g) = 1\}.$$

The following proposition is inspired from Proposition 28 of [5] and Proposition 2 of [3]. It will enable to construct and enumerate LCD skew cyclic and negacyclic codes over $\mathbb{F}_{p^2}$.

Proposition 5. *Consider* $\mathbb{F}_q$ *a finite field,* θ *an automorphism of* $\mathbb{F}_q$ *of order* μ, $R = \mathbb{F}_q[x; \theta]$. *Consider* $F(x^\mu) = f_1(x^\mu) \cdots f_r(x^\mu)$ *where* $f_1(x^\mu), \ldots, f_r(x^\mu)$ *are polynomials of* $\mathbb{F}_q^\theta[x^\mu]$ *such that* f_i *is coprime with* f_j *and* $f_j^\natural$ *for all* $i \neq j$. *The application*

$$\phi : \left\{ \begin{array}{ccc} \mathcal{L}^{(b)}_{f_1(x^\mu)} \times \cdots \times \mathcal{L}^{(b)}_{f_r(x^\mu)} & \to & \mathcal{L}^{(b)}_{F(x^\mu)} \\ (g_1, \ldots, g_r) & \mapsto & \mathrm{lclm}(g_1, \ldots, g_r) \end{array} \right.$$

is bijective.

Proof. • The application ϕ is well-defined.

Consider $(g_1, \ldots, g_r)$ in $\mathcal{L}^{(b)}_{f_1(x^\mu)} \times \cdots \times \mathcal{L}^{(b)}_{f_r(x^\mu)}$ and $g = \mathrm{lclm}(g_1, \ldots, g_r)$. Consider $h_1, \ldots, h_r$ such that $g_i \cdot h_i = h_i \cdot g_i = f_i(x^\mu)$ and $\mathrm{gcrd}(g_i, \Theta^b(h_i^\natural)) = 1$. Consider $h = \mathrm{lcrm}(h_1, \ldots, h_r)$. Let us prove that $g \cdot h = F(x^\mu)$ and that $\mathrm{gcrd}(g, h^\natural) = 1$.

First of all, as $h_1, \dots, h_r$ divide respectively $f_1(x^\mu), \dots, f_r(x^\mu)$, and as $f_1(x^\mu), \dots, f_r(x^\mu)$ are pairwise coprime central polynomials, the degree of $h = \text{lcrm}(h_1, \dots, h_r)$ is equal to $\sum_{i=1}^{r} \deg(h_i)$. In the same way, the degree of $g = \text{lclm}(g_1, \dots, g_r)$ is equal to $\sum_{i=1}^{r} \deg(g_i)$. Furthermore, as $g_i \cdot h_i = f_i(x^\mu)$, the degree of $g_i \cdot h_i$ is equal to the degree of $f_i(x^\mu)$ in x, therefore the degree of $g \cdot h$ is equal to the degree of $F(x^\mu)$ in x.

Consider, for i in $\{1, \dots, r\}$, A_i in R such that $g = A_i \cdot g_i$ and B_i in R such that $h = h_i \cdot B_i$. One gets $g \cdot h = A_i \cdot g_i \cdot h_i \cdot B_i = A_i \cdot f_i(x^\mu) \cdot B_i$. As $f_i(x^\mu)$ is central, it divides $g \cdot h$. The polynomials $f_i(x^\mu)$ are pairwise coprime in $\mathbb{F}_q^\theta[x^\mu]$, therefore their least common right multiple is equal to their product $F(x^\mu)$, and $F(x^\mu)$ divides $g \cdot h$. As $\deg(g \cdot h) = \deg(F(x^\mu))$, one gets $g \cdot h = F(x^\mu)$. Now $\text{gcrd}(g, \Theta^b(h^\natural)) = \text{gcrd}(\text{lclm}(g_1, \dots, g_r), \text{lclm}(\Theta^b(h_1^\natural), \dots, \Theta^b(h_r^\natural)))$. One can notice that the skew polynomials g_i and $\Theta^b(h_j^\natural)$ are right coprime. Namely, if $i = j$, $\text{gcrd}(g_i, \Theta^b(h_i^\natural)) = 1$ by hypothesis. If $i \neq j$ consider a right divisor u of g_i and $\Theta^b(h_j^\natural)$, then u divides $f_i(x^\mu)$ and $f_j^\natural(x^\mu)$, as $f_i(x^\mu)$ and $f_j^\natural(x^\mu)$ are coprime one gets that $u = 1$. One deduces that $\text{gcrd}(g, \Theta^b(h^\natural)) = 1$. To conclude, the skew polynomial g belongs to $\mathcal{L}^{(b)}_{F(x^\mu)}$ therefore ϕ is well defined.

- The application ϕ is bijective.

  Consider g in $\mathcal{L}^{(b)}_{F(x^\mu)}$, then g divides $F(x^\mu)$, therefore, according to Theorem 4.1 of [11], $g = \text{lclm}(g_1, \dots, g_r)$ where $g_i = \text{gcrd}(f_i(x^\mu), g)$ and this lclm-decomposition into skew polynomials dividing $f_1(x^\mu), \dots, f_r(x^\mu)$ is unique. Furthermore $\deg(g) = \sum_{i=1}^{r} \deg(g_i)$ because $f_i(x^\mu)$ and $f_j(x^\mu)$ are coprime. Let us prove that g_i belongs to $\mathcal{L}^{(b)}_{f_i(x^\mu)}$. Consider h in R such that $g \cdot h = h \cdot g = F(x^\mu)$ and $\text{gcrd}(g, \Theta^b(h^\natural)) = 1$. As h divides $F(x^\mu)$, according to Theorem 4.1 of [11], $h = \text{lcrm}(h_1, \dots, h_r)$ where $h_i = \text{gcld}(f_i(x^\mu), h)$. This lcrm-decomposition into skew polynomials dividing $f_1(x^\mu), \dots, f_r(x^\mu)$ is unique and $\deg(h) = \sum_{i=1}^{r} \deg(h_i)$.

  Consider, for i in $\{1, \dots, r\}$, A_i in R such that $g = A_i \cdot g_i$ and B_i in R such that $h = h_i \cdot B_i$. As $g \cdot h = F(x^\mu)$ and as $F(x^\mu)$ is central, the skew polynomial $g_i \cdot h_i$ divides $F(x^\mu)$ on the right. Therefore, $g_i \cdot h_i = \text{lclm}(\text{gcrd}(g_i \cdot h_i, f_j(x^\mu)), j = 1, \dots, r) = \text{gcrd}(g_i \cdot h_i, f_i(x^\mu))$ divides $f_i(x^\mu)$. As $\sum_{i=1}^{r} \deg(g_i \cdot h_i) = \deg(g) + \deg(h) = \deg(F(x^\mu)) = \sum_{i=1}^{r} \deg(f_i(x^\mu))$, one gets $g_i \cdot h_i = f_i(x^\mu)$. Lastly, consider u in R such that u divides on the right g_i and $\Theta^b(h_i^\natural)$. As h_i divides on the left h, $\Theta^b(h_i^\natural)$ divides on the right $\Theta^b(h^\natural)$, therefore u divides on the right both g and $\Theta^b(h^\natural)$, and $u = 1$.

□

We now introduce some notations that will be useful later :

$$\mathcal{D}_{F(x^\mu)} := \{f \in \mathbb{F}_q^\theta[x^\mu] \mid f \text{ monic and divides } F(x^\mu) \text{ in } \mathbb{F}_q^\theta[x^\mu]\}$$

$$\mathcal{F}_{ir} := \{f = f(x^\mu) \in \mathbb{F}_q^\theta[x^\mu] \mid f = f^\natural \text{ irreducible in } \mathbb{F}_q^\theta[x^\mu], \deg_{x^\mu} f > 1\}$$

$$\mathcal{F}_{red} := \{f = f(x^\mu) \in \mathbb{F}_q^\theta[x^\mu] \mid f = f_{ir} f_{ir}^\natural,\ f_{ir} \neq f_{ir}^\natural \text{ irreducible in } \mathbb{F}_q^\theta[x^\mu]\}.$$

Theorem 3. *Consider $\mathbb{F}_q$ a finite field with q elements, θ an automorphism over $\mathbb{F}_q$ with order μ, $R = \mathbb{F}_q[x; \theta]$, $\lambda \in \{-1, 1\}, b \in \{0, 1\}$. Consider n a multiple of μ and $x^n - \lambda = f_1(x^\mu)^{p^s} \cdots f_r(x^\mu)^{p^s}$ where $f_1(x^\mu), \dots, f_r(x^\mu)$ are polynomials of $\mathbb{F}_p[x^\mu]$ belonging to $\{x^\mu \pm 1\} \cup \mathcal{F}_{ir} \cup \mathcal{F}_{red}$. Consider a (θ, λ)-constacyclic code C of length n and skew generator polynomial g.*

