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

Ranya Boulanouar, Aicha Batoul, Delphine Boucher

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

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

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 $\mathbb{F}_{p^2}$.

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 polynomial 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.

On the other hand, constacyclic code 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 [14]. They provide an optimum linear coding solution for the two-user binary adder channel, and in [15] it was shown that asymptotically good LCD codes exist. Since then, several authors have studied these codes ([7, 10, 11, 12, 21]). But until now just a few works have been done on LCD codes in the noncommutative case.

This paper 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 (Theorem 1). In Section 4, the notion of LCD skew constacyclic codes is introduced and we give some characterizations of their skew generator polynomials (Theorem 2 and Theorem 3). Section 5 focuses on the construction (Algorithm 4) and the enumeration (Proposition 7) of LCD skew cyclic and negacyclic codes of even lengths over $\mathbb{F}_{p^2}$. If p is odd, the Euclidean LCD skew cyclic codes of length $2p^s$ and dimension p^s over $\mathbb{F}_{p^2}$ are all Hermitian LCD codes. Over $\mathbb{F}_{p^2}$, all MDS LCD skew codes of length $\leq \min(1+p^2, 16)$ are

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

[†]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

obtained when $p \in \{3, 5, 7\}$ (Tables 5, 6 and 7) as well as all $[2p, p]$ MDS LCD skew codes for $p \in \{3, 5, 7, 11\}$ (Table 1).

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

$$R = \mathbb{F}_q[x; \theta] = \{a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} \mid a_i \in \mathbb{F}_q \text{ and } n \in \mathbb{N}\}$$

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 [17], 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 $(c_0 + c_1 x^{\mu} + \ldots + c_n x^{n\mu}) x^l$, where l is an integer and c_i belongs to $\mathbb{F}_q^{\theta}$. Central elements of R are the generators of two-sided ideals in R [2]. 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

$$g = q \cdot f + r \text{ and } \deg(r) < \deg(f).$$

If $r = 0$ then f is a right divisor of g in R ([17]). There exist 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 $\mathbb{F}_q^*$.

According to [2] and [8], 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

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

Any element of the left R-module $R/R(x^n - \lambda)$ is uniquely represented by a polynomial $c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}$ of degree less than n, hence is identified with a word $(c_0, c_1, \ldots, c_{n-1})$ 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 R-submodule of the left R-module $R/R(x^n - \lambda)$, 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 $C = \langle g \rangle_n$.

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 $\mathbb{F}_q$ 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 [13]).

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 $\mathbb{F}_q^n$, $< x, y >:= \sum_{i=1}^n x_i y_i$ 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 $g^* = \Sigma_{i=0}^k \theta^i(g_{k-i}) x^i$. If g_0 does not cancel, 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 C a skew λ-constacyclic code of length n and skew generator polynomial g. According to Theorem 1 and Lemma 2 of [3], the Euclidean dual $C^\perp$ of C is a skew λ^{-1}-constacyclic code generated by $h^\natural$ where $\Theta^n(h) \cdot g = x^n - \lambda$ and for $a(x) = \sum a_i x^i \in R$, $\Theta(a(x)) := \sum \theta(a_i) x^i$. In particular, when λ is fixed by θ and n is a multiple of the order μ of θ, then h is fixed by Θ^n and $x^n - \lambda$ is central, therefore one gets $h \cdot g = g \cdot h = x^n - \lambda$. 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 lemmas will be useful later.

Lemma 1 *[4, Lemma 4] Consider h and g in R. Then $(h \cdot g)^* = \Theta^{\deg(h)}(g^*) \cdot h^*$.*

The following Lemma is given in Theorem 6.3.7 of [8] when $x^n - \lambda$ is a central element of R. We give a new proof and adapt it when $x^n - \lambda$ belongs to R.

Lemma 2 *Consider C_1 and C_2 two skew λ-constacyclic codes of length n over $\mathbb{F}_q$ with skew generator polynomials g_1 and g_2.*

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* $\mathrm{gcrd}(g_1, g_2)$.

Proof. In the left R-module $R/R(x^n - \lambda)$, we identify the image of P in R under the canonical morphism $R \to R/R(x^n - \lambda)$ with the remainder in the right division of P by $x^n - \lambda$ in R.

1. Consider $g = \mathrm{lclm}(g_1, g_2)$ in R. As g_1 and g_2 divide on the right $x^n - \lambda$, g divides $x^n - \lambda$ on the right therefore the skew λ-constacyclic code C of length n generated by g is well-defined. Let c in $R/R(x^n - \lambda)$. Then c belongs to $C_1 \cap C_2$ if and only if g_1 and g_2 divide c on the right in R, therefore c belongs to $C_1 \cap C_2$ if and only if g divides c on the right in R and one concludes that $C_1 \cap C_2 = C$.

2. Consider $g = \mathrm{gcrd}(g_1, g_2)$ in R. As g_1 and g_2 divide on the right $x^n - \lambda$, g divides $x^n - \lambda$ on the right, therefore one can consider the skew λ-constacyclic code C of length n generated by g.

As g divides g_1 and g_2 on the right, C_1 and C_2 are subsets of C, therefore $C_1 + C_2 \subset C$.

Conversely, consider c in C. As g divides c on the right, it follows by [19, Theorem 4] that $c = a \cdot g_1 + b \cdot g_2$ for some a and b in R, therefore c belongs to $C_1 + C_2$.

■

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 $\mathbb{F}_q^*$ and n in $\mathbb{N}^*$. For i in $\mathbb{N}^*$ and α element of $\mathbb{F}_q$, the i^{th} norm of α is defined as

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

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 *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 $\mathbb{F}_q$.*

2. 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.

