Some constructions and existence conditions for Hermitian self-dual skew codes

D Boucher, E K Nouetowa

Some constructions and existence conditions for Hermitian self-dual skew codes.

D. Boucher and E.K. Nouetowa *

Abstract

In this text, we first consider the existence conditions and the construction of Hermitian self-dual $\boldsymbol{\theta}$-cyclic and $\boldsymbol{\theta}$-negacyclic codes over $\mathbb{F}_{p^2}$, where p is a prime number and $\boldsymbol{\theta}$ is the Frobenius automorphism over $\mathbb{F}_{p^2}$. We then give necessary and sufficient conditions for the existence of Hermitian self-dual $\boldsymbol{\theta}$-cyclic and $\boldsymbol{\theta}$-negacyclic codes over $\mathbb{F}_{p^e}$ where e is an even integer greater than 2.

Keywords: skew polynomial ring; coding theory; duality

Acknowledgments.

The authors benefit from the support of the French government Investissements d'Avenir program integrated to France 2030, bearing the reference ANR−11−LABX−0020 − 01.

1 Introduction

For θ an automorphism of a finite field $\mathbb{F}_q$, θ-cyclic codes (also called skew cyclic codes) of length n were defined in [5]. These codes are such that a right circular shift of each codeword gives another word which belongs to the code after application of θ to each of its n coordinates. If θ is the identity, θ-cyclic codes are cyclic codes.

Skew cyclic codes have an interpretation in the Ore ring $R = \mathbb{F}_q[X;\theta]$ of skew polynomials where multiplication is defined by the rule $X \cdot a = \theta(a)X$ for a in $\mathbb{F}_q$. Euclidean self-dual skew cyclic codes of length n over $\mathbb{F}_q$ have been considered in many previous works among which [11, 14]. Their existence conditions were first established in [7], then their construction and enumeration were obtained over $\mathbb{F}_{p^2}$ when p is a prime number ([8]) and over $\mathbb{F}_{p^n}$ when p is a prime number and θ is the Frobenius automorphism ([1]). In this text we are concerned with Hermitian self-dual skew cyclic and skew negacyclic codes whose study was briefly initiated in [9]. We first consider

*Univ Rennes, CNRS, IRMAR - UMR 6625, Rennes Cedex, France

Hermitian self-dual θ-cyclic and θ-negacyclic codes over $\mathbb{F}_{p^2}$ where p is a prime number and θ is the Frobenius automorphism over $\mathbb{F}_{p^2}$. Then we give necessary and sufficient existence conditions for Hermitian self-dual skew cyclic and skew negacyclic codes over $\mathbb{F}_q$.

The text is organized as follows. In Section 2, we first give generalities on θ-cyclic and θ-negacyclic codes. In Section 3, we consider Hermitian self-dual θ-cyclic and θ-negacyclic codes over $\mathbb{F}_{p^2}$ when θ is the Frobenius automorphism. In subsection 3.1, we first characterize these codes by a system of homogeneous polynomial equations of degree $p+1$ (Algorithm 1). Then, in subsection 3.2, by using factorization properties of skew polynomials, we prove that there exists no Hermitian self-dual θ-cyclic code of any dimension over $\mathbb{F}_{p^2}$ (Theorem 2). We also provide a construction and an exact formula for the number of Hermitian self-dual θ-negacyclic codes (Algorithm 5 and Theorem 1). We give many examples of Hermitian self-dual codes over $\mathbb{F}_4$ and $\mathbb{F}_9$, including a $[68, 34, 18]$ Hermitian self-dual code over $\mathbb{F}_4$, which improves the best known Hermitian self-dual code of length 68 over $\mathbb{F}_4$ (according to [13]). All the computations were made with the Magma algebra system ([4]). In Section 4, we prove that there is no Hermitian self-dual θ-cyclic code over any finite field $\mathbb{F}_{p^e}$ with e even and p odd (Theorem 2). Then we give necessary and sufficient existence conditions for Hermitian self-dual θ-negacyclic codes defined over $\mathbb{F}_{p^e}$ with $e > 2$ (Theorem 3).

2 Generalities on self-dual skew constacyclic codes

For a finite field $\mathbb{F}_q$ and θ an automorphism of $\mathbb{F}_q$ one considers the ring $R = \mathbb{F}_q[X;\theta]$ where addition is defined to be the usual addition of polynomials and where multiplication is defined by the rule: for a in $\mathbb{F}_q$

$$X \cdot a = \theta(a)\, X. \tag{1}$$

The ring R is called a skew polynomial ring or Ore ring (cf. [17]) and its elements are skew polynomials. When θ is not the identity, the ring R is not commutative, it is a left and right Euclidean ring whose left and right ideals are principal. Left and right gcd (gcld, gcrd) and lcm (lclm, lcrm) exist in R and can be computed using the left and right Euclidean algorithms. The center of R is the commutative polynomial ring $Z(R) = \mathbb{F}_q^{\theta}[X^{\ell}]$ where $\mathbb{F}_q^{\theta}$ is the fixed field of θ and ℓ is the order of θ.

Definition 1 ([6, Definition 1])**.** *Consider a non-zero element a of $\mathbb{F}_q$ and two integers n, k such that $0 \leq k \leq n$. A (θ, a)-**constacyclic code** or **skew constacyclic** code C of length n is a left R-submodule $Rg/R(X^n - a) \subset R/R(X^n - a)$ in the basis $1, X, \ldots, X^{n-1}$ where g is a monic skew polynomial dividing $X^n - a$ on the right in R with degree $n - k$. If $a = 1$, the code is θ-**cyclic** and if $a = -1$, it is θ-**negacyclic**. The skew polynomial g is called* **skew generator polynomial** *of C.*

If θ is the identity then θ-cyclic and θ-negacylic codes are respectively cyclic and negacyclic codes.

Definition 2 ([6, Definition 2]). *Consider an integer d and $h = \sum_{i=0}^{d} h_i X^i$ in R of degree d. The* **skew reciprocal polynomial** *of h is*

$$h^* = \sum_{i=0}^{d} X^{d-i} \cdot h_i = \sum_{i=0}^{d} \theta^i(h_{d-i})\, X^i.$$

If m is the degree of the trailing term of h, the **left monic skew reciprocal polynomial** *of h is $h^\natural := \frac{1}{\theta^{d-m}(h_m)} \cdot h^*$.*

The **Euclidean dual** of a linear code C of length n over $\mathbb{F}_q$ is defined as $C^\perp = \{x \in \mathbb{F}_q^n \mid \forall y \in C, \langle x, y\rangle = 0\}$ where for x, y in $\mathbb{F}_q^n$, $\langle x, y\rangle := \sum_{i=1}^n x_i y_i$ is the (Euclidean) scalar product of x and y. The code C is **Euclidean self-dual** if C is equal to $C^\perp$. Assume that q is an even power of an arbitrary prime and denote σ the automorphism of $\mathbb{F}_q$ defined by $\sigma(a) = a^{\sqrt{q}}$ for a in $\mathbb{F}_q$. The **Hermitian dual** of a linear code C of length n over $\mathbb{F}_q$ is defined as $C^{\perp_H} = \{x \in \mathbb{F}_q^n \mid \forall y \in C, \langle x, y\rangle_H = 0\}$ where for x, y in $\mathbb{F}_q^n$, $\langle x, y\rangle_H := \sum_{i=1}^n x_i \sigma(y_i)$ is the (Hermitian) scalar product of x and y. The code C is **Hermitian self-dual** if C is equal to $C^{\perp_H}$.

In what follows we will only consider (θ, ε)-constacyclic codes with $\varepsilon^2 = 1$ and with length n divisible by the order ℓ of θ. That implies that the skew polynomial $X^n - \varepsilon$ is a central polynomial. Following [10, Proposition 2], the Hermitian dual of a (θ, ε)-constacyclic code C of length n and skew generator polynomial g is a (θ, ε)-constacyclic code of skew generator polynomial $\sigma(h^\natural)$ where h is defined by $h \cdot g = g \cdot h = X^n - \varepsilon$ and where the automorphism σ is extended to R by $\sum a_i X^i \mapsto \sum \sigma(a_i) X^i$. In particular the code C is Hermitian self-dual if, and only if,

$$\sigma(h^\natural) \cdot h = X^n - \varepsilon. \tag{2}$$

The equation (2) is called **Hermitian self-dual skew equation**.

For $F = F(X^\ell)$ in $\mathbb{F}_q^\theta[X^\ell]$, we define

$$\mathcal{H}_F := \{h \in R \mid h \text{ is monic and } \sigma(h^\natural) \cdot h = F(X^\ell)\}.$$

3 Hermitian self-dual θ-cyclic and θ-negacyclic codes over $\mathbb{F}_{p^2}$

We consider here the existence and the construction of Hermitian self-dual θ-cyclic and θ-negacyclic codes of length $n = 2k$ defined over $\mathbb{F}_{p^2}$ where θ is the Frobenius automorphism over $\mathbb{F}_{p^2}$.

As $q = p^2$, the automorphisms θ and σ are both equal to the Frobenius automorphism. The fixed field $\mathbb{F}_q^\theta$ of $\mathbb{F}_q$ is therefore $\mathbb{F}_p$ and the order of θ is $\ell = 2$.

A first result was obtained in [9] for θ-cyclic codes with dimension coprime with p. Namely, there exists a Hermitian self-dual θ-cyclic code of dimension coprime to p

over $\mathbb{F}_{p^2}$ if, and only if, $p = 2$. Furthermore, the number of Hermitian self-dual θ-cyclic codes with odd dimension over $\mathbb{F}_4$ was computed in [9, Theorem 3.7].

3.1 Polynomial system strategy

Hermitian self-dual θ-cyclic (resp. θ-negacyclic) codes of dimension k are completely determined by the set $\mathcal{H}_{X^{2k}-\varepsilon}$ where $\epsilon = 1$ (resp. $\epsilon = -1$). In order to compute $\mathcal{H}_{X^{2k}-\varepsilon}$, a first strategy consists of solving the polynomial system satisfied by the coefficients of the solutions h of the equation $\theta(h^\natural) \cdot h = X^n - \epsilon$ (the automorphism θ being naturally extended to R by : $\sum a_i X^i \mapsto \sum \theta(a_i) X^i$). Namely consider $h = \sum_{i=0}^{k} h_i X^i$ in R with $h_0 \neq 0$, then

$$\theta(h^\natural) \cdot h = \frac{1}{\theta^{k+1}(h_0)} \sum_{\ell=0}^{2k} \left(\sum_{i=\max(0,\ell-k)}^{\min(k,\ell)} \theta^i(\theta(h_{k-i}) h_{\ell-i}) \right) X^\ell.$$

Therefore we get that $\theta(h^\natural) \cdot h = X^{2k} - \epsilon$ if, and only if,

$$\begin{cases} \theta^{k+1}(h_0) = -\epsilon h_0 \neq 0, \\ \forall \ell \in \{1, \ldots, k-1\}, \sum_{i=0}^{\ell} \theta^i(\theta(h_{k-i}) h_{\ell-i}) = 0, \\ \sum_{i=0}^{k} \theta^i(\theta(h_{k-i}) h_{k-i}) = 0, \\ \forall \ell \in \{k+1, \ldots, 2k-1\}, \sum_{i=\ell-k}^{k} \theta^i(\theta(h_{k-i}) h_{\ell-i}) = 0. \end{cases}$$

