Construction and number of self-dual skew codes over F_p^2

Delphine Boucher

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

D. Boucher *

December 4, 2014

Abstract

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

1 Introduction

Self-dual codes have been extensively studied for their practical and theoretical importance. Cyclic, negacyclic and quasi-cyclic self-dual codes were investigated over finite fields in many ways ([1, 6, 8, 9, 11, 12, 14]). There is no cyclic self-dual code over $\mathbb{F}_q$ when q is odd, and the number of self-dual cyclic codes over $\mathbb{F}_{2^r}$ is given in Theorem 3.6 of [12] (see also [11]). For p prime number, negacyclic self-dual codes of dimension p^s over $\mathbb{F}_q$ are constructed and counted in Corollary 3.3 of [6] when $q = p^r$ and in Theorems 3 and 4 of [1] when q is prime to p.

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

Over $\mathbb{F}_{p^2}$, θ-cyclic codes form, up to equivalence, a subclass of the class of 2-quasi-cyclic codes ([18]). The number of self-dual 2-quasi-cyclic codes of dimension prime to p over fields of characteristic p is given in Proposition 6.2 of [14]. A construction (without counting formula) of self-dual 2-quasi-cyclic codes of dimension not prime to p is given in Theorem 6.2 of [15].

Self-dual θ-cyclic and θ-negacyclic codes of dimension k are characterized by the equations $h^{\natural}h = X^{2k} - \epsilon$ in $\mathbb{F}_{p^2}[X;\theta]$ where h is the skew check polynomial of the code and $h^{\natural}$ is the left skew reciprocal polynomial of h. The solutions of this equation are constructed in [Proposition 28 of [4]] as least common right multiples of intermediate skew polynomials which satisfy equations of the type $h^{\natural}h = f(X^2)^{p^s}$ where $f(Y) \in \mathbb{F}_p[Y]$ is a self-reciprocal polynomial either irreducible or product of two distinct irreducible polynomials. In the particular case when $p = 2$ and $f(X^2) = X^2+1$, these equations were solved for any s in [4] using factorization properties of h. This led to the characterization of self-dual skew codes of dimension 2^s over $\mathbb{F}_4$. In the general case, up to now, these intermediate skew polynomials were determined by solving the polynomial systems satisfied by their coefficients for fixed values of s. In this text, one gives a new construction of these intermediate skew polynomials which enables to obtain a counting formula for self-dual skew codes. The main ingredients to achieve this goal are some factorization properties of skew polynomials in $\mathbb{F}_{p^2}[X;\theta]$ and Cauchy interpolations in $\mathbb{F}_{p^2}[Z]$.

*IRMAR, CNRS, UMR 6625, Université de Rennes 1, Université européenne de Bretagne, Campus de Beaulieu, F-35042 Rennes

The text is organized as follows. In section 2 some facts about self-dual skew codes are recalled. In section 3 a strategy for constructing and counting self-dual θ-cyclic and θ-negacyclic codes over $\mathbb{F}_{p^2}$ for p prime number and θ the Frobenius automorphism is set up. It is based on the resolution in $R = \mathbb{F}_{p^2}[X;\theta]$ of the equation $h^\natural h = X^{2k} - \epsilon$ where $h^\natural$ is the left skew reciprocal polynomial of h. This equation can be reduced to intermediate equations $h^\natural h = f(X^2)^{p^s}$ where $f(Y) \in \mathbb{F}_p[Y]$ (Proposition 28 of [4]) . The main idea is to split this equation into a finite number of equations of the type $h^\natural h = f(X^2)^m$ where h and $f(X^2)$ have no common non constant factor in $R \cap \mathbb{F}_p[X^2]$. In section 4, the equations $h^\natural h = (X^2 - \epsilon)^m$ are considered for p odd prime and this leads to a first counting formula, for self-dual θ-cyclic and θ-negacyclic codes over $\mathbb{F}_{p^2}$ with dimension a power of p (Proposition 2) . This construction generalizes the construction for $p = 2$ given in [4]. Some experimental results and a conjecture about the weight enumerators of these codes are also given. In section 5, the equations $h^\natural h = f(X^2)^m$ for f of degree > 1 are then considered. For $m = 1$, this equation is solved by Cauchy interpolation problems in $\mathbb{F}_{p^2}[Z]$ whereas for $m > 1$ one uses factorization properties of h. Lastly in section 6, the number of self-dual θ-cyclic and θ-negacyclic codes with any dimension is obtained (Theorem 1) and some perspectives are given.

2 Generalities on self-dual skew codes

For a finite field $\mathbb{F}_q$ and θ an automorphism of $\mathbb{F}_q$ we consider 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 basic rule $X \cdot a = \theta(a)\, X$ $(a \in \mathbb{F}_q)$ and extended to all elements of R by associativity and distributivity. The noncommutative ring R is called a skew polynomial ring or Ore ring (cf. [17]) and its elements are skew polynomials. 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 algorithm. The center of R is the commutative polynomial ring $Z(R) = \mathbb{F}_q^\theta[X^{|\theta|}]$ where $\mathbb{F}_q^\theta$ is the fixed field of θ and $|\theta|$ is the order of θ. The **bound** $B(h)$ of $h \in R$ with a nonzero constant term is the monic skew polynomial f with a non zero constant term belonging to $\mathbb{F}_q^\theta[X^{|\theta|}]$ of minimal degree such that h divides f on the right in R.

Definition 1 (definition 2 of [2] or definition 1 of [4]) *A* **module θ-code** *(or module skew code) $\mathcal{C}$ is a left R-submodule $Rg/Rf \subset R/Rf$ in the basis $1, X, \ldots, X^{n-1}$ where $g \in R = \mathbb{F}_q[X;\theta]$ and f is a left multiple of g in R of degree n. If there exists an $a \in \mathbb{F}_q \setminus \{0\}$ such that g divides $X^n - a$ on the right, then the code $\mathcal{C}$ is* **(θ,a)-constacyclic**. *If $a = 1$, the code is* **θ-cyclic** *and if $a = -1$, it is* **θ-negacyclic**. *The skew polynomial g is called* **skew generator polynomial** *of $\mathcal{C}$.*

If θ is the identity then a θ-cyclic (resp. θ-negacyclic) code is a cyclic code (resp. negacyclic) code.

The **(Euclidean) dual** of a linear code C of length n over $\mathbb{F}_q$ is defined with the **Euclidean scalar product** $< x, y >= \sum_{i=1}^n x_i y_i$ in $\mathbb{F}_q^n$ as $C^\perp = \{x \in \mathbb{F}_q^n \mid \forall y \in C, < x, y >= 0\}$. A linear code C over $\mathbb{F}_q$ is **Euclidean self-dual** or **self-dual** if $C = C^\perp$. To characterize self-dual module θ-codes, the skew reciprocal polynomial of a skew polynomial (definition 3 of [4]) and also the left monic skew reciprocal polynomial will be useful.

Definition 2 ([4], Definition 2) *The* **skew reciprocal polynomial** *of* $h = \sum_{i=0}^{d} h_i\, X^i \in R$ *of degree* d *is* $h^* = \sum_{i=0}^{d} X^{d-i} \cdot h_i = \sum_{i=0}^{d} \theta^i(h_{d-i})\, X^i$. *The* **left monic skew reciprocal polynomial** *of* h *is* $h^\natural := \frac{1}{\theta^d(h_0)} \cdot h^*$. *The polynomial* h *is* **self-reciprocal** *if* $h = h^\natural$.

According to Corollary 1 of [4], a module θ-code with skew generator polynomial $g \in R$ monic of degree k is self-dual if and only if there exists $h \in R$ monic (called **skew check polynomial** of the code) such that $g = h^\natural$ and

$$h^\natural h = X^{2k} - \varepsilon \text{ with } \varepsilon \in \{-1, 1\}. \tag{1}$$

In particular a self-dual θ-code must be either θ-cyclic or θ-negacyclic.

Some properties of the skew reciprocal polynomial and the left skew reciprocal polynomial will be useful (see also Lemma 24 of [4]).

Lemma 1 *Consider* $R = \mathbb{F}_q[X;\theta]$ *where* q *is a prime power,* θ *an automorphism of* $\mathbb{F}_q$ *and* Θ *is the morphism defined on* R *by* $\Theta(\sum a_i X^i) = \sum \theta(a_i) X^i$.

1. *For* $f, g \in R$, $(fg)^* = \Theta^k(g^*) f^*$, *where* $k = \deg(f)$.
2. *For* $f \in \mathbb{F}_q^\theta[X^{|\theta|}], g \in R$, $(fg)^* = (gf)^* = f^* g^*$ *and* $(fg)^\natural = f^\natural g^\natural$.
3. *Consider* $h = h_1 \cdots h_m \in R$ *where for* $i = 1, \ldots, m$, h_i *is a monic skew polynomial of* R *with degree* d *and constant coefficients* λ_i. *Then*

$$h^\natural = \prod_{i=m}^{1} \Theta^{d(i-1)} \left(\frac{1}{\theta^d(\mu_i)} \cdot h_i^\natural \cdot \mu_i \right)$$

with $\mu_i = \lambda_1 \cdots \lambda_{i-1}$ *and* $\mu_1 = 1$.

Proof. Point 1 is in Lemma 4 of [4] and Point 2. is deduced from it. Point 3. is a generalization of Lemma 24 of [4]. For $m = 1$, the property is true. Consider m an integer ≥ 2 and assume that the property is true for $m-1$. Consider $h = h_1 \cdots h_m$ and $H = h_1 \cdots h_{m-1}$.

$$\begin{aligned}
h^\natural &= \frac{1}{\theta^{md}(\mu_{m+1})} (H h_m)^* = \frac{1}{\theta^{md}(\mu_{m+1})} \Theta^{(m-1)d}(h_m^*) \cdot H^* \\
&= \frac{1}{\theta^{md}(\mu_{m+1})} \cdot \Theta^{(m-1)d} \left(\theta^d(\lambda_m) h_m^\natural \right) \cdot \theta^{(m-1)d}(\mu_m) \cdot H^\natural \\
&= \frac{1}{\theta^{md}(\mu_m)} \cdot \Theta^{(m-1)d} \left(h_m^\natural \right) \cdot \theta^{(m-1)d}(\mu_m) \cdot H^\natural \\
&= \Theta^{(m-1)d} \left(\frac{1}{\theta^d(\mu_m)} h_m^\natural \mu_m \right) \cdot \prod_{i=m-1}^{1} \Theta^{d(i-1)} \left(\frac{1}{\theta^d(\mu_i)} h_i^\natural \mu_i \right) \\
&= \prod_{i=m}^{1} \Theta^{d(i-1)} \left(\frac{1}{\theta^d(\mu_i)} \cdot h_i^\natural \cdot \mu_i \right).
\end{aligned}$$

■

To solve the equation (1), a first approach consists in solving the polynomial system whose unknowns are the coefficients of h. If $q = p^2$ and θ is the Frobenius automorphism, another construction (Proposition 28 of [4]) is based on a lcrm computation of skew polynomials whose

coefficients are also solutions to auxiliary polynomial systems coming from equations of the type $H^\natural H = F(X^2)$ where $H \in R$ and $F(X^2) \in \mathbb{F}_p[X^2]$ is a self-reciprocal polynomial. The aim of this text is to give a new way to solve these equations which enables to give a counting formula.

3 Strategy

Consider, for $F(Y) = \sum a_i Y^i \in \mathbb{F}_p[Y]$ the skew polynomial $F(X^2) = \sum a_i X^{2i} \in R$ and define the set $\mathcal{H}_{F(X^2)}$ by

$$\mathcal{H}_{F(X^2)} := \{h \in R \mid h \text{ monic and } h^\natural h = F(X^2)\}. \tag{2}$$

Following (1), for $\epsilon \in \{-1, 1\}$, the set $\mathcal{H}_{X^{2k}-\epsilon}$ is the set of the skew check polynomials of all the self-dual (θ, ϵ)-constacyclic codes of dimension k over $\mathbb{F}_{p^2}$. The aim is therefore to provide a construction of the set $\mathcal{H}_{X^{2k}-\epsilon}$ which enables to count its number of elements. The starting point of this construction is given in Lemma 2 below and is based on Proposition 28 of [4] :

Lemma 2 *Consider p prime number, $\theta : x \mapsto x^p$ Frobenius automorphism over $\mathbb{F}_{p^2}$, $k \in \mathbb{N}^*$, $\epsilon \in \{-1, 1\}$, $s = \mathrm{val}_p(k)$, $t = k/p^s$. The number of self-dual (θ, ϵ)-constacyclic codes of dimension k is*

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

where $\mathcal{F}_{k,\epsilon}$ is the set of all monic factors $f(Y) = f^\natural(Y)$ in $\mathbb{F}_p[Y]$ of $Y^t - \epsilon$ with degree > 1 such that $f(Y)$ is irreducible, $\mathcal{G}_{k,\epsilon}$ is the set of all monic factors $f(Y) = f^\natural(Y)$ in $\mathbb{F}_p[Y]$ of $Y^t - \epsilon$ with degree > 1 such that $f(Y) = g(Y)g^\natural(Y)$ with $g(Y) \neq g^\natural(Y)$ monic irreducible in $\mathbb{F}_p[Y]$) and N_ϵ is defined below :

for $p = 2$, $N_\epsilon = \begin{cases} 1 & \text{if } s = 0 \\ 3 & \text{if } s > 0 \end{cases}$;

