A construction of self-dual skew cyclic and negacyclic codes of length n over $\_p^n$

Aicha Batoul, Delphine Boucher, Ranya Boulanouar

A construction of self-dual skew cyclic and negacyclic codes of length n over $\mathbb{F}_{p^n}$.

Aicha Batoul *
Delphine Boucher †
Ranya Djihad Boulanouar ‡

July 19, 2020

Abstract

The aim of this note is to give a construction and an enumeration of self-dual θ-cyclic and θ-negacyclic codes of length n over $\mathbb{F}_{p^n}$ where p is a prime number and θ is the Frobenius automorphism over $\mathbb{F}_{p^n}$. We use the notion of isodual codes to achieve this construction.

1 Introduction

Isodual codes ([17]) have been recently studied on many aspects ([2], [3], [1]). Meanwhile, in [5], a construction and an enumeration formula for self-dual θ-cyclic and θ-negacyclic codes of even length n over $\mathbb{F}_{p^2}$ were given in the case when p is a prime number and θ is the Frobenius automorphism over $\mathbb{F}_{p^2}$. The aim of this note is to give a construction and an enumeration formula for self-dual θ-cyclic and θ-negacyclic codes of length n over $\mathbb{F}_{p^n}$ when θ is the Frobenius automorphism over $\mathbb{F}_{p^n}$. To this end, we will use and develop the notion of (θ, ν)-isodual codes which form a subfamily of the family of isodual codes. Lastly we will consider the construction of some self-dual Gabidulin evaluation codes.

The text is organized as follows. In Section 2 we define the notion of (θ, ν)-isodual codes over $\mathbb{F}_q$ where θ is an automorphism of $\mathbb{F}_q$ and ν belongs to $\mathbb{F}_q^*$. We recall the definitions of (θ, a)-constacyclic, θ-cyclic and θ-negacyclic codes and some generalities on the dual of a (θ, a)-constacyclic code. Then we characterize (θ, ν)-isodual θ-cyclic and θ-negacyclic codes thanks to an equation satisfied by the skew check polynomials of the codes. In Section 3 we consider the special case when q is equal to p^n where p is a prime number and θ is the Frobenius automorphism over $\mathbb{F}_{p^n}$. After having given a necessary and sufficient condition for the existence of (θ, ν)-isodual θ-cyclic and θ-negacyclic codes, we give a construction and an enumeration formula for (θ, ν)-isodual and self-dual θ-cyclic and θ-negacyclic codes. In Section 4, we consider a subclass of self-dual θ-cyclic codes over $\mathbb{F}_{p^n}$ which are self-dual Gabidulin codes. We parametrize this family by a parameter which satisfies a polynomial system.

2 Some generalities on isodual skew codes

We first recall that a *linear code* C of length n and dimension k over $\mathbb{F}_q$ is a subspace of dimension k of $\mathbb{F}_q^n$. A *generator matrix* G of C is a $k \times n$ matrix with coefficients in $\mathbb{F}_q$ and rank k such that

*Faculty of Mathematics, University of Science and Technology Houari Boumedienne (USTHB), 16111 Bab Ezzouar, Algiers, Algeria
†Univ Rennes, CNRS, IRMAR - UMR 6625, F-35000 Rennes, France
‡Faculty of Mathematics, University of Science and Technology Houari Boumedienne (USTHB), 16111 Bab Ezzouar, Algiers, Algeria

$C = \{m\ G \mid m \in \mathbb{F}_q^k\}$. Furthermore the dual of C is $C^\perp = \{x \in \mathbb{F}_q^n \mid \forall c \in C, < x, c >= 0\}$ where for $x = (x_0, \ldots, x_{n-1}), y = (y_0, \ldots, y_{n-1})$ in $\mathbb{F}_q^n$, $< x, y >:= \sum_{i=0}^{n-1} x_i y_i$ is the Euclidean scalar product of x and y. Isodual codes ([17]) have been recently studied on many aspects ([2], [3], [1]).

Definition 1 ([17] page 199)**.** *A code C with generator matrix G is* isodual *if it is equivalent to its dual. That means that there exists a monomial matrix D such that $G \cdot D$ is a generator matrix of the dual $C^\perp$ of C.*

In what follows, we define a special class of isodual codes which are parameterized by an automorphism θ of $\mathbb{F}_q$ and an element ν of $\mathbb{F}_q^*$.

Definition 2. *Consider $n \in \mathbb{N}^*$, $\nu \in \mathbb{F}_q^*$ and $\theta \in Aut(\mathbb{F}_q)$. A linear code C of length n and generator matrix G is a (θ, ν)-*isodual *code if $G \cdot D$ is a generator matrix of $C^\perp$ where D is the $n \times n$ diagonal matrix with diagonal coefficients $\nu, \theta(\nu), \ldots, \theta^{n-1}(\nu)$.*

Remark 1. *A code C is self-dual if and only if there exists ν fixed by θ such that C is (θ, ν)-isodual.*

Recall that if θ is an automorphism of $\mathbb{F}_q$, the skew polynomial ring R is defined as $R = \mathbb{F}_q[X; \theta]$ under usual addition of polynomials and where multiplication is defined by the commutation law : $\forall a \in \mathbb{F}_q, X \cdot a = \theta(a)X$ ([16]). The ring R is noncommutative unless θ is the identity automorphism on $\mathbb{F}_q$. The ring R is right-Euclidean and left-Euclidean. For $f = \sum a_i X^i$ in R and α in $\mathbb{F}_q$, the *evaluation* $f(\alpha)$ of f at α is the remainder in the right division of f by $X - \alpha$. We have $f(\alpha) = \sum_i a_i N_i(\alpha)$ where $N_i(x) := x\theta(x) \cdots \theta^{i-1}(x)$ (see [14]). Recall also that if $q = p^n$ and θ is the Frobenius automorphism, then the center of R is $\mathbb{F}_p[X^n]$.

For a in $\mathbb{F}_q^*$ and θ in $Aut(\mathbb{F}_q)$, a (θ, a)-*constacyclic* code C of length n and dimension k is a left R-submodule $Rg/R(X^n - a) \subset R/R(X^n - a)$ where g is a monic skew polynomial of degree $n - k$ right-dividing $X^n - a$ in R ([7]). That means that a word $c = (c_0, \ldots, c_{n-1}) \in \mathbb{F}_q^n$ belongs to C if and only if the skew polynomial g right-divides the skew polynomial $c_0 + c_1 X + \cdots + c_{n-1} X^{n-1}$ in R. The skew polynomial g is called the *skew generator polynomial* of C. The monic skew polynomial h defined by

$$\Theta^n(h) \cdot g = X^n - a \tag{1}$$

is called *skew check polynomial* of C.

The (θ, a)-constacyclic code C is denoted $C = (g)_{n,\theta}^a$. If $a = 1$, the code is θ-*cyclic* and if $a = -1$, the code is θ-*negacyclic*.

A generator matrix of C is

$$G = \begin{pmatrix} g_0 & g_1 & \ldots & \ldots & 1 & 0 & \ldots & 0 \\ 0 & \theta(g_0) & \theta(g_1) & \ldots & \ldots & 1 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & & & \ddots & 0 \\ 0 & \ldots & 0 & \theta^{k-1}(g_0) & \theta^{k-1}(g_1) & \ldots & \ldots & 1 \end{pmatrix}. \tag{2}$$

The *skew reciprocal polynomial* of $h = \Sigma_{i=0}^k h_i X^i \in R$ of degree k is $h^* = \Sigma_{i=0}^k \theta^i(h_{k-i}) X^i$. If $h_0 \neq 0$, the *left monic skew reciprocal polynomial of h* is $h^\natural = \frac{1}{\theta^k(h_0)} h^*$. The following technical lemma will be useful later. We will use the application $\Theta : R \mapsto R$ given by $\sum_{i=0}^k a_i X^i \mapsto \sum_{i=0}^k \theta(a_i) X^i$.

Lemma 1 (Lemma 1 of [8])**.** *Consider $\theta \in Aut(\mathbb{F}_q)$, $R = \mathbb{F}_q[X; \theta]$, h and g in R. Then $(h \cdot g)^* = \Theta^{\deg(h)}(g^*) \cdot h^*$.*

Example 1. *Consider $n = 4$, $\mathbb{F}_{2^4} = \mathbb{F}_2(a)$ with $a^4 + a + 1 = 0$ and $R = \mathbb{F}_{2^4}[X; \theta]$. We have*

$$X^4 + 1 = (X^2 + a^5 X + a^5) \cdot (X^2 + a^5 X + a^{10})$$

therefore the skew polynomial $g_1 = X^2 + a^5 X + a^{10}$ generates a θ-cyclic code C_1 of length 4 and dimension 2 over $\mathbb{F}_{2^4}$. As Θ^4 is the identity over $\mathbb{F}_{2^4}$, the skew check polynomial of the code is $h_1 = X^2 + a^5 X + a^5$.

We have

$$X^4+1=(X^2+aX+a^{14})\cdot(X^2+a^4X+a)$$

therefore the skew polynomial $g_2=X^2+a^4X+a$ *generates a* θ*-cyclic code* C_2 *of length* 4 *and dimension* 2 *over* $\mathbb{F}_{2^4}$ *with skew check polynomial* $h_2=X^2+aX+a^{14}$*.*

The following proposition describes the dual of a (θ,a)-constacyclic code.