The symmetries of the system enable to get rid of the last $k-1$ equations and we get :

$$\theta(h^\natural) \cdot h = X^{2k} - \epsilon \Leftrightarrow \begin{cases} \theta^{k+1}(h_0) = -\epsilon h_0 \neq 0, \\ \forall \ell \in \{1, \ldots, k-1\}, \sum_{\substack{0 \leq i \leq \ell \\ i \bmod 2 = 0}} h_{k-i}^p h_{\ell-i} + \sum_{\substack{0 \leq i \leq \ell \\ i \bmod 2 = 1}} h_{k-i} h_{\ell-i}^p = 0, \\ \sum_{i=0}^{k} h_i^{p+1} = 0. \end{cases}$$

Remark 1. *The solutions of the above system belong to the non-degenerate Hermitian variety defined by $h_0^{p+1} + \cdots + h_{k-1}^{p+1} + h_k^{p+1} = 0$. Therefore according to Theorem 8.1 of [3], there are at most $\frac{(p^{k+1}-(-1)^{k+1})(p^k-(-1)^k)}{p^2-1}$ solutions. Furthermore, according to Theorem 6.3 of [12], the number of solutions of this homogeneous polynomial system of k linearly independent equations into $k+1$ variables with degree $p+1$ is at most $p^{2k-1} + \frac{p^{2k-2}-1}{p^2-1}$. The aim of this section is to give an exact formula for the number of solutions of this system by using an approach based on the factorization of skew polynomials (Theorem 1).*

We can simplify this system in the following way. Consider $N = \lfloor \frac{k-1}{2} \rfloor$ and assume that $h_k = 1$. Then we get

$$\theta(h^\natural)\cdot h = X^{2k} - \epsilon \Leftrightarrow \begin{cases} \forall \ell \in \{N+1, \ldots, k-1\}, \displaystyle\sum_{\substack{0 \le i \le \ell \\ i \bmod 2 = 0}} h_{k-i}^p h_{\ell-i} + \sum_{\substack{0 \le i \le \ell \\ i \bmod 2 = 1}} h_{k-i} h_{\ell-i}^p = 0, \\ \displaystyle\sum_{i=0}^{k} h_i^{p+1} = 0, \end{cases}$$

where

$$\begin{cases} \theta^{k+1}(h_0) = -\epsilon h_0 \neq 0, \\ \forall \ell \in \{1, \ldots, N\}, h_\ell = - \displaystyle\sum_{\substack{1 \le i \le \ell \\ i \bmod 2 = 0}} h_{k-i}^p \times h_{\ell-i} - \sum_{\substack{1 \le i \le \ell \\ i \bmod 2 = 1}} h_{k-i} \times h_{\ell-i}^p. \end{cases}$$

Therefore we get a polynomial system of N equations with $k - N$ unknowns which we solve in Algorithm 1 by using an exhaustive search.

Example 1. *We consider the Hermitian self-dual θ-cyclic codes of dimension $k = 3$ over $\mathbb{F}_4 = \mathbb{F}_2(a)$ where $a^2 + a + 1 = 0$. Their skew check polynomials $h = X^3 + h_2 X^2 + h_1 X + h_0$ satisfy the polynomial system :*

$$\begin{cases} h_2 + h_2 h_1^2 + h_1^2 h_0 = 0, \\ h_0^3 + h_1^3 + h_2^3 + 1 = 0, \end{cases}$$

where

$$\begin{cases} h_0 \in \mathbb{F}_4^*, \\ h_1 + h_2 h_0^2 = 0. \end{cases}$$

We get 9 solutions :$(a,0,0), (a^2,0,0), (1,0,0)$ which give three Hermitian self-dual $[6,3,2]$ codes and $(1,a,a), (1,a^2,a^2), (a,1,a^2), (a,a^2,a^2), (a^2,1,a), (a^2,a,a)$, which give 6 Hermitian self-dual $[6,3,4]$ codes.

Example 2. *We consider the Hermitian self-dual θ-negacyclic codes of dimension $k = 2, 3, 4$ over $\mathbb{F}_9 = \mathbb{F}_3(a)$ where $a^2 + 2a + 2 = 0$.*

- $k = 2$

  The skew check polynomials $h = X^2 + h_1 X + h_0$ of the Hermitian self-dual codes of dimension 2 satisfy the polynomial system

  $$\begin{cases} h_0^3 - h_0 = 0, \\ h_0^4 + h_1^4 + 1 = 0, \\ h_1 + h_1^3 h_0 = 0. \end{cases}$$

  The set of solutions is $\{(-1,-1), (-1,1), (-1,a^6), (-1,a^2)\}$. The corresponding codes are $[4,2,3]_9$ Hermitian self-dual codes.
- $k = 3$

Algorithm 1 Computation of $\mathcal{H}_{X^n-\epsilon}$ wit $\epsilon^2=1$ (polynomial system strategy)

Require: k, ϵ such that $\epsilon^2=1$
Ensure: $\mathcal{H}_{X^{2k}-\epsilon}$
1: $h_k \leftarrow 1$
2: $F_0 \leftarrow \{h_0 \in \mathbb{F}_{p^2}^* \mid \theta^{k+1}(h_0) = -\epsilon h_0\}$
3: $M \leftarrow \lfloor \frac{k-1}{2} \rfloor$
4: $\mathcal{E} \leftarrow F_0 \times \mathbb{F}_{p^2}^{k-N-1}$
5: **while** $\mathcal{E} \neq \emptyset$ **do**
6: Pick $(h_0, h_{N+1}, \ldots, h_{k-1})$ in $\mathcal{E}$
7: **for** $\ell = 1, \ldots, N$ **do**
8: $h_\ell \leftarrow -\sum_{\substack{1\le i\le \ell \\ i \bmod 2=0}} h_{k-i}^p \times h_{\ell-i} - \sum_{\substack{1\le i\le \ell \\ i \bmod 2=1}} h_{k-i} \times h_{\ell-i}^p$
9: **end for**
10: **if** $\sum_{i=0}^{k} h_i^{p+1} \neq 0$ **then**
11: go to 6:
12: **end if**
13: **for** $\ell = 1, \ldots, k-1-N$ **do**
14: **if** $\sum_{\substack{0\le i\le \ell+N \\ i \bmod 2=0}} h_{k-i}^p \times h_{\ell+N-i} + \sum_{\substack{0\le i\le \ell+N \\ i \bmod 2=1}} h_{k-i} \times h_{\ell+N-i}^p \neq 0$ **then**
15: go to 6:
16: **end if**
17: **end for**
18: $\mathcal{H} \leftarrow \mathcal{H} \cup \{X^k + \sum_{i=0}^{k-1} h_i X^i\}$
19: $\mathcal{E} \leftarrow \mathcal{E} \setminus \{(h_0, h_{N+1}, \ldots, h_{k-1})\}$
20: **end while**
21: **return** $\mathcal{H}$

We look for $(h_0, h_1, h_2) \in \mathbb{F}_9^3$ *such that :*

$$\begin{cases} h_2 + h_2 h_1^3 + h_1^3 h_0 = 0, \\ h_0^4 + h_1^4 + h_2^4 + 1 = 0, \end{cases}$$

where

$$\begin{cases} h_0 \in \mathbb{F}_9^*, \\ h_1 + h_2 h_0^3 = 0. \end{cases}$$

We get the set of solutions $\{(a,0,0),(a^3,0,0),(a^5,0,0),(a^7,0,0),(a,1,a),(a,a,a^2),(a,a^3,2),(a^3,1,a^3),(a^3,a,2),(a^3,a^3,a^6),(a^5,a^3,1),(a^5,1,a^5),(a^5,a,a^6),(a^7,a,1),(a^7,a^3,a^2),(a^7,1,a^7)\}$*, therefore we have* 16 *Hermitian self-dual* θ*-negacyclic codes of length* 6.
For example the Hermitian self-dual θ*-negacyclic code of length* 6 *with skew check polynomial* $h = X^3 + X^2 + aX + a^7$ *is a* $[6,3,4]$ *code.*

- $k = 4$
  We look for $(h_0, h_1, h_2, h_3) \in \mathbb{F}_9^4$ *such that :*

$$\begin{cases} h_3 + h_3 h_2^3 + h_2^3 h_1 + h_1^3 h_0 = 0, \\ h_2 + h_3 h_1^3 + h_2^3 h_0 = 0, \\ h_0^4 + h_1^4 + h_2^4 + h_3^4 + 1 = 0, \end{cases}$$

  where

$$\begin{cases} h_0 \in \mathbb{F}_3^*, \\ h_1 = -h_3 h_0. \end{cases}$$

  We get the set $\{(1,0,a^6,0),(1,0,a^2,0),(1,2,a,1),(1,a^2,a^3,a^6),(1,a^6,a,a^2),$ $(2,0,2,0),(1,1,a,2),(2,0,1,0),(1,a^6,a^3,a^2),(1,a^2,a,a^6),(1,1,a^3,2),(1,2,a^3,1)\}$, *therefore we have* 12 *Hermitian self-dual* θ*-negacyclic codes of length* 8.
  For example the Hermitian self-dual θ*-negacyclic code of length* 8 *with skew check polynomial* $h = X^4 + X^3 + a^3X^2 + 2X + 1$ *is a* $[8,4,4]$ *code.*

3.2 Factorization strategy.

In what follows we propose a strategy which was already used for Euclidean self-dual skew codes over $\mathbb{F}_{p^2}$ ([8, Theorem 6.1]) and for Hermitian self-dual θ-negacyclic codes of dimension coprime to p ([9, Theorem 3.7]). We give a practical way to construct the solutions which avoids the resolution of a polynomial system and we provide a counting formula for the number of solutions. This construction is based on Proposition 2 of [9] that we recall below.

Proposition 1. *Consider* $\mathbb{F}_q$ *a finite field with* $q = p^2$ *elements where* p *is a prime number,* $\theta : x \mapsto x^p$ *the Frobenius automorphism over* $\mathbb{F}_{p^2}$ *and* $R = \mathbb{F}_q[X;\theta]$. *Consider* $F(X^2) = f_1(X^2)\cdots f_r(X^2)$ *where* $f_1(X^2),\ldots,f_r(X^2)$ *are pairwise coprime polynomials of* $\mathbb{F}_p[X^2]$ *satisfying* $f_i^\natural = f_i$. *The map*

$$\phi : \begin{cases} \mathcal{H}_{f_1(X^2)} \times \cdots \times \mathcal{H}_{f_r(X^2)} & \to \mathcal{H}_{F(X^2)} \\ (h_1,\ldots,h_r) & \mapsto \operatorname{lcrm}(h_1,\ldots,h_r) \end{cases}$$

is bijective.

We introduce the following notations: for $f = f(X^2) \in \mathbb{F}_p[X^2]$,

$\overline{\mathcal{H}}_f := \{h \in \mathcal{H}_f \mid$ no non-constant divisor of $f(X^2)$ in $\mathbb{F}_p[X^2]$ divides h in $R\}$,
$\mathcal{F} := \{f = f(X^2) \in \mathbb{F}_p[X^2] \mid f = f^\natural$ is irreducible in $\mathbb{F}_p[X^2]$ and $\deg_{X^2}(f) > 1\}$,
$\mathcal{G} := \{f = f(X^2) \in \mathbb{F}_p[X^2] \mid f = gg^\natural$ with $g \neq g^\natural$ irreducible in $\mathbb{F}_p[X^2]\}$.

3.2.1 Non-existence of Hermitian self-dual θ-cyclic codes for p odd prime

Recall that there exists a Hermitian self-dual θ-cyclic code of dimension coprime to p over $\mathbb{F}_{p^2}$ if, and only if, $p = 2$ (Theorem 3.7 of [9]). In what follows we prove that this result remains true if the dimension of the code is divisible by p (Proposition 2).

Lemma 1. *If* k *and* p *are odd then* $\mathcal{H}_{X^{2k}-1} = \emptyset$.