1. *C is an Euclidean LCD code if and only if $g = \text{lclm}(g_1, \dots, g_r)$ where for all i in $\{1, \dots, r\}$, $g_i \in \mathcal{L}^{(0)}_{f_i(x^\mu)^{p^s}}$.*
2. *C is an Hermitian LCD code if and only if $g = \text{lclm}(g_1, \dots, g_r)$ where for all i in $\{1, \dots, r\}$, $g_i \in \mathcal{L}^{(1)}_{f_i(x^\mu)^{p^s}}$.*

Proof. According to Theorem 2, the Euclidean (resp. Hermitian) LCD θ-cyclic codes of length n are generated by the elements of the set $\mathcal{L}^{(b)}_{x^n-1}$ where $b=0$ (resp. $b=1$). The Euclidean (resp. Hermitian) LCD θ-negacyclic codes of length n are associated to the set $\mathcal{L}^{(b)}_{x^n+1}$ where $b=0$ (resp. $b=1$). As $x^n \pm 1$ is self-reciprocal, one has $x^n \pm 1 = f_1(x^\mu)^{p^s} \cdots f_r(x^\mu)^{p^s}$ where $f_1(x^\mu), \ldots, f_r(x^\mu)$ are self-reciprocal polynomials of $\mathbb{F}_p[x^\mu]$ who are either irreducible or products of an irreducible polynomial and its reciprocal polynomial. Therefore for $i \neq j$, f_i is coprime with f_j and $f_j^\natural$ and Theorem 5 can be applied to $F(x^\mu) = x^n \pm 1$.

□

Remark 2. *The Euclidean LCD skew cyclic (resp. negacyclic) codes of length n over $\mathbb{F}_q$ are the skew cyclic (resp. negacyclic) codes $C = \bigcap_{i=1}^r C_i$ where C_i is a skew cyclic (resp. negacyclic) code generated by $g_i \in \mathcal{L}^{(0)}_{f_i(x^\mu)^{p^s}}$ and where the polynomial $F(x^\mu) = x^n - 1$ (resp. $x^n + 1$) factorizes in $\mathbb{F}_q^\theta[x^\mu]$ as $F(x^\mu) = \prod_{i=1}^r f_i(x^\mu)^{p^s}$, $f_i(x^\mu) \in \mathcal{F}_{ir} \bigcup \mathcal{F}_{red} \bigcup \{x^\mu \pm 1\}$. The same remark holds for Hermitian LCD skew cyclic and negacyclic codes where $g_i \in \mathcal{L}^{(1)}_{f_i(x^\mu)^{p^s}}$ instead of $g_i \in \mathcal{L}^{(1)}_{f_i(x^\mu)^{p^s}}$.*

5 LCD skew cyclic and negacyclic codes over $\mathbb{F}_{p^2}$

In this section, we construct and enumerate LCD skew cyclic and negacyclic codes in the particular case when $q = p^2$ is the square of a prime number p and $\theta : a \mapsto a^p$ is the Frobenius automorphism over $\mathbb{F}_q$. Therefore the order μ of θ is equal to 2 and the fixed field $\mathbb{F}_q^\theta$ of θ is $\mathbb{F}_p$. We will use the characterization of LCD skew cyclic and negacyclic given by Theorem 3. This point of view is useful for the construction and the enumeration of the codes (Propositions 7, 8, 9).

According to Theorem 3, LCD θ-cyclic and θ-negacyclic codes of even length n over $\mathbb{F}_{p^2}$ are generated by skew polynomials which are least common left multiples of skew polynomials $g_i \in \mathcal{L}^{(b)}_{f_i(x^2)^{p^s}}$ where $f = f_i \in \mathcal{D}_{x^n \pm 1}$ is a divisor of $x^n \pm 1$ in $\mathbb{F}_p[x^2]$ satisfying one of the following cases :

- $f(x^2) = x^2 - \epsilon$ where $\epsilon = \pm 1$ (see Lemma 6)
- $f(x^2) \in \mathcal{F}_{ir}$ irreducible in $\mathbb{F}_p[x^2]$ with degree $d > 1$ in x^2 (see Lemma 6);
- $f(x^2) \in \mathcal{F}_{red}$ is the product of two irreducible distinct polynomials in $\mathbb{F}_p[x^2]$ (see Lemma 7).

The following proposition enables to characterize those skew polynomials having a unique factorization into the product of monic irreducible skew polynomials. It will be useful later.

Proposition 6 (Proposition 16 of [5])**.** *Consider p a prime number, $\theta : a \mapsto a^p$ the Frobenius automorphism over $\mathbb{F}_q$ with $q = p^2$, $R = \mathbb{F}_q[x;\theta]$, $f \in \mathbb{F}_p[x^2]$ irreducible in $\mathbb{F}_p[x^2]$ and $h = h_m \cdots h_1$ a product of irreducible monic polynomials dividing f. The following assertions are equivalent*

(i) h has a unique factorization into irreducible monic polynomials;

(ii) f does not divide h in R;

(iii) for all i in $\{1, \ldots, m-1\}$, $f \neq h_{i+1} \cdot h_i$.

5.1 Length $2p^s$ over $\mathbb{F}_{p^2}$

Lemma 6 describes the set $\mathcal{L}^{(b)}_{f(x^2)^m}$ where $f(x^2) \in \mathcal{F}_{ir} \bigcup \{x^2 \pm 1\}$. It will be useful to characterize all nontrivial LCD skew cyclic and negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^2}$ (Proposition 7 and algorithm 1).

Lemma 6. *Consider p a prime number, $\theta : a \mapsto a^p$ the Frobenius automorphism over $\mathbb{F}_q$ with $q = p^2$, $R = \mathbb{F}_q[x;\theta]$, $f(x^2) \in \mathcal{F}_{ir} \bigcup \{x^2 \pm 1\}$ with degree d in x^2, g in R and $m \in \mathbb{N}$. The skew polynomial g belongs to the set $\mathcal{L}^{(b)}_{f(x^2)^m}$ if, and only if, $g = 1$ or $g = f(x^2)^m$ or g has a unique factorization into the product of m monic irreducible skew polynomials $g = g_m \cdots g_1$ where*

$$\begin{cases} \forall i \in \{1, \ldots, m\}, \deg(g_i) = d \\ g_i \text{ divides on the right } f(x^2) \\ \forall i \in \{1, \ldots, m-1\}, g_{i+1} \cdot g_i \neq f(x^2) \\ g_1 \neq \Theta^b(h_1^\natural) \text{ where } \Theta^b(h_1^\natural) \cdot h_1 = f(x^2). \end{cases} \tag{1}$$

Proof. Consider g in $\mathcal{L}^{(b)}_{f(x^2)^m} \setminus \{f(x^2)^m, 1\}$. Consider h in R such that $g \cdot h = h \cdot g = f(x^2)^m$. As $f(x^2)$ is central and irreducible in $\mathbb{F}_p[x^2]$, the skew polynomials g and h are products of irreducible monic factors dividing $f(x^2)$. As $\deg(g) > 2dm$ and $\deg(h) + \deg(g) = 2dm$, there exists $r \in \{1, \ldots, 2m-1\}$, $g_1, \ldots, g_{2m-r}, h_1, \ldots, h_r$ monic of degree d dividing $f(x^2)$ such that

$$g = g_{2m-r} \cdots g_1$$

and

$$h = h_1 \cdots h_r.$$

The skew polynomial $\Theta^b(h_1^\natural)$ is an irreducible right factor of $\Theta^b(h^\natural)$ which divides $\Theta^b(f^\natural(x^2)) = f(x^2)$ and does not divide g on the right because $\text{gcrd}(\Theta^b(h^\natural), g) = 1$. Therefore $f(x^2)$ does not divide g. Similarly, one gets that $f(x^2)$ does not divide $\Theta^b(h^\natural)$ and h. Therefore, according to Proposition 6, the above factorizations of g and h into the products of monic irreducible factors are unique and for all i in $\{1, \ldots, m-1\}$, $g_{i+1} \cdot g_i \neq f(x^2)$.
As $g \cdot h = h \cdot g = f(x^2)^m$ one gets that for all i, $g_i \cdot h_i = f(x^2)$, therefore, $r = m$.
Laslty, as g and $\Theta^b(h^\natural)$ are right coprime, necessarily, $g_1 \neq \Theta^b(h_1^\natural)$.