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

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

Let us prove that the application Φ_α is an isomorphism which 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) :consider $f(x) = \sum a_i x^i$ and $g(x) = \sum b_i x^i$ in $R/R(x^n - 1)$ such that $\phi_\alpha(f(x)) = \phi_\alpha(g(x))$, then $a_i N_i(\alpha) = b_i N_i(\alpha)$ therefore $f(x) = g(x)$.
- 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 $R/R(x^n - 1)$. One has
  $f(x) \cdot g(x) = \sum_{j=0}^{n-1} \left(\sum_{i=0}^{j} a_i \theta^i(b_{j-i}) + \sum_{i=j+1}^{n-1} a_i \theta^i(b_{n-i+j}) \right) x^j$
  because $x^{j+n} = x^j$ in $R/R(x^n - 1)$.
  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, one has
  $\Phi_\alpha(f(x)) \cdot \Phi_\alpha(g(x)) = \sum_{j=0}^{n-1} \left(\sum_{i=0}^{j} a_i N_i(\alpha) \theta^i(b_{j-i} N_{j-i}(\alpha)) \right) x^j +$
  $\sum_{j=0}^{n-1} \left(\sum_{i=j+1}^{n-1} a_i N_i(\alpha) \theta^i(b_{n-i+j} N_{n+j-i}(\alpha)) \right) x^{j+n}.$
  As $x^{j+n} = x^j \cdot (x^n - \lambda) + x^j \lambda = \theta^j(\lambda) x^j$ in $R/R(x^n - \lambda)$, one gets
  $\Phi_\alpha(f(x)) \cdot \Phi_\alpha(g(x)) = \sum_{j=0}^{n-1} \left(\sum_{i=0}^{j} a_i \theta^i(b_{j-i}) N_i(\alpha) \theta^i(N_{j-i}(\alpha)) + \right.$
  $\left. \sum_{i=j+1}^{n-1} a_i \theta^i(b_{n-i+j}) N_i(\alpha) \theta^i(N_{n+j-i}(\alpha)) \theta^j(\lambda) \right) x^j.$
  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 $c(x) = \sum_{i=0}^{n-1} c_i x^i \in R/R(x^n - 1)$, then $\Phi_\alpha(c(x)) = \sum_{i=0}^{n-1} c_i N_i(\alpha) x^i$, therefore $wt(c(x)) = wt(\Phi_\alpha(c(x)))$.

To conclude, consider the monomial transformation $T : (c_0, \ldots, c_{n-1}) \mapsto (N_0(\alpha)c_0, \ldots, N_{n-1}(\alpha)c_{n-1})$. Then for any right divisor g of $x^n - 1$, T takes the skew cyclic code $C =< g >_n$ to the skew λ-constacyclic code with skew generator polynomial $\Phi_\alpha(g)$.

2. Consider α in $\mathbb{F}_q^*$ such that $\lambda = -N_n(\alpha^{-1})$. Define
$$\begin{aligned} \Psi_\alpha \ : \ R/R(x^n + 1) &\longrightarrow R/R(x^n - \lambda) \\ f(x) &\longmapsto f(\alpha x) \end{aligned}$$
As for the proof of item 1, we prove that Ψ_α is a ring isomorphism.

- One has $\Psi_\alpha(x^n+1) = N_n(\alpha)x^n + 1 = N_n(\alpha)(x^n - \lambda)$, therefore Ψ_α is well defined.
- Ψ_α is injective and bijective.
- 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 $R/R(x^n+1)$. One has $\Psi_\alpha(f(x)) \cdot \Psi_\alpha(g(x)) = \sum_{j=0}^{n-1} \left(\sum_{i=0}^{j} a_i \theta^i(b_{j-i}) - \sum_{i=j+1}^{n-1} a_i \theta^i(b_{n-i+j}) \right) N_j(\alpha) x^j = \Psi_\alpha(f(x) \cdot g(x))$.

■

Example 1 *Consider $\mathbb{F}_{2^4} = \mathbb{F}_2(w)$ where $w^4 = w + 1$, θ the automorphism of $\mathbb{F}_{2^4}$ given by $a \mapsto a^{2^2}$. We have 33 skew cyclic codes of length 4 over $\mathbb{F}_{16}$. For example, as $x^4 - 1 = (x^2 + w^{13}x + w^9) \cdot (x^2 + w^{13}x + w^6)$, the skew polynomial $g = x^2 + w^{13}x + w^6$ generates a skew cyclic code C of length 4 over $\mathbb{F}_{2^4}$. Consider $\lambda = w^5$. The set of α in $\mathbb{F}_{2^4}^*$ such that $N_4(\alpha^{-1}) = \lambda$ is $\{w, w^4, w^7, w^{10}, w^{13}\}$. The skew polynomial $\Phi_{w^{13}}(g) = x^2 + w^6 x + w$ generates a skew w^5-constacyclic code of length 4 over $\mathbb{F}_{16}$ equivalent to the skew cyclic code C.*

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

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 $\lambda = N_n(-1)$. As n is odd, $\lambda = -1$ and we conclude with point 1. of 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 $C = \langle x^3 + x^2 + x + 1 \rangle_4$ 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 *[1, Lemma 3.1] Let α be a primitive element of $\mathbb{F}_q$ and $\lambda = \alpha^i$ for $i \leq q - 1$. Then the equation $\delta^s = \lambda$ has a solution in $\mathbb{F}_q$ if and only if $\gcd(s, q-1) \mid i$.*