Proof. Assume that $\mathcal{H}_{X^{2k}-1} \neq \emptyset$. Consider h in $\mathcal{H}_{X^{2k}-1}$ with constant coefficient h_0. As $\theta(h^\natural) \cdot h = X^{2k} - 1$, we have $\theta(1/\theta^k(h_0)) \times h_0 = -1$. As the order of θ is 2 and k is odd, we get $1/h_0 \times h_0 = -1$, which is impossible over $\mathbb{F}_{p^2}$ because p is an odd prime number. ∎

Proposition 2. *If p is odd, then there exists no Hermitian self-dual θ-cyclic code over $\mathbb{F}_{p^2}$.*

Proof. Let us prove that for any k, $\mathcal{H}_{X^{2k}-1} = \emptyset$. Consider s, t in $\mathbb{N}$ such that $k = p^s \times t$ and p does not divide t. According to Lemma 1, the set $\mathcal{H}_{X^{2p^s}-1} = \mathcal{H}_{(X^2-1)^{p^s}}$ is empty. We have $X^{2k} - 1 = f_1(X^2) f_2(X^2)$ where $f_1(X^2) = (X^2-1)^{p^s} = f_1^\natural(X^2)$ and $f_2(X^2) = (\sum_{i=0}^{t-1} X^{2i})^{p^s} = f_2^\natural(X^2)$. As p does not divide t, these two polynomialrs are coprime polynomials of $\mathbb{F}_p[X^2]$. Therefore, according to Proposition 1, the set $\mathcal{H}_{X^{2k}-1}$ is empty. ∎

3.2.2 Construction of $\mathcal{H}_{(X^2+1)^{p^s}}$

The aim of this section is to construct and to enumerate Hermitian self-dual θ-negacyclic codes over $\mathbb{F}_{p^2}$ whose dimension is p^s where θ is the Frobenius automorphism (Proposition 4 and Algorithm 2). In order to construct the set $\mathcal{H}_{X^{2k}+1} = \mathcal{H}_{(X^2+1)^{p^s}}$, factorization properties specific to $\mathbb{F}_{p^2}[X;\theta]$ will be useful. The following proposition enables to characterize the skew polynomials that have a unique factorization into the product of monic linear skew polynomials dividing $X^2 + 1$ (see also [6, Proposition 16]).

Proposition 3. *Consider p a prime number, θ the Frobenius automorphism over $\mathbb{F}_{p^2}$, $R = \mathbb{F}_{p^2}[X;\theta]$, m a non-negative integer, $f(X^2)$ in $\mathbb{F}_p[X^2]$ irreducible and $h = h_1 \cdots h_m$ in R where for all i in $\{1, \ldots, m\}$, h_i is irreducible in R, monic, and divides $f(X^2)$. The following assertions are equivalent :*

(i) The above factorization of h is not unique.
(ii) $f(X^2)$ divides h.
(iii) There exists i in $\{1, \ldots, m-1\}$ such that $h_i \cdot h_{i+1} = f(X^2)$.

Corollary 1. *Consider p a prime number, θ the Frobenius automorphism over $\mathbb{F}_{p^2}$, $R = \mathbb{F}_{p^2}[X;\theta]$, m a non-negative integer and $h = (X + \lambda_1) \cdots (X + \lambda_m)$ in R where for all i in $\{1, \ldots, m\}$, $\lambda_i^{p+1} = -1$. The following assertions are equivalent :*

(i) The above factorization of h is not unique.
(ii) $X^2 + 1$ divides h.
(iii) There exists i in $\{1, \ldots, m-1\}$ such that $(X + \lambda_i) \cdot (X + \lambda_{i+1}) = X^2 + 1$ i.e. $\lambda_i \lambda_{i+1} = 1$.

This proposition and its corollary motivate the following partition (see Lemma 3.2 of [8]) :

Lemma 2. *Consider p a prime number, θ the Frobenius automorphism over $\mathbb{F}_{p^2}$, $R = \mathbb{F}_{p^2}[X;\theta]$, s a non-negative integer and $f = f(X^2) \in \{X^2 + 1\} \cup \mathcal{F}$. One has the*

following partition :

$$\mathcal{H}_{f^{p^s}} = \bigsqcup_{i=0}^{\lfloor \frac{p^s}{2} \rfloor} f^i \cdot \overline{\mathcal{H}}_{f^{p^s-2i}}. \tag{3}$$

Lemma 3. *Consider p an odd prime number, θ the Frobenius automorphism, $R = \mathbb{F}_{p^2}[X;\theta]$, m a non-negative integer and $M = \lfloor \frac{m-1}{2} \rfloor$. The number of elements of the set $\overline{\mathcal{H}}_{(X^2+1)^m}$ is*

$$\#\overline{\mathcal{H}}_{(X^2+1)^m} = \begin{cases} (p+1) \times p^M & \text{if } p \text{ is odd,} \\ 3 & \text{if } p = 2 \text{ and } m = 1, \\ 0 & \text{if } p = 2 \text{ and } m > 1. \end{cases}$$

If $m \equiv 0 \pmod 2$, then

$$\overline{\mathcal{H}}_{(X^2+1)^m} = \{(X^2 + 2\alpha_1 X - 1) \cdots (X^2 + 2\alpha_{M+1} X - 1) \mid \alpha_i^{p+1} = -1, \alpha_{i+1} \neq -\alpha_i\}.$$

If $m \equiv 1 \pmod 2$, then

$$\overline{\mathcal{H}}_{(X^2+1)^m} = \{(X^2+2\alpha_1 X-1) \cdots (X^2+2\alpha_M X-1) \cdot (X+\alpha_{M+1}) \mid \alpha_i^{p+1} = -1, \alpha_{i+1} \neq -\alpha_i\}.$$

Proof.

- One first proves that the elements of $\overline{\mathcal{H}}_{(X^2+1)^m}$ are obtained as products of linear monic skew polynomials $(X + \lambda_1) \cdots (X + \lambda_m)$ where $\lambda_1, \ldots, \lambda_m$ are elements of $\mathbb{F}_{p^2}$ such that

$$\begin{cases} \forall i \in \{1, \ldots, m\}, \lambda_i^{p+1} = -1, \\ \forall i \in \{1, \ldots, m-1\}, \lambda_i \lambda_{i+1} \neq 1, \\ \forall j \in \{1, \ldots, \lfloor \frac{m}{2} \rfloor\}, (\lambda_{2j-1}\lambda_{2j})^2 = 1. \end{cases} \tag{4}$$

  Namely, consider h in $\overline{\mathcal{H}}_{(X^2+1)^m}$. As h divides $(X^2+1)^m$ and as X^2+1 is irreducible with degree 1 in $\mathbb{F}_p[X^2]$, h is a (not necessarily commutative) product of linear monic skew polynomials dividing $X^2 + 1$ ([6, Lemma 13 (2)] or [16, page 6]). Furthermore, the degree of h is equal to m (because $\deg(\theta(h^\natural) \cdot h) = 2m$), therefore there exists $\lambda_1, \ldots, \lambda_m$ in $\mathbb{F}_{p^2}$ such that :

$$h = (X + \lambda_1) \cdots (X + \lambda_m) \text{ where } \forall i \in \{1, \ldots, m\}, \lambda_i^{p+1} = -1.$$

  In particular, the first relation of (4) is satisfied. As $X^2 + 1$ does not divide h, according to Corollary 1, we have :

$$\forall i \in \{1, \ldots, m-1\}, (X + \lambda_i) \cdot (X + \lambda_{i+1}) \neq X^2 + 1. \tag{5}$$

  Therefore

$$\forall i \in \{1, \ldots, m-1\}, \lambda_i \lambda_{i+1} \neq 1,$$

  which is the second relation of (4). The following expression of $h^\natural$ can be obtained using an induction argument (left to the reader) :

$$h^\natural = (X + \tilde{\lambda}_m) \cdots (X + \tilde{\lambda}_1)$$

where for i in $\{1,\dots,m\}$, $\tilde{\lambda}_i$ is defined by :

$$\tilde{\lambda}_i := \begin{cases} -1/\lambda_i \times (\lambda_1 \cdots \lambda_i)^2 & if\ i \equiv 1 \pmod 2, \\ -1/\lambda_i \times \dfrac{1}{(\lambda_1 \cdots \lambda_{i-1})^2} & if\ i \equiv 0 \pmod 2. \end{cases} \tag{6}$$

Furthermore, X^2+1 does not divide $h^\natural$, otherwise X^2+1 would divide h. Therefore

$$\forall i \in \{1,\dots,m-1\}, (X+\tilde{\lambda}_{i+1}) \cdot (X+\tilde{\lambda}_i) \neq X^2+1. \tag{7}$$

The relation $\theta(h^\natural) \cdot h = (X^2+1)^m$ can be written

$$(X+\theta(\tilde{\lambda}_m)) \cdots (X+\theta(\tilde{\lambda}_1)) \cdot (X+\lambda_1) \cdots (X+\lambda_m) = (X^2+1)^m. \tag{8}$$

As X^2+1 is central, the factorization of the skew polynomial $(X^2+1)^m$ into the product of monic skew polynomials dividing X^2+1 is not unique, therefore, according to Corollary 1, X^2+1 is necessarily the product of two consecutive monic linear factors of the left hand side of (8). According to (5) and (7), the only possibility is

$$(X+\theta(\tilde{\lambda}_1)) \cdot (X+\lambda_1) = X^2+1.$$

As X^2+1 is central, the relation (8) can be simplified and one gets

$$(X+\theta(\tilde{\lambda}_m)) \cdots (X+\theta(\tilde{\lambda}_2)) \cdot (X+\lambda_2) \cdots (X+\lambda_m) = (X^2+1)^{m-1}.$$

By repeating the same argument we get :

$$\begin{gathered} (X+\theta(\tilde{\lambda}_2)) \cdot (X+\lambda_2) = X^2+1, \\ \vdots \\ (X+\theta(\tilde{\lambda}_m)) \cdot (X+\lambda_m) = X^2+1. \end{gathered}$$

Considering the constant coefficients of the skew polynomials involved in the above equalities, we get that

$$\forall i \in \{1,\dots,m\}, \lambda_i \theta(\tilde{\lambda}_i) = 1 \Leftrightarrow \theta(\lambda_i)\tilde{\lambda}_i = 1,$$

and using the definition of $\tilde{\lambda}_i$ given in (6), one gets, for i odd, $(\lambda_i\lambda_{i+1})^2 = 1$ (third relation of (4)).
Conversely, consider $h = (X+\lambda_1)\cdots(X+\lambda_m)$ where $\lambda_1,\dots,\lambda_m$ are elements of $\mathbb{F}_{p^2}$ satisfying (4). According to the first relation of (4), the monic skew polynomials $X+\lambda_i$ divide X^2+1. According to the second relation of (4) and to Corollary 1, X^2+1 does not divide h. The skew polynomial $h^\natural$ is equal to $(X+\tilde{\lambda}_m)\cdots(X+\tilde{\lambda}_1)$ where $\tilde{\lambda}_i$ is defined by the relations (6). Furthermore, according to the third relation of (4), if i is odd, $(\lambda_1 \cdots \lambda_i)^2 = -1$, therefore for all i in $\{1,\dots,m\}$, $\lambda_i\theta(\tilde{\lambda}_i) = 1$ and

$X^2+1 = (X+\theta(\tilde{\lambda}_i))\cdot(X+\lambda_i)$. The product $\theta(h^\natural)\cdot h$ can be simplified as follows :

$$\begin{aligned}\theta(h^\natural)\cdot h &= (X+\theta(\tilde{\lambda}_m))\cdots(X+\theta(\tilde{\lambda}_1))\cdot(X+\lambda_1)\cdots(X+\lambda_m)\\ &= (X^2+1)\cdot(X+\theta(\tilde{\lambda}_m))\cdots(X+\theta(\tilde{\lambda}_2))\cdot(X+\lambda_2)\cdots(X+\lambda_m)\\ &\quad \text{(because } X^2+1 \text{ is central)}\\ &\vdots\\ &= (X^2+1)^{m-1}\cdot(X+\theta(\tilde{\lambda}_m))\cdot(X+\lambda_m)\\ &= (X^2+1)^m\end{aligned}$$

and one concludes that h belongs to $\overline{\mathcal{H}}_{(X^2+1)^m}$.