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

Proof. Consider $t, s \in \mathbb{N}$ such that $k = p^s t$ with t prime to p and $Y^t - \epsilon = f_1(Y) \cdots f_r(Y)$ in $\mathbb{F}_p[Y]$ where $f_i(Y)$ are monic self-reciprocal polynomials which are either irreducible or products of two monic irreducible polynomials. Then according to Proposition 28 of [4], if $h \in \mathcal{H}_{X^{2k}-\epsilon}$, then $h = \mathrm{lcrm}(h_1, \ldots, h_r)$ where for all i in $\{1, \ldots, r\}$, $h_i^\natural = \mathrm{gcrd}(f_i(X^2)^{p^s}, h^\natural)$ and h_i belongs to $\mathcal{H}_{f_i(X^2)^{p^s}}$. Consider therefore the application

$$\phi : \begin{cases} \mathcal{H}_{X^{2k}-\epsilon} & \to & \mathcal{H}_{f_1(X^2)^{p^s}} \times \cdots \times \mathcal{H}_{f_r(X^2)^{p^s}} \\ h & \mapsto & (h_1, \ldots, h_r) \text{ where } h_i^\natural = \mathrm{gcrd}(f_i(X^2)^{p^s}, h^\natural). \end{cases}$$

Consider $(h_1, \ldots, h_r) \in \mathcal{H}_{f_1(X^2)^{p^s}} \times \cdots \times \mathcal{H}_{f_r(X^2)^{p^s}}$ and $h = \mathrm{lcrm}(h_1, \ldots, h_r)$. According to Proposition 28 of [4], the skew polynomial h belongs to $\mathcal{H}_{X^{2k}-\epsilon}$. Let us prove that $h_i^\natural = \mathrm{gcrd}(f_i(X^2)^{p^s}, h^\natural)$. As h belongs to $\mathcal{H}_{X^{2k}-\epsilon}$, $h = \mathrm{lcrm}(H_1, \ldots, H_r)$, where $H_i^\natural = \mathrm{gcrd}(f_i(X^2)^{p^s}, h^\natural)$ and H_i belongs to $\mathcal{H}_{f_i(X^2)^{p^s}}$. As $h_i^\natural$ divides $f_i(X^2)^{p^s}$ and h_i divides on

the left h, $h_i^\natural$ divides on the right h and $f_i(X^2)^{p^s}$, therefore h_i divides on the right H_i, furthermore, h_i and H_i have the same degree because they both belong to $\mathcal{H}_{f_i(X^2)^{p^s}}$, so $h_i = H_i$ and $h_i^\natural = \mathrm{gcrd}(f_i(X^2)^{p^s}, h^\natural)$. Therefore ϕ is bijective and one gets that

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

where $N_\epsilon = \prod_{f(Y)=f^\natural(Y)|Y^t-\epsilon,\deg(f)=1} \#\mathcal{H}_{f(X^2)^{p^s}}$. The irreducible self-reciprocal polynomials of $\mathbb{F}_p[Y]$ of degree 1 are $Y+1$ and $Y-1$. For $p=2$, $N_\epsilon = \#\mathcal{H}_{(X^2+1)^{2^s}} = 1$ if $s=0$, 3 if $s>0$ according to Proposition 24 of [4]. If p is odd, then the set of self-reciprocal divisors of degree 1 of $Y^t-\epsilon$ is empty if $\epsilon=-1$ and $k\equiv 0 \pmod 2$, $\{Y-\epsilon\}$ if $k\equiv 1 \pmod 2$; $\{Y-1, Y+1\}$ if $\epsilon=1$ and $k\equiv 0 \pmod 2$. The expression of N_ϵ follows. ∎

It remains now to determine the number of elements of each intermediate set $\mathcal{H}_{f(X^2)^{p^s}}$. These sets were computed in [4] for $p=2$ and $f(X^2)=X^2-\epsilon$ by using factorization properties of the skew check polynomials.

The strategy here is based on a partition (Lemma 3) of the sets $\mathcal{H}_{f(X^2)^{p^s}}$ into subsets $\overline{\mathcal{H}}_{f(X^2)^m}$ who contains the elements of $\mathcal{H}_{f(X^2)^m}$ which are not divisible by the non constant factors of $f(X^2)$ in $\mathbb{F}_p[X^2]$.

Lemma 3 *Consider $R=\mathbb{F}_{p^2}[X;\theta]$ with p prime number, $\theta: x\mapsto x^p$, $s\in\mathbb{N}$ and $f(Y)=f^\natural(Y)$ in $\mathbb{F}_p[Y]$. For $m\in\mathbb{N}$, consider $\overline{\mathcal{H}}_{f(X^2)^m}$ the set of elements of $\mathcal{H}_{f(X^2)^m}$ which are divisible by no non constant divisor in $\mathbb{F}_p[X^2]$ of $f(X^2)$.*

1. *If $f(Y)=f^\natural(Y)$ is irreducible in $\mathbb{F}_p[Y]$ then*

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

2. *If $f(Y)=g(Y)g^\natural(Y)$ with $g(Y)\neq g^\natural(Y)$ irreducible in $\mathbb{F}_p[Y]$ then*

$$\mathcal{H}_{f(X^2)^{p^s}} = \bigsqcup_{i=0}^{p^s} \bigsqcup_{j=0}^{p^s-i} g(X^2)^i g^\natural(X^2)^j \cdot \overline{\mathcal{H}}_{f(X^2)^{p^s-(i+j)}}. \tag{4}$$

Proof.

1. Consider $M=\lfloor \frac{p^s}{2} \rfloor$, $h=h(X)$ in $\mathcal{H}_{f(X^2)^{p^s}}$ and i the biggest integer in $\{0,\dots,M\}$ such that $f(X^2)^i$ divides h. Consider $H=H(X)$ in R such that $h=f(X^2)^i H$ and $f(X^2)$ does not divide H. As $f(X^2)^i$ is central, according to point 2. of Lemma 1, $h^\natural = f(X^2)^i H^\natural$ and $H^\natural H = f(X^2)^{p^s-2i}$. Conversely, if $H^\natural H = f(X^2)^{p^s-2i}$ and $f(X^2)$ does not divide H, then $f(X^2)^i H$ belongs to $\mathcal{H}_{f(X^2)^{p^s}}$. Therefore $\mathcal{H}_{f(X^2)^{p^s}} = \bigcup_{i=0}^{M} f(X^2)^i \overline{\mathcal{H}}_{f(X^2)^{p^s-2i}}$. Furthermore consider $i>i'$, $H\in\mathcal{H}_{f^{p^s-2i}(X^2)}$ and $H'\in\mathcal{H}_{f^{p^s-2i'}(X^2)}$ such that $f(X^2)^i H = f(X^2)^{i'} H'$ then $f(X^2)^{i-i'}$ divides H', which is impossible as $f(X^2)$ does not divide H'. Therefore, the sets $f(X^2)^i \cdot \overline{\mathcal{H}}_{f(X^2)^{p^s-2i}}$ and $f(X^2)^{i'} \cdot \overline{\mathcal{H}}_{f(X^2)^{p^s-2i'}}$ are disjoints.

2. Consider h in $\mathcal{H}_{f(X^2)^{p^s}}$ and i, j such that $h = g(X^2)^i g^\natural(X^2)^j H$ where $g(X^2)$ and $g^\natural(X^2)$ do not divide H. Then according to point 2. of Lemma 1, $h^\natural = g^\natural(X^2)^i g(X^2)^j H^\natural$, therefore $H^\natural H = f^{p^s-(i+j)}$ and $h \in g(X^2)^i g^\natural(X^2)^j \overline{\mathcal{H}}_{f(X^2)^{p^s-(i+j)}}$. Conversely, if $H^\natural H = f^{p^s-(i+j)}(X^2)$ and $f(X^2)$ does not divide H, then $g(X^2)^i g^\natural(X^2)^j H \in \mathcal{H}_{f(X^2)^m}$. It remains to prove that the sets are disjoint. Consider $(i, j) \neq (i', j')$ with $i > i'$ and $g(X^2)^i g^\natural(X^2)^j u = g(X^2)^{i'} g^\natural(X^2)^{j'} u'$ where $g(X^2)$ and $g^\natural(X^2)$ do not divide u and u'. If $j \geq j'$ then $g(X^2)$ divides u' which is impossible. Assume that $j < j'$ and denotes $\beta = j' - j$. Necessarily, $g(X^2)$ divides $g^\natural(X^2)^\beta u'$. As $g(X^2)$ and $g^\natural(X^2)$ both divide $g^\natural(X^2)^\beta u'$, there lclm is also a divisor of $g^\natural(X^2)^\beta u'$. But $g(X^2)$ and $g^\natural(X^2)$ are right coprime and belongs 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 $g^\natural(X^2)^{\beta-1}u'$. After repeating the same argument one gets that $g(X^2)$ divides $g^\natural(X^2)^{\beta-2}u', \ldots g^\natural(X^2)u'$, therefore $g(X^2)$ divides u', contradiction.

■

The construction of the sets $\overline{\mathcal{H}}_{f(X^2)^m}$ for $m = 1$ will be reduced to Cauchy interpolation problems in the ring $\mathbb{F}_{p^2}[Z]$. For $m > 1$ this construction will require factorization properties given by Proposition 16 of [4] for $f(Y)$ irreducible. These factorization properties are recalled below in Proposition 1 which is a generalization of Proposition 16 of [4] to the case when $f(Y) = g(Y)g^\natural(Y)$ with $g(Y) \neq g^\natural(Y)$ irreducible in $\mathbb{F}_p[Y]$.

Remark 1 *The unique factorization of h in Proposition 1 below is the unique representation of h as the product of maximal completely reducible factors as it is defined in [17] page 498. If $f(Y)$ is irreducible in $\mathbb{F}_p[Y]$ (and $f(X^2) \in R$ does not divide h), then this factorization coincides with the factorization of h into irreducible monic skew polynomials.*

Proposition 1 *Consider $R = \mathbb{F}_{p^2}[X; \theta]$ where p is a prime number and $\theta : x \mapsto x^p$ the Frobenius automorphism. Consider $f(Y)$ in $\mathbb{F}_p[Y]$ self-reciprocal with degree d either irreducible in $\mathbb{F}_p[Y]$ or product of two distinct irreducible polynomials in $\mathbb{F}_p[Y]$. Assume that $h = h_1 \cdots h_m$ is a product of monic skew polynomials of degree d bounded by $f(X^2)$. The following assertions are equivalent :*

(i) the above factorization of h is unique;

(ii) no non constant factor of $f(X^2)$ in $\mathbb{F}_p[X^2]$ divides h in R;

(iii) for all i in $\{1, \ldots, m-1\}$, no non constant factor of $f(X^2)$ in $\mathbb{F}_p[X^2]$ divides $h_i h_{i+1}$ in R.

Proof. If $f(Y)$ is irreducible, then the proof follows from Proposition 16 of [4] and Theorem 21, 24 of [10]. In the following, we assume that $f(Y) = g(Y)g^\natural(Y)$ with $g(Y) \neq g^\natural(Y)$ with same degree δ. To simplify the notations we denote $f = f(X^2)$, $g = g(X^2)$ and $g^\natural = g^\natural(X^2)$.

The implication $(ii) \Rightarrow (iii)$ is immediate. Let us prove that $(i) \Rightarrow (ii)$. If g divides h, then it divides h on the right and h has at least two distinct right factors u and v irreducible bounded by g. As the factors h_i of h are all bounded by $f = gg^\natural$, necessarily, h has an irreducible right factor w bounded by $g^\natural$. Then $\mathrm{lclm}(u, w)$ and $\mathrm{lclm}(v, w)$ are two right factors of h with degree d dividing f. According to Theorem 13 of [17], as u (resp. v) and

w are irreducible and do not have the same bound, the lclm-decompositions $\mathrm{lclm}(u,w)$ and $\mathrm{lclm}(v,w)$ are unique. Furthermore, u and v are distinct, so the skew polynomials $\mathrm{lclm}(u,w)$ and $\mathrm{lclm}(v,w)$ 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 of degree d dividing f, then there are two consecutive factors whose product is divisible by g or $g^\natural$.

Consider $h = h_1 h_2 = g_1 g_2$ where g_i, h_i are skew polynomials of degree d bounded by f. Assume that g and $g^\natural$ do not divide h. Then $\mathrm{gcrd}(h,g)$ is an irreducible skew polynomial of degree δ dividing g which is also equal to $\mathrm{gcrd}(h_2,g)$ and $\mathrm{gcrd}(g_2,g)$. Similarly, $\mathrm{gcrd}(h_2,g^\natural) = \mathrm{gcrd}(g_2,g^\natural)$. Furthermore, according to Theorem 4.1 of [7], $h_2 = \mathrm{lclm}(\mathrm{gcrd}(h_2,g),\mathrm{gcrd}(h_2,g^\natural))$ and $g_2 = \mathrm{lclm}(\mathrm{gcrd}(g_2,g),\mathrm{gcrd}(g_2,g^\natural))$, 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 of degree d bounded by 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 δ dividing g and $g^\natural$.

