



**HAL**  
open science

# Construction and number of self-dual skew codes over $F_{p^2}$

Delphine Boucher

► **To cite this version:**

Delphine Boucher. Construction and number of self-dual skew codes over  $F_{p^2}$ . *Advances in Mathematics of Communications*, 2016, Volume 10 (Issue 4), pp.765 - 795. 10.3934/amc.2016040 . hal-01090922v2

**HAL Id: hal-01090922**

**<https://hal.science/hal-01090922v2>**

Submitted on 1 Feb 2016

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Construction and number of self-dual skew codes over $\mathbb{F}_{p^2}$ .

February 1, 2016

DELPHINE BOUCHER

IRMAR (UMR 6625)

Université de Rennes 1, Campus de Beaulieu

F-35042 Rennes

## Abstract

The aim of this text is to construct and to enumerate self-dual  $\theta$ -cyclic and  $\theta$ -negacyclic codes over  $\mathbb{F}_{p^2}$  where  $p$  is a prime number and  $\theta$  is the Frobenius automorphism.

## 1 Introduction

A linear code over a finite field  $\mathbb{F}_q$  is a  $k$ -dimensional subspace of  $\mathbb{F}_q^n$ . Cyclic codes over  $\mathbb{F}_q$  form a class of linear codes who are invariant under a cyclic shift of coordinates. This cyclicity condition enables to describe a cyclic code as an ideal of  $\mathbb{F}_q[X]/(X^n - 1)$ . A self-dual linear code is a code who is equal to its annihilator (with respect to the scalar product). One reason of the interest in self-dual codes is that they have strong connections with combinatorics.

In 1983, N. J. A. Sloane and J. G. Thompson investigated the construction and the enumeration of self-dual cyclic binary codes with a given length  $n$  ([19]). These codes are determined by a polynomial equation whose solutions can be described thanks to some factorization properties of  $X^n + 1$  in  $\mathbb{F}_2[X]$ . Later this study was generalized to self-dual cyclic codes over finite fields of characteristic 2 ([11, 10]) and to self-dual negacyclic codes over finite fields of odd characteristic ([5], [17]).

For  $\theta$  automorphism of a finite field  $\mathbb{F}_q$ ,  $\theta$ -cyclic codes (also called skew cyclic codes) of length  $n$  were defined in [2]. These codes are such that a right circular shift of each codeword gives another word who belongs to the code after application of  $\theta$  to each of its  $n$  coordinates. If  $\theta$  is the identity,  $\theta$ -cyclic codes are cyclic codes; if  $q$  is the square of a prime number and  $\theta$  is the Frobenius automorphism (who therefore has order 2),  $\theta$ -cyclic codes form a subclass of the class of quasi-cyclic codes of index 2 ([18]). Self-dual quasi-cyclic codes have been also studied in [8], [13], [14].

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  $\mathbb{F}_q$ . Like self-dual cyclic codes, self-dual  $\theta$ -cyclic codes over  $\mathbb{F}_q$  are characterized by an equation, called "self-dual skew equation" and defined in the Ore ring  $\mathbb{F}_q[X; \theta]$ . When  $q$  is the square of a prime number and  $\theta$  is the Frobenius automorphism over  $\mathbb{F}_q$ , properties specific to the ring  $\mathbb{F}_q[X; \theta]$  will enable to extend N. J. A. Sloane and J. G. Thompson original approach to solve the self-dual skew equation.

The text is organized as follows. In Section 2, some definitions and facts about  $\theta$ -cyclic codes,  $\theta$ -negacyclic codes and self-dual codes are recalled. The self-dual skew equation characterizing self-dual  $\theta$ -cyclic or  $\theta$ -negacyclic codes is recalled. Its solutions are least common right multiples of skew polynomials who satisfy intermediate skew equations in  $\mathbb{F}_q[X; \theta]$  ([3]). The main goal of this paper consists in constructing and enumerating the solutions of these intermediate skew equations when  $q$  is the square of a prime number  $p$  and  $\theta$  is the Frobenius automorphism over  $\mathbb{F}_{p^2}$ .

In Section 3, self-dual  $\theta$ -cyclic and  $\theta$ -negacyclic codes whose dimension is a power of  $p$  are considered over  $\mathbb{F}_{p^2}$ . In this case, the self-dual skew equation splits into one single intermediate skew equation. When  $p$  is equal to 2, the complete description of its solutions was obtained in [3] thanks to some factorization properties (recalled in Proposition 3) specific to  $\mathbb{F}_{p^2}[X; \theta]$ . Using the same arguments, one can also describe the solutions of the self-dual skew equation when  $p$  is an odd prime number (Proposition 4). The results are summed up in Table 1.

In Section 4, self-dual  $\theta$ -cyclic and  $\theta$ -negacyclic codes whose dimension is prime to  $p$  are considered over  $\mathbb{F}_{p^2}$  (Proposition 8). A resolution of the intermediate skew equations based on Cauchy interpolations over  $\mathbb{F}_{p^2}$  (Propositions 6 and 7) enables to provide a parametrization of the solutions.

In Section 5, self-dual  $\theta$ -cyclic and  $\theta$ -negacyclic codes of any dimension over  $\mathbb{F}_{p^2}$  are constructed and enumerated (Theorem 1). The steps of the resolutions of the intermediate skew equations are summed up in Tables 4 and 5. Proposition 4 (Section 3) and Proposition 8 (Section 4) can be seen as particular cases of Theorem 1.

The text ends in Section 6 with some concluding remarks and perspectives.

## 2 Generalities on self-dual skew constacyclic codes

For a finite field  $\mathbb{F}_q$  and  $\theta$  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  $\mathbb{F}_q$

$$X \cdot a = \theta(a) X. \quad (1)$$

The ring  $R$  is called a skew polynomial ring or Ore ring (cf. [16]) and its elements are skew polynomials. When  $\theta$  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 and lcm exist in  $R$  and can be computed using the left and right Euclidean algorithms. The center of  $R$  is the commutative polynomial ring  $Z(R) = \mathbb{F}_q^\theta[X^m]$  where  $\mathbb{F}_q^\theta$  is the fixed field of  $\theta$  and  $m$  is the order of  $\theta$ . The **bound**  $B(h)$  of a skew polynomial  $h$  with a nonzero constant term is the monic skew polynomial  $f$  with a nonzero constant term belonging to  $Z(R)$  of minimal degree such that  $h$  divides  $f$  on the right in  $R$  ([9]).

**Definition 1 (definition 1 of [3])** *Consider an element  $a$  of  $\mathbb{F}_q$  and two integers  $n, k$  such that  $0 \leq k \leq n$ . A  $(\theta, a)$ -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  $1, X, \dots, X^{n-1}$  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  $\theta$ -cyclic and if  $a = -1$ , it is  $\theta$ -negacyclic. The skew polynomial  $g$  is called **skew generator polynomial** of  $C$ .*

If  $\theta$  is the identity then  $\theta$ -cyclic and  $\theta$ -negacyclic codes are respectively cyclic and negacyclic codes.

**Example 1** Consider  $p$  a prime number,  $\theta : x \mapsto x^p$  the Frobenius automorphism over  $\mathbb{F}_{p^2}$  and  $\alpha$  in  $\mathbb{F}_{p^2}$ . The remainder in the right division of  $X^2 - 1$  by  $X + \alpha$  in  $\mathbb{F}_{p^2}[X; \theta]$  is equal to  $\alpha^{p+1} - 1$  :

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

Therefore, there are  $p+1$   $\theta$ -cyclic codes of length 2 and dimension 1 over  $\mathbb{F}_{p^2}$ ; their skew generator polynomials are the skew polynomials  $X + \alpha$  where  $\alpha^{p+1} = 1$ .

**Definition 2 ([3], 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 skew polynomial  $h$  is **self-reciprocal** if  $h = h^\natural$ .

**Remark 1** For  $f, g$  in  $R$ ,  $(f \cdot g)^* = \Theta^{\deg(f)}(g^*) \cdot f^*$  (Lemma 4 of [3]). In particular, for  $f, h$  in  $R$  if  $f$  divides  $h$  on the left then  $f^\natural$  divides  $h^\natural$  on the right.

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 **self-dual** if  $C$  is equal to  $C^\perp$ .

According to [3], self-dual  $\theta$ -constacyclic codes are necessarily  $\theta$ -cyclic or  $\theta$ -negacyclic. They can be characterized by a skew polynomial equation who is recalled below.

**Proposition 1 (Corollary 1 of [3])** Consider  $\varepsilon$  in  $\{-1, 1\}$ , two integers  $k, n$  with  $k \leq n$  and  $C$  a  $(\theta, \varepsilon)$ -constacyclic code with length  $n$ , dimension  $k$ . Consider  $g$  the skew generator polynomial of  $C$  and  $h$  the **skew check polynomial** of  $C$  defined by  $g \cdot h = X^n - \varepsilon$ . The Euclidean dual  $C^\perp$  of  $C$  is a  $(\theta, \varepsilon)$ -constacyclic code generated by  $h^\natural$ . The code  $C$  is Euclidean self-dual if, and only if,

$$h^\natural \cdot h = X^{2k} - \varepsilon. \quad (2)$$

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

When  $k$  is fixed, a first approach to solve the self-dual skew equation consists in constructing the polynomial system satisfied by the unknown coefficients of a solution :

**Example 2** Consider  $p$  a prime number and  $\theta : x \mapsto x^p$  the Frobenius automorphism over  $\mathbb{F}_{p^2}$ . The self-dual  $\theta$ -cyclic codes of dimension 1 over  $\mathbb{F}_{p^2}$  are the  $\theta$ -cyclic codes whose skew check polynomials  $h$  satisfy the self-dual skew equation

$$h^\natural \cdot h = X^2 - 1.$$

The monic skew solutions of the self-dual skew equation are the monic skew polynomials  $h = X + \alpha$  where  $\alpha$  is in  $\mathbb{F}_{p^2}$  and

$$\left( X + \frac{1}{\theta(\alpha)} \right) \cdot (X + \alpha) = X^2 - 1.$$

Developing the left hand side of this relation thanks to the commutation law (1) and equating the terms of both sides, one gets the conditions  $\alpha^2 + 1 = 0$  and  $\alpha^{p-1} = -1$ . If  $p = 2$  then  $\alpha = 1$  and if  $p$  is an odd prime number then  $\alpha^2 = -1$  and  $(-1)^{\frac{p-1}{2}} = -1$ . Therefore if  $p = 2$  there is one self-dual  $\theta$ -cyclic code of dimension 1 over  $\mathbb{F}_4$ ; if  $p \equiv 3 \pmod{4}$  there are two self-dual  $\theta$ -cyclic codes of dimension 1 over  $\mathbb{F}_{p^2}$ ; if  $p \equiv 1 \pmod{4}$  then there is no self-dual  $\theta$ -cyclic code of dimension 1 over  $\mathbb{F}_{p^2}$ .

When  $k$  is not fixed, a second approach is based on the factorization properties of the monic solutions of the self-dual skew equation. The starting point of the study is inspired from Sloane and Thompson construction of self-dual binary cyclic codes ([19]) who is extended to finite fields with characteristic 2 in [10]. Let us recall their strategy (and therefore assume that  $\mathbb{F}_q$  has characteristic 2 and that  $\theta$  is the identity). Consider two integers  $s$  and  $t$  such that  $k = 2^s \times t$  with  $t$  odd. The polynomial  $X^n + 1 = X^{2k} + 1$  is factorized in  $\mathbb{F}_q[X]$  as the product of  $r$  polynomials  $f_i(X)^{2^{s+1}}$  where  $f_i(X)$  is a self-reciprocal polynomial which is either irreducible or product of two distinct irreducible polynomials  $g_i(X)$  and  $g_i^{\natural}(X)$  in  $\mathbb{F}_q[X]$ . Consider  $h$  in  $\mathbb{F}_q[X]$  such that  $h^{\natural}h = X^{2k} + 1$ . Necessarily,  $h$  is the product of polynomials  $f_i(X)^{\alpha_i}$ ,  $g_i(X)^{\beta_i}$  and  $g_i^{\natural}(X)^{\gamma_i}$ , where  $\alpha_i, \beta_i$  and  $\gamma_i$  are integers of  $\{0, \dots, 2^{s+1}\}$ . The relation  $h^{\natural}h = X^{2k} + 1$  is satisfied if and only if  $\alpha_i = 2^s$  and  $\beta_i + \gamma_i = 2^{s+1}$ , therefore there are  $(2^{s+1} + 1)^m$  self-dual cyclic codes of dimension  $k$  where  $m$  is the number of polynomials  $f_i(X) = g_i(X)g_i^{\natural}(X)$  dividing  $X^n + 1$  in  $\mathbb{F}_q[X]$ . Lastly one can notice that the polynomials  $h$  who satisfy the relation  $h^{\natural}h = X^{2k} + 1$  are least common multiples of polynomials  $h_i$  who are defined by the intermediate equations  $h_i^{\natural}h_i = f_i(X)^{2^{s+1}}$  :

$$h^{\natural}h = X^{2k} + 1 \Leftrightarrow h = \text{lcm}(h_1, \dots, h_r), h_i^{\natural}h_i = f_i(X)^{2^{s+1}}.$$

In [3], this lcm decomposition was generalized to a lcrm decomposition over  $R = \mathbb{F}_q[X; \theta]$  in the particular case when  $q$  is the square of a prime number and  $\theta$  is the Frobenius automorphism (Proposition 28 of [3]). This decomposition enables to derive a first formula for the number of  $(\theta, \varepsilon)$ -constacyclic codes of dimension  $k$  (Proposition 2 below). First one introduces some notations that will be useful later :

**Notation 1** For  $F = F(X^2)$  in  $\mathbb{F}_p[X^2]$ ,  $k$  in  $\mathbb{N}^*$  and  $\varepsilon$  in  $\{-1, 1\}$ ,

$$\mathcal{H}_F := \{h \in R \mid h \text{ is monic and } h^{\natural} \cdot h = F(X^2)\}$$

$$\overline{\mathcal{H}}_F := \{h \in \mathcal{H}_F \mid \text{no non constant divisor of } F(X^2) \text{ in } \mathbb{F}_p[X^2] \text{ divides } h \text{ in } R\}$$

$$\mathcal{D}_F := \{f = f(X^2) \in \mathbb{F}_p[X^2] \mid f \text{ is monic and } f \text{ divides } F(X^2)\}$$

$$\mathcal{F} := \{f = f(X^2) \in \mathbb{F}_p[X^2] \mid f \text{ is irreducible in } \mathbb{F}_p[X^2] \text{ and } \deg_{X^2}(f) > 1\}$$

$$\mathcal{G} := \{f = f(X^2) \in \mathbb{F}_p[X^2] \mid f = gg^{\natural} \text{ with } g \neq g^{\natural} \text{ irreducible in } \mathbb{F}_p[X^2]\}$$

$$\mathcal{F}_{k,\varepsilon} := \mathcal{D}_{X^{2k-\varepsilon}} \cap \mathcal{F}$$

$$\mathcal{G}_{k,\varepsilon} := \mathcal{D}_{X^{2k-\varepsilon}} \cap \mathcal{G}$$

Following this notation, the monic solutions of the self-dual skew equation are the elements of  $\mathcal{H}_{X^{2k-\varepsilon}}$ .

**Proposition 2** Consider  $p$  a prime number,  $\theta$  the Frobenius automorphism over  $\mathbb{F}_{p^2}$ ,  $R = \mathbb{F}_{p^2}[X; \theta]$ ,  $k$  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  $(\theta, \varepsilon)$ -constacyclic codes of dimension  $k$  over  $\mathbb{F}_{p^2}$  is

$$\#\mathcal{H}_{X^{2k}-\varepsilon} = N_\varepsilon \times \prod_{f \in \mathcal{F}_{k,\varepsilon}} \#\mathcal{H}_{f^{p^s}} \times \prod_{f \in \mathcal{G}_{k,\varepsilon}} \#\mathcal{H}_{f^{p^s}}$$

where

$$N_1 = \begin{cases} \#\mathcal{H}_{(X^2+1)^{p^s}} & \text{if } p = 2 \\ \#\mathcal{H}_{(X^2-1)^{p^s}} & \text{if } k \equiv 1 \pmod{2} \text{ and } p \text{ odd} \\ \#\mathcal{H}_{(X^2-1)^{p^s}} \times \#\mathcal{H}_{(X^2+1)^{p^s}} & \text{if } k \equiv 0 \pmod{2} \text{ and } p \text{ odd} \end{cases}$$

and

$$N_{-1} = \begin{cases} \#\mathcal{H}_{(X^2+1)^{p^s}} & \text{if } k \equiv 1 \pmod{2} \text{ and } p \text{ odd} \\ 1 & \text{if } k \equiv 0 \pmod{2} \text{ and } p \text{ odd.} \end{cases}$$

**Proof.** Consider the factorization of  $X^{2t} - \varepsilon$  over  $\mathbb{F}_p[X^2]$  into the product of distinct irreducible polynomials of  $\mathbb{F}_p[X^2]$  and split this product into two sub-products, the product of self-reciprocal irreducible factors and the product of non self-reciprocal irreducible factors. In this second product, factors appear by pairs  $(g, g^\natural \neq g)$  therefore  $X^{2k} - \varepsilon = (X^{2t} - \varepsilon)^{p^s} = \prod_{i=1}^r f_i^{p^s}$  where  $f_i = f_i(X^2)$  is self-reciprocal, either irreducible in  $\mathbb{F}_p[X^2]$  or product of two distinct irreducible polynomials  $g_i(X^2)$  and  $g_i^\natural(X^2)$  of  $\mathbb{F}_p[X^2]$ . Following [3], one has

1.  $\mathcal{H}_{X^{2k}-\varepsilon} = \{\text{lcm}(h_1, \dots, h_r) \mid h_i \in \mathcal{H}_{f_i^{p^s}}\}$  ([3], Proposition 28);
2. If  $h$  belongs to  $\mathcal{H}_{X^{2k}-\varepsilon}$ , then  $h = \text{lcm}(h_1, \dots, h_r)$  where  $h_i^\natural = \text{gcd}(f_i^{p^s}, h^\natural)$  and  $h_i \in \mathcal{H}_{f_i^{p^s}}$  ([3], Proposition 28, point (2)).