- The relations (4) enable to count the number of elements of $\overline{\mathcal{H}}_{(X^2+1)^m}$. Namely according to Corollary 1, the elements of $\overline{\mathcal{H}}_{(X^2+1)^m}$ have a unique factorization into the product of linear monic skew polynomials dividing X^2+1. Therefore the number of elements of the set $\overline{\mathcal{H}}_{(X^2+1)^m}$ is the number of m-tuples $(\lambda_1,\ldots,\lambda_m)$ of $(\mathbb{F}_{p^2})^m$ satisfying the conditions (4).
  Assume that $p=2$ and that m is an integer greater than 1. Then the conditions $\lambda_1\lambda_2 \neq 1$ and $(\lambda_1\lambda_2)^2 = 1$ are not compatible, therefore the set $\overline{\mathcal{H}}_{(X^2-1)^m}$ is empty. If $m=1$, it is reduced to $\{X+1, X+a, X+a^2\}$ where $a^2+a+1=0$.
  Assume that p is odd, then according to conditions (4), we have $p+1$ choices for λ_1, 1 choice for λ_2, p choices for λ_3, etc ... therefore one gets $(p+1)p^{\lfloor (m-1)/2\rfloor}$ elements.
- Lastly, thanks to (4), the expression of $h=(X+\lambda_1)\cdots(X+\lambda_m)$ can be simplified as $h=(X+\lambda_1)\cdot(X-\frac{1}{\lambda_1})\cdots(X+\lambda_3)\cdot(X-\frac{1}{\lambda_3})\cdots = (X^2+2\lambda_1 X-1)\cdot(X^2+2\lambda_3 X-1)\cdots$.

■

Remark 2. *Consider $p=2$, $f(X^2)=X^2+1$ and s a positive integer. According to Lemma 2, the set $\mathcal{H}_{(X^2+1)^{2^s}}$ can be written as :*

$$\mathcal{H}_{(X^2+1)^{2^s}} = \bigsqcup_{i=0}^{2^{s-1}} (X^2+1)^i\cdot\overline{\mathcal{H}}_{(X^2+1)^{2^s-2i}}.$$

According to Lemma 3, the sets $\overline{\mathcal{H}}_{(X^2+1)^{2^s-2i}}$ are empty when $2^s-2i\geq 2$. Therefore the above equality can be simplified as follows :

$$\begin{aligned}\mathcal{H}_{(X^2+1)^{2^s}} &= (X^2+1)^{2^{s-1}}\cdot\overline{\mathcal{H}}_{(X^2+1)^0},\\ &= \{(X+1)^{2^s}\}.\end{aligned}$$

One gets that for $s>0$ there is only one Hermitian self-dual θ-cyclic code of dimension 2^s over $\mathbb{F}_4$.

Proposition 4 below gives a formula for the number of Hermitian self-dual θ-negacyclic codes whose dimension is a power of p when p is an odd prime number.

Proposition 4. *Consider p an odd prime number, s a non-negative integer and θ the Frobenius automorphism over $\mathbb{F}_{p^2}$. The number of Hermitian self-dual θ-negacyclic codes of dimension p^s over $\mathbb{F}_{p^2}$ is*

Algorithm 2 Computation of $\mathcal{H}_{X^{2p^s}+1}$ for p odd prime

Require: s
Ensure: $\mathcal{H}_{X^{2p^s}+1}$
1: $\mathcal{H} \leftarrow \emptyset$
2: **for** $i = 0, \ldots, \frac{p^s-1}{2}$ **do**
3: $\quad M \leftarrow \frac{p^s-2i-1}{2}$
4: $\quad L \leftarrow \{\alpha \in \mathbb{F}_{p^2}^{M+1} \mid \alpha_i^{p+1} = -1, \alpha_{i+1} \neq -\alpha_i\}$
5: $\quad$ **for** $\alpha \in L$ **do**
6: $\quad\quad \mathcal{H} \leftarrow \{(X^2+1)^i \cdot (X^2 + 2\alpha_1 X - 1) \cdots (X^2 + 2\alpha_M X - 1) \cdot (X + \alpha_{M+1})\} \cup \mathcal{H}$
7: $\quad$ **end for**
8: **end for**
9: **return** $\mathcal{H}$

$$(p+1)\frac{p^{\frac{p^s+1}{2}}-1}{p-1}.$$

Proof.

Consider $R = \mathbb{F}_{p^2}[X;\theta]$. The number of Hermitian self-dual θ-negacyclic codes of dimension p^s over $\mathbb{F}_{p^2}$ is equal to $\#\mathcal{H}_{X^{2p^s}+1}$. According to Lemma 2, one has the following partition :

$$\mathcal{H}_{X^{2p^s}+1} = \bigsqcup_{i=0}^{M} (X^2+1)^i \cdot \overline{\mathcal{H}}_{(X^2+1)^{p^s-2i}},$$

where $M = \frac{p^s-1}{2}$. According to Lemma 3, one has $\#\overline{\mathcal{H}}_{(X^2+1)^{p^s-2i}} = (p+1) \times p^{\lfloor M-i \rfloor}$, therefore

$$\#\mathcal{H}_{X^{2p^s}+1} = (p+1)\sum_{i=0}^{M} p^{M-i} = (p+1)\frac{p^{M+1}-1}{p-1}.$$

■

Example 3. *Consider $\mathbb{F}_9 = \mathbb{F}_3(a)$ where $a^2 + 2a + 2 = 0$ and θ the Frobenius automorphism over $\mathbb{F}_9$. The monic solutions $h \in \mathbb{F}_9[X;\theta]$ to the self-dual skew equation $\theta(h^\natural) \cdot h = X^6 + 1$ are*

$$h = (X^2+1) \cdot (X + \alpha),$$

where $\alpha^4 = -1$ and

$$h = (X^2 + 2\alpha_1 X - 1) \cdot (X + \alpha_2),$$

where $\alpha_1^4 = \alpha_2^4 = -1$ and $\alpha_2 \neq -\alpha_1$. We get the 16 Hermitian self-dual θ-negacyclic codes of dimension 3 over $\mathbb{F}_9$ obtained in Example 2.

Example 4. *Consider $\mathbb{F}_9 = \mathbb{F}_3(a)$ where $a^2 + 2a + 2 = 0$ and θ the Frobenius automorphism over $\mathbb{F}_9$. Consider*

$$\alpha = (a, a, a^3, a, a^3, a, a, a^3, a^5, a^5, a^7, a^5, a^5, a^3) \in \mathbb{F}_9^{14}.$$

For all i in $\{1,\dots,14\}$, we have $\alpha_i^4 = -1$ and for all i in $\{1,\dots,13\}$, $\alpha_{i+1} \neq -\alpha_i$, therefore according to Lemma 3, the skew polynomial

$$h = (X^2 + 2\alpha_1 X - 1)\cdots(X^2 + 2\alpha_{13} X - 1)\cdot(X + \alpha_{14}) \in \mathbb{F}_9[X;\theta],$$

satisfies $\theta(h^\natural)\cdot h = X^{54} + 1$, and the skew polynomial $g = \theta(h^\natural)$ generates a $[54,27]_9$ Hermitian self-dual code. Furthermore, its minimum distance is 18, which is the best known minimum distance of $[54,27]$ linear codes over $\mathbb{F}_9$.

3.2.3 Construction of $\mathcal{H}_{f^{p^s}}$ for f in $\mathcal{F}$

The aim of this subsection is to construct $\mathcal{H}_{f^{p^s}}$ for f in $\mathcal{F}$ and to compute its number of elements.

Consider $f = f(X^2)$ in $\mathcal{F}$. Recall that according to Lemma 2, one has the partition:

$$\mathcal{H}_{f^{p^s}} = \bigsqcup_{i=0}^{\lfloor \frac{p^s}{2} \rfloor} f^i \cdot \overline{\mathcal{H}}_{f^{p^s-2i}},$$

where for m in $\mathbb{N}$, the set $\overline{\mathcal{H}}_{f^m}$ is defined by

$$\overline{\mathcal{H}}_{f^m} = \{h \in \mathcal{H}_{f^m} \mid f \text{ does not divide } h\}.$$

Lemma 4 below generalizes Lemma 3 and uses the same type of arguments linked to the factorization of skew polynomials.

Lemma 4. *Consider p a prime number, θ the Frobenius automorphism over $\mathbb{F}_{p^2}$, $R = \mathbb{F}_{p^2}[X;\theta]$, m a non-negative integer and $f = f(X^2)$ in $\mathcal{F}$ with degree $d = 2\delta > 1$ in X^2. The set $\overline{\mathcal{H}}_{f^m}$ is equal to*

$$\left\{h_1 \cdots h_m \mid h_j \in \mathcal{H}_f, h_j \neq \theta(h_{j-1}^\natural)\right\}$$

and has $(1+p^\delta)p^{\delta(m-1)}$ elements.

Proof. To simplify the presentation, the following notations will be used in this proof: $h = h(X)$, $f = f(X^2)$.

Consider h in $\overline{\mathcal{H}}_{f^m}$. As h divides f^m and f is irreducible in $\mathbb{F}_p[X^2]$, all the irreducible factors of h divide f and have the same degree d ([6, Lemma 13 (2)] or [16, page 6]):

$$h = \prod_{i=1}^{m} h_i,\ h_i \text{ monic}, \deg(h_i) = d, h_i | f,\ h_i \text{ irreducible}.$$

Furthermore, f does not divide h, therefore according to Proposition 3, for all j in $\{1,\dots,m-1\}$, $h_j \cdot h_{j+1}$ is distinct from f.

Using an induction argument (left to the reader), one gets the following expression of $h^\natural$:

$$h^\natural = \prod_{i=0}^{m-1} \frac{1}{\mu_{m-i}} h_{m-i}^\natural \cdot \mu_{m-i},$$

where $\mu_1 = 1$ and for $i \in \{2, \dots, m\}$, $\mu_i = (h_1 \cdots h_{i-1})_0$ is defined as the constant coefficient of $h_1 \cdots h_{i-1}$. Furthermore, this factorization (into the product of irreducible monic polynomials of same degree d dividing f) is unique (because the factorization of h is unique).

As the factorization of f^m into the product of irreducible factors is not unique (because f^m is central), according to Proposition 3, $f^m = \theta(h^\natural) \cdot h$ must have two consecutive irreducible monic factors whose product is f. As h and $h^\natural$ do not possess two consecutive factors whose product is f, necessarily, $\theta(\frac{1}{\mu_1} h_1^\natural \cdot \mu_1) \cdot h_1 = f$, and proceeding by induction, one gets

$$\forall j \in \{1, \dots, m\}, \theta\left(\frac{1}{\mu_j} h_j^\natural \cdot \mu_j\right) \cdot h_j = f \text{ and } h_{j+1} \neq \theta(\frac{1}{\mu_j} h_j^\natural \cdot \mu_j) \text{ when } j \neq m. \quad (9)$$

Conversely, consider $h = h_1 \cdots h_m$ with $\theta(\frac{1}{\mu_j} h_j^\natural \cdot \mu_j) \cdot h_j = f, h_{j+1} \neq \theta(\frac{1}{\mu_j} h_j^\natural \cdot \mu_j)$ and μ_j constant coefficient of $h_1 \cdots h_{j-1}$. Then $\theta(h^\natural) \cdot h = f^m$ and $h_j \cdot h_{j+1} \neq f$. Furthermore, the skew polynomials h_j are all irreducible because they are non-trivial factors of f, and f is irreducible in $\mathbb{F}_p[X^2]$. Therefore according to Proposition 3, the skew polynomial h is not divisible by f and it belongs to $\overline{\mathcal{H}}_{f^m}$.