In the following, we give a similar result of [1, 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 $\gcd([n], q - 1) = 1$ where $[n] := \frac{p^{rn}-1}{p^r-1}$. Then for all λ in $\mathbb{F}_q^*$, the 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. Consider λ in $\mathbb{F}_q^*$ and α a primitive element of $\mathbb{F}_q$. Then there exists an integer i such that $\lambda = \alpha^i$. As $\gcd([n], q-1) = 1 \mid i$, according to Lemma 4, there exists δ in $\mathbb{F}_q^*$ such that $\lambda = \delta^{[n]}$. Furthermore $N_n(\delta) = \delta^{[n]}$, therefore by Theorem 1 (with $\alpha = 1/\delta$), 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. Consider a a primitive element of $\mathbb{F}_q$ and $\lambda = a^{\frac{p^n-1}{2}} = -1$. As $\gcd(\frac{p^n-1}{p-1}, p^n-1) = \frac{p^n-1}{p-1}$ divides $\frac{p^n-1}{2}$, according to Lemma 4, there exists δ in $\mathbb{F}_q^*$ such that $\delta^{\frac{p^n-1}{p-1}} = \lambda$. Taking $\alpha = 1/\delta$ one gets $N_n(\alpha) = -1$. One concludes thanks to point 1 of Theorem 1. ∎

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 $\theta : a \mapsto a^3$ and $w \in \mathbb{F}_9$ such that $w^2 = w+1$. The application*

$$\Phi_w : \left\{ \begin{array}{ccc} R/R(x^2-1) & \to & R/R(x^2+1) \\ x & \mapsto & wx \end{array} \right.$$

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

Lemma 5 *Assume that n is odd and consider 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 $\phi_\alpha(h)^* = (-1)^k \phi_\alpha(h^*)$. ∎

Lemma 6 *If n is odd and C is a skew cyclic code of length n then the (Euclidean) 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 monic skew generator polynomial g. Then the monic skew generator polynomial of $D = \Phi_{-1}(C)$ is $G = (-1)^r \Phi_{-1}(g)$ where $r = \deg(g) = n - k$. Furthermore, consider h in R such that $\Theta^n(h) \cdot g = x^n - 1$, then $\Theta^n(H) \cdot G = x^n + 1$ 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. ∎

Proposition 3 *Let C be an LCD skew cyclic code of odd length over $\mathbb{F}_q$ then C is equivalent to an LCD skew negacyclic code.*

Proof. According to Theorem 1, the code C is equivalent to the skew negacyclic code $D = \Phi_{-1}(C)$. Let us prove that D is LCD. Consider c in $D \cap D^{\perp}$. According to Lemma 6 we have : $\Phi_{-1}(C) \cap \Phi_{-1}(C)^{\perp} = \Phi_{-1}(C) \cap \Phi_{-1}(C^{\perp})$. Therefore there exists u in C and v in $C^{\perp}$ such that $c = \Phi_{-1}(u) = \Phi_{-1}(v)$. As Φ_{-1} is a bijection, $u = v$ and as C is LCD, $u = v = 0$, therefore $c = 0$. ∎

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

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 positive integer. 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 in $\mathbb{N}^*$ and $\lambda \in \{-1, 1\}$. Consider a (θ, λ)-constacyclic code C with length n, skew generator polynomial g. Consider h in R such that $\Theta^n(h) \cdot g = x^n - \lambda$.*

1. *C is a EuclideanLCD 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 a 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 $x^n - \lambda$ on the right, f divides $x^n - \lambda$ on the right. Assume that $C \cap C^{\perp} = \{0\}$, then $x^n - \lambda$ divides f on the right, therefore $x^n - \lambda = f$. According to [19], $\deg(\mathrm{gcrd}(g, h^{\natural})) + \deg(\mathrm{lclm}(g, h^{\natural})) = \deg(g) + \deg(h^{\natural})$, 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 $x^n - \lambda$ on the right, $f = x^n - \lambda$, 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* $C = \langle x^2+w^7x+1\rangle_4$ *of length* 4 *and minimum distance* 3 *is a EuclideanLCD code over* $\mathbb{F}_9$.

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* $C = \langle x^3+w^7x^2+x+2\rangle_6$ *of length* 6 *and minimum distance* 4 *is a Hermitian LCD code over* $\mathbb{F}_9$.

Over a finite field $\mathbb{F}_q$, if a cyclic code C generated by a monic polynomial g is a EuclideanLCD code then $g = g^\natural$. Furthermore if q is coprime with n, then $g = g^\natural$ if and only if C is a EuclideanLCD code ([14], [16]). This comes from the fact that when q is coprime with n then $x^n - 1 = gh = \mathrm{lclm}(g, h)$ is squarefree in $\mathbb{F}_q[x]$ therefore, if $g = g^\natural$, then g and $h = h^\natural$ are coprime in $\mathbb{F}_q[x]$.

Over $\mathbb{F}_q[x;\theta]$ we generalize this result in Proposition 4 by using the notion of similarity :

Definition 1 ([19]) *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* $\mathrm{gcrd}(a, u) = 1$.

Proposition 4 *Consider* $\mathbb{F}_q$ *a finite field,* θ *an automorphism of* $\mathbb{F}_q$, $R = \mathbb{F}_q[x;\theta]$, n *a positive integer,* $k \leq n$, λ *in* $\{-1, 1\}$, g *a monic right divisor of* $x^n - \lambda$ *in* R *with constant coefficient* g_0 *and degree* $n-k$, $G = \Theta^{k-n}(g^* \cdot \frac{1}{g_0})$ *and* h *in* R *such that* $\Theta^n(h) \cdot g = x^n - \lambda$. *Consider a* (θ, λ)*-constacyclic code* C *with length* n *and monic skew generator polynomial* g.

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

Proof. As $\Theta^n(h) \cdot g = x^n - \lambda$, according to Lemma 1, $x^n - 1/\lambda = -1/\lambda\Theta^{k-n}(g^*) \cdot h^*$, therefore $G \cdot h^\natural = x^n - \lambda$ where $G = \Theta^{k-n}(g^* \cdot \frac{1}{g_0})$. In particular, $f = \mathrm{lclm}(g, h^\natural)$ divides $x^n - \lambda$ on the right.