Conversely, consider $g = g_m \cdots g_1$ where $g_1, \ldots, g_m$ are monic skew polynomials satisfying (1). Consider $h = h_1 \cdots h_m$ with $g_i \cdot h_i = h_i \cdot g_i = f(x^2)$ then $g \cdot h = h \cdot g = f(x^2)^m$. Furthermore as $g_{i+1} \cdot g_i \neq f(x^2)$, according to Proposition 6, the above factorization of g into the product of monic irreducible factors is unique. Similarly, the factorizations of h and $\Theta^b(h^\natural)$ into the products of monic irreducible factors are unique.
Consider u a right factor of g and $\Theta^b(h^\natural)$ with degree > 1. Necessarily, u has a unique factorization into the product of monic skew polynomials. The unique monic linear right factor of u is also the unique monic right factor of g and $\Theta^b(h^\natural)$, therefore $u = g_1 = \Theta^b(h_1^\natural)$, which is impossible according to (1). Therefore $\text{gcrd}(g, \Theta^b(h^\natural)) = 1$ and g belong to $\mathcal{L}^{(b)}_{f(x^2)^m}$. □

Lemma 6 enables to characterize all nontrivial LCD skew cyclic and negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^2}$ (Proposition 7). Their dimensions are necessarily equal to p^s :

Proposition 7. *Consider p a prime number, $\theta : a \mapsto a^p$ the Frobenius automorphism over $\mathbb{F}_q$ with $q = p^2$, $R = \mathbb{F}_q[x;\theta]$, $\epsilon \in \{-1, 1\}$, s in $\mathbb{N}$, $n = 2p^s$ and $k \leq n$.*

1. *There is no non trivial (Euclidean and Hermitian) LCD (θ, ϵ)-constacyclic codes of length $n = 2p^s$ and dimension $k \neq p^s$.*
2. *The number of Euclidean LCD (θ, ϵ)-constacyclic codes of length $n = 2p^s$ and dimension $k = p^s$ over $\mathbb{F}_{p^2}$ is*

$$\begin{cases} 2^k & \text{if } \ p = 2 \\ p^{k-1}(p - \epsilon(-1)^{(p+1)/2}) & \text{if } \ p \neq 2. \end{cases}$$

3. *The number of Hermitian LCD (θ, ϵ)-constacyclic codes of length $n = 2p^s$ and dimension $k = p^s$ over $\mathbb{F}_{p^2}$ is*

$$\begin{cases} 0 & \text{if } \ p = 2 \text{ or } p \text{ odd and } \epsilon = -1 \\ p^{k-1}(p+1) & \text{if } \ p \text{ odd and } \epsilon = 1. \end{cases}$$

Proof. • The Euclidean LCD θ-cyclic (resp. θ-negacyclic) codes of length $n = 2p^s$ over $\mathbb{F}_{p^2}$ are generated by the monic irreducible skew polynomials belonging to $\mathcal{L}^{(0)}_{(x^2-\epsilon)^{p^s}}$ where $\epsilon = 1$ (resp. $\epsilon = -1$). According to Lemma 6, a monic skew polynomial g belongs to the set $\mathcal{L}^{(0)}_{(x^2-\epsilon)^{p^s}}$ if, and only if, $g = 1$ or $g = (x^2-\epsilon)^{p^s}$ or $g = g_{p^s} \cdots g_1$ where $g_1, \ldots, g_{p^s}$ are monic skew polynomials satisfying :

$$\begin{cases} \deg(g_i) = 1 \\ g_i \text{ divides on the right } x^2 - \epsilon \\ g_{i+1} \cdot g_i \neq x^2 - \epsilon \\ g_1 \neq h_1^{\natural} \text{ where } h_1^{\natural} \cdot h_1 = x^2 - \epsilon. \end{cases}$$

Therefore $g \neq 1, (x^2-\epsilon)^{p^s}$ belongs to the set $\mathcal{L}^{(0)}_{(x^2-\epsilon)^{p^s}}$ if, and only if, $g = (x+\alpha_{p^s}) \cdots (x+\alpha_1)$ where

$$\begin{cases} \alpha_i^{p+1} = \epsilon \\ \alpha_{i+1} \neq -\epsilon/\alpha_i \\ \epsilon \neq -\theta(\alpha_1)/\alpha_1. \end{cases} \tag{2}$$

Furthermore the above factorization of g is unique, therefore the number of skew polynomials of degree $k = p^s$ in $\mathcal{L}^{(0)}_{(x^2-\epsilon)^k}$ is

$$\begin{cases} p^{k-1}(p-1) & \text{if} \quad p \text{ odd and } \epsilon = (-1)^{(p+1)/2} \\ p^{k-1}(p+1) & \text{if} \quad p \text{ odd and } \epsilon \neq (-1)^{(p+1)/2} \\ 2^k & \text{if} \quad p = 2. \end{cases}$$

- The Hermitian LCD θ-cyclic (resp. θ-negacyclic) codes of length $n = 2p^s$ over $\mathbb{F}_{p^2}$ are generated by the monic skew polynomials belonging to $\mathcal{L}^{(1)}_{(x^2-\epsilon)^{p^s}}$ where $\epsilon = 1$ (resp. $\epsilon = -1$). According to Lemma 6, a monic skew polynomial g belongs to the set $\mathcal{L}^{(1)}_{(x^2-\epsilon)^{p^s}}$ if, and only if, $g = 1$ or $g = (x^2-\epsilon)^{p^s}$ or $g = (x+\alpha_{p^s}) \cdots (x+\alpha_1)$ where

$$\begin{cases} x + \alpha_i \text{ divides on the right } x^2 - \epsilon \\ (x+\alpha_{i+1}) \cdot (x+\alpha_i) \neq x^2 - \epsilon \\ x + \alpha_1 \neq \Theta(h_1^{\natural}) \text{ where } \Theta(h_1^{\natural}) \cdot h_1 = x^2 - \epsilon. \end{cases}$$

If $\epsilon = -1$ or $p = 2$, $\mathcal{L}^{(1)}_{(x^2-\epsilon)^{p^s}} = \{1, (x^2-\epsilon)^{p^s}\}$. If $\epsilon = 1$ and $p \neq 2$, the skew polynomial $g \neq 1, (x^2-\epsilon)^{p^s}$ belongs to the set $\mathcal{L}^{(1)}_{(x^2-\epsilon)^{p^s}} = \mathcal{L}^{(1)}_{(x^2-1)^{p^s}}$ if, and only if, $g = (x+\alpha_{p^s}) \cdots (x+\alpha_1)$ where

$$\begin{cases} \alpha_i^{p+1} = 1 \\ \alpha_{i+1} \neq -1/\alpha_i. \end{cases} \tag{3}$$

In this case there are $(p+1)p^{k-1}$ skew polynomials of degree $k = p^s$ in $\mathcal{L}^{(1)}_{(x^2-\epsilon)^k}$.

□

Remark 3. *Over $\mathbb{F}_4$, one can notice that when $k = 2^s$, the number of Euclidean LCD θ-cyclic codes $[2k, k]$ growths exponentially with k (Point 1. of Proposition 7), while the number of Euclidean self-dual θ-cyclic codes $[2k, k]$ is constant (Corollary 26 of [5]).*

Remark 4. *When p is odd, the Euclidean LCD θ-cyclic codes of length $2p^s$ and dimension p^s over $\mathbb{F}_{p^2}$ are all Hermitian LCD codes (because (2) $\Rightarrow$ (3) when $\epsilon = 1$). Assume now that $p \equiv 1 \pmod 4$, then there does not exist α in $\mathbb{F}_{p^2}$ such that $\alpha^{p+1} = 1$ and $\alpha^2 = -1$, therefore when $\epsilon = 1$, (2) $\Leftrightarrow$ (3) and a $[2p, p]$ θ-cyclic code over $\mathbb{F}_{p^2}$ is an Euclidean LCD code if and only if it is an Hermitian LCD code.*

From the proof of Proposition 7, one deduces the following algorithm 1 for the construction of all LCD skew cyclic and negacyclic codes over $\mathbb{F}_{p^2}$:

Algorithm 1 Non trivial LCD θ-cyclic and -negacyclic codes of length $2p^s$ and dimension p^s over $\mathbb{F}_{p^2}$