To conclude, we get that

$$h \in \overline{\mathcal{H}}_{f^m} \Leftrightarrow \begin{cases} h = h_1 \cdots h_m, \\ \theta(\frac{1}{\mu_j} h_j^\natural \cdot \mu_j) \cdot h_j = f, \\ h_{j+1} \neq \theta(\frac{1}{\mu_j} h_j^\natural \cdot \mu_j), \\ \mu_1 = 1, \\ \mu_j = (h_1 \cdots h_{j-1})_0, j \neq 1. \end{cases}$$

Lastly, as $f(X^2) = f^\natural(X^2)$, the degree of $f(X^2)$ in X^2 is even, therefore, from the equality (9), one gets that for all $j \in \{1, \dots, m\}$, the degree of h_j is even and the constant coefficient of $h_j^\natural$ is $\frac{1}{\theta^{\deg(h_j)}((h_j)_0)} = \frac{1}{(h_j)_0}$. Furthermore, the constant coefficient of f is equal to 1 because $f(X^2) = f^\natural(X^2)$, therefore, following (9), we get

$$\forall j \in \{1, \dots, m\}, \theta\left(\frac{1}{\mu_j} \frac{1}{(h_j)_0} \mu_j\right) (h_j)_0 = 1$$

and

$$\forall j \in \{1, \dots, m\}, \theta((h_j)_0) = (h_j)_0.$$

As μ_j is defined as the constant coefficient of $h_1 \cdots h_{j-1}$, it is fixed by θ, therefore we get :

$$h \in \overline{\mathcal{H}}_{f^m} \Leftrightarrow \begin{cases} h = h_1 \cdots h_m, \\ \theta(h_j^\natural) \cdot h_j = f, \\ h_{j+1} \neq \theta(h_j^\natural). \end{cases}$$

The number of elements of $\overline{\mathcal{H}}_{f^m}$ follows from the fact that $\mathcal{H}_f$ has $1 + p^\delta$ elements ([9, Lemma 3.3]).

■

Algorithm 3 Computation of $\mathcal{H}_{f^{p^s}}$ for $f \in \mathcal{F}$

Require: f, s,
Ensure: $\mathcal{H}_{f^{p^s}}$
1: $\mathcal{H}_f \leftarrow \{h \in R \mid \theta(h^\natural) \cdot h = f(X^2)\}$
2: $\mathcal{H} \leftarrow \emptyset$
3: **for** $i = 0, \ldots, \lfloor \frac{p^s-1}{2} \rfloor$ **do**
4: $\quad m \leftarrow p^s - 2i$
5: $\quad L \leftarrow \{u = (u_1, \ldots, u_m) \in {\mathcal{H}_f}^m \mid u_{i+1} \neq \theta(u_i)\}$
6: $\quad$ **for** $u \in L$ **do**
7: $\quad\quad \mathcal{H} \leftarrow \{f(X^2)^i \cdot u_1 \cdots u_m\} \cup \mathcal{H}$
8: $\quad$ **end for**
9: **end for**
10: **return** $\mathcal{H}$

The construction of the set $\mathcal{H}_{f^{p^s}}$ for f in $\mathcal{F}$ is deduced from Lemma 2 and Lemma 4.

Proposition 5. *Consider p a prime number, θ the Frobenius automorphism over $\mathbb{F}_{p^2}$, $R = \mathbb{F}_{p^2}[X;\theta]$, s a non-negative integer and $f = f(X^2)$ in $\mathcal{F}$ with degree $d = 2\delta > 1$ in X^2. The set $\mathcal{H}_{f^{p^s}}$ has $\dfrac{p^{\delta(p^s+1)}-1}{p^\delta - 1}$ elements.*

Proof. According to Lemma 2, $\mathcal{H}_{f^{p^s}} = \bigsqcup_{i=0}^{\lfloor \frac{p^s}{2} \rfloor} f^i \cdot \overline{\mathcal{H}}_{f^{p^s-2i}}$ and according to Lemma 4, $\overline{\mathcal{H}}_{f^m}$ has $(1+p^\delta)(p^\delta)^{m-1}$ if $m \neq 0$ and 1 element if $m = 0$. Therefore $\mathcal{H}_{f^{p^s}}$ has $\sum_{i=0}^{(p^s-1)/2}(1+p^\delta)(p^\delta)^{p^s-2i-1}$ elements if p is odd and $1 + \sum_{i=0}^{2^{s-1}-1}(1+2^\delta)(2^\delta)^{2^s-2i-1}$ elements otherwise. In both cases one gets $\#\mathcal{H}_{f^{p^s}} = \frac{p^{\delta(p^s+1)}-1}{p^\delta-1}$. ∎

Corollary 2. *If $X^{4\delta}+1$ belongs to $\mathcal{F}$, then there are $\frac{p^{\delta(p^s+1)}-1}{p^\delta-1}$ Hermitian self-dual θ-negacyclic codes of length $n = 4\delta p^s$ over $\mathbb{F}_{p^2}$.*

Proof. We apply Proposition 5 to $f = f(X^2) = X^{4\delta}+1$. ∎

Example 5. *We give here an example of a $[36, 18, 13]$ Hermitian self-dual code over $\mathbb{F}_9 = \mathbb{F}_3(a)$ where $a^2 + 2a + 2 = 0$. Consider θ the Frobenius automorphism over $\mathbb{F}_9$ and the skew polynomial ring $R = \mathbb{F}_9[X;\theta]$. We have $X^4+1 \in \mathcal{F}$, and the set $\mathcal{H}_{X^4+1}$ of the irreducible skew polynomials H satisfying $\theta(H^\natural) \cdot H = X^4+1$ is equal to $\{X^2+X+2, X^2+a^2X+2, X^2+2X+2, X^2+a^6X+2\}$.*

Consider the product of 9 elements of $\mathcal{H}_{X^4+1}$: $h = (X^2+X+2)\cdot(X^2+X+2)\cdot(X^2+a^2X+2)\cdot(X^2+a^2X+2)\cdot(X^2+X+2)\cdot(X^2+a^2X+2)\cdot(X^2+a^2X+2)\cdot(X^2+a^2X+2)\cdot(X^2+2X+2) = X^{18}+a^3X^{17}+a^5X^{16}+2X^{15}+a^2X^{14}+a^2X^{13}+aX^{12}+a^7X^{11}+a^7X^{10}+a^3X^9+a^3X^8+a^7X^7+a^5X^6+a^2X^5+a^6X^4+2X^3+aX^2+a^3X+2$ in R.

The skew polynomial h belongs to $\mathcal{H}_{(X^4+1)^9}$ and the skew polynomial $g = \theta(h^\natural)$ generates a Hermitian self-dual θ-negacyclic $[36, 18, 13]$ code over $\mathbb{F}_9$.

3.2.4 Construction of $\mathcal{H}_{fp^s}$ for f in $\mathcal{G}$

In this section we propose an algorithm for the construction of $\mathcal{H}_{fp^s}$ for $f = gg^{\natural}$ in $\mathcal{G}$ which relies on the construction of all the irreducible skew polynomials dividing $g(X^2)$ in R (see Appendix A of [9]).

We first recall that the set $\mathcal{H}_{fp^s}$ can be partitioned as follows (see Lemma 3.2 of [8]).

Lemma 5. *Consider p a prime number, θ the Frobenius automorphism over $\mathbb{F}_{p^2}$, $R = \mathbb{F}_{p^2}[X;\theta]$, s a non-negative integer and $f = f(X^2) = g(X^2)g^{\natural}(X^2)$ in $\mathcal{G}$ with $g = g(X^2) \neq g^{\natural}(X^2)$ irreducible in $\mathbb{F}_p[X^2]$. One has the following partition*

$$\mathcal{H}_{fp^s} = \sqcup_{i=0}^{p^s} \sqcup_{j=0}^{p^s-i} g^i g^{\natural j} \cdot \overline{\mathcal{H}}_{fp^{s-(i+j)}}.$$

The construction of each set $\overline{\mathcal{H}}_{f^m}$ will rely on the construction of a new set of special factors of $g(X^2)^m$.

Lemma 6. *Consider p a prime number, θ the Frobenius automorphism over $\mathbb{F}_{p^2}$, $R = \mathbb{F}_{p^2}[X;\theta]$. Consider $g(X^2)$ an irreducible polynomial of $\mathbb{F}_p[X^2]$ and $\mathcal{R}_{g(X^2)^m}$ the set of all right factors u of $g(X^2)^m$ which are not divisible by $g(X^2)$ and which do not divide $g(X^2)^{m-1}$. We have*

$$\mathcal{R}_{g(X^2)^m} = \{u_1 \cdots u_m \mid u_i \text{ monic irreducible}, u_i | g(X^2) \text{ and } u_i \cdot u_{i+1} \neq g(X^2)\}.$$

Proof.

1. As $g(X^2)$ is irreducible in $\mathbb{F}_p[X^2]$, it is the product of two irreducible skew polynomials of degree equal to $\deg_{X^2} g(X^2)$, therefore $g(X^2)^m$ is the product of $2m$ irreducible skew polynomials of same degree. Assume that $g(X^2)^m = u_1 \cdots u_r \cdot v_1 \cdots v_s$ with $r+s = 2m$ and $r \geq m+1$; then $g(X^2)$ divides $u := u_1 \cdots u_r$. Namely, assume that $g(X^2)$ does not divide u. As $g(X^2)$ divides $u_1 \cdots u_r \cdot v_1 \cdots v_s$ then, according to Proposition 3, $g(X^2) = u_r \cdot v_1$ or there exists i in $\{1, \ldots, s-1\}$ such that $g(X^2) = v_i \cdot v_{i+1}$, therefore $g(X^2)^{m-1} = \tilde{u}_1 \cdots \tilde{u}_{\tilde{r}} \cdot \tilde{v}_1 \cdots \tilde{v}_{\tilde{s}}$ with $\tilde{r} \geq m$ and $\tilde{r} + \tilde{s} = 2(m-1)$; using an induction argument, we get a contradiction.
2. Assume that $u = u_1 \cdots u_m$ where for i in $\{1, \ldots, m\}$, u_i is a monic irreducible skew polynomial dividing $g(X^2)$ and $u_i \cdot u_{i+1} \neq g(X^2)$ for $i \in \{1, \ldots, m-1\}$.