1. Assume that $\mathrm{gcrd}(g, h^\natural) = 1$, then $\deg(f) = \deg(g) + \deg(h^\natural) = n$, therefore, one has $f = x^n - \lambda = G \cdot h^\natural$. As $\mathrm{lclm}(g, h^\natural) = G \cdot h^\natural$ 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 $\mathrm{lclm}(g, h) = x^n - \lambda$, one deduces that $\mathrm{gcrd}(g, h^\natural) = \mathrm{gcrd}(g, h) = 1$, therefore C is a EuclideanLCD 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* $\Theta(G)$.

We are now going to characterize the skew generators of LCD skew cyclic and negacyclic codes as least common left multiples of skew polynomials when the order of θ divides the length of the codes. This will enable to give a construction and an enumeration of LCD skew cyclic and negacyclic codes of even length 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 [4] and Proposition 2 of [5]. 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 $h_1, \ldots, h_r$ in 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 $\mathrm{gcrd}(g, \Theta^b(h^\natural)) = 1$.

  First of all, as $h_1, \ldots, h_r$ divide respectively $f_1(x^\mu), \ldots, f_r(x^\mu)$, and as $f_1(x^\mu), \ldots, f_r(x^\mu)$ are pairwise coprime central polynomials, the degree of $h = \mathrm{lcrm}(h_1, \ldots, h_r)$ is equal to $\sum_{i=1}^{r} \deg(h_i)$. In the same way, the degree of $g = \mathrm{lclm}(g_1, \ldots, g_r)$ 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 $\{1, \ldots, r\}$, 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 $\mathrm{gcrd}(g, \Theta^b(h^\natural)) = \mathrm{gcrd}(\mathrm{lclm}(g_1, \ldots, g_r), \mathrm{lclm}(\Theta^b(h_1^\natural), \ldots, \Theta^b(h_r^\natural)))$. One can notice that the skew polynomials g_i and $\Theta^b(h_j^\natural)$ are right coprime. Namely, if $i = j$, $\mathrm{gcrd}(g_i, \Theta^b(h_i^\natural)) = 1$ 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 $F(x^\mu) = f_1(x^\mu) \cdots f_r(x^\mu)$, therefore, as f_i and f_j are coprime, according to Theorem 4.1 of [9], $g = \text{lclm}(g_1, \ldots, g_r)$ where $g_i = \text{gcrd}(f_i(x^\mu), g)$ and this lclm-decomposition into skew polynomials dividing $f_1(x^\mu), \ldots, f_r(x^\mu)$ 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 [9], $h = \text{lcrm}(h_1, \ldots, h_r)$ where $h_i = \text{gcld}(f_i(x^\mu), h)$. This lcrm-decomposition into skew polynomials dividing $f_1(x^\mu), \ldots, f_r(x^\mu)$ is unique and $\deg(h) = \sum_{i=1}^r \deg(h_i)$.

  Consider, for i in $\{1, \ldots, r\}$, 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, $g_i \cdot h_i = \text{lclm}(\text{gcrd}(g_i \cdot h_i, f_j(x^\mu)), j = 1, \ldots, r) = \text{gcrd}(g_i \cdot h_i, f_i(x^\mu))$ 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 additional 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 $f_1(x^\mu), \ldots, f_r(x^\mu)$ are distinct 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. C is a Euclidean(resp. a Hermitian) LCD code if and only if*

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

where

$$\begin{cases} I, J \subset \{1, \ldots, r\} \\ I \cap J = \emptyset \\ \forall j \in J, g_j \in \mathcal{L}^{(b)}_{f_j(x^\mu)^{p^s}} \setminus \{1, f_j(x^\mu)^{p^s}\} \text{ with } b = 0 \text{ (resp } b = 1). \end{cases}$$

Proof. According to Theorem 2, the Euclidean (resp. Hermitian) LCD (θ, λ)-constacyclic codes of length n are generated by the elements of the set $\mathcal{L}^{(b)}_{x^n - \lambda}$ 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

distinct self-reciprocal polynomials of $\mathbb{F}_p[x^\mu]$ which 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 Proposition 5 can be applied to $F(x^\mu) = x^n \pm 1$. One gets that $g = \mathrm{lclm}(g_1, \ldots, g_r)$ where for all i in $\{1, \ldots, r\}$, $g_i \in \mathcal{L}^{(b)}_{f_i(x^\mu)^{p^s}}$.

Now consider the sets $I, J, K \subset \{1, \ldots, r\}$ that form a partition of $\{1, \ldots, r\}$ such that $\forall i \in I, g_i = f_i(x^\mu)^{p^s}, \forall i \in J, g_i \in \mathcal{L}^{(b)}_{f_i(x^\mu)^{p^s}} \setminus \{1, f_i(x^\mu)^{p^s}\}$ and $\forall i \in K, g_i = 1$. As $f_i(x^\mu)$ is central and as the f_i are pairwise coprime, one gets that $g = \prod_{i \in I} f_i(x^\mu)^{p^s} \ \mathrm{lclm}_{j \in J}(g_j)$.

■

Remark 1 *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 of length n generated by $g_i \in \mathcal{L}^{(0)}_{f_i(x^\mu)^{p^s}}$. 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 $g_i \in \mathcal{L}^{(0)}_{f_i(x^\mu)^{p^s}}$).*

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

In [7, 10, 21], constructions and enumerations of families of LCD codes were provided. 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 codes given by Theorem 3 to design an algorithm of construction of these codes (Algorithm 4). In the case when the skew generator polynomials of the codes are not divisible by any central polynomial, a counting formula will be given (Proposition 7).

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 8);
- $f(x^2) \in \mathcal{F}_{ir}$ irreducible in $\mathbb{F}_p[x^2]$ with degree $d > 1$ in x^2 (see Lemma 7);
- $f(x^2) \in \mathcal{F}_{red}$ is the product of two irreducible distinct polynomials in $\mathbb{F}_p[x^2]$ (see Lemma 9).