Therefore, the following application  $\phi$  is well defined and is injective :

$$\phi : \begin{cases} \mathcal{H}_{X^{2k}-\varepsilon} & \rightarrow \mathcal{H}_{f_1^{p^s}} \times \dots \times \mathcal{H}_{f_r^{p^s}} \\ h & \mapsto (h_1, \dots, h_r), \quad h_i^\natural = \text{gcd}(f_i^{p^s}, h^\natural). \end{cases}$$

Let us prove that  $\phi$  is surjective. Consider  $(h_1, \dots, h_r)$  in  $\mathcal{H}_{f_1^{p^s}} \times \dots \times \mathcal{H}_{f_r^{p^s}}$  and  $h = \text{lcm}(h_1, \dots, h_r)$ . According to point 1., the skew polynomial  $h$  belongs to  $\mathcal{H}_{X^{2k}-\varepsilon}$ . It remains to prove that for all  $i$  in  $\{1, \dots, r\}$ ,  $h_i^\natural = \text{gcd}(f_i^{p^s}, h^\natural)$ . According to point 2.,  $h = \text{lcm}(\tilde{h}_1, \dots, \tilde{h}_r)$  where  $\tilde{h}_i^\natural = \text{gcd}(f_i^{p^s}, h^\natural)$  and  $\tilde{h}_i \in \mathcal{H}_{f_i^{p^s}}$ . Consider  $i$  in  $\{1, \dots, r\}$ , one has  $h_i^\natural \cdot h_i = f_i^{p^s}$  and  $f_i$  is central, therefore  $h_i^\natural$  divides  $f_i^{p^s}$  on the right. Furthermore  $h = \text{lcm}(h_1, \dots, h_r)$  therefore  $h_i$  divides  $h$  on the left and  $h_i^\natural$  divides  $h^\natural$  on the right (see Remark 1). As  $\tilde{h}_i^\natural$  is the greatest common right divisor of  $f_i^{p^s}$  and  $h^\natural$ ,  $h_i^\natural$  divides  $\tilde{h}_i^\natural$  on the right. Furthermore  $h_i^\natural \cdot h_i = \tilde{h}_i^\natural \cdot \tilde{h}_i = f_i^{p^s}$  so  $h_i$  and  $\tilde{h}_i$  have the same degree and  $h_i^\natural = \tilde{h}_i^\natural = \text{gcd}(f_i^{p^s}, h^\natural)$ . To conclude  $\phi$  is bijective and

$$\#\mathcal{H}_{X^{2k}-\varepsilon} = \prod_{i=1}^r \#\mathcal{H}_{f_i^{p^s}} = N_\varepsilon \times \prod_{f \in \mathcal{F}_{k,\varepsilon}} \#\mathcal{H}_{f^{p^s}} \times \prod_{f \in \mathcal{G}_{k,\varepsilon}} \#\mathcal{H}_{f^{p^s}}$$

where  $N_\varepsilon = \prod_{\deg(f_i)=1} \#\mathcal{H}_{f_i^{p^s}}$ .

Let us determine  $N_\varepsilon$  in the three following cases :  $p = 2, \varepsilon = 1$ ;  $p$  odd prime,  $\varepsilon = 1$  and  $p$  odd prime,  $\varepsilon = -1$ .

For  $p = 2$ , the self-reciprocal polynomial of degree 1 in  $X^2$  dividing  $X^{2k} - 1$  is  $X^2 + 1$  therefore  $N_1 = \#\mathcal{H}_{(X^2+1)^{p^s}}$ .

For  $p$  odd prime, the self-reciprocal polynomials of degree 1 in  $X^2$  dividing  $X^{2k} - 1$  are  $X^2 - 1$  if  $k$  is odd;  $X^2 - 1$  and  $X^2 + 1$  if  $k$  is even therefore,

$$N_1 = \begin{cases} \#\mathcal{H}_{(X^2-1)^{p^s}} & \text{if } k \equiv 1 \pmod{2} \\ \#\mathcal{H}_{(X^2-1)^{p^s}} \times \#\mathcal{H}_{(X^2+1)^{p^s}} & \text{if } k \equiv 0 \pmod{2}. \end{cases}$$

For  $p$  odd prime and  $k$  even number,  $X^{2k} + 1$  has no self-reciprocal factor of degree 1 in  $X^2$ . If  $k$  is odd,  $X^2 + 1$  is the only self-reciprocal polynomial of degree 1 in  $X^2$  dividing  $X^{2k} + 1$ . Therefore,

$$N_{-1} = \begin{cases} \#\mathcal{H}_{(X^2+1)^{p^s}} & \text{if } k \equiv 1 \pmod{2} \\ 1 & \text{if } k \equiv 0 \pmod{2}. \end{cases}$$

■

The rest of the paper will be devoted to the enumeration of the elements of the set  $\mathcal{H}_{X^{2k}-\varepsilon}$  when  $k$  is a power of  $p$  (Section 3),  $k$  is coprime with  $p$  (Section 4) and  $k$  is any integer (Section 5). Following Proposition 2, the main task will consist in constructing  $\mathcal{H}_{f^{p^s}}$  for  $f = X^2 \pm 1$ ,  $f$  in  $\mathcal{F}$  and  $f$  in  $\mathcal{G}$ . The main difficulty comes from the non unicity of the factorization of skew polynomials in the Ore ring  $R$ .

In Section 3, one assumes that  $k$  is a power of  $p$ , therefore  $X^{2k} - \varepsilon$  factorizes over  $\mathbb{F}_p[X^2]$  as  $X^{2k} - \varepsilon = (X^2 - \varepsilon)^{p^s}$  and the self-dual skew equation splits into one single intermediate skew equation. For  $s > 0$ , it is solved by using a partition and factorization properties specific to  $\mathbb{F}_{p^2}[X; \theta]$ .

### 3 Self-dual $\theta$ -cyclic and $\theta$ -negacyclic codes with dimension $p^s$ over $\mathbb{F}_{p^2}$ .

The aim of this section is to construct and to enumerate self-dual  $\theta$ -cyclic and  $\theta$ -negacyclic codes over  $\mathbb{F}_{p^2}$  whose dimension is  $p^s$  where  $\theta$  is the Frobenius automorphism. Recall that over  $\mathbb{F}_4$ , there is one single self-dual cyclic code of dimension  $2^s$ . When  $p$  is an odd prime number there is no self-dual cyclic code over  $\mathbb{F}_{p^2}$  and there are  $p^s + 1$  self-dual negacyclic codes of dimension  $p^s$  (Corollary 3.3 of [5]). Lastly, there are only three self-dual  $\theta$ -cyclic codes of dimension  $2^s > 1$  over  $\mathbb{F}_4$  (Corollary 26 of [3]). In what follows one proves that the number of self-dual  $\theta$ -cyclic and  $\theta$ -negacyclic codes of dimension  $p^s$  over  $\mathbb{F}_{p^2}$  is exponential in the dimension  $p^s$  when  $p$  is an odd prime number (Proposition 4 and Table 1).

In order to construct the set  $\mathcal{H}_{X^{2k}-\varepsilon} = \mathcal{H}_{(X^2-\varepsilon)^{p^s}}$ , 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  $X^2 - \varepsilon$  (see also Proposition 16 of [3]).

**Proposition 3** *Consider  $p$  a prime number,  $\theta$  the Frobenius automorphism over  $\mathbb{F}_{p^2}$ ,  $R = \mathbb{F}_{p^2}[X; \theta]$ ,  $m$  a nonnegative integer,  $f(X^2)$  in  $\mathbb{F}_p[X^2]$  irreducible and  $h = h_1 \cdots h_m$  in  $R$  where  $h_i$  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  $\{1, \dots, m-1\}$  such that  $h_i \cdot h_{i+1} = f(X^2)$ .

**Proof.** Consider  $f(X^2) \in \mathbb{F}_p[X^2]$  irreducible with degree  $d > 1$  such that  $f^\natural(X^2) = f(X^2)$ . According to [15], page 6 (or Lemma 1.4.11 of [4] with  $e = 2$ ), as  $f(X^2)$  is irreducible in the center of  $R$ , the skew polynomial  $f(X^2)$  has  $((p^2)^d - 1)/(p^d - 1) = p^d + 1$  irreducible monic right factors of degree  $d$  in  $R$ , in particular it is reducible in  $R$ . According to Proposition 16 of [3] the points (i), (ii) and (iii) are therefore equivalent. ■

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

(i) The above factorization of  $h$  is not unique.

(ii)  $X^2 - \varepsilon$  divides  $h$ .

(iii) There exists  $i$  in  $\{1, \dots, m-1\}$  such that  $(X + \lambda_i) \cdot (X + \lambda_{i+1}) = X^2 - \varepsilon$  i.e.  $\lambda_i \lambda_{i+1} = -\varepsilon$ .

**Proof.** This is a consequence of Proposition 3 with  $f(X^2) = X^2 - \varepsilon$ . It suffices to notice that  $X + \lambda_i$  divides  $X^2 - \varepsilon$  if and only if  $\lambda_i^{p+1} = \varepsilon$ . In this case  $(X + \lambda_i) \cdot (X + \lambda_{i+1}) = X^2 + (\lambda_i + \frac{\varepsilon}{\lambda_{i+1}})X + \lambda_i \lambda_{i+1}$  and  $(X + \lambda_i) \cdot (X + \lambda_{i+1}) = X^2 - \varepsilon \Leftrightarrow \lambda_i \lambda_{i+1} = -\varepsilon$ . ■

The elements of  $\mathcal{H}_{(X^2 - \varepsilon)^{p^s}}$  who have a unique factorization in  $R$  into the product of monic irreducible skew polynomials are therefore not divisible by  $X^2 - \varepsilon$ . In what follows one constructs for  $m$  in  $\mathbb{N}$  the set of elements of  $\mathcal{H}_{(X^2 - \varepsilon)^m}$  who are not divisible by  $X^2 - \varepsilon$ . Recall that one denotes  $\overline{\mathcal{H}}_{(X^2 - \varepsilon)^m}$  this set of elements (see notations in Section 2) :

$$\overline{\mathcal{H}}_{(X^2 - \varepsilon)^m} := \{h \in \mathcal{H}_{(X^2 - \varepsilon)^m} \mid X^2 - \varepsilon \text{ does not divide } h\}.$$

**Lemma 1** Consider  $p$  a prime number,  $\theta$  the Frobenius automorphism,  $R = \mathbb{F}_{p^2}[X; \theta]$ ,  $m$  a nonnegative integer and  $\varepsilon$  in  $\{-1, 1\}$ . Assume that  $p$  is odd and  $m$  is odd, then the number of elements of  $\overline{\mathcal{H}}_{(X^2 - \varepsilon)^m}$  is

$$\#\overline{\mathcal{H}}_{(X^2 - \varepsilon)^m} = \begin{cases} 0 & \text{if } \varepsilon = 1, p \equiv 1 \pmod{4} \text{ or } \varepsilon = -1, p \equiv 3 \pmod{4} \\ 2p^{\frac{m-1}{2}} & \text{if } \varepsilon = 1, p \equiv 3 \pmod{4} \text{ or } \varepsilon = -1, p \equiv 1 \pmod{4}. \end{cases}$$

Assume that  $p$  is equal to 2, then the number of elements of  $\overline{\mathcal{H}}_{(X^2 + 1)^m}$  is

$$\#\overline{\mathcal{H}}_{(X^2 + 1)^m} = \begin{cases} 0 & \text{if } m > 2 \\ 2 & \text{if } m = 2 \\ 1 & \text{if } m = 1. \end{cases}$$

**Proof.**



- One first proves that the elements  $h$  of  $\overline{\mathcal{H}}_{(X^2-\varepsilon)^m}$  are

$$h = (X + \lambda_1) \cdots (X + \lambda_m)$$

where

$$\begin{cases} \forall i \in \{1, \dots, m\}, \lambda_i^{p+1} = \varepsilon \\ \forall i \in \{1, \dots, m-1\}, \lambda_i \lambda_{i+1} \neq -\varepsilon \\ \lambda_1^2 = -1 \\ \forall j \in \{1, \dots, \lfloor \frac{m-1}{2} \rfloor\}, (\lambda_{2j} \lambda_{2j+1})^2 = 1. \end{cases} \quad (3)$$

Namely, consider  $h$  in  $\overline{\mathcal{H}}_{(X^2-\varepsilon)^m}$ . As  $h$  divides  $(X^2 - \varepsilon)^m$  and as  $X^2 - \varepsilon$  is irreducible with degree 1 in  $\mathbb{F}_p[X^2]$ ,  $h$  is a (non necessarily commutative) product of linear monic skew polynomials dividing  $X^2 - \varepsilon$  (Lemma 13 (2) of [3] or [15] page 6). Furthermore, the degree of  $h$  is equal to  $m$  (because  $\deg(h^\natural \cdot h) = 2m$ ) therefore one has :

$$h = (X + \lambda_1) \cdots (X + \lambda_m) \text{ where } \lambda_i \in \mathbb{F}_{p^2}, \lambda_i^{p+1} = \varepsilon.$$

In particular, the first relation of (3) is satisfied. As  $X^2 - \varepsilon$  does not divide  $h$ , according to Corollary 1 :

$$\forall i \in \{1, \dots, m-1\}, (X + \lambda_i) \cdot (X + \lambda_{i+1}) \neq X^2 - \varepsilon \quad (4)$$

therefore

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

which is the second relation of (3). 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 :

$$\tilde{\lambda}_i := \begin{cases} 1/\lambda_i \times \varepsilon \times (\lambda_1 \cdots \lambda_i)^2 & \text{if } i \equiv 1 \pmod{2} \\ 1/\lambda_i \times \frac{\varepsilon}{(\lambda_1 \cdots \lambda_{i-1})^2} & \text{if } i \equiv 0 \pmod{2}. \end{cases} \quad (5)$$

Furthermore,  $X^2 - \varepsilon$  does not divide  $h^\natural$ , otherwise  $X^2 - \varepsilon$  would divide  $h$ , therefore

$$\forall i \in \{1, \dots, m-1\}, (X + \tilde{\lambda}_{i+1}) \cdot (X + \tilde{\lambda}_i) \neq X^2 - \varepsilon. \quad (6)$$

The relation  $h^\natural \cdot h = (X^2 - \varepsilon)^m$  can be written

$$(X + \tilde{\lambda}_m) \cdots (X + \tilde{\lambda}_1) \cdot (X + \lambda_1) \cdots (X + \lambda_m) = (X^2 - \varepsilon)^m. \quad (7)$$

As  $X^2 - \varepsilon$  is central, the factorization of the skew polynomial  $(X^2 - \varepsilon)^m$  into the product of monic skew polynomials dividing  $X^2 - \varepsilon$  is not unique, therefore, according

to Corollary 1,  $X^2 - \varepsilon$  is necessarily the product of two consecutive monic linear factors of the left hand side of (7). According to (4) and (6), the only possibility is

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

As  $X^2 - \varepsilon$  is central, the relation (7) can be simplified and one gets

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

Using the same argument as before, one gets

$$\begin{aligned} (X + \tilde{\lambda}_2) \cdot (X + \lambda_2) &= X^2 - \varepsilon \\ &\vdots \\ (X + \tilde{\lambda}_m) \cdot (X + \lambda_m) &= X^2 - \varepsilon. \end{aligned}$$

From the equalities above, one deduces that

$$\forall i \in \{1, \dots, m\}, \lambda_i \tilde{\lambda}_i = -\varepsilon$$

and using the definition of  $\tilde{\lambda}_i$  given in (5), one gets  $\lambda_1^2 = -1$  (third relation of (3)) and for  $i$  odd,  $(\lambda_i \lambda_{i+1})^2 = 1$  (fourth relation of (3)).

Conversely, consider  $h = (X + \lambda_1) \cdots (X + \lambda_m)$  where  $\lambda_1, \dots, \lambda_m$  are defined by (3). According to the first relation of (3), the monic skew polynomials  $X + \lambda_i$  divide  $X^2 - \varepsilon$ . According to the second relation of (3) and to Corollary 1,  $X^2 - \varepsilon$  does not divide  $h$ . Like previously 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 (5). Furthermore, according to the third and fourth relations of (3), if  $i$  is odd,  $(\lambda_1 \cdots \lambda_i)^2 = -1$ , so for all  $i$  in  $\{1, \dots, m\}$ ,  $\lambda_i \tilde{\lambda}_i = -\varepsilon$  and  $X^2 - \varepsilon = (X + \tilde{\lambda}_i) \cdot (X + \lambda_i)$ . The product  $h^\natural \cdot h$  can be simplified as follows :

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

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

- The relations (3) enable to count the number of elements of  $\overline{\mathcal{H}}_{(X^2 - \varepsilon)^m}$ . Namely according to Corollary 1, the elements of  $\overline{\mathcal{H}}_{(X^2 - \varepsilon)^m}$  have a unique factorization into the product of monic skew linear polynomials dividing  $X^2 - \varepsilon$ . Therefore the number of elements of the set  $\overline{\mathcal{H}}_{(X^2 - \varepsilon)^m}$  is the number of  $m$ -tuples  $(\lambda_1, \dots, \lambda_m)$  of  $(\mathbb{F}_{p^2})^m$  satisfying the conditions (3).

Assume that  $p = 2$  and that  $m$  is an integer greater than 2. Then the conditions  $\lambda_2 \lambda_3 \neq -1$  and  $(\lambda_2 \lambda_3)^2 = 1$  are not compatible, therefore the set  $\overline{\mathcal{H}}_{(X^2 - 1)^m}$  is empty. If  $m = 1$ , it is reduced to  $\{X + 1\}$  (see Example 1). If  $m = 2$ , the set  $\overline{\mathcal{H}}_{(X^2 - 1)^m}$  is equal

to  $\{(X + \lambda_1) \cdot (X + \lambda_2) \mid \lambda_1 = 1, \lambda_2 \neq 1\} = \{(X + 1) \cdot (X + a), (X + 1) \cdot (X + a^2)\}$  where  $a^2 + a + 1 = 0$ .

Assume that  $p$  and  $m$  are odd, then the conditions (3) can be simplified as follows :

$$\begin{cases} \lambda_1^2 = -1 \\ \lambda_2 \neq \varepsilon \lambda_1 \\ \forall i \in \{1, \dots, m\}, \lambda_i^{p+1} = \varepsilon \\ \forall j \in \{1, \dots, (m-1)/2\}, \lambda_{2j+1} = \varepsilon / \lambda_{2j} \\ \forall j \in \{1, \dots, (m-3)/2\}, \lambda_{2j+2} \neq -\lambda_{2j} \end{cases}$$

First, the conditions  $\lambda_1^2 = -1$  and  $\lambda_1^{p+1} = \varepsilon$  imply  $(-1)^{(p+1)/2} = \varepsilon$  so  $\overline{\mathcal{H}}_{(X^2 - \varepsilon)^m}$  is empty if  $p \equiv 3 \pmod{4}$  and  $\varepsilon = -1$  or  $p \equiv 1 \pmod{4}$  and  $\varepsilon = 1$ .

If  $p \equiv 3 \pmod{4}$  and  $\varepsilon = 1$  or  $p \equiv 1 \pmod{4}$  and  $\varepsilon = -1$ , then there are two possibilities for  $\lambda_1$ ,  $p$  possibilities for  $\lambda_2$ , one possibility for  $\lambda_3$ ,  $p$  possibilities for  $\lambda_4$ , one for  $\lambda_5$ , and so on, therefore  $\overline{\mathcal{H}}_{(X^2 - \varepsilon)^m}$  has  $2p^{\frac{m-1}{2}}$  elements.

