A first step towards the skew duadic codes

Delphine Boucher

A first step towards the skew duadic codes.

D. Boucher *

July 11, 2017

Abstract

This text gives a first draft of the definition of θ-duadic codes where θ is an automorphism of $\mathbb{F}_q$. A link with the weakly self-dual θ-cyclic codes is established. A construction and an enumeration is provided when q is the square of a prime number p. Lastly a parametrization of irreducible skew polynomials of $\mathbb{F}_{p^2}[X;\theta]$ is given as an extension of this construction.

1 Introduction

A linear code with length n and dimension k defined 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 $\mathbb{F}_q[X]/(X^n-1)$. The monic generator g of this principal ideal divides X^n-1 and is called the generator polynomial of the code. For n coprime with q, the polynomial g can be characterized by its defining set S, namely a subset of $\{0,\dots,n-1\}$ such that $g(X)=\prod_{i\in S}(X-\alpha^i)$ where α is a primitive nth root of unity in an extension of $\mathbb{F}_q$. For n odd number coprime with q, the class of duadic codes of length n is a sub-family of the family of cyclic codes of length n and dimension $(n\pm 1)/2$. Their generators are divisors of $(X^n-1)/(X-1)$ with degree $(n\pm 1)/2$ and with specific designing sets (see chapter of [7] for an introduction to duadic codes). A weakly self-dual linear code is a code who is a subset of its annihilator (with respect to the scalar product). It is self-dual if he coincides with its annihilator. The class of duadic codes contains good codes, the most famous being the binary Golay code G_{23}, which is a Quadratic Residue code. The dual of G_{23} is in fact weakly self-dual and G_{23} can be extended to the famous self-dual binary Golay code G_{24}.

For θ automorphism of a finite field $\mathbb{F}_q$, θ-cyclic codes (also called skew cyclic codes) of length n were defined in [1]. These codes are such that a right circular shift of each codeword gives another word who belongs to the code after application of θ to each of its n coordinates. If θ is the identity, θ-cyclic codes are cyclic codes. Skew cyclic codes have an interpretation in the Ore ring $R=\mathbb{F}_q[X;\theta]$ of skew polynomials where multiplication is defined by the rule $X\cdot a=\theta(a)X$ for a in $\mathbb{F}_q$.

This text gives a first draft of the definition and of the construction of θ-duadic codes. A link with the weakly self-dual θ-cyclic codes is also established and some examples of self-dual extended θ-cyclic codes are given. The text is organized as follows.

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

In Section 2, a new sub-family of θ-cyclic codes over $\mathbb{F}_q$ is defined. This family generalizes the family of duadic codes with multipliers -1 and $-r$ (when $q = r^2$). These codes are called θ-duadic codes with multiplier -1 (Definition 3) and multiplier $-r$ (Definition 4, when $q = r^2$). A property on the minimum odd weight of some θ-duadic codes is given (Proposition 1).

Section 3 is the most technical part of the text and is inspired from [4]. The aim is to construct and to enumerate the θ-duadic codes of length $2k$ with multipliers -1 and $-p$ over $\mathbb{F}_{p^2}$ when θ is the Frobenius automorphism and k is an integer not divisible by p (Proposition 3 and Proposition 4).

In Section 4, a link is established between the θ-duadic codes (defined in Definition 3 and Definition 4) and the weakly self-dual θ-cyclic codes. In the particular case of $\mathbb{F}_{p^2}$, a complete description of the $[2k, k-1]_{p^2}$ weakly self-dual θ-cyclic codes is given. Furthermore, some constructions of self-dual extended θ-cyclic codes are provided.

Lastly, in Section 5, an application of the techniques developed in Section 3 is given (without link with coding theory). It consists in a parametrization of irreducible skew polynomials over $\mathbb{F}_{p^2}[X;\theta]$ with given degree and given bound.

2 A sub-family of θ-cyclic codes.

Consider q a prime power, θ an automorphism over $\mathbb{F}_q$ and the ring $R = \mathbb{F}_q[X;\theta]$ where addition is defined to be the usual addition of polynomials and where multiplication is defined by the rule : for a in $\mathbb{F}_q$

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

The ring R is called a skew polynomial ring or Ore ring (cf. [10]) and its elements are skew polynomials. When θ is not the identity, the ring R is not commutative, it is a left and right Euclidean ring whose left and right ideals are principal. Left and right gcd 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 θ and m is the order of θ. 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 $\mathbb{F}_q^{\theta}[X^m]$ of minimal degree such that h divides f on the right in R ([8]).

Definition 1 (definition 1 of [3]) *Consider two integers n, k such that $0 \leq k \leq n$. A* **θ-cyclic code** *or* **skew cyclic** *code C of length n and dimension k is a left R-submodule $Rg/R(X^n-1) \subset R/R(X^n-1)$ in the basis $1, X, \ldots, X^{n-1}$ where g is a monic skew polynomial dividing $X^n - 1$ on the right in R with degree $n-k$. The skew polynomial g is called* **skew generator polynomial** *of C.*

If θ is the identity then a θ-cyclic code is cyclic.

If the skew generator g of a θ-cyclic code is irreducible in R, then one calls the corresponding θ-cyclic code an **irreducible θ-cyclic code**. If g is reducible in R, the code is a **reducible θ-cyclic** code. An **even-like code** is a code who has only even-like codewords, that means codewords whose sum of coordinates cancel. It is **odd-like** otherwise.

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 the constant term of h does not cancel then the* **left monic skew reciprocal polynomial** *of h is $h^\natural := \frac{1}{\theta^d(h_0)} \cdot h^*$. The skew polynomial h is* **self-reciprocal** *if $h = h^\natural$.*

Definition 3 (θ-duadic codes given by the multiplier -1) *Consider a prime power q, θ an automorphism over $\mathbb{F}_q$ of order m, $R = \mathbb{F}_q[X;\theta]$ and an integer k coprime with q such that $mk - m$ is even. A θ-cyclic code of length $n = mk$ is an* **even-like (resp. odd-like) θ-duadic code given by the multiplier -1** *if it is generated by $(X^m - 1) \cdot h^\natural$ (resp. $h^\natural$) where h is a monic polynomial of R satisfying*

$$(X^m - 1) \cdot h^\natural \cdot h = X^n - 1. \tag{2}$$

One says that the skew polynomials $(X^m - 1) \cdot h^\natural$ and $h^\natural$ generate a **pair of θ-duadic codes of length mk given by the multiplier -1.**

Remark 1 *The above skew polynomial $h^\natural$ is not divisible by $X - 1$ because it is coprime with $X^m - 1$, which is the bound of $X - 1$, therefore the θ-cyclic code generated by $h^\natural$ is odd-like. Furthermore the codewords of the θ-cyclic code generated by $(X^m - 1) \cdot h^\natural$ are divisible by $X^m - 1$ therefore they are divisible by $X - 1$ and are even-like.*

Remark 2 *If $\theta = id$, then equation (2) becomes*

$$(X - 1)h^\natural h = X^n - 1.$$

This equation characterizes duadic codes given by the multiplier -1 (Theorem 6.1.5 of [7]). Namely consider an odd number n coprime with q and α a primitive n-th root of unity.

Consider an odd-like duadic code given by the multiplier -1. According to Theorem 6.1.5 of [7], it is generated by a polynomial $g = \prod_{i \in S}(X - \alpha^i)$ where S is a subset of $\{1, \ldots, n\}$ such that $S \cap -S = \emptyset$ and $S \cup -S = \{1, \ldots n\}$. Consider $h = \prod_{i \in -S}(X - \alpha^i)$, then $(X-1)gh = X^n - 1$ and $g = h^\natural$.

Conversely, consider the cyclic code C with generator $g = h^\natural$ where $h \in \mathbb{F}_q[X]$ is such that $(X-1)h^\natural h = X^n - 1$. Consider the subsets S and T of $\{1, \ldots, n-1\}$ of cardinality $(n-1)/2$ such that $g = \prod_{i \in S}(X - \alpha^i)$ and $h = \prod_{i \in T}(X - \alpha^i)$. As g and h belong to $\mathbb{F}_q[X]$, the sets S and T are unions of q-cyclotomic cosets modulo n. Furthermore g and h are coprime and their product is $(X^n - 1)/(X - 1)$, therefore $S \cap T = \emptyset$ and $S \cup T = \{1, \ldots n\}$. Lastly, as $h^\natural = g$, $T = -S$ (and $S = -T$). According to Theorem 6.1.5 of [7], C is an odd-like duadic code given by the multiplier -1.

If $q = r^2$ is an even power of an arbitrary prime number, one defines for a in $\mathbb{F}_q$, $\overline{a} = a^r$ and for $h = \sum h_i X^i$ in R, $\overline{h} = \sum \overline{h_i} X^i$.

Definition 4 (θ-duadic codes given by the multiplier $-r$) *Consider $q = r^2$ an even power of an arbitrary prime number, θ an automorphism over $\mathbb{F}_q$ of order m, $R = \mathbb{F}_q[X;\theta]$ and an integer k coprime with q such that $mk - m$ is even. A θ-cyclic code of length $n = mk$ is*

an even-like (resp. odd-like) θ**-duadic code given by the multiplier** $-r$ *if it is generated by* $(X^m-1)\cdot\overline{h^\natural}$ *(resp.* $\overline{h^\natural}$*) where* h *is a monic polynomial of* R *satisfying*

$$(X^m-1)\cdot\overline{h^\natural}\cdot h = X^n-1. \tag{3}$$

One says that the skew polynomials $(X^m-1)\cdot\overline{h^\natural}$ *and* $\overline{h^\natural}$ *generate a* **pair of** θ**-duadic codes of length** mk **given by the multiplier** $-r$.

Remark 3 *If* $\theta = id$*, then equation (3) characterizes duadic codes given by the multiplier* $-r$*. Namely consider an odd number* n *coprime with* q *and* α *a primitive* n*-th root of unity, consider the cyclic code* C *with generator* $g = \overline{h^\natural}$ *where* $h \in \mathbb{F}_q[X]$ *is such that* $(X-1)\overline{h^\natural}h = X^n-1$*. Consider the subset* S *of* $\{1,\ldots,n-1\}$ *of cardinality* $(n-1)/2$ *such that* $g = \prod_{i\in S}(X-\alpha^i)$ *and the subset* T *of* $\{1,\ldots,n-1\}$ *of cardinality* $(n-1)/2$ *such that* $h = \prod_{i\in T}(X-\alpha^i)$*. As* $g = \overline{h^\natural}$*, one gets* $S = -rT$*. Furthermore* $r^2 = q$*, so* $T = -rS$ *and* C *is a duadic code given by the multiplier* $-r$*.*

Example 1 *Consider* p *an odd prime number and* θ *an automorphism over* $\mathbb{F}_{p^2}$*. Let us determine the* θ*-duadic codes of length* 4 *given by the multipliers* -1 *and* $-p$ *over* $\mathbb{F}_{p^2}$*. If* θ *is the identity then* $m = 1$ *and there is no* θ*-duadic code of length* 4 *because* 4 *is even. Assume that* θ *is the Frobenius automorphism* $x \mapsto x^p$*; his order is* $m = 2$*.*

- *The* θ*-duadic codes of length* 4 *given by the multiplier* -1 *are defined by the skew equation*

  $$(X^2-1)\cdot h^\natural\cdot h = X^4-1 \Leftrightarrow h^\natural\cdot h = X^2+1.$$