The following proposition enables to characterize those skew polynomials over $\mathbb{F}_{p^2}[x; \theta]$ having a unique factorization into the product of monic irreducible skew polynomials. It will be useful later.

Proposition 6 (Proposition 16 of [4]) *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 skew polynomials dividing f. The following assertions are equivalent :*

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

(ii) f *does not divide* h *in* R*;*

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

Lemma 7 describes the set $\mathcal{L}^{(b)}_{f(x^2)^m}$ and its number of elements where $f(x^2)$ belongs to $\mathcal{F}_{ir}$. Algorithm 1 enables to construct this set.

Lemma 7 *Consider* p *a prime number,* $\theta : a \mapsto a^p$ *the Frobenius automorphism over* $\mathbb{F}_q$ *with* $q = p^2$, $R = \mathbb{F}_q[x;\theta]$, $f(x^2) \in \mathcal{F}_{ir}$ *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*

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

Furthermore, the number of elements of $\mathcal{L}^{(b)}_{f(x^2)^m} \setminus \{1, f(x^2)^m\}$ *is* $(p^d - p^{d/2})p^{d(m-1)}$.

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 $\{1,\dots,2m-1\}$, $g_1,\dots,g_{2m-r}, h_1,\dots,h_r$ monic of degree d dividing $f(x^2)$ in R 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 $\mathrm{gcrd}(\Theta^b(h^{\natural}), g) = 1$. 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 $\{1,\dots,m-1\}$, $g_{i+1}\cdot g_i \neq f(x^2)$.
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 $g_1,\dots,g_m$ 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 monic 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 $\mathrm{gcrd}(g, \Theta^b(h^{\natural})) = 1$ and g belongs to $\mathcal{L}^{(b)}_{f(x^2)^m}$.

Let us compute the number of elements of $\mathcal{L}^{(b)}_{f(x^2)^m} \setminus \{1, f(x^2)^m\}$. We first notice that $g_1 \neq \Theta^b(h_1^{\natural})$ where $g_1\cdot h_1 = f(x^2)$ if and only if g_1 is a divisor of $f(x^2)$ which does not belong to $\{\Theta^b(u^{\natural}) \mid \Theta^b(u^{\natural})\cdot u = f(x^2)\}$. According to [18], the number of monic irreducible right factors of $f(x^2)$ is equal to $1+p^d$, where d is the degree of $f(x^2)$. According to Lemma 3.4 of [6], the number of irreducible monic right factors u of $f(x^2)$ such that $\Theta^b(u^{\natural})\cdot u = f(x^2)$ is equal to $1+p^{d/2}$. Therefore, the number of monic skew polynomials of degree md in $\mathcal{L}^{(b)}_{f(x^2)^m} \setminus \{1, f(x^2)^m\}$ is $((p^d+1)-(1+p^{d/2}))(1+p^d-1)^{m-1} = (p^d - p^{d/2})p^{d(m-1)}$. ∎

Algorithm 1 $\mathcal{L}^{(b)}_{f(x^2)^m}$ for $f(x^2) \in \mathcal{F}_{ir}$, $b \in \{0,1\}$ 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 $f(x^2) \in \mathcal{F}_{ir}$
Ensure: : $\mathcal{L}^{(b)}_{f(x^2)^m}$
1: $E \leftarrow \{1, f(x^2)^m\}$
2: $d \leftarrow \deg_{x^2}(f(x^2))$
3: $I \leftarrow \{g \in R, g \text{ monic, } g \text{ irreducible of degree } d \text{ dividing } f(x^2)\}$ (using Algorithm 1 of Appendix A of [6])
4: **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**
5: $\quad E \leftarrow E \cup \{g_m \cdots g_1\}$
6: **end for**
7: **return** E

Lemma 8 describes the set $\mathcal{L}^{(b)}_{(x^2 \pm 1)^m}$ and its number of elements. Algorithm 2 enables to construct this set.

Lemma 8 *Consider p a prime number, $\theta : a \mapsto a^p$ the Frobenius automorphism over $\mathbb{F}_q$ with $q = p^2$, $R = \mathbb{F}_q[x;\theta]$, $\epsilon \in \{-1,1\}$, g in R and $m \in \mathbb{N}$. The skew polynomial g belongs to the set $\mathcal{L}^{(b)}_{(x^2-\epsilon)^m}$ if and only if $g = 1$ or $g = (x^2-\epsilon)^m$ or g has a unique factorization into the product of m monic linear skew polynomials $g = (x+\alpha_m)\cdots(x+\alpha_1)$ where*

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

if $b = 0$ and

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

if $b = 1$, $\epsilon = 1$ and $p \neq 2$.
Furthermore, the number of elements of $\mathcal{L}^{(b)}_{(x^2-\epsilon)^m} \setminus \{1, (x^2-\epsilon)^m\}$ is

$$\begin{cases} 2^m & \text{if } p = 2, b = 0; \\ p^{m-1}(p - \epsilon(-1)^{(p+1)/2}) & \text{if } p \neq 2, b = 0; \\ 0 & \text{if } b = 1, p = 2 \text{ or } p \text{ odd and } \epsilon = -1; \\ p^{m-1}(p+1) & \text{if } b = 1, p \text{ odd and } \epsilon = 1. \end{cases}$$

Proof. Consider g in R. Like in proof of Lemma 7, one gets that g belongs to $\mathcal{L}^{(b)}_{(x^2-\epsilon)^m}$ if and only if $g = 1$ or $g = (x^2-\epsilon)^m$ or g has a unique factorization into the product of m monic linear skew polynomials $g = (x+\alpha_m)\cdots(x+\alpha_1)$ where