■

**Remark 2** If  $m$  is odd, one can simplify the relations (3) by taking  $\alpha_0 = \lambda_1$ ,  $\alpha_1 = \lambda_2$  and for  $i$  in  $\{2, \dots, (m-1)/2\}$ ,  $\alpha_i = \lambda_{2i}$ . Therefore one gets :

$$\begin{aligned} \overline{\mathcal{H}}_{(X^2 - \varepsilon)^m} &= \{(X + \alpha_0) \cdot (X^2 + 2\alpha_1 X + \varepsilon) \cdots (X^2 + 2\alpha_{(m-1)/2} X + \varepsilon) \mid \\ &\alpha_0^2 = -1, \alpha_1 \neq \varepsilon \alpha_0, \\ &\forall i \in \{0, \dots, (m-1)/2\}, \alpha_i^{p+1} = \varepsilon, \\ &\forall i \in \{2, \dots, (m-1)/2\}, \alpha_i \neq -\alpha_{i-1}\}. \end{aligned}$$

To describe the set  $\mathcal{H}_{(X^2 - \varepsilon)^{p^s}}$  one uses the following partition :

**Lemma 2** Consider  $p$  a prime number,  $\theta$  the Frobenius automorphism over  $\mathbb{F}_{p^2}$ ,  $R = \mathbb{F}_{p^2}[X; \theta]$ ,  $s$  in  $\mathbb{N}$  and  $f = f(X^2) \in \{X^2 \pm 1\} \cup \mathcal{F}$ . One has the following partition :

$$\mathcal{H}_{f^{p^s}} = \bigsqcup_{i=0}^{\lfloor \frac{p^s}{2} \rfloor} f^i \cdot \overline{\mathcal{H}}_{f^{p^s-2i}}. \quad (8)$$

**Proof.** Consider  $M = \lfloor \frac{p^s}{2} \rfloor$ ,  $h = h(X)$  in  $\mathcal{H}_{f^{p^s}}$  and  $i$  the biggest integer in  $\{0, \dots, M\}$  such that  $f^i$  divides  $h$ . Consider  $H = H(X)$  in  $R$  such that  $h = f^i \cdot H$  and  $f$  does not divide  $H$ . As  $f^i$  is central,  $h^\natural = f^i \cdot H^\natural$  therefore  $H^\natural \cdot H = f^{p^s-2i}$  and  $H$  belongs to  $\overline{\mathcal{H}}_{f^{p^s-2i}}$ . Conversely, if  $H$  in  $\overline{\mathcal{H}}_{f^{p^s-2i}}$ , then  $f^i \cdot H$  belongs to  $\mathcal{H}_{f^{p^s}}$ .

Furthermore consider  $i > i'$ ,  $H$  in  $\overline{\mathcal{H}}_{f^{p^s-2i}}$  and  $H'$  in  $\overline{\mathcal{H}}_{f^{p^s-2i'}}$  such that  $f^i \cdot H = f^{i'} \cdot H'$  then  $f^{i-i'}$  divides  $H'$ , which is impossible as  $f$  does not divide  $H'$ . Therefore, for  $i \neq i'$ , the sets  $f^i \cdot \overline{\mathcal{H}}_{f^{p^s-2i}}$  and  $f^{i'} \cdot \overline{\mathcal{H}}_{f^{p^s-2i'}}$  are disjoint.

■

**Remark 3** If  $p = 2$  and  $f(X^2) = X^2 + 1$ , according to Lemma 2, one gets the following partition :

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

According to Lemma 1, the sets  $\overline{\mathcal{H}}_{(X^2+1)^{2^s-2i}}$  are empty when  $2^s - 2i > 2$  and  $\overline{\mathcal{H}}_{(X^2+1)^2} = \{(X+1) \cdot (X+a), (X+1) \cdot (X+a^2)\}$  where  $a^2 + a + 1 = 0$ . Therefore :

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

One gets that for  $s > 0$  there are only three self-dual  $\theta$ -cyclic codes of dimension  $2^s$  over  $\mathbb{F}_4$  (see also Corollary 26 of [3]).

Proposition 4 below gives a formula for the number of self-dual  $\theta$ -cyclic and  $\theta$ -negacyclic codes whose dimension is a power of  $p$  when  $p$  is an odd prime number. The results are also summed up in Table 1.

**Proposition 4** Consider  $p$  an odd prime number,  $s$  an integer,  $\varepsilon$  in  $\{-1, 1\}$  and  $\theta$  the Frobenius automorphism over  $\mathbb{F}_{p^2}$ . The number of self-dual  $(\theta, \varepsilon)$ -constacyclic codes of dimension  $p^s$  over  $\mathbb{F}_{p^2}$  is

$$\begin{cases} 0 & \text{if } \varepsilon = 1, p \equiv 1 \pmod{4} \text{ or } \varepsilon = -1, p \equiv 3 \pmod{4} \\ 2 \frac{p^{(p^s+1)/2} - 1}{p-1} & \text{if } \varepsilon = 1, p \equiv 3 \pmod{4} \text{ or } \varepsilon = -1, p \equiv 1 \pmod{4}. \end{cases}$$

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

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

where  $M = \frac{p^s-1}{2}$ . According to Lemma 1, each set  $\overline{\mathcal{H}}_{(X^2-\varepsilon)^{p^s-2i}}$  is empty if  $\varepsilon \neq (-1)^{\frac{p+1}{2}}$  and has  $2p^{M-i}$  elements if  $\varepsilon = (-1)^{\frac{p+1}{2}}$ . Therefore, if  $\varepsilon \neq (-1)^{\frac{p+1}{2}}$ ,  $\mathcal{H}_{X^{2p^s-\varepsilon}}$  is empty and otherwise it has  $\sum_{i=0}^M 2p^{M-i} = 2 \frac{p^{M+1}-1}{p-1} = 2 \frac{p^{(p^s+1)/2}-1}{p-1}$  elements. ■

**Example 3** According to Corollary 3.3 of [5], there are 4 self-dual negacyclic codes of dimension 3 over  $\mathbb{F}_9$ . The corresponding skew check polynomials are the polynomials  $(X-\gamma)^i(X+\gamma)^{3-i} \in \mathbb{F}_9[X]$  where  $i$  is in  $\{0, 1, 2, 3\}$  and  $\gamma^2 = -1$ .

According to Proposition 4, for  $\theta : x \mapsto x^3$  Frobenius automorphism over  $\mathbb{F}_9$ , there are  $2 \times (3^{(3+1)/2} - 1)/(3-1) = 8$  self-dual  $\theta$ -cyclic codes of dimension 3 over  $\mathbb{F}_9$ . Their skew check polynomials are the elements of  $\mathcal{H}_{X^6-1}$  and according to Lemma 2,  $\mathcal{H}_{X^6-1} = \overline{\mathcal{H}}_{(X^2-1)^3} \sqcup (X^2-1) \cdot \overline{\mathcal{H}}_{(X^2-1)}$ . The sets  $\overline{\mathcal{H}}_{(X^2-1)}$  (with cardinal 2) and  $\overline{\mathcal{H}}_{(X^2-1)^3}$  (with cardinal 6) are constructed with Lemma 1 and Remark 2 :

$$\overline{\mathcal{H}}_{X^2-1} = \{X + \alpha_0 \mid \alpha_0^2 = -1, \alpha_0^4 = 1\} = \{X + \gamma, X - \gamma\}$$

| $p$                   | negacyclic | $\theta$ -cyclic                | $\theta$ -negacyclic           |
|-----------------------|------------|---------------------------------|--------------------------------|
| $p \equiv 3 \pmod{4}$ | $p^s + 1$  | $2 \frac{p^{(p^s+1)/2-1}}{p-1}$ | 0                              |
| $p \equiv 1 \pmod{4}$ | $p^s + 1$  | 0                               | $2 \frac{p^{(p^s+1)2-1}}{p-1}$ |

Table 1: Numbers of self-dual negacyclic (Corollary 3.3 of [5]),  $\theta$ -cyclic (Proposition 4) and  $\theta$ -negacyclic (Proposition 4) codes over  $\mathbb{F}_{p^2}$  of dimension  $p^s$  with  $p$  odd prime number and  $\theta : x \mapsto x^p$ .

and  $\overline{\mathcal{H}}_{(X^2-1)^3} = \{(X + \alpha_0) \cdot (X^2 + 2\alpha_1 X + 1) \mid \alpha_0 = \pm\gamma, \alpha_1 \neq \alpha_0, \alpha_1 \in \{\pm\gamma, \pm 1\}\}$ . The  $2 \times 3 = 6$  elements of  $\overline{\mathcal{H}}_{(X^2-1)^3}$  are listed below :

$$\left\{ \begin{array}{l} (X + \gamma) \cdot (X^2 + 2X + 1) = X^3 + (\gamma - 1)X^2 + (1 - \gamma)X + \gamma \\ (X + \gamma) \cdot (X^2 + X + 1) = X^3 + (\gamma + 1)X^2 + (\gamma + 1)X + \gamma \\ (X + \gamma) \cdot (X^2 - 2\gamma X + 1) = X^3 + \gamma \\ (X - \gamma) \cdot (X^2 + 2X + 1) = X^3 + (-\gamma - 1)X^2 + (1 + \gamma)X - \gamma \\ (X - \gamma) \cdot (X^2 + X + 1) = X^3 + (-\gamma + 1)X^2 + (-\gamma + 1)X - \gamma \\ (X - \gamma) \cdot (X^2 + 2\gamma X + 1) = X^3 - \gamma. \end{array} \right.$$

Proposition 4 enables also to simplify Proposition 2 as follows. It will be useful in the two next sections.

**Proposition 5** Consider  $p$  a prime number,  $\theta$  the Frobenius automorphism over  $\mathbb{F}_{p^2}$ ,  $R = \mathbb{F}_{p^2}[X; \theta]$ ,  $k$  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  $(\theta, \varepsilon)$ -constacyclic codes over  $\mathbb{F}_{p^2}$  with dimension  $k$  is

$$\#\mathcal{H}_{X^{2k-\varepsilon}} = N_\varepsilon \times \prod_{f \in \mathcal{F}_{k,\varepsilon}} \#\mathcal{H}_{fp^s} \times \prod_{f \in \mathcal{G}_{k,\varepsilon}} \#\mathcal{H}_{fp^s}$$

where

$$N_1 = \begin{cases} 0 & \text{if } k \equiv 1 \pmod{2} \text{ and } p \equiv 1 \pmod{4} \\ & \text{or } k \equiv 0 \pmod{2} \text{ and } p \text{ odd} \\ 1 & \text{if } s = 0 \text{ and } p = 2 \\ 3 & \text{if } s > 0 \text{ and } p = 2 \\ 2 \frac{p^{(p^s+1)/2} - 1}{p-1} & \text{if } k \equiv 1 \pmod{2} \text{ and } p \equiv 3 \pmod{4} \end{cases}$$

and

$$N_{-1} = \begin{cases} 0 & \text{if } k \equiv 1 \pmod{2} \text{ and } p \equiv 3 \pmod{4} \\ 1 & \text{if } k \equiv 0 \pmod{2} \text{ and } p \text{ odd} \\ 2 \frac{p^{(p^s+1)/2} - 1}{p-1} & \text{if } k \equiv 1 \pmod{2} \text{ and } p \equiv 1 \pmod{4}. \end{cases}$$

**Proof.** One starts with Proposition 2 where the expression of  $N_\varepsilon$  is given in function of  $\#\mathcal{H}_{(X^2 \pm 1)^{p^s}}$ . One simplifies  $N_\varepsilon$  thanks to Proposition 4 (for  $p$  odd prime) and Remark 3 (for  $p = 2$ ). ■

## 4 Self-dual $\theta$ -cyclic and $\theta$ -negacyclic codes with dimension prime to $p$ over $\mathbb{F}_{p^2}$ .

Over  $\mathbb{F}_{p^2}$  with  $p$  odd prime number, there is no self-dual cyclic code and the number of self-dual negacyclic codes with dimension  $k$  prime to  $p$  is given in Theorem 2 of [17]. Self-dual cyclic codes over  $\mathbb{F}_4$  with odd dimension are studied in [10],

The aim of this section is to construct and to enumerate self-dual  $\theta$ -cyclic and  $\theta$ -negacyclic codes over  $\mathbb{F}_{p^2}$  whose dimension is prime to  $p$  when  $p$  is a prime number and  $\theta$  is the Frobenius automorphism (Proposition 8).

The starting point of the study is Proposition 5 applied in the particular case when the dimension  $k$  of the code is prime to  $p$  (i.e.  $k = p^s \times t$ ,  $s = 0$  and  $p \nmid t$ ). One wants to determine now the set  $\mathcal{H}_f$  for  $f$  in  $\mathcal{F} \cup \mathcal{G}$ .

Consider  $f = f(X^2)$  in  $\mathcal{F} \cup \mathcal{G}$ . Note that if  $f$  is in  $\mathcal{F}$  then the degree  $d$  of  $f$  in  $X^2$  is even (see exercise 3.14 page 141 of [12]). Consider  $\delta$  in  $\mathbb{N}$  such that  $d = 2\delta$  where  $\delta$  is in  $\mathbb{N}^*$ . Let  $h$  in  $R$  monic with degree  $2\delta$  :

$$\begin{aligned} h &= X^{2\delta} + \sum_{i=0}^{2\delta-1} h_i X^i \\ &= (X^{2\delta} + \sum_{i=0}^{\delta-1} h_{2i} X^{2i}) + X \cdot \left( \sum_{i=0}^{\delta-1} \theta(h_{2i+1}) X^{2i} \right). \end{aligned}$$

The skew reciprocal polynomial  $h^*$  of  $h$  is

$$h^* = 1 + \sum_{i=1}^{\delta} h_{2\delta-2i} X^{2i} + \left( \sum_{i=0}^{\delta-1} \theta(h_{2\delta-2i-1}) X^{2i} \right) \cdot X .$$

One can associate to  $h$  the two polynomials defined in  $\mathbb{F}_{p^2}[Z]$  by

$$A(Z) := Z^\delta + \sum_{i=0}^{\delta-1} h_{2i} Z^i \text{ and } B(Z) := \sum_{i=0}^{\delta-1} \theta(h_{2i+1}) Z^i. \quad (9)$$

Using the commutation law (1), one gets that  $h^\natural \cdot h = f(X^2)$  if and only if the following polynomial relations in  $\mathbb{F}_{p^2}[Z]$  are satisfied :

$$\begin{cases} Z^\delta A\left(\frac{1}{Z}\right) A(Z) + Z^\delta B\left(\frac{1}{Z}\right) B(Z) - h_0 f(Z) = 0 \\ Z^\delta A\left(\frac{1}{Z}\right) \Theta(B)(Z) + Z^{\delta-1} B\left(\frac{1}{Z}\right) \Theta(A)(Z) = 0 \end{cases} \quad (10)$$

where  $\Theta : \sum a_i Z^i \mapsto \sum a_i^p Z^i$ .

In the rest of the section, the following notation will be useful :

**Notation 2** Consider  $P(X^2) = \sum P_i X^{2i}$  in  $\mathbb{F}_p[X^2]$ , one denotes  $P(Z)$  the polynomial in  $\mathbb{F}_{p^2}[Z]$  defined by  $P(Z) = \sum P_i Z^i$ . For  $a$  in  $\overline{\mathbb{F}_{p^2}}$  and  $P(X^2)$  in  $\mathbb{F}_p[X^2]$ ,  $P(a)$  is  $\sum P_i a^i$ . The Frobenius automorphism  $\theta$  defined over  $\mathbb{F}_{p^2}$  is extended to  $\overline{\mathbb{F}_{p^2}}$  and is denoted with the same letter  $\theta$ .

Finding  $(A, B)$  in  $\mathbb{F}_{p^2}[Z] \times \mathbb{F}_{p^2}[Z]$  satisfying (10) with  $A$  monic,  $\deg(A) = \delta$  and  $\deg(B) \leq \delta - 1$  enables to construct the elements  $h$  of  $\mathcal{H}_f$ . One first considers the resolution of (10) when  $B(Z) = 0$ . This amounts to find the elements of  $\mathcal{H}_f \cap \mathbb{F}_{p^2}[X^2]$ .

**Lemma 3** 1. Consider  $f = f(X^2)$  in  $\mathcal{F}$  with degree  $2\delta$  in  $X^2$  and  $f(X^2) = \tilde{f}(X^2) \times \Theta(\tilde{f})(X^2)$  the factorization of  $f(X^2)$  in  $\mathbb{F}_{p^2}[X^2]$ .

$$\mathcal{H}_f \cap \mathbb{F}_{p^2}[X^2] = \begin{cases} \emptyset & \text{if } \delta \equiv 0 \pmod{2} \\ \{\tilde{f}(X^2), \Theta(\tilde{f})(X^2)\} & \text{if } \delta \equiv 1 \pmod{2} \end{cases}$$

2. Consider  $f = f(X^2)$  in  $\mathcal{G}$  with degree  $2\delta$  in  $X^2$  and  $g(X^2)$  such that  $f(X^2) = g(X^2)g^\natural(X^2)$ . When  $\delta$  is even, consider the factorization of  $g(X^2)$  in  $\mathbb{F}_{p^2}[X^2] : g(X^2) = \tilde{g}(X^2) \times \Theta(\tilde{g})(X^2)$ .  $\mathcal{H}_f \cap \mathbb{F}_{p^2}[X^2] =$

$$\begin{cases} \{g(X^2), g^\natural(X^2), \tilde{g}(X^2)\Theta(\tilde{g}^\natural)(X^2), \tilde{g}^\natural(X^2)\Theta(\tilde{g})(X^2)\} & \text{if } \delta \equiv 0 \pmod{2} \\ \{g(X^2), g^\natural(X^2)\} & \text{if } \delta \equiv 1 \pmod{2} \end{cases}$$

**Proof.** Recall that  $h$  is in  $\mathcal{H}_f$  if and only if  $(A(Z), B(Z))$  defined by (9) satisfies the relation (10). Furthermore  $h$  is in  $\mathbb{F}_{p^2}[X^2]$  if and only if  $B(Z) = 0$ . The elements of  $\mathcal{H}_f \cap \mathbb{F}_{p^2}[X^2]$  are therefore characterized by the relations  $B(Z) = 0$  and  $Z^\delta A(\frac{1}{Z})A(Z) = h_0 f(Z)$  where  $h_0$  is the constant term of  $A$ .

■

Here are now necessary conditions for  $h$  belonging to  $\mathcal{H}_f \setminus \mathbb{F}_{p^2}[X^2]$ .