  Consider $h = X+\alpha$ *in* R *with* $\alpha \neq 0$*, then* $h^\natural = X + \frac{1}{\theta(\alpha)}$ *therefore*

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

  and $h^\natural\cdot h = X^2+1 \Leftrightarrow \alpha^2+1 = \alpha^{p-1}-1 = 0$*.*

  Therefore there are 2 *pairs of* θ*-duadic codes of length* 4 *given by the multiplier* -1 *over* $\mathbb{F}_{p^2}$ *if* $p \equiv 1 \pmod 4$*. They are generated by* $X+\alpha$ *and* $(X^2-1)\cdot(X+\alpha)$ *where* $\alpha^2 = -1$*. If* $p \equiv 3 \pmod 4$*, there is no* θ*-duadic codes of length* 4 *given by the multiplier* -1 *over* $\mathbb{F}_{p^2}$*.*

- *The* θ*-duadic codes of length* 4 *given by the multiplier* -2 *are defined by the equation*

  $$(X^2-1)\cdot\overline{h^\natural}\cdot h = X^4-1 \Leftrightarrow \overline{h^\natural}\cdot h = X^2+1.$$

  Consider $h = X+\alpha$ *in* R *with* $\alpha \neq 0$*, then*

  $$\overline{h^\natural}\cdot h = (X+1/\alpha)\cdot(X+\alpha) = X^2 + (1/\alpha+\alpha^p)X + 1.$$

  Therefore $\overline{h^\natural}\cdot h = X^2+1 \Leftrightarrow \alpha^{p+1} = -1$ *and there are* $p+1$ *pairs of* θ*-duadic codes of length* 4 *given by the multiplier* -2 *over* $\mathbb{F}_{p^2}$*. They are generated by* $(X^2-1)\cdot(X+\frac{1}{\theta(\alpha)})$ *and* $X+\frac{1}{\theta(\alpha)}$ *where* $\alpha^{p+1} = -1$*.*

The following proposition gives a bound on the minimum odd weight of odd-like θ-duadic codes. It is inspired from Theorem 6.5.2 of [7].

Proposition 1 *Consider a prime power q, θ an automorphism over $\mathbb{F}_q$ of order m, $R = \mathbb{F}_q[X;\theta]$ and an integer k coprime with q such that $mk-m$ is even. Consider C an odd-like θ-duadic code with length mk over $\mathbb{F}_q$. For each odd-like word in C with weight d, $k \leq d^2$.*

Proof. Consider g the skew generator polynomial of an odd-like θ-duadic code C with length mk given by the multiplier -1, then $g = h^\natural$ and $(X^m-1)\cdot h^\natural \cdot h = X^{mk}-1$. Consider c an odd-like word in C, then X^m-1 does not divide $c(X)$ and $g = h^\natural$ divides $c(X)$. There exists $u(X)$ in $\mathbb{F}_q[X;\theta]$ such that $c(X) = u(X)\cdot h^*(X)$. Using the two properties $(f\cdot g)^* = \Theta^{\deg(f)}(g^*)\cdot f^*$ and $(f^*)^* = \Theta^{\deg(f)}(f)$, one gets $\Theta^{-\deg(c)}(c^*) = h\cdot\Theta^{-\deg(c)}(u^*)$ and $c\cdot\Theta^{-\deg(c)}(c^*)$ is a multiple of $\frac{X^{mk}-1}{X^m-1}$ not divisible by X^m-1. Consider $e = c\cdot\Theta^{-\deg(c)}(c^*) \bmod X^{mk}-1$ and E the θ-cyclic code of length mk and generator polynomial $\sum_{i=0}^{k-1} X^{mi}$. As the minimum distance of the code E is k and as e is a nonzero codeword of E with weight less than or equal to d^2, one gets $k \leq d^2$.

The same proof holds for odd-like θ-duadic code given by the multiplier $-r$ when $q = r^2$.

■

When q is the square of a prime number p and θ is the Frobenius automorphism, equation (2) is equivalent to

$$(X^2-1)\cdot h^\natural \cdot h = X^{2k}-1 \tag{4}$$

and equation (3) is equivalent to

$$(X^2-1)\cdot \Theta(h^\natural)\cdot h = X^{2k}-1 \tag{5}$$

where $\Theta : \sum a_i X^i \mapsto \sum \theta(a_i)X^i = \sum \overline{a_i}X^i = \overline{\sum a_i X^i}$.

Next section will be devoted to these two skew equations. Let us first introduce some notations.

For $F(X^2) \in \mathbb{F}_p[X^2]$ and b in $\{0,1\}$,

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

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

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

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

Note that the θ-duadic codes of length $2k$ given by the multiplier -1 are associated to the set $\mathcal{H}^{(0)}_{(X^{2k}-1)/(X^2-1)}$ while the θ-duadic codes given by the multiplier $-p$ are associated to the set $\mathcal{H}^{(1)}_{(X^{2k}-1)/(X^2-1)}$.

3 Construction and enumeration of θ-duadic codes over $\mathbb{F}_{p^2}$ given by the multipliers -1 and $-p$

The aim of this section is to construct and count pairs of θ-duadic codes defined over $\mathbb{F}_{p^2}$ and given by the multipliers -1 and $-p$. It amounts to construct the set $\mathcal{H}^{(b)}_{F(X^2)}$ where b

belongs to $\{0,1\}$ and $F(X^2)$ is the polynomial $\frac{X^{2k}-1}{X^2-1}$. Most of the work consists of using the techniques developped in [4] for the Euclidean scalar product and adapting them to Hermitian scalar product. Furthermore an application to the parametrization of the irreducible skew polynomials with given bound will be developped in Section 6.

The following proposition is inspired from Proposition 28 of [3] and Proposition 2 of [4].

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

$$\phi : \left\{ \begin{array}{rcl} \mathcal{H}^{(b)}_{f_1(X^2)} \times \cdots \times \mathcal{H}^{(b)}_{f_r(X^2)} & \to & \mathcal{H}^{(b)}_{F(X^2)} \\ (h_1,\ldots,h_r) & \mapsto & \mathrm{lcrm}(h_1,\ldots,h_r) \end{array} \right.$$

is bijective.

Proof.

- The application ϕ is well-defined.

  Consider $(h_1,\ldots,h_r)$ in $\mathcal{H}^{(b)}_{f_1(X^2)} \times \cdots \times \mathcal{H}^{(b)}_{f_r(X^2)}$ and $h = \mathrm{lcrm}(h_1,\ldots,h_r)$.

  Firstofall as $h_1,\ldots h_r$ divide respectively $f_1(X^2),\ldots,f_r(X^2)$, and as $f_1(X^2),\ldots,f_r(X^2)$ are pairwise coprime central polynomials, the degree of $\mathrm{lcrm}(h_1,\ldots,h_r)$ is equal to $\sum_{i=1}^r \deg(h_i)$. Furthermore, as $\Theta^b(h_i^\natural)\cdot h_i = f_i(X^2)$, the degree of h_i is equal to the degree of $f_i(X^2)$ in X^2, therefore the degree of h is equal to the degree of $F(X^2)$ in X^2.

  Consider for i in $\{1,\ldots r\}$, Q_i in R such that $h = h_i \cdot Q_i$, then $\Theta^b(h^\natural) = \tilde{Q}_i \cdot \Theta^b(h_i^\natural)$ where $\tilde{Q}_i \in R$ therefore $\Theta^b(h^\natural)\cdot h = \tilde{Q}_i \cdot \Theta^b(h_i^\natural)\cdot h_i \cdot Q_i = \tilde{Q}_i \cdot f_i(X^2)\cdot Q_i$. As $f_i(X^2)$ is central, it divides $\Theta^b(h^\natural)\cdot h$. The polynomials $f_i(X^2)$ are pairwise coprime in $\mathbb{F}_p[X^2]$, therefore their least common right multiple is equal to their product $F(X^2)$, and $F(X^2)$ divides $\Theta^b(h^\natural)\cdot h$. Considerations on the degrees of the involved polynomials imply the equality $\Theta^b(h^\natural)\cdot h = F(X^2)$.

  The skew polynomial h belongs to $\mathcal{H}^{(b)}_{F(X^2)}$ therefore ϕ is well defined.

- The application ϕ is bijective.

  Consider h in $\mathcal{H}^{(b)}_{F(X^2)}$, then h divides $F(X^2)$, therefore, according to Theorem 4.1 of [6], $h = \mathrm{lcrm}(h_1,\ldots,h_r)$ where $h_i = \mathrm{gcld}(f_i(X^2), h)$ and this lcrm-decomposition into skew polynomials dividing $f_1(X^2),\ldots f_r(X^2)$ is unique. Let us prove that h_i belongs to $\mathcal{H}^{(b)}_{f_i(X^2)}$.

  As h_i divides $f_i(X^2)$ on the left, $\Theta^b(h_i^\natural)$ divides $\Theta^b(f_i^\natural)(X^2)$ on the right. As $f_i(X^2)$ is central, one gets that $\Theta^b(h_i^\natural)\cdot h_i$ divides $f_i(X^2)^2$. In particular,

  $$\forall j \in \{1,\ldots,r\}\setminus\{i\}, \mathrm{gcrd}(\Theta^b(h_i^\natural)\cdot h_i, f_j(X^2)) = 1 \tag{6}$$

  As h_i divides h on the left, $\Theta^b(h_i^\natural)$ divides $\Theta^b(h^\natural)$ on the right. Furthermore $F(X^2) = \Theta^b(h^\natural)\cdot h$ is central, therefore $\Theta^b(h_i^\natural)\cdot h_i$ divides $F(X^2) = f_1(X^2)\cdots f_i(X^2)\cdots f_r(X^2)$.

According to (6), $\Theta^b(h_i^\natural) \cdot h_i$ divides $f_i(X^2)$. Furthermore, $2\deg(h) = \sum_{i=1}^r 2\deg(h_i) = \sum_{i=1}^r \deg(f_i(X^2))$, therefore $\forall i \in \{1,\dots,r\}, \deg(f_i(X^2)) = 2\deg(h_i)$ and $\Theta^b(h_i^\natural) \cdot h_i = f_i(X^2)$.

■

3.1 Irreducible case

The aim of this subsection is to construct and enumerate irreducible odd-like θ-duadic codes defined over $\mathbb{F}_{p^2}$ of length $2k$ where k is coprime with p. One therefore assumes that $X^{2k}-1 = (X^2-1)f(X^2)$ where $f(X^2)$ is irreducible in $\mathbb{F}_p[X^2]$. Necessarily $f(X^2)$ is self-reciprocal.

If $f(X^2)$ has degree 1 then $f(X^2) = X^2+1$, $k=2$ and p is odd. According to Example 1, there are 2 irreducible odd-like θ-duadic codes of length 4 given by the multiplier -1 if $p \equiv 1 \pmod 4$. If $p \equiv 3 \pmod 4$, such codes do not exist. Furthermore, for any prime number p, there are $p+1$ irreducible odd-like θ-duadic codes of length 4 given by the multiplier $-p$.

In what follows, one constructs the set $\mathcal{H}^{(b)}_{f(X^2)}$ when b belongs to $\{0,1\}$ and $f = f(X^2)$ belongs to $\mathcal{F}$. When $b=0$, Lemma 5 of [4] gives a construction based on Cauchy interpolation in $\mathbb{F}_{p^2}(Z)$. We give here a slightly different presentation and a generalization to the case when b is equal to 1.