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

Therefore $g \neq 1, (x^2-\epsilon)^m$ belongs to the set $\mathcal{L}^{(b)}_{(x^2-\epsilon)^m}$ if and only if g has a unique factorization in R as $g = (x+\alpha_m)\cdots(x+\alpha_1)$ where

$$\begin{cases} \alpha_i^{p+1} = \epsilon \\ \alpha_{i+1} \neq -\epsilon/\alpha_i \\ \epsilon \neq -\theta^{b+1}(\alpha_1)/\alpha_1. \end{cases} \quad (4)$$

If $b = 0$, the condition (4) is equivalent to $\alpha_i^{p+1} = \epsilon, \alpha_{i+1} \neq -\epsilon/\alpha_i$ and $\alpha_1^2 \neq -\epsilon$. Therefore the number of skew polynomials in $\mathcal{L}^{(0)}_{(x^2-\epsilon)^m} \setminus \{1, (x^2-\epsilon)^m\}$ is

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

In the same way, one gets that $\mathcal{L}^{(1)}_{(x^2-\epsilon)^m} = \{1, (x^2-\epsilon)^m\}$ if $p = 2$ or p is odd and $\epsilon = -1$. If $\epsilon = 1$ and $p \neq 2$, condition (4) is equivalent to $\alpha_i^{p+1} = 1$ and $\alpha_{i+1} \neq -1/\alpha_i$. In this case there are $(p+1)p^{m-1}$ skew polynomials of degree m in $\mathcal{L}^{(1)}_{(x^2-\epsilon)^m} \setminus \{1, (x^2-\epsilon)^m\}$.

■

Algorithm 2 $\mathcal{L}^{(b)}_{(x^2\pm1)^m}$ for $b \in \{0,1\}$ and $m \in \mathbb{N}^*$

Require: : p, prime number, $m \in \mathbb{N}^*$, $\epsilon \in \{-1, 1\}$, $b \in \{0, 1\}$
Ensure: : $\mathcal{L}^{(b)}_{(x^2-\epsilon)^m}$
1: $E \leftarrow \{1, (x^2-\epsilon)^m\}$
2: **if** $b = 0$ **then**
3: **for** $\alpha_1, \ldots, \alpha_m \in \mathbb{F}_{p^2}$ such that $\alpha_1^2 \neq -1, \alpha_i^{p+1} = \epsilon$ and $\alpha_{i+1} \neq -\epsilon/\alpha_i$ **do**
4: $E \leftarrow E \cup \{(x+\alpha_m)\cdots(x+\alpha_1)\}$
5: **end for**
6: **else**
7: **if** p odd and $\epsilon = 1$ **then**
8: **for** $\alpha_1, \ldots, \alpha_m \in \mathbb{F}_{p^2}$ such that $\alpha_i^{p+1} = 1$ and $\alpha_{i+1} \neq -1/\alpha_i$ **do**
9: $E \leftarrow E \cup \{(x+\alpha_m)\cdots(x+\alpha_1)\}$
10: **end for**
11: **end if**
12: **end if**
13: **return** E

Lemma 9 describes the set $\mathcal{L}^{(b)}_{f(x^2)^m}$ and its number of elements where $f(x^2)$ belongs to $\mathcal{F}_{red}$. Algorithm 3 enables to construct this set.

Lemma 9 *Consider p a prime number, $\theta : a \mapsto a^p$ the Frobenius automorphism over $\mathbb{F}_q$ with $q = p^2$, $R = \mathbb{F}_q[x;\theta]$, $f(x^2) = f_{ir}(x^2)f_{ir}^{\natural}(x^2)$ in $\mathcal{F}_{red}$ with degree $d = 2\delta$ in x^2. The monic 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 $g = \mathrm{lclm}(g_1, g_2)$ 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 :*

$$\begin{cases} \deg(g_{i,j}) = \delta \\ g_{1,j} \text{ divides } f_{ir}(x^2) \text{ and } g_{2,j} \text{ divides } f_{ir}^{\natural}(x^2) \\ g_{1,j} \cdot g_{1,j-1} \neq f_{ir}(x^2) \text{ and } g_{2,j} \cdot g_{2,j-1} \neq f_{ir}^{\natural}(x^2) \\ g_{1,1} \neq \Theta^b(h_{2,1}^{\natural}), h_{2,1} \cdot g_{2,1} = f_{ir}^{\natural}(x^2). \end{cases} \tag{5}$$

Furthermore, the number of elements of $\mathcal{L}_{f(x^2)^m}^{(b)} \setminus \{1, f(x^2)^m\}$ *is* $(1+p^{d/2})p^{(2m-1)d/2}$.

Proof. Consider g in $\mathcal{L}_{f(x^2)^m}^{(b)} \setminus \{1, f_{ir}(x^2)^m f_{ir}^{\natural}(x^2)^m\}$ and h in R such that $g \cdot h = h \cdot g = f_{ir}(x^2)^m f_{ir}^{\natural}(x^2)^m$ with $\gcrd(g, \Theta^b(h^{\natural})) = 1$. As g divides $f_{ir}(x^2)^m f_{ir}^{\natural}(x^2)^m$ and $f_{ir}(x^2)^m$ and $f_{ir}^{\natural}(x^2)^m$ are coprime in $\mathbb{F}_p[x^2]$, according to Theorem 4.1 of [9], $g = \lclm(g_1, g_2)$ where $g_1 = \gcrd(f_{ir}(x^2)^m, g)$ and $g_2 = \gcrd(f_{ir}^{\natural}(x^2)^m, g)$. Similarly, $h = \lcrm(h_1, h_2)$, where $h_1 = \gcld(f_{ir}(x^2), h)$ and $h_2 = \gcld(f_{ir}^{\natural}(x^2), h)$.

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

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, $f_{ir}^{\natural}(x^2)$ does not divide g_2 and h_2, therefore using Proposition 6, one gets that :

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

Furthermore the above factorizations of g_1, g_2 are unique (according to Proposition 6). As g and $\Theta^b(h^{\natural})$ are right coprime, g_1 and $\Theta^b(h_2^{\natural})$ are right coprime, therefore $g_{1,1} \neq \Theta^b(h_{2,1}^{\natural})$.