If $\mathrm{gcrd}(h_m,g_m) = 1$ then $\mathrm{lclm}(h_m,g_m) = \overline{h}_{m-1}h_m$ divides $h_1 \cdots h_m$ and $\overline{h}_{m-1}$ is a monic skew polynomial of degree d dividing f which is the product of two irreducible monic skew polynomials of degree δ dividing g and $g^\natural$. Consider $H \in R$ such that $H\overline{h}_{m-1} = h_1 \cdots h_{m-1}$. If $\overline{h}_{m-1} = h_{m-1}$ then $\mathrm{lclm}(h_m,g_m) = h_{m-1}h_m$ has two factorizations into the product of two monic skew polynomials of degree d dividing f, therefore, g or $g^\natural$ divides $h_{m-1}h_m$. Otherwise, as $h_1,\ldots,h_{m-1},\overline{h}_{m-1}$ 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 bounded by g and $m-2$ skew polynomials bounded by $g^\natural$. In particular, H divides $g^{m-2}(g^\natural)^{m-2}$. According to Theorem 4.1 of [7], $H = \mathrm{lclm}(G,\tilde{G})$ where $G = \mathrm{gcrd}(H,g^{m-2})$ and $\tilde{G} = \mathrm{gcrd}(H,(g^\natural)^{m-2})$. As $g(Y)$ (resp. $g^\natural(Y)$) is irreducible in $\mathbb{F}_p[Y]$, the skew polynomial G (resp. $\tilde{G}$) is the product of N (resp. $\tilde{N}$) monic irreducible skew polynomials bounded by 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 bounded by g (resp. $g^\natural$). As g (resp. $g^\natural$) does not divide G (resp $\tilde{G}$), these factorizations are unique. Therefore, according to Theorem 14 of [17], $H = H_1 \cdots H_N$ where $H_i = \mathrm{lclm}(\overline{G_i},\overline{\tilde{G}_i})$ with $R/\overline{G_i}R$ and R/G_iR (resp. $R/\overline{\tilde{G}_i}R$ and $R/\tilde{G}_iR$) isomorphic modules. As G_i is bounded by g, according to Corollary of Theorem 10 of [10], $\overline{G_i}$ is also bounded by g. As G_i and $\tilde{G}_i$ are right coprime with same degree $d/2$, so are $\overline{G}_i$ and $\overline{\tilde{G}}_i$ 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 $H\overline{h}_{m-1}$.

Assume that $\mathrm{gcrd}(h_m,g_m) = u \neq 1$. Necessarily u is an irreducible monic skew polynomial of degree δ which divides g or $g^\natural$ let's say g. Consider v such that $\mathrm{lclm}(g_m,h_m) = vh_m$ and $H \in R$ such that $h_1 \cdots h_m = Hvh_m$ i.e $h_1 \cdots h_{m-1} = Hv$. Necessarily v is an irreducible monic skew polynomial of degree δ dividing $g^\natural$ and $H = \tilde{h_1} \cdots \tilde{h}_{m-2}w$ where w is irreducible dividing g, $\tilde{h}_i$ is a product of two irreducible monic skew polynomials of degree δ dividing g and $g^\natural$. If $h_{m-1} = wv$, then $w\mathrm{lclm}(g_m,h_m) = h_{m-1}h_m$ and one concludes that g or $g^\natural$ divides $h_{m-1}h_m$. If $h_{m-1} \neq wv$ then $h_1 \cdots h_{m-1} = \tilde{h}_1 \cdots \tilde{h}_{m-2}(wv)$ where wv is a monic skew polynomial of degree d dividing f, and one concludes using the induction hypothesis. ∎

4 Construction of the sets $\mathcal{H}_{(X^2\pm 1)^{p^s}}$

In [4], it is proven that there are three self-dual skew codes of dimension 2^s over $\mathbb{F}_4$ with $s \neq 0$ (and one self-dual skew code if $s = 0$). The aim of this section is to construct and count self-dual skew codes over $\mathbb{F}_{p^2}$ with dimension a power of p when p is an odd prime number. Following Lemma 3, for p odd prime, the set $\mathcal{H}_{(X^2-\epsilon)^{p^s}}$ is equal to the union of pairwise disjoint sets $\bigsqcup_{i=0}^{\frac{p^s-1}{2}} (X^2-\epsilon)^i \cdot \overline{\mathcal{H}}_{(X^2-\epsilon)^{p^s-2i}}$ where $\overline{\mathcal{H}}_{(X^2-\epsilon)^{p^s-2i}}$ is the set of elements of $\mathcal{H}_{(X^2-\epsilon)^{p^s-2i}}$ which are not divisible by $X^2-\epsilon$. Lemma 4 below gives for odd number m, a construction of the set $\overline{\mathcal{H}}_{(X^2-\epsilon)^m}$ from which one easily deduces its number of elements. Lemma 3 and 4 enable therefore to derive a formula for the number of (θ,ϵ)-constacyclic codes of dimension a power of p over $\mathbb{F}_{p^2}$ for p odd prime (Proposition 2).

Lemma 4 *Consider $\epsilon \in \{-1,1\}$, $R = \mathbb{F}_{p^2}[X;\theta]$ with p odd prime number, θ the Frobenius automorphism, m odd number and $M = \frac{m-1}{2}$. If $\epsilon \neq (-1)^{\frac{p+1}{2}}$ then the set $\overline{\mathcal{H}}_{(X^2-\epsilon)^m}$ is empty, otherwise it has $2p^M$ elements and it satisfies $\overline{\mathcal{H}}_{(X^2-\epsilon)^m} =$*

$$\left\{ (X+\alpha_0)\prod_{i=1}^{M}(X+\alpha_i)(X+\theta(\alpha_i)) \mid \alpha_0^2 = -1, \alpha_i^{p+1} = \epsilon, \alpha_1 \neq \epsilon\alpha_0, \alpha_{i+1} \neq -\alpha_i \right\}.$$

Proof.

For $m = 1$, $\overline{\mathcal{H}}_{X^2-\epsilon} = \mathcal{H}_{X^2-\epsilon} = \{X+\alpha_0 \mid \theta(\alpha_0)^2+1 = 0, \theta(\alpha_0) = -\epsilon\alpha_0\} = \{X+\alpha_0 \mid \alpha_0^2 = -1, \alpha_0^{p+1} = \epsilon\}$.

- Consider $m \geq 3$. Assume that $h^{\natural}h = (X^2-\epsilon)^m$ and $X^2-\epsilon$ does not divide h. As h divides $(X^2-\epsilon)^m$ and as $X^2-\epsilon$ is irreducible in $\mathbb{F}_p[X^2]$, the bound of h is a power of $X^2-\epsilon$, therefore the skew polynomial h is the product of irreducible monic skew polynomials bounded by $X^2-\epsilon$. Furthermore all irreducible skew polynomials bounded by $X^2-\epsilon$ are of degree 1 with a nonzero constant coefficient and the degree of h is equal to m, therefore h is the product of m irreducible monic skew polynomials of degree 1 :

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

As $X^2-\epsilon$ does not divide h, according to Proposition 1 (or Proposition 16 of [4]), this factorization is unique and

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

Furthermore, according to Lemma 1,

$$h^{\natural} \quad = \quad (X+\tilde{\lambda}_m)\cdots(X+\tilde{\lambda}_2)(X+\tilde{\lambda}_1) \tag{6}$$

where $(\tilde{\lambda}_i)_{1\leq i\leq m}$ is defined by

$$\tilde{\lambda}_{2i} = \frac{\theta(\mu_{2i})}{\mu_{2i+1}} \text{ and } \tilde{\lambda}_{2i+1} = \frac{\mu_{2i+1}}{\theta(\mu_{2i+2})} \tag{7}$$

and $(\mu_i)_{1\leq i\leq m}$ is defined by

$$\mu_1 = 1,\ \forall i \in \{2,\dots,m\}, \mu_i = \lambda_1 \cdots \lambda_{i-1}. \tag{8}$$

This factorization of $h^\natural$ into the product of monic irreducible skew polynomials is unique (otherwise the factorization of h would not be unique) therefore, according to Proposition 1 (or Proposition 16 of [4]),

$$\forall i \in \{1,\dots,m-1\}, (X+\tilde{\lambda}_{i+1})(X+\tilde{\lambda}_i) \neq X^2-\epsilon. \tag{9}$$

As $h^\natural h = (X^2-\epsilon)^m$ and $(X^2-\epsilon)^m$ does not have a unique factorization into the product of monic linear polynomials, according to Proposition 1 (or Proposition 16 of [4]), there must exist two irreducible consecutive monic factors in the decomposition of $h^\natural h$ whose product is $X^2-\epsilon$. According to the relations (5) and (9), the only possibility is $(X+\lambda_1)(X+\tilde{\lambda}_1) = X^2-\epsilon$ and by induction one gets

$$\forall i \in \{1,\dots,m\}, (X+\lambda_i)(X+\tilde{\lambda}_i) = X^2-\epsilon. \tag{10}$$

Developping (10) yields $\tilde{\lambda}_i = -\epsilon/\lambda_i = -\theta(\lambda_i)$ therefore $\lambda_i\theta(\lambda_i) = \lambda_i^{p+1} = \epsilon$ and $\tilde{\lambda}_{2i}\tilde{\lambda}_{2i+1} = \theta(\lambda_{2i})\theta(\lambda_{2i+1})$ (note that one can consider this product for $i \geq 1$ because $m \geq 3$). The relation (7) gives $\tilde{\lambda}_{2i}\tilde{\lambda}_{2i+1} = \frac{\theta(\mu_{2i})}{\mu_{2i+1}}\frac{\mu_{2i+1}}{\theta(\mu_{2i+2})} = \dfrac{1}{\theta(\lambda_{2i})\theta(\lambda_{2i+1})}$ therefore $(\lambda_{2i}\lambda_{2i+1})^2 = 1$. Furthermore, according to (5) and (10) , $X+\lambda_{i+1} \neq X+\tilde{\lambda}_i$, therefore $\lambda_{2i+1} \neq \tilde{\lambda}_{2i} = -\dfrac{\epsilon}{\lambda_{2i}}$ and as p is *odd* the relation $(\lambda_{2i}\lambda_{2i+1})^2 = 1$ implies that $\lambda_{2i+1} = \frac{\epsilon}{\lambda_{2i}} = \theta(\lambda_{2i})$ (note that for $p=2$, one gets an impossibility, see also Remark 2). Assume furthermore that m is odd and consider $M = \frac{m-1}{2}$. Considering $\alpha_0 = \lambda_1$ and for $i = 1 \dots M$, $\alpha_i = \lambda_{2i}$, one gets

$$h \ = \ (X+\alpha_0)\textstyle\prod_{i=1}^{M}(X+\alpha_i)(X+\theta(\alpha_i))$$

with $\forall i \in \{0,\dots,M\}$, $\alpha_i\theta(\alpha_i) = \alpha_i^{p+1} = \epsilon$. Furthermore, $\tilde{\lambda}_1 = \frac{\mu_1}{\theta(\mu_2)}$, $\lambda_2 \neq \tilde{\lambda_1}$ and $\lambda_{2i+2} \neq \tilde{\lambda}_{2i+1}$ therefore $\alpha_0^2 = -1$, $\alpha_1 \neq \epsilon\alpha_0$ and $\alpha_{i+1} \neq -\alpha_i$.

- Conversely consider

$$h = (X+\alpha_0)\left[\prod_{i=1}^{M}(X+\alpha_i)(X+\theta(\alpha_i))\right]$$

where $\alpha_0^2 = -1, \forall i \in \{0,\dots,M\}, \alpha_i\theta(\alpha_i) = \alpha_i^{p+1} = \epsilon, \alpha_1 \neq \epsilon\alpha_0, \forall i \in \{1,\dots,M\}, \alpha_{i+1} \neq -\alpha_i$. The expression of $h^\natural$ is given by (6) with (8) and (7) where $\lambda_{2i} = \alpha_i$ and $\lambda_{2i+1} = \theta(\alpha_i)$. The expressions of μ_i and $\tilde{\lambda}_i$ can be simplified as follows: for $i \geq 1$,

$$\begin{cases} \mu_{2i+1} = \mu_{2i}\alpha_i \\ \mu_{2i} = \alpha_0\left[\displaystyle\prod_{j=1}^{i-1}\alpha_j\theta(\alpha_j)\right] = \alpha_0\prod_{j=1}^{i-1}\epsilon = \alpha_0\epsilon^{i-1} \end{cases}$$

and

$$\begin{cases} \tilde{\lambda}_{2i} = \frac{\theta(\alpha_0)}{\alpha_0\alpha_i} = \frac{\theta(\alpha_0)\alpha_0}{\alpha_0^2\alpha_i} = -\frac{\epsilon}{\alpha_i} = -\theta(\alpha_i) \\ \tilde{\lambda}_{2i+1} = \dfrac{\mu_{2i+1}}{\theta(\mu_{2i+2})} = \dfrac{\alpha_0\epsilon^{i-1}\alpha_i}{\theta(\alpha_0)\epsilon^i} = -\alpha_i. \end{cases}$$

Therefore the expression of $h^\natural$ in (6) becomes

$$h^\natural = \left[\prod_{i=M}^{1}(X-\alpha_i)(X-\theta(\alpha_i))\right](X-\theta(\alpha_0)).$$

Furthermore $(X-\theta(\alpha_0))(X+\alpha_0) = X^2-\alpha_0\theta(\alpha_0) = X^2-\epsilon$ and for $i=1,\ldots,M$, $(X-\alpha_i)(X-\theta(\alpha_i))(X+\alpha_i)(X+\theta(\alpha_i)) = (X-\alpha_i)(X^2-\epsilon)(X+\theta(\alpha_i)) = (X^2-\epsilon)(X-\alpha_i)(X+\theta(\alpha_i)) = (X^2-\epsilon)^2$. As $X^2-\epsilon$ is central one gets $h^\natural h = (X^2-\epsilon)^{1+2M}$.