   As u_i divides $g(X^2)$, u divides $g(X^2)^m$. Furthermore, according to Proposition 3, $g(X^2)$ does not divide u because $u_i \cdot u_{i+1} \neq g(X^2)$. Assume that u divides $g(X^2)^{m-1}$, then there exist $m-2$ irreducible skew polynomials $v_1, \ldots, v_{m-2}$ such that $g(X^2)^{m-1} = u_1 \cdots u_m \cdot v_1 \cdots v_{m-2} = u_1 \cdots u_r \cdot v_1 \cdots v_s$ with $r+s = 2(m-1)$ and $r \geq m$. Then according to point 1 of the proof, $g(X^2)$ divides u, which is impossible.
3. Assume that u divides $g(X^2)^m$, u does not divide $g(X^2)^{m-1}$ and $g(X^2)$ does not divide u. Consider $r \leq 2m$ such that $u = u_1 \cdots u_r$ where u_i is irreducible and divides $g(X^2)$. Necessarily, u divides $g(X^2)^r$, therefore, as u does not divide $g(X^2)^{m-1}$, we have $r \geq m$. Assume that $r \geq m+1$, then according to point 1 of the proof, $g(X^2)$ divides u, which is impossible. Therefore, $r = m$ and as $g(X^2)$ does not divide u, according to Lemma 3, we have for all i in $\{1, \ldots, r-1\}$, $u_i \cdot u_{i+1} \neq g(X^2)$.

■

Proposition 6. *Consider p a prime number, θ the Frobenius automorphism over $\mathbb{F}_{p^2}$, $R = \mathbb{F}_{p^2}[X;\theta]$. Consider $f(X^2) = g(X^2)g^\natural(X^2)$ where $g(X^2) \neq g^\natural(X^2)$ is an irreducible polynomial of $\mathbb{F}_p[X^2]$ and the map ϕ defined by :*

$$\phi : \begin{cases} \mathcal{R}_{g(X^2)^m} & \to \overline{\mathcal{H}}_{f(X^2)^m} \\ u & \mapsto \operatorname{lcrm}(u, v) \text{ where } \theta(u^\natural) \cdot v = g^\natural(X^2)^m. \end{cases}$$

The map ϕ is a bijection and the set $\overline{\mathcal{H}}_{f(X^2)^m}$ has $(1+p^\delta)p^{\delta(m-1)}$ elements where δ is the degree of $g(X^2)$ in X^2.

Proof.

- First the map ϕ is well defined. Namely, consider u in $\mathcal{R}_{g(X^2)^m}$, then u divides $g(X^2)^m$, it does not divide $g(X^2)^{m-1}$ and it is not divisible by $g(X^2)$. Furthermore, according to Lemma 6, the degree of u is equal to δm. Consider v in R such that $g^\natural(X^2)^m = \theta(u^\natural) \cdot v$ and $h = \operatorname{lcrm}(u, v)$, then the degree of v is δm and as u and v are leftcoprime, the degree of h is equal to $2\delta m$. As $g(X^2)$ does not divide u and $g^\natural(X^2)$ does not divide v, $g(X^2)$ and $g^\natural(X^2)$ do not divide h. Consider $\tilde{u}$ and $\tilde{v}$ in R such that $h = u \cdot \tilde{u} = v \cdot \tilde{v}$. Then, $\theta(h^\natural) \cdot h = V \cdot \theta(v^\natural) \cdot u \cdot \tilde{u} = U \cdot \theta(u^\natural) \cdot v \cdot \tilde{v}$ is divisible by the central polynomials $\theta(v^\natural) \cdot u = g(X^2)^m$ and $\theta(u^\natural) \cdot v = g^\natural(X^2)^m$, therefore $f(X^2)^m$ divides $\theta(h^\natural) \cdot h$. Considerations on the degrees lead to $\theta(h^\natural) \cdot h = f(X^2)^m$.
- Consider h in $\overline{\mathcal{H}}_{f(X^2)^m}$, then $\theta(h^\natural) \cdot h = f(X^2)^m$ with $g(X^2) \nmid h$ and $g^\natural(X^2) \nmid h$. Then $h = \operatorname{lcrm}(u, v)$ where $u = \operatorname{gcld}(h, g(X^2)^m)$ and $v = \operatorname{gcld}(h, g(X^2)^{\natural^m})$.
  The skew polynomial u belongs to the set $\mathcal{R}_{g(X^2)^m}$. Namely, u divides $g(X^2)^m$ by construction; $g(X^2)$ does not divide h, therefore it does not divide u; lastly u does not divide $g(X^2)^{m-1}$, otherwise $g(X^2)$ would divide $\theta(h^\natural)$, which is impossible. Therefore, according to Lemma 6, $u = u_1 \cdots u_m$ where $u_1, \ldots, u_m$ are m irreducible skew polynomials dividing $g(X^2)$ and such that $u_i \cdot u_{i+1} \neq g(X^2)$ for i in $\{1, \ldots, m-1\}$.
  In the same way, one gets that $v = v_1 \cdots v_m$ where $v_1, \ldots, v_m$ are m irreducible skew polynomials dividing $g^\natural(X^2)$ and such that $v_i \cdot v_{i+1} \neq g^\natural(X^2)$ for i in $\{1, \ldots, m-1\}$. Now consider U and V in R such that $h = u \cdot U = v \cdot V$, then $\theta(h^\natural) = \tilde{V} \cdot \theta(v^\natural)$ and $\theta(h^\natural) \cdot h = \tilde{V} \cdot \theta(v^\natural) \cdot u \cdot U$. As $\theta(h^\natural) \cdot h = g(X^2)^m g^\natural(X^2)^m$ is central, we get $\theta(v^\natural) \cdot u \cdot U \cdot \tilde{V} = g(X^2)^m g^\natural(X^2)^m$. We deduce from this equality that $\operatorname{lclm}(g(X^2)^m, U \cdot \tilde{V})$ divides $\theta(v^\natural) \cdot u \cdot U \cdot \tilde{V}$. Therefore $g(X^2)^m$ divides $\theta(v^\natural) \cdot u$ and considerations on the degrees of the polynomials lead to $g(X^2)^m = \theta(v^\natural) \cdot u$.
- The elements of $\mathcal{R}_{g(X^2)^m}$ are of the form $g_1 \cdots g_m$ where $g_1, \ldots, g_m$ are irreducible monic factors of $g(X^2)$ and $g_i \cdot g_{i+1} \neq g(X^2)$. As $g(X^2)$ has $1+p^\delta$ monic irreducible factors ([16] or [9, Appendix A]), we get that $\#\overline{\mathcal{H}}_{f(X^2)^m} = (1+p^\delta)p^{\delta(m-1)}$.

■

Proposition 7. *Consider p a prime number, θ the Frobenius automorphism over $\mathbb{F}_{p^2}$, $R = \mathbb{F}_{p^2}[X;\theta]$, s a non-negative integer and $f = f(X^2)$ in $\mathcal{G}$ with degree $d = 2\delta > 1$ in X^2. The set $\mathcal{H}_{f^{p^s}}$ has $\frac{(p^{\delta(p^s+1)}-2p^s-3)(1+p^\delta)+4p^s+4}{(p^\delta-1)^2}$ elements.*

Algorithm 4 Computation of $\mathcal{H}_{f^{p^s}}$ for $f = g \cdot g^\natural \in \mathcal{G}$

Require: $f \in \mathcal{G}, s$
Ensure: $\mathcal{H}_{f^{p^s}}$
$\mathcal{I} \leftarrow$ set of monic irreducible right divisors of $g(X^2)$ in R
$\mathcal{H} \leftarrow \emptyset$
for $i = 0, \ldots, p^s$ **do**
  for $j = 0, \ldots, p^s - i$ **do**
    $m \leftarrow p^s - i - j$
    $\mathcal{R} \leftarrow \{u_1 \cdots u_m \mid u_i \in \mathcal{I}, u_i \cdot u_{i+1} \neq g(X^2)\}$
    for $u \in \mathcal{R}$ **do**
      $v \leftarrow$ quotient of the division of $g^\natural(X^2)^m$ by $\theta(u^\natural)$
      $\mathcal{H} \leftarrow \{g(X^2)^i \cdot g^\natural(X^2)^j \cdot \mathrm{lcrm}(u, v)\} \cup \mathcal{H}$
    end for
  end for
end for
return $\mathcal{H}$

Corollary 3. *If $X^{4\delta} + 1$ belongs to $\mathcal{G}$, then there are $\frac{(p^{\delta(p^s+1)} - 2p^s - 3)(1+p^\delta) + 4p^s + 4}{(p^\delta - 1)^2}$ Hermitian self-dual θ-negacyclic codes of length $n = 4\delta p^s$ over $\mathbb{F}_{p^2}$.*

Proof. We apply Proposition 7 to $f = f(X^2) = X^{4\delta} + 1$. ∎

Example 6. *The polynomial $f(X^2) = X^{16} + 1$ factorizes over $\mathbb{F}_3[X^2]$ as $f(X^2) = g(X^2)g^\natural(X^2)$ where $g(X^2) = X^8 + X^4 + 2$ and $g^\natural(X^2) = X^8 + 2X^4 + 2$ are irreducible in $\mathbb{F}_3[X^2]$. Consider $\mathbb{F}_9 = \mathbb{F}3(a)$ with $a^2 + 2a + 2 = 0$ and θ Frobenius automorphism over $\mathbb{F}_9$. Consider the following irreducible skew polynomials dividing $X^8 + X^4 + 2$ in $R = \mathbb{F}_9[X; \theta]$: $u_1 = X^4 + a^3X^3 + a^7X^2 + 2X + a^7, u_2 = X^4 + a^6X^3 + 2X^2 + a^2X + a^7$ and $u_3 = X^4 + a^2X^2 + a^5X + a$. As $u_1 \cdot u_2$ and $u_2 \cdot u_3$ are distinct of $X^8 + X^4 + 2$, the skew polynomial $u = u_1 \cdot u_2 \cdot u_3$ belongs to $\mathcal{R}_{(X^8+X^4+2)^3}$. Consider v in R such that $\theta(u^\natural) \cdot v = (X^8 + 2X^4 + 2)^3$ and $h = \mathrm{lcrm}(u, v)$. Then the skew polynomial $g = \theta(h^\natural) = X^{24} + aX^{23} + a^5X^{22} + X^{21} + X^{20} + aX^{19} + a^6X^{18} + a^2X^{17} + a^3X^{15} + X^{14} + a^7X^{13} + a^6X^{12} + a^3X^{11} + X^{10} + a^7X^9 + a^6X^7 + a^6X^6 + a^5X^5 + X^4 + 2X^3 + a^5X^2 + a^5X + 1$ generates a $[48, 24, 16]$ Hermitian self-dual θ-negacyclic code over $\mathbb{F}_9$.*

3.2.5 Construction and enumeration of Hermitian self-dual θ-negacyclic codes.

Recall that there is a counting formula for Hermitian self-dual θ-cyclic codes of odd dimension over $\mathbb{F}_4$. In what follows we give a formula for the number of Hermitian self-dual θ-negacyclic codes of any dimension over $\mathbb{F}_{p^2}$ where p is a prime number and θ is the Frobenius automorphism over $\mathbb{F}_{p^2}$. When p is even, θ-negacyclic codes are θ-cyclic codes.