Lemma 1 *Consider f in $\mathcal{F}$ with degree $d = 2\delta$ where δ is in $\mathbb{N}^*$. The skew polynomial $h(X) = \Theta^b(A)(X^2) + X \cdot \Theta^b(B)(X^2)$ belongs to $\mathcal{H}^{(b)}_{f(X^2)} \setminus \mathbb{F}_{p^2}[X^2]$ if and only if the polynomial $P(Z)$ of degree $< d$ defined in $\mathbb{F}_{p^2}[Z]$ by*

$$\frac{A}{B} \equiv P \pmod f$$

satisfies the two following equations in $\mathbb{F}_{p^2}[Z]$:

$$\begin{cases} P(Z)\Theta(P)(Z) \equiv Z \pmod{f(Z)} \\ Z^{2\delta-1}P(1/Z) + Z^{2\delta-2}\Theta^{b+1}(P)(Z) \equiv 0 \pmod{f(Z)}. \end{cases} \tag{7}$$

Proof. Consider $h = \sum_{i=0}^d h_i X^i$ in R, monic with degree d. Consider A and B defined by $h(X) = \Theta^b(A)(X^2) + X \cdot \Theta^b(B)(X^2)$, then $h^\natural = \tilde{A}(X^2) + \tilde{B}(X^2) \cdot X$ where $\tilde{A}(Z) = \lambda Z^\delta \Theta^b(A)(1/Z)$ and $\tilde{B}(Z) = \lambda Z^{\delta-1}\Theta^b(B)(1/Z)$, $\lambda = \theta^b(1/h_0)$.

Therefore h belongs to $\mathcal{H}^{(b)}_{f(X^2)}$ if and only if the following polynomial relations in $\mathbb{F}_{p^2}[Z]$ are satisfied :

$$\begin{cases} \tilde{A}(Z)A(Z) + Z\tilde{B}(Z)B(Z) = f(Z) \\ \tilde{A}(Z)\Theta(B)(Z) + \tilde{B}(Z)\Theta(A)(Z) = 0. \end{cases} \tag{8}$$

As $B \neq 0$, and as $\deg(B) < \deg(f)/2$, B and f are coprime, therefore A and B are coprime. The relation (8) is equivalent to

$$\begin{cases} A(Z)\Theta(A)(Z) - ZB(Z)\Theta(B)(Z) = f(Z) \\ Z^\delta A(1/Z)\Theta^{b+1}(B)(Z) + Z^{\delta-1}B(1/Z)\Theta^{b+1}(A)(Z) = 0. \end{cases} \tag{9}$$

Consider P in $\mathbb{F}_{p^2}[Z]$ with degree less than d such that

$$\frac{A(Z)}{B(Z)} \equiv P(Z) \pmod{f(Z)}.$$

This polynomial exists because B and f are coprime. Furthermore the relation (9) is equivalent to (7).

■

The following lemma will be also useful in subsection 3.2 and in section 5.

Lemma 2 *Consider f in $\mathbb{F}_p[Z]$ irreducible in $\mathbb{F}_p[Z]$ with degree d and α in $\mathbb{F}_{p^d}$ such that $f(\alpha)=0$. Consider $P(Z)$ in $\overline{\mathbb{F}_{p^2}}[Z]$ with degree $< d$ and $y_i = P(\alpha^{p^i})$ for $0 \le i \le d-1$.*

$$\left\{ \begin{array}{l} P(Z)\Theta(P)(Z) \equiv Z \pmod{f(Z)} \\ P(Z) \in \mathbb{F}_{p^2}[Z] \end{array} \right.$$

$$\Updownarrow$$

$$\left\{ \begin{array}{ll} y_i = y_0^{p^i} & \textit{if } i \in \{0,\dots,d-1\} \textit{ is even} \\ y_i = \alpha^{p^i}/y_0^{p^i} & \textit{if } i \in \{0,\dots,d-1\} \textit{ is odd} \\ y_0^{p^d-1} = 1 & \textit{if } d \textit{ is even} \\ y_0^{p^d+1} = \alpha & \textit{if } d \textit{ is odd.} \end{array} \right. \tag{10}$$

Proof. Consider $P(Z)$ in $\overline{\mathbb{F}_{p^2}}[Z]$ with degree $< d$ and $y_i = P(\alpha^{p^i})$ for $0 \le i \le d-1$.

- Assume that $P(Z)$ is a polynomial of $\mathbb{F}_{p^2}[Z]$ such that $P(Z)\Theta(P)(Z) \equiv Z \pmod{f(Z)}$. As $P(Z)$ belongs to $\mathbb{F}_{p^2}[Z]$, $\Theta^2(P)(Z) - P(Z)$ cancels at the points $\theta^i(\alpha)$ where $i \in \{0,\dots,d-1\}$ therefore $\left\{ \begin{array}{ll} P(\alpha^{p^i}) = P(\alpha)^{p^i} & \text{if } i \in \{0,\dots,d-1\} \text{ is even} \\ P(\alpha^{p^i}) = P(\alpha^p)^{p^{i-1}} & \text{if } i \in \{0,\dots,d-1\} \text{ is odd.} \end{array} \right.$

  Furthermore $\alpha^{p^d} = \alpha$ therefore $\left\{ \begin{array}{ll} P(\alpha)^{p^d-1} = 1 & \text{if } d \text{ is even} \\ P(\alpha^p)^{p^{d-1}} = P(\alpha) & \text{if } d \text{ is odd.} \end{array} \right.$

  The condition $y_1 = \alpha^p/y_0^p$ comes from the evaluation of $P(Z)\Theta(P)(Z) - Z$ at α and (10) follows from these relations.

- Conversely, assume that (10) is satisfied. Then

$$\left\{ \begin{array}{ll} P(\alpha^{p^i}) = P(\alpha)^{p^i} & \text{if } i \in \{0,\dots,d-1\} \text{ is even} \\ P(\alpha^{p^i}) = P(\alpha^p)^{p^{i-1}} & \text{if } i \in \{0,\dots,d-1\} \text{ is odd} \\ P(\alpha)^{p^d} = P(\alpha) & \text{if } d \text{ is even} \\ P(\alpha^p)^{p^{d-1}} = P(\alpha) & \text{if } d \text{ is odd} \\ P(\alpha^p)P(\alpha)^p = \alpha^p. & \end{array} \right.$$

  Let us prove first that $\Theta^2(P)(Z) - P(Z) = 0$. As $\deg(P) < d$, $\Theta^2(P)(Z) - P(Z)$ cancels at $\theta^i(\alpha)$ for i in $\{0,\dots,d-1\}$. Consider $i \in \{2,\dots,d-1\}$ then $(\Theta^2(P) - P)(\theta^i(\alpha)) = \theta^2(y_{i-2}) - y_i = 0$, furthermore

$$(\Theta^2(P)-P)(\alpha) = \Theta^2(P)(\alpha^{p^d}) - P(\alpha) = \theta^2(y_{d-2}) - y_0 = \left\{ \begin{array}{rll} y_0^{p^d} - y_0 & = 0 & \text{if } d \text{ is even} \\ \alpha^{p^d}/y_0^{p^d} - y_0 & = 0 & \text{if } d \text{ is odd} \end{array} \right.$$

$$(\Theta^2(P)-P)(\theta(\alpha)) = \theta^2(y_{d-1}) - y_1 = \begin{cases} \alpha^{p^{d+1}}/y_0^{p^{d+1}} - \alpha^p/y_0^p = 0 & \text{if } d \text{ is even} \\ y_0^{p^{d+1}} - \alpha^p/y_0^p = 0 & \text{if } d \text{ is odd.} \end{cases}$$

Therefore $\Theta^2(P)(Z) = P(Z)$ and $P(Z)\Theta(P)(Z) - Z$ is in $\mathbb{F}_p[Z]$.

The condition $P(\alpha^p)P(\alpha)^p = \alpha^p$ implies that $P(Z)\Theta(P)(Z) - Z$ cancels at α and is therefore divisible by $f(Z)$.

■

The following lemma describes the set $\mathcal{H}^{(b)}_{f(X^2)}$ where $f(X^2) \in \mathcal{F}$ is an irreducible self-reciprocal polynomial of $\mathbb{F}_p[X^2]$ with degree > 1 and b belongs to $\{0,1\}$. It is a generalization of Lemma 5 of [4] (where $\mathcal{H}^{(0)}_{f(X^2)}$ is constructed).

Lemma 3 *Consider b in $\{0,1\}$, $f = f(X^2)$ in $\mathcal{F}$ of degree $d = 2\delta$ where δ is in $\mathbb{N}^*$. The set $\mathcal{H}^{(b)}_{f(X^2)}$ has $1 + p^\delta$ elements.*

Proof. Consider $f(X^2) = \tilde{f}(X^2)\Theta(\tilde{f})(X^2)$ the factorization of $f(X^2)$ in $\mathbb{F}_{p^2}[X^2]$.
Then

$$\mathcal{H}^{(b)}_{f(X^2)} \cap \mathbb{F}_{p^2}[X^2] = \begin{cases} \emptyset & \text{if } \delta + b \equiv 0 \pmod 2 \\ \{\tilde{f}(X^2), \Theta(\tilde{f})(X^2)\} & \text{if } \delta + b \equiv 1 \pmod 2 \end{cases} \tag{11}$$

According to Lemma 1, $h(X) = \Theta^b(A)(X^2) + X \cdot \Theta^b(B)(X^2)$ belongs to $\mathcal{H}^{(b)}_{f(X^2)} \setminus \mathbb{F}_{p^2}[X^2]$ if and only if (A,B) is the unique solution to the Cauchy interpolation problem :

$$\frac{A}{B} \equiv P \pmod f$$

where the polynomial $P(Z)$ in $\mathbb{F}_{p^2}[Z]$ of degree $< d$ is defined by the relations (7) :

$$\begin{cases} P(Z)\Theta(P)(Z) \equiv Z \pmod{f(Z)} \\ Z^{2\delta-1}P(1/Z) + Z^{2\delta-2}\Theta^{b+1}(P)(Z) \equiv 0 \pmod{f(Z)}. \end{cases}$$

As there is a unique solution (A,B) (with $\deg(A) = \delta$, $\deg(B) \le \delta - 1$ and A monic) to the above Cauchy interpolation problem for each P, the number of elements of $\mathcal{H}^{(b)}_{f(X^2)} \setminus \mathbb{F}_{p^2}[X^2]$ is equal to the number of P in $\mathbb{F}_{p^2}[Z]$ with degree $< d$ satisfying (7). For $0 \le i \le d-1$, denote $y_i = P(\alpha^{p^i}) \in \mathbb{F}_{p^d}$. Let us prove that (7) is equivalent to

$$\begin{cases} y_i = y_0^{p^i} & \text{if } i \in \{0,\dots,d-1\} \text{ is even} \\ y_i = \alpha^{p^i}/y_0^{p^i} & \text{if } i \in \{0,\dots,d-1\} \text{ is odd} \end{cases} \tag{12}$$

and

$$\begin{cases} y_0^{p^\delta - 1} = -1/\alpha & \text{if } \delta + b \equiv 1 \pmod 2 \\ y_0^{p^\delta + 1} = -1 & \text{if } \delta + b \equiv 0 \pmod 2. \end{cases} \tag{13}$$

Assume that (7) is satisfied. Then according to Lemma 2, (12) is satisfied. Furthermore, as $Z^{2\delta-1}P(1/Z) + Z^{2\delta-2}\Theta^{b+1}(P)(Z)$ cancels at α, (13) is also satisfied. Conversely, assume (12) and (13), then according to Lemma 2, $P(Z)\Theta(P)(Z) \equiv Z \pmod{f(Z)}$. Furthermore $Z^{2\delta-1}P(1/Z) + Z^{2\delta-2}\Theta^{b+1}(P)(Z)$ cancels at α and α^p, therefore $Z^{2\delta-1}P(1/Z) +$

$Z^{2\delta-2}\Theta^{b+1}(P)(Z) \equiv 0 \pmod{f(Z)}$. To conclude the proof, according to (13), the set $\mathcal{H}^{(b)}_{f(X^2)} \setminus \mathbb{F}_{p^2}[X^2]$ has $p^\delta - 1$ elements if $\delta + b \equiv 1 \pmod 2$ and $p^\delta + 1$ elements if $\delta + b \equiv 0 \pmod 2$. The relation (11) enables to conclude.