Lastly, to prove that $X^2-\epsilon$ does not divide h, according to Proposition 1, it suffices to prove that no product of two consecutive factors in the decomposition of $h = (X+\alpha_0)\prod_{i=1}^{M}(X+\alpha_i)(X+\theta(\alpha_i))$ is equal to $X^2-\epsilon$ i.e. $(X+\alpha_0)(X+\alpha_1)$, $(X+\alpha_i)(X+\theta(\alpha_i))$ and $(X+\theta(\alpha_i))(X+\alpha_{i+1})$ are distinct from $X^2-\epsilon$. The constant coefficients of these polynomials are all distinct from $-\epsilon$; namely $\alpha_0\alpha_1 \neq \epsilon\alpha_0^2 = -\epsilon$, $\alpha_i\theta(\alpha_i) = \epsilon \neq -\epsilon$ and $\alpha_{i+1}\theta(\alpha_i) \neq -\alpha_i\theta(\alpha_i) = -\epsilon$, therefore no product of two consecutive factors in the decomposition of h is equal to $X^2-\epsilon$.

- We now count the number of elements of the set $\overline{\mathcal{H}}_{(X^2-\epsilon)^m}$: it is empty if and only if there is not $\alpha_0 \in \mathbb{F}_{p^2}$ such that $\alpha_0^2 = -1$ and $\alpha_0^{p+1} = \epsilon$. Over $\mathbb{F}_{p^2}$, -1 is always a square, therefore $\overline{\mathcal{H}}_{(X^2-\epsilon)^m}$ is empty if and only if $(-1)^{(p+1)/2} \neq \epsilon$. (i.e. if and only if $p \equiv 1 \pmod 4$ and $\epsilon = 1$ or $p \equiv 3 \pmod 4$ and $\epsilon = -1$). If $\epsilon = (-1)^{(p+1)/2}$, then there are as many elements in $\overline{\mathcal{H}}_{(X^2-\epsilon)^m}$ as the number of $(M+1)$-uplets $(\alpha_0, \alpha_1, \ldots, \alpha_M)$ such that $\alpha_0^2 = -1$, $\alpha_i^{p+1} = \epsilon$, $\alpha_1 \neq \epsilon\alpha_0$, $\alpha_{i+1} \neq -\alpha_i$. Therefore there are 2 choices for α_0 and p choices for $\alpha_1, \ldots, \alpha_M$, so $\overline{\mathcal{H}}_{(X^2-\epsilon)^m}$ has $2p^M$ elements.

■

Remark 2 *From the first part of the proof of the previous lemma, one deduces that for $m \geq 3$ and $p = 2$, the sets $\overline{\mathcal{H}}_{(X^2-\epsilon)^m}$ are empty. Therefore according to Lemma 3, for $s \in \mathbb{N}^*$,*

$$\mathcal{H}_{(X^2+1)^{2^s}} \;=\; (X^2+1)^{2^{s-1}}\,\overline{\mathcal{H}}_{(X^2+1)^0} \bigsqcup (X^2+1)^{2^{s-1}-1}\,\overline{\mathcal{H}}_{(X^2+1)^2}.$$

Furthermore $\overline{\mathcal{H}}_{(X^2+1)^2} = \{(X+1)(X+u) \mid u \in \{a, a^2\}\}$ where $\mathbb{F}_4 = \mathbb{F}_2(a)$. Therefore $\mathcal{H}_{(X^2+1)^{2^s}} = \{(X+1)^{2^s-1}(X+u) \mid u \in \{1, a, a^2\}\}$ and one gets that for $s > 0$ there are only three self-dual skew codes of dimension 2^s over $\mathbb{F}_4$ (see Corollary 26 of [4]).

Proposition 2 below gives a formula for the number of self-dual θ-cyclic and θ-negacyclic codes whose dimension is a power of p for p odd prime. It is deduced from Lemma 3 and 4.

Proposition 2 *Consider p an odd prime number , $s \in \mathbb{N}$, $\theta : x \mapsto x^p$ defined over $\mathbb{F}_{p^2}$ and $\epsilon \in \{-1, 1\}$. The number of self-dual (θ, ϵ)-constacyclic codes of dimension p^s over $\mathbb{F}_{p^2}$ is*

$$\#\mathcal{H}_{(X^2-\epsilon)^{p^s}} = \begin{cases} 0 & \text{if} \quad \epsilon \neq (-1)^{\frac{p+1}{2}} \\ 2\dfrac{p^{(p^s+1)/2}-1}{p-1} & \text{if} \quad \epsilon = (-1)^{\frac{p+1}{2}}. \end{cases}$$

Proof.
Consider $s \in \mathbb{N}^*$ and $M = \frac{p^s-1}{2}$. According to Lemma 3, $\mathcal{H}_{X^{2p^s}-\epsilon} = \bigsqcup_{i=0}^{M}(X^2-1)^i\overline{\mathcal{H}}_{(X^2-\epsilon)^{p^s-2i}}$ and according to Lemma 4, each set $\overline{\mathcal{H}}_{(X^2-\epsilon)^{p^s-2i}}$ is empty if $\epsilon \neq (-1)^{\frac{p+1}{2}}$ and has $2p^{M-i}$ elements if $\epsilon = (-1)^{\frac{p+1}{2}}$. Therefore, if $\epsilon \neq (-1)^{\frac{p+1}{2}}$, $\mathcal{H}_{X^{2p^s}-\epsilon}$ 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. ∎

To conclude this section, some experimental results about the weight enumerators of self-dual skew codes with dimension p^s and their links to the sets $\overline{\mathcal{H}}_{(X^2-\epsilon)^m}$ are given below.

Over $\mathbb{F}_4$ the best minimum distance reached by self-dual θ-codes of dimension 2^s does not depend on s and is only 3 for $s = 2$ and 4 for $s \geq 3$ (Theorem 1 [3]). The following proposition gives a family of self-dual θ-codes of dimension p^s whose minimal distance depends only on p and does not grow with s either (which is quite bad !). The skew check polynomials of the corresponding codes all belong to $(X^2-\epsilon)^{\frac{p^s-1}{2}}\overline{\mathcal{H}}_{X^2-\epsilon}$.

Proposition 3 *Consider p odd prime, $\alpha \in \mathbb{F}_{p^2}$ such that $\alpha^2+1=0$, $\epsilon = (-1)^{\frac{p+1}{2}}$ and $\theta : x \mapsto x^p$. For each nonnegative integer s, the (ϵ,θ)-constacyclic code over $\mathbb{F}_{p^2}$ of dimension p^s generated by the skew polynomial $(X^2-\epsilon)^{\frac{p^s-1}{2}}(X+\alpha)$ is a self-dual code with minimum distance $\leq \frac{p+3}{2}$.*

Proof. According to Lemma 4, the skew polynomial $h = (X^2-\epsilon)^{\frac{p^s-1}{2}}(X-\alpha)$ belongs to $(X^2-\epsilon)^{\frac{p^s-1}{2}}\overline{\mathcal{H}}_{X^2-\epsilon}$. Therefore, according to Lemma 3, it belongs to $\mathcal{H}_{X^{2p^s}-\epsilon}$ and $g = h^\natural = (X^2-\epsilon)^{\frac{p^s-1}{2}}(X+\alpha)$ generates a self-dual θ-code of dimension p^s.

The skew polynomial $(X^2-\epsilon)^{\frac{p^{s-1}(p+1)}{2}} = (X^{2p^{s-1}}-\epsilon)^{\frac{p+1}{2}}$ has $\frac{p+3}{2}$ terms and it is also a right multiple of degree $< 2p^s$ of the skew polynomial g as $(X^{2p^{s-1}}-\epsilon)^{\frac{p+1}{2}} = (X^2-\epsilon)^{\frac{p^{s-1}-1}{2}}(X+\epsilon\alpha)g$. So the code has a word of weight $\frac{p+3}{2}$. ∎

Table 1 shows that the weight enumerators of self-dual skew codes over $\mathbb{F}_{p^2}$ (in the third column) with dimension p (first column) for $p = 3, 5, 7$ can be classified in function of the sets $\mathcal{H}^{(i)} := (X^2-\epsilon)^i\overline{\mathcal{H}}_{(X^2-\epsilon)^{p-2i}}$ where $0 \leq i \leq \frac{p-1}{2}$ (second column). The computations were made using MAGMA. From this table, on can notice two facts about self-dual skew codes of dimension p over $\mathbb{F}_{p^2}$ that we cannot explain at the moment. First for $p = 3, 5, 7$, two codes with skew check polynomials belonging to two distinct sets $\mathcal{H}^{(i)}$ and $\mathcal{H}^{(j)}$ cannot have the same weight enumerator and we have the following conjecture :

Conjecture 1 *Let us denote, for $0 \leq i \leq \frac{p^s-1}{2}$, $\mathcal{H}^{(i)} := (X^2-\epsilon)^i\overline{\mathcal{H}}_{(X^2-\epsilon)^{p^s-2i}}$. Consider $i \neq j \in \{0, \ldots, \frac{p^s-1}{2}\}$, $h \in \mathcal{H}^{(i)}$ and $h' \in \mathcal{H}^{(j)}$. The weight enumerators of the self-dual (θ,ϵ)-constacyclic codes of dimension p^s with skew check polynomials h and h' are distinct.*

Secondly, for each $p \in \{3, 5, 7\}$, the skew check polynomials of the self-dual θ-codes of dimension p who reach the best distances all belong to $\mathcal{H}^{(0)}$ (they are not divisible by $X^2-\epsilon$ and have therefore a unique factorization into the product of monic skew polynomials of degree 1). Here are some examples :

- There are 4 $[6,3,4]_9$ self-dual θ-cyclic codes, one of them has check polynomial $h = (X+a^2)(X+1)(X+1) = (X+a^2)(X^2+2X+1) = X^3+aX^2+a^5X+a^2$ and generator polynomial $g = X^3+a^7X^2+a^5X+a^2$ where $a^2+2a+2=0$.

- There are 32 $[10,5,6]_{25}$ self-dual θ-negacyclic codes, one of them has check polynomial $h = (X+2)[(X+a^{22})(X+a^{14})][(X+a^2)(X+a^{10})] = (X+2)(X^2+a^4X+4)(X^2+a^8X+4) = X^5+a^{17}X^4+X^3+2X^2+a^7X+2$ and generator polynomial $g = X^5+aX^4+X^3+3X^2+a^7X+3$ where $a^2+4a+2=0$.

- There are 72 $[14,7,8]_{49}$ self-dual θ-cyclic codes and one of them has check polynomial $h = (X+a^{36})[(X+a^6)(X+a^{42})][(X+a^6)(X+a^{42})][(X+a^{12})(X+a^{36})] = (X+a^{36})(X^2+a^{22}X+1)(X^2+a^{22}X+1)(X^2+a^{28}X+1) = X^7+a^{47}X^6+a^{38}X^5+a^{36}X^4+X^3+a^{14}X^2+a^{29}X+a^{36}$ and generator polynomial $g = X^7+a^{17}X^6+a^{38}X^5+a^{36}X^4+X^3+a^{26}X^2+a^{29}X+a^{36}$ where $a^2+6a+3=0$.

Paradoxically, as proved below, the set $\mathcal{H}^{(0)}$ also provides skew codes with very bad distance (2) for any s : consider $\alpha \in \mathbb{F}_{p^2}$ such that $\alpha^2 = -1$, the skew polynomial $X^{p^s}+\alpha$ generates a self-dual θ-code of minimum distance 2. One can notice that it factorizes uniquely as the product of monic skew polynomials of degree 1 :

- if $p \equiv 1 \pmod 4$, $X^{p^s}+\alpha = (X+\alpha)^{p^s}$

- if $p \equiv 3 \pmod 4$, $X^{p^s}+\alpha = (X+\alpha)(X-\alpha)(X+\alpha)\cdots(X-\alpha)(X+\alpha)$.

Namely, as $X^{p^s}+\alpha$ divides on the right $(X^2+1)^{p^s}$, its factors are $X+u$ with $u^2=-1$. As the bound of $X^{p^s}+\alpha$ is $(X^2+1)^{p^s}$, the factorization is unique and is necessarily the one above.

The self-dual θ-cyclic codes $[18,9]_9$ are not optimal, as the best distance they reach is 8 which is less than the best known distance (9) for these codes. Conjecture 1 is however satisfied for these codes (i.e. for $p=3$ and $s=2$). Some of the $[54,27]_9$ self-dual θ-cyclic codes reach the best known distance, 18. Their skew check polynomials belong to $\mathcal{H}^{(2)}$ (divisible exactly by $(X^2-1)^2$), $\mathcal{H}^{(1)}$ (divisible exactly by (X^2-1)) or $\mathcal{H}^{(0)}$ (not divisible by X^2-1), but none of them is divisible by $(X^2-1)^3$. As there are 4782968 self-dual θ-cyclic codes with dimension 27, it remains quite long to compute all the minimal distances. A good strategy would be to exploit the factorization of the skew check polynomial more deeply to keep the best codes.