Proposition 1 (Theorem 1 and Lemma 2 of [8], Proposition 1 of [6])**.** *Consider* $n\in\mathbb{N}^*$*,* $a\in\mathbb{F}_q^*$*,* $\theta\in Aut(\mathbb{F}_q)$ *and* C *a* (θ,a)*-constacyclic code of length* n *with skew generator polynomial* g *and skew check polynomial* h*. Then the dual* $C^\perp$ *of* C *is a* $(\theta,1/a)$*-constacyclic code with skew generator polynomial* $h^\natural$*.*

Proof. (proof of Proposition 1 of [6]) We consider the equality (1) in $R=\mathbb{F}_q[X;\theta]$ and we multiply both members of this equality by h on the right. We get $\Theta^n(h)\cdot g\cdot h=(X^n-a)\cdot h$ and we deduce from this equality that $\Theta^n(h)\cdot(X^n-g\cdot h)=a\cdot h$. As the skew polynomials $\Theta^n(h)$ and $a\cdot h$ have the same degrees, the skew polynomial $X^n-g\cdot h$ is a constant that we will denote λ and $\Theta^n(h)\cdot\lambda-a\cdot h=0$. As the leading coefficient of $\Theta^n(h)\cdot\lambda-a\cdot h$ is equal to $\theta^k(\lambda)-a$, we get that $\lambda=\theta^{-k}(a)$.

Furthermore, as $\Theta^n(h)\cdot g=X^n-a$, according to Lemma 1, we have $-\frac{1}{a}\Theta^{k-n}(g^*)\cdot h^*=X^n-\frac{1}{a}$. Therefore $h^\natural$ right-divides $X^n-\frac{1}{a}$ and is the skew generator polynomial of a $(\theta,\frac{1}{a})$-constacyclic code of length n.

A quick computation gives that for all (i,j) in $\{0,\dots,k-1\}\times\{0,\dots,n-k-1\}$, the Euclidean scalar product of the words associated to $X^i\cdot g$ and $X^j\cdot h^*$ is equal to $\theta^i((g\cdot h)_{j-i+k})$. Therefore the scalar product is equal to 0 and the words of the code $(g)^a_{n,\theta}$ are orthogonal to the words of the code $(h^\natural)^{1/a}_{n,\theta}$. □

In what follows, we characterize (θ,a)-constacyclic codes which are (θ,ν)-isodual.

Proposition 2. *Consider* $k\in\mathbb{N}^*$*,* $n=2k$*,* $\nu\in\mathbb{F}_q^*$*,* $a\in\mathbb{F}_q$*,* $\theta\in Aut(\mathbb{F}_q)$*,* $R=\mathbb{F}_q[X;\theta]$*,* $h\in R$ *monic. The* (θ,a)*-constacyclic code of length* n*, dimension* k *and skew check polynomial* h *is* (θ,ν)*-isodual if and only if*

$$\Theta^n(h)\cdot\theta^k(\nu)\cdot h^\natural\cdot\frac{1}{\nu}=X^n-a. \tag{3}$$

In this case we have $a^2=\theta^n(\nu)/\nu$*.*

Proof. Consider $C=(g)^a_{n,\theta}$ the (θ,a)-constacyclic code of length $n=2k$, dimension k, skew check polynomial h and skew generator polynomial g. According to (1), we have $\Theta^n(h)\cdot g=X^n-a$. Therefore, the relation (3) is satisfied if and only if $h^\natural=\tilde{g}$ where $\tilde{g}=\theta^k(1/\nu)\cdot g\cdot\nu$.

Let us prove that C is (θ,ν)-isodual if and only if $h^\natural=\tilde{g}$. As g right-divides X^n-a, $\tilde{g}$ right-divides $X^n-\tilde{a}$ where $\tilde{a}=a\frac{\nu}{\theta^n(\nu)}$. Therefore we can consider the $(\theta,\tilde{a})$-constacyclic code of length n and skew generator polynomial $\tilde{g}$. Furthermore, according to Proposition 1, $C^\perp$ is a $(\theta,1/a)$-constacyclic code of length n with skew generator polynomial $h^\natural$.

Let us prove that C is (θ,ν)-isodual if and only if $(h^\natural)^{1/a}_{n,\theta}=(\tilde{g})^{\tilde{a}}_{n,\theta}$.

Denote $g=\sum_{i=0}^{n-k}g_iX^i=\sum_{i=0}^{k}g_iX^i$ and $\tilde{g}=\sum_{i=0}^{k}\tilde{g}_iX^i$. We have $\tilde{g}_i=\theta^k(1/\nu)g_i\theta^i(\nu)$ for all i in $\{0,\dots,k\}$. Therefore a generator matrix of $(\tilde{g})^{\tilde{a}}_{n,\theta}$ is

$$\tilde{G}=\begin{pmatrix}\tilde{g}_0 & \tilde{g}_1 & \dots & \dots & 1 & 0 & \dots & 0\\ 0 & \theta(\tilde{g}_0) & \theta(\tilde{g}_1) & \dots & \dots & 1 & \ddots & \vdots\\ \vdots & & \ddots & \ddots & & & \ddots & 0\\ 0 & \dots & 0 & \theta^{k-1}(\tilde{g}_0) & \theta^{k-1}(\tilde{g}_1) & \dots & \dots & 1\end{pmatrix}=G\cdot D$$

where G is given by (2) and D is the diagonal matrix with diagonal elements $\nu,\theta(\nu),\dots,\theta^{n-1}(\nu)$.

According to Definition 2, the code C is (θ,ν)-isodual if and only if a generator matrix of $C^\perp = (h^\natural)^{1/a}_{n,\theta}$ is $G \cdot D$. As $G \cdot D = \tilde{G}$ is a generator matrix of $(\tilde{g})^{\tilde{a}}_{n,\theta}$, we obtain that C is (θ,ν)-isodual if and only if $(h^\natural)^{1/a}_{n,\theta} = (\tilde{g})^{\tilde{a}}_{n,\theta}$.

Lastly as $\tilde{g}$ right-divides $X^n - a\frac{\nu}{\theta^n(\nu)}$ and $h^\natural$ right-divides $X^n - \frac{1}{a}$, we obtain $a^2 = \theta^n(\nu)/\nu$. $\square$

In the case when θ is the Frobenius automorphism over $\mathbb{F}_q$ and $q = p^n$ where p is prime and n is the length of the code we obtain the following corollary that will be useful in next section.

Corollary 1. *Consider $k \in \mathbb{N}^*$, $n = 2k$, p a prime number, $\nu \in \mathbb{F}_{p^n}^*$, $a \in \mathbb{F}_{p^n}$, $\theta : x \mapsto x^p \in Aut(\mathbb{F}_{p^n})$, $R = \mathbb{F}_{p^n}[X;\theta]$, $h \in R$ monic. The (θ,a)-constacyclic code of length n and skew check polynomial h is (θ,ν)-isodual if and only if*

$$h \cdot \theta^k(\nu) \cdot h^\natural \cdot \frac{1}{\nu} = h^\natural \cdot \frac{1}{\nu} \cdot h \cdot \theta^k(\nu) = X^n - a. \tag{4}$$

Furthermore, $a^2 = 1$.

Proof. As θ is the Frobenius automorphism over $\mathbb{F}_{p^n}$, the order of θ is equal to n. Therefore $\Theta^n(h) = h$ and $\theta^n(\nu) = \nu$. According to Proposition 2, the (θ,a)-constacyclic code of length n and skew check polynomial h is (θ,ν)-isodual if and only if $h \cdot \theta^k(\nu) \cdot h^\natural \cdot \frac{1}{\nu} = X^n - a$. In this case $a^2 = 1$. Therefore $X^n - a$ is central in R, and we have $h \cdot \theta^k(\nu) \cdot h^\natural \cdot \frac{1}{\nu} = X^n - a = h^\natural \cdot \frac{1}{\nu} \cdot h \cdot \theta^k(\nu)$. $\square$

Example 2. *(Example 1 continued) The left monic skew reciprocal polynomial of $h_1 = X^2 + a^5X + a^5$ is $h_1^\natural = X^2 + a^5X + a^{10}$ and $X^4 + 1 = (X^2 + a^5X + a^5) \cdot (X^2 + a^5X + a^{10}) = (X^2 + a^5X + a^{10}) \cdot (X^2 + a^5X + a^5)$, therefore the θ-cyclic code C_1 with skew check polynomial h_1 is self-dual.*

The left monic skew reciprocal polynomial of $h_2 = X^2 + aX + a^{14}$ is $h_2^\natural = X^2 + a^6X + a^4$. Furthermore, $X^4+1 = (X^2+aX+a^{14}) \cdot (X^2+a^4X+a) = (X^2+aX+a^{14}) \cdot \frac{1}{a^4} \cdot (X^2+a^6X+a^4) \cdot \frac{1}{a^{14}}$, therefore the θ-cyclic code C_2 with skew check polynomial h_2 is (θ, a^{14})-isodual.

Lastly, we consider below a technical lemma which will be useful later and which deals with the factorization of skew polynomials right-dividing $X^n \pm 1$ in $\mathbb{F}_{p^n}[X;\theta]$ where θ is the Frobenius automorphism. These skew polynomials belong to a wide class of skew polynomials, called Wedderburn polynomials, which have been extensively studied (see Theorem 6.4 of [11] for the factorizations of these skew polynomials). Lemma 2 can be directly deduced from Theorem 6.4 of [11] as well as from Proposition 2.2.2. of [10]. We propose here a proof very specific to our special case.