Require: : p, prime number, $s \in \mathbb{N}$, $\epsilon \in \{-1, 1\}$, $b \in \{0, 1\}$

Ensure: : $\mathcal{L}^{(b)}_{(x^2-\epsilon)^{p^s}}$: the set of monic skew generators g of (θ, ϵ)-constacyclic codes $[2p^s, p^s]$ who are Euclidean LCD codes if $b = 0$ and Hermitian LCD codes if $b = 1$

$k \leftarrow p^s$
$E \leftarrow \emptyset$
if $b = 0$ **then**
  for $\alpha_1, \ldots, \alpha_k \in \mathbb{F}_{p^2}$ such that $\alpha_1^2 \neq -1, \alpha_i^{p+1} = \epsilon$ and $\alpha_{i+1} \neq -\epsilon/\alpha_i$ **do**
    $E \leftarrow E \cup \{(x + \alpha_k) \cdots (x + \alpha_1)\}$
  end for
else
  if p odd and $\epsilon = 1$ **then**
    for $\alpha_1, \ldots, \alpha_k \in \mathbb{F}_{p^2}$ such that $\alpha_i^{p+1} = 1$ and $\alpha_{i+1} \neq -1/\alpha_i$ **do**
      $E \leftarrow E \cup \{(x + \alpha_k) \cdots (x + \alpha_1)\}$
    end for
  end if
end if
return E

Example 9. *There are* $16 = 2^{2^2}$ *nontrivial Euclidean LCD* θ*-cyclic codes of length* 8 *over* $\mathbb{F}_4 = \mathbb{F}_2(w)$ *where* θ *is the Frobenius automorphism over* $\mathbb{F}_4$*. Their dimensions are all equal to* 4*. Consider* $g = (x + 1) \cdot (x + w^2) \cdot (x + w^2) \cdot (x + w^2) = x^4 + wx^3 + wx^2 + x + 1$*. As* $p = 2$*,* $(w^2)^{p+1} = 1^{p+1} = 1$*,* $(w^2)^2 \neq -1$*,* $w^2 \neq 1/w^2$ *and* $1 \neq 1/w^2$*, according to Proposition 7 and Algorithm 1,* g *generates an Euclidean LCD* $[8, 4]_4$ θ*-cyclic code which is not an Hermitian LCD code. The systematic generator matrix of* C *is* $(I_4|P)$ *where* $P = \begin{pmatrix} 1 & 1 & w & w \\ w^2 & w & 0 & w \\ w^2 & 1 & w & 1 \\ 1 & w^2 & w^2 & 1 \end{pmatrix}$*. One checks that* $1 \notin Spec(P \times^t P)$ *therefore according to Proposition 4 of [9]* C *is an Euclidean LCD code. Furthermore* $1 \in Spec(P \times^t \overline{P})$ *therefore according to Proposition 6 of [9]* C *is not an Hermitian LCD code.*

Example 10. *Consider* $\mathbb{F}_9 = \mathbb{F}_3(w)$ *where* $w^2 = w + 1$*. There are* $18 = 3^2 \times (3 - (-1)^2)$ *nontrivial Euclidean LCD* θ*-cyclic codes and* $36 = 3^2 \times (3 + 1)$ *nontrivial Hermitian LCD* θ*-cyclic codes of length* 6 *over* $\mathbb{F}_9$*. Their dimensions are equal to* 3*.*

- *Consider* $g = (x+w^2)\cdot(x+w^6)\cdot(x+1) = x^3+w^5x^2+w^5x+1$ *and* $h = (x+2)\cdot(x+w^6)\cdot(x+w^2)$*. Then* $g \cdot h = h \cdot g = x^6 - 1$*,* $h^\natural = (x+w^6)\cdot(x+w^2)\cdot(x+2)$ *and* $\Theta(h^\natural) = (x+w^2)\cdot(x+w^6)\cdot(x+2)$*. These factorizations of* g*,* h *and* $\Theta(h^\natural)$ *into the products of monic linear skew polynomials are unique. As* $x + 2 \neq x + 1$*,* $h^\natural$ *is right coprime with* g *and* $\Theta(h^\natural)$ *is also rigth coprime to* g*. Therefore* g *generates a* θ*-cyclic code of length* 6 *which is both an Euclidean LCD code and a Hermitian LCD code.*
- *Consider* $g = (x - 1)^2 \cdot (x - w^6)$ *and* $h = (x - w^6) \cdot (x + 1)^2$*. Then* $g \cdot h = h \cdot g = x^6 - 1$*. Consider the* θ*-cyclic code* C *of length* 6 *and dimension* 3 *generated by* g*. This code is MDS. Furthermore* $h^\natural = g$*, therefore* C *is not an Euclidean LCD code and* $\Theta(h^\natural) = (x-1)^2 \cdot (x-a^2)$ *is right coprime with* g*, therefore* C *is a MDS Hermitian LCD code.*

Example 11. *Consider* $\mathbb{F}_9 = \mathbb{F}_3(w)$ *where* $w^2 = w + 1$*. There are* $36 = 3^2 \times (3 - (-1))$ *nontrivial Euclidean LCD* θ*-negacyclic codes of length* 6 *over* $\mathbb{F}_9$*. Their dimensions are equal to* 3*. Consider*

p	nbr of Euclidean LCD skew cyc.		nbr of Hermitian LCD skew cyc.	
	$[2p,p]_{p^2}$	$[2p,p,p+1]_{p^2}$	$[2p,p]_{p^2}$	$[2p,p,p+1]_{p^2}$
3	18	16	36	32
5	3750	2412	3750	2412
7	705984	39564	941192	52752
11	259374246010	≥ 1	311249095212	≥ 1

Table 3: Number of Euclidean and Hermitian LCD $[2p,p]_{p^2}$ and $[2p,p]_{p^2}$ MDS skew-cyclic codes for $p = 3, 5, 7, 11$

$g = (x+w^5)\cdot(x+w^7)\cdot(x+w^3) = x^3+x^2+wx+w^7$ *and* $h = (x+w^5)\cdot(x+w)\cdot(x+w^3)$. *Then* $g\cdot h = h\cdot g = x^6+1$, $h^\natural = (x+w^3)\cdot(x+w)\cdot(x+w)$ *and* $\Theta(h^\natural) = (x+w^2)\cdot(x+w^3)\cdot(x+w^3)$. *These factorizations of* g, h *and* $\Theta(h^\natural)$ *into the products of monic linear skew polynomials are unique. As* $x+w^3 \neq x+w$, $h^\natural$ *is right coprime with* g. *Therefore* g *generates a* θ*-negacyclic code of length* 6 *which is an Euclidean LCD code. However* g *and* $\Theta(h^\natural)$ *are not right coprime because* $x+w^3$ *divides both* g *and* $\Theta(h^\natural)$ *and the code is not an Hermitian LCD code.*

Example 12. *Consider* $\mathbb{F}_{25} = \mathbb{F}_5(w)$ *where* $w^2 = w-2$. *The skew polynomials* $g = (x+1)^3\cdot(x+w)\cdot(x+1) = x^5+w^{16}x^4+w^5x^3+2x^2+wx+w^4$ *and* $h = (x-1)\cdot(x+w^8)\cdot(x-1)^3$ *satisfy* $g\cdot h = h\cdot g = x^{10}-1$. *Furthermore* $h^\natural = (x+w^4)\cdot(x+w^{20})\cdot(x+w^4)\cdot(x+w^{16})\cdot(x-1)$, $\Theta(h^\natural) = (x+w^{20})\cdot(x+w^4)\cdot(x+w^{20})\cdot(x+w^8)\cdot(x-1)$. *The factorizations of* g, h *and* $\Theta(h^\natural)$ *into the products of monic linear skew polynomials are unique. As* $x-1 \neq x+1$, $h^\natural$ *and* $\Theta(h^\natural)$ *are right coprime with* g. *Therefore* g *generates a* θ*-cyclic code* $[10,5]$ *which is an Euclidean LCD code and an Hermitian LCD code. Furthermore, this is an MDS code.*

The following table 3 sums up the number of $[2p,p]_{p^2}$ LCD θ-cyclic codes and the number of $[2p,p]_{p^2}$ MDS LCD θ-cyclic codes for $p \in \{3,5,7,11\}$.