Conversely, assume that $g = \lclm(g_1, g_2)$ where $g_1 = g_{1,m} \cdots g_{1,1}$, $g_2 = g_{2,m} \cdots g_{2,1}$ and (5) is satisfied. Consider $h_{i,j}$ such that $g_{1,i} \cdot h_{1,i} = f_{ir}(x^2)$ and $g_{2,i} \cdot h_{2,i} = f_{ir}^{\natural}(x^2)$. Consider $h_1 = h_{1,1} \cdots h_{1,m}$, $h_2 = h_{2,1} \cdots h_{2,m}$ and $h = \lcrm(h_1, h_2)$. Then $g \cdot h = h \cdot g = f_{ir}(x^2)^m f_{ir}^{\natural}(x^2)^m$ and g and $\Theta^b(h^{\natural})$ are right coprime.

Let us compute the number of elements of $\mathcal{L}_{f(x^2)^m}^{(b)} \setminus \{1, f(x^2)^m\}$. The elements of $\mathcal{L}_{f(x^2)^m}^{(b)} \setminus \{1, f(x^2)^m\}$ are the skew polynomials g in bijection with the couples (g_1, g_2) satisfying (5). 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.

■

From Theorem 3, Algorithms 1, 2 and 3, one deduces Algorithm 4 for the construction of LCD θ-cyclic and θ-negacyclic codes of length n and dimension k over $\mathbb{F}_{p^2}$.

Lastly we give an enumeration formulae (Proposition 7) for 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.

Algorithm 3 $\mathcal{L}^{(b)}_{f(x^2)^m}$ for $f(x^2) \in \mathcal{F}_{red}$, $b \in \{0,1\}$ 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 $f(x^2) = f_{ir}(x^2)f^{\natural}_{ir}(x^2) \in \mathcal{F}_{red}$

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

$E \leftarrow \{1, f(x^2)^m\}$
$d \leftarrow \deg_{x^2}(f(x^2))$
$I_1 \leftarrow \{g \in R, g \text{ monic, } g \text{ irreducible of degree } d \text{ dividing } f_{ir}(x^2)\}$
$I_2 \leftarrow \{g \in R, g \text{ monic, } g \text{ irreducible of degree } d \text{ dividing } f^{\natural}_{ir}(x^2)\}$
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**
    $E \leftarrow E \cup \{\text{lclm}(g_{1,m} \cdots g_{1,1}, g_{2,m} \cdots g_{2,1})\}$
  end for
end for
return E

Algorithm 4 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 $n = 2p^s t$, $p \not| t$, $b \in \{0,1\}$, $\lambda \in \{-1,1\}$, $\theta : a \mapsto a^p \in Aut(\mathbb{F}_{p^2})$

Ensure: : monic skew generators g of (θ, λ)-constacyclic codes of length n and dimension k over $\mathbb{F}_{p^2}$ which 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, 2 and 3
end for
for $I, J \subset \{1, \ldots, r\}$ with $I \cap J = \emptyset$ and $k = p^s(2t - 2\sum_{i \in I} d_i - \sum_{j \in J} d_j)$ **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**
    $E \leftarrow E \cup \{\prod_{i \in I} f_i(x^2)^{p^s} \text{ lclm}_{j \in J}(g_j)\}$
  end for
end for
return E

Proposition 7 *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*

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

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

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

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*

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

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

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

Proof. Consider the factorization of $x^n - \lambda = f_1(x^2)^{p^s} \cdots f_r(x^2)^{p^s}$ where $f_1(x^2), \ldots, f_r(x^2)$ are distinct polynomials of $\mathbb{F}_p[x^2]$ belonging to $\{x^2 \pm 1\} \cup \mathcal{F}_{ir} \cup \mathcal{F}_{red}$. According to Theorem 3, the Euclidean (resp. Hermitian) LCD (θ, λ)-constacyclic codes of length $2k$ and dimension k with skew generator polynomial not divisible by any central polynomial are generated by the monic skew polynomials $g = \mathrm{lclm}_{j \in J}(g_j)$ where J is a subset of $\{1, \ldots, r\}$ and $\forall j \in J, g_j \in \mathcal{L}^{(b)}_{f_j(x^2)^{p^s}} \setminus \{1, f_j(x^2)^{p^s}\}$ with $b = 0$ (resp. $b = 1$). Furthermore the dimension of the codes are equal to $k = p^s \sum_{j \in J} \deg_{x^2} f_j(x^2)$. As $k = p^s \sum_{j=1}^r \deg_{x^2} f_j(x^2)$, J must be equal to $\{1, \ldots, r\}$ and $g = \mathrm{lclm}_{1 \le i \le r}(g_i)$ where g_i belongs to $\mathcal{L}^{(b)}_{f_i(x^2)^{p^s}} \setminus \{1, f_i(x^2)^{p^s}\}$. The number of such skew polynomials g is $N_\lambda \times M_\lambda$ where

$$N_\lambda = \prod_{\substack{f \in \{x^2 \pm 1\} \\ f \in \mathcal{D}_{x^n-\lambda}}} \#\mathcal{L}^{(b)}_{f(x^2)^{p^s}} \setminus \{1, f(x^2)^{p^s}\}$$

and

$$M_\lambda = \prod_{\substack{f \in \mathcal{F}_{ir} \cup \mathcal{F}_{red} \\ f \in \mathcal{D}_{x^n-\lambda}}} \#\mathcal{L}^{(b)}_{f(x^2)^{p^s}} \setminus \{1, f(x^2)^{p^s}\}.$$

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

For $\epsilon=\pm 1$, $x^2-\epsilon \in \mathcal{D}_{x^n-\lambda}$ if and only if $\epsilon^k=\lambda$ therefore using the enumeration formulae for $\mathcal{L}^{(b)}_{(x^2-\epsilon)^{p^s}} \setminus \{1,(x^2-\epsilon)^{p^s}\}$ given by Lemma 8, one deduces the value of N_λ.