Lemma 2. *Consider $n \in \mathbb{N}^*$, p a prime number, $\theta : x \mapsto x^p \in Aut(\mathbb{F}_{p^n})$, $R = \mathbb{F}_{p^n}[X;\theta]$, f in R of degree d and $\epsilon \in \{-1,1\}$ such that f right-divides $X^n - \epsilon$ in R. Then f is the product of d linear factors right-dividing $X^n - \epsilon$ and*

$$\#\{(\alpha_1,\ldots,\alpha_d) \in \mathbb{F}_{p^n}^d \mid f = (X+\alpha_1)\cdots(X+\alpha_d)\} = \prod_{i=1}^{d} \frac{p^i - 1}{p-1}.$$

Proof. Consider $y_1,\ldots,y_n$ in $\mathbb{F}_{p^n}$ linearly independent over $\mathbb{F}_p$. Consider ξ in $\mathbb{F}_{p^n}$ such that $X - \xi$ right-divides $X^n - \epsilon$, which means $N_n(\xi) = \epsilon$. Denote $\alpha_1 := \xi\frac{\theta(y_1)}{y_1}, \ldots, \alpha_n = \xi\frac{\theta(y_n)}{y_n}$. According to [14], the least common left multiple of $X - \alpha_1, \ldots, X - \alpha_n$ is $\mathrm{lclm}_{1\le i\le n}(X - \alpha_i) = X^n - \epsilon$. As f right-divides $X^n - \epsilon$, according to Theorem 4 of [16], there exist $\beta_1,\ldots,\beta_d$ in $\mathbb{F}_{p^n}$ such that $f = \mathrm{lclm}_{1\le i\le d}(X - \beta_i)$. Furthermore $N_n(\beta_i) = \epsilon = N_n(\xi)$. Therefore according to Theorem 27 of [13], there exists z_i in $\mathbb{F}_{p^n}^*$ such that $\beta_i = \xi\frac{\theta(z_i)}{z_i}$. According to [14], $z_1,\ldots,z_d$ are linearly independent over $\mathbb{F}_p$. Denote $f = \sum_{i=0}^d a_iX^i$, we have $\{\alpha \in \mathbb{F}_{p^n} \mid f(\alpha) = 0\} = \{\alpha = \xi\frac{\theta(y)}{y} = \xi y^{p-1} \in \mathbb{F}_{p^n} \mid L(y) = 0\}$ where $L(y) := \sum_{i=0}^d a_iN_i(\xi)\theta^i(y)$. As the equation $L(y) = 0$ has d solutions $(z_1,\ldots,z_d)$ in $\mathbb{F}_{p^n}$ linearly independent over $\mathbb{F}_p$, there are $p^d - 1$ nonzero y in $\mathbb{F}_{p^n}$ such that $L(y) = 0$. Therefore $\{\alpha \in \mathbb{F}_{p^n} \mid X - \alpha$ right-divides $f\}$ has $(p^d - 1)/(p - 1)$ elements. We conclude using an inductive argument.

$\square$

Remark 2. *It could be noted that the number* $\prod_{i=1}^{d} \frac{p^i-1}{p-1}$ *is the size of the general linear group* $GL(d,p)$ *modulo diagonal matrices, and corresponds to choosing a set of 1-dimensional vector spaces spanning a d-dimensional vector space.*

Example 3. *(Example 1 continued) The skew polynomial* $h_1 = X^2+a^5X+a^5$ *has* 3 *factorizations into the product of linear monic skew polynomials, namely* $h_1 = (X+a^{14})\cdot(X+a^6) = (X+a^{11})\cdot(X+a^9) = (X+1)\cdot(X+a^5)$. *The skew polynomial* $h_2 = X^2+aX+a^{14}$ *has also* 3 *factorizations into the product of linear monic skew polynomials, namely* $h_2 = (X+a^7)\cdot(X+a^7) = (X+a^{11})\cdot(X+a^3) = (X+a^{10})\cdot(X+a^4)$.

3 Construction and enumeration of (θ,ν)-isodual θ-cyclic and θ-negacyclic codes of length n over $\mathbb{F}_{p^n}$

The aim of this section is to construct and to enumerate self-dual θ-cyclic and θ-negacyclic codes of length n over $\mathbb{F}_{p^n}$ where θ is the Frobenius automorphism. Note that in this setting, θ-cyclic codes are called *Gabidulin p-cyclical codes* (page 6 of [12]).

To achieve this construction, we will consider θ-cyclic and θ-negacyclic codes which are (θ,ν)-isodual.

We introduce some notation. Consider $R = \mathbb{F}_{p^n}[X;\theta]$. We will denote, for $\epsilon \in \{-1,1\}$ and $\nu \in \mathbb{F}_q^*$:

$$\mathcal{H}_{\nu,\epsilon} := \{h \in R \mid h \text{ monic}, h^\natural \cdot \frac{1}{\nu} \cdot h \cdot \theta^k(\nu) = X^n - \epsilon\}.$$

According to Corollary 1, the set $\mathcal{H}_{\nu,\epsilon}$ is the set of the skew check polynomials of (θ,ν)-isodual (θ,ϵ)-constacyclic codes. Following Remark 1, the set $\mathcal{H}_{1,\epsilon}$ is the set of the skew check polynomials of self-dual (θ,ϵ)-constacyclic codes.

3.1 Necessary and sufficient existence condition for (θ,ν)-isodual θ-cyclic and θ-negacyclic codes of length n over $\mathbb{F}_{p^n}$

In [4] a necessary and sufficient condition for the existence of self-dual (θ,ϵ)-constacyclic codes over a finite field $\mathbb{F}_q$ was derived where θ is an automorphism of $\mathbb{F}_q$ and $\epsilon \in \{-1,1\}$. In what follows we give a necessary and sufficient condition for the existence of (θ,ν)-isodual (θ,ϵ)-constacyclic codes of length n over $\mathbb{F}_{p^n}$ where p is a prime number and θ is the Frobenius automorphism.

Proposition 3. *Consider* $k \in \mathbb{N}^*$, $n = 2k$, *p a prime number,* $\theta : x \mapsto x^p \in Aut(\mathbb{F}_{p^n})$, $\epsilon \in \{-1,1\}$.

(i) If $p = 2$, *then there exists a* (θ,ν)*-isodual* θ*-cyclic code of length n for all* ν *in* $\mathbb{F}_{p^n}^*$.

(ii) If p is odd, then for $\nu \in \mathbb{F}_{p^n}^*$, *there exists a* (θ,ν)*-isodual* (θ,ϵ)*-constacyclic code of length* $2k$ *if and only if*

$$\nu^{\frac{p^n-1}{2}} = -\epsilon(-1)^{k\frac{p-1}{2}}.$$

Proof. According to Corollary 1, there exists a (θ,ν)-isodual (θ,ϵ)-constacyclic code of length n if and only if the set $\mathcal{H}_{\nu,\epsilon}$ is nonempty.

- Assume that $p = 2$ (therefore $\epsilon = 1$) and $\nu \in \mathbb{F}_{2^n}^*$. Consider α in $\mathbb{F}_{2^n}$ such that $\alpha^2 = 1/\nu^{2^k-1} = \frac{\nu}{\theta^k(\nu)}$ and $h = X^k + \alpha$. We have

$$\begin{aligned} h^\natural \cdot \tfrac{1}{\nu} \cdot h \cdot \theta^k(\nu) &= \left(X^k + \frac{1}{\theta^k(\alpha)}\right) \cdot \left(X^k + \frac{\theta^k(\nu)\alpha}{\nu}\right) \\ &= X^{2k} + \theta^k\left(\frac{1}{\alpha} + \alpha\frac{\theta^k(\nu)}{\nu}\right) X^k + \frac{\theta^k(\nu)\alpha}{\theta^k(\alpha)\nu}. \end{aligned}$$

As $\nu/\theta^k(\nu) = \alpha^2$, we obtain

$$h^\natural \cdot \frac{1}{\nu} \cdot h \cdot \theta^k(\nu) = X^{2k} + \frac{1}{\alpha\theta^k(\alpha)}.$$

As $\theta(\alpha) = \alpha^2 = \frac{\nu}{\theta^k(\nu)}$, we obtain $\theta^{k+1}(\alpha) = \frac{\theta^k(\nu)}{\nu}$, $\theta(\alpha)\theta^{k+1}(\alpha) = 1$ and $\alpha\theta^k(\alpha) = 1$. Therefore the skew polynomial h belongs to $\mathcal{H}_{\nu,\epsilon}$.

- Assume that p is odd and $\nu^{\frac{p^n-1}{2}} = -\epsilon(-1)^{k\frac{p-1}{2}}$.

  We have

$$\begin{aligned}(-\tfrac{\theta^k(\nu)}{\nu})^{(p^n-1)/2} &= (-1)^{(p^n-1)/2}\,\tfrac{\theta^k(\nu^{(p^n-1)/2})}{\nu^{(p^n-1)/2}} \\ &= (-1)^{(p^n-1)/2} \\ &= 1 \text{ (because } p \text{ is odd, therefore } p^2 \equiv 1 \pmod 4 \text{ and } p^n \equiv 1 \pmod 4).\end{aligned}$$

  Therefore $-\frac{\nu}{\theta^k(\nu)}$ is a square. Consider α such that $-\frac{\nu}{\theta^k(\nu)} = \alpha^2$. Consider $h = X^k + \alpha$ in R.

$$\begin{aligned}h^\natural \cdot \tfrac{1}{\nu} \cdot h \cdot \theta^k(\nu) &= \left(X^k + \frac{1}{\theta^k(\alpha)}\right) \cdot \left(X^k + \frac{\theta^k(\nu)\alpha}{\nu}\right) \\ &= X^{2k} + \theta^k\left(\frac{1}{\alpha} + \alpha\frac{\theta^k(\nu)}{\nu}\right)X^k + \frac{\theta^k(\nu)\alpha}{\theta^k(\alpha)\nu}.\end{aligned}$$

  As $\nu/\theta^k(\nu) = -\alpha^2$, we obtain

$$h^\natural \cdot \frac{1}{\nu} \cdot h \cdot \theta^k(\nu) = X^{2k} + \frac{\theta^k(\nu)\alpha}{\theta^k(\alpha)\nu}.$$

  Furthermore

$$\begin{aligned}\tfrac{\theta^k(\nu)\alpha}{\theta^k(\alpha)\nu} &= \tfrac{\theta^k(\nu)}{\nu}\left(-\tfrac{\theta^k(\nu)}{\nu}\right)^{\frac{p^k-1}{2}} \quad \text{(because } -\theta^k(\nu)/\nu = 1/\alpha^2\text{)} \\ &= (-1)^{\frac{p^k-1}{2}}\nu^{\frac{p^n-1}{2}} \\ &= -\epsilon \text{ (because } \nu^{\frac{p^n-1}{2}} = -\epsilon(-1)^{k\frac{p-1}{2}}\text{)}.\end{aligned}$$

  Therefore

$$h^\natural \cdot \tfrac{1}{\nu} \cdot h \cdot \theta^k(\nu) = X^n - \epsilon.$$

- Assume that p is odd and that there exists a (θ,ϵ)-constacyclic code of length $2k$ which is (θ,ν)-isodual. Consider h its skew check polynomial and h_0 the constant term of h. Necessarily the degree of h is equal to k.