**Lemma 4** Consider  $f = f(X^2)$  in  $\mathcal{F} \cup \mathcal{G}$  with degree  $2\delta$  in  $X^2$ ,  $h$  in  $R$  monic with degree  $2\delta$  and  $(A(Z), B(Z))$  defined in (9). If  $h \in \mathcal{H}_f \setminus \mathbb{F}_{p^2}[X^2]$  then

- (i)  $\gcd(A(Z), B(Z)) = 1$
- (ii)  $\gcd(B(Z), f(Z)) = 1$ .

**Proof.**

- (i) Assume that  $A(Z)$  and  $B(Z)$  have a common factor in  $\mathbb{F}_{p^2}[Z]$  then according to the first relation of (10), this factor must divide  $f(Z)$ . Furthermore,  $B(Z) \neq 0$  and the degree of  $B(Z)$  is  $\leq \delta - 1$ , therefore  $f(Z)$  must have a nontrivial factor in  $\mathbb{F}_{p^2}[Z]$  with degree  $\leq \delta - 1$ . Necessarily  $\delta$  is even,  $f = gg^\natural$  with  $g = \tilde{g}\Theta(\tilde{g})$  product of two irreducible polynomials of degree  $\delta/2$  in  $\mathbb{F}_{p^2}[Z]$ . Without loss of generality one can assume that  $\tilde{g}(Z)$  is the common factor of  $A(Z)$  and  $B(Z)$  in  $\mathbb{F}_{p^2}[Z]$ .

Consider  $\beta$  such that  $\tilde{g}(\beta) = 0$ ,  $a(Z)$  and  $b(Z)$  in  $\mathbb{F}_{p^2}[Z]$  such that  $A(Z) = \tilde{g}(Z)a(Z)$  and  $B(Z) = \tilde{g}(Z)b(Z)$ . From relations (10), one gets that

$$\begin{cases} Z^{\delta/2}a(1/Z)a(Z) + Z^{\delta/2}b(1/Z)b(Z) & = \lambda\Theta(\tilde{g})(Z)\tilde{g}^\natural(Z) \\ Z^{\delta/2}a(1/Z)\Theta(b)(Z) + Z^{\delta/2-1}b(1/Z)\Theta(a)(Z) & = 0 \end{cases} \quad (11)$$

where  $\lambda$  is a nonzero constant. Consider  $u$  in  $\mathbb{F}_{p^\delta} \setminus \{0\}$  such that  $a(\gamma) = u \times b(\gamma)$ . According to (11) evaluated at  $\gamma$ ,

$$\begin{cases} a(\gamma)a(1/\gamma) + b(\gamma)b(1/\gamma) & = 0 \\ \gamma\Theta(b)(\gamma)a(1/\gamma) + \Theta(a)(\gamma)b(1/\gamma) & = 0. \end{cases}$$

From the first relation, one deduces that  $a(1/\gamma) = -1/u \times b(1/\gamma)$  and from the second relation, one deduces  $-\gamma/u\Theta(b)(\gamma) + \Theta(a)(\gamma) = 0$  so  $(-\gamma/u)^p \times b(\gamma^p) + a(\gamma^p) = 0$ . As  $a(\gamma^p)a(1/\gamma^p) + b(\gamma^p)b(1/\gamma^p) = 0$ , one gets  $a(1/\gamma^p) = (u/\gamma)^p \times b(1/\gamma^p)$ . Therefore

$$\begin{cases} a(\gamma) &= u \times b(\gamma) \\ a(1/\gamma) &= -1/u \times b(1/\gamma) \\ a(\gamma^p) &= \gamma^p/u^p \times b(\gamma^p) \\ a(1/\gamma^p) &= -u^p/\gamma^p \times b(1/\gamma^p). \end{cases}$$

In particular, the polynomial  $Z^{\delta/2}a(1/Z)a(Z) + Z^{\delta/2}b(1/Z)b(Z)$  cancels at  $\gamma, 1/\gamma, \gamma^p, 1/\gamma^p$ , therefore it is divisible by  $f(Z)$ , which is impossible because of the first relation of (11).

- (ii) Assume that  $B(Z)$  and  $f(Z)$  are not coprime in  $\mathbb{F}_{p^2}[Z]$ . Necessarily  $\delta$  is even,  $f = gg^{\natural}$  with  $g = \tilde{g}\Theta(\tilde{g})$  product of two irreducible polynomials of degree  $\delta/2$  in  $\mathbb{F}_{p^2}[Z]$ . Without loss of generality one can assume that  $\tilde{g}(Z)$  is the common factor of  $f(Z)$  and  $B(Z)$  in  $\mathbb{F}_{p^2}[Z]$ . Consider  $\beta$  such that  $\tilde{g}(\beta) = 0$ , one has  $B(\beta) = 0, B(\beta^{-1}), B(\beta^p), B(\beta^{-p}) \neq 0$ . Furthermore  $\Theta(B)(\beta^p) = 0$  so according to the second relation of (10),  $\Theta(A)(\beta^p)B(1/\beta^p) = 0$  and  $A(\beta) = 0$ . Therefore  $A(Z)$  and  $B(Z)$  have a common factor in  $\mathbb{F}_{p^2}[Z]$ , which is impossible according to (i).

■

To characterize the elements  $h$  of  $\mathcal{H}_f$  such that  $h$  does not belong to  $\mathbb{F}_{p^2}[X^2]$ , one will use the following rational interpolation problem or Cauchy interpolation problem (Section 5.8 of [20]): given  $2\delta$  distinct points  $x_0, \dots, x_{2\delta-1}$  in  $\mathbb{F}_{p^{2\delta}}$  and  $2\delta$  values  $y_0, \dots, y_{2\delta-1}$  in  $\mathbb{F}_{p^{2\delta}}$ , find a rational function  $r/t \in \mathbb{F}_{p^{2\delta}}(Z)$  such that

$$(RI) : t(x_i) \neq 0, \frac{r(x_i)}{t(x_i)} = y_i \text{ for } 0 \leq i < 2\delta - 1, \deg(r) < \delta + 1, \deg(t) \leq \delta - 1$$

Note that this problem can be rewritten as

$$\gcd(t, f) = 1, r \equiv P \times t^{-1} \pmod{f}, \deg(r) < \delta + 1, \deg(t) \leq \delta - 1$$

where  $f = \prod_{i=0}^{2\delta-1} (Z - x_i)$ ,  $P$  has degree  $\leq 2\delta - 1$  and  $P(x_i) = y_i$  for  $0 \leq i < 2\delta - 1$ . This problem can be solved using extended Euclidean algorithm ([20]).

#### 4.1 Construction of $\mathcal{H}_f$ for $f$ in $\mathcal{F}$

For  $f$  in  $\mathcal{F}$ , one first gives a characterization of the elements  $h$  of  $\mathcal{H}_f \setminus \mathbb{F}_{p^2}[X^2]$ .

**Lemma 5** Consider  $f = f(X^2)$  in  $\mathcal{F}$  with degree  $d = 2\delta$  in  $X^2$  and  $\alpha$  in  $\mathbb{F}_{p^{2\delta}}$  such that  $f(\alpha) = 0$ .

1. Consider  $h$  in  $R$  monic with degree  $d = 2\delta$  and  $(A(Z), B(Z))$  defined in (9). Then  $h \in \mathcal{H}_f \setminus \mathbb{F}_{p^2}[X^2]$  if and only if there exists  $u$  in  $\mathbb{F}_{p^d}$  such that

$$\begin{cases} A(\alpha) &= u \times B(\alpha) \\ A(\alpha^p) &= \alpha^p/u^p \times B(\alpha^p) \\ \gcd(A(Z), B(Z)) &= 1 \\ \gcd(B(Z), f(Z)) &= 1 \end{cases} \quad (12)$$



and

$$\begin{cases} u^{p^\delta+1} = -1 & \text{if } \delta \text{ even} \\ u^{p^\delta-1} = -1/\alpha & \text{if } \delta \text{ odd.} \end{cases} \quad (13)$$

2. Consider  $u$  in  $\mathbb{F}_{p^d}$  such that the condition (13) is satisfied. There exists a unique solution  $(A, B)$  in  $\mathbb{F}_{p^2}[Z] \times \mathbb{F}_{p^2}[Z]$  to (12) with  $A$  monic,  $\deg(A) = \delta$ ,  $\deg(B) \leq \delta - 1$ .

3. The set  $\mathcal{H}_f \setminus \mathbb{F}_{p^2}[X^2]$  has  $p^\delta + 1$  elements if  $\delta$  is even and  $p^\delta - 1$  elements if  $\delta$  is odd.

**Proof.** As  $f$  belongs to  $\mathcal{F}$ ,  $f(\alpha^{-1}) = 0$  so there exists  $i$  in  $\{0, \dots, d-1\}$  such that  $\alpha^{-1} = \alpha^{p^i}$ . As  $\alpha^{p^{2i}} = (\alpha^{-1})^{p^i} = \alpha$ , and as  $f(X^2)$  is irreducible in  $\mathbb{F}_p[X^2]$  with degree  $d = 2\delta$ , necessarily  $i = \delta$  and  $\alpha^{-1} = \alpha^{p^\delta}$ .

1. Consider  $h$  in  $R$  with degree  $d = 2\delta$  and  $(A(Z), B(Z))$  defined by (9).

If  $h$  belongs to  $\mathcal{H}_f \setminus \mathbb{F}_{p^2}[X^2]$  then the relations (10) are satisfied by  $(A(Z), B(Z))$  with

$B(Z) \neq 0$ . Consider  $u, v$  in  $\mathbb{F}_{p^d}$  such that  $\begin{cases} A(\alpha) = u \times B(\alpha) \\ A(\alpha^p) = v \times B(\alpha^p) \end{cases}$ . According to

Lemma 4,  $\gcd(B, f) = 1$  so  $B(\alpha), B(\alpha^p) \neq 0$ . If  $\delta$  is even, then  $A(\alpha^{-1}) = A(\alpha)^{p^\delta}$  and  $B(\alpha^{-1}) = B(\alpha)^{p^\delta}$ . Evaluating (10) at  $\alpha$  one gets :

$$\begin{cases} u^{p^\delta} \times u + 1 = 0 \\ \alpha \times u^{p^\delta} + \theta^{-1}(v) = 0 \end{cases}$$

therefore  $v = \alpha^p/u^p$  and  $u^{p^\delta+1} = -1$ . If  $\delta$  is odd, then  $A(\alpha^{-1}) = A(\alpha^p)^{p^{\delta-1}}$  and  $B(\alpha^{-1}) = B(\alpha^p)^{p^{\delta-1}}$ . Evaluating (10) at  $\alpha$ , one gets :

$$\begin{cases} v^{p^{\delta-1}} \times u + 1 = 0 \\ \alpha \times v^{p^{\delta-1}} + \theta^{-1}(v) = 0 \end{cases}$$

therefore  $v = \alpha^p/u^p$  and  $u^{p^\delta-1} = -1/\alpha$ .

Conversely, if there exists  $u$  in  $\mathbb{F}_{p^d}$  such that (12) and (13) are satisfied, then one can

check that the polynomials  $Z^\delta A\left(\frac{1}{Z}\right)A(Z) + Z^\delta B\left(\frac{1}{Z}\right)B(Z) - h_0 f(Z)$  and

$Z^\delta A\left(\frac{1}{Z}\right)\Theta(B)(Z) + Z^{\delta-1}B\left(\frac{1}{Z}\right)\Theta(A)(Z)$  cancel at  $\alpha$  and  $\alpha^p$ . Therefore the relations

(10) are satisfied and  $h$  belongs to  $\mathcal{H}_f$ . As  $\gcd(B, f) = 1$ ,  $B \neq 0$  so  $h$  belongs to  $\mathcal{H}_f \setminus \mathbb{F}_{p^2}[X^2]$ .

2. Consider  $u$  in  $\mathbb{F}_{p^{2\delta}}$  such that the condition (13) is satisfied. Consider the  $2\delta$  points  $(x_i, y_i)_{0 \leq i \leq 2\delta-1}$  defined by

$$(x_i, y_i) = \begin{cases} (\theta^i(\alpha), \theta^i(u)) & \text{if } i \equiv 0 \pmod{2} \\ (\theta^i(\alpha), \theta^i(\alpha/u)) & \text{if } i \equiv 1 \pmod{2}. \end{cases}$$

According to Corollary 5.18 of [20] there exists two nonzero polynomials  $A$  and  $B$  in  $\mathbb{F}_{p^{2\delta}}[Z]$  such that  $\deg(A) < \delta + 1$ ,  $\deg(B) \leq \delta - 1$  and  $A(x_i) = y_i B(x_i)$ . Without loss of

generality, one can assume that  $A$  and  $B$  are coprime and that  $A$  is monic. Furthermore, the set  $(x_i, y_i)_{0 \leq i \leq 2\delta-1}$  is stable under the action of  $\theta^2$ , therefore  $(\Theta^2(A), \Theta^2(B))$  satisfies the relations  $\Theta^2(A)(x_i) = y_i \Theta^2(B)(x_i)$ . As  $A$  and  $B$  are coprime and  $A$  is monic,  $\Theta^2(A) = A$ ,  $\Theta^2(B) = B$ . Therefore  $A$  and  $B$  are polynomials of  $\mathbb{F}_{p^2}[Z]$ .

Considering the two first relations  $A(x_0) = y_0 B(x_0)$  and  $A(x_1) = y_1 B(x_1)$  one gets the relation (12), so the relation (10) is satisfied and the skew polynomial  $h$  associated to  $A$  and  $B$  belongs to  $\mathcal{H}_f$ . As  $A$  and  $B$  are coprime,  $B$  and  $f$  are also coprime (see Lemma 4). Assume that  $\deg(A) \neq \delta$ , then  $Z^\delta A(1/Z)A(Z) + Z^\delta B(1/Z)B(Z)$  would be the zero polynomial and  $h$  would satisfy  $h^* \cdot h = 0$  which is impossible.

Therefore for  $u$  in  $\mathbb{F}_{p^{2\delta}}$  such that the condition (13) is satisfied, there exists  $(A, B)$  in  $\mathbb{F}_{p^2}[Z] \times \mathbb{F}_{p^2}[Z]$  satisfying (12) with  $A$  monic,  $\deg(A) = \delta$  and  $\deg(B) \leq \delta - 1$ .

The unicity of  $(A, B)$  follows from the fact that  $A/B$  is the unique solution to the rational interpolation problem (RI) with  $A$  and  $B$  coprime (Corollary 5.18 of [20]).

3. According to 1.,  $\mathcal{H}_f = \sqcup_u \{h \in R \mid h \text{ monic, } \deg(h) = d, (A, B) \text{ defined in (9) solution of (12)}\}$  where  $u$  satisfies (13). According to 2., for each  $u$  satisfying (13), there is a unique  $h$  in  $R$  monic of degree  $d$  such that  $(A, B)$  defined in (9) is solution of (12). Therefore, the number of elements of  $\mathcal{H}_f$  is the number of  $u$  in  $\mathbb{F}_{p^d}$  satisfying  $u^{p^\delta+1} = -1$  if  $\delta$  is even and  $u^{p^\delta-1} = -1/\alpha$  if  $\delta$  is odd.

■

**Proposition 6** Consider  $p$  a prime number,  $m$  a positive integer,  $\theta$  the Frobenius automorphism over  $\mathbb{F}_{p^2}$  and  $R = \mathbb{F}_{p^2}[X; \theta]$ . Let  $f = f(X^2)$  in  $\mathcal{F}$  and  $d = 2\delta$  its degree in  $X^2$ , then the set  $\overline{\mathcal{H}}_f = \mathcal{H}_f$  has  $1 + p^\delta$  elements.

**Proof.** The elements of  $\mathcal{H}_f \cap \mathbb{F}_{p^2}[X^2]$  are given in point 1. of Lemma 3: there are two elements if  $\delta$  is odd and no element if  $\delta$  is even. The elements of  $\mathcal{H}_f$  who do not belong to  $\mathbb{F}_{p^2}[X^2]$  are given in point 3. of Lemma 5. There are  $p^\delta - 1$  elements if  $\delta$  is odd and  $p^\delta + 1$  elements if  $\delta$  is even. ■

**Example 4** Consider  $p = 2$ ,  $\theta$  the Frobenius automorphism over  $\mathbb{F}_4 = \mathbb{F}_2(a)$  where  $a^2 + a + 1 = 0$ ,  $R = \mathbb{F}_4[X; \theta]$  and  $f(X^2) = X^4 + X^2 + 1$  in  $\mathcal{F}$ . Consider  $h = X^2 + h_1 X + h_0$  in  $R$ ,  $A(Z) = Z + h_0$  and  $B(Z) = \theta(h_1)$  in  $\mathbb{F}_4[Z]$ . One has

$$h^\natural \cdot h = X^4 + X^2 + 1 \Leftrightarrow \begin{cases} ZA(1/Z)A(Z) + ZB(1/Z)B(Z) = h_0(Z^2 + Z + 1) \\ ZA(1/Z)\Theta(B)(Z) + B(1/Z)\Theta(A)(Z) = 0. \end{cases}$$

If  $h_1 = 0$ , one gets  $h^\natural \cdot h = X^4 + X^2 + 1$  if and only if  $ZA(\frac{1}{Z})A(Z) = h_0(Z^2 + Z + 1)$ . As  $Z^2 + Z + 1 = (Z + a)(Z + a^2)$  and  $a^2 = 1/a$ , one gets  $A(Z) = Z + a$  or  $A(Z) = Z + a^2$  (see Lemma 3), therefore if  $h_1 = 0$ ,  $h = X^2 + a$  or  $h = X^2 + a^2$ .