Theorem 1. *Consider p a prime number, θ the Frobenius automorphism over $\mathbb{F}_{p^2}$, k a positive integer, s, t two integers such that $k = p^s \times t$ and p does not divide t. The*

number of self-dual θ-negacyclic codes over $\mathbb{F}_{p^2}$ with dimension k is $\#\mathcal{H}_{X^{2k}+1} =$

$$N \times \prod_{\substack{f\in\mathcal{F}, f\mid X^{2k}+1\\ \deg(f)=2\delta}} \frac{p^{\delta(p^s+1)}-1}{p^\delta-1} \times \prod_{\substack{f\in\mathcal{G}, f\mid X^{2k}+1\\ \deg(f)=2\delta}} \frac{(p^{\delta(p^s+1)}-2p^s-3)(1+p^\delta)+4p^s+4}{(p^\delta-1)^2}$$

where

$$N = \begin{cases} 3 & \text{if } p=2 \text{ and } s=0,\\ 1 & \text{if } p=2 \text{ and } s>0 \text{ or } p \text{ odd and } t \text{ even},\\ (p+1)\frac{p^{\frac{p^s+1}{2}}-1}{p-1} & \text{if } p \text{ odd and } t \text{ is odd.}\end{cases}$$

Proof. According to Proposition 1 we have

$$\#\mathcal{H}_{X^{2k}+1} = N \times \prod_{\substack{f\in\mathcal{F}\cup\mathcal{G}, f\mid X^{2k}+1,\\ \deg(f)=2\delta}} \#\mathcal{H}_{f^{p^s}}$$

where

$$N = \begin{cases} 1 & \text{if } X^2+1 \text{ does not divide } X^{2k}+1,\\ \#\mathcal{H}_{(X^2+1)^{p^s}} & \text{otherwise.}\end{cases}$$

Therefore, $N = 1$ if t is even and p odd; otherwise $N = \#\mathcal{H}_{(X^2+1)^{p^s}}$ is given by Remark 2 and Proposition 4. Furthermore, for f in $\mathcal{F}\cup\mathcal{G}$, $\#\mathcal{H}_{f^{p^s}}$ is given by Proposition 5 and Proposition 7. ∎

Algorithm 5 Computation of $\mathcal{H}_{X^n+1}$ (factorization strategy)

Require: k
Ensure: $\mathcal{H}_{X^{2k}+1}$
1: Compute s, t such that $k = p^s \times t$ and $p \nmid t$
2: Compute $f_1(X^2), \ldots, f_r(X^2) \in \{X^2+1\} \cup \mathcal{F} \cup \mathcal{G}$ such that $X^{2t}+1 = f_1(X^2)\cdots f_r(X^2)$ in $\mathbb{F}_p[X^2]$ and $\gcd(f_i(X^2), f_j(X^2)) = 1$ in $\mathbb{F}_p[X^2]$ for $i \neq j$.
3: Using Algorithms 2, 3 and 4, compute $\mathcal{H}_{f_i(X^2)^{p^s}}$
4: $\mathcal{H} \leftarrow \emptyset$
5: **for** $(h_1, \ldots, h_r) \in \mathcal{H}_{f_1(X^2)^{p^s}} \times \cdots \times \mathcal{H}_{f_r(X^2)^{p^s}}$ **do**
6: $\quad \mathcal{H} \leftarrow \mathcal{H} \cup \{\mathrm{lcrm}(h_1, \ldots, h_r)\}$
7: **end for**
8: **return** $\mathcal{H}$

Example 7. *We give here an example of a $[30, 15, 12]$ Hermitian self-dual code over $\mathbb{F}_9 = \mathbb{F}_3(a)$ where $a^2+2a+2=0$. Consider θ, the Frobenius automorphism over $\mathbb{F}_9$ and the skew polynomial ring $R = \mathbb{F}_9[X;\theta]$. We have $X^{30}+1 = ((X^2)^5+1)^3 = (X^2+1)^3(X^8-X^6+X^4-X^2+1)^3$.*

Consider $h_1 = X^3+a^2X^2+a^3X+a^7 \in \mathcal{H}_{(X^2+1)^3}$ and $h_2 = X^{12}+aX^{11}+a^7X^{10}+X^9+a^5X^8+a^6X^7+2X^6+a^2X^5+a^5X^4+2X^3+a^7X^2+a^5X+1 \in \mathcal{H}_{(X^8-X^6+X^4-X^2+1)^3}$, then the skew polynomial $h = \mathrm{lcrm}(h_1, h_2)$ belongs to $\mathcal{H}_{X^{30}+1}$ and the skew polynomial $g = \theta(h^\natural)$ generates a $[30, 15, 12]$ Hermitian self-dual θ-negacyclic code over $\mathbb{F}_9$.

Example 8. *We consider here Hermitian self-dual θ-cyclic codes with length* 68 *over* $\mathbb{F}_4 = \mathbb{F}_2(a)$ *where* $a^2 + a + 1 = 0$ *and* θ *is the Frobenius automorphism over* $\mathbb{F}_4$. *According to [13], the best known minimum distance of Hermitian self-dual codes of length* 68 *over* $\mathbb{F}_4$ *is equal to 16. We provide here an example of a* $[68, 34, 18]$ *Hermitian self-dual code over* $\mathbb{F}_4$. *Consider* $h_1 = X^2 + 1$,

$$h_2 = (X^8+X^5+X^4+X^3+1)\cdot(X^8+a^2X^7+aX^6+a^2X^5+a^2X^4+a^2X^3+aX^2+a^2X+1)$$

and

$$h_3 = (X^8+a^2X^7+aX^5+X^4+aX^3+a^2X+1)\cdot(X^8+a^2X^7+X^5+X^4+X^3+a^2X+1).$$

We have $h_1 \in \mathcal{H}_{(X^2+1)^2}, h_2 \in \mathcal{H}_{(X^{16}+X^{10}+X^8+X^6+1)^2}$ *and* $h_3 \in \mathcal{H}_{(X^{16}+X^{14}+X^{12}+X^8+X^4+X^2+1)^2}$, *therefore* $h = \mathrm{lcrm}(h_1, h_2, h_3)$ *belongs to* $\mathcal{H}_{(X^{34}+1)^2}$. *One checks that the θ-cyclic code of length* 68 *and skew generator polynomial* $g = \Theta(h^*)$ *is a Hermitian self-dual* $[68, 34, 18]$ *code. We give below the expression of g :* $g = X^{34} + aX^{33} + a^2X^{32} + aX^{31} + aX^{30} + a^2X^{26} + aX^{23} + a^2X^{22} + X^{21} + a^2X^{20} + a^2X^{19} + a^2X^{15} + a^2X^{14} + X^{13} + a^2X^{12} + aX^{11} + a^2X^8 + aX^4 + aX^3 + a^2X^2 + aX + 1$.

4 Existence conditions of Hermitian self-dual θ-cyclic and θ-negacyclic codes over $\mathbb{F}_{p^e}$ with $e > 2$ even.

In what follows, we assume that $q = p^e$ where p is a prime number and e is an even integer. Therefore the automorphism σ is defined by $\sigma = Frob^{\frac{e}{2}} : x \mapsto x^{p^{\frac{e}{2}}}$ where $Frob : x \mapsto x^p$ is the Frobenius automorphism over $\mathbb{F}_q$. We consider the non-negative integer r defined by

$$\theta = Frob^r : x \mapsto x^{p^r},$$

and the ring $R = \mathbb{F}_q[X; \theta]$ of skew polynomials.

We denote ℓ the order of θ and $\mathbb{F}_q^\theta$ the fixed field of θ.

We denote μ the integer such that $2^\mu \mid\mid p + 1$, which means that 2^μ divides $p + 1$ and $2^{\mu+1}$ does not divide $p + 1$.

We recall that for $F = F(X^\ell)$ in $\mathbb{F}_q^\theta[X^\ell]$, the set $\mathcal{H}_F$ is defined by

$$\mathcal{H}_F := \{h \in R := \mathbb{F}_q[X; \theta] \mid h \text{ is monic and } \sigma(h^\natural) \cdot h = F(X^\ell)\}.$$

The Hermitian self-dual θ-cyclic codes of length n over $\mathbb{F}_q$ are completely determined by the set $\mathcal{H}_{X^n-1}$ while the Hermitian self-dual θ-negacyclic codes are determined by $\mathcal{H}_{X^n+1}$. Recall also that we assume here that the order ℓ of θ divides the length n of the considered codes.

4.1 Existence conditions of Hermitian self-dual θ-cyclic codes over $\mathbb{F}_{p^e}$ with $e > 2$ even.

Recall that over $\mathbb{F}_{p^2}$, there is no Hermitian self-dual θ-cyclic code if p is an odd prime number. In what follows we prove that this non-existence result can be extended to $\mathbb{F}_q = \mathbb{F}_{p^e}$. We start with an intermediate lemma :

Lemma 7. *Consider $F(X^\ell) = F_1(X^\ell)F_2(X^\ell) \in \mathbb{F}_q^\theta[X^\ell]$ where $F_1(X^\ell)$ and $F_2(X^\ell)$ are coprime in $\mathbb{F}_q^\theta[X^\ell]$ and such that $\sigma(F_i^\natural) = F_i$. If $\mathcal{H}_F \neq \emptyset$ then $\mathcal{H}_{F_i} \neq \emptyset$.*

Proof. Consider h in R such that $\sigma(h^\natural) \cdot h = F(X^\ell)$. Consider, for $i \in \{1, 2\}$, $h_i = \text{gcld}(h, F_i(X^\ell))$ and H_i in R such that $h = h_i \cdot H_i$. We have $\sigma(h^\natural) = \tilde{H}_i \cdot \sigma(h_i^\natural)$ where $\tilde{H}_i$ is in R. Therefore $F(X^\ell) = \sigma(h^\natural) \cdot h = \tilde{H}_1 \cdot \sigma(h_1^\natural) \cdot h_1 \cdot H_1$. As $F(X^\ell)$ is central, we get that $\sigma(h_1^\natural) \cdot h_1$ divides $F(X^\ell)$. As $F_2(X^\ell)$ also divides $F(X^\ell)$, $\text{lcrm}(\sigma(h_1^\natural) \cdot h_1, F_2(X^\ell))$ divides $F(X^\ell)$. But $F_2(X^\ell)$ is a central polynomial which has no common factor with $\sigma(h_1^\natural) \cdot h_1$ because h_1 and $\sigma(h_1^\natural)$ both divide $F_1(X^\ell) = \sigma(F_1^\natural(X^\ell))$ and $F_1(X^\ell)$ is coprime with $F_2(X^\ell)$. Therefore $\text{lcrm}(\sigma(h_1^\natural) \cdot h_1, F_2(X^\ell)) = \sigma(h_1^\natural) \cdot h_1 \cdot F_2(X^\ell)$ divides $F(X^\ell) = F_1(X^\ell)F_2(X^\ell)$ and $\sigma(h_1^\natural) \cdot h_1$ divides $F_1(X^\ell)$. In the same way, $\sigma(h_2^\natural) \cdot h_2$ divides $F_2(X^\ell)$. We conclude by noticing that $2\deg(h) = 2(\deg(h_1) + \deg(h_2)) = \deg(F_1) + \deg(F_2)$. Assume that $2\deg(h_1) < \deg(F_1)$, then $\deg(F_1) + \deg(F_2) < \deg(F_1) + 2\deg(h_2)$, therefore $\deg(F_2) < 2\deg(h_2)$, which is impossible. Therefore we get that $\sigma(h_1^\natural) \cdot h_1 = F_1(X^\ell)$. ∎

Theorem 2. *If p is an odd prime number then there is no Hermitian self-dual θ-cyclic code over $\mathbb{F}_{p^e}$.*

Proof.