5.2 Any length over $\mathbb{F}_{p^2}$

The aim of this section is to give a complete description of Euclidean and Hermitian LCD skew cyclic and skew negacyclic codes over $\mathbb{F}_{p^2}$ (Proposition 8 and algorithm 3). In the case when the skew generator polynomials are not divisible by any central polynomial a complete counting formula is given (Proposition 9). Some examples and tables are given to illustrate the obtained results. Some MDS LCD codes are obtained over $\mathbb{F}_9$, $\mathbb{F}_{25}$ and $\mathbb{F}_{49}$.

In order to consider LCD skew cyclic and negacyclic codes of any even length over $\mathbb{F}_{p^2}$, we will characterize $\mathcal{L}^{(b)}_{f(x^2)^m}$ for $f(x^2) \in \mathcal{F}_{red}$ (Lemma 7 below). We deduce from Lemma 6 and 7 an algorithm for the construction of $\mathcal{L}^{(b)}_{f(x^2)^m}$ for $f(x^2) \in \mathcal{F}_{irr} \cup \mathcal{F}_{red}$ (algorithm 2).

Lemma 7. *Consider* p *a prime number,* $\theta : a \mapsto a^p$ *the Frobenius automorphism over* $\mathbb{F}_q$ *with* $q = p^2$, $R = \mathbb{F}_q[x;\theta]$, $f(x^2) = f_{ir}(x^2)f^\natural_{ir}(x^2)$ *in* $\mathcal{F}_{red}$ *with degree* $d = 2\delta$ *in* x^2. *The monic skew polynomial* $g \in R$ *belongs to the set* $\mathcal{L}^{(b)}_{f(x^2)^m}$ *if, and only if,* $g = 1$ *or* $g = f(x^2)^m$ *or* $g = \mathrm{lclm}(g_1, g_2)$ *where* $g_1 = g_{1,m}\cdots g_{1,1}$ *and* $g_2 = g_{2,m}\cdots g_{2,1}$ *have unique factorizations into the products of* m *monic irreducible skew polynomials satisfying :*

$$\begin{cases} \deg(g_{i,j}) = \delta \\ g_{1,j} \text{ divides } f_{ir}(x^2) \\ g_{2,j} \text{ divides } f^\natural_{ir}(x^2) \\ g_{1,j}\cdot g_{1,j-1} \neq f_{ir}(x^2) \\ g_{2,j}\cdot g_{2,j-1} \neq f^\natural_{ir}(x^2) \\ g_{1,1} \neq \Theta^b(h^\natural_{2,1}), h_{2,1}\cdot g_{2,1} = f^\natural_{ir}(x^2) \end{cases} \tag{4}$$

Proof. Consider g in $\mathcal{L}^{(b)}_{f(x^2)^m} \setminus \{1, f_{ir}(x^2)^m f^{\natural}_{ir}(x^2)^m\}$ and h in R such that $g \cdot h = h \cdot g = f_{ir}(x^2)^m f^{\natural}_{ir}(x^2)^m$ and $\mathrm{gcrd}(g, \Theta^b(h^{\natural})) = 1$. As g divides $f_{ir}(x^2)^m f^{\natural}_{ir}(x^2)^m$, according to Theorem 4.1 of [11], $g = \mathrm{lclm}(g_1, g_2)$ where $g_1 = \mathrm{gcrd}(f_{ir}(x^2)^m, g)$ and $g_2 = \mathrm{gcrd}(f^{\natural}_{ir}(x^2)^m, g)$. Similarly, $h = \mathrm{lcrm}(h_1, h_2)$, where $h_1 = \mathrm{gcld}(f_{ir}(x^2), h)$ and $h_2 = \mathrm{gcld}(f^{\natural}_{ir}(x^2), h)$.

As $g \cdot h = h \cdot g = f_{ir}(x^2)^m f^{\natural}_{ir}(x^2)^m$, one has $g_1 \cdot h_1 = f_{ir}(x^2)^m$ and $g_2 \cdot h_2 = f^{\natural}_{ir}(x^2)^m$, therefore g_1 and h_1 (resp. g_2 and h_2) are products of irreducible skew polynomials dividing $f_{ir}(x^2)$ (resp. $f^{\natural}_{ir}(x^2)$).

If $f_{ir}(x^2)$ divides g_1, then, as $\Theta^b(h_2^{\natural})$ divides $f_{ir}(x^2)^m$, g_1 and $\Theta^b(h_2^{\natural})$ have a common right divisor (dividing $f_{ir}(x^2)$), therefore g and $\Theta^b(h^{\natural})$ also have a common nontrivial right divisor, which is impossible as g and $\Theta^b(h^{\natural})$ are right coprime. Therefore $f_{ir}(x^2)$ does not divide g_1. In the same way, $f_{ir}(x^2)$ does not divide h_1, $f^{\natural}_{ir}(x^2)$ does not divide g_2 and h_2, therefore using Proposition 6, one gets that the factorizations of g_1, g_2, h_1 and h_2 into the products of monic irreducible skew polynomials are unique and

$$\begin{cases} g_1 = g_{1,m} \cdots g_{1,1} \\ g_2 = g_{2,m} \cdots g_{2,1} \\ h_1 = h_{1,1} \cdots h_{1,m} \\ h_2 = h_{2,1} \cdots h_{2,m} \\ \deg(g_{i,j}) = \delta \\ g_{1,j} \cdot g_{1,j-1} \neq f_{ir}(x^2) \\ g_{2,j} \cdot g_{2,j-1} \neq f^{\natural}_{ir}(x^2) \\ g_{1,i} \cdot h_{1,i} = f(x^2) \\ g_{2,i} \cdot h_{2,i} = f^{\natural}(x^2) \end{cases}$$

As g and $\Theta^b(h^{\natural})$ are right coprime, g_1 and $\Theta^b(h_2^{\natural})$ are right coprime, therefore $g_{1,1} \neq \Theta^b(h^{\natural}_{2,1})$.

Conversely, assume that $g = \mathrm{lclm}(g_1, g_2)$ where $g_1 = g_{1,m} \cdots g_{1,1}$, $g_2 = g_{2,m} \cdots g_{2,1}$ and (4) is satisfied. Consider $h_{i,j}$ such that $g_{1,i} \cdot h_{1,i} = f_{ir}(x^2)$ and $g_{2,i} \cdot h_{2,i} = f^{\natural}_{ir}(x^2)$. Consider $h_1 = h_{1,1} \cdots h_{1,m}$, $h_2 = h_{2,1} \cdots h_{2,m}$ and $h = \mathrm{lcrm}(h_1, h_2)$. Then $g \cdot h = h \cdot g = f_{ir}(x^2)^m f^{\natural}_{ir}(x^2)^m$ and g and $\Theta^b(h^{\natural})$ are right coprime.

□

From Lemma 6 and Lemma 7, one deduces the following algorithm 2 for the construction of $\mathcal{L}^{(b)}_{f(x^2)^m}$ where $m \in \mathbb{N}$ and $f(x^2) \in \mathcal{F}_{ir} \bigcup \mathcal{F}_{red}$.

Theorem 3, Lemma 6 and Lemma 7 enable to characterize the skew generators of LCD θ-cyclic and θ-negacyclic codes over $\mathbb{F}_{p^2}$ as follows :

Proposition 8. *Consider $\mathbb{F}_q$ a finite field with $q = p^2$ elements where p is a prime number, $\theta : a \mapsto a^p$ the Frobenius automorphism over $\mathbb{F}_{p^2}$, $R = \mathbb{F}_q[x; \theta]$, $\lambda \in \{-1, 1\}, b \in \{0, 1\}$, $k \in \mathbb{N}$ and $n = 2p^s t$ an even integer with t not divisible by p. Consider $x^n - \lambda = f_1(x^2)^{p^s} \cdots f_r(x^2)^{p^s}$ where $f_1(x^2), \ldots, f_r(x^2)$ are polynomials of $\mathbb{F}_p[x^2]$ belonging to $\{x^2 \pm 1\} \cup \mathcal{F}_{ir} \cup \mathcal{F}_{red}$. Consider a (θ, λ)-constacyclic code C of length n and with skew generator g. C is an Euclidean (resp Hermitian) LCD code of length n and dimension k if and only if*

$$g = \prod_{i \in I} f_i(x^2)^{p^s} \ \mathrm{lclm}_{j \in J}(g_j)$$

where

$$\begin{cases} I, J \subset \{1, \ldots, r\} \\ I \cap J = \emptyset \\ \forall j \in J, g_j \in \mathcal{L}^{(b)}_{f_j(x^2)^{p^s}} \setminus \{1, f_j(x^2)^{p^s}\} \text{ with } b = 0 \text{ (resp } b = 1) \\ p^s(2\sum_{i \in I} d_i + \sum_{j \in J} d_j) = n - k. \end{cases}$$

In this case, C is the intersection of the skew constacyclic codes of length n generated by $\prod_{i \in I} f_i(x^2)^{p^s}$ and g_j where $j \in J$.

