A Note on the Existence of Self-Dual Skew Codes over Finite Fields

Delphine Boucher

A note on the existence of self-dual skew codes over finite fields

D. Boucher *

May 7, 2015

Abstract

Conditions on the existence of self-dual θ-codes defined over a finite field $\mathbb{F}_q$ are studied for θ automorphism of $\mathbb{F}_q$. When $q \equiv 1 \pmod 4$ it is proven that there always exists a self-dual θ-code in any dimension and that self-dual θ-codes of a given dimension are either all θ-cyclic or all θ-negacyclic. When $q \equiv 3 \pmod 4$, there does not exist a self-dual θ-cyclic code and a necessary and sufficient condition for the existence of self-dual θ-negacyclic codes is given.

1 Introduction

Conditions for the existence of self-dual cyclic and negacyclic codes have been widely studied ([4], [6]) as well as for quasi-cyclic codes ([11], [12], [7]). In [3] a formula for the number of self-dual θ-cyclic codes and self-dual θ-negacyclic codes is given over $\mathbb{F}_{p^2}$ where p is a prime number and θ is the Frobenius automorphism. The aim of this text is to give conditions for the existence of self-dual θ-cyclic codes and θ-negacyclic codes over any finite field $\mathbb{F}_q$ where θ is an automorphism of $\mathbb{F}_q$.

The text is organized as follows. In Section 2, some facts about self-dual skew codes are recalled. In Section 3, the question of the existence of self-dual skew codes generated by skew binomials (Proposition 1) is studied. One deduces from this part that for $q \equiv 1 \pmod 4$ there always exists a self-dual skew code in any dimension. In Section 4, a construction of self-dual skew codes over $\mathbb{F}_q$ using least common right multiples of skew polynomials and generalizing Proposition 28 of [2] is considered (Proposition 2). This proposition is used in Section 5 when $q \equiv 3 \pmod 4$ to prove that there does not exist a self-dual θ-cyclic code in any dimension and to give a necessary and sufficient condition for the existence of self-dual θ-negacyclic codes (Proposition 4). Lastly when $q \equiv 1 \pmod 4$, one proves that the sufficient conditions of existence of self-dual θ-cyclic and θ-negacyclic codes given by Proposition 1 are also necessary (Proposition 5). The results of Proposition 4 and Proposition 5 are summed up in Table 1.

2 Generalities on self-dual skew codes

For a finite field $\mathbb{F}_q$ and θ an automorphism of $\mathbb{F}_q$ the ring R is defined by $R = \mathbb{F}_q[X;\theta] = \{a_n X^n + \ldots + a_1 X + a_0 \,|\, a_i \in \mathbb{F}_q \text{ and } n \in \mathbb{N}\}$ where addition is defined to be the usual addition of polynomials and where multiplication is defined by the basic rule $X \cdot a = \theta(a)\, X$

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

($a \in \mathbb{F}_q$) and extended to all elements of R by associativity and distributivity. The noncommutative ring R is called a **skew polynomial ring** or Ore ring (cf. [13]) and its elements are **skew polynomials**. It is a left and right Euclidean ring whose left and right ideals are principal. Left and right gcd and lcm exist in R and can be computed using the left and right Euclidean algorithm. Recall that the center of R is the commutative polynomial ring $Z(R) = \mathbb{F}_q^\theta[X^{|\theta|}]$ where $\mathbb{F}_q^\theta$ is the fixed field of θ and $|\theta|$ is the order of θ. Below, module θ-codes are defined using the skew polynomial ring R.

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

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

Definition 2 ([1], Definition 3) *The* **skew reciprocal polynomial** *of $h = \sum_{i=0}^{m} h_i\, X^i \in R$ of degree m is $h^* = \sum_{i=0}^{m} X^{m-i} \cdot h_i = \sum_{i=0}^{m} \theta^i(h_{m-i})\, X^i$. The* **left monic skew reciprocal polynomial** *of h is $h^\natural := \frac{1}{\theta^m(h_0)} \cdot h^*$.*

Since θ is an automorphism, the map $*\colon R \to R$ given by $h \mapsto h^*$ is a bijection. In particular for any $g \in R$ there exists a unique $h \in R$ such that $g = h^*$ and, if g is monic, there exists a unique $h \in R$ such that $g = h^\natural$.

In order to describe some properties of the skew reciprocal polynomial, the morphism of rings $\Theta\colon R \to R$ given by $\sum_{i=0}^{n} a_i X^i \mapsto \sum_{i=0}^{n} \theta(a_i) X^i$ ([1], Lemma 1) is useful:

Lemma 1 (see also Lemma 1 of [1]) *Let f and g be skew polynomials in R and $n = \deg(f)$. Then*

1. $(fg)^* = \Theta^n(g^*) f^*$.
2. $(f^*)^* = \Theta^n(f)$.

According to Proposition 5 of [2], a self-dual θ-code must be either θ-cyclic or θ-negacyclic. Furthermore, according to Corollary 1 of [2], a module θ-code with skew generator polynomial $g \in \mathbb{F}_q[X;\theta]$ of degree k is self-dual if and only if there exists $h \in R$ (called **skew check polynomial** of the code) such that $g = h^\natural$ and

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

Self-dual cyclic codes exist over $\mathbb{F}_q$ if and only if the characteristic of q is 2 (Theorem 3.3 of [9] or Theorem 1 of [8]). Necessary and sufficient conditions for the existence of self-dual

negacyclic codes are given in [6] when $q \equiv 1 \pmod 4$ and in [4] when the dimension is a power of the characteristic of $\mathbb{F}_q$.