■

Proposition 3 *Consider p a prime number, θ the Frobenius automorphism over $\mathbb{F}_{p^2}$, b in $\{0,1\}$ and k an integer coprime with p. The number of irreducible θ-duadic codes of length $2k$ with given multiplier $-p^b$ over $\mathbb{F}_{p^2}$ is*

$$\begin{cases} 1 + p^{(k-1)/2} & \text{if } k \text{ is an odd prime and } p \text{ generates } \mathbb{Z}/k\mathbb{Z}^*; \\ 0 & \text{ortherwise.} \end{cases}$$

Proof. Let us prove that there exists an irreducible θ-duadic codes of length $2k$ with given multiplier $-p^b$ over $\mathbb{F}_{p^2}$ if and only if k is an odd prime and p generates $\mathbb{Z}/k\mathbb{Z}^*$.

Assume that there exists an irreducible θ-duadic code of length $2k$ with given multiplier $-p^b$ over $\mathbb{F}_{p^2}$. Consider g its skew generator polynomial, necessarily g is irreducible therefore $g = h^\natural$ where $\Theta^b(h^\natural) \cdot h = \frac{X^{2k}-1}{X^2-1}$. The bound $B(g)$ of g is an irreducible polynomial of $\mathbb{F}_p[X^2]$ with degree $2\deg(g) = 2k$. Therefore $\frac{X^{2k}-1}{X^2-1} = B(g)$ and $\frac{X^{2k}-1}{X^2-1}$ is irreducible in $\mathbb{F}_p[X^2]$. Necessarily, k is and odd prime and p generates $\mathbb{Z}/k\mathbb{Z}^*$.

Assume that k is and odd prime and p generates $\mathbb{Z}/k\mathbb{Z}^*$, then $F(X^2) := \frac{X^{2k}-1}{X^2-1}$ is irreducible in $\mathbb{F}_p[X^2]$, therefore according to Lemma 3, $\mathcal{H}^{(b)}_{F(X^2)}$ is nonempty. Its elements have degree k and divides $F(X^2)$. As $F(X^2)$ is an irreducible polynomial of $\mathbb{F}_p[X^2]$ of degree $2k$. the elements of $\mathcal{H}^{(b)}_{F(X^2)}$ are irreducible skew polynomials. To conclude, there exists an irreducible θ-duadic code of length $2k$ with given multiplier $-p^b$ over $\mathbb{F}_{p^2}$.

Lastly, the set $\mathcal{H}^{(b)}_{F(X^2)}$ has $1 + p^{(k-1)/2}$ elements according to Lemma 3.

■

Example 2 *Consider $\theta : x \mapsto x^2$ the Frobenius automorphism over $\mathbb{F}_4 = \mathbb{F}_2(a)$. The number of irreducible θ-duadic codes of length 22 with given multiplier -1 over $\mathbb{F}_4$ is $1+2^5 = 33$. They are generated by the skew polynomials $h^\natural$ in $\mathbb{F}_4[X;\theta]$ where h is a monic solution to the kew eqquation*

$$h^\natural \cdot h = \frac{X^{22}-1}{X^2-1} = X^{20} + X^{18} + \cdots + X^2 + 1.$$

For example $h = X^{10} + X^9 + aX^6 + a^2X^4 + X + 1$ is a solution and $g = h^\natural = X^{10} + X^9 + a^2\,X^6 + a\,X^4 + X + 1$ generates a $[22, 12, 6]_4$ irreducible odd-like θ-duadic codes with multiplier -1.

Example 3 *Consider $\theta : x \mapsto x^2$ the Frobenius automorphism over $\mathbb{F}_4$. The number of irreducible θ-duadic codes of length 22 with given multiplier -2 over $\mathbb{F}_4$ is $1 + 2^5 = 33$. They are generated by the skew polynomials $\Theta(h^\natural)$ in $\mathbb{F}_4[X;\theta]$ where h is a monic solution to the equation*

$$\Theta(h^\natural) \cdot h = \frac{X^{22}-1}{X^2-1} = X^{20} + X^{18} + \cdots + X^2 + 1.$$

One of these solutions is $h = X^{10} + X^9 + a^2X^6 + X^5 + a^2X^4 + X + 1$ and $g = \Theta(h^\natural) = X^{10} + X^9 + a\,X^6 + X^5 + a\,X^4 + X + 1$ generates a $[22, 12, 6]_4$ irreducible odd-like θ-duadic codes with multiplier -2

3.2 Reducible case

The aim of this section is to construct and to enumerate reducible odd-like θ-duadic codes over $\mathbb{F}_{p^2}$ of length $2k$ where k is coprime with p (Proposition 4). One therefore assumes that $F(X^2) := \frac{X^{2k}-1}{X^2-1}$ is reducible in $\mathbb{F}_p[X^2]$.

If $F(X^2)$ is the product of self-reciprocal polynomials $f(X^2)$ irreducible in $\mathbb{F}_p[X^2]$, then one can conclude thanks to Proposition 2 and Lemma 3.

Otherwise, as $F(X^2)$ is self-reciprocal, its irreducible factors in $\mathbb{F}_p[X^2]$ which are not self-reciprocal appear by pairs $(g(X^2), g^\natural(X^2))$.

In what follows we construct $\mathcal{H}^{(b)}_{f(X^2)}$ when $f(X^2) \in \mathcal{G}$ is the product of two irreducible polynomials of $\mathbb{F}_p[X^2]$ which are a pair of reciprocal polynomials $g(X^2)$ and $g^\natural(X^2)$. The following Lemma is a generalization of Lemma 6 of [4] (where $\mathcal{H}^{(1)}_{f(X^2)}$ is constructed).

Lemma 4 *Consider b in $\{0,1\}$, $f = f(X^2)$ in $\mathcal{G}$ with degree 2δ in X^2 and $g(X^2)$ such that $f(X^2) = g(X^2)g^\natural(X^2)$. The set $\mathcal{H}^{(b)}_{f(X^2)}$ has $3 + p^\delta$ elements.*

Proof.

When δ is even, consider the factorization of $g(X^2)$ in $\mathbb{F}_{p^2}[X^2]$: $g(X^2) = \tilde{g}(X^2) \times \Theta(\tilde{g})(X^2)$. Then $\mathcal{H}^{(b)}_{f(X^2)} \cap \mathbb{F}_{p^2}[X^2] = \{g(X^2), g^\natural(X^2), \tilde{g}(X^2)\Theta^{1+b}\left(\tilde{g}^\natural(X^2)\right), \Theta^b(\tilde{g})^\natural(X^2)\Theta(\tilde{g})(X^2)\}$. If δ is odd, then $g(X^2)$ is irreducible in $\mathbb{F}_{p^2}[X^2]$ and $\mathcal{H}^{(b)}_{f(X^2)} \cap \mathbb{F}_{p^2}[X^2] = \{g(X^2), g^\natural(X^2)\}$. In what follows, one proves that the number of elements of $\mathcal{H}^{(b)}_{f(X^2)} \setminus \mathbb{F}_{p^2}[X^2]$ is $p^\delta - 1$ if δ is even and $p^\delta + 1$ if δ is odd.

Consider β in $\mathbb{F}_{p^\delta}$ such that $g(\beta) = 0$. Consider $h = \sum_{i=0}^{d} h_i X^i$ in R, monic with degree d. Consider A and B defined by $h(X) = \Theta^b(A)(X^2) + X \cdot \Theta^b(B)(X^2)$, then $h^\natural = \tilde{A}(X^2) + \tilde{B}(X^2) \cdot X$ where $\tilde{A}(Z) = \lambda Z^\delta \Theta^b(A)(1/Z)$ and $\tilde{B}(Z) = \lambda Z^{\delta-1}\Theta^b(B)(1/Z)$, $\lambda = \theta^b(1/h_0)$.

Therefore h belongs to $\mathcal{H}^{(b)}_{f(X^2)} \setminus \mathbb{F}_{p^2}[X^2]$ if and only if the following polynomial relations in $\mathbb{F}_{p^2}[Z]$ are satisfied :

$$\begin{cases} \tilde{A}(Z)A(Z) + Z\tilde{B}(Z)B(Z) = f(Z) \\ \tilde{A}(Z)\Theta(B)(Z) + \tilde{B}(Z)\Theta(A)(Z) = 0. \end{cases} \tag{14}$$

Necessarily, as $B \neq 0$, B and f are coprime therefore A, B and f are pairwise coprime. Consider $P = P(Z)$ in $\mathbb{F}_{p^2}[Z]$ with degree less than d such that

$$\frac{A(Z)}{B(Z)} \equiv P(Z) \pmod{f(Z)}.$$

The polynomial P exists because B and f are coprime. The relation (14) is equivalent to

$$\begin{cases} P(Z)\Theta(P)(Z) \equiv Z \pmod{f(Z)} \\ Z^{2\delta-1}P(1/Z) + Z^{2\delta-2}\Theta^{b+1}(P)(Z) \equiv 0 \pmod{f(Z)}. \end{cases} \tag{15}$$

Consider $y_i = P(\beta^{p^i})$ if $0 \leq i \leq \delta - 1$ and $y_{i+\delta} = P(1/\beta^{p^i})$ if $0 \leq i \leq \delta - 1$.

Let us prove that (15) is equivalent to conditions (16), (17) and (18) defined below :

$$\begin{cases} y_i = y_0^{p^i} & \text{if } i \in \{0,\ldots,\delta-1\} \text{ is even} \\ y_i = \beta^{p^i}/y_0^{p^i} & \text{if } i \in \{0,\ldots,\delta-1\} \text{ is odd} \\ y_0^{p^\delta-1} = 1 & \text{if } \delta \text{ is even} \\ y_0^{p^\delta+1} = \beta & \text{if } \delta \text{ is odd} \end{cases} \tag{16}$$

$$\begin{cases} y_\delta = -1/y_0 & \text{if} \quad b=0 \\ y_\delta = -y_0/\beta & \text{if} \quad b=1 \end{cases} \tag{17}$$

$$\begin{cases} y_{i+\delta} = y_\delta^{p^i} & \text{if } i \in \{0,\ldots,\delta-1\} \text{ is even} \\ y_{i+\delta} = 1/(\beta^{p^i} y_\delta^{p^i}) & \text{if } i \in \{0,\ldots,\delta-1\} \text{ is odd.} \end{cases} \tag{18}$$

Assume that (15) is satisfied. As $P(Z)\Theta(P)(Z) \equiv Z \pmod{f(Z)}$, $P(Z)\Theta(P)(Z) \equiv Z \pmod{g(Z)}$ therefore according to Lemma 2 applied to g, (16) is satisfied. The condition $Z^{2\delta-1}P(1/Z) + Z^{2\delta-2}\Theta^{b+1}(P)(Z) \equiv 0 \pmod{f(Z)}$ implies furthermore (17). Lastly $P(Z)\Theta(P)(Z) \equiv Z \pmod{g^\natural(Z)}$ therefore according to Lemma 2 applied to $g^\natural$, (18) is satisfied.