Following Lemma 5, if  $h_1 \neq 0$ , then  $h^\natural \cdot h = X^4 + X^2 + 1$  if and only if there exists  $u$  in  $\mathbb{F}_4$  such that  $u = 1/a$  and

$$\begin{cases} A(a) &= u \times B(a) = 1/a \times B(a) \\ A(a^2) &= \frac{a^2}{u^2} \times B(a^2) = a \times B(a^2). \end{cases}$$

Therefore when  $h_1 \neq 0$ , one gets  $h \in \mathcal{H}_{X^4+X^2+1}$  if and only  $h = X^2 + X + 1$ . As a conclusion the set  $\mathcal{H}_{X^4+X^2+1}$  is

$$\mathcal{H}_{X^4+X^2+1} = \overline{\mathcal{H}}_{X^4+X^2+1} = \{X^2 + a, X^2 + a^2, X^2 + X + 1\}.$$

**Example 5** Consider  $p = 2$ ,  $\theta$  the Frobenius automorphism over  $\mathbb{F}_4 = \mathbb{F}_2(a)$  with  $a^2 + a + 1 = 0$  and  $R = \mathbb{F}_4[X; \theta]$ . The skew polynomial  $X^{12} + X^6 + 1$  belongs to  $\mathcal{F}$  and its degree in  $X^2$  is 6. Consider  $\alpha$  in  $\mathbb{F}_{2^6}$  such that  $\alpha^6 + \alpha^3 + 1 = 0$ . According to Lemma 3 the elements of  $\mathcal{H}_{X^{12}+X^6+1}$  with no term of odd degree are  $X^6 + a$  and  $X^6 + a^2$ . According to Lemma 5, the other elements of  $\mathcal{H}_{X^{12}+X^6+1}$  are the monic skew polynomials  $h$  of degree 6 such that  $(A(Z), B(Z))$  defined by relations (9) are solutions of (12) with  $u^7 = 1/\alpha$ . The table below gives the solutions corresponding to the seven problems (12).

| $u$                                       | $h$                                       |
|---|---|
| $1 + \alpha$                              | $X^6 + a^2X^5 + aX^4 + aX^2 + a^2X + a^2$ |
| $1 + \alpha + \alpha^5$                   | $X^6 + X^5 + a^2X^4 + aX^2 + X + 1$       |
| $\alpha + \alpha^3 + \alpha^4 + \alpha^5$ | $X^6 + X^4 + a^2X^3 + a^2X^2 + a^2$       |
| $\alpha^5$                                | $X^6 + X^3 + 1$                           |
| $1 + \alpha^3 + \alpha^4$                 | $X^6 + X^4 + aX^3 + aX^2 + a$             |
| $\alpha + \alpha^3 + \alpha^4$            | $X^6 + X^5 + aX^4 + a^2X^2 + X + 1$       |
| $1 + \alpha^3 + \alpha^4 + \alpha^5$      | $X^6 + aX^5 + a^2X^4 + a^2X^2 + aX + a$   |

The number of elements of  $\mathcal{H}_{X^{12}+X^6+1}$  is  $9 = 1 + 2^3$ .

## 4.2 Construction of $\mathcal{H}_f$ for $f$ in $\mathcal{G}$

For  $f$  in  $\mathcal{G}$ , one gives a characterization of the elements of  $\mathcal{H}_f \setminus \mathbb{F}_{p^2}[X^2]$ .

**Lemma 6** Consider  $f = f(X^2)$  in  $\mathcal{G}$  with degree  $2\delta$  in  $X^2$  and  $g$  irreducible in  $\mathbb{F}_p[X^2]$  such that  $f(X^2) = g(X^2)g^{\natural}(X^2)$ . Consider  $\beta$  in  $\mathbb{F}_{p^\delta}$  such that  $g(\beta) = 0$ .

1. Consider  $h$  in  $R$  monic with degree  $2\delta$  and  $(A(Z), B(Z))$  defined by relations (9). Then  $h \in \mathcal{H}_f \setminus \mathbb{F}_{p^2}[X^2]$  if and only if there exists  $u$  in  $\mathbb{F}_{p^d}$  such that

$$\left\{ \begin{array}{l} A(\beta) = u \times B(\beta) \\ A(1/\beta) = -1/u \times B(1/\beta) \\ A(\beta^p) = \beta^p/u^p \times B(\beta^p) \\ A(1/\beta^p) = -u^p/\beta^p \times B(1/\beta^p) \\ \gcd(A(Z), B(Z)) = 1 \\ \gcd(B(Z), f(Z)) = 1 \end{array} \right. \quad (14)$$

and

$$\left\{ \begin{array}{l} u^{p^\delta-1} = 1 \quad \text{if } \delta \text{ even} \\ u^{p^\delta+1} = \beta \quad \text{if } \delta \text{ odd.} \end{array} \right. \quad (15)$$

2. Consider  $u$  in  $\mathbb{F}_{p^d}$  such that the condition (15) is satisfied. There exists a unique solution  $(A, B)$  in  $\mathbb{F}_{p^2}[Z] \times \mathbb{F}_{p^2}[Z]$  to (14) with  $A$  monic,  $\deg(A) = \delta$ ,  $\deg(B) \leq \delta - 1$ .

3. The set  $\mathcal{H}_f \setminus \mathbb{F}_{p^2}[X^2]$  has  $p^\delta - 1$  elements if  $\delta$  is even and  $p^\delta + 1$  elements if  $\delta$  is odd.

**Proof.**

1. Consider  $h$  in  $R$  with degree  $d = 2\delta$  and  $(A(Z), B(Z))$  defined by (9).

If  $h \in \mathcal{H}_f \setminus \mathbb{F}_{p^2}[X^2]$  then  $(A(Z), B(Z))$  satisfies the relation (10) with  $B(Z) \neq 0$ . According to Lemma 4,  $B$  is coprime with  $f$ , therefore  $B(\beta)$ ,  $B(1/\beta)$ ,  $B(\beta^p)$  and  $B(1/\beta^p) \neq 0$ . Consider  $u$  in  $\mathbb{F}_{p^\delta}$  such that  $A(\beta) = u \times B(\beta)$ . According to (10) evaluated at  $\beta$ ,

$$\begin{cases} A(\beta)A(1/\beta) + B(\beta)B(1/\beta) & = 0 \\ \beta\Theta(B)(\beta)A(1/\beta) + \Theta(A)(\beta)B(1/\beta) & = 0. \end{cases}$$

From the first relation, one deduces that  $A(1/\beta) = -1/u \times B(1/\beta)$  and from the second relation, one deduces  $-\beta/u\Theta(B)(\beta) + \Theta(A)(\beta) = 0$  so  $(-\beta/u)^p \times B(\beta^p) + A(\beta^p) = 0$ . As  $A(\beta^p)A(1/\beta^p) + B(\beta^p)B(1/\beta^p) = 0$ , one gets  $A(1/\beta^p) = (u/\beta)^p \times B(1/\beta^p)$ . Therefore the relations (14) are satisfied.

Furthermore, if  $\delta$  is odd, one gets another constraint, namely as  $\beta = \beta^{p^\delta}$  one gets  $\Theta(A)(\beta) = (\Theta(A)(\beta^p))^{p^{\delta-1}} = (u^p B(\beta^p))^{p^{\delta-1}} = u^{p^\delta} \Theta(B)(\beta)$ . Furthermore,  $-\beta/u\Theta(B)(\beta) + \Theta(A)(\beta) = 0$ , so  $-\beta/u + u^{p^\delta} = 0$  and  $u^{p^\delta+1} = \beta$ . The relations (15) are therefore satisfied.

Conversely, if there exists  $u$  in  $\mathbb{F}_{p^\delta}$  such that (14) and (15) are satisfied, then one can check that the polynomials  $Z^\delta A\left(\frac{1}{Z}\right)A(Z) + Z^\delta B\left(\frac{1}{Z}\right)B(Z) - h_0 f(Z)$  and

$Z^\delta A\left(\frac{1}{Z}\right)\Theta(B)(Z) + Z^{\delta-1}B\left(\frac{1}{Z}\right)\Theta(A)(Z)$  cancel at  $\beta$ ,  $1/\beta$ ,  $\beta^p$  and  $1/\beta^p$ . Therefore the relations (10) are satisfied and  $h$  belongs to  $\mathcal{H}_f$ . As  $\gcd(B, f) = 1$ ,  $B$  is nonzero so  $h$  belongs to  $\mathcal{H} \setminus \mathbb{F}_{p^2}[X^2]$ .

2. Consider  $u$  in  $\mathbb{F}_{p^{2\delta}}$  such that the condition (15) is satisfied. Consider the  $2\delta$  points  $(x_i, y_i)_{0 \leq i < 2\delta-1}$  defined by

$$(x_i, y_i) = \begin{cases} (\theta^i(\beta), \theta^i(u)) & \text{if } i \equiv 0 \pmod{2}, i < \delta \\ (\theta^i(\beta), \theta^i(\beta/u)) & \text{if } i \equiv 1 \pmod{2}, i < \delta \end{cases}$$

$$(x_{i+\delta}, y_{i+\delta}) = \begin{cases} (\theta^i(1/\beta), -\theta^i(1/u)) & \text{if } i \equiv 0 \pmod{2}, i < \delta \\ (\theta^i(1/\beta), -\theta^i(u/\beta)) & \text{if } i \equiv 1 \pmod{2}, i < \delta. \end{cases}$$

According to Corollary 5.18 of [20] there exists two nonzero polynomials  $A$  and  $B$  in  $\mathbb{F}_{p^{2\delta}}[Z]$  such that  $\deg(A) < \delta + 1$ ,  $\deg(B) \leq \delta - 1$  and for  $i$  in  $\{0, \dots, 2\delta - 1\}$ ,  $A(x_i) = y_i B(x_i)$ . Without loss of generality, one can assume that  $A$  and  $B$  are coprime and that  $A$  is monic. Furthermore, as the set of points  $\{(x_i, y_i)\}$  is stable under the application of  $\theta^2$ ,  $A(Z)$  and  $B(Z)$  belong to  $\mathbb{F}_{p^2}[Z]$ .

Considering the four relations  $A(x_0) = y_0 B(x_0)$ ,  $A(x_1) = y_1 B(x_1)$ ,  $A(x_\delta) = y_\delta B(x_\delta)$  and  $A(x_{\delta+1}) = y_{\delta+1} B(x_{\delta+1})$  one gets the relation (14), so the relation (10) is satisfied and the skew polynomial  $h$  associated to  $A$  and  $B$  belongs to  $\mathcal{H}_f$ . As  $A$  and  $B$  are coprime,  $B$  and  $f$  are also coprime (see Lemma 4). Assume that  $\deg(A) \neq \delta$ , then

$Z^\delta A(1/Z)A(Z) + Z^\delta B(1/Z)B(Z)$  would be the zero polynomial and  $h$  would satisfy  $h^* \cdot h = 0$  which is impossible.

Therefore for  $u$  in  $\mathbb{F}_{p^{2\delta}}$  such that the condition (15) is satisfied, there exists  $(A, B)$  in  $\mathbb{F}_{p^2}[Z] \times \mathbb{F}_{p^2}[Z]$  satisfying (14) with  $A$  monic,  $\deg(A) = \delta$  and  $\deg(B) \leq \delta - 1$  with  $A$  and  $B$  coprime.

The unicity follows from the fact that  $A/B$  is the unique solution to the rational interpolation problem  $(RI)$  with  $A$  and  $B$  coprime ( Corollary 5.18 of [20] ).

3. Like in Lemma 5, the number of elements of  $\mathcal{H}_f$  is deduced from points 1. and 2.

■

**Proposition 7** Consider  $p$  a prime number,  $\theta$  the Frobenius automorphism over  $\mathbb{F}_{p^2}$  and  $R = \mathbb{F}_{p^2}[X; \theta]$ . Let  $f = f(X^2)$  in  $\mathcal{G}$  and  $d = 2\delta$  its degree in  $X^2$ , then the set  $\mathcal{H}_f$  has  $3 + p^\delta$  elements and  $\overline{\mathcal{H}}_f$  has  $1 + p^\delta$  elements.

**Proof.** The result is deduced from point 2. of Lemma 3 and point 3. of Lemma 6. Furthermore if  $f(X^2) = g(X^2)g^\natural(X^2)$  belongs to  $\mathcal{G}$ , then  $\overline{\mathcal{H}}_{f(X^2)} = \mathcal{H}_{f(X^2)} \setminus \{g(X^2), g^\natural(X^2)\}$  has  $1 + p^\delta$  elements. ■

**Example 6** Consider  $\mathbb{F}_4 = \mathbb{F}_2(a)$  where  $a^2 + a + 1 = 0$ ,  $\theta$  the Frobenius automorphism,  $R = \mathbb{F}_4[X; \theta]$  and  $f(X^2) = (X^6 + X^2 + 1)(X^6 + X^4 + 1)$  in  $\mathcal{G}$  with degree  $6 = 2 \times 3$  in  $X^2$ . Consider  $\beta$  in  $\mathbb{F}_{2^3}$  such that  $\beta^3 + \beta^2 + 1 = 0$ . According to Lemma 3, the elements of  $\mathcal{H}_f$  with no term of odd degree are  $X^6 + X^2 + 1$  and  $X^6 + X^4 + 1$ . According to Lemma 6, the other elements of  $\mathcal{H}_f$  are deduced from the polynomials  $A(Z)$  and  $B(Z)$  of  $\mathbb{F}_4[Z]$  satisfying (14) with  $u^9 = \beta$ ,  $A(Z)$  monic of degree 3 and  $B(Z)$  of degree  $\leq 2$ .

For example take  $u = v^3$  where  $v^6 + v^4 + v^3 + v + 1 = 0$ , then  $u^9 = \beta$  and the unique solution  $(A, B)$  in  $\mathbb{F}_4[Z] \times \mathbb{F}_4[Z]$  of (14) with  $A$  monic of degree 3 and  $B$  of degree  $\leq 2$  is  $(A, B) = (Z^3 + a, aZ^2 + a^2Z + 1)$ . Therefore,  $h(X) = (X^6 + a) + X \cdot (aX^4 + a^2X^2 + 1) = X^6 + a^2X^5 + aX^3 + X + a$  is an element of  $\mathcal{H}_f$  with at least one non zero term of odd degree. The entire set  $\mathcal{H}_f$  is  $\{X^6 + X^2 + 1, X^6 + X^4 + 1, X^6 + X^5 + aX^3 + a^2X + a, X^6 + a^2X^5 + X^4 + X^2 + aX + 1, X^6 + aX^5 + X^4 + X^2 + a^2X + 1, X^6 + X^5 + X^4 + X^3 + X^2 + X + 1, X^6 + aX^4 + aX^3 + X^2 + a, X^6 + a^2X^4 + a^2X^3 + X^2 + a^2, X^6 + aX^5 + a^2X^3 + X + a^2, X^6 + X^5 + a^2X^3 + aX + a^2, X^6 + a^2X^5 + aX^3 + X + a\}$ . It has  $2^\delta + 3 = 11$  elements (Proposition 7).

### 4.3 Conclusion

The proposition below gives a formula for the number of self-dual  $\theta$ -cyclic and  $\theta$ -negacyclic codes over  $\mathbb{F}_{p^2}$  whose dimension is prime to  $p$ . Tables 2 and 3 illustrate this proposition over  $\mathbb{F}_4$  and  $\mathbb{F}_9$  and give some elements of comparison with cyclic and negacyclic codes.

**Proposition 8** Consider  $p$  a prime number,  $\theta$  the Frobenius automorphism over  $\mathbb{F}_{p^2}$ ,  $k$  a positive integer not divisible by  $p$  and  $\varepsilon$  in  $\{-1, 1\}$ . The number of self-dual  $(\theta, \varepsilon)$ -constacyclic codes with dimension  $k$  defined over  $\mathbb{F}_{p^2}$  is

$$N_\varepsilon \times \prod_{f \in \mathcal{F}_{k,\varepsilon}} (p^\delta + 1) \times \prod_{f \in \mathcal{G}_{k,\varepsilon}} (p^\delta + 3)$$

where  $2\delta$  is the degree of  $f$  in  $X^2$  and  $N_\varepsilon$  is defined below :

$$N_1 = \begin{cases} 0 & \text{if } k \equiv 1 \pmod{2} \text{ and } p \equiv 1 \pmod{4} \\ & \text{or } k \equiv 0 \pmod{2} \text{ and } p \text{ odd} \\ 1 & \text{if } p = 2 \\ 2 & \text{if } k \equiv 1 \pmod{2} \text{ and } p \equiv 3 \pmod{4} \end{cases}$$

$$N_{-1} = \begin{cases} 0 & \text{if } k \equiv 1 \pmod{2} \text{ and } p \equiv 3 \pmod{4} \\ 1 & \text{if } k \equiv 0 \pmod{2} \text{ and } p \text{ odd} \\ 2 & \text{if } k \equiv 1 \pmod{2} \text{ and } p \equiv 1 \pmod{4}. \end{cases}$$

**Proof.** According to Proposition 5, with  $s = 0$ , the number of self-dual  $(\theta, \varepsilon)$ -constacyclic codes over  $\mathbb{F}_{p^2}$  with dimension  $k$  is

$$\#\mathcal{H}_{X^{2k-\varepsilon}} = N_\varepsilon \times \prod_{f \in \mathcal{F}_{k,\varepsilon}} \#\mathcal{H}_f \times \prod_{f \in \mathcal{G}_{k,\varepsilon}} \#\mathcal{H}_f$$

where  $N_\varepsilon$  satisfies the above conditions. The final result follows from Proposition 6 and Proposition 7. ■

**Example 7** Consider  $\theta : x \mapsto x^2$  the Frobenius automorphism over  $\mathbb{F}_4 = \mathbb{F}_2(a)$  where  $a^2 + a + 1 = 0$ . The self-dual  $\theta$ -cyclic codes of dimension 9 over  $\mathbb{F}_4$  are characterized by the monic solutions of the self-dual skew equation  $h^\natural \cdot h = X^{18} + 1$ . As  $X^{18} + 1 = (X^2 + 1)(X^4 + X^2 + 1)(X^{12} + X^6 + 1)$  in  $\mathbb{F}_2[X^2]$  and as the polynomials  $X^4 + X^2 + 1$  and  $X^{12} + X^6 + 1$  are self-reciprocal and irreducible in  $\mathbb{F}_2[X^2]$ , the set  $\mathcal{F}_{9,1}$  is  $\{X^4 + X^2 + 1, X^{12} + X^6 + 1\}$  and the set  $\mathcal{G}_{9,1}$  is empty. According to Proposition 8, the number of self-dual  $\theta$ -cyclic codes of dimension 9 over  $\mathbb{F}_4$  is  $1 \times (2^1 + 1) \times (2^3 + 1) = 27$ . More precisely the set  $\mathcal{H}_{X^{18+1}}$  is given by

$$\mathcal{H}_{X^{18+1}} = \{\text{lcrm}(h_1, h_2, h_3) \mid h_1 \in \mathcal{H}_{X^2+1}, h_2 \in \mathcal{H}_{X^4+X^2+1}, h_3 \in \mathcal{H}_{X^{12}+X^6+1}\}$$

and the sets  $\mathcal{H}_{X^2+1}$ ,  $\mathcal{H}_{X^4+X^2+1}$  and  $\mathcal{H}_{X^{12}+X^6+1}$  with cardinalities 1, 3 and 9 were previously computed in Examples 2, 4 and 5.

## 5 Self-dual $\theta$ -cyclic and $\theta$ -negacyclic codes with any dimension over $\mathbb{F}_{p^2}$ .

In this section, one constructs and enumerates all self-dual  $\theta$ -cyclic and  $\theta$ -negacyclic codes over  $\mathbb{F}_{p^2}$  where  $p$  is a prime number and  $\theta$  is the Frobenius automorphism.

Like in Section 4, the starting point of the construction is Proposition 5, who enables to write the monic solutions of the self-dual skew equation as least common right multiples of skew polynomials satisfying intermediate skew equations. The main topic of this section is therefore to construct the intermediate sets  $\mathcal{H}_{f^{p^s}}$  where  $s > 0$  and  $f = f(X^2)$  belongs to  $\mathcal{F} \cup \mathcal{G}$ .