  As the code is (θ,ϵ)-constacyclic of length $2k$, h right-divides $X^{2k} - \epsilon$. As the code is defined over $\mathbb{F}_{p^{2k}}$ with $\theta : x \mapsto x^p$, $X^{2k} - \epsilon$ is central of degree 1 in $\mathbb{F}_p[X^{2k}]$ and h is the product of k linear skew polynomials $X + \alpha_1, \ldots, X + \alpha_k$ right-dividing $X^{2k} - \epsilon$. Therefore h_0 is the product of the k constant terms $\alpha_1, \ldots, \alpha_k$. As $N_{2k}(-\alpha_i) = \epsilon$, we have :

$$N_{2k}(h_0) = \epsilon^k = N_k(h_0)N_k(\theta^k(h_0)).$$

  As the code is (θ,ν)-isodual, we have $h^\natural \cdot \frac{1}{\nu} \cdot h \cdot \theta^k(\nu) = X^n - \epsilon$ and

$$h_0\theta^k(\nu) + \epsilon\theta^k(h_0)\nu = 0.$$

  As $N_k(h_0)N_k(\theta^k(h_0)) = \epsilon^k$, we obtain $N_k(h_0)^2(-\epsilon)^{k\frac{N_{2k}(\nu)}{N_k(\nu)^2}} = \epsilon^k$ and

$$N_{2k}(\nu) = (-1)^k N_k(\nu/h_0)^2.$$

Furthermore, $\theta(N_k(\nu/h_0)) = N_k(\nu/h_0)^{\frac{\theta^k(\nu/h_0)}{\nu/h_0}} = N_k(\nu/h_0)(-\epsilon)$. Therefore we have $N_k(\nu/h_0)^{p-1} = -\epsilon$. To conclude, if p is odd,

$$\nu^{\frac{p^n-1}{2}} = N_{2k}(\nu)^{(p-1)/2} = (-1)^{k\frac{p-1}{2}} N_k(\nu/h_0)^{p-1} = -\epsilon(-1)^{k\frac{p-1}{2}}.$$

□

Remark 3. *Consider $k \in \mathbb{N}^*$, $n = 2k$, p an odd prime number, $\theta : x \mapsto x^p \in Aut(\mathbb{F}_{p^n})$, $\epsilon \in \{-1, 1\}$. According to Proposition 3 and Remark 1, there exists a self-dual (θ, ϵ)-constacyclic code of length $n = 2k$ over $\mathbb{F}_{p^n}$ if and only if $1 = -\epsilon(-1)^{k\frac{p-1}{2}}$. We therefore obtain the previous result of Proposition 5 of [4]: if p is odd, there exists a self-dual θ-cyclic code of dimension k if and only if $p \equiv 3 \pmod 4$ and k is odd; there exists a self-dual θ-negacyclic code of dimension k if and only if $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$ and k even.*

The existence result of Proposition 3 is not constructive and the aim of what follows is to design a construction of the set $\mathcal{H}_{\nu,\epsilon}$ based on the construction of the sets $\tilde{\mathcal{H}}_{\mu,\epsilon}$ defined for $\mu \in \mathbb{F}_{p^n}^*$ by

$$\tilde{\mathcal{H}}_{\mu,\epsilon} := \{h \in R \mid h \in \mathcal{H}_{h_0/\mu,\epsilon}\}.$$

Thanks to factorization properties of the elements of $\tilde{\mathcal{H}}_{\mu,\epsilon}$, we will give both a construction and an enumeration formula.

3.2 Construction and enumeration formula for the set $\tilde{\mathcal{H}}_{\mu,\epsilon}$

The following technical lemma (Lemma 3) will be useful for the construction of $\tilde{\mathcal{H}}_{\mu,\epsilon}$ (Proposition 4).

Lemma 3. *Consider $k \in \mathbb{N}^*$, $n = 2k$, p a prime number, $\theta : x \mapsto x^p \in Aut(\mathbb{F}_{p^n})$, $R = \mathbb{F}_{p^n}[X;\theta]$, $P \in R$ and $\ell \in \{0, \dots, k\}$ such that $\Theta^{k+\ell}(P^*) = P$ and $\deg(P) = 2k - 2\ell$. If $X + \alpha$ right-divides P then there exists $Q \in R$ satisfying the two following properties :*

1. *$P = \Theta^{k-\ell-1}((X+\alpha)^*) \cdot Q \cdot (X+\alpha)$;*
2. *$\Theta^{k+\ell+1}(Q^*) = Q$.*

Proof. Consider $f \in R$ such that $P = f \cdot (X + \alpha)$.

1. Let us prove that $P = \Theta^{k-1-\ell}((X+\alpha)^*) \cdot \Theta^{k+\ell}(f^*)$ and that $X + \alpha$ right-divides $\Theta^{k+\ell}(f^*)$.

   As $P = f \cdot (X+\alpha)$, according to Lemma 1, we have $P^* = \Theta^{2k-2\ell-1}((X+\alpha)^*) \cdot f^*$. Therefore $P = \Theta^{k+\ell}(P^*) = \Theta^{k-\ell-1}((X+\alpha)^*) \cdot \Theta^{k+\ell}(f^*)$.

   Denote $K = k - \ell$ and $f = \sum_{j=0}^{2K-1} a_j X^j$, then $f^* = \sum_{j=0}^{2K-1} \theta^{2K-1-j}(a_j) X^{2K-1-j}$. Consider $\beta = -\theta^K(\alpha)$, then $X + \alpha$ right-divides $\Theta^{k+\ell}(f^*)$ if and only if f^* cancels at β.

   Let us prove that

   $$\sum_{j=0}^{K-1} \theta^{2K-1-j}(a_j) N_{2K-1-j}(\beta) = -\sum_{j=K}^{2K-1} \theta^{2K-j-1}(a_j) N_{2K-j-1}(\beta).$$

   As $P = f \cdot (X+\alpha) = \Theta^{K-1}((X+\alpha)^*) \cdot \Theta^{K+2\ell}(f^*)$, we obtain :

   $$\forall j \in \{1, \dots, K\}, a_{j-1} = \sum_{i=1}^{j} \frac{N_{i-1}(-\alpha)}{N_j(-\alpha)} \theta^K(\theta^{2\ell+i-1}(a_{2K-i}) + \alpha\theta^{2\ell+i-1}(a_{2K-i+1})).$$

Therefore,
$\sum_{j=0}^{K-1} \theta^{2K-1-j}(a_j)N_{2K-1-j}(\beta)$

$$
\begin{aligned}
&= \sum_{j=1}^{K} \theta^{2K-j}(a_{j-1})N_{2K-j}(\beta) \\
&= -\sum_{j=1}^{K} N_{2K-j}(\beta)\theta^{2K-j}\left(\sum_{i=1}^{j}\frac{N_{i-1}(-\alpha)}{N_j(-\alpha)}\theta^K(\theta^{2\ell+i-1}(a_{2K-i})+\alpha\theta^{2\ell+i-1}(a_{2K-i+1}))\right) \\
&= -\sum_{j=1}^{K} N_{2K-j}(\beta)\sum_{i=1}^{j}\theta^{K-j}\left(\frac{N_{i-1}(\beta)}{N_j(\beta)}\right)\theta^{3K-j}\left(\theta^{2\ell+i-1}(a_{2K-i})+\alpha\theta^{2\ell+i-1}(a_{2K-i+1})\right) \\
&= -\sum_{i=1}^{K}\sum_{j=i}^{K} N_{2K-j}(\beta)\theta^{K-j}\left(\frac{N_{i-1}(\beta)}{N_j(\beta)}\right)\theta^{i+K-j-1}(a_{2K-i}) \\
&\quad -\sum_{i=1}^{K-1}\sum_{j=i+1}^{K} N_{2K-j}(\beta)\theta^{K-j}\left(\frac{N_i(\beta)}{N_j(\beta)}\right)\theta^{i+K-j}(a_{2K-i})\theta^{3K-j}(\alpha)
\end{aligned}
$$

$$
\begin{aligned}
&= -\sum_{i=1}^{K} N_K(\beta)\frac{N_{i-1}(\beta)}{N_K(\beta)}\theta^{i-1}(a_{2K-i}) \\
&\quad -\sum_{i=1}^{K-1}\sum_{j=i}^{K-1}\Big(N_{2K-j}(\beta)\theta^{K-j}\left(\tfrac{N_{i-1}(\beta)}{N_j(\beta)}\right)\theta^{i+K-j-1}(a_{2K-i}) \\
&\qquad +N_{2K-(j+1)}(\beta)\theta^{K-(j+1)}\left(\tfrac{N_i(\beta)}{N_{j+1}(\beta)}\right)\theta^{i+K-j-1}(a_{2K-i})\,\theta^{3K-j-1}(\alpha)\Big) \\
&= -\sum_{i=1}^{K} N_{i-1}(\beta)\theta^{i-1}(a_{2K-i}) \\
&\quad -\sum_{i=1}^{K-1}\sum_{j=i}^{K-1}\Big(N_{2K-j-1}(\beta)\,\theta^{K-j-1}\left(\frac{N_i(\beta)}{N_{j+1}(\beta)}\right)\theta^{i+K-j-1}(a_{2K-i}) \\
&\qquad (\theta^{2K-j-1}(\beta)+\theta^{3K-j-1}(\alpha))\Big).
\end{aligned}
$$

As $\beta = -\theta^K(\alpha)$, we obtain $\theta^{2K-j-1}(\beta) + \theta^{3K-j-1}(\alpha) = 0$. Therefore

$$
\begin{aligned}
\sum_{j=0}^{K-1}\theta^{2K-1-j}(a_j)N_{2K-1-j}(\beta) &= -\sum_{i=1}^{K} N_{i-1}(\beta)\theta^{i-1}(a_{2K-i}) \\
&= -\sum_{j=K}^{2K-1}\theta^{2K-j-1}(a_j)N_{2K-j-1}(\beta).
\end{aligned}
$$

We conclude that $f^*(\beta) = 0$ and that $X+\alpha$ right-divides $\Theta^{k+\ell}(f^*)$. We deduce the existence of a skew polynomial Q such that $\Theta^{k+\ell}(f^*) = Q\cdot(X+\alpha)$ and we obtain $P = \Theta^{k-1-\ell}((X+\alpha)^*)\cdot Q\cdot(X+\alpha)$.