5 Construction of the sets $\mathcal{H}_{f(X^2)^{p^s}}$ for f of degree > 1

For $f(Y) = f^\natural(Y)$ of degree $d > 1$ such that $f(Y)$ is irreducible in $\mathbb{F}_p[Y]$ (resp. such that $f(Y) = g(Y)g^\natural(Y)$ with $g(Y) \neq g^\natural(Y)$ irreducible in $\mathbb{F}_p[Y]$), the set $\mathcal{H}_{f(X^2)^{p^s}}$ will be constructed by using the partition (3) (resp. (4)) given in Lemma 3. It requires the computation of the sets $\overline{\mathcal{H}}_{f(X^2)^m}$ whose elements will be constructed (Lemma 8) using products of elements of $\overline{\mathcal{H}}_{f(X^2)}$. In the following subsection, the sets $\mathcal{H}_{f(X^2)}$ are constructed via Cauchy interpolations in $\mathbb{F}_{p^2}[Z]$.

p	i	Weight enumerators	nbe codes
3	1	$1+16Y^3+72Y^4+288Y^5+352Y^6$	2
	0	$1+24Y^2+192Y^4+512Y^6$	
		$\mathbf{1+120Y^4+240Y^5+368Y^6}$	4
5	2	$1+240Y^4+1008Y^5+\cdots$	2
	1	$1+240Y^4+48Y^5+\cdots$	2
		$1+48Y^5+\cdots$	8
	0	$1+120Y^2+\cdots$	2
		$1+120Y^4+240Y^5+\cdots$	8
		$1+120Y^4+480Y^5+\cdots$	8
		$\mathbf{1+5040Y^6}+\cdots$	32
7	3	$1+2016Y^5+\cdots$	2
	2	$1+672Y^6+5472Y^7+\cdots$	12
		$1+3024Y^6+8160Y^7+\cdots$	2
	1	$1+1008Y^4+\cdots$	2
		$1+336Y^6+2112Y^7+\cdots$	12
		$1+336Y^6+4800Y^7+\cdots$	12
		$1+336Y^6+4128Y^7+\cdots$	12
		$1+672Y^6+4800Y^7+\cdots$	12
		$1+96Y^7+143472Y^8+\cdots$	12
		$1+2784Y^7+124656Y^8+\cdots$	12
		$1+4128Y^7+115248Y^8+\cdots$	24

p	i	Weight enumerators	nbe codes
7	0	$1+336Y^2+\cdots$	2
		$1+336Y^4+\cdots$	36
		$1+336Y^6+2688Y^7+\cdots$	36
		$1+336Y^6+3360Y^7+\cdots$	12
		$1+336Y^6+1344Y^7+\cdots$	24
		$1+336Y^6+2016Y^7+\cdots$	60
		$1+336Y^6+4032Y^7+\cdots$	12
		$1+672Y^6+3360Y^7+\cdots$	12
		$1+672Y^6+4704Y^7+\cdots$	24
		$1+1008Y^6+4032Y^7+\cdots$	24
		$1+1008Y^6+4704Y^7+\cdots$	12
		$1+1680Y^6+\cdots$	12
		$1+672Y^7+\cdots$	84
		$1+1344Y^7+\cdots$	24
		$1+2016Y^7+\cdots$	72
		$1+2688Y^7+\cdots$	84
		$1+3360Y^7+\cdots$	36
		$1+4032Y^7+\cdots$	4
		$1+4704Y^7+\cdots$	16
		$1+6048Y^7+\cdots$	28
		$\mathbf{1+144144Y^8}+\cdots$	72

Table 1: Weight enumerators of self-dual skew codes over $\mathbb{F}_{p^2}$ with dimension p for $p=3,5,7$ in function of $i=\frac{p-1}{2},\ldots,1,0$ where i is the biggest integer such that $(X^2-\epsilon)^i$ divides the skew check polynomial of the codes

5.1 Construction of the sets $\mathcal{H}_{f(X^2)}$.

Consider $f(Y)\in\mathbb{F}_p[Y]$ with degree $d>1$ such that $f(Y)=f^\natural(Y)$ and $f(Y)$ irreducible. According to [16], page 6 (or Lemma 1.4.11 of [5] with $e=2$), the skew polynomial $f(X^2)\in R$ has $((p^2)^d-1)/(p^d-1)=p^d+1$ irreducible monic right factors of degree d. The set $\mathcal{H}_{f(X^2)}$ is a subset of this set of factors. Its construction is mainly based on Cauchy interpolations (Lemma 6). The following Lemma (see also exercise 3.14 page 141 of [13]) will be useful next

Lemma 5 *Consider $f(Y)\in\mathbb{F}_p[Y]$ with degree $d>1$ such that $f(Y)=f^\natural(Y)$ and $f(Y)$ irreducible in $\mathbb{F}_p[Y]$. Consider $\alpha\in\mathbb{F}_{p^d}$ such that $f(\alpha)=0$. Then d is necessarily even and $\alpha^{-1}=\alpha^{p^\delta}$ where $2\delta=d$.*

Proof. Consider $f(Y)\in\mathbb{F}_p[Y]$ irreducible with degree $d>1$ and such that $f(Y)=f^\natural(Y)$. Consider $\alpha\in\mathbb{F}_{p^d}$ such that $f(\alpha)=0$ and j the order of α. As $f^\natural(Y)=f(Y)$, α^{-1} is a root of $f(Y)$, so there exists $k\in\{0,\ldots d-1\}$ such that $\alpha^{-1}=\alpha^{p^k}$. Therefore $p^k\equiv -1 \pmod j$ and $p^{2k}\equiv 1 \pmod j$. Furthermore, d is the order of p modulo j, so d divides $2k$. If d was odd then it would divide k, which is impossible as $p^k\equiv -1 \pmod j$. Consider δ such that $d=2\delta$, it divides $k\in\{0,\ldots,d-1\}$ therefore $k=\delta$ and $\alpha^{-1}=\alpha^{p^\delta}$. ∎

The construction of $\mathcal{H}_{f(X^2)}$ below is given for $f(Y)$ self-reciprocal irreducible in $\mathbb{F}_p[Y]$ or product of two distinct irreducible polynomials.

Lemma 6 *Consider $R=\mathbb{F}_{p^2}[X;\theta]$ with p prime number, $\theta: x\mapsto x^p$, $m\in\mathbb{N}^*$ and $f(Y)$ in $\mathbb{F}_p[Y]$ with degree $d=2\delta>1$ in Y such that $f(Y)=f^\natural(Y)$ with $f(Y)$ irreducible or product of two irreducible polynomials with degree δ. The set $\mathcal{H}_{f(X^2)}$ has $1+p^\delta$ elements if f is irreducible and $3+p^\delta$ elements if f is reducible.*

Proof. Assume that $f(Y)$ is irreducible, as its degree is even (Lemma 5) $f(Z)$ factorizes in $\mathbb{F}_{p^2}[Z]$ as the product of two irreducible polynomials $\tilde{f}(Z)$ and $\Theta(\tilde{f})(z)$. If $h\in R\cap\mathbb{F}_{p^2}[X^2]$ then the equation $h^\natural h=f(X^2)$ in R is equivalent to the equation $A(X^2)A^\natural(X^2)=f(X^2)$

in $\mathbb{F}_{p^2}[X^2]$. If δ is even then $\tilde{f} = \tilde{f}^\natural$, so there is no solution; if δ is odd, then $\tilde{f}^\natural = \Theta(\tilde{f})$ therefore $\tilde{f}(X^2)$ and $\Theta(\tilde{f})(X^2)$ are solutions. Consider now $\alpha \in \mathbb{F}_{p^d}$ such that $f(\alpha) = 0$. If $h \in R \setminus \mathbb{F}_{p^2}[X^2]$, then writing $h(X) = A(X^2) + XB(X^2)$, with $B \neq 0$, one gets that $h^\natural h = f(X^2)$ is equivalent to

$$\left\{ \begin{array}{lcl} A^*(X^2)A(X^2) + B^*(X^2)B(X^2)X^2 & = & \lambda f(X^2) \in R \\ A^*(X^2)\Theta(B)(X^2) + B^*(X^2)\Theta(A)(X^2) & = & 0 \in R. \end{array} \right.$$

The skew polynomials which appear in the equations belong to $\mathbb{F}_{p^2}[X^2;\theta] = \mathbb{F}_{p^2}[X^2]$ therefore, replacing X^2 with Z one gets the equivalent system in $\mathbb{F}_{p^2}[Z]$:

$$\left\{ \begin{array}{lcl} A^*(Z)A(Z) + B^*(Z)B(Z)Z & = & \lambda f(Z) \in \mathbb{F}_{p^2}[Z] \\ A^*(Z)\Theta(B)(Z) + B^*(Z)\Theta(A)(Z) & = & 0 \in \mathbb{F}_{p^2}[Z] \end{array} \right. \tag{11}$$

where the expressions above belong now to the commutative ring $\mathbb{F}_{p^2}[Z]$ and the morphism of $\mathbb{F}_{p^2}[Z]$: $\sum a_i Z^i \mapsto \sum a_i^p Z^i$ is again denoted Θ. As $A(Z)$ and $B(Z)$ are polynomials of degree δ and $\leq \delta - 1$ whereas $f(Z)$ has degree 2δ, these two last equalities can be replaced with relations of divisibility :

$$\left\{ \begin{array}{lcl} f(Z) & | & A^*(Z)A(Z) + B^*(Z)B(Z)Z \\ f(Z) & | & A^*(Z)\Theta(B)(Z) + B^*(Z)\Theta(A)(Z). \end{array} \right. \tag{12}$$

As the degree of $B(Z)$ is $\leq \delta - 1$ and as $f(Z)$ factors over $\mathbb{F}_{p^2}$ into the product of two irreducible polynomials of degree δ, B and f are coprime i.e. $B(\alpha) \neq 0$ and $B(\alpha^p) \neq 0$. Evaluating right hand sides of (12) at α and α^p and replacing α^{-1} with α^{p^δ} (cf Lemma 5), one gets $h(X) = A(X^2) + XB(X^2) \in \mathcal{H}_{f(X^2)}$ with $B \neq 0$

$$\Leftrightarrow \quad \left\{ \begin{array}{lcl} A(\alpha^{p^\delta})A(\alpha) + B(\alpha^{p^\delta})B(\alpha) & = & 0 \\ A(\alpha^{p^{\delta+1}})A(\alpha^p) + B(\alpha^{p^{\delta+1}})B(\alpha^p) & = & 0 \\ \alpha A(\alpha^{p^\delta})\Theta(B)(\alpha) + B(\alpha^{p^\delta})\Theta(A)(\alpha) & = & 0 \\ \alpha^p A(\alpha^{p^{\delta+1}})\Theta(B)(\alpha^p) + B(\alpha^{p^{\delta+1}})\Theta(A)(\alpha^p) & = & 0. \end{array} \right.$$

If δ is even, then $A(\alpha^{p^\delta}) = A(\alpha)^{p^\delta}$ and $B(\alpha^{p^\delta}) = B(\alpha)^{p^\delta}$, therefore one gets the equivalent system

$$\left\{ \begin{array}{lcl} u^{p^\delta+1} & = & -1 \\ A(\alpha) & = & u \times B(\alpha) \\ A(\theta(\alpha)) & = & \theta(\frac{\alpha}{u}) \times B(\theta(\alpha)) \end{array} \right. \tag{13}$$

Consider for $u \in \mathbb{F}_{p^{2\delta}}$ satisfying $u^{p^\delta+1} = -1$ the unique polynomial P_u of $\mathbb{F}_{p^2}[Z]$ with degree $\leq 2\delta - 1$ defined by $P_u(\alpha) = u$ and $P_u(\theta(\alpha)) = \theta(\alpha/u)$. The relation (13) is equivalent to

$$\left\{ \begin{array}{lcll} u^{p^\delta+1} & = & -1 & \\ A & \equiv & P_u \times B & (\mathrm{mod}\ \tilde{f}) \\ A & \equiv & P_u \times B & (\mathrm{mod}\ \Theta(\tilde{f})). \end{array} \right.$$

Therefore $h(X) = A(X^2) + XB(X^2) \in \mathcal{H}_{f(X^2)}$ with $B \neq 0$ is equivalent to the following Cauchy interpolations problems

$$\mathcal{R}I_{P_u} \; : \; \begin{array}{l} \gcd(B(Z), f(Z)) = 1 \\ \dfrac{A(Z)}{B(Z)} \equiv P_u(Z) \pmod{f(Z)} \end{array}$$

for u such that $u^{p^\delta+1} = -1$.

As there is a unique solution (A, B) to RI_{P_u} with A monic (section 5.8 of [19]) for each u such that $u^{p^\delta+1} = -1$, and as two distinct u provide two distinct solutions, the set $\mathcal{H}_{f(X^2)} \setminus \mathbb{F}_{p^2}[X^2]$ has $p^\delta + 1$ elements.

If δ is odd, using the relations $A(\alpha^{p^\delta}) = A(\alpha^p)^{p^{\delta-1}}$ and $B(\alpha^{p^\delta}) = B(\alpha^p)^{p^{\delta-1}}$, one gets the equivalent system

$$\left\{ \begin{array}{rcl} u^{p^\delta-1} & = & -1/\alpha \\ A(\alpha) & = & \frac{\alpha}{u} \times B(\alpha) \\ A(\theta(\alpha)) & = & \theta(u) \times B(\theta(\alpha)) \end{array} \right.$$

which is equivalent to the interpolation problem $\mathcal{R}I_P$ where P is the unique polynomial of $\mathbb{F}_{p^2}[Z]$ with degree $\leq 2\delta - 1$ defined by $P(\alpha) = \frac{\alpha}{u}$ and $P(\theta(\alpha)) = \theta(u)$ for $u^{p^\delta-1} = -1/\alpha$. The number of elements of $\mathcal{H}_f$ is therefore $p^\delta + 1 + 0$ if δ is even and $(p^\delta - 1) + 2 = p^\delta + 1$ if δ is odd.