First, one assumes that  $f = f(X^2)$  belongs to  $\mathcal{F}$ .

| $k$ | $c$ | $\theta$ - $c$ |
|-----|-----|----------------|
| 1   | 1   | 1              |
| 3   | 3   | 3              |
| 5   | 1   | 5              |
| 7   | 3   | 11             |
| 9   | 9   | 27             |
| 11  | 3   | 33             |
| 13  | 1   | 65             |
| 15  | 9   | 285            |
| 17  | 1   | 289            |
| 19  | 3   | 513            |
| 21  | 9   | 2211           |
| 23  | 3   | 2051           |
| 25  | 1   | 5125           |
| 27  | 27  | 13851          |
| 29  | 1   | 16385          |
| 31  | 3   | 42875          |
| 33  | 9   | 107811         |

| $k$ | $c$ | $\theta$ - $c$ |
|-----|-----|----------------|
| 35  | 9   | 225445         |
| 37  | 1   | 262145         |
| 39  | 9   | 799305         |
| 41  | 1   | 1050625        |
| 43  | 3   | 2146689        |
| 45  | 81  | 10513935       |
| 47  | 3   | 8388611        |
| 49  | 9   | 23068705       |
| 51  | 9   | 58159227       |
| 53  | 1   | 67108865       |
| 55  | 9   | 173015535      |
| 57  | 9   | 405017091      |
| 59  | 3   | 536870913      |
| 61  | 1   | 1073741825     |
| 63  | 9   | 5984882937     |
| 65  | 1   | 5801453125     |
| 67  | 3   | 8589934593     |

| $k$ | $c$ | $\theta$ - $c$   |
|-----|-----|------------------|
| 69  | 9   | 25807570971      |
| 71  | 3   | 34359738371      |
| 73  | 3   | 70344300625      |
| 75  | 27  | 306316140375     |
| 77  | 27  | 389768283201     |
| 79  | 3   | 549755813891     |
| 81  | 81  | 1859049764379    |
| 83  | 3   | 2199023255553    |
| 85  | 3   | 6502298510645    |
| 87  | 9   | 13194944987145   |
| 89  | 3   | 17695491973201   |
| 91  | 9   | 49242466343785   |
| 93  | 9   | 139327459600875  |
| 95  | 9   | 176265457835535  |
| 97  | 1   | 281475010265089  |
| 99  | 81  | 1041914208570939 |

Table 2: Numbers of self-dual cyclic codes ( $c$ , Corollary 1 of [10]) and  $\theta$ -cyclic codes ( $\theta$ - $c$ , prop. 8) over  $\mathbb{F}_4$  in odd dimension  $k < 100$  where  $\theta : x \mapsto x^2$ .

| $k$ | nc   | $\theta$ - $c$ | $\theta$ -nc |
|-----|------|----------------|--------------|
| 1   | 2    | 2              | 0            |
| 2   | 4    | 0              | 4            |
| 4   | 4    | 0              | 12           |
| 5   | 8    | 20             | 0            |
| 7   | 8    | 56             | 0            |
| 8   | 4    | 0              | 84           |
| 10  | 64   | 0              | 336          |
| 11  | 8    | 492            | 0            |
| 13  | 32   | 1800           | 0            |
| 14  | 64   | 0              | 3136         |
| 16  | 4    | 0              | 6564         |
| 17  | 8    | 13124          | 0            |
| 19  | 8    | 39368          | 0            |
| 20  | 1024 | 0              | 84672        |
| 22  | 64   | 0              | 236208       |
| 23  | 8    | 354300         | 0            |
| 25  | 32   | 1181000        | 0            |

| $k$ | nc   | $\theta$ - $c$ | $\theta$ -nc  |
|-----|------|----------------|---------------|
| 26  | 1024 | 0              | 2143296       |
| 28  | 64   | 0              | 6429888       |
| 29  | 8    | 9565940        | 0             |
| 31  | 8    | 28697816       | 0             |
| 32  | 4    | 0              | 43046724      |
| 34  | 64   | 0              | 172186896     |
| 35  | 512  | 297608640      | 0             |
| 37  | 32   | 774919712      | 0             |
| 38  | 64   | 0              | 1549839424    |
| 40  | 1024 | 0              | 4182119424    |
| 41  | 2048 | 7414796864     | 0             |
| 43  | 8    | 20920706408    | 0             |
| 44  | 64   | 0              | 41845664448   |
| 46  | 64   | 0              | 125524238448  |
| 47  | 8    | 188286357660   | 0             |
| 49  | 32   | 585779779424   | 0             |
| 50  | 1024 | 0              | 1171559559744 |

Table 3: Numbers of self-dual negacyclic (nc, Theorem 2 of [17]), self-dual  $\theta$ -cyclic ( $\theta$ - $c$ , prop. 8) and self-dual  $\theta$ -negacyclic ( $\theta$ -nc, prop. 8) codes over  $\mathbb{F}_9$  in dimension  $k \leq 50$  coprime with 3 where  $\theta : x \mapsto x^3$ .

## 5.1 Construction of $\mathcal{H}_{fp^s}$ for $f$ in $\mathcal{F}$

The aim of this subsection is to compute  $\mathcal{H}_{fp^s}$  for  $f$  in  $\mathcal{F}$  and to compute its number of elements. The final result is given in Proposition 9 and the main steps are summed up in Table 4.

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

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

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

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

Lemma 7 below generalizes Lemma 1 and uses the same type of arguments linked to the factorization of skew polynomials.

**Lemma 7** *Consider  $p$  a prime number,  $\theta$  the Frobenius automorphism over  $\mathbb{F}_{p^2}$ ,  $R = \mathbb{F}_{p^2}[X; \theta]$ ,  $m$  a nonnegative integer and  $f = f(X^2)$  in  $\mathcal{F}$  with degree  $d = 2\delta > 1$  in  $X^2$ .*

1. *The constant coefficients of the elements of  $\overline{\mathcal{H}}_f$  are squares in  $\mathbb{F}_{p^2}$ .*
2. *The set  $\overline{\mathcal{H}}_{fm}$  has  $(1 + p^\delta)p^{\delta(m-1)}$  elements and is equal to*

$$\left\{ \left( h_1 \cdot \frac{1}{\nu_1} \right) \cdots \left( h_m \cdot \frac{1}{\nu_m} \right) \cdot \left( \prod_{j=1}^m \nu_j \right) \mid h_j \in \overline{\mathcal{H}}_f, \nu_j^2 = (h_j)_0, h_j \neq \nu_{j-1} \cdot h_{j-1}^{\natural} \cdot \frac{1}{\nu_{j-1}} \right\}.$$

### Proof.

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

1. Consider  $h = X^d + \sum_{i=0}^{d-1} h_i X^i$  in  $\overline{\mathcal{H}}_f = \mathcal{H}_f$ . If  $p = 2$ , then  $h_0$  is a nonzero element of  $\mathbb{F}_4$  and therefore is a square in  $\mathbb{F}_4$ . Assume that  $p$  is odd. According to Section 4, the polynomials  $A(Z) = Z^\delta + \sum_{i=0}^{\delta-1} h_{2i} Z^i$  and  $B(Z) = \sum_{i=0}^{\delta-1} \theta(h_{2i+1}) Z^i$  defined in (9) satisfy the relations (10). If  $f(Z)$  and  $B(Z)$  are coprime then  $f(Z) = f^\natural(Z)$  and  $Z^{\delta-1} B(1/Z)$  are also coprime. Therefore the relations (10) imply that  $f(Z) = A(Z)\Theta(A)(Z) - ZB(Z)\Theta(B)(Z)$ ,  $Z^{\delta-1} B(1/Z) = -h_0\Theta(B)(Z)$  and  $Z^\delta A(1/Z) = h_0\Theta(A)(Z)$ . In particular, one has  $1 - h_0 h_0^p = 0$  so  $h_0$  is a square. If  $f(Z)$  and  $B(Z)$  are not coprime, then according to Lemma 4,  $B(Z) = 0$  and using Lemma 3, one gets  $A(Z) = \tilde{f}(Z)$  or  $\Theta(\tilde{f})(Z)$  where  $f(Z) = \tilde{f}(Z)\Theta(\tilde{f})(Z)$  is the factorization of  $f(Z)$  into irreducible polynomials of  $\mathbb{F}_{p^2}[Z]$ . As  $f = f^\natural$ , the constant coefficient of  $f$  is equal to 1, so one gets  $h_0^{p+1} = 1$  and  $h_0$  is a square.



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  $d$  (Lemma 13 (2) of [3] or [15] 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 of  $f$ .

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  $\mu_i = (H_1 \cdots H_{i-1})_0$  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,  $f^m = h^\natural \cdot h$  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,  $\frac{1}{\mu_1} H_1^\natural \cdot \mu_1 \cdot H_1 = f$  and proceeding by induction, one gets

$$\forall j \in \{1, \dots, m-1\}, \frac{1}{\mu_j} H_j^\natural \cdot \mu_j \cdot H_j = f \text{ and } H_{j+1} \neq \frac{1}{\mu_j} H_j^\natural \cdot \mu_j. \quad (16)$$

Conversely, consider  $h = H_1 \cdots H_m$  with  $\frac{1}{\mu_j} H_j^\natural \cdot \mu_j \cdot H_j = f, H_{j+1} \neq \frac{1}{\mu_j} H_j^\natural \cdot \mu_j$  and  $\mu_j$  constant coefficient of  $H_1 \cdots H_{j-1}$ , then  $h^\natural \cdot h = f^m$  and  $H_j \cdot H_{j+1} \neq f$ . Furthermore, the skew polynomials  $H_j$  are all irreducible because they are nontrivial 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  $\overline{\mathcal{H}}_{f^m}$ .

The conclusion follows thanks to the following equivalence :

$$\left\{ \begin{array}{l} h = H_1 \cdots H_m \\ \frac{1}{\mu_j} H_j^\natural \cdot \mu_j \cdot H_j = f \\ H_{j+1} \neq \frac{1}{\mu_j} H_j^\natural \cdot \mu_j \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} h = \left( h_1 \cdot \frac{1}{\nu_1} \right) \cdots \left( h_m \cdot \frac{1}{\nu_m} \right) \cdot \prod_{j=1}^m \nu_j \\ h_j^\natural \cdot h_j = f \\ h_{j+1} \neq \nu_j h_j^\natural \cdot \frac{1}{\nu_j} \end{array} \right.$$

where  $\mu_j = (H_1 \cdots H_{j-1})_0$  is the constant coefficient of  $H_1 \cdots H_{j-1}$ ,  $\nu_j$  is defined in  $\mathbb{F}_{p^2}$  by  $\nu_j^2 = (H_j)_0 = (h_j)_0$  and  $h_j = (\nu_0 \cdots \nu_j) H_j \cdot \frac{1}{\nu_0 \cdots \nu_j}$ .

3. The number of elements of  $\overline{\mathcal{H}}_{f^m}$  follows from the fact that  $\overline{\mathcal{H}}_f$  has  $1 + p^\delta$  elements (Proposition 6).

■

The construction of the set  $\mathcal{H}_{fp^s}$  for  $f$  in  $\mathcal{F}$  is deduced from Lemma 2 and Lemma 7. The whole construction is illustrated in Table 4.

|   |  |                                      |
|---|--|--------------------------------------|
| Lemma 3 and<br>Cauchy in-<br>terpolation<br>(Lemma 5) | Decomposition<br>into the products<br>of elements of $\overline{\mathcal{H}}_f$<br>(Proposition 3) | Partition<br>(Lemma 2)               |
| ↓   | ↓  | ↓                                    |
| $\overline{\mathcal{H}}_f$ (Proposition 6)            | $\overline{\mathcal{H}}_{f^m}$ (Lemma 7)   | $\mathcal{H}_{fp^s}$ (Proposition 9) |

Table 4: Main steps of the construction of  $\mathcal{H}_{fp^s}$  for  $f$  in  $\mathcal{F}$

**Proposition 9** Consider  $p$  a prime number,  $\theta$  the Frobenius automorphism over  $\mathbb{F}_{p^2}$ ,  $R = \mathbb{F}_{p^2}[X; \theta]$ ,  $s$  a nonnegative integer and  $f = f(X^2)$  in  $\mathcal{F}$  with degree  $d = 2\delta > 1$  in  $X^2$ . The set  $\mathcal{H}_{fp^s}$  has  $\frac{p^{\delta(p^s+1)} - 1}{p^\delta - 1}$  elements.

**Proof.** According to Lemma 2,  $\mathcal{H}_{fp^s} = \bigsqcup_{i=0}^{\lfloor \frac{p^s}{2} \rfloor} f^i \cdot \overline{\mathcal{H}}_{fp^{s-2i}}$  and according to Lemma 7,  $\overline{\mathcal{H}}_{f^m}$  has  $(1 + p^\delta)(p^\delta)^{m-1}$  if  $m \neq 0$  and 1 element if  $m = 0$ . Therefore  $\mathcal{H}_{fp^s}$  has  $\sum_{i=0}^{(p^s-1)/2} (1 + p^\delta)(p^\delta)^{p^s-2i-1}$  elements if  $p$  is odd and  $1 + \sum_{i=0}^{2^s-1} (1 + 2^\delta)(2^\delta)^{2^s-2i-1}$  elements otherwise. In both cases one gets  $\#\mathcal{H}_{fp^s} = \frac{p^{\delta(p^s+1)} - 1}{p^\delta - 1}$ . ■

**Example 8** Consider  $\mathbb{F}_4 = \mathbb{F}_2(a)$ ,  $\theta$  the Frobenius automorphism and  $f(X^2) = X^4 + X^2 + 1$  in  $\mathcal{F}$ . According to Proposition 9, the set  $\mathcal{H}_{f_2}$  has  $\frac{2^{1 \times (2^1+1)} - 1}{2^1 - 1} = 7$  elements. More precisely,  $\mathcal{H}_{f_2} = f^1 \cdot \overline{\mathcal{H}}_{f_0} \sqcup f^0 \cdot \overline{\mathcal{H}}_{f_2} = \{f\} \sqcup \overline{\mathcal{H}}_{f_2}$ . Furthermore, according to Lemma 7, the elements of  $\overline{\mathcal{H}}_{f_2}$  are constructed by using products of elements of  $\overline{\mathcal{H}}_f = \{X^2 + a, X^2 + a^2, X^2 + X + 1\}$  (see Example 4 for the construction of  $\overline{\mathcal{H}}_f$ ). Here are the 6 elements of  $\overline{\mathcal{H}}_{f_2}$  :

$$\left\{ \begin{array}{l} (X^2 + X + 1) \cdot (1/1)(X^2 + a) \cdot (1/a^2)a^2 = X^4 + X^3 + a^2X^2 + a^2X + a \\ (X^2 + X + 1) \cdot (1/1)(X^2 + a^2) \cdot (1/a)a = X^4 + X^3 + aX^2 + aX + a^2 \\ (X^2 + a) \cdot (1/a^2)(X^2 + a) \cdot (1/a^2)a = X^4 + a^2 \\ (X^2 + a) \cdot (1/a^2)(X^2 + X + 1) \cdot a^2 = X^4 + a^2X^3 + a^2X^2 + X + a \\ (X^2 + a^2) \cdot (1/a)(X^2 + a^2) \cdot (1/a)a^2 = X^4 + a \\ (X^2 + a^2) \cdot (1/a)(X^2 + X + 1) \cdot a = X^4 + aX^3 + aX^2 + X + a^2. \end{array} \right.$$

In next subsection one constructs the set  $\mathcal{H}_{fp^s}$  when  $f = f(X^2)$  belongs to  $\mathcal{G}$ .

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

In this subsection, one computes  $\mathcal{H}_{fp^s}$  for  $f$  in  $\mathcal{G}$  (Proposition 11). The construction is summed up in Table 5.

Assume that  $f = f(X^2) = g(X^2)g^\natural(X^2)$  with  $g(X^2) \neq g^\natural(X^2)$  irreducible in  $\mathbb{F}_p[X^2]$ . Recall that the set  $\overline{\mathcal{H}}_{f^m}$  is defined by

$$\overline{\mathcal{H}}_{f^m} = \{h \in \mathcal{H}_{f^m} \mid g(X^2) \text{ and } g^{\natural}(X^2) \text{ do not divide } h\}.$$

One first starts with a partition of  $\mathcal{H}_{fp^s}$  which generalizes Lemma 2 :

**Lemma 8** Consider  $p$  a prime number,  $\theta$  the Frobenius automorphism over  $\mathbb{F}_{p^2}$ ,  $R = \mathbb{F}_{p^2}[X; \theta]$ ,  $s \in \mathbb{N}$  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  $\mathbb{F}_p[X^2]$ .

$$\mathcal{H}_{fp^s} = \bigsqcup_{i=0}^{p^s} \bigsqcup_{j=0}^{p^s-i} g^i g^{\natural j} \cdot \overline{\mathcal{H}}_{fp^{s-(i+j)}}. \quad (17)$$

**Proof.** Consider  $h$  in  $\mathcal{H}_{fp^s}$  and  $i \in \{0, \dots, p^s\}, j \in \{0, \dots, p^s - i\}$  such that  $h = g(X^2)^i g^{\natural}(X^2)^j \cdot H$  where  $g(X^2)$  and  $g^{\natural}(X^2)$  do not divide  $H$ . One has  $h^{\natural} = g^{\natural}(X^2)^i g(X^2)^j \cdot H^{\natural}$ , therefore  $H^{\natural} \cdot H = f^{p^s-(i+j)}$  and  $h$  belongs to the set  $g(X^2)^i g^{\natural}(X^2)^j \cdot \overline{\mathcal{H}}_{fp^{s-(i+j)}}$ . Conversely, consider  $i \in \{0, \dots, p^s\}, j \in \{0, \dots, p^s - i\}$  and  $H$  in  $\overline{\mathcal{H}}_{fp^{s-(i+j)}}$ , then  $g(X^2)^i g^{\natural}(X^2)^j \cdot H$  belongs to  $\mathcal{H}_{fp^s}$ . Consider  $(i, j) \neq (i', j')$  with  $i > i' \in \{0, \dots, p^s\}, j \in \{0, \dots, p^s - i\}, j' \in \{0, \dots, p^s - i'\}$ ,  $u \in \overline{\mathcal{H}}_{fp^{s-(i+j)}}$ ,  $u' \in \overline{\mathcal{H}}_{fp^{s-(i'+j')}}$ . Assume that  $g(X^2)^i g^{\natural}(X^2)^j \cdot u = g(X^2)^{i'} g^{\natural}(X^2)^{j'} \cdot u'$ . If  $j \geq j'$  then  $g(X^2)$  divides  $u'$  which is impossible, therefore  $j < j'$ . Necessarily,  $g(X^2)$  divides  $g^{\natural}(X^2)^{j'-j} \cdot u'$ . As  $g(X^2)$  and  $g^{\natural}(X^2)$  both divide  $g^{\natural}(X^2)^{j'-j} \cdot u'$ , their lclm is also a divisor of  $g^{\natural}(X^2)^{\beta} \cdot u'$ . But  $g(X^2)$  and  $g^{\natural}(X^2)$  are right coprime and belong to  $\mathbb{F}_p[X^2]$  therefore their lclm coincides with their lcm i.e.  $g(X^2)g^{\natural}(X^2)$ . So one gets that  $g(X^2)$  divides  $g^{\natural}(X^2)^{j'-j-1} \cdot u'$ . After repeating the same argument one gets that  $g(X^2)$  divides  $g^{\natural}(X^2) \cdot u'$ . As  $g(X^2)$  and  $g^{\natural}(X^2)$  both divide  $g^{\natural}(X^2)u'$  their lclm  $g(X^2)g^{\natural}(X^2)$  divides  $g^{\natural}(X^2)u'$  therefore  $g(X^2)$  divides  $u'$ , contradiction.