2. Let us prove that $Q = \Theta^{k+1+\ell}(Q^*)$. According to Lemma 1, as $\Theta^{k+\ell}(f^*) = Q\cdot(X+\alpha)$, we obtain $f = \Theta^{k-1-\ell}((X+\alpha)^*)\cdot\Theta^{k+1+\ell}(Q^*)$. Therefore $P = \Theta^{k-1-\ell}((X+\alpha)^*)\cdot Q\cdot(X+\alpha) = \Theta^{k-1-\ell}((X+\alpha)^*)\cdot\Theta^{k+1+\ell}(Q^*)\cdot(X+\alpha)$ and $Q = \Theta^{k+1+\ell}(Q^*)$.

□

We are now giving a construction and an enumeration formula for the sets $\tilde{\mathcal{H}}_{\mu,\epsilon}$ (Proposition 4 and Algorithm 1).

Proposition 4. *Consider $k\in\mathbb{N}^*$, $n=2k$, p a prime number, $\theta : x\mapsto x^p \in Aut(\mathbb{F}_{p^n})$, $R = \mathbb{F}_{p^n}[X;\theta]$, $\epsilon\in\{-1,1\}$, $\mu\in\mathbb{F}_{p^n}^*$ and $P_k = -\mu\epsilon(X^{2k}-\epsilon)\in R$. The set $\tilde{\mathcal{H}}_{\mu,\epsilon}$ is nonempty if and only if $\theta^k(\mu)+\epsilon\mu = 0$. In this case we have*

$$\tilde{\mathcal{H}}_{\mu,\epsilon} = \{(X+\alpha_1)\cdots(X+\alpha_k) \mid \begin{array}{l} X+\alpha_k \textit{ right-divides } P_k \\ X+\alpha_{k-1} \textit{ right-divides } P_{k-1}(\alpha_k) \\ \vdots \\ X+\alpha_1 \textit{ right-divides } P_1(\alpha_2,\ldots,\alpha_k)\} \end{array}$$

where for $i = k, k-1, \ldots, 2$, $P_{i-1}(\alpha_i,\ldots,\alpha_k)$ is the quotient in the left-division of Q_{i-1} by $\Theta^{i-1}((X+\alpha_i)^*)$ and Q_{i-1} the quotient in the right-division of $P_i(\alpha_{i+1},\ldots,\alpha_k)$ by $X+\alpha_i$:

$$P_i(\alpha_{i+1},\ldots,\alpha_k) = \underbrace{\Theta^{i-1}((X+\alpha_i)^*)\cdot P_{i-1}(\alpha_i,\ldots,\alpha_k)}_{Q_{i-1}}\cdot(X+\alpha_i). \tag{5}$$

Furthermore $\tilde{\mathcal{H}}_{\mu,\epsilon}$ has $\prod_{i=1}^{k}(p^i+1)$ elements.

Proof. Consider h in $\tilde{\mathcal{H}}_{\mu,\epsilon}$ and $\nu = h_0/\mu$ then $h^*\cdot\frac{1}{\nu}\cdot h = \theta^k(h_0)\cdot h^\natural\cdot\frac{1}{\nu}\cdot h = \theta^k(h_0)\cdot(X^n-\epsilon)\cdot\frac{1}{\theta^k(\nu)} = P_k$. Furthermore, $\Theta^k(P_k^*) = -(1-\epsilon X^n)\cdot(\epsilon\theta^k(\mu)) = (X^n-1)(-\epsilon\mu) = P_k$. As $X^n-\epsilon$ is central in R of degree one in $\mathbb{F}_p[X^n]$, the skew polynomial h is the product of k linear factors right-dividing $X^n-\epsilon$ and therefore $P_k : h = (X+\alpha_1)\cdots(X+\alpha_k)$. As the skew polynomial $X+\alpha_k$ right-divides P_k, according to Lemma 3 applied to $P = P_k$ and $\ell = 0$, there exists $P_{k-1}(\alpha_k) = P_{k-1} \in R$ such that

$$P_k = \Theta^{k-1}((X+\alpha_k)^*)\cdot P_{k-1}\cdot(X+\alpha_k)$$

and $\Theta^{k+1}(P_{k-1}^*) = P_{k-1}$. Consider $H = (X+\alpha_1)\cdots(X+\alpha_{k-1})$, according to Lemma 1, we have $h^* = \Theta^{k-1}((X+\alpha_k)^*)\cdot H^*$. We obtain

$$\Theta^{k-1}((X+\alpha_k)^*)\cdot P_{k-1}\cdot(X+\alpha_k) = \Theta^{k-1}((X+\alpha_k)^*)\cdot H^*\cdot\frac{1}{\nu}\cdot H\cdot(X+\alpha_k).$$

Therefore $P_{k-1} = H^*\cdot\frac{1}{\nu}\cdot H$ and $X+\alpha_{k-1}$ right-divides P_{k-1}. We conclude using an inductive argument and Lemma 3.

Conversely, consider $h = (X+\alpha_1)\cdots(X+\alpha_k)$ in R such that $X+\alpha_i$ right-divides $P_i(\alpha_{i+1},\ldots,\alpha_k)$ defined by (5). According to Lemma 3, $\Theta^{k+1}(P_{k-1}^*) = P_{k-1},\ldots,\Theta^{2k-1}(P_1^*) = P_1$; furthermore, as $X+\alpha_1$ right-divides P_1, there exist P_0 such that $P_1 = (X+\alpha_1)^*\cdot P_0\cdot(X+\alpha_1)$. According to Lemma 1, $h^* = \Theta^{k-1}((X+\alpha_k)^*)\cdots\Theta^0((X+\alpha_1)^*)$. Therefore, we obtain $h^*\cdot P_0\cdot h = P_k$. In particular, the constant term of both polynomials is $P_0h_0 = \mu$. Considering $\nu = h_0/\mu$, we obtain $h^*\cdot\frac{1}{\nu}\cdot h = -\epsilon\mu(X^n-\epsilon)$ and $h^\natural\cdot\frac{1}{\nu}\cdot h\cdot\theta^k(\nu) = -\frac{1}{\theta^k(h_0)}\epsilon\mu(X^n-\epsilon)\cdot\theta^k(\nu) = -\frac{1}{\theta^k(\mu)}\epsilon\mu(X^n-\epsilon) = X^n-\epsilon$.

Let us determine the cardinality of $\tilde{\mathcal{H}}_{\mu,\epsilon}$. According to Lemma 2, the number of factorizations (as a product of k linear monic factors) of any monic skew polynomial of degree k right-dividing $X^n-\epsilon$ in R is $\prod_{i=1}^{k}\frac{p^i-1}{p-1}$. Furthermore, as P_i has degree $2i$ and right-divides $X^n-\epsilon$, the number of $\alpha_i \in \mathbb{F}_q$ such that $X+\alpha_i$ right-divides P_i is $\frac{p^{2i}-1}{p-1}$. The number of elements of $\tilde{\mathcal{H}}_{\mu,\epsilon}$ is therefore

$$\frac{\prod_{i=1}^{k}\frac{p^{2i}-1}{p-1}}{\prod_{i=1}^{k}\frac{p^i-1}{p-1}} = \prod_{i=1}^{k}(p^i+1).$$

□

Example 4. *Consider $\mathbb{F}_{2^4} = \mathbb{F}_2(a)$ with $a^4+a+1=0$ and $n=4$. For $\mu \in \{1, a^5, a^{10}\}$, $\tilde{\mathcal{H}}_{\mu,1}$ has 15 elements :*

$\tilde{\mathcal{H}}_{1,1} = \{X^2+a^{14}\ X+a, X^2+a\ X+a^{14}, X^2+a^{11}\ X+a^4, X^2+a^2\ X+a^{13}, X^2+a^{13}\ X+a^2, X^2+a^4\ X+a^{11}, X^2+a^5\ X+a^{10}, X^2+1, X^2+a^8\ X+a^7, X^2+a^9, X^2+a^7\ X+a^8, X^2+a^{12}, X^2+a^3, X^2+a^6, X^2+a^{10}\ X+a^5\}$,

$\tilde{\mathcal{H}}_{a^5,1} = \{X^2+a^5\ X+a^5, X^2+a^{14}\ X+a^{11}, X^2+a^6\ X+a^4, X^2+a^8\ X+a^2, X^2+a^{11}\ X+a^{14}, X^2+X+a^{10}, X^2+a^2\ X+a^8, X^2+1, X^2+a^3\ X+a^7, X^2+a^9\ X+a, X^2+a^9, X^2+a^{12}\ X+a^{13}, X^2+a^{12}, X^2+a^3, X^2+a^6\}$,

Algorithm 1 Construction of the set $\tilde{\mathcal{H}}_{\mu,\epsilon}$

Require: : μ in $\mathbb{F}_{p^n}^*$ such that $\theta^k(\mu) + \epsilon\mu = 0$

Ensure: : $\tilde{\mathcal{H}}_{\mu,\epsilon}$

1: $P_k \leftarrow -\epsilon\mu(X^n - \epsilon)$

2: $S \leftarrow \emptyset$

3: Construct the sequences $(\alpha_i, P_{i-1})_{i=k,\ldots,1}$ such that

- $X + \alpha_i$ right-divides P_i;
- P_{i-1} is the quotient in the left-division of Q_{i-1} by $\Theta^{i-1}((X + \alpha_i)^*)$ where Q_{i-1} is the quotient in the right-division of P_i by $X + \alpha_i$.