Conversely, assume that (16), (17) and (18) are satisfied, then according to Lemma 2, $P(Z)\Theta(P)(Z) \equiv Z \pmod{g(Z)}$ and $P(Z)\Theta(P)(Z) \equiv Z \pmod{g^\natural(Z)}$. To prove that $Z^{2\delta-1}P(1/Z) + Z^{2\delta-2}\Theta^{b+1}(P)(Z) \equiv 0 \pmod{f(Z)}$, it suffices to prove that $uP(1/u) + \Theta^{b+1}(P)(u)$ cancels when u belongs to $\{\beta, \beta^p, 1/\beta, 1/\beta^p\}$:

$$\begin{aligned} &\beta P(\tfrac{1}{\beta}) + \Theta^{b+1}(P)(\beta) = \begin{cases} -\beta/y_0 + \beta/y_0 & = 0 \quad \text{if } b=0 \\ -y_0 + y_0 & = 0 \quad \text{if } b=1 \end{cases} \\ &\beta^p P(\tfrac{1}{\beta^p}) + \Theta^{b+1}(P)(\beta^p) = \begin{cases} -y_0^p + y_0^p & = 0 \quad \text{if } b=0 \\ -\beta^p/y_0^p + \beta^p/y_0^p & = 0 \quad \text{if } b=1 \end{cases} \\ &1/\beta \times P(\beta) + \Theta^{b+1}(P)(1/\beta) = y_0/\beta - y_0/\beta = 0 \\ &1/\beta^p \times P(\beta^p) + \Theta^{b+1}(P)(1/\beta^p) = 1/y_0^p - 1/y_0^p = 0. \end{aligned}$$

To conclude, according to the two last relations of (16), the number of elements of $\mathcal{H}^{(b)}_{f(X^2)} \setminus \mathbb{F}_{p^2}[X^2]$ is $p^\delta - 1$ if δ is even and $p^\delta + 1$ if δ is odd.

■

Proposition 4 *Consider p a prime number, θ the Frobenius automorphism over $\mathbb{F}_{p^2}$, k an integer coprime with p and b in $\{0,1\}$. The number of pairs of θ-duadic codes of length $2k$ with given multiplier $-p^b$ over $\mathbb{F}_{p^2}$ is*

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

where

$$N_b = \begin{cases} 0 & \text{if} \quad b=0, k \equiv 0 \pmod 2, p \equiv 3 \pmod 4 \\ 2 & \text{if} \quad b=0, k \equiv 0 \pmod 2, p \equiv 1 \pmod 4 \\ p+1 & \text{if} \quad b=1, k \equiv 0 \pmod 2 \\ 1 & \text{if} \quad k \equiv 1 \pmod 2. \end{cases}$$

Proof. The number of pairs of θ-duadic codes defined over $\mathbb{F}_{p^2}$ of length $2k$ with given multipliers $-p^b$ is equal to the cardinal of $\mathcal{H}^{(b)}_{F(X^2)}$ where $F(X^2) := \frac{X^{2k}-1}{X^2-1}$. If k is odd,

$$F(X^2) = \prod_{f\in\mathcal{F}\cap\mathcal{D}_F} f \prod_{f\in\mathcal{G}\cap\mathcal{D}_F} f$$

and if k is even then p is odd and

$$F(X^2) = (X^2+1) \prod_{f \in \mathcal{F} \cap \mathcal{D}_F} f \prod_{f \in \mathcal{G} \cap \mathcal{D}_F} f.$$

According to Proposition 2, $\#\mathcal{H}^{(b)}_{F(X^2)} = N_b \times \prod_{f \in \mathcal{F} \cap \mathcal{D}_F} \#\mathcal{H}^{(b)}_{f(X^2)} \times \prod_{f \in \mathcal{G} \cap \mathcal{D}_F} \#\mathcal{H}^{(b)}_{f(X^2)}$ where $N_b = 1$ if k is odd and $N_b = \#\mathcal{H}^{(b)}_{X^2+1}$ if k is even. The conclusion follows from Lemma 3, Lemma 4 and from the equality :

$$\#\mathcal{H}^{(b)}_{X^2+1} = \begin{cases} \{X+\alpha \mid \alpha^2 = -1\} & \text{if} \quad b = 0 \text{ and } p \equiv 1 \pmod 4 \\ \{X+\alpha \mid \alpha^{p+1} = -1\} & \text{if} \quad b = 1 \\ \emptyset & \text{if} \quad b = 0 \text{ and } p \equiv 3 \pmod 4. \end{cases}$$

■

Example 4 *Consider θ the Frobenius automorphism over $\mathbb{F}_4$. The odd-like θ-duadic codes of length 34 over $\mathbb{F}_4$ given by the multiplier -1 are characterized by the skew equation in $\mathbb{F}_4[X;\theta]$:*

$$h^\natural \cdot h = \frac{X^{34}-1}{X^2-1} = (X^{16}+X^{10}+X^8+X^6+1)(X^{16}+X^{14}+X^{12}+X^8+X^4+X^2+1).$$

Consider the skew polynomials $h_1 = X^8 + a^2\ X^7 + a^2\ X^6 + a\ X^4 + X^2 + a^2\ X + a^2$ and $h_2 = X^8 + a^2\ X^6 + a\ X^5 + a\ X^3 + a^2\ X^2 + a$. They satisfy $h_1^\natural \cdot h_1 = X^{16}+X^{10}+X^8+X^6+1$ and $h_2^\natural \cdot h_2 = X^{16}+X^{14}+X^{12}+X^8+X^4+X^2+1$. Therefore the skew polynomial $h = \mathrm{lcrm}(h_1, h_2) = X^{16} + a\ X^{15} + X^{14} + X^{13} + a^2\ X^{12} + X^{11} + a\ X^9 + X^7 + a\ X^5 + X^4 + a\ X^3 + a^2\ X^2 + X + a^2$ satisfies $h^\natural \cdot h = \frac{X^{34}-1}{X^2-1}$. The skew polynomial

$$g = h^\natural = X^{16} + aX^{15} + X^{14} + X^{13} + aX^{12} + X^{11} + aX^9 + X^7 + aX^5 + X^4 + aX^3 + aX^2 + X + a$$

generates an odd-like θ-duadic code C over $\mathbb{F}_4$ given by the multiplier -1, which is a $[34, 18, 9]_4$ code.

Example 5 *Consider θ the Frobenius automorphism over $\mathbb{F}_9$. There is no odd-like θ-duadic code of length 32 over $\mathbb{F}_9$ given by the multiplier -1.*

Example 6 *Consider θ the Frobenius automorphism over $\mathbb{F}_9$. The odd-like θ-duadic codes of length 32 over $\mathbb{F}_9 = \mathbb{F}_3(a)$ given by the multiplier -3 are generated by $h^\natural$ where h is a monic solution to the skew equation in $\mathbb{F}_9[X;\theta]$:*

$$\begin{aligned} \Theta(h^\natural) \cdot h &= (X^{32}-1)/(X^2-1) \\ &= (X^2+1)(X^4+1) \\ &\quad \big((X^4+X^2+2)(X^4+2X^2+2)\big)\ \big((X^8+X^4+2)(X^8+2X^4+2)\big) \end{aligned}$$

There are $16128 = (3+1)(1+3^1)(3+3^2)(3+3^4)$ such codes. One of them is a $[32, 17, 11]_9$ code generated by $h^\natural$ where $h = X^{15} + a^5X^{14} + a^6X^{13} + 2X^{12} + 2X^{11} + a^5X^9 + a^3X^8 + 2X^7 + 2X^6 + a^3X^4 + a^5X^3 + a^5X^2 + a^6X + a^7$.

4 Weakly self-dual $[2k, k-1]$ θ-cyclic codes over $\mathbb{F}_{p^2}$

The aim of this section is to construct weakly self-dual $[2k, k-1]$ θ-cyclic codes over $\mathbb{F}_{p^2}$ when k is coprime with p for both Euclidean and Hermitian scalar products.

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

According to ([7], theorems 6.4.1), a cyclic code of odd length n and dimension $(n-1)/2$ over $\mathbb{F}_q$ is Euclidean weakly self-dual if and only if it is an even-like duadic code given by the multiplier -1. According to ([7], theorem 6.4.4), a cyclic code of odd length n and dimension $(n-1)/2$ over $\mathbb{F}_4$ is Hermitian weakly self-dual if and only if it is an even-like duadic code given by the multiplier -2.

Recall that the Euclidean dual of a θ-cyclic code of length $2k$ with skew generator polynomial g is the θ-cyclic code with skew generator polynomial $h^{\natural}$ where $h \cdot g = X^{2k} - 1$ ([2], [3]). Euclidean self-dual θ-cyclic $[2k, k]$ codes are constructed and enumerated for any k in [4]. Consider q an even power of an arbitrary prime number. As the hermitian product of $x, y \in \mathbb{F}_q^n$ is equal to $< x, \overline{y} >$, the Hermitian dual of a code is the Euclidean dual of $\overline{C}$. In particular, if C is a θ-cyclic code of length n and skew generator polynomial g, then its Hermitian dual is the θ-cyclic code of length n with skew generator polynomial $\overline{h^{\natural}}$ (see [2]) .

The following proposition gives a sufficient weak self-duality condition for θ-cyclic codes of length mk and dimension $(mk-m)/2$.

Proposition 5 *Consider q a prime power, θ an automorphism of $\mathbb{F}_q$ of order m and an integer k coprime with q such that $mk - m$ is even.*

- *The even-like θ-duadic codes of length mk given by the multiplier -1 are Euclidean weakly self-dual θ-cyclic codes.*
- *Assume that $q = r^2$ is an even power of an arbitrary prime number. The even-like θ-duadic codes of length mk given by the multiplier $-r$ are Hermitian weakly self-dual θ-cyclic codes.*

Proof. Consider an even-like θ-duadic code of length mk given by the multiplier -1. Its skew generator polynomial is $(X^m - 1) \cdot h^{\natural}$ where $(X^m - 1) \cdot h^{\natural} \cdot h = X^{mk} - 1$. The Euclidean dual $C^{\perp}$ of C is generated by $h^{\natural}$, therefore $C \subset C^{\perp}$.

Assume that $q = r^2$. Consider an even-like θ-duadic code of length mk given by the multiplier $-r$. Its skew generator polynomial is $(X^m - 1) \cdot \overline{h^{\natural}}$ where $(X^m - 1) \cdot \overline{h^{\natural}} \cdot h = X^{mk} - 1$. The Hermitian dual $C^{\perp_H}$ of C is generated by $\overline{h^{\natural}}$, therefore $C \subset C^{\perp_H}$.

■

Proposition 6 characterizes Euclidean weakly self-dual θ-cyclic codes with length $2k$ and maximum dimension $k-1$ over $\mathbb{F}_{p^2}$. Even-like θ-duadic codes are a special case of weakly

self-dual θ-cyclic codes.