When $f(Y)$ is reducible, the relation (12) still holds. If δ is even then $g(Z)$ is the product of two irreducible polynomials $\tilde{g}(Z)$ and $\Theta(\tilde{g})(Z)$ belonging to $\mathbb{F}_{p^2}[Z]$ and the set $\mathcal{H}_f \bigcap \mathbb{F}_{p^2}[X^2]$ is $\{g(X^2), g^\natural(X^2), \tilde{g}(X^2)\Theta(\tilde{g}^\natural)(X^2), \tilde{g}^\natural(X^2)\Theta(\tilde{g})(X^2)\}$. If δ is odd, then $g(Z)$ is irreducible in $\mathbb{F}_{p^2}[Z]$ and the set $\mathcal{H}_f \bigcap \mathbb{F}_{p^2}[X^2]$ is $\{g(X^2), g^\natural(X^2)\}$. Consider β in $\mathbb{F}_{p^\delta}$ such that $g(\beta) = 0$. Then, for δ even, if $h(X) = A(X^2) + XB(X^2)$, with $B \neq 0$ is such that $h^\natural h = f(X^2)$ then $f(Z)$ and $B(Z)$ are coprime i.e. $B(\beta), B(1/\beta), B(\beta^p), B(1/\beta^p) \neq 0$. Indeed if $B(\beta) = 0$ then $B(\beta^p), B(1/\beta), B(1/\beta^p) \neq 0$ otherwise the condition on the degree of B would give $B = 0$. Furthermore according to the second relation of (12), $B^*(\beta^p)\Theta(A)(\beta^p) = 0$, so $A(\beta) = 0$ and $A^*(1/\beta) = 0$. According to (12), $B^*(1/\beta)\Theta(A)(1/\beta) = 0$, so $\Theta(A)(1/\beta) = 0$ and $A(1/\beta^p) = 0$. Then first part of (12) gives $B^*(1/\beta^p)B(1/\beta^p) = 0$ which is impossible. In the same way, one gets that $B(1/\beta), B(\beta^p), B(1/\beta^p) \neq 0$. Therefore

$h(X) = A(X^2) + XB(X^2) \in \mathcal{H}_{f(X^2)}$, $B \neq 0 \Leftrightarrow$

$$\left\{ \begin{array}{rcl} A(\beta)A(1/\beta) + B(\beta)B(1/\beta) & = & 0 \\ A(\beta^p)A(1/\beta^p) + B(\beta^p)B(1/\beta^p) & = & 0 \\ \beta\Theta(B)(\beta)A(1/\beta) + \Theta(A)(\beta)B(1/\beta) & = & 0 \\ 1/\beta\Theta(B)(1/\beta)A(\beta) + \Theta(A)(1/\beta)B(\beta) & = & 0 \\ \beta^p\Theta(B)(\beta^p)A(1/\beta^p) + \Theta(A)(\beta^p)B(1/\beta^p) & = & 0 \\ 1/\beta^p\Theta(B)(1/\beta^p)A(\beta^p) + \Theta(A)(1/\beta^p)B(\beta^p) & = & 0 \end{array} \right. \Leftrightarrow \left\{ \begin{array}{rcl} u^{p^\delta-1} & = & 1 \\ A(\beta) & = & u \times B(\beta) \\ A(\frac{1}{\beta}) & = & -\frac{1}{u} \times B(\frac{1}{\beta}) \\ A(\theta(\beta)) & = & \theta(\frac{\beta}{u}) \times B(\theta(\beta)) \\ A(\theta(\frac{1}{\beta})) & = & -\theta(\frac{u}{\beta}) \times B(\theta(\frac{1}{\beta})) \end{array} \right.$$

which is equivalent to $\mathcal{R}I_P$ where P is the unique polynomial of $\mathbb{F}_{p^2}[Z]$ with degree $\leq 2\delta-1$ defined by $P(\beta) = u, P(\frac{1}{\beta}) = -\frac{1}{u}, P(\theta(\beta)) = \theta(\frac{\beta}{u})$ and $P(\theta(\frac{1}{\beta})) = -\theta(\frac{u}{\beta})$ for $u^{p^\delta-1} = 1$. If δ is odd, then g is irreducible over $\mathbb{F}_{p^2}$ and $g^\natural$ is irreducible over $\mathbb{F}_{p^2}$ with root $1/\beta$, therefore for $B \neq 0$ with degree $\deg(B) \leq \delta - 1$, $B(\beta), B(1/\beta) \neq 0$ and $h(X) = A(X^2) + XB(X^2) \in \mathcal{H}_{f(X^2)}$, $B \neq 0 \Leftrightarrow$

$$\left\{ \begin{array}{rcl} u\theta^\delta(u) & = & \beta \\ A(\beta) & = & u \times B(\beta) \\ A(\frac{1}{\beta}) & = & -\frac{1}{u} \times B(\frac{1}{\beta}) \end{array} \right.$$

which is equivalent to $\mathcal{R}I_P$ where $P(\beta) = u, P(\frac{1}{\beta}) = -\frac{1}{u}$ for $u^{p^\delta+1} = \beta$. The number of elements of $\mathcal{H}_f$ is therefore $p^\delta - 1 + 4 = p^\delta + 3$ if δ is even and $(p^\delta + 1) + 2 = p^\delta + 3$ if δ is odd.

■

Example 1 *Consider $\mathbb{F}_4 = \mathbb{F}_2(a)$, θ Frobenius automorphism, $R = \mathbb{F}_4[X, \theta]$ and $f(Y) = Y^2 + Y + 1 \in \mathbb{F}_2[Y]$ irreducible and self-reciprocal. The polynomial $f(Z)$ factorizes in $\mathbb{F}_4[Z]$ as $f(Z) = (Z+a)(Z+a^2)$ where $a^2+a+1 = 0$. As $\delta = \deg(f(Y))/2 = 1$ is odd, the equation $h^\natural h = f(X^2)$ has two solutions in $R \bigcap \mathbb{F}_4[X^2]$ namely $X^2 + a$ and $X^2 + a^2$. Consider $\alpha \in \mathbb{F}_4$ such that $f(\alpha) = 0$ and u such that $u^{2^\delta - 1} = -1/\alpha$ i.e. $\alpha = a$ and $u = a^2$. The polynomial $P \in \mathbb{F}_4[Z]$ of degree ≤ 1 such that $P(\alpha) = \alpha/u$ and $P(\alpha^2) = u^2$ i.e. $P(a) = a^2$ and $P(a^2) = a$ is $P(Z) = Z+1$ and the unique solution (A, B) in $\mathbb{F}_4[Z] \times \mathbb{F}_4[Z]$ of $\frac{A}{B} \equiv Z+1 \pmod{Z^2+Z+1}$ is $(A, B) = (Z + 1, 1)$. Therefore, the equation $h^\natural h = f(X^2)$ has one solution in $R \setminus \mathbb{F}_4[X^2]$ namely $(X^2 + 1) + X \times 1$. The set $\mathcal{H}_f$ is $\{X^2 + a, X^2 + a^2, X^2 + X + 1\}$ and has $2^\delta + 1 = 3$ elements.*

Example 2 *Consider $\mathbb{F}_4 = \mathbb{F}_2(a)$, θ Frobenius automorphism, $R = \mathbb{F}_4[X, \theta]$ and $f(Y) = (Y^3 + Y + 1)(Y^3 + Y^2 + 1) \in \mathbb{F}_2[Y]$ self-reciprocal and product of two irreducible polynomials. As $\delta = \deg(f(Y))/2 = 1$ is odd, the equation $h^\natural h = f(X^2)$ has two solutions in $R \bigcap \mathbb{F}_4[X^2]$ namely $X^6 + X^2 + 1$ and $X^6 + X^4 + 1$. Consider $\beta \in \mathbb{F}_8$ such that $\beta^3 + \beta^2 + 1 = 0$ and u such that $u^{2^3+1} = \beta$ for example $u = v^3$ where $v^6 + v^4 + v^3 + v + 1 = 0$. The polynomial $P \in \mathbb{F}_4[Z]$ monic of degree ≤ 3 such that $P(\beta) = u$ and $P(1/\beta) = -1/u$ is $P(Z) = aZ^4 + Z^3 + Z^2 + 1$ and the unique solution (A, B) in $\mathbb{F}_4[Z] \times \mathbb{F}_4[Z]$ of $\frac{A}{B} \equiv P(Z) \pmod{f(Z)}$ with A monic is $(A, B) = (Z^3 + a, aZ^2 + a^2Z + 1)$. Therefore, $h(X) = X^6 + a + X(aX^4 + a^2X^2 + 1) = X^6 + a^2X^5 + aX^3 + X + a$ is solution to the equation $h^\natural h = f(X^2)$ in $R \setminus \mathbb{F}_4[X^2]$. The 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.*

Remark 3 *If $f(Y)$ is irreducible then $\overline{\mathcal{H}}_{f(X^2)} = \mathcal{H}_{f(X^2)}$ and if $f(Y) = g(Y)g^\natural(Y)$ with $g(Y) \neq g^\natural(Y)$ irreducible, then $\overline{\mathcal{H}}_{f(X^2)} = \mathcal{H}_{f(X^2)} \setminus \{g(X^2), g^\natural(X^2)\}$. In both cases, $\overline{\mathcal{H}}_f$ has $p^\delta + 1$ elements.*

The proposition below gives a formula for the number of self-dual θ-cyclic and θ-negacyclic codes whose dimension is prime to p. It is deduced from Lemma 6, Lemma 2 and Proposition 2.

Proposition 4 *Consider p prime number, $\theta : \mathbb{F}_{p^2} \to \mathbb{F}_{p^2}, x \mapsto x^p$ the Frobenius automorphism, $k \in \mathbb{N}^*$ not divisible by p. For $\epsilon \in \{-1, 1\}$, consider $\mathcal{F}_{k,\epsilon}$ and $\mathcal{G}_{k,\epsilon}$ defined in Lemma 2. For $f(Y)$ in $\mathcal{F}_{k,\epsilon} \bigcup \mathcal{G}_{k,\epsilon}$, denote $\delta = \deg(f(Y))/2$ and for $p = 2$, $N_\epsilon = 1$; for p odd,*

$$N_\epsilon = \begin{cases} 0 & \text{if} \quad k \equiv 1 \pmod 2 \text{ and } \epsilon \neq (-1)^{\frac{p+1}{2}} \text{ or } k \equiv 0 \pmod 2 \text{ and } \epsilon = 1 \\ 1 & \text{if} \quad k \equiv 0 \pmod 2 \text{ and } \epsilon = -1 \\ 2 & \text{if} \quad k \equiv 1 \pmod 2 \text{ and } \epsilon = (-1)^{\frac{p+1}{2}}. \end{cases}$$

The number of self-dual (θ, ϵ)-constacyclic codes with dimension k defined over $\mathbb{F}_{p^2}$ is

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

Proof. According to Lemma 2,

$$\#\mathcal{H}_{X^{2k}-\epsilon} = N_\epsilon \times \prod_{f(Y)\in\mathcal{F}_{k,\epsilon}} \#\mathcal{H}_{f(X^2)} \times \prod_{f(Y)\in\mathcal{G}_{k,\epsilon}} \#\mathcal{H}_{f(X^2)}$$

The expression of N_ϵ is deduced from Proposition 2 for p odd prime number and Remark 2 for $p = 2$. The expressions of the two products $\prod_{f(Y)\in\mathcal{F}_{k,\epsilon}} \#\mathcal{H}_{f(X^2)}$ and $\prod_{f(Y)\in\mathcal{G}_{k,\epsilon}} \#\mathcal{H}_{f(X^2)}$ come from Lemma 6. ∎

Remark 4 *According to Proposition 6.2 of [14], the number of self-dual 2-quasi-cyclic codes of dimension k over $\mathbb{F}_{p^r}$ with k prime to p depends on the factorization of Y^k-1 over $\mathbb{F}_{p^r}[Y]$:*

$$N \prod_{f\in\mathcal{F}} (p^{r\delta}+1) \prod_{f\in\mathcal{G}} (p^{r\delta}+3)$$

where 2δ is the degree of f; $\mathcal{F}$ (resp. $\mathcal{G}$) is the set of all monic factors $f(Y) = f^\natural(Y)$ in $\mathbb{F}_{p^r}[Y]$ of Y^k-1 with degree > 1 such that $f(Y)$ is irreducible (resp. $f(Y) = g(Y)g^\natural(Y)$ with $g(Y) \neq g^\natural(Y)$ monic irreducible in $\mathbb{F}_{p^r}[Y]$); $N = 1$ if $p = 2$; $N = 2$ if p is odd and $k \equiv 1 \pmod 2$; $N = 4$ if p is odd and $k \equiv 0 \pmod 2$. Therefore, for k odd number, $p = 2$ or $p \equiv 3 \pmod 4$, the number of self-dual θ-cyclic codes over $\mathbb{F}_{p^2}$ with dimension k is equal to the number of self-dual 2-quasi-cyclic codes over $\mathbb{F}_p$ with dimension k.