4: **for** each sequence $(\alpha_1, \ldots, \alpha_k)$ **do**

5: $\quad S \leftarrow S \cup \{(X + \alpha_1) \cdots (X + \alpha_k)\}$

6: **end for**

7: **return** S

$\tilde{\mathcal{H}}_{a^{10},1} = \{X^2 + a^{10}\ X + a^{10}, X^2 + a^{13}\ X + a^7, X^2 + a^{12}\ X + a^8, X^2 + a^9\ X + a^{11}, X^2 + X + a^5, X^2 + a\ X + a^4, X^2 + 1, X^2 + a^6\ X + a^{14}, X^2 + a^3\ X + a^2, X^2 + a^9, X^2 + a^4\ X + a, X^2 + a^{12}, X^2 + a^7\ X + a^{13}, X^2 + a^3, X^2 + a^6\}$.

3.3 Enumeration of (θ, ν)-isodual and self-dual θ-cyclic and θ-negacyclic codes

From Proposition 4, we deduce the number of (θ, ϵ)-constacyclic codes of length $2k$ which are (θ, ν)-isodual. Let us first consider the particular case when $k = 1$:

Example 5. *Consider $k = 1, n = 2$. If $p = 2$ and $\nu \in \mathbb{F}_{2^2}^*$, then $\mathcal{H}_{\nu,\epsilon} = \{X + \alpha\}$ where $\alpha^2 = \nu$. If p is odd and $\nu^{\frac{p^2-1}{2}} = -\epsilon(-1)^{\frac{p-1}{2}}$, then $\mathcal{H}_{\nu,\epsilon} = \{X + \alpha \mid \alpha^2 = -\nu^{p-1}\}$. Namely, consider $h = X + \alpha \in R$, then*

$$\begin{aligned} h^\natural \cdot \nu \cdot h \cdot \tfrac{1}{\theta(\nu)} &= (X + \frac{1}{\theta(\alpha)}) \cdot (X + \frac{\nu\alpha}{\theta(\nu)}) \\ &= X^2 + \frac{\nu + \theta(\nu)\theta(\alpha^2)}{\theta(\alpha)\nu} X + \frac{\nu\alpha}{\theta(\nu\alpha)}. \end{aligned}$$

Therefore h belongs to $\mathcal{H}_{\nu,\epsilon}$ if and only if $\alpha^2 = -\theta(\nu)/\nu$.

Proposition 5. *Consider $k \in \mathbb{N}^*$, $n = 2k$, p a prime number, $\theta : x \mapsto x^p \in Aut(\mathbb{F}_{p^n})$, $\epsilon \in \{-1, 1\}$ and $\nu \in \mathbb{F}_{p^n}^*$. If $\nu^{\frac{p^n-1}{2}} = -\epsilon(-1)^{k\frac{p-1}{2}}$ then the number of (θ, ν)-isodual (θ, ϵ)-constacyclic codes of length n over $\mathbb{F}_{p^n}$ is*

$$N \prod_{i=1}^{k-1} (p^i + 1)$$

where $N = 1$ if $p = 2$ and $N = 2$ if p is odd.

Proof. We first prove that for ν in $\mathbb{F}_{p^n}^*$, if $\mathcal{H}_{\nu,\epsilon}$ is nonempty, then its cardinality does not depend on ν. Consider ν, ν' in $\mathbb{F}_{p^n}^*$ such that

$$\nu^{\frac{p^n-1}{N}} = (\nu')^{\frac{p^n-1}{N}} = -\epsilon(-1)^{k\frac{p-1}{N}}.$$

Then according to Proposition 3, $\mathcal{H}_{\nu,\epsilon}$ and $\mathcal{H}_{\nu',\epsilon}$ are nonempty. Consider $\xi = \frac{\nu}{\nu'}$ and a a square root of $\theta^k(\xi)$. As $\xi^{\frac{p^n-1}{N}} = 1$, a is well defined. The application

$$f : \left\{ \begin{array}{ccc} \mathcal{H}_{\nu,\epsilon} & \to & \mathcal{H}_{\nu',\epsilon} \\ h & \mapsto & \frac{1}{\theta^k(a)} \cdot h \cdot a \end{array} \right.$$

is also well defined : namely, consider for h in $\mathcal{H}_{\nu,\epsilon}$, $H = \frac{1}{\theta^k(a)} \cdot h \cdot a$, then $H^* = (h \cdot a)^* \cdot \frac{1}{\theta^k(a)} = \theta^k(a) \cdot h^* \cdot \frac{1}{\theta^k(a)}$. Therefore $H^\natural = \theta^k(\theta^k(a)/(h_0 a))\theta^k(a)\theta^k(h_0) \cdot h^\natural \cdot \frac{1}{\theta^k(a)} = a \cdot h^\natural \cdot \frac{1}{\theta^k(a)}$ and

$$H^\natural \cdot \frac{1}{\nu'} \cdot H \cdot \theta^k(\nu') = a \cdot h^\natural \cdot \frac{1}{\theta^k(a)} \cdot \frac{\xi}{\nu} \frac{1}{\theta^k(a)} \cdot h \cdot a \theta^k(\nu') = a \cdot h^\natural \cdot \frac{1}{\nu} \cdot h \cdot a \frac{\theta^k(\nu)}{\theta^k(\xi)} = a(X^n - \epsilon) \frac{a}{\theta^k(\xi)} = X^n - \epsilon.$$

Therefore H belongs to $\mathcal{H}_{\nu',\epsilon}$.

Consider H in $\mathcal{H}_{\nu',\epsilon}$ then $h = \theta^k(a) H \cdot \frac{1}{a}$ is the unique pre-image of H in $\mathcal{H}_{\nu,\epsilon}$. Therefore f is bijective and all nonempty sets $\mathcal{H}_{\nu,\epsilon}$ have the same number of elements, M : for all ν in $\mathbb{F}_{p^n}$ such that $\nu^{\frac{p^n-1}{N}} = -\epsilon(-1)^{k\frac{p-1}{N}}$, the number of (θ,ν)-isodual (θ,ϵ)-constacyclic codes of length $2k$ is M. Furthermore, we have

$$\forall h \in R, (\exists \mu \colon h \in \tilde{\mathcal{H}}_{\mu,\epsilon} \Leftrightarrow \exists \mu \colon h \in \mathcal{H}_{h_0\mu,\epsilon} \Leftrightarrow \exists \nu \colon h \in \mathcal{H}_{\nu,\epsilon}). \tag{6}$$

Therefore

$$\cup_\mu \tilde{\mathcal{H}}_{\mu,\epsilon} = \cup_\nu \mathcal{H}_{\nu,\epsilon}.$$

Now consider the union of the intersections $\tilde{\mathcal{H}}_{\mu,\epsilon} \cap \tilde{\mathcal{H}}_{\mu',\epsilon}$ for $\mu \neq \mu'$ and $\tilde{\mathcal{H}}_{\mu,\epsilon}, \tilde{\mathcal{H}}_{\mu',\epsilon}$ nonempty. We have, according to (6) :

$$\bigcup_{\mu \neq \mu'} (\tilde{\mathcal{H}}_{\mu,\epsilon} \cap \tilde{\mathcal{H}}_{\mu',\epsilon}) = \bigcup_{\nu \neq \nu'} (\mathcal{H}_{\nu,\epsilon} \cap \mathcal{H}_{\nu',\epsilon}).$$

Similarly, we get

$$\bigcup_{\mu \neq \mu' \neq \mu''} (\tilde{\mathcal{H}}_{\mu,\epsilon} \cap \tilde{\mathcal{H}}_{\mu',\epsilon} \cap \tilde{\mathcal{H}}_{\mu'',\epsilon}) = \bigcup_{\nu \neq \nu' \neq \nu''} (\mathcal{H}_{\nu,\epsilon} \cap \mathcal{H}_{\nu',\epsilon} \cap \mathcal{H}_{\nu'',\epsilon}) \dots$$

$$\vdots$$

where the involved sets $\mathcal{H}_{\nu,\epsilon}$ and $\tilde{\mathcal{H}}_{\mu,\epsilon}$ are nonempty. Furthermore, $\#(\cup_\mu \tilde{\mathcal{H}}_{\mu,\epsilon}) = \sum_\mu \#\tilde{\mathcal{H}}_{\mu,\epsilon} - \sum_{\mu \neq \mu'} \#(\tilde{\mathcal{H}}_{\mu,\epsilon} \cap \tilde{\mathcal{H}}_{\mu',\epsilon}) + \sum_{\mu \neq \mu' \neq \mu''} \#(\tilde{\mathcal{H}}_{\mu,\epsilon} \cap \tilde{\mathcal{H}}_{\mu',\epsilon} \cap \tilde{\mathcal{H}}_{\mu'',\epsilon}) - \cdots$ and $\#(\cup_\nu \mathcal{H}_{\nu,\epsilon}) = \sum_\nu \#\mathcal{H}_{\nu,\epsilon} - \sum_{\nu \neq \nu'} \#(\mathcal{H}_{\nu,\epsilon} \cap \mathcal{H}_{\nu',\epsilon}) + \sum_{\nu \neq \nu' \neq \nu''} \#(\mathcal{H}_{\nu,\epsilon} \cap \mathcal{H}_{\nu',\epsilon} \cap \mathcal{H}_{\nu'',\epsilon}) - \cdots$. Therefore

$$\sum_\mu \#\tilde{\mathcal{H}}_{\mu,\epsilon} = \sum_\nu \#\mathcal{H}_{\nu,\epsilon}.$$