Proposition 6 *Consider p a prime number, θ the Frobenius automorphism over $\mathbb{F}_{p^2}$. There exists an Euclidean weakly self-dual $[2k, k-1]$ θ-cyclic code over $\mathbb{F}_{p^2}$ for any integer k coprime with p. The skew generator polynomial of such a code is $P \cdot h^\natural$ where P and h satisfy one of these conditions :*

1. *$P = X^2 - 1$ and*
$$h^\natural \cdot h = \frac{X^{2k} - 1}{X^2 - 1}. \tag{19}$$
In this case the code is an even-like θ-duadic code (given by the multiplier -1).
Furthermore $p = 2$ or ($k \equiv 0 \pmod 2$ and $p \equiv 1 \pmod 4$) or $k \equiv 1 \pmod 2$.

2. *$P = X^2 + 1$ and*
$$h^\natural \cdot h = \frac{X^{2k} - 1}{X^2 + 1}. \tag{20}$$
Furthermore $k \equiv 0 \pmod 2$ and $p \equiv 3 \pmod 4$.

3. *$P = (X - \lambda) \cdot (X + 1/\lambda)$, $(\lambda^{p+1})^k = 1$, $h = H \cdot (X + \lambda^p)$ or $h = H \cdot (X - 1/\lambda)$and*
$$H^\natural \cdot H = \frac{X^{2k} - 1}{(X^2 - \lambda^{p+1})(X^2 - 1/\lambda^{p+1})}. \tag{21}$$
Furthermore $k \equiv 1 \pmod 2$, $p \equiv 3 \pmod 4$ and $\gcd(k, p-1) \neq 1$.

Proof. Consider a θ-cyclic code C with length $2k$ and dimension $k-1$. It is generated by a skew polynomial g of degree $k+1$ which divides $X^{2k} - 1$. Its Euclidean dual is generated by $h^\natural$ where the skew polynomial h is defined by $g \cdot h = X^{2k} - 1$. The code C is Euclidean weakly self-dual if and only if the skew polynomial g is a right multiple of the skew polynomial $h^\natural$. That means that there exists P in R with degree 2 such that $g = P \cdot h^\natural$. Therefore C is weakly self-dual if and only if $P \cdot h^\natural \cdot h = X^{2k} - 1$.

1. If $P = X^2 - 1$ then one gets the equation (19). As k is coprime with p, $X^2 - 1$ does not divide $F(X^2) = \frac{X^{2k}-1}{X^2-1}$. If k is even or if $p = 2$, then $X^2 + 1$ does not divide $F(X^2)$, therefore $F(X^2) = \prod_{f \in \mathcal{F} \cap \mathcal{D}_F} f(X^2) \times \prod_{f \in \mathcal{G} \cap \mathcal{D}_F} f(X^2)$. According to Lemma 3 and Lemma 4, the set $\mathcal{H}_f^{(0)}$ is not empty when f belongs to $\mathcal{F} \cup \mathcal{G}$, therefore, according to Proposition 2, the set $\mathcal{H}_F^{(0)}$ is also not empty. If k is odd and p is odd then $X^2 + 1$ divides $F(X^2)$ and $F(X^2) = (X^2 + 1) \times \prod_{f \in \mathcal{F} \cap \mathcal{D}_F} f(X^2) \times \prod_{f \in \mathcal{G} \cap \mathcal{D}_F} f(X^2)$. As $\mathcal{H}_{X^2+1}^{(0)}$ is nonempty if and only if $p \equiv 1 \pmod 4$, the set $\mathcal{H}_F^{(0)}$ is not empty if and only if $p \equiv 1 \pmod 4$.

2. Assume that p is odd and that $P = X^2 + 1$ then one gets the equation (20). Necessarily, k must be even. As $X^2 + 1$ does not divide $F(X^2) = \frac{X^{2k}-1}{X^2+1}$ and as $X^2 - 1$ divides $F(X^2)$, one has $F(X^2) = (X^2 - 1) \times \prod_{f \in \mathcal{F} \cap \mathcal{D}_F} f(X^2) \times \prod_{f \in \mathcal{G} \cap \mathcal{D}_F} f(X^2)$. Furthermore $\mathcal{H}_{X^2-1}^{(0)}$ is nonempty if and only if $p \equiv 3 \pmod 4$ therefore, there is a solution if and only if $p \equiv 3 \pmod 4$.

3. Assume that p is odd and $P \neq X^2 \pm 1$.

   Let us show that P must be reducible. Assume that P is irreducible and consider his bound $f(X^2)$. $f(X^2)$ is an irreducible polynomial in $\mathbb{F}_p[X^2]$ and each factorization of $f(X^2)$ into the product of irreducible skew polynomials contains two terms with degree 2. The same property holds for $f^\natural(X^2)$ as $f^\natural(X^2)$ is also irreducible in $\mathbb{F}_p[X^2]$. As $X^{2k}-1$ is squarefree in $\mathbb{F}_p[X^2]$, each factorization of $X^{2k}-1$ in R contains exactly two irreducible factors bounded by $f(X^2)$ and two irreducible factors bounded by $f^\natural(X^2)$.

   Let r (resp. s) denote the number of irreducible factors bounded by $f(X^2)$ (resp. $f^\natural(X^2)$) in any factorization of h over R.

   Necessarily $f \neq f^\natural$ otherwise there is an even number of factors bounded by $f(X^2)$ in each factorization of $\Theta^b(h^\natural)\cdot h$ in the product of irreducible skew polynomials, which is impossible.

   As $f \neq f^\natural$, there are $r+s+1$ (resp. $r+s$) factors bounded by $f(X^2)$ (resp. $f^\natural(X^2)$) in any factorization of $P\cdot h^\natural \cdot h$, therefore, $r+s+1 = 2 = r+s$, which is a contradiction.

   Therefore $P = (X-\lambda)\cdot(X-\mu)$ where $\lambda, \mu \in \mathbb{F}_{p^2}$. Let $X^2-a \in \mathbb{F}_p[X^2]$ denote the bound of $X-\lambda$ and $X^2-b \in \mathbb{F}_p[X^2]$ denote the bound of $X-\mu$. Necessarily, $a^k = b^k = 1$ as X^2-a and X^2-b divide $X^{2k}-1$.

   Consider $f_1(X^2) = lcm(X^2-a, X^2-b)$ and $f_2(X^2) = (X^{2k}-1)/f_1(X^2)$.

   Assume that $a = b$, then $(X-\lambda)\cdot(X-\mu)\cdot h^\natural \cdot h = (X^2-a)f_2(X^2)$, and $h^\natural \cdot h$ is coprime with X^2-a, furthermore X^2-a is central, therefore $\mathrm{lclm}(X^2-a, h^\natural\cdot h) = (X^2-a)h^\natural\cdot h$. As X^2-a and $h^\natural\cdot h$ divide $X^{2k}-1$, their lclm also divides $X^{2k}-1 = (X^2-a)f_2(X^2)$ therefore $h^\natural\cdot h$ divides $f_2(X^2)$. Considerations on the degrees of these two skew polynomials enable to conclude that $h^\natural\cdot h = f_2(X^2)$. Furthermore $f_2(X^2)$ must be self-reciprocal (as $h^\natural\cdot h$ is self-reciprocal), therefore $f_1(X^2)$ is also self-reciprocal and $a^2 = 1$. Lastly, $(X-\lambda)\cdot(X-\mu) = X^2-a = P$. One gets the first and second cases of the Proposition.

   Assume that $a \neq b$, then $(X-\lambda)\cdot(X-\mu)\cdot h^\natural\cdot h = (X^2-a)(X^2-b)f_2(X^2)$. Necessairly p is here an odd prime number.

   $X^{2k}-1$ has two factors bounded by X^2-a and two factors with bound X^2-b. Necessarily, $h^\natural\cdot h$ contains two factors bounded by X^2-a and X^2-b. Assume that these two factors appear in h, then $h^\natural$ has two factors bounded by X^2-1/a and X^2-1/b. Necessarily $1/a \neq a, b$ and $1/b \neq b$. $(X-\lambda)\cdot(X-\mu)\cdot h^\natural\cdot h$ has two factors bounded by X^2-1/a and X^2-1/b, whereas $X^{2k}-1$ has four factors bounded by X^2-1/a and X^2-1/b. There is a contradiction, therefore h has one factor bounded by X^2-a or X^2-b.

   Furthermore $h = \mathrm{lcrm}(h_1, h_2)$ where $h_1 = \mathrm{gcld}(h, f_1(X^2))$ and $h_2 = \mathrm{gcld}(h, f_2(X^2))$. Consider $H_2 = X+u$ such that $h = h_2 \cdot H_2$, then $h_2^\natural \cdot h_2$ divides $X^{2k}-1$. As $h_2^\natural\cdot h_2$ is coprime with $f_1(X^2)$, $h_2^\natural\cdot h_2$ divides $f_2(X^2)$. Furthermore the degree of H_2 is one, and H_2 and h_2 are coprime so $\deg(h) = \deg(h_2)+1$, therefore $\deg(h_2^\natural\cdot h_2) = \deg(f_2(X^2))$ and one gets $h_2^\natural\cdot h_2 = f_2(X^2)$. Furthermore $f_1(X^2)$ must be self-reciprocal, therefore $b = 1/a$.

   One has

$h = h_2 \cdot (X+u)$ and $h_2^\natural \cdot h_2 = f_2(X^2)$ therefore $h^\natural = (X - \frac{1}{u}) \cdot h_2^\natural$ and the equality $(X-\lambda)\cdot(X-\mu)\cdot h^\natural \cdot h = X^{2k}-1$ leads to

$$(X-\lambda)\cdot(X-\mu)\cdot(X-1/u)\cdot(X+u) = (X^2-a)(X^2-1/a).$$

A small computation leads to $\mu = -1/\lambda$ and $u = \frac{a}{\lambda} = \lambda^p$ or $u = \frac{-1}{\lambda}$.