Algorithm 2 $\mathcal{L}^{(b)}_{f(x^2)^m}$ for $f(x^2) \in \mathcal{F}_{ir} \cup \mathcal{F}_{red}$, $b \in \{0,1\}$ and $m \in \mathbb{N}^*$

Require: : p, prime number, $m \in \mathbb{N}$, $b \in \{0,1\}$, $f(x^2) \in \mathbb{F}_p[x^2]$ such that $f(x^2) \in \mathcal{F}_{ir}$ or $f(x^2) = f_{ir}(x^2)f^{\natural}_{ir}(x^2) \in \mathcal{F}_{red}$

Ensure: : $\mathcal{L}^{(b)}_{f(x^2)^m}$

if $f(x^2) \in \mathcal{F}_{ir}$ **then**
  $E \leftarrow \{1, f(x^2)^m\}$
  $d \leftarrow \deg_{x^2}(f(x^2))$
  $I \leftarrow \{g \in R, g$ monic, g irreducible of degree d dividing $f(x^2)\}$ (using Algorithm 1 of Appendix A of [7])
  for $g_1, \ldots, g_m \in I$ such that $g_i \cdot g_{i+1} \neq f(x^2)$ and $g_1 \neq \Theta^b(h_1^{\natural})$ where $\Theta^b(h_1^{\natural}) \cdot h_1 = f(x^2)$ **do**
    $E \leftarrow E \cup \{g_m \cdots g_1\}$
  end for
else
  $I_1 \leftarrow \{g \in R, g$ monic, g irreducible of degree d dividing $f_{ir}(x^2)\}$
  $I_2 \leftarrow \{g \in R, g$ monic, g irreducible of degree d dividing $f^{\natural}_{ir}(x^2)\}$
  for $g_{2,1}, \ldots, g_{2,m} \in I_2$ such that $g_{2,i} \cdot g_{2,i+1} \neq f^{\natural}_{ir}(x^2)$ **do**
    $h_{2,1} \leftarrow$ quotient of the division of $f^{\natural}_{ir}(x^2)$ by $g_{2,1}$
    for $g_{1,1}, \ldots, g_{1,m} \in I_1$ such that $g_{1,i} \cdot g_{1,i+1} \neq f_{ir}(x^2)$ and $g_{1,1} \neq \Theta^b(h^{\natural}_{2,1})$ **do**
      $E \leftarrow E \cup \{\mathrm{lclm}(g_{1,m} \cdots g_{1,1}, g_{2,m} \cdots g_{2,1})\}$
    end for
  end for
end if
return E

Proof. Proposition 5, Lemma 6 and Lemma 7. □

Remark 5. *In Proposition 8, if J is empty then g is central; if I is empty then g is not divisible by any central polynomial. If $J = \{1, \ldots, r\}$ (and $I = \emptyset$), then g is not divisible by any central polynomial and* $\deg(g) = \sum_{i=1}^{r} \deg(g_i) = k$.

From Proposition 8, one deduces the Algorithm 3 for the construction of LCD θ-cyclic and θ-negacyclic codes of length n and dimension k over $\mathbb{F}_{p^2}$.

The following proposition characterizes LCD skew cyclic and negacyclic codes of even length $n = 2k$ and of dimension k whose generator polynomials are not divisible by any central polynomial ($J = \{1, \ldots, r\}$ and $I = \emptyset$ in Proposition 8).

Proposition 9. *Consider a prime number p, $\theta : a \mapsto a^p$ the Frobenius automorphism over $\mathbb{F}_{p^2}$, $\lambda \in \{-1, 1\}$ and $n = 2k = 2p^s t$ where s is an integer and t is an integer not divisible by p.*

1. *The number of Euclidean LCD (θ, λ)-constacyclic codes of length $2k$ and dimension k with skew generator polynomial not divisible by any central polynomial is*

$$N_\lambda \times \prod_{\substack{f \in \mathcal{F}_{ir} \cap \mathcal{D}_{x^n - \lambda} \\ d = \deg(f)}} (p^d - p^{d/2}) p^{d(p^s-1)} \times \prod_{\substack{f \in \mathcal{F}_{red} \cap \mathcal{D}_{x^n - \lambda} \\ d = \deg(f)}} (1 + p^{d/2}) p^{(2p^s-1)d/2}$$

where $N_1 = \begin{cases} 2^{2^s} & \text{if } p=2 \\ (p^{p^s-1})^2(p^2-1) & \text{if } k \text{ is even and } p \text{ is odd} \\ p^{p^s-1}(p - (-1)^{(p+1)/2}) & \text{if } k \text{ is odd and } p \text{ is odd} \end{cases}$

and $N_{-1} = \begin{cases} 1 & \text{if } k \text{ is even and } p \text{ is odd} \\ p^{p^s-1}(p - (-1)^{(p-1)/2}) & \text{if } k \text{ is odd and } p \text{ is odd} \end{cases}$

Algorithm 3 LCD θ-cyclic and θ-negacyclic codes of length n and dimension k over $\mathbb{F}_{p^2}$

Require: : p, prime number, $k \leq n \in \mathbb{N}$ with n even, $b \in \{0,1\}$, $\epsilon \in \{-1,1\}$, $\theta : a \mapsto a^p \in Aut(\mathbb{F}_{p^2})$

Ensure: : monic skew generators g of (θ,ϵ)-constacyclic codes of length n and dimension k over $\mathbb{F}_{p^2}$ who are Euclidean LCD codes if $b=0$ and Hermitian LCD codes if $b=1$.

$E \leftarrow \emptyset$
Compute $f_1(x^2), f_2(x^2), \ldots, f_r(x^2)$ such that $x^n - \lambda = f_1(x^2)^{p^s} \cdots f_r(x^2)^{p^s} \in \mathbb{F}_p[x^2]$ where $s \in \mathbb{N}$,$f_1(x^2), \ldots, f_r(x^2) \in \{x^2 \pm 1\} \cup \mathcal{F}_{ir} \cup \mathcal{F}_{red}$
for $i = 1, \ldots, r$ **do**
  $d_i \leftarrow \deg_{x^2}(f_i(x^2))$
  Compute $\mathcal{L}^{(b)}_{f_i(x^2)^{p^s}}$ with Algorithms 1 and 2
end for
for $I, J \subset \{1, \ldots, r\}$ with $I \cap J = \emptyset$ and $n - k = p^s \times (2\sum_{i\in I} d_i + \sum_{j\in J} d_j)$ **do**
  for $(g_j)_{j\in J} \in \prod_{j\in J} \mathcal{L}^{(b)}_{f_j(x^2)^{p^s}} \setminus \{1, f_j(x^2)^{p^s}\}$ **do**
    $E \leftarrow E \cup \{\prod_{i\in I} f_i(x^2)^{p^s} \ \mathrm{lclm}_{j\in J}(g_j)\}$
  end for
end for
return E

2. The number of Hermitian LCD (θ,λ)-constacyclic codes of length $2k$ and dimension k with skew generator polynomial not divisible by any central polynomial is

$$N_\lambda \times \prod_{\substack{f\in\mathcal{F}_{ir}\cap\mathcal{D}_{x^n-\lambda}\\ d=\deg(f)}} (p^d - p^{d/2})p^{d(p^s-1)} \times \prod_{\substack{f\in\mathcal{F}_{red}\cap\mathcal{D}_{x^n-\lambda}\\ d=\deg(f)}} (1+p^{d/2})p^{(2p^s-1)d/2}$$

where $N_1 = \begin{cases} 0 & \text{if } p=2 \\ 0 & \text{if } k \text{ is even and } p \text{ is odd} \\ p^{p^s-1}(p+1) & \text{if } k \text{ is odd and } p \text{ is odd} \end{cases}$

and $N_{-1} = \begin{cases} 1 & \text{if } k \text{ is even and } p \text{ is odd} \\ 0 & \text{if } k \text{ is odd and } p \text{ is odd.} \end{cases}$

Proof. If $f(x^2) \in \mathbb{F}_p[x^2]$ is irreducible in $\mathbb{F}_p[x^2]$ with degree d, according to [21], the number of monic irreducible right factors of $f(x^2)$ is equal to $1+p^d$, and according to Lemma 3.4 of [7], the number of irreducible monic right factors h_1 of $f(x^2)$ such that $\Theta^b(h_1^\natural)\cdot h_1 = f(x^2)$ is equal to $1+p^{d/2}$. Therefore according to Lemma 6, if $f(x^2)$ belongs to $\mathcal{F}_{ir}$, the number of monic skew polynomials of degree md in $\mathcal{L}^{(b)}_{f(x^2)^m}$ is $((p^d+1)-(1+p^{d/2}))(1+p^d-1)^{m-1} = (p^d-p^{d/2})p^{d(m-1)}$.