Lastly, according to Proposition 4, the $p^k - 1$ nonempty sets $\tilde{\mathcal{H}}_{\mu,\epsilon}$ all have $\prod_{i=1}^k (1+p^i)$ elements. As the $\frac{p^{2k}-1}{N}$ nonempty sets $\mathcal{H}_{\nu,\epsilon}$ all have M elements, we obtain

$$\prod_{i=1}^k (1+p^i)\,(p^k-1) = M\,\frac{p^{2k}-1}{N}.$$

□

Example 6. *Consider the (θ,ν)-isodual θ-cyclic codes of length 4 over $\mathbb{F}_{2^4} = \mathbb{F}_2(a)$ where $a^4 + a + 1 = 0$. For $\mu \in \{1, a^5, a^{10}\}$, $\tilde{\mathcal{H}}_{\mu,1}$ has 15 elements (Example 4) and $\bigcup \tilde{\mathcal{H}}_{\mu,1} = \bigcup \mathcal{H}_{\nu,\epsilon}$ has 35 elements. For $\nu \in \mathbb{F}_{2^4}^*$, $\mathcal{H}_{\nu,\epsilon}$ has 3 elements : there are 3 (θ,ν)-isodual θ-cyclic codes :*

$\mathcal{H}_{1,1} = \{X^2+1, X^2+a^{10}\ X+a^{10}, X^2+a^5\ X+a^5\}$, $\mathcal{H}_{a^{14},1} = \{X^2+a\ X+a^{14}, X^2+a^9, X^2+a^6\ X+a^4\}$, $\mathcal{H}_{a^{13},1} = \{X^2+a^2\ X+a^{13}, X^2+a^{12}\ X+a^8, X^2+a^3\}$, $\mathcal{H}_{a^{12},1} = \{X^2+a^8\ X+a^2, X^2+a^{13}\ X+a^7, X^2+a^{12}\}$, $\mathcal{H}_{a^{11},1} = \{X^2+a^9\ X+a, X^2+a^6, X^2+a^4\ X+a^{11}\}$, $\mathcal{H}_{a^{10},1} = \{X^2+1, X^2+X+a^5, X^2+a^5\ X+a^{10}\}$, $\mathcal{H}_{a^9,1} = \{X^2+a\ X+a^4, X^2+a^{11}\ X+a^{14}, X^2+a^9\}$,

$\mathcal{H}_{a^8,1} = \{X^2 + a^7\ X + a^8, X^2 + a^{12}\ X + a^{13}, X^2 + a^3\}$, $\mathcal{H}_{a^7,1} = \{X^2 + a^8\ X + a^7, X^2 + a^{12}, X^2 + a^3\ X + a^2\}$, $\mathcal{H}_{a^6,1} = \{X^2 + a^{14}\ X + a^{11}, X^2 + a^4\ X + a, X^2 + a^6\}$, $\mathcal{H}_{a^5,1} = \{X^2 + 1, X^2 + X + a^{10}, X^2 + a^{10}\ X + a^5\}$, $\mathcal{H}_{a^4,1} = \{X^2 + a^{11}\ X + a^4, X^2 + a^9, X^2 + a^6\ X + a^{14}\}$, $\mathcal{H}_{a^3,1} = \{X^2 + a^2\ X + a^8, X^2 + a^7\ X + a^{13}, X^2 + a^3\}$, $\mathcal{H}_{a^2,1} = \{X^2 + a^3\ X + a^7, X^2 + a^{13}\ X + a^2, X^2 + a^{12}\}$, $\mathcal{H}_{a,1} = \{X^2 + a^{14}\ X + a, X^2 + a^9\ X + a^{11}, X^2 + a^6\}$.

We check that

$$\bigcup_{\mu \neq \mu'} (\tilde{\mathcal{H}}_{\mu,1} \cap \tilde{\mathcal{H}}_{\mu',1}) = \bigcup_{\nu \neq \nu'} (\mathcal{H}_{\nu,\epsilon} \cap \mathcal{H}_{\nu',\epsilon}) = \{X^2 + 1, X^2 + a^9, X^2 + a^3, X^2 + a^{12}, X^2 + a^6\},$$

$$\tilde{\mathcal{H}}_{1,1} \cap \tilde{\mathcal{H}}_{a^5,1} \cap \tilde{\mathcal{H}}_{a^{10},1} = \bigcup_{\nu \neq \nu' \neq \nu''} (\mathcal{H}_{\nu,\epsilon} \cap \mathcal{H}_{\nu',\epsilon} \cap \mathcal{H}_{\nu'',\epsilon}) = \{X^2 + 1, X^2 + a^9, X^2 + a^3, X^2 + a^{12}, X^2 + a^6\},$$

$$\emptyset = \bigcup_{\nu \neq \nu' \neq \nu'' \neq \nu'''} (\mathcal{H}_{\nu,\epsilon} \cap \mathcal{H}_{\nu',\epsilon} \cap \mathcal{H}_{\nu'',\epsilon} \cap \mathcal{H}_{\nu''',\epsilon}).$$

In [5], a formula for the number of self-dual (θ, ϵ)-constacyclic codes of length n is given over $\mathbb{F}_{p^2} \subset \mathbb{F}_{p^n}$ when $\epsilon^2 = 1$. In what follows, we deduce from Proposition 5 the number of self-dual (θ, ϵ)-constacyclic codes of length n over $\mathbb{F}_{p^n}$.

Proposition 6. *Consider $k \in \mathbb{N}^*$, $n = 2k$, $\epsilon \in \{-1, 1\}$, p a prime number and $\theta : x \mapsto x^p \in Aut(\mathbb{F}_{p^n})$. If $p = 2$, there are $\prod_{i=1}^{k-1}(p^i + 1)$ self-dual θ-cyclic codes of length n over $\mathbb{F}_{p^n}$. If $p \neq 2$, and if $(-1)^{k\frac{p-1}{2}}\epsilon = -1$, there are $2\prod_{i=1}^{k-1}(p^i + 1)$ self-dual (θ, ϵ)-constacyclic codes of length n over $\mathbb{F}_{p^n}$.*

Proof. Self-dual (θ, ϵ)-constacyclic codes are $(\theta, 1)$-isodual (θ, ϵ)-constacyclic codes. The result follows from Proposition 5. □

Algorithm 2 (θ, ν)-isodual (θ, ϵ)-constacyclic codes of length n over $\mathbb{F}_{p^n}$

Require: : $k \in \mathbb{N}^*$, $n = 2k$, p, prime number, $\epsilon \in \{-1, 1\}$, $\nu \in \mathbb{F}_{p^n}^*$

Ensure: : $\mathcal{H}_{\nu,\epsilon}$: the set of the skew check polynomials h of (θ, ν)-isodual (θ, ϵ)-constacyclic codes of length n and dimension k over $\mathbb{F}_{p^n}$.

1: $S \leftarrow \emptyset$
2: **for** μ in $\mathbb{F}_{p^n}^*$ such that $\theta^k(\mu) + \epsilon\mu = 0$ **do**
3: $P_k \leftarrow -\epsilon\mu(X^n - \epsilon)$
4: Construct the sequences (α_i, P_{i-1}) for $i = k, \ldots, 1$ such that

- $X + \alpha_i$ right-divides P_i;
- P_{i-1} is the quotient in the left-division of Q_{i-1} by $\Theta^{i-1}((X + \alpha_i)^*)$ where Q_{i-1} is the quotient in the right-division of P_i by $X + \alpha_i$;
- $P_0 = \mu / \prod_{i=1}^{k} \alpha_i = \nu$.

5: **for** each $(\alpha_1, \ldots, \alpha_k)$ **do**
6: $S \leftarrow S \cup \{(X + \alpha_1) \cdots (X + \alpha_k)\}$
7: **end for**
8: **end for**
9: **return** S

Example 7. *There are 3 self-dual θ-cyclic codes of length 4 over $\mathbb{F}_{2^4}$, given in Example 6 by $\mathcal{H}_{1,1}$. There are 15 self-dual θ-cyclic codes of length 6 over $\mathbb{F}_{2^6} = \mathbb{F}_2(a)$ where $a^6 + a^4 + a^3 + a + 1 = 0$. Their skew check polynomials are : $X^3 + a^{52}X^2 + a^{23}X + a^{54}$, $X^3 + X^2 + a^9X + a^{36}$, $X^3 + a^{36}\ X^2 + a^{36}\ X + a^{45}$, $X^3 + 1$, $X^3 + a^{19}\ X^2 + a^{29}\ X + a^{27}$, $X^3 + a^{41}\ X^2 + a^{46}\ X + a^{45}$, $X^3 + a^{18}\ X^2 + a^{18}\ X + a^{54}$, $X^3 + a^{21}\ X^2 + a^{42}\ X + 1$, $X^3 + a^{26}\ X^2 + a^{43}\ X + a^{27}$, $X^3 + a^9\ X^2 + a^9\ X + a^{27}$, $X^3 + a^{42}\ X^2 + a^{21}\ X + 1$, $X^3 + a^{13}\ X^2 + a^{53}\ X + a^{45}$, $X^3 + a^{38}\ X^2 + a^{58}\ X + a^{54}$, $X^3 + X^2 + a^{18}\ X + a^9$ and $X^3 + X^2 + a^{36}\ X + a^{18}$.*

4 A construction of self-dual θ-cyclic codes over $\mathbb{F}_{p^n}$ which are Gabidulin evaluation codes

We consider here a special subfamily of self-dual θ-cyclic codes of length n over $\mathbb{F}_{p^n}$ which are in fact Gabidulin evaluation codes and therefore Maximum Rank Distance (MRD) codes (see [12] for the theory of MRD codes). In previous sections we have provided a construction of self-dual codes based on the factorization of the skew check polynomials into the product of linear skew polynomials. Here we change the point of view by writting the skew generator polynomials as least common left multiples (lclm) of special linear skew polynomials, namely skew polynomials of the form $X - \theta^i(\alpha)$.