Enumeration formulae for $\#\mathcal{L}^{(b)}_{f(x^2)^{p^s}} \setminus \{1,f(x^2)^{p^s}\}$ given by Lemma 7 (when $f(x^2)\in\mathcal{F}_{ir}$) and Lemma 9 (when $f(x^2)\in\mathcal{F}_{red}$) enable to obtain M_λ. ∎

Remark 2 *From Proposition 7, one gets that over $\mathbb{F}_4$, when $k=2^s$, the number of Euclidean LCD θ-cyclic codes $[2k,k]$ is 2^k and growths exponentially with k. On the other hand, the number of Euclidean self-dual θ-cyclic codes $[2k,k]$ is constant (Corollary 26 of [4]).*

Remark 3 *Over $\mathbb{F}_{p^2}$, according to Theorem 5.5 of [20], there are only 2 LCD cyclic codes of length 2^r if $p=2$, while there are $2^{2^{r-1}}$ LCD skew cyclic codes of length 2^r. If p is an odd prime number, there are 4 LCD cyclic codes of length $2p^r$ while there are $p^{p^r-1}(p-(-1)^{(p+1)/2})$ LCD skew cyclic codes with length $2p^r$.*

To finish we give below an example and some tables of results. All the computations were made with the computer algebra system MAGMA.

Example 8 *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 $1\neq 1/w^2$, therefore according to Algorithm 2, g generates a EuclideanLCD $[8,4]_4$ θ-cyclic code which is not a 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 [7] C is a EuclideanLCD code. Furthermore $1\in Spec(P\times^t \overline{P})$ therefore according to Proposition 6 of [7], C is not a Hermitian LCD code.*

The following Table 1 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 $p\in\{3,5,7,11\}$. One can notice that there exists MDS LCD θ-cyclic codes of length $2p$ over $\mathbb{F}_{p^2}$, while according to Corollary 4.2 of [20], there are no MDS LCD repeated-root cyclic codes over $\mathbb{F}_{p^2}$ of length $2p$.

Table 2, Table 3 and Table 4 illustrate Proposition 7 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 $\mathbb{F}_9$

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 2: 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

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.

Table 5 sums up the dimensions of *MDS* LCD skew codes of given length ≤ 10 over $\mathbb{F}_9$. Tables 6 and 7 sum up the dimensions of *MDS* LCD skew codes of length ≤ 18 over $\mathbb{F}_{25}$ and of length ≤ 16 over $\mathbb{F}_{49}$.

6 Conclusion

In this text, we gave some conditions on the equivalence of skew constacyclic codes and a first study of skew LCD codes was proposed. LCD skew cyclic and negacyclic codes were constructed and enumerated over $\mathbb{F}_{p^2}$. Some computations were made and MDS LCD codes were constructed. It could be interesting to see if there exist $[2p, p]_{p^2}$ MDS LCD codes for p odd prime greater than 11 and to find a necessary and sufficient condition on p for the existence of $[2p, p]_{p^2}$ MDS LCD skew codes.

Acknowledgements. The authors thank the referees for their very helpful suggestions to improve the paper. The third author is supported by the French government Investissements d'Avenir program `ANR-11-LABX-0020-01`.

References

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

[2] D. Boucher, W. Geiselmann and F. Ulmer, Skew-cyclic codes, *Appl. Algebra Engin. Commun. Comp.*, **18** (2007), 379–389.

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

Table 3: 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

	Hermitian LCD			
	skew cyc		skew negacyc	
length	best dist	nbr	best dist	nbr
2	2*	4	0	0
4	0	0	3*	6
6	4*	361	0	0
8	0	0	5*	90
10	6*	288	0	0
12	0	0	6*	486
14	7*	2 808	0	0
16	0	0	8*	6 642
18	9*	26 244	0	0
20	0	0	10*	39 852
22	9*	237 168	0	0
24	0	0	10*	590 490

Table 4: 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 5: 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 6: 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 7: Dimensions of *MDS* LCD skew codes over $\mathbb{F}_{49}$ with length $n \leq 16$ and dimension $1 < k < n-1$

[3] D. Boucher and F. Ulmer, A note on the dual codes of module skew codes, *Cryptography and coding*, Lecture Notes in Computer Science, **7089** (2011), 230–243.

[4] D. Boucher and F. Ulmer, Self-dual skew codes and factorization of skew polynomials, *J. Symb. Comp.*, **60** (2014), 47–61.

[5] D. Boucher, Construction and number of self-dual skew codes over $\mathbb{F}_{p^2}$, *Advances in Mathematics of Communications (AMC)*, **10** (2016), 4, 765–795.

[6] D. Boucher, A First Step Towards the Skew Duadic Codes, *Advances of Mathematics of Communications*, **12** (2018), 3, 553–577.

[7] C. Carlet, S. Mesnager, C. Tang and Y. Qi, Euclidean and Hermitian LCD MDS codes, *Designs, Codes and Cryptography* **86** (2018), 11, 2605-2618.

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

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

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

[11] C. Li, Hermitian LCD codes from cyclic codes, *Des. Codes Cryptogr.*, **86** (2018), 2261–2278.

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

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

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

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

[16] J. L. Massey, Reversible codes, *Inform. and Control*, **7** (1964), 369–380.

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

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

[19] O. Ore, Theory of Non-Commutative Polynomials, *Ann. Math.*, **34** (1933), 480–508.

[20] B. Pang, S. Zhu and J. Li, On LCD repeated-root cyclic codes over finite fields, *J. Appl. Math. Comput.*, **56** (2018), 1-2, 625–635.

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