Assume that there exists a Hermitian self-dual $\theta-$cyclic code of dimension k over $\mathbb{F}_{p^e}$. Then the set $\mathcal{H}_{X^{2k}-1}$ is non-empty. Consider $f_1(X^\ell) = (X^\ell - 1)^{p^s}$ and $f_2(X^\ell) = (X^{2k}-1)/(X^\ell-1)^{p^s}$. As $f_1(X^\ell)$ is a central polynomial coprime with $f_2(X^\ell)$ and satisfying $\sigma(f_1^\natural) = f_1$, according to Proposition 7, the set $\mathcal{H}_{f_1(X^\ell)}$ is non-empty. Consider $H \in \mathbb{F}_{p^e}[X;\theta]$ with degree d and constant coefficient α such that

$$\sigma(H^\natural) \cdot H = \left(X^\ell - 1\right)^{p^s}.$$

Then we have

$$\sigma\left(\frac{1}{\theta^d(\alpha)}\right)\alpha = -1.$$

Furthermore, we have $\ell = \dfrac{e}{gcd(e,r)}$ therefore $\ell r = e\mu$ where $\mu = \dfrac{r}{gcd(e,r)}$ and we have :

$$\sigma \circ \theta^d = Frob^{\frac{e}{2}+\frac{r\ell p^s}{2}} = Frob^{\frac{e}{2}+\frac{e\mu p^s}{2}} = Frob^{\frac{e}{2}(1+\mu p^s)} = \sigma^{1+\mu p^s}.$$

As the order of σ is 2, if μ is odd, then $\sigma \circ \theta^d$ is the identity and we have $-1 = \sigma\left(\dfrac{1}{\theta^d(\alpha)}\right)\alpha = 1$ which is not possible because the characteristic of the field is odd. If

μ is even, we have $\sigma \circ \theta^d = \sigma$. Therefore θ^d is the identity, so ℓ divide $d = \frac{\ell}{2}p^s$, which is impossible because p is odd. ∎

4.2 Existence conditions of Hermitian self-dual θ-negacyclic codes over $\mathbb{F}_{p^e}$ with $e > 2$ even.

In what follows, we will give necessary and sufficient conditions for the existence of Hermitian self-dual $\theta-$negacyclic codes over $\mathbb{F}_{p^e}$ where p is an odd prime number.

Lemma 8. *If one of the following conditions is satisfied, then there exists a Hermitian self-dual θ-negacyclic code of dimension k over $\mathbb{F}_{p^e}$:*

(i) $\frac{e}{2} \equiv 1 \pmod 2$ *and* $r \equiv 1 \pmod 2$*;*
(ii) $p \equiv 1 \pmod 4$*;*
(iii) $p \equiv 3 \pmod 4$ *and* $\frac{e}{2} \equiv 0 \pmod 2$*;*
(iv) $p \equiv 3 \pmod 4$, $\frac{e}{2} \equiv 1 \pmod 2$, $r \equiv 0 \pmod 2$ *and* $k \equiv 0 \pmod{2^{\mu-1}}$.

Proof.

Assume that (i) is satisfied, then the restrictions of θ and of σ to $\mathbb{F}_{p^2}$ are equal to the Frobenius automorphism, therefore according to Theorem 1, there is a monic skew polynomial h in $\mathbb{F}_{p^2}[X;\theta] \subset R$ such that $\sigma(h^\natural) \cdot h = X^{2k} + 1$.

Assume that one of the assertions $(ii), (iii)$ or (iv) is satisfied. As the order ℓ of θ is equal to $\frac{e}{\gcd(e,r)}$, if (iii) is satisfied, we have $k \times \gcd(e,r) \equiv 0 \pmod 2$ and $r \times k \equiv 0 \pmod 2$. Therefore, according to [7, Proposition 4 and Proposition 5 or Table 1], the equation $h^\natural \cdot h = X^{2k}+1$ has a solution in $\mathbb{F}_{p^{e/2}}[X;\theta]$. Furthermore, as σ is the identity over $\mathbb{F}_{p^{e/2}}$, we get that there exists h in $\mathbb{F}_{p^{e/2}}[X;\theta] \subset R$ such that $\sigma(h^\natural) \cdot h = X^{2k}+1$. ∎

Lemma 9. *Assume that $p \equiv 3 \pmod 4$, $\frac{e}{2} \equiv 1 \pmod 2$, $r \equiv 0 \pmod 2$. If $k \not\equiv 0 \pmod{2^{\mu-1}}$, then there is no Hermitian self-dual $\theta-$negacyclic of length $n = 2k$ over $\mathbb{F}_{p^e}$.*

Proof. Assume that there exists a Hermitian self-dual $\theta-$negacyclic code of length n over $\mathbb{F}_{p^e}$, then $\mathcal{H}_{X^n+1} \neq \emptyset$. Consider $s \in \mathbb{N}$, $t \in \mathbb{N}^*$ not divisible by p such that $n = \ell t p^s$ and a in $\mathbb{N}^*$ such that 2^{a-1} divides exactly k. That means that 2^{a-1} divides k but 2^a does not divide k. Furthermore, $p \equiv 3 \pmod 4$, $\frac{e}{2} \equiv 1 \pmod 2$, $r \equiv 0 \pmod 2$, therefore p and $\ell = \frac{e}{\gcd(e,r)}$ are odd numbers, and 2^a divides exactly t. As a consequence, we have

$$\begin{aligned} X^n + 1 &= \left(\left(X^\ell\right)^t + 1\right)^{p^s} \\ &= \left(\left(X^\ell\right)^{2^a} + 1\right)^{p^s} F(X^\ell)^{p^s}, \end{aligned}$$

where $F(X^\ell) \in \mathbb{F}_p[X^\ell]$ is coprime with $\left(\left(X^\ell\right)^{2^a} + 1\right)^{p^s}$.

As $k \not\equiv 0 \pmod{2^{\mu-1}}$, we have $\mu > a$, therefore, according to [2, Theorem 1], the factorization of $Y^{2^a} + 1 \in \mathbb{F}_p[Y]$ over $\mathbb{F}_p$ into the product of distinct irreducible

polynomials is of the form

$$Y^{2^a}+1=f_1(Y)\cdots f_{2^{a-1}}(Y),$$

where $f_i=Y^2+b_iY+1$ is irreducible in $\mathbb{F}_p[Y]$. Furthermore $f_i(Y)=g_ig_i^{\natural}$ over $\mathbb{F}_{p^2}$ where $g_i=Y+a_i$. One has $g_i^{\natural}=Y+\dfrac{1}{a_i}$ and $\sigma(g_i^{\natural})=g_i$.

Therefore, according to Lemma 7 applied to $F_1(X^\ell)=\left(g_i(X^\ell)\right)^{p^s}$ and $F_2(X^\ell)=(X^n+1)/F_1(X^\ell)$, there exists a skew polynomial $H_i\in\mathbb{F}_{p^e}[X;\theta]$ such that

$$\sigma(H_i^{\natural})\cdot H_i=\left(g_i(X^\ell)\right)^{p^s}=\left(X^\ell+a_i\right)^{p^s}.$$

The degree of $\sigma(H_i^{\natural})\cdot H_i$ is even and the degree of $\left(X^\ell+a_i\right)^{p^s}$ is odd, a contradiction. ∎

Theorem 3. *Consider p an odd prime number, e an even positive integer, r a non-negative integer, k a positive integer and θ the automorphism over $\mathbb{F}_q=\mathbb{F}_{p^e}$ defined by: $a\mapsto a^{p^r}$. There exists a Hermitian self-dual $\theta-$negacyclic code over $\mathbb{F}_{p^e}$ of dimension k if, and only if, one of the following conditions is satisfied :*

1. $p\equiv 1 \pmod 4$;
2. $p\equiv 3 \pmod 4$ *and* $\frac{e}{2}\equiv 0 \pmod 2$;
3. $p\equiv 3 \pmod 4$, $\frac{e}{2}\equiv 1 \pmod 2$ *and* $r\equiv 1 \pmod 2$;
4. $p\equiv 3 \pmod 4$, $\frac{e}{2}\equiv 1 \pmod 2$, $r\equiv 0 \pmod 2$ *and* $k\equiv 0 \pmod{2^{\mu-1}}$.

Proof. The proof is directly deduced from Lemma 8 and Lemma 9. ∎

Remark 3. *Recall that if $\theta=id$ (i.e. $r=0$), and $e=2$, we get Hermitian self-dual negacyclic codes over $\mathbb{F}_{p^2}$. According to Theorem 3, there exists a Hermitian self-dual negacyclic code of dimension k over $\mathbb{F}_{p^2}$ if, and only if, one of the following conditions is satisfied*

1. $p\equiv 1 \pmod 4$
2. $p\equiv 3 \pmod 4$ *and* $k\equiv 0 \pmod{2^{\mu-1}}$ *where* $2^\mu||p+1$.

This is equivalent to $p+1\not\equiv 0 \pmod{2^{a+1}}$ where $2^a \mid\mid n$ and we get the existence conditions given in [18, Theorem 3.9].

Remark 4. *If θ is the Frobenius automorphism (i.e. $r=1$), then there always exists a Hermitian self-dual θ-negacyclic code of any dimension over $\mathbb{F}_{p^e}$.*

5 Conclusion.

This text gives an overview of the construction of Hermitian self-dual θ-cyclic and θ-negacyclic codes of length n over $\mathbb{F}_{p^2}$ when θ is the Frobenius automorphism. Existence conditions for these codes over any finite finite field $\mathbb{F}_q$ where q is an even power of a prime number are also given. The construction of this family of codes could be generalized over $\mathbb{F}_{p^n}$ following [1]. Furthermore it happens that one can also consider Hermitian self-dual skew constacyclic codes which are not skew negacyclic nor

skew cyclic, on the contrary to Euclidean self-dual skew constacyclic codes which are necessarily skew cyclic or skew negacyclic.

References

[1] Batoul A., Boucher D., and Boulanouar R. D.: A construction of self-dual skew cyclic and negacyclic codes of length n over $\mathbb{F}_{p^n}$. Lecture Notes in Computer Science, **12542** (2020).

[2] Blake I.F., Gao S., Mullin R. C.: Explicit factorization of $x^{2^k}+1$ over $\mathbb{F}_p$ with prime $p \equiv 3 \bmod 4$. Appl. Algebra Engrg. Comm. Comput., **4**, (1993), 2, 89–94.

[3] Bose R. C., Chakravarti I. M. : Hermitian varieties in a finite projective space PG(N, q^2). Canadian J. Math., **18**, (1966), 1161–1182.

[4] Bosma W., Cannon J., Playoust C.: The Magma algebra system. I. The user language. Journal of Symbolic Computation, **24**, (1997), 3-4, 235–265 .

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

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

[7] Boucher D.: A note on the existence of self-dual skew codes over finite fields. Lecture Notes in Comput. Sci., **9084**, 228–239. (2015).

[8] Boucher D.: Construction and number of self-dual skew codes over $\mathbb{F}_{p^2}$. Adv. Math. Commun., **10** (2016), 765–795.

[9] Boucher D.: A first step towards the skew duadic codes. Adv. Math. Commun., 12(3) (2018), 553–577.

[10] Boucher D.: Autour de codes définis à l'aide de polynômes tordus. HDR, Université de Rennes 1, juin 2020.

[11] Caruso X., Drain F.: Selfdual skew cyclic codes. hal-04127001

[12] Datta M., Ghorpade S.R.: Number of solutions of systems of homogeneous polynomial equations over finite fields. Proceedings of the American Mathematical Society, 145, 2017, 2, 525–541.

[13] Gaborit P.: Table of Hermitian self-dual codes over $\mathbb{F}_4$. https://www.unilim.fr/pages_perso/philippe.gaborit/SD/GF4H/GF4H.htm

[14] Irwansyah et al.,: A note on the construction and enumeration of Euclidean self-dual skew-cyclic codes Appl. Algebra Eng. Commun. Comput. 32, No. 3, 345–358, 2021

[15] Jacobson N.: The Theory of Rings. American Mathematical Society Mathematical Surveys, vol. II. American Mathematical Society, New York, 1943.

[16] Odoni R. W. K.: On additive polynomials over a finite field. Proc. Edinburgh Math. Soc. (2), 42(1):1–16, 1999.

[17] Ore O.: Theory of non-commutative polynomials. Ann. of Math. (2), 34(3):480–508, 1933.

[18] Yang Y., Cai W.: On self-dual constacyclic codes over finite fields. Designs, Codes and Cryptography., 74, (2015), 355–364.