■

Example 7 *The even-like θ-duadic code associated to the $[34,18,9]_4$ odd-like θ-duadic code C of Example 4 is Euclidean weakly self-dual. Furthermore C can be extended to a $[36,18,11]_4$ self-dual code $\tilde{C}$ which is not equivalent to the previous $[36,18,11]_4$ self-dual θ-cyclic codes (computed in [2]). A generator matrix of $\tilde{C}$ is the block-matrix $\tilde{G} = \begin{pmatrix} G & M \end{pmatrix}$ where*

$$G = \begin{pmatrix}
a & 1 & a & a & 1 & a & 0 & 1 & 0 & a & 0 & 1 & a & 1 & 1 & a & 1 & 0 & \cdots & & 0 \\
0 & a^2 & 1 & a^2 & a^2 & 1 & a^2 & 0 & 1 & 0 & a^2 & 0 & 1 & a^2 & 1 & 1 & a^2 & 1 & 0 & \cdots & 0 \\
\vdots & & & & & & & & & & & & & & & & & & & & \\
0 & \cdots & 0 & a & 1 & a & a & 1 & a & 0 & 1 & 0 & a & 0 & 1 & a & 1 & 1 & a & 1 & 0 \\
0 & \cdots & 0 & 0 & a^2 & 1 & a^2 & a^2 & 1 & a^2 & 0 & 1 & 0 & a^2 & 0 & 1 & a^2 & 1 & 1 & a^2 & 1
\end{pmatrix}$$

is a generator matrix of C and M is the 18×2 matrix defined by

$${}^tM = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
a & a^2 & a & a^2 & a & a^2 & a & a^2 & a & a^2 & a & a^2 & a & a^2 & a & a^2 & a & a^2
\end{pmatrix}.$$

Example 8 *Example 5 shows that there is no even-like θ-duadic code of length 32 and dimension 15 over $\mathbb{F}_9$ given by the multiplier -1. However, there exists Euclidean weakly self-dual θ-cyclic codes of length 32 and dimension 15 over $\mathbb{F}_9$. They are generated by $(X^2+1)\cdot h^\natural$ where h satisfies the following skew equation*

$$\begin{aligned} h^\natural \cdot h &= (X^{32}-1)/(X^2+1) \\ &= (X^2-1)(X^4+1)(X^4+X^2+2)(X^4+2X^2+2)(X^8+X^4+2)(X^8+2X^4+2). \end{aligned}$$

There are $8064 = 2(1+3^1)(3+3^2)(3+3^4)$ solutions. For $h = X^{15}+a^7\,X^{14}+a^3\,X^{13}+a^7\,X^{11}+a^5\,X^{10}+a^2\,X^8+2\,X^7+a^5\,X^5+a^3\,X^4+a^7\,X^2+a^3\,X+a^6$, the skew polynomial $(X^2+1)\cdot h^\natural$ generates a Euclidean weakly self-dual θ-cyclic code. Furthermore the corresponding odd-like θ-duadic code (generated by $h^\natural$) C can be extended to a self-dual $[34,17,12]_9$ code $\tilde{C}$. A generator matrix of $\tilde{C}$ is the block-matrix $\tilde{G} = \begin{pmatrix} G & M \end{pmatrix}$ where

$$G = \begin{pmatrix}
a^6 & a^3 & a & 0 & a^5 & a^5 & 0 & 2 & a^2 & 0 & a^3 & a^7 & 0 & a^3 & a & 1 & 0 & \cdots \\
0 & a^2 & a & a^3 & 0 & a^7 & a^7 & 0 & 2 & a^6 & 0 & a & a^5 & 0 & a & a^3 & 1 & \cdots \\
\vdots & & & & & & & & & & & & & & & & &
\end{pmatrix}$$

is a generator matrix of C and M is the 17×2 matrix defined by

$${}^tM = \begin{pmatrix}
1 & a^6 & 2 & a^2 & 1 & a^6 & 2 & a^2 & 1 & a^6 & 2 & a^2 & 1 & a^6 & 2 & a^2 & 1 \\
a^2 & 2 & a^6 & 1 & a^2 & 2 & a^6 & 1 & a^2 & 2 & a^6 & 1 & a^2 & 2 & a^6 & 1 & a^2
\end{pmatrix}.$$

Proposition 7 characterizes Hermitian weakly self-dual θ-cyclic codes with length $2k$ and maximum dimension $k-1$ over $\mathbb{F}_{p^2}$.They are necessarily even-like θ-duadic codes.

Proposition 7 *Consider p a prime number, θ the Frobenius automorphism over $\mathbb{F}_{p^2}$. There exists Hermitian weakly self-dual $[2k, k-1]$ θ-cyclic codes over $\mathbb{F}_{p^2}$ for any integer k coprime with p. Furthermore they are necessarily even-like θ-duadic codes (given by the multiplier $-p$).*

Proof. Consider a θ-cyclic code C with length $2k$ and dimension $k-1$. It is generated by a skew polynomial g of degree $k+1$ which divides $X^{2k}-1$. Its Hermitian dual is generated by $\Theta(h^\natural)$ where the skew polynomial h is defined by $g \cdot h = X^{2k}-1$. The code C is Hermitian weakly self-dual if and only if the skew polynomial g is a right multiple of the skew polynomial $\Theta(h^\natural)$. That means that there exists P in R with degree 2 such that $g = P \cdot \Theta(h^\natural)$. Therefore C is Hermitian weakly self-dual if and only if $P \cdot \Theta(h^\natural) \cdot h = X^{2k}-1$.

If $P = X^2-1$, one gets an even-like θ-duadic code (given by the multiplier $-p$).

If $P = X^2+1$, one gets $\Theta(h^\natural) \cdot h = \frac{X^{2k}-1}{X^2+1}$ and this equation has no solution because X^2-1 divides $\frac{X^{2k}-1}{X^2+1}$ and $\mathcal{H}^{(1)}_{X^2-1} = \emptyset$.

If $P \neq X^2 \pm 1$, then like in proof of Proposition 6, one can prove that P is reducible and that $h = h_2 \cdot H_2$ where $\Theta(h_2^\natural) \cdot h_2 = \frac{X^{2k}-1}{(X^2-a)(X^2-1/a)}$ and $a \in \mathbb{F}_p \setminus \{\pm 1\}$. As X^2-1 divides $\frac{X^{2k}-1}{(X^2-a)(X^2-1/a)}$, there is no solution.

■

Example 9 *The even-like θ-duadic code associated to the odd-like θ-duadic codes of Examples 3 and 6 are Hermitian weakly self-dual.*

5 An application : parametrization of the irreducible skew polynomials of $\mathbb{F}_{p^2}[X;\theta]$ with given bound

According to [9], the number of irreducible monic skew polynomials in $\mathbb{F}_{p^2}[X;\theta]$ of degree d is equal to $M_d \times N_d$ where N_d is the number of irreducible polynomials in $\mathbb{F}_p[X^2]$ of degree d in X^2 and $M_d = p^d+1$ is the number of monic skew polynomials bounded by $f(X^2)$ where $f(X^2)$ is irreducible in $\mathbb{F}_p[X^2]$ of degree d in X^2.

The aim of this section is to give a parametrization of all irreducible monic skew polynomials of $\mathbb{F}_{p^2}[X;\theta]$ with a given bound. This construction is based on the previous Lemma 2 and the Lemma 5 given below.

Lemma 5 *Consider $f = f(X^2)$ an irreducible polynomial of $\mathbb{F}_p[X^2]$ with degree d greater than 1. If d is even, consider the irreducible factors $\tilde{f}(Z)$ and $\Theta(\tilde{f})(Z)$ of $f(Z)$ in $\mathbb{F}_{p^2}[Z]$.*

1. *If $d = 2\delta$, then the irreducible skew polynomials of $\mathbb{F}_{p^2}[X;\theta]$ with bound $f(X^2)$ are the skew polynomials $\tilde{f}(X^2)$, $\Theta(\tilde{f})(X^2)$ and $h = A(X^2) + X \cdot B(X^2)$ where A is monic of degree δ, B is of degree $\leq \delta - 1$ coprime with f, (A,B) is solution to the Cauchy interpolation problem in $\mathbb{F}_{p^2}[Z]$*

$$\frac{A}{B} \equiv P \pmod{f}$$

and $P(Z)$ is a polynomial in $\mathbb{F}_{p^2}[Z]$ of degree $< d$ satisfying the relation

$$P\Theta(P) \equiv z \pmod{f}.$$

2. *If $d = 2\delta + 1$, then the irreducible skew polynomials of $\mathbb{F}_{p^2}[X;\theta]$ with bound $f(X^2)$ are the skew polynomials $h = A(X^2) + X \cdot B(X^2)$ where B is monic of degree δ coprime with f, A is of degree $\leq \delta$, (A, B) is solution to the Cauchy interpolation problem in $\mathbb{F}_{p^2}[Z]$*

$$\frac{A}{B} \equiv P \pmod{f}$$

and $P(Z)$ is a polynomial in $\mathbb{F}_{p^2}[Z]$ of degree $< d$ satisfying the relation

$$P\Theta(P) \equiv z \pmod{f}.$$

Proof. A monic skew polynomial h is an irreducible skew polynomial bounded by $f(X^2)$ if and only if, there exists $\tilde{h}$ monic of degree $d = \deg(h)$ such that

$$\tilde{h} \cdot h = f(X^2). \tag{22}$$

1. Assume that d is even and consider $\tilde{f}(Z)$ irreducible in $\mathbb{F}_{p^2}[Z]$ such that $f(Z) = \tilde{f}(Z)\Theta(\tilde{f})(Z)$. Consider $A(Z), \tilde{A}(Z) \in \mathbb{F}_{p^2}[Z]$ monic of degree δ and $B(Z), \tilde{B}(Z) \in \mathbb{F}_{p^2}[Z]$ of degree $\leq \delta - 1$ such that $h = A(X^2) + X \cdot B(X^2)$ and $\tilde{h} = \tilde{A}(X^2) + \tilde{B}(X^2) \cdot X$. Then (22) is equivalent to

$$\begin{cases} \tilde{A}(Z)A(Z) + Z\tilde{B}(Z)B(Z) = f(Z) \\ \tilde{A}(Z)\Theta(B)(Z) + \tilde{B}(Z)\Theta(A)(Z) = 0 \end{cases} \tag{23}$$

   If $B = 0$ then $h = A(X^2) + X \cdot B(X^2) = A(X^2)$ is an irreducible skew polynomial with bound $f(X^2)$ if and only if $h = \tilde{f}(X^2)$ or $\Theta(\tilde{f})(X^2)$.

   If $B \neq 0$ then B and f are coprime because $\deg(B) < \delta$ therefore A and B are coprime and

$$(23) \quad \Leftrightarrow \quad \begin{cases} \tilde{A}(Z) = \Theta(A)(Z) \\ \tilde{B}(Z) = -\Theta(B)(Z) \\ A(Z)\Theta(A)(Z) - ZB(Z)\Theta(B)(Z) = 0. \end{cases}$$

   Consider P in $\mathbb{F}_{p^2}[Z]$ with degree $< d$ such that

$$\frac{A}{B} \equiv P \pmod{f}$$

   then $h = A(X^2) + X \cdot B(X^2)$ is an irreducible skew polynomial with bound $f(X^2)$ if and only if

$$P \times \Theta(P) \equiv Z \pmod{f}.$$

2. If d is odd, consider $A(Z), \tilde{A}(Z) \in \mathbb{F}_{p^2}[Z]$ of degree $\leq \delta$ and $B(Z), \tilde{B}(Z) \in \mathbb{F}_{p^2}[Z]$ monic of degree δ such that $h = A(X^2) + X \cdot B(X^2)$ and $\tilde{h} = \tilde{A}(X^2) + \tilde{B}(X^2) \cdot X$. Then (22) is equivalent to (23). Furthermore, f and B are necessarily coprime because f is irreducible in $\mathbb{F}_{p^2}[Z]$ and $\deg(B) < \deg(f)$, therefore

u	$P(Z) \in \mathbb{F}_4[Z]$	$h(X) \in \mathbb{F}_4[X;\theta]$
γ	$Z^2 + a^2\,Z + 1$	$X^3 + a\,X^2 + a\,X + a$
γ^8	$Z^2 + a\,Z + 1$	$X^3 + a^2\,X^2 + a^2\,X + a^2$
γ^{15}	$a^2\,Z^2 + a^2\,Z$	$X^3 + X + a^2$
γ^{22}	$a\,Z^2 + Z + a$	$X^3 + a^2\,X^2 + a\,X + a^2$
γ^{29}	$a\,Z^2 + a^2\,Z + a$	$X^3 + X^2 + a^2\,X + 1$
γ^{36}	$Z^2 + Z$	$X^3 + X + 1$
γ^{43}	$a^2\,Z^2 + a\,Z + a^2$	$X^3 + X^2 + a\,X + 1$
γ^{50}	$a^2\,Z^2 + Z + a^2$	$X^3 + a\,X^2 + a^2\,X + a$
γ^{57}	$a\,Z^2 + a\,Z$	$X^3 + X + a$