If $f(x^2)$ belongs to $\mathcal{F}_{red}$, $\mathcal{L}^{(b)}_{f(x^2)^m} \setminus \{1, f(x^2)^m\}$ has $(1+p^{d/2})p^{(2m-1)d/2}$ elements where $\delta = d/2$ and d is the degree of $f(x^2)$ in x^2. Namely, according to Lemma 7, the elements of $\mathcal{L}^{(b)}_{f(x^2)^m} \setminus \{1, f(x^2)^m\}$ are the skew polynomials g in bijection with the couples (g_1, g_2) satisfying (4). There are $1+p^\delta$ possibilities for $g_{1,1}$ and p^δ possibilities for each $g_{1,j}$, with $j = 2, \ldots, m$, therefore $(1+p^\delta)p^{\delta(m-1)}$ possibilities for g_1. For each j in $\{1, \ldots, m\}$ there are p^δ possibilities for $g_{2,j}$, therefore, one gets $p^{\delta m}$ possibilities for g_2.

Lastly the value of N is deduced from the cardinalities of $\mathcal{L}^{(b)}_{(x^2\pm1)^{p^s}}$ (Proposition 7).

□

We give below some detailed examples over $\mathbb{F}_4$, $\mathbb{F}_{25}$ and $\mathbb{F}_{49}$ who illustrate Proposition 9 and Algorithm 3.

Example 13. *One has $x^6+1 = (x^2+1)(x^4+x^2+1)$ in $\mathbb{F}_2[x^2]$. For $\theta : a \mapsto a^2$, the Euclidean LCD θ-cyclic codes of length 6 over $\mathbb{F}_4 = \mathbb{F}_2(w)$ are generated by the monic skew polynomials*

Dimension	Number	Best minimum distance	A skew generator polynomial
10	4	2	$g_1 = (x+1)\cdot(x+w^2)$
8	9	3	$g_2 = (x^2+ax+1)\cdot(x^2+w^2x+1)$
6	32	5	$\mathrm{lclm}(g_1, g_2)$
4	9	6	$(x^4+1)\cdot g_2$
2	4	9	$(x^8+x^4+1)\cdot g_1$

Table 4: Euclidean LCD skew-cyclic codes over $\mathbb{F}_4$ of length 12 and dimension $\leqslant 12$

$g = \mathrm{lclm}(g_1, g_2)$ where $g_1 \in \mathcal{L}^{(0)}_{x^2+1} = \{x+w, x+w^2, 1, x^2+1\}$ and $g_2 \in \mathcal{L}^{(0)}_{x^4+x^2+1} = \{x^2+wx+1, x^2+w^2x+1, 1, x^4+x^2+1\}$. There are four $[6,3]_4$ Euclidean LCD θ-cyclic codes.

These codes are also Hermitian self-dual. Namely $x+w = \Theta(x+w^2) = \Theta((x+w^2)^\natural)$ and $\Theta((x+w^2)^\natural)\cdot(x+w^2) = x^2+1$. Furthermore, $x^2+wx+1 = \Theta(x^2+w^2x+1) = \Theta((x^2+wx+1)^\natural)$ and $\Theta((x^2+wx+1)^\natural)\cdot(x^2+wx+1) = x^4+x^2+1$ therefore the above skew polynomials g all satisfy $g = \Theta(h^\natural)$ where $\Theta(h^\natural)\cdot h = x^6-1$.

Example 14. *There are 32 Euclidean LCD θ-cyclic codes of length 12 and dimension 6 over $\mathbb{F}_4$ where $\theta : a \mapsto a^2$. They are generated by the skew polynomials $g = \mathrm{lclm}(g_1, g_2)$ where $g_1 \in \{(x+1)\cdot(x+w), (x+w)\cdot(x+w), (x+1)\cdot(x+w^2), (x+w^2)\cdot(x+w^2)\}$ and $g_2 \in \{(x^2+w)\cdot(x^2+wx+1), (x^2+w^2)\cdot(x^2+wx+1), (x^2+x+1)\cdot(x^2+wx+1), (x^2+w^2x+1)\cdot(x^2+wx+1), (x^2+w)\cdot(x^2+w^2x+1), (x^2+w^2)\cdot(x^2+w^2x+1), (x^2+x+1)\cdot(x^2+w^2x+1), (x^2+wx+1)\cdot(x^2+w^2x+1)\}$.*

Table 4 below sums up the repartition of all the Euclidean LCD θ-cyclic codes of length 12 over $\mathbb{F}_4$ and gives one example for each dimension.

Example 15. *As $x^{14}+1 = (x^2+1)(x^6+x^4+1)(x^6+x^2+1)$ over $\mathbb{F}_2[x^2]$, there are $2\times(1+2^3)\times 2^3 = 144$ Euclidean LCD θ-cyclic codes of length 14 and dimension 7 over $\mathbb{F}_4$ where $\theta : a \mapsto a^2$. For example, consider $g_0 = x+w$, $g_1 = x^3+x^2+w^2x+1$ and $g_2 = x^3+w^2x^2+x+w$. g_1 is a right divisor of x^6+x^2+1 and g_2 is a right divisor of x^6+x^4+1. Furthermore $h_2 = x^3+wx^2+x+w^2$ is such that $g_2\cdot h_2 = x^6+x^4+1$ and $h_2^\natural = x^3+w^2x^2+wx+w^2 \neq g_1$ therefore $g = \mathrm{lclm}(g_0, g_1, g_2) = 1+w^2x+wx^2+w^2x^4+w^2x^5+wx^6+x^7$ generates an Euclidean LCD θ-cyclic code of length 14 over $\mathbb{F}_4$. The minimum distance of the code is equal to 6.*

Example 16. *Consider θ the Frobenius automorphism over $\mathbb{F}_{25} = \mathbb{F}_5(w)$ where $w^2+4w+2 = 0$. The skew polynomial $g = x^7+4x^6+w^4x^5+w^7x^4+w^7x^3+w^{16}x^2+w^8x+w^{20}$ generates a MDS $[14,7,8]_{25}$ θ-cyclic code over $\mathbb{F}_{25}$ which a LCD code for the Euclidean scalar product and for the Hermitian scalar product. The skew polynomial g is obtained as $g = \mathrm{lclm}(g_1, g_2)$ where $g_1 = x+w^{16}$ belongs to $\mathcal{L}^{(0)}_{x^2-1} \cap \mathcal{L}^{(1)}_{x^2-1}$ and $g_2 = x^6+w^{11}x^5+2x^4+w^3x^3+2x^2+w^{11}x+1$ belongs to $\mathcal{L}^{(0)}_{x^{12}+x^{10}+x^8+x^6+x^4+x^2+1} \cap \mathcal{L}^{(1)}_{x^{12}+x^{10}+x^8+x^6+x^4+x^2+1}$.*

Example 17. *Consider θ the Frobenius automorphism over $\mathbb{F}_{49} = \mathbb{F}_7(w)$ where $w^2+6w+3 = 0$. The skew polynomial $g = x^8+6x^7+w^7x^6+w^{28}x^5+w^{11}x^4+w^{47}x^3+w^{10}x^2+w^{30}x+w^{12}$ generates a MDS $[16,8,9]_{49}$ θ-negacyclic code over $\mathbb{F}_{49}$ which is both an Euclidean LCD code and a Hermitian LCD code. The skew polynomial g is obtained as $g = \mathrm{lclm}(g_1, g_2)$ where $g_1 = x^4+w^{39}x^3+w^3x^2+w^{33}x+1$ belongs to $\mathcal{L}^{(0)}_{x^8+4x^4+1} \cap \mathcal{L}^{(1)}_{x^8+4x^4+1}$ and $g_2 = x^4+5x^3+w^{30}x^2+w^{35}x+w^6$ belongs to $\mathcal{L}^{(0)}_{x^8+3x^4+1} \cap \mathcal{L}^{(1)}_{x^8+3x^4+1}$.*

Lastly, Table 5 and Table 6 illustrate Proposition 9 over $\mathbb{F}_4$ and $\mathbb{F}_9$. Best minimum distances and numbers of LCD $[2k,k]$ skew cyclic and negacyclic codes over $\mathbb{F}_4$ and $\mathbb{F}_9$ are given in the case when the skew generator polynomials are not divisible by any central polynomial. The index $*$ means that the minimum distance is the best known minimum distance of codes with these parameters.