In next subsection, the construction of the sets $\mathcal{H}_{f(X^2)^m}$ is considered.

5.2 Construction of the sets $\mathcal{H}_{f(X^2)^{p^s}}$ for $s > 0$

The following technical Lemma will be useful in the proof of Lemma 8. It can be deduced from the construction given in Lemma 6.

Lemma 7 *Consider $R = \mathbb{F}_{p^2}[X;\theta]$ with p prime number, $\theta : x \mapsto x^p$, $m \in \mathbb{N}$ and $f(Y)$ in $\mathbb{F}_p[Y]$ with degree $d = 2\delta > 1$ such that $f(Y) = f^\natural(Y)$ with $f(Y)$ irreducible or product of two irreducible polynomials with degree δ. The constant coefficients of the elements of $\mathcal{H}_{f(X^2)}$ are squares in $\mathbb{F}_{p^2}$.*

Proof.

Consider $h \in \mathcal{H}_{f(X^2)} \setminus \mathbb{F}_{p^2}[X^2]$ and $A(X^2), B(X^2) \in R$ with $B \neq 0$ such that $h(X) = A(X^2) + XB(X^2)$. According to (11), one gets $\Theta(A)(Z) \times (A^*(Z)A(Z) + B^*(Z)B(Z)Z) - (A^*(Z)\Theta(B)(Z) + B^*(Z)\Theta(A)(Z)) = \Theta(A)(Z)\lambda f(Z)$ where λ is the constant coefficient of h. As $B \neq 0$, $f(Z)$ and $A(Z)$ have no common factor, therefore, $f(Z)$ divides $A(Z)\Theta(A)(Z) - ZB(Z)\Theta(B)(Z)$. These two polynomials are monic with the same degree, therefore, they are equal and $A^* = \lambda\Theta(A)$. One deduces that $\lambda^{p+1} = 1$ and therefore, λ is a square in $\mathbb{F}_{p^2}$.

The elements of $\mathcal{H}_{f(X^2)} \bigcap \mathbb{F}_{p^2}[X^2]$ are given in proof of Lemma 6. Namely, if $f(Y)$ is irreducible,

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

Denote λ the constant coefficient of $\tilde{f}$. As the constant coefficient of f is equal to 1 (because $f(Y) = f^\natural(Y)$ and f is monic), one has $1 = \lambda\lambda^p$, therefore λ is a square in $\mathbb{F}_{p^2}$.

If $f(Y) = g(Y)g^\natural(Y)$ then

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

As $g(Y)$ and $g^\natural(Y)$ belong to $\mathbb{F}_p[Y]$ their constant coefficients are squares in $\mathbb{F}_{p^2}$. Denotes μ the constant coefficient of $\tilde{g}$, then the constant coefficient of $\tilde{g}\Theta(\tilde{g}^\natural)$ is $\mu\theta(\frac{1}{\mu}) = \frac{1}{\mu^{p-1}}$ which is a square in $\mathbb{F}_{p^2}$. ∎

Lemma 8 generalizes Lemma 4 and uses the same type of arguments linked to the factorization of skew polynomials.

Lemma 8 *Consider $R = \mathbb{F}_{p^2}[X;\theta]$ with p prime number, $\theta : x \mapsto x^p$, $m \in \mathbb{N}^*$ and $f(Y)$ in $\mathbb{F}_p[Y]$ with degree $d = 2\delta > 1$ in Y such that $f(Y) = f^\natural(Y)$ with $f(Y)$ irreducible or product of two irreducible polynomials with degree δ. The set $\overline{\mathcal{H}}_{f(X^2)^m}$ has $(1+p^\delta)p^{\delta(m-1)}$ elements and is equal to*

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

Proof.

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

1. Assume that $f(Y)$ is irreducible in $\mathbb{F}_p[Y]$.

   Consider $h \in R$ such that $h^\natural h = f^m$ and $f \not| h$. As f is irreducible in $\mathbb{F}_p[X^2]$ and central, all the irreducible factors of h are bounded by f with the same degree d (Lemma 13 (2) of [4] or [16] page 6) :

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

   Furthermore, f does not divide h, therefore according to Proposition 1 (or Proposition 16 of [4]), for all $j \in \{1 \dots m-1\}$, $H_j H_{j+1} \neq f$.

   According to Lemma 5, d is even therefore the order of θ divides d and part 3. of Lemma 1 enables to conclude that

   $$h^\natural = \prod_{i=m}^{1} \frac{1}{\mu_i} H_i^\natural \mu_i$$

   where $\mu_i = (H_1 \cdots H_{i-1})_0$. 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 each factorization of f commutes), according to Proposition 1 (or Proposition 16 of [4]), $f^m = h^\natural h$ 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, $\frac{1}{\mu_1} H_1^\natural \mu_1 H_1 = f$ and proceeding by induction, one gets

   $$\frac{1}{\mu_j} H_j^\natural \mu_j H_j = f \text{ and } H_{j+1} \neq \frac{1}{\mu_j} H_j^\natural \mu_j. \tag{14}$$

   Conversely, if $h = H_1 \cdots H_m$ with $\frac{1}{\mu_j} H_j^\natural \mu_j H_j = f, H_{j+1} \neq \frac{1}{\mu_j} H_j^\natural \mu_j, \mu_j = (H_1 \cdots H_{j-1})_0$, then $h^\natural h = f^m$ and $H_j H_{j+1} \neq f$. Furthermore, the skew polynomials H_j are all

irreducible because they are nontrivial factors of f and $f(Y) \in \mathbb{F}_p[Y]$ is irreducible, therefore according to Proposition 1 (or Proposition 16 of [4]), the skew polynomial h is not divisible by f and it belongs to $\overline{\mathcal{H}}_{f(X^2)^m}$.

The set $\overline{\mathcal{H}}_{f^m}$ is therefore equal to the set

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

The conclusion follows by observing that $h = H_1 \cdots H_m$ with $\frac{1}{\mu_j} H_j^{\natural} \mu_j H = f$ and $H_{j+1} \neq \frac{1}{\mu_j} H_j^{\natural} \mu_j$ is equivalent to $h = \left(h_1 \frac{1}{\nu_1}\right) \cdots \left(h_m \frac{1}{\nu_m}\right) \prod_{j=1}^{m} \nu_j$ with $h_j^{\natural} h_j = f$ and $h_{j+1} \neq \nu_j h_j^{\natural} \frac{1}{\nu_j}$ where $h_j = (\nu_0 \cdots \nu_j) H_j \frac{1}{(\nu_0 \cdots \nu_j)}$ and ν_j is such that $\nu_j^2 = (H_j)_0 = (h_j)_0$ and ν_j belongs to $\mathbb{F}_{p^2}$ (according to Lemma 7).

2. Assume that $f(Y) = g(Y) g^{\natural}(Y)$ with $g(Y) \neq g^{\natural}(Y)$ irreducible in $\mathbb{F}_p[Y]$. Like in the previous case it suffices to prove that $\overline{\mathcal{H}}_{f^m} = \Big\{H_1 \cdots H_m \mid \frac{1}{\mu_i} H_i^{\natural} \mu_i H_i = f,$

$\mu_i = (H_1 \cdots H_{i-1})_0, H_{i+1} \neq \frac{1}{\mu_i} H_i^{\natural} \mu_i, g, g^{\natural}\Big\}$.

Consider $h = h(X) \in R$ such that $h^{\natural} h = f^m$ and $g, g^{\natural}$ do not divide h. Let us prove that h can be written as the product of m monic skew polynomials of degree d bounded by f. As h divides f^m, according to Theorem 4.1 of [7], $h = \mathrm{lclm}(G, \tilde{G})$ where $G = \mathrm{gcrd}(h, g^m)$ and $\tilde{G} = \mathrm{gcrd}(h, (g^{\natural})^m)$. As $g(Y)$ (resp. $g^{\natural}(Y)$) is irreducible in $\mathbb{F}_p[Y]$, the skew polynomial G (resp. $\tilde{G}$) is the product of N (resp. $\tilde{N}$) monic irreducible skew polynomials bounded by 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 bounded by g (resp. $g^{\natural}$). According to Proposition 1, as g (resp. $g^{\natural}$) does not divide G (resp $\tilde{G}$), these factorizations are unique. Therefore, according to Theorem 14 of [17], $h = H_1 \cdots H_N$ where $H_i = \mathrm{lclm}(\overline{G_i}, \overline{\tilde{G}_i})$ with $R/\overline{G_i}R$ and R/G_iR (resp. $R/\overline{\tilde{G}_i}R$ and $R/\tilde{G}_iR$) isomorphic modules. As G_i is bounded by g, according to Corollary of Theorem 10 of [10], $\overline{G_i}$ is also bounded by g. As G_i and $\tilde{G}_i$ are right coprime with same degree $d/2$, so are $\overline{G}_i$ and $\overline{\tilde{G}}_i$ therefore H_i is a skew polynomial of degree d which divides f. Lastly, as h has degree md one gets $N = m$. Therefore

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

By hypothesis $h^{\natural} h = f^m = \prod_{i=m}^{1} \frac{1}{\mu_i} H_i^{\natural} \mu_i \prod_{i=1}^{m} H_i$ is the product of $2m$ monic factors of degree d bounded by f and as the decomposition of f^m (as the product of monic factors of degree d dividing f) is not unique, according to Proposition 1, there exists two consecutive factors in $h^{\natural} h$ whose product is divisible by g or $g^{\natural}$. Such a product can be of three types : $\frac{1}{\mu_{i+1}} H_{i+1}^{\natural} \mu_{i+1} \frac{1}{\mu_i} H_i^{\natural} \mu_i$, $H_i H_{i+1}$ or $\frac{1}{\mu_1} H_1^{\natural} \mu_1 H_1$. However g and $g^{\natural}$ do not divide $H_i H_{i+1}$, otherwise, they would divide h, and they do not divide $\frac{1}{\mu_{i+1}} H_{i+1}^{\natural} \mu_{i+1} \frac{1}{\mu_i} H_i^{\natural} \mu_i = \frac{1}{\mu_i} (H_i H_{i+1})^* \mu_i$ either. Therefore g *or* $g^{\natural}$ divides $\frac{1}{\mu_1} H_1^{\natural} \mu_1 H_1$. Using Lemma 1, one gets that g *and* $g^{\natural}$ divide $\frac{1}{\mu_1} H_1^{\natural} \mu_1 H_1$, therefore f divides $\frac{1}{\mu_1} H_1^{\natural} \mu_1 H_1$

and as these two skew polynomials are monic with the same degree they are equal. By induction, one gets

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

Conversely, consider $h = \prod_{i=1}^{m} H_i$, with $\frac{1}{\mu_i}H_i^\natural\mu_i H_i = f$, $H_{i+1} \neq \frac{1}{\mu_i}H_i^\natural\mu_i, g, g^\natural$. According to Lemma 1, $h^\natural = \prod_{i=m}^{1} \frac{1}{\mu_i}H_i^\natural\mu_i$, therefore $h^\natural h = f^m$. It remains to prove that g and $g^\natural$ do not divide h. Assume that g divides h, all the 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 1, there exists i such that g divides H_iH_{i+1}. Consider $u \in R$ such that $H_iH_{i+1} = gu$. As both H_i and H_{i+1} are bounded by f, they are the products of two irreducible polynomials bounded by g and $g^\natural$, therefore the skew polynomial u is the product of two irreducible skew polynomials bounded by $g^\natural$ and u divides $(g^\natural)^2$. The relation $(H_iH_{i+1})^* = (g^\natural u)^*$ gives $H_{i+1}^\natural\lambda_i H_i^\natural = \lambda_i u^\natural g^\natural$ where $\lambda_i := (H_i)_0$. Multiplying on the left by $\mu_{i+1}H_{i+1}\frac{1}{\mu_{i+1}}$ and on the right by $\mu_i H_i\frac{1}{\mu_i}$ yields $f^2 = (\frac{1}{\lambda_i}\mu_{i+1}H_{i+1}\frac{1}{\mu_{i+1}}\lambda_i u^\natural g^\natural\mu_i)(H_i\frac{1}{\mu_i})$. As f^2 is central, the two terms of the product commute and $f^2 = H_i(\frac{1}{\mu_i}\frac{1}{\lambda_i}\mu_{i+1})H_{i+1}(\frac{1}{\mu_{i+1}}\lambda_i)u^\natural g^\natural\mu_i = H_iH_{i+1}\frac{1}{\mu_i}u^\natural g^\natural\mu_i = gu\frac{1}{\mu_i}u^\natural g^\natural\mu_i$ therefore $(u\frac{1}{\mu_i}u^\natural\mu_i)g^\natural = g(g^\natural)^2 = uvg$, where $v \in R$ is such that $uv = (g^\natural)^2$. One gets the relation $\frac{1}{\mu_i}u^\natural\mu_i g^\natural = vg$. The skew polynomials g and $g^\natural$ divide vg and $\deg(vg) = \deg(f)$, therefore $f = vg$, $v = g^\natural$ and $u = g^\natural$ which is impossible because $H_iH_{i+1} \neq f$.

3. The number of elements of $\overline{\mathcal{H}}_{f(X^2)^m}$ follows from the fact that $\overline{\mathcal{H}}_{f(X^2)}$ has $1+p^\delta$ elements.