Table 1: Parametrization of the irreducible monic skew polynomials of $\mathbb{F}_4[X;\theta]$ bounded by $X^6 + X^2 + 1$.

$$(23) \quad \Leftrightarrow \quad \begin{cases} \tilde{B}(Z) = \Theta(B)(Z) \\ \tilde{A}(Z) = -\Theta(A)(Z) \\ A(Z)\Theta(A)(Z) - ZB(Z)\Theta(B)(Z) = 0. \end{cases}$$

Consider P in $\mathbb{F}_{p^2}[Z]$ with degree $< d$ such that

$$\frac{A}{B} \equiv P \pmod{f}$$

then $h = A(X^2) + X \cdot B(X^2)$ is an irreducible skew polynomial with bound $f(X^2)$ if and only if

$$P \times \Theta(P) \equiv Z \pmod{f}.$$

■

Proposition 8 *Algorithm 1 is correct.*

Proof. Lemma 2 and Lemma 5. ■

Example 10 *The irreducible monic skew polynomials of $\mathbb{F}_4[X;\theta]$ bounded by $X^6 + X^2 + 1$ are the 9 skew polynomials listed in the third column of table 10 (where $a^2 + a + 1 = 0$). Each irreducible monic skew polynomial writes as $h(X) = A(X^2) + X \cdot B(X^2)$ where (A, B) is the unique solution to the Cauchy interpolation problem $\frac{A(Z)}{B(Z)} \equiv P(Z) \pmod{f(Z)}$ with B monic, $\deg(A) \leq 1$ and $\deg(B) = 1$ (see Section 5.8 of [11] for the computation of (A, B)). The polynomials $P(Z)$ (second column of the table) are associated to the 9 parameters u in $\mathbb{F}_{2^6} = \mathbb{F}_2(\gamma)$ satisfying $u^9 = \alpha$ where $\alpha^3 + \alpha + 1 = 0$ and $\gamma^6 + \gamma^4 + \gamma^3 + \gamma + 1 = 0$ (first column of the table).*

Example 11 *The irreducible monic skew polynomials of $\mathbb{F}_4[X;\theta]$ bounded by $X^8 + X^2 + 1$ are $X^4 + X^2 + a$, $X^4 + X^2 + a^2$ and the 15 skew polynomials $h = A(X^2) + X \cdot B(X^2)$ listed in the third column of table 11 where $\frac{A(Z)}{B(Z)} \equiv P(Z) \pmod{f(Z)}$, A monic, $\deg(A) = 2$ and $\deg(B) < 2$. The polynomials $P(Z)$ (second column of the table) are associated to the 15 nonzero parameters u belonging $\mathbb{F}_{2^4} = \mathbb{F}_2(\alpha)$ where $\alpha^4 + \alpha + 1 = 0$ (first column of the table).*

Algorithm 1 Construction of irreducible skew polynomials over $\mathbb{F}_{p^2}[X;\theta]$ with given bound

Require: $f \in \mathbb{F}_p[X^2]$ irreducible in $\mathbb{F}_p[X^2]$
Ensure: All irreducible skew polynomials with bound $f(X^2)$

$d \leftarrow \deg_{X^2} f(X^2)$
$\alpha \leftarrow$ root of f in $\overline{\mathbb{F}_p}$
if d is odd **then**
  $\delta \leftarrow (d-1)/2$
  $E \leftarrow \emptyset$
  for $u \in \mathbb{F}_{p^{2d}}$ such that $u^{p^d+1} = \alpha$ **do**
    $P \leftarrow$ Interpolation Polynomial in $\mathbb{F}_{p^2}[Z]$ at the d points $[\alpha^{p^{2i}}, u^{p^{2i}}]_{0\le i\le\delta}$ and $[\alpha^{p^{2i+1}}, \alpha^{p^{2i+1}}/u^{p^{2i+1}}]_{0\le i\le\delta-1}$
    $(A,B) \leftarrow$ solution of the Cauchy interpolation problem $\dfrac{A}{B} \equiv P \pmod f$ with B monic, $\deg(B) = \delta$, $\deg(A) \le \delta$
    add $A(X^2) + X \cdot B(X^2)$ to the set E
  end for
else
  $\delta \leftarrow d/2$
  $E \leftarrow \{\tilde{f}(X^2), \Theta(\tilde{f})(X^2)\}$ where $\tilde{f}(Z)\Theta(\tilde{f})(Z) = f(Z)$ is the factorization of $f(Z)$ in $\mathbb{F}_{p^2}[Z]$
  for $u \in \mathbb{F}_{p^d}$ such that $u \neq 0$ **do**
    $P \leftarrow$ Interpolation Polynomial in $\mathbb{F}_{p^2}[Z]$ at the d points $[\alpha^{p^{2i}}, u^{p^{2i}}]_{0\le i\le\delta-1}$ and $[\alpha^{p^{2i+1}}, \alpha^{p^{2i+1}}/u^{p^{2i+1}}]_{0\le i\le\delta-1}$
    $(A,B) \leftarrow$ solution of the Cauchy interpolation problem $\dfrac{A}{B} \equiv P \pmod f$ with A monic, $\deg(A) = \delta$, $\deg(B) < \delta$
    add $A(X^2) + X \cdot B(X^2)$ to the set E
  end for
end if
return E

u	$P(Z) \in \mathbb{F}_4[Z]$	$h(X) \in \mathbb{F}_4[X;\theta]$
1	$Z^3 + a^2\,Z + a^2$	$X^4 + a^2\,X^3 + a^2\,X^2 + a$
α	$Z^3 + a\,Z + a$	$X^4 + a\,X^3 + a\,X^2 + a^2$
α^2	$a^2\,Z^3 + a^2\,Z^2 + a$	$X^4 + a^2\,X^3 + a\,X^2 + a^2\,X + a$
α^3	$a^2\,Z^2 + a^2$	$X^4 + a^2\,X + 1$
α^4	$a^2\,Z^3 + a^2\,Z^2 + 1$	$X^4 + a^2\,X^3 + a^2\,X^2 + a^2\,X + a^2$
α^5	$a\,Z^3 + Z + 1$	$X^4 + X^3 + a^2\,X^2 + a$
α^6	$a\,Z^3 + a^2\,Z + a^2$	$X^4 + a^2\,X^3 + a\,X^2 + a^2$
α^7	$Z^3 + Z^2 + a^2$	$X^4 + X^3 + a\,X^2 + X + a$
α^8	$Z^2 + 1$	$X^4 + X + 1$
α^9	$Z^3 + Z^2 + a$	$X^4 + X^3 + a^2\,X^2 + X + a^2$
α^{10}	$a^2\,Z^3 + a\,Z + a$	$X^4 + a\,X^3 + a^2\,X^2 + a$
α^{11}	$a^2\,Z^3 + Z + 1$	$X^4 + X^3 + a\,X^2 + a^2$
α^{12}	$a\,Z^3 + a\,Z^2 + 1$	$X^4 + a\,X^3 + a\,X^2 + a\,X + a$
α^{13}	$a\,Z^2 + a$	$X^4 + a\,X + 1$
α^{14}	$a\,Z^3 + a\,Z^2 + a^2$	$X^4 + a\,X^3 + a^2\,X^2 + a\,X + a^2$

Table 2: Parametrization of the irreducible monic skew polynomials of $\mathbb{F}_4[X;\theta]$ bounded by $X^8 + X^2 + 1$ and distinct of $X^4 + X^2 + a$ and $X^4 + X^2 + a^2$.

6 Conclusion and perspectives

This text gives a first step to the construction of θ-duadic codes defined over a finite field $\mathbb{F}_q$. Indeed a generalization of duadic codes given by the multiplier -1 (and the multiplier $-\sqrt{q}$ when q is a square) is obtained. One could generalize this definition to the θ-duadic codes given by more general multipliers such as $\pm p^b$ where b belongs to $\{0, \ldots, m-1\}$ and where θ is the Frobenius automorphism of order m. However it seems that a deeper study is needed to extend the definition to much more general multipliers. In particular, the notion of idempotent is absent here. When q is the square of a prime number p, a more detailed study is achieved, namely the construction and enumeration of pairs of θ-duadic codes given by the multipliers -1 and $-p$ (Proposition 3 and Proposition 4). The lemmas 3 and 4 also give an answer to the question of the enumeration of Hermitian self-dual θ-cyclic codes whose dimension is coprime with p as shown below (see perspectives of [4]) :

Proposition 9 *Consider p a prime number, θ the Frobenius automorphism over $\mathbb{F}_{p^2}$ and k an integer coprime with p. If p is odd, there exists no Hermitian self-dual θ-cyclic codes of length $2k$ over $\mathbb{F}_{p^2}$. Over $\mathbb{F}_4$, the number of Hermitian self-dual θ-cyclic codes of length $2k$ is*

$$3 \times \prod_{f \in \mathcal{F} \cap \mathcal{D}_{X^{2k}-1}} (2^\delta + 1) \times \prod_{f \in \mathcal{G} \cap \mathcal{D}_{X^{2k}-1}} (2^\delta + 3)$$

where 2δ is the degree of f in X^2.

Proof. According to Proposition 2, the number of Hermitian self-dual θ-cyclic codes over $\mathbb{F}_{p^2}$ with dimension k is $\#\mathcal{H}^{(1)}_{X^{2k}-1} = \#\mathcal{H}^{(1)}_{X^2-1} \times \prod_{f \in \mathcal{F} \cap \mathcal{D}_{X^{2k}-1}} \#\mathcal{H}^{(1)}_f \times \prod_{f \in \mathcal{G} \cap \mathcal{D}_{X^{2k}-1}} \#\mathcal{H}^{(1)}_f$. The

final result follows from Lemma 3, Lemma 4 and from the fact that the equation $\Theta(h^\natural) \cdot h = X^2 - 1$ has no solution if p is odd, and 3 solutions if $p = 2$. ∎

Over $\mathbb{F}_{p^2}$, the class of the θ-cyclic codes who are weakly self-dual, of length $2k$ and of dimension $k-1$ is also explored (where k is coprime with p and θ is the Frobenius automorphism). A link with the θ-duadic codes is obtained. Some examples of self-dual extended θ-cyclic codes are given (a $[36, 18, 11]_4$ Euclidean self-dual code in Example 7 and a $[34, 17, 12]_9$ Euclidean self-dual code in Example 8). This extension would deserve to be systemized. Furthermore an interesting remaining question is to find conditions for the existence of self-dual codes which are extended θ-cyclic.

Lastly, the techniques developed in $\mathbb{F}_{p^2}[X;\theta]$ for the enumeration of the θ-duadic codes can be applied to obtain the parametrization of the monic irreducible skew polynomials with a given bound.

References

[1] Boucher, D., Geiselmann W. and Ulmer, F. *Skew-cyclic codes*, Applicable Algebra in Engineering, Communication and Computing, Vol 18, 2007, No 4, 379–389

[2] 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

[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] Boucher D. *Construction and number of self-dual skew codes over* $\mathbb{F}_{p^2}$ Advances in Mathematics of Communications, Volume 10, No. 4, 2016, 767-797

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

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

[7] Huffman, W. Cary and Pless, Vera, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge, 2003

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

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

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

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