■

In what follows one constructs the set  $\overline{\mathcal{H}}_{f^m}$  for  $f$  in  $\mathcal{G}$  and  $m$  greater than 1 (Lemma 9). This construction requires a generalization of Proposition 3 :

**Proposition 10** Consider  $p$  a prime number,  $\theta$  the Frobenius automorphism over  $\mathbb{F}_{p^2}$ ,  $R = \mathbb{F}_{p^2}[X; \theta]$ ,  $f(X^2) = g(X^2)g^{\natural}(X^2)$  in  $\mathbb{F}_p[X^2]$  with degree  $d$  in  $X^2$  where  $g(X^2) \neq g^{\natural}(X^2)$  is irreducible in  $\mathbb{F}_p[X^2]$ . Assume that  $h = h_1 \cdots h_m$  is a product of monic skew polynomials of degree  $d$  whose bound is  $f(X^2)$ . The following assertions are equivalent :

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

**Proof.** To simplify the presentation, one denotes  $f = f(X^2)$ ,  $g = g(X^2)$  and  $g^{\natural} = g^{\natural}(X^2)$ .

The implication (iii)  $\Rightarrow$  (ii) comes from the fact that  $g$  and  $g^{\natural}$  are central. Let us prove that (ii)  $\Rightarrow$  (i). If  $g$  divides  $h$ , then it divides  $h$  on the right so  $h$  has at least two distinct right factors  $u$  and  $v$  irreducible dividing  $g$ . As the bound of  $h_m$  is equal to  $f = gg^{\natural}$ , necessarily,  $h$  has an irreducible right factor  $w$  dividing  $g^{\natural}$ . The skew polynomials  $\text{lclm}(u, w)$  and  $\text{lclm}(v, w)$  are two right factors of  $h$  with degree  $d$  dividing  $f$ . According to Theorem 13 of [16], as  $u$  and  $w$  are irreducible and do not have the same bound, the lclm-decomposition  $\text{lclm}(u, w)$  is unique. Similarly, the lclm decomposition  $\text{lclm}(v, w)$  is unique. Furthermore,  $u$  and  $v$  are distinct, so the skew polynomials  $\text{lclm}(u, w)$  and  $\text{lclm}(v, w)$  are distinct.

Let us prove by induction on  $m$  that if  $h_1 \cdots h_m = g_1 \cdots g_m$  are two distinct decompositions of  $h$  into the product of monic skew polynomials whose bound is  $f$  and whose degree is  $d$ , then there are two consecutive factors whose product is divisible by  $g$  or  $g^\natural$ .

Consider  $h = h_1 \cdot h_2 = g_1 \cdot g_2$  where  $g_i, h_i$  are skew polynomials with degree  $d$  and with bound  $f$ . Assume that  $g$  and  $g^\natural$  do not divide  $h$ . Then  $\text{gcd}(h, g)$  is an irreducible skew polynomial of degree  $\delta$  dividing  $g$  which is also equal to  $\text{gcd}(h_2, g)$  and  $\text{gcd}(g_2, g)$ . Similarly,  $\text{gcd}(h_2, g^\natural) = \text{gcd}(g_2, g^\natural)$ . Furthermore, according to Theorem 4.1 of [6],  $h_2 = \text{lcm}(\text{gcd}(h_2, g), \text{gcd}(h_2, g^\natural))$  and  $g_2 = \text{lcm}(\text{gcd}(g_2, g), \text{gcd}(g_2, g^\natural))$ , therefore  $g_2 = h_2$  and  $(h_1, h_2) = (g_1, g_2)$ .

Consider  $m > 2$  and assume the property is true for  $m - 1$ . Consider two distinct decompositions of  $h$  into the product of monic skew polynomials with degree  $d$  and bound  $f$  :  $h = h_1 \cdots h_m = g_1 \cdots g_m$ . Therefore,  $h_i$  and  $g_j$  are products of two irreducible monic skew polynomials of degree  $\delta$  dividing  $g$  and  $g^\natural$ .

If  $\text{gcd}(h_m, g_m) = 1$  then  $\text{lcm}(h_m, g_m) = \bar{h}_{m-1} \cdot h_m$  divides  $h_1 \cdots h_m$  and  $\bar{h}_{m-1}$  is a monic skew polynomial of degree  $d$  dividing  $f$  which is the product of two irreducible monic skew polynomials of degree  $\delta$  dividing  $g$  and  $g^\natural$ . Consider  $H$  in  $R$  such that  $H\bar{h}_{m-1} = h_1 \cdots h_{m-1}$ . If  $\bar{h}_{m-1} = h_{m-1}$  then  $\text{lcm}(h_m, g_m) = h_{m-1} \cdot h_m$  has two factorizations into the product of two monic skew polynomials of degree  $d$  dividing  $f$ , therefore,  $g$  or  $g^\natural$  divides  $h_{m-1} \cdot h_m$ . Otherwise, as  $h_1, \dots, h_{m-1}, \bar{h}_{m-1}$  are the products of an irreducible polynomial dividing  $g$  and an irreducible polynomial dividing  $g^\natural$ ,  $H$  is the product of  $m - 2$  irreducible polynomials dividing  $g$  and  $m - 2$  skew polynomials dividing  $g^\natural$ . In particular,  $H$  divides  $g^{m-2}(g^\natural)^{m-2}$ . According to Theorem 4.1 of [6],  $H = \text{lcm}(G, \tilde{G})$  where  $G = \text{gcd}(H, g^{m-2})$  and  $\tilde{G} = \text{gcd}(H, (g^\natural)^{m-2})$ . As  $g$  (resp.  $g^\natural$ ) is irreducible in  $\mathbb{F}_p[X^2]$ , the skew polynomial  $G$  (resp.  $\tilde{G}$ ) is the product of  $N$  (resp.  $\tilde{N}$ ) monic irreducible skew polynomials dividing  $g$  (resp.  $g^\natural$ ). Without loss of generality, one can assume that  $N \leq \tilde{N}$ . Consider  $G = G_1 \cdots G_N$  (resp.  $\tilde{G} = \tilde{G}_1 \cdots \tilde{G}_{\tilde{N}}$ ) the factorization of  $G$  as the product of  $N$  (resp.  $\tilde{N}$ ) monic irreducible factors dividing  $g$  (resp.  $g^\natural$ ). As  $g$  (resp.  $g^\natural$ ) does not divide  $G$  (resp.  $\tilde{G}$ ), according to Proposition 3, these factorizations are unique. Therefore, according to Theorem 14 of [16],  $H = H_1 \cdots H_N$  where  $H_i = \text{lcm}(\overline{G_i}, \overline{\tilde{G}_i})$  with  $R/\overline{G_i}R$  and  $R/\overline{\tilde{G}_i}R$  (resp.  $R/\tilde{G}_iR$  and  $R/\tilde{G}_iR$ ) isomorphic modules. As  $G_i$  divides  $g$ , according to Corollary of Theorem 10 of [9],  $\overline{G_i}$  also divides  $g$ . As  $G_i$  and  $\tilde{G}_i$  are right coprime with same degree  $d/2$ ,  $\overline{G_i}$  and  $\overline{\tilde{G}_i}$  are also right coprime therefore  $H_i$  is a skew polynomial of degree  $d$  which divides  $f$ . Lastly, as  $H$  has degree  $(m - 2)d$  one gets  $N = m - 2$ . Therefore,  $H$  can be written as the product of  $m - 2$  monic skew polynomials of degree  $d$  dividing  $f$  and one can apply the induction hypothesis to  $H \cdot \bar{h}_{m-1}$ .

Assume that  $\text{gcd}(h_m, g_m) = u \neq 1$ . Necessarily  $u$  is an irreducible monic skew polynomial of degree  $\delta$  which divides  $g$  or  $g^\natural$ . Without loss of generality, one can assume that  $u$  divides  $g$ . Consider  $v$  such that  $\text{lcm}(g_m, h_m) = v \cdot h_m$  and  $H$  in  $R$  such that  $h_1 \cdots h_m = H \cdot v \cdot h_m$  i.e  $h_1 \cdots h_{m-1} = H \cdot v$ . Necessarily  $v$  is an irreducible monic skew polynomial of degree  $\delta$  dividing  $g^\natural$  and  $H = \tilde{h}_1 \cdots \tilde{h}_{m-2} \cdot w$  where  $w$  is an irreducible skew polynomial dividing  $g$ ,  $\tilde{h}_i$  is a product of two irreducible monic skew polynomials of degree  $\delta$  dividing  $g$  and  $g^\natural$ . If  $h_{m-1} = w \cdot v$ , then  $w \cdot \text{lcm}(g_m, h_m) = h_{m-1} \cdot h_m$  and one concludes that  $g$  or  $g^\natural$  divides  $h_{m-1} \cdot h_m$ . If  $h_{m-1} \neq w \cdot v$  then  $h_1 \cdots h_{m-1} = \tilde{h}_1 \cdots \tilde{h}_{m-2} \cdot (w \cdot v)$  where  $w \cdot v$  is a monic skew polynomial of degree  $d$  dividing  $f$ , and one concludes using the induction hypothesis. ■

**Remark 4** *The unique factorization of  $h$  in Proposition 10 below is the unique representation of  $h$  as the product of maximal completely reducible factors as it is defined in [16] page 498.*

If  $f(X^2)$  is irreducible in  $\mathbb{F}_p[X^2]$  (and  $f(X^2) \in R$  does not divide  $h$ ), then this factorization coincides with the factorization of  $h$  into irreducible monic skew polynomials.

Lemma 9 generalizes Lemma 7 (where  $\mathcal{F}$  is replaced with  $\mathcal{G}$ ). It uses the same type of arguments linked to the factorization of skew polynomials. The elements of  $\overline{\mathcal{H}}_{f^m}$  are constructed by using products of elements of  $\overline{\mathcal{H}}_f$ .

**Lemma 9** Consider  $p$  a prime number,  $\theta$  the Frobenius automorphism over  $\mathbb{F}_{p^2}$ ,  $R = \mathbb{F}_{p^2}[X; \theta]$ ,  $m$  a nonnegative integer and  $f = f(X^2)$  in  $\mathcal{G}$  with degree  $d = 2\delta > 1$  in  $X^2$ .

1. The constant coefficients of the elements of  $\overline{\mathcal{H}}_f$  are squares in  $\mathbb{F}_{p^2}$ .
2. The set  $\overline{\mathcal{H}}_{f^m}$  has  $(1 + p^\delta)p^{\delta(m-1)}$  elements and is equal to

$$\left\{ \left( h_1 \cdot \frac{1}{\nu_1} \right) \cdots \left( h_m \cdot \frac{1}{\nu_m} \right) \cdot \left( \prod_{j=1}^m \nu_j \right) \mid h_j \in \overline{\mathcal{H}}_f, \nu_j^2 = (h_j)_0, h_j \neq \nu_{j-1} h_{j-1}^\natural \cdot \frac{1}{\nu_{j-1}} \right\}.$$

**Proof.**

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

1. If  $p = 2$  the nonzero elements of  $\mathbb{F}_{p^2}$  are squares. Assume that  $p$  is an odd prime number. Consider  $h$  in  $\overline{\mathcal{H}}_{f^m}$  with constant term  $h_0$ ,  $A(Z)$  and  $B(Z)$  defined in (9). Like in point 1. of Lemma 7, if  $B(Z)$  and  $f(Z)$  are coprime then  $h_0^{p+1} = 1$  so  $h_0$  is a square in  $\mathbb{F}_{p^2}$ . If  $B(Z)$  and  $f(Z)$  are not coprime, then according to Lemma 4,  $\delta$  is necessarily odd and  $A(Z) = \tilde{g}(Z)\Theta(\tilde{g}^\natural)(Z)$  or  $A(Z) = \tilde{g}^\natural(Z)\Theta(\tilde{g})(Z)$  where  $g(Z) = \tilde{g}(Z)\Theta(\tilde{g})(Z)$  is the factorization of  $g(Z)$  in  $\mathbb{F}_{p^2}[Z]$ . Denote  $\mu$  the constant coefficient of  $\tilde{g}(Z)$ , then the constant coefficient  $h_0$  of  $A(Z)$  is such that  $h_0 = \mu/\mu^p = 1/\mu^{p-1}$  if  $A(Z) = \tilde{g}(Z)\Theta(\tilde{g}^\natural)(Z)$  or such that  $h_0 = \mu^p/\mu = \mu^{p-1}$  if  $A(Z) = \tilde{g}^\natural(Z)\Theta(\tilde{g})(Z)$ , therefore  $h_0$  is a square in  $\mathbb{F}_{p^2}$ .
2. Like in Lemma 7, it suffices to prove that  $\overline{\mathcal{H}}_{f^m} =$

$$\left\{ H_1 \cdots H_m \mid \frac{1}{\mu_i} H_i^\natural \cdot \mu_i \cdot H_i = f, \mu_i = (H_1 \cdots H_{i-1})_0, H_{i+1} \neq \frac{1}{\mu_i} H_i^\natural \cdot \mu_i, g, g^\natural \right\}.$$

Consider  $h$  in  $\overline{\mathcal{H}}_{f^m}$ . Let us prove that  $h$  can be written as the product of  $m$  monic skew polynomials with degree  $d$  and with bound  $f$ . As  $h$  divides  $f^m$ , according to Theorem 4.1 of [6],  $h = \text{lcm}(G, \tilde{G})$  where  $G = \text{gcd}(h, g^m)$  and  $\tilde{G} = \text{gcd}(h, (g^\natural)^m)$ . As  $g$  (resp.  $g^\natural$ ) is irreducible in  $\mathbb{F}_p[X^2]$ , the skew polynomial  $G$  (resp.  $\tilde{G}$ ) is the product of  $N$  (resp.  $\tilde{N}$ ) monic irreducible skew polynomials dividing  $g$  (resp.  $g^\natural$ ). Without loss of generality, one can assume that  $N \leq \tilde{N}$ . Consider  $G = G_1 \cdots G_N$  (resp.  $\tilde{G} = \tilde{G}_1 \cdots \tilde{G}_{\tilde{N}}$ ) the factorization of  $G$  as the product of  $N$  (resp.  $\tilde{N}$ ) monic irreducible factors dividing  $g$  (resp.  $g^\natural$ ). According to Proposition 3, as  $g$  (resp.  $g^\natural$ ) does not divide  $G$  (resp.  $\tilde{G}$ ), these factorizations are unique. Therefore, according to Theorem 14 of [16],  $h = H_1 \cdots H_N$  where  $H_i = \text{lcm}(\overline{G_i}, \tilde{G}_i)$  with  $R/\overline{G_i}R$  and  $R/\tilde{G}_iR$  (resp.  $R/\overline{G_i}R$  and  $R/\tilde{G}_iR$ ) isomorphic modules. As  $\tilde{G}_i$  divides  $g$ , according to Corollary of Theorem 10 of [9],  $\overline{G_i}$  also divides  $g$ . As  $G_i$  and  $\tilde{G}_i$  are right coprime with same degree  $d/2$ ,  $\overline{G_i}$  and  $\tilde{G}_i$  are also coprime therefore  $H_i$  is a skew polynomial of degree  $d$  which divides  $f$ . Lastly, the degree of  $h$  is equal to  $m \times d$  and one gets  $N = m$ . Therefore

$$h = \prod_{i=1}^m H_i, H_i \text{ monic, } \deg(H_i) = d, H_i \text{ divides } f, H_i \neq g, H_i \neq g^{\natural}.$$

Consider  $\mu_i = (H_1 \cdots H_{i-1})_0$  the constant coefficient of  $H_1 \cdots H_{i-1}$ . Using an induction argument, one has :

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

By hypothesis  $h^{\natural} \cdot h = f^m$ , therefore

$$\left( \frac{1}{\mu_m} H_m^{\natural} \cdot \mu_m \right) \cdots \left( \frac{1}{\mu_2} H_2^{\natural} \cdot \mu_2 \right) \cdot \left( \frac{1}{\mu_1} H_1^{\natural} \cdot \mu_1 \right) \cdot H_1 \cdot H_2 \cdots H_m = f^m$$

is the product of  $2m$  monic factors with degree  $d$  and with bound  $f$ . As  $f^m$  is central, the above decomposition is not unique. Therefore, according to Proposition 10, there exists two consecutive factors in  $h^{\natural} \cdot h$  whose product is divisible by  $g$  or  $g^{\natural}$ . Such a product can be of three types :  $\left( \frac{1}{\mu_{i+1}} H_{i+1}^{\natural} \cdot \mu_{i+1} \right) \cdot \left( \frac{1}{\mu_i} H_i^{\natural} \cdot \mu_i \right)$ ,  $H_i \cdot H_{i+1}$  or  $\frac{1}{\mu_1} H_1^{\natural} \cdot \mu_1 \cdot H_1$ . However  $g$  and  $g^{\natural}$  do not divide  $H_i \cdot H_{i+1}$ , otherwise, they would divide  $h$ , and they do not divide  $\frac{1}{\mu_{i+1}} H_{i+1}^{\natural} \cdot \mu_{i+1} \frac{1}{\mu_i} H_i^{\natural} \cdot \mu_i = \frac{1}{\mu_i} (H_i \cdot H_{i+1})^* \mu_i$  either. Therefore  $g$  or  $g^{\natural}$  divides  $\frac{1}{\mu_1} H_1^{\natural} \cdot \mu_1 \cdot H_1$ . As  $g$  is central, one gets that  $g$  and  $g^{\natural}$  divide  $\frac{1}{\mu_1} H_1^{\natural} \cdot \mu_1 \cdot H_1$ , therefore  $f$  divides  $\frac{1}{\mu_1} H_1^{\natural} \cdot \mu_1 \cdot H_1$  and as these two skew polynomials are monic with the same degree they are equal. By induction, one gets

$$\frac{1}{\mu_i} H_i^{\natural} \cdot \mu_i \cdot H_i = f, H_{i+1} \neq \frac{1}{\mu_i} H_i^{\natural} \cdot \mu_i, g, g^{\natural}.$$