■

Example 3 . *Consider* $\mathbb{F}_4 = \mathbb{F}_2(a)$, $\theta : x \mapsto x^2$ *and* $f(Y) = Y^2 + Y + 1 \in \mathbb{F}_2[Y]$. *According to Example 1, the set* $\mathcal{H}_{f(X^2)}$ *is* $\{X^2 + X + 1, X^2 + a, X^2 + a^2\}$. *The* $6 = (1 + 2^1) \times 2^1$ *skew polynomials of* $\overline{\mathcal{H}}_{f(X^2)^2}$ *are :*
$X^4 + X^3 + a^2X^2 + a^2X + a = (X^2 + X + 1)(1/1)(X^2 + a)(1/a^2)a^2$,
$X^4 + X^3 + aX^2 + aX + a^2 = (X^2 + X + 1)(1/1)(X^2 + a^2)(1/a)a$,
$X^4 + a^2 = (X^2 + a)(X^2 + a) = (X^2 + a)(1/a^2)(X^2 + a)(1/a^2)a$,
$X^4 + a^2X^3 + a^2X^2 + X + a = (X^2 + a)(X^2 + a^2X + 1) = (X^2 + a)(1/a^2)(X^2 + X + 1)(1/1)a^2$,
$X^4 + a = (X^2 + a^2)(X^2 + a^2) = (X^2 + a^2)(1/a)(X^2 + a^2)(1/a)a^2$,
$X^4 + aX^3 + aX^2 + X + a^2 = (X^2 + a^2)(X^2 + aX + 1) = (X^2 + a^2)(1/a)(X^2 + X + 1)(1/1)a$.

Example 4 . *Consider* $\mathbb{F}_4 = \mathbb{F}_2(a)$, $\theta : x \mapsto x^2$ *and* $f(Y) = (Y^3 + Y + 1)(Y^3 + Y^2 + 1) \in \mathbb{F}_2[Y]$. *There are* $72 = (1+2^3)\times 2^3$ *skew polynomials in* $\overline{\mathcal{H}}_{f(X^2)^2}$. *Here is one of these elements :* $h = X^{12} + aX^{11} + a^2X^{10} + a^2X^7 + a^2X^6 + X^5 + a^2X^2 + aX + a = (h_1\frac{1}{\nu_1}) \times (h_2\frac{1}{\nu_2}) \times (\nu_1\nu_2)$ *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* $\overline{\mathcal{H}}_f$ *(constructed in example 2),* $\nu_1 = a^2$ *is the square root of the constant coefficient of* h_1 *and* $\nu_2 = 1$.

Proposition 5 *Consider* $R = \mathbb{F}_{p^2}[X;\theta]$ *with* p *prime number,* $\theta : x \mapsto x^p$, $s \in \mathbb{N}$ *and* $f(Y)$ *in* $\mathbb{F}_p[Y]$ *with degree* $d = 2\delta > 1$ *in* Y *such that* $f(Y) = f^\natural(Y)$.

- *If $f(Y)$ is irreducible, the set $\mathcal{H}_{f(X^2)^{p^s}}$ has $\dfrac{p^{\delta(p^s+1)}-1}{p^\delta-1}$ elements.*
- *If $f(Y)=g(Y)g^\natural(Y)$ with $g(Y)\neq g^\natural(Y)$ irreducible in $\mathbb{F}_p[Y]$, the set $\mathcal{H}_{f(X^2)^{p^s}}$ has $\dfrac{\left(p^{\delta(p^s+1)}-2p^s-3\right)\left(1+p^\delta\right)+4p^s+4}{\left(p^\delta-1\right)^2}$ elements.*

Proof.

Assume that $f(Y)$ is irreducible in $\mathbb{F}_p[Y]$. According to Lemma 3, $\mathcal{H}_{f(X^2)^{p^s}}=\bigsqcup_{i=0}^{\lfloor\frac{p^s}{2}\rfloor} f^i\,\overline{\mathcal{H}}_{f(X^2)^{p^s-2i}}$ and according to Lemma 8, $\overline{\mathcal{H}}_{f(X^2)^m}$ has $(1+p^\delta)(p^\delta)^{m-1}$ if $m\neq 0$ and 1 element if $m=0$. Therefore $\mathcal{H}_{f(X^2)^{p^s}}$ has $\sum_{i=0}^{(p^s-1)/2}(1+p^\delta)(p^\delta)^{p^s-2i-1}$ elements if p is odd and $1+\sum_{i=0}^{2^{s-1}-1}(1+2^\delta)(2^\delta)^{2^s-2i-1}$ elements otherwise. In both cases one gets $\#\mathcal{H}_{f(X^2)^{p^s}}=\frac{p^{\delta(p^s+1)}-1}{p^\delta-1}$. Assume that $f(Y)=g(Y)g^\natural(Y)$ with $g(Y)\neq g^\natural(Y)$ irreducible in $\mathbb{F}_p[Y]$, then according to Lemma 3, $\mathcal{H}_{f(X^2)^{p^s}} = \bigsqcup_{i=0}^{p^s}\bigsqcup_{j=0}^{p^s-i} g(X^2)^j g^\natural(X^2)^{i-j}\overline{\mathcal{H}}_{f(X^2)^{p^s-i-j}}$. Furthermore, the set $\overline{\mathcal{H}}_{f(X^2)^m}$ 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 $\mathcal{H}_{f(X^2)^{p^s}}$ is $\displaystyle\sum_{i=0}^{p^s}\left[\sum_{j=0}^{p^s-i-1}(1+p^\delta)(p^\delta)^{p^s-i-1-j}+1\right]=\frac{\left(p^{\delta(p^s+1)}-2p^s-3\right)\left(1+p^\delta\right)+4p^s+4}{\left(p^\delta-1\right)^2}$.

■

Example 5 *Consider $f(Y)=Y^2+Y+1$ defined in Example 3. The skew polynomials h satisfying $h^\natural h=f^2$ are $f=X^4+X^2+1\in f^1\times\overline{\mathcal{H}}_{f^0}$ (whose factorization is not unique : $f=(X^2+X+1)(X^2+X+1)=(X^2+a)(X^2+a^2)=(X^2+a^2)(X^2+a)$) and the six skew polynomials, who have a unique factorization into the product of irreducible monic polynomials and who describe $f^0\times\overline{\mathcal{H}}_{f(X^2)^2}$ given in Example 3.*

Example 6 *Consider $f(Y)=(Y^3+Y^2+1)(Y^3+Y+1)$ with degree $d=6$ defined in Example 4. There are 93 skew polynomials h satisfying $h^\natural h=(X^6+X^4+1)^2(X^6+X^2+1)^2$. The only one which is divisible by X^6+X^4+1 and X^6+X^2+1 is $(X^6+X^4+1)(X^6+X^2+1)$. There are 10 polynomials which are divisible by X^6+X^4+1 without being divisible by X^6+X^2+1; 10 other skew polynomials which are divisible by X^6+X^2+1 without being divisible by X^6+X^4+1 and 72 skew polynomials which are not divisible by X^6+X^2+1 or X^6+X^4+1.*

6 Conclusion and perspectives

The following theorem gives the number of self-dual θ-cyclic and θ-negacyclic codes of any dimension over $\mathbb{F}_{p^2}$ for θ Frobenius automorphism.

Theorem 1 *Consider p prime number, $\theta: x\mapsto x^p$ Frobenius automorphism, $k\in\mathbb{N}^*$ and $s,t\in\mathbb{N}$ such that $k=p^st$ with t not divisible by p. For $\epsilon\in\{-1,1\}$, consider $\mathcal{F}_{k,\epsilon}$ and $\mathcal{G}_{k,\epsilon}$ defined in Lemma 2. For $f(Y)$ in $\mathcal{F}_{k,\epsilon}\bigcup\mathcal{G}_{k,\epsilon}$, denote $\delta=\deg(f(Y))/2$ and for $p=2$,*

$$N_\epsilon = \begin{cases} 1 & \text{if} \quad s = 0 \\ 3 & \text{if} \quad s > 0 \end{cases} \text{; for } p \text{ odd,}$$

$$N_\epsilon = \begin{cases} 0 & \text{if} \quad k \equiv 1 \pmod 2 \text{ and } \epsilon \neq (-1)^{\frac{p+1}{2}} \\ & \text{or} \quad k \equiv 0 \pmod 2 \text{ and } \epsilon = 1 \\ 1 & \text{if} \quad k \equiv 0 \pmod 2 \text{ and } \epsilon = -1 \\ 2\dfrac{p^{(p^s+1)/2}-1}{p-1} & \text{if} \quad k \equiv 1 \pmod 2 \text{ and } \epsilon = (-1)^{\frac{p+1}{2}}. \end{cases}$$

The number of self-dual (θ, ϵ)-constacyclic codes of dimension k over $\mathbb{F}_{p^2}$ is
$$N_\epsilon \times \prod_{f(Y)\in\mathcal{F}_{k,\epsilon}} \frac{p^{\delta(p^s+1)}-1}{p^\delta-1} \times \prod_{f(Y)\in\mathcal{G}_{k,\epsilon}} \frac{\left(p^{\delta(p^s+1)}-2p^s-3\right)\left(1+p^\delta\right)+4p^s+4}{\left(p^\delta-1\right)^2}.$$

Proof. According to Lemma 2,

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

The expression of N_ϵ is deduced from Proposition 2 for p odd prime number and Remark 2 for $p = 2$. The expressions of the two products $\prod_{f(Y)\in\mathcal{F}_{k,\epsilon}} \#\mathcal{H}_{f(X^2)^{p^s}}$ and $\prod_{f(Y)\in\mathcal{G}_{k,\epsilon}} \#\mathcal{H}_{f(X^2)^{p^s}}$ come from Proposition 5. ∎

Remark 5 *Proposition 2 is a particular case of Theorem 1 for $t = 1$ while Proposition 4 is a particular case for $s = 0$.*

To conclude, this formula should be generalized for self-dual (θ, ϵ)-codes defined over $\mathbb{F}_q$ with θ automorphism of order 2. A future work would consist in studying the case when θ is an automorphism of order > 2.

Lastly, one can hope that these constructions help for the study of the minimal distances of self-dual skew codes. Some experimental results and observations in dimension a power of p were made and need to be examined in more details.

Acknowledgments

I thank Felix Ulmer for his encouragement and his fruitful remarks.

References

[1] Bakshi, Gurmeet K. and Raka, Madhu, *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. and Ulmer, F., *Coding with skew polynomial rings*, Journal of Symbolic Computation, 44, 1644-1656 (2009).

[3] Boucher D., Ulmer F. *A note on the dual codes of module skew codes*, Lecture Notes in Computer Science, 2011, Volume 7089, Cryptography and Coding, Pages 230-243

[4] Boucher D., Ulmer F. *Self-dual skew codes and factorization of skew polynomials* Journal of Symbolic Computation, Volume 60, January 2014, Pages 4761

[5] Caruso X. and Leborgne J. *Some algorithms for skew polynomials over finite fields* arXiv:1212.3582, 2012

[6] Hai Q. Dinh *Repeated-root constacyclic codes of length* $2p^s$ Finite Fields and Their Applications 18 (2012) 133-143

[7] Giesbrecht, M., *Factoring in skew-polynomial rings over finite fields.* J. Symbolic Comput. 1998, 26 (4), 463–486.

[8] Guenda K., Gulliver T.A. *Self-dual Repeated Root Cyclic and Negacyclic Codes over Finite Fields* 2012 IEEE International Syposium on Information Theory Proceedings

[9] Han, Sunghyu and Kim, Jon-Lark and Lee, Heisook and Lee, Yoonjin, *Construction of quasi-cyclic self-dual codes*, Finite Fields and their Applications, 18, 2012, 3, 613–633

[10] Jacobson, N. *The Theory of Rings* Mathematical Surveys and Monographs, Vol 2, American Mathematical Society, 1943

[11] Jia, S., Ling S., Xing C. *On Self-Dual Cyclic Codes Over Finite Fields*, IEEE Transactions on Information Theory, Vol. 57, No. 4, 2011

[12] Kai, X. and Zhu, S., *On cyclic self-dual codes*, Applicable Algebra in Engineering, Communication and Computing, 19, 2008, 6, 509–525,

[13] Lidl, R., 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.

[14] Ling, San and Solé, Patrick, *On the algebraic structure of quasi-cyclic codes. I. Finite fields*, IEEE Trans. Inform. Theory, 47, 2001, 7, 2751–2760

[15] Ling, San and Niederreiter, Harald and Solé, Patrick, *On the algebraic structure of quasi-cyclic codes IV : Repeated Roots Chain rings*, Designs, Codes and Cryptography., 38, 2006, 337–361

[16] Odoni, R. W. K. *On additive polynomials over a finite field* Proceedings of the Edinburgh Mathematical Society (199) 42, 1-16

[17] O. Ore, *Theory of Non-Commutative Polynomials*, *The Annals of Mathematics*, 2nd Ser, Vol. 34, No. 3. pp 480-508 (1933)

[18] Siap, Irfan and Abualrub, Taher and Aydin, Nuh and Seneviratne, Padmapani, *Skew cyclic codes of arbitrary length*, Int. J. Inf. Coding Theory, 2, 2011, 1, 10–20

[19] von zur Gathen, Joachim and Gerhard, Jürgen, *Modern computer algebra*, Cambridge University Press, Cambridge,2013