Tables 7 sums up the dimensions of MDS LCD skew codes of given length ≤ 10 over $\mathbb{F}_9$. Tables 8 and 9 sum up the dimensions of MDS LCD skew codes of length ≤ 18 over $\mathbb{F}_{25}$ and of length ≤ 16 over $\mathbb{F}_{49}$.

Euclidean LCD skew cyc.			Euclidean LCD skew cyc.		
length	best dist	nbr	length	best dist	nbr
2	2*	2	26	9	8 064
4	3*	4	28	11*	18 432
6	4*	4	30	12*	13 056
8	4*	16	32	10	65 536
10	5*	24	34	11*	115 200
12	5	32	36	11	114 688
14	6*	144	38	12*	523 264
16	6	256	40	12*	786 432
18	7	224	42	12	1 198 080
20	8*	768	44	13	4 063 232
22	8*	1 984	46	14*	8 392 704
24	9*	2 048	48	14*	8 388 608

Table 5: Best minimum distances and numbers of Euclidean LCD $[2k, k]$ skew cyclic codes of length ≤ 48 over $\mathbb{F}_4$ with skew generator polynomial not divisible by a central polynomial

	Euclidean LCD				Hermitian LCD			
	skew cyc		skew negacyc		skew cyc		skew negacyc	
length	best dist	nbr	best dist	nbr	best dist	nbr	best dist	nbr
2	2*	2	2*	4	2*	4	0	0
4	3*	32	3*	6	0	0	3*	6
6	4*	18	4*	36	4*	361	0	0
8	5*	192	5*	90	0	0	5*	90
10	6*	144	6*	288	6*	288	0	0
12	6*	5 408	6*	486	0	0	6*	486
14	7*	1 404	7*	2 808	7*	2 808	0	0
16	7	17 280	8*	6 642	0	0	8*	6 642
18	9*	13 122	9*	26 244	9*	26 244	0	0
20	9	165 888	9	39 852	0	0	10*	39 852
22	9*	118 584	9*	237 168	9*	237 168	0	0
24	10*	2 628 288	10*	590 490	0	0	10*	590 490

Table 6: Best minimum distances and numbers of LCD $[2k, k]$ skew codes of length ≤ 24 over $\mathbb{F}_9$ with skew generator polynomial not divisible by a central polynomial

	MDS Euclidean LCD		MDS Hermitian LCD	
length	skew cyc	skew nega	skew cyc	skew nega
4	2	2	no	2
6	3	3	3	no
8	3,4,5	4	3,5	4
10	5	5	5	no

Table 7: Dimensions of *MDS* LCD skew codes over $\mathbb{F}_9$ with length $n \leq 10$ and dimension $1 < k < n - 1$

	MDS Euclidean LCD		MDS Hermitian LCD	
length	skew cyc	skew nega	skew cyc	skew nega
4	2	2	no	2
6	2,3,4	2,3,4	2,3,4	2,4
8	3,4,5	4	3,5	4
10	5	5	5	no
12	3,5,6,7,9	6	3,5,7,9	6
14	7	7	7	no
16	7,8,9	no	7,9	no
18	9	9	9	no

Table 8: Dimensions of *MDS* LCD skew codes over $\mathbb{F}_{25}$ with length $n \leq 18$ and dimension $1 < k < n - 1$

	MDS Euclidean LCD		MDS Hermitian LCD	
length	skew cyc	skew nega	skew cyc	skew nega
4	2	2	no	2
6	2,3,4	2,3,4	2,3,4	2,4
8	3,4,5	2,4,6	3,5	2,4,6
10	4,5,6	4,5,6	4,5,6	4,6
12	3,5,6,7,9	6	3,5,7,9	6
14	7	7	7	no
16	3,5,7,8,9,11,13	8	3,5,7,9,11,13	8

Table 9: Dimensions of *MDS* LCD skew codes over $\mathbb{F}_{49}$ with length $n \leq 16$ and dimension $1 < k < n - 1$

6 Conclusion

In this text, skew LCD codes are studied. LCD skew cyclic and negacyclic codes are constructed and enumerated over $\mathbb{F}_{p^2}$. Some computations are made and MDS LCD codes are constructed. It could be interesting to see if there exists $[2p, p]_{p^2}$ MDS LCD codes for p odd prime greater than 11.

Acknowledgements. The third author is supported by the French government Investissements d'Avenir program `ANR-11-LABX-0020-01`.

References

[1] Abualrub, T., Aydin, N., Ghrayeb, A. and Siap, I. : *On the construction of skew quasicyclic codes*, IEEE. Trans. Inf. Theory 56, 2081-2090 (2010).

[2] Batoul, A., Guenda, K., Gulliver, T.A. :*Some constacyclic codes over finite chain rings*, Advances in Mathematics of Communications, 10, 683-694 (2016).

[3] Boucher, D. : *Construction and number of self-dual skew codes over* $\mathbb{F}_{p^2}$, Advances in Mathematics of Communications (AMC), Vol. 10, no. 4 November 2016, Pages 765-795

[4] Boucher, D. and Ulmer, F. : *Coding with skew polynoial rings*, Journal of Symbolic Computation, 44,1644-1656 (2009).

[5] Boucher, D. and Ulmer, F. : *Self-dual skew codes and factorization of skew polynomials.* Journal of Symbolic Computation, 60, 47-61 (2014).

[6] Boucher, D., Geiselmann, W. and Ulmer, F. : *Skew cyclic codes.* Applicable Algebra in Engineering, Communication and Computing, 18, 379-389 (2007).

[7] Boucher, D. : *A First Step Towards the Skew Duadic Codes.*Advances of Mathematics of Communications,Volume 12,No3,553-577,(2018)

[8] Boucher, D. and Ulmer, F. : *A note on the dual codes of module skew codes.* Cryptography and coding: 13th IMA international conference, IMACC 2011, Oxford, UK, December 12-15, 2011, Lecture Notes in Computer Science, vol. 7089, 978-3-642-25515-1.

[9] Carlet C., Mesnager S.,Tang C. and Qi Y. *Euclidean and Hermitian LCD MDS codes*, (2018), Volume 86, Issue 11, 2605-2618

[10] Fogarty, N.L. : *On Skew-Constacyclic Codes.*University of Kentucky, Phd dissertation (2016).

[11] Giesbrecht, M., *Factoring in skew-polynomial rings over finite fields*, Journal of Symbolic Computation, 26, 1998, 4, 463–486

[12] Güneria, C. and ÖOzkayaa B. and Solé P. *Quasi-cyclic complementary dual codes* Finite Fields and Their Applications, 42 (2016) 67-80

[13] M. Grassl, Table of bounds on linear codes, Available at: http://www.codetables.

[14] Li, Chengju, *Hermitian LCD codes from cyclic codes*, Des. Codes Cryptogr., 86, 2018, 2261–2278

[15] Li, C. and Ding, C. and Li, S., *LCD cyclic codes over finite fields*, IEEE Trans. Inform. Theory, 63, 2017, 7, 4344–4356

[16] MacWilliams, F. J. : *Combinatorial Properties of Elementary Abelian Groups*, Ph.D. thesis, Radcliffe College, Cambridge, MA, (1962).

[17] Massey, J.L., Yang, X. : *The condition for a cyclic code to have a complementary dual*. Discrete Mathematics, 126,391-393, (1994).

[18] Massey J.L. ,*Linear codes with complementary duals*,Discr. Math., 106-107, 337–342, (1992).

[19] Massey, J.L. : *Reversible codes*. Inform. and Control 7, 369-380, (1964).

[20] McDonald, B. R. : *Finite Rings With Identity*, Marcel Dekker Inc.,New York, (1974).

[21] Odoni R. W. K. :*On additive polynomials over a finite field*, Proc. Edinburgh Math. Soc., **42** (1999), 1-16.

[22] Ore, O. : *Theory of non-commutative polynomials*. Annals Math, 34, 480-508,(1933).

[23] Sharma, A. and Kaur, T., *Enumeration formulae for self-dual, self-orthogonal and complementary-dual quasi-cyclic codes over finite fields*, Cryptogr. Commun., 10, 2018, 3, 401–435