Conversely, consider  $h = \prod_{i=1}^m H_i$ , with  $\frac{1}{\mu_i} H_i^{\natural} \cdot \mu_i \cdot H_i = f$ ,  $H_{i+1} \neq \frac{1}{\mu_i} H_i^{\natural} \cdot \mu_i, g, g^{\natural}$ . One

has  $h^{\natural} = \prod_{i=0}^{m-1} \frac{1}{\mu_{m-i}} H_{m-i}^{\natural} \cdot \mu_{m-i}$  therefore  $h^{\natural} \cdot h = f^m$ . It remains to prove that  $g$  and  $g^{\natural}$  do not divide  $h$ . Assume that  $g$  divides  $h$ , all the skew factors  $H_i$  in the decomposition of  $h$  are monic, with degree  $d$ , divide  $f$  and are distinct of  $g, g^{\natural}$ , therefore, according to Proposition 10, there exists  $i$  such that  $g$  divides  $H_i \cdot H_{i+1}$ . Consider  $u$  in  $R$  such that  $H_i \cdot H_{i+1} = g \cdot u$ . As both  $H_i$  and  $H_{i+1}$  divide  $f$  without dividing  $g$  or  $g^{\natural}$ , they are the products of two irreducible polynomials dividing respectively  $g$  and  $g^{\natural}$ , therefore the skew polynomial  $u$  is the product of two irreducible skew polynomials both dividing  $g^{\natural}$  and  $u$  divides  $(g^{\natural})^2$ . The relation  $(H_i \cdot H_{i+1})^* = (g^{\natural} \cdot u)^*$  gives  $H_{i+1}^{\natural} \cdot \lambda_i H_i^{\natural} = \lambda_i u^{\natural} \cdot g^{\natural}$  where  $\lambda_i$  is the constant coefficient of  $H_i$ . Multiplying the above equality on the left by  $\mu_{i+1} H_{i+1} \cdot \frac{1}{\mu_{i+1}}$  and on the right by  $\mu_i H_i \cdot \frac{1}{\mu_i}$  yields  $f^2 = \left( \frac{1}{\lambda_i} \mu_{i+1} H_{i+1} \cdot \frac{1}{\mu_{i+1}} \lambda_i u^{\natural} \cdot g^{\natural} \cdot \mu_i \right) \cdot \left( H_i \cdot \frac{1}{\mu_i} \right)$ . As  $f^2$  is central, the two terms of the product commute and  $f^2 = H_i \cdot \left( \frac{1}{\mu_i} \frac{1}{\lambda_i} \mu_{i+1} \right) H_{i+1} \cdot \left( \frac{1}{\mu_{i+1}} \lambda_i \right) u^{\natural} \cdot g^{\natural} \cdot \mu_i = H_i \cdot H_{i+1} \cdot \frac{1}{\mu_i} \cdot u^{\natural} \cdot g^{\natural} \cdot \mu_i = g \cdot u \cdot \frac{1}{\mu_i} \cdot u^{\natural} \cdot g^{\natural} \cdot \mu_i$  therefore  $\left( u \cdot \frac{1}{\mu_i} \cdot u^{\natural} \cdot \mu_i \right) \cdot g^{\natural} = g \cdot (g^{\natural})^2 = u \cdot v \cdot g$ , where  $v$  in  $R$  is such that  $u \cdot v = (g^{\natural})^2$ . One gets the relation  $\frac{1}{\mu_i} u^{\natural} \cdot \mu_i \cdot g^{\natural} = v \cdot g$ . The skew polynomials  $g$  and  $g^{\natural}$  divide  $v \cdot g$  and  $\deg(v \cdot g) = \deg(f)$ , therefore  $f = v \cdot g$ ,  $v = g^{\natural}$  and  $u = g^{\natural}$  which is impossible because  $H_i \cdot H_{i+1} \neq f$ .

|   |   |  |
|---|---|--|
| Lemma 3 and<br>Cauchy in-<br>terpolation<br>(Lemma 6) | Decomposition<br>into the products<br>of elements of $\overline{\mathcal{H}}_f$<br>(Proposition 10) | Partition<br>(Lemma 8)   |
| ↓   | ↓   | ↓  |
| $\overline{\mathcal{H}}_f$ (Proposition 7)            | → $\overline{\mathcal{H}}_{f^m}$ (Lemma 9)  | → <span style="border: 1px solid black; padding: 2px;"><math>\mathcal{H}_{fp^s}</math> (Proposition 11)</span> |

Table 5: Main steps of the construction of  $\mathcal{H}_{fp^s}$  for  $f$  in  $\mathcal{G}$

The number of elements of  $\overline{\mathcal{H}}_{f^m}$  follows from the fact that  $\overline{\mathcal{H}}_f$  has  $1 + p^\delta$  elements (Proposition 7).

■

The construction of the set  $\mathcal{H}_{fp^s}$  for  $f$  in  $\mathcal{G}$  is deduced from Lemma 8 and Lemma 9. The whole construction is illustrated in Table 5.

**Proposition 11** Consider  $p$  a prime number,  $\theta$  the Frobenius automorphism over  $\mathbb{F}_{p^2}$ ,  $R = \mathbb{F}_{p^2}[X; \theta]$ ,  $s$  a nonnegative integer and  $f = f(X^2)$  in  $\mathcal{G}$  with degree  $d = 2\delta > 1$  in  $X^2$ . The set  $\mathcal{H}_{fp^s}$  has  $\frac{(p^{\delta(p^s+1)} - 2p^s - 3)(1 + p^\delta) + 4p^s + 4}{(p^\delta - 1)^2}$  elements.

**Proof.**

Consider  $f = f(X^2) = g(X^2)g^\natural(X^2)$  in  $\mathcal{G}$ , then according to Lemma 8, one has the partition

$$\mathcal{H}_{fp^s} = \bigsqcup_{i=0}^{p^s} \bigsqcup_{j=0}^{p^s-i} g(X^2)^j g^\natural(X^2)^{i-j} \cdot \overline{\mathcal{H}}_{fp^{s-i-j}} .$$

Furthermore, according to Lemma 9,

the set  $\overline{\mathcal{H}}_{f^m}$  has  $(p^\delta + 1)p^{\delta(m-1)}$  if  $m \geq 1$  and 1 element if  $m = 0$ . Therefore the number of elements of the set  $\mathcal{H}_{fp^s}$  is

$$\sum_{i=0}^{p^s} \left[ \sum_{j=0}^{p^s-i-1} (1 + p^\delta)(p^\delta)^{p^s-i-1-j} + 1 \right] = \frac{(p^{\delta(p^s+1)} - 2p^s - 3)(1 + p^\delta) + 4p^s + 4}{(p^\delta - 1)^2} .$$

■

**Example 9** Consider  $\mathbb{F}_4 = \mathbb{F}_2(a)$ ,  $\theta : x \mapsto x^2$  and  $f = f(X^2) = (X^6 + X^2 + 1)(X^6 + X^4 + 1) \in \mathcal{G}$  with degree  $d = 6$  in  $X^2$ . According to Proposition 11, the set  $\mathcal{H}_{f^2}$  has 93 elements. More precisely,

$$\begin{aligned} \mathcal{H}_{f^2} = & \overline{\mathcal{H}}_{f^2} \sqcup (X^6 + X^2 + 1)\overline{\mathcal{H}}_f \sqcup (X^6 + X^4 + 1)\overline{\mathcal{H}}_f \\ & \sqcup \{(X^6 + X^2 + 1)^2, (X^6 + X^4 + 1)^2, (X^6 + X^2 + 1)(X^6 + X^4 + 1)\}. \end{aligned}$$

There are 9 elements in  $\overline{\mathcal{H}}_f = \mathcal{H}_f \setminus \{X^6 + X^2 + 1, X^6 + X^4 + 1\}$  (see example 6) and  $72 = (1 + 2^3) \times 2^3$  skew polynomials in  $\overline{\mathcal{H}}_{f^2}$ . Here is one of these elements :  $h = X^{12} + aX^{11} + a^2X^{10} + a^2X^7 + a^2X^6 + X^5 + a^2X^2 + aX + a = (h_1 \cdot \frac{1}{\nu_1}) \cdot (h_2 \cdot \frac{1}{\nu_2}) \cdot (\nu_1\nu_2)$  where  $h_1 = X^6 + X^5 + aX^3 + a^2X + a, h_2 = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$  are two elements of  $\overline{\mathcal{H}}_f, \nu_1 = a^2$  is the square root of the constant coefficient of  $h_1$  and  $\nu_2 = 1$ .

### 5.3 Conclusion

The following theorem gives the number of self-dual  $\theta$ -cyclic and  $\theta$ -negacyclic codes of any dimension  $k$  over  $\mathbb{F}_{p^2}$  for  $p$  prime number and  $\theta$  Frobenius automorphism. Tables 6 and 7 illustrate this theorem over  $\mathbb{F}_4$  for  $k = 2^s \times t$  and  $t \in \{1, 3, 5, 7, 9\}$  and over  $\mathbb{F}_9$  for  $k = 3^s \times t$  and  $t \in \{1, 2, 4, 5, 7\}$ .

**Theorem 1** Consider  $p$  prime number,  $\theta$  the Frobenius automorphism over  $\mathbb{F}_{p^2}$ ,  $k$  a positive integer,  $\varepsilon$  in  $\{-1, 1\}$ ,  $s, t$  two integers such that  $k = p^s \times t$  and  $p$  does not divide  $t$ . The number of self-dual  $(\theta, \varepsilon)$ -constacyclic codes of dimension  $k$  over  $\mathbb{F}_{p^2}$  is

$$N_\varepsilon \times \prod_{f \in \mathcal{F}_{k,\varepsilon}} \frac{p^{\delta(p^s+1)} - 1}{p^\delta - 1} \times \prod_{f \in \mathcal{G}_{k,\varepsilon}} \frac{(p^{\delta(p^s+1)} - 2p^s - 3)(1 + p^\delta) + 4p^s + 4}{(p^\delta - 1)^2}$$

where

$$N_1 = \begin{cases} 0 & \text{if } k \equiv 1 \pmod{2} \text{ and } p \equiv 1 \pmod{4} \\ & \text{or } k \equiv 0 \pmod{2} \text{ and } p \text{ odd} \\ 1 & \text{if } s = 0 \text{ and } p = 2 \\ 3 & \text{if } s > 0 \text{ and } p = 2 \\ 2 \frac{p^{(p^s+1)/2} - 1}{p - 1} & \text{if } k \equiv 1 \pmod{2} \text{ and } p \equiv 3 \pmod{4} \end{cases}$$

and

$$N_{-1} = \begin{cases} 0 & \text{if } k \equiv 1 \pmod{2} \text{ and } p \equiv 3 \pmod{4} \\ 1 & \text{if } k \equiv 0 \pmod{2} \text{ and } p \text{ odd} \\ 2 \frac{p^{(p^s+1)/2} - 1}{p - 1} & \text{if } k \equiv 1 \pmod{2} \text{ and } p \equiv 1 \pmod{4}. \end{cases}$$

**Proof.** According to Proposition 5, the number of self-dual  $(\theta, \varepsilon)$ -constacyclic codes over  $\mathbb{F}_{p^2}$  with dimension  $k$  is

$$\#\mathcal{H}_{X^{2k-\varepsilon}} = N_\varepsilon \times \prod_{f \in \mathcal{F}_{k,\varepsilon}} \#\mathcal{H}_{fp^s} \times \prod_{f \in \mathcal{G}_{k,\varepsilon}} \#\mathcal{H}_{fp^s}$$

where  $N_\varepsilon$  satisfies the above conditions. The final result follows from Proposition 9 and Proposition 11. ■

**Remark 5** Proposition 4 is a particular case of Theorem 1 for  $t = 1$  while Proposition 8 is a particular case for  $s = 0$ .



| Dimension      | cyclic            | $\theta$ -cyclic  |
|----------------|-------------------|---|
| $2^s$          | 1                 | 3 ([3])   |
| $3 \times 2^s$ | $1 + 2^{s+1}$     | $3 \times (2^{2s+1} - 1)$                                 |
| $5 \times 2^s$ | 1                 | $4^{2s+1} - 1$  |
| $7 \times 2^s$ | $1 + 2^{s+1}$     | $3 \times (9 \times 8^{2s+1} - 7 \times 2^{s+1} - 23)/49$ |
| $9 \times 2^s$ | $(1 + 2^{s+1})^2$ | $3 \times (2^{2s+1} - 1) \times (8^{2s+1} - 1)/7$         |

Table 6: Number of self-dual cyclic codes (Theorem 3.6 of [11]) and self-dual  $\theta$ -cyclic codes (Theorem 1) over  $\mathbb{F}_4$  in dimension  $t \times 2^s$  with  $s \in \mathbb{N}^*$ ,  $t \in \{1, 3, 5, 7, 9\}$  and  $\theta : x \mapsto x^2$

| Dimension      | $\theta$ -cyclic                                 | $\theta$ -negacyclic                           |
|----------------|--|--|
| $3^s$          | $3^{(3^s+1)/2} - 1$                              | 0  |
| $2 \times 3^s$ | 0  | $(3^{3^s+1} - 1)/2$                            |
| $4 \times 3^s$ | 0  | $(5 \times 9^{3^s+1} - 8 \times 3^s - 13)/2^5$ |
| $5 \times 3^s$ | $(3^{(3^s+1)/2} - 1) \times (9^{3^s+1} - 1)/8$   | 0  |
| $7 \times 3^s$ | $(3^{(3^s+1)/2} - 1) \times (27^{3^s+1} - 1)/26$ | 0  |

Table 7: Number of self-dual  $\theta$ -cyclic and  $\theta$ -negacyclic codes (Theorem 1) over  $\mathbb{F}_9$  in dimensions  $t \times 3^s$  with  $s \in \mathbb{N}$ ,  $t \in \{1, 2, 4, 5, 7\}$  and  $\theta : x \mapsto x^3$ .

## 6 Conclusion and perspectives

This text provides a construction and an enumeration of Euclidean self-dual  $\theta$ -cyclic and  $\theta$ -negacyclic codes over  $\mathbb{F}_{p^2}$  where  $p$  is a prime number and  $\theta$  is the Frobenius automorphism. The main ingredient of this study relies on the adaptation of Sloane and Thompson approach ([19]) to solve the self-dual skew equation over  $\mathbb{F}_{p^2}[X; \theta]$ . Some comparisons with the number of cyclic and negacyclic codes with the same dimensions are also provided.

This construction should be generalized to Hermitian self-dual  $\theta$ -negacyclic codes over  $\mathbb{F}_{p^2}$  (work in progress). However, the question of the enumeration of self-dual skew codes over  $\mathbb{F}_{p^e}$  with  $e$  greater than 2 remains open. Namely, many properties in this text are specific to the ring  $\mathbb{F}_{p^2}[X; \theta]$  and a new approach should be adopted to hope a generalization. Lastly, a lot of work still remains in the study of the minimal distances of the codes constructed in this text.

### Acknowledgments

I thank Felix Ulmer for his encouragement and the referees for helpful suggestions to improve the construction of the text.

## References

- [1] Bakshi, G. K. and Raka, M., *Self-dual and self-orthogonal negacyclic codes of length  $2p^n$  over a finite field*, Finite Fields and their Applications, 19, 2013, 39–54
- [2] Boucher, D., Geiselmann W. and Ulmer, F.

*Skew-cyclic codes*, Applicable Algebra in Engineering, Communication and Computing, Vol 18, 2007, No 4, 379–389

- [3] Boucher D. and Ulmer F. *Self-dual skew codes and factorization of skew polynomials* Journal of Symbolic Computation, Volume 60, January 2014, Pages 4761
- [4] Caruso X. and Leborgne J. *Some algorithms for skew polynomials over finite fields* arXiv:1212.3582, 2012
- [5] Dinh H. Q. *Repeated-root constacyclic codes of length  $2p^s$*  Finite Fields and Their Applications 18 (2012) 133-143
- [6] Giesbrecht, M., *Factoring in skew-polynomial rings over finite fields*. J. Symbolic Comput. 1998, 26 (4), 463–486.
- [7] Guenda K. and Gulliver T.A. *Self-dual Repeated Root Cyclic and Negacyclic Codes over Finite Fields* 2012 IEEE International Symposium on Information Theory Proceedings
- [8] Han S. and Kim J.-L. and Lee H. and Lee Y., *Construction of quasi-cyclic self-dual codes*, Finite Fields and their Applications, 18, 2012, 3, 613–633
- [9] Jacobson, N. *The Theory of Rings* Mathematical Surveys and Monographs, Vol 2, American Mathematical Society, 1943
- [10] Jia, S., Ling S. and Xing C. *On Self-Dual Cyclic Codes Over Finite Fields*, IEEE Transactions on Information Theory, Vol. 57, No. 4, 2011
- [11] Kai, X. and Zhu, S., *On cyclic self-dual codes*, Applicable Algebra in Engineering, Communication and Computing, 19, 2008, 6, 509–525,
- [12] Lidl, R. and Niederreiter, H., 1983. *Finite fields*. Vol. 20 of Encyclopedia of Mathematics and its Applications. Book Program, Reading, MA, with a foreword by P. M. Cohn.
- [13] Ling S. and Solé P., *On the algebraic structure of quasi-cyclic codes. I. Finite fields*, IEEE Trans. Inform. Theory, 47, 2001, 7, 2751–2760
- [14] Ling S., Niederreiter H. and Solé P., *On the algebraic structure of quasi-cyclic codes IV : Repeated Roots Chain rings*, Designs, Codes and Cryptography., 38, 2006, 337–361
- [15] Odoni, R. W. K. *On additive polynomials over a finite field* Proceedings of the Edinburgh Mathematical Society (199) 42, 1-16
- [16] Ore O., *Theory of Non-Commutative Polynomials*, *The Annals of Mathematics*, 2nd Ser, Vol. 34, No. 3. pp 480-508 (1933)
- [17] Sahni A. and Sehgal, P. T., *Enumeration of self-dual and self-orthogonal negacyclic codes over finite fields*, Advances in Mathematics of Communications,9, 2015,4,437–447,
- [18] Siap I., Abualrub, T., Aydin N. and Seneviratne P., *Skew cyclic codes of arbitrary length*, Int. J. Inf. Coding Theory, 2, 2011, 1, 10–20
- [19] Sloane, N. J. A. and Thompson, J. G., *Cyclic self-dual codes*, IEEE Trans. Inform. Theory, Vol 29, 1983, No 3, pp 364–366, ISSN = 0018-9448

[20] von zur Gathen, J. and Gerhard, J., *Modern computer algebra*, Cambridge University Press, Cambridge, 2013