Definition 3. *[12] Consider $k \leq n \in \mathbb{N}^*$, p a prime number, $\theta : x \mapsto x^p \in Aut(\mathbb{F}_{p^n})$, $y_1, \ldots, y_n \in \mathbb{F}_{p^n}$ linearly independent over $\mathbb{F}_p$. The* Gabidulin evaluation code *of length n, dimension k and support $(y_1, \ldots, y_n)$ is the code with generator matrix*

$$G = \begin{pmatrix} y_1 & y_1 & \ldots & y_n \\ \theta(y_1) & \theta(y_2) & \ldots & \theta(y_n) \\ \vdots & & & \\ \theta^{k-1}(y_1) & \theta^{k-1}(y_2) & \ldots & \theta^{k-1}(y_n) \end{pmatrix}. \tag{7}$$

The following Proposition 7 can be found in [9] (Proposition 3, part 1).

Proposition 7 (Proposition 3 of [9])**.** *Consider $k \leq n \in \mathbb{N}^*$, p a prime number, $\theta : x \mapsto x^p \in Aut(\mathbb{F}_{p^n})$, $R = \mathbb{F}_{p^n}[X;\theta]$, $\alpha \in \mathbb{F}_{p^n}$, $\epsilon = N_n(\alpha)$. Assume that $\epsilon^2 = 1$ and that $1, \alpha, N_2(\alpha), \ldots, N_{n-1}(\alpha)$ are linearly independent over $\mathbb{F}_p$. The θ-cyclic code of length n and skew generator polynomial $g = \mathrm{lclm}_{0 \leq i \leq k-1}(X - \theta^i(\alpha))$ is the dual of the Gabidulin evaluation code of length n, dimension k and support $(1, \alpha, N_2(\alpha), \ldots, N_{n-1}(\alpha))$.*

Proof. Consider $c = (c_0, \ldots, c_{n-1}) \in \mathbb{F}_{p^n}^n$. The word c belongs to the θ-cyclic code generated by g if and only if for all i in $\{0, \ldots, k-1\}$, $X - \theta^i(\alpha)$ right-divides g. As the remainder in the right division of c by $X - \theta^i(\alpha)$ is $\sum_{j=0}^{n-1} c_j N_j(\theta^i(\alpha)) = \sum_{j=0}^{n-1} c_j \theta^i(N_j(\alpha))$, we obtain that a check matrix for the code is the matrix G given by (7) where $y_1 = 1, y_2 = \alpha, \ldots, y_n = N_{n-1}(\alpha)$. □

According to Theorem 4.10 of [15], if a Gabidulin evaluation code of length $2k$ and dimension k is self-dual then $p \equiv 3 \pmod 4$ and k is odd. In what follows we construct a family of self-dual Gabidulin evaluation codes parameterized by an element α of $\mathbb{F}_{p^n}$.

Proposition 8. *Consider $k \in \mathbb{N}^*$, $n = 2k$, p a prime number, $\theta : x \mapsto x^p \in Aut(\mathbb{F}_{p^n})$, $R = \mathbb{F}_{p^n}[X;\theta]$, $\alpha \in \mathbb{F}_{p^n}$ such that $N_n(\alpha) = 1$ and $1, \alpha, N_2(\alpha), \ldots, N_{n-1}(\alpha)$ are linearly independent over $\mathbb{F}_p$. The θ-cyclic code of length n and skew generator polynomial $g = \mathrm{lclm}_{0 \leq i \leq k-1}(X - \theta^i(\alpha))$ is self-dual if and only if $\sum_{i=0}^{n-1} N_i(\alpha)^{1+p^\ell} = 0, \forall \ell \in \{0, \ldots, k-1\}$.*

Proof. The code is self-dual if and only if the lines of G are pairwise orthogonal i.e. $G\,G^T = 0$ where G is the matrix defined by (7) with $y_1 = 1, y_2 = \alpha, \ldots, y_n = N_{n-1}(\alpha)$. □

Example 8. *For $p = 3$ and $k = 3$, according to Proposition 5, there are 80 self-dual θ-cyclic codes of length 6 over $\mathbb{F}_{3^3}$. The polynomial system*

$$\begin{cases} \sum_{i=0}^{6} N_i(\alpha)^2 = 0 \\ \sum_{i=0}^{6} N_i(\alpha)^4 = 0 \\ \sum_{i=0}^{6} N_i(\alpha)^{10} = 0 \end{cases}$$

has 18 solutions α : $a^{580}, a^{406}, a^{378}, a^{436}, a^{124}, a^8, a^{648}, a^{126}, a^{388}, a^{216}, a^{42}, a^{72}, a^{14}, a^{284}, a^{24}, a^{372}, a^{488}, a^{490}$ and we get 18 self-dual θ-cyclic codes generated by the skew polynomials $g = \mathrm{lclm}(X - \alpha, X - \theta(\alpha), X - \theta^2(\alpha))$. These codes are self-dual Gabidulin evaluation codes (and therefore self-dual MRD codes). For example, take $\alpha = a^8$, then $g = \mathrm{lclm}(X - a, X - \theta(a), X - \theta^2(a)) = X^3 + a^{185}X^2 + a^{383}X + a^{322}$ generates a self-dual θ-cyclic code of length 6 which is the Gabidulin evaluation code of dimension 3 and support $(1, a, \ldots, N_5(a)) = (1, a^8, a^{32}, a^{104}, a^{320}, a^{240})$.

An open question is to determine the number of self-dual θ-cyclic codes generated by $g = \mathrm{lclm}_{0\leq i\leq k-1}(X-\theta^i(\alpha))$ over $\mathbb{F}_{p^n}$ with $n = 2k$. More generally, it could be interesting to construct and count self-dual θ-cyclic codes which are MRD.

5 Conclusion

This note was devoted to the construction of self-dual θ-constacyclic codes of length n over $\mathbb{F}_{p^m}$ when m is equal to n and θ is the Frobenius automorphism over $\mathbb{F}_{p^n}$. This work completes previous works on self-dual θ-constacyclic codes over $\mathbb{F}_{p^m}$ when $m = 1$ (then θ is the identity and codes are classical constacyclic codes) and when $m = 2$. As a further work, it could be interesting to study the cases when $2 < m < n$ and to have a more general classification only based on the order of the automorphism θ in $Aut(\mathbb{F}_{p^n})$.

References

[1] A. Alahmadia, S. Alsulami, R. Hijazi, P. Solé, Isodual cyclic codes over finite fields of odd characteristic, *Discrete Mathematics*, **339** (2016), 344–353.

[2] A. Batoul, K. Guenda and T. A. Gulliver, Repeated-root isodual cyclic codes over finite fields, *Codes, cryptology, and information security*, Lecture Notes in Comput. Sci., **9084** (2015), 119–132.

[3] A. Batoul, K. Guenda, A. Kaya and B. Yildiz, Cyclic Isodual and Formally Self-dual Codes over $\mathbb{F}_q + v\mathbb{F}_q$, *European Journal of Pure and Applied Mathematics*, **8** (2015), 64–80.

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

[5] D. Boucher, Construction and number of self-dual skew codes over $\mathbb{F}_{p^2}$, *Advances in Mathematics of Communications (AMC)*, **10**, no. 4 (2016), 765–795.

[6] D. Boucher, Autour de codes définis à l'aide de polynômes tordus, *HDR Université Rennes 1* (2 juin 2020).

[7] D. Boucher and F. Ulmer, Codes as modules over skew polynomial rings, *Cryptography and coding. Springer, Berlin*, **5921** (2009), 38-55.

[8] D. Boucher and F. Ulmer, A note on the dual codes of module skew codes, *Lecture Notes in Comput. Sci.*, **7089** (2011), 230–243.

[9] D. Boucher and F. Ulmer, Linear codes using skew polynomials with automorphisms and derivations, *Designs, Codes and Cryptography*, , **70**, (2014), 405–431.

[10] X. Caruso and J.L. Le Borgne, A new faster algorithm for factoring skew polynomials over finite fields, *Journal of Symbolic Computation*, **79** (2017), 411-443.

[11] J. Delenclos and A. Leroy, Noncommutative symmetric functions and W-polynomials, *Journal of Algebra and its Applications*, **6** (2007), 815–837.

[12] È. M. Gabidulin, Theory of codes with maximum rank distance, *Problemy Peredachi Informatsii, Akademiya Nauk SSSR. Institut Problem Peredachi Informatsii Akademii Nauk SSSR. Problemy Peredachi Informatsii*, **21**, (1985), 1, 3–16

[13] N. Jacobson, The Theory of Rings, *American Mathematical Society Mathematical Surveys*, vol. II (1943), vi+150.

[14] T. Y. Lam and A. Leroy, Vandermonde and Wronskian matrices over division rings, *Bull. Soc. Math. Belg. Sér. A*, **40** (1988), 2, 281–286.

[15] G. Nebe and W. Willems, On self-dual MRD codes, *Advances in Mathematics of Communications*, **10** (2016), 3, 633–642.

[16] O. Ore, Theory of non-commutative polynomials, *Annals Math*, **34** (1933), 480–508.

[17] Rains, Eric M. and Sloane, N. J. A., Self-dual codes, Handbook of coding theory, Vol. I, II, 177–294, 1998