According to Theorem 18 of [14], a θ-cyclic code of length n is equivalent to a quasi-cyclic code of index ℓ where $\ell = \gcd(|\theta|, n)$. Therefore, as equivalence preserves self-duality, if there exists a self-dual θ-cyclic code of length n then there exists a self-dual quasi-cyclic code of length n and index $\ell = \gcd(|\theta|, n)$. According to Lemma 2.1 of [7], for m coprime with q, self-dual quasi-cyclic codes of index ℓ with length ℓm exist over a finite field $\mathbb{F}_q$ if and only if q is of characteristic 2 and $2|\ell$ or $q \equiv 1 \pmod 4$ and $2|\ell$ or $q \equiv 3 \pmod 4$ and $4|\ell$. Therefore, if there exists a self-dual θ-cyclic code over $\mathbb{F}_q$ with $n/\gcd(|\theta|, n)$ coprime with q, then $\gcd(|\theta|, n)$ must be even if q is a power of 2 or $q \equiv 1 \pmod 4$ and it must be divisible by 4 if $q \equiv 3 \pmod 4$. If the characteristic of $\mathbb{F}_q$ is equal to 2, then for all nonnegative integer k there exists a self-dual θ-code of length $2k$. Namely, the code $(X^k + 1)^\theta_{2k}$ is such a code as the relation (1) is satisfied for $h = X^k + 1$:

$$(X^k + 1)^\natural (X^k + 1) = (X^k + 1)(X^k + 1) = X^{2k} + 1.$$

In next section, necessary and sufficient conditions for the existence of self-dual codes generated by skew binomials are given when *the characteristic of* $\mathbb{F}_q$ *is odd.*

3 Self-dual skew codes generated by skew binomials

Over a finite field of odd characteristic, there is no self-dual cyclic code ([8]). The example below shows that it is not the case for θ-cyclic codes when θ is not the identity.

Example 1 *Consider* $\mathbb{F}_{3^2} = \mathbb{F}_3(a)$ *with* $a^2 - a - 1 = 0$, $\alpha = a^2$ *and* $\theta : x \mapsto x^3$. *The skew polynomial* $X + \alpha \in \mathbb{F}_{3^2}[X; \theta]$ *is the skew check polynomial of a self-dual* θ*-cyclic code :* $(X + \alpha)^\natural = \frac{1}{\alpha^3}(1 + \alpha^3 X) = X + \alpha$ *and*

$$\begin{aligned} (X + \alpha)^\natural (X + \alpha) &= (X + \alpha)(X + \alpha) \\ &= X^2 + (\alpha + \alpha^3)X + \alpha^2 \\ &= X^2 - 1. \end{aligned}$$

According to Section VI A of [11], this code is, up to equivalence, the unique self-dual code of length 2 *over* $\mathbb{F}_{3^2}$, *its generator matrix is* $(1, \alpha)$.

The following proposition gives a necessary and sufficient condition for the existence of self-dual θ-cyclic codes and self-dual θ-negacyclic codes defined over finite fields of odd characteristic and generated by skew binomials.

Proposition 1 *Assume that* $\mathbb{F}_q$ *is a finite field with* $q = p^e$, p *odd prime number,* $e \in \mathbb{N}^*$. *Consider* $r \in \mathbb{N}$, θ *the automorphism of* $\mathbb{F}_q$ *defined by* $\theta : x \mapsto x^{p^r}$ *and* k *a nonnegative integer.*

1. *There exists a self-dual* θ*-cyclic code over* $\mathbb{F}_q$ *of dimension* k *generated by a skew binomial if and only if* $p \equiv 3 \pmod 4$, e *is even and* $r \times k$ *is odd.*

2. *There exists a self-dual* θ*-negacyclic code over* $\mathbb{F}_q$ *of dimension* k *generated by a skew binomial if and only if* $p \equiv 1 \pmod 4$ *or* $p \equiv 3 \pmod 4$, e *is even and* $r \times k$ *is even.*

Proof.

- Consider $h = X^k + \alpha \in R = \mathbb{F}_q[X;\theta]$ and $\epsilon = \pm 1$. The skew binomial h is the skew reciprocal polynomial of a self-dual (θ, ϵ)-constacyclic code if, and only if, h satisfies the relation (1) i.e.
$$\left(X^k + \frac{1}{\theta^k(\alpha)}\right) \cdot \left(X^k + \alpha\right) = X^{2k} - \epsilon.$$
Developping this skew polynomial relation, one gets the equivalent conditions
$$\theta^k(\alpha) + \epsilon\alpha = \alpha^2 + 1 = 0.$$

- One then proves that there exists $\alpha \in \mathbb{F}_q$ such that $\theta^k(\alpha) + \alpha = \alpha^2 + 1 = 0$ if and only if $p \equiv 3 \pmod 4$, e is even, r and k are odd.

  Let us assume that $p \equiv 3 \pmod 4$, $e \equiv 0 \pmod 2$ and $r, k \equiv 1 \pmod 2$. Then -1 is a square in $\mathbb{F}_q$ and one can consider $\alpha \in \mathbb{F}_q$ such that $\alpha^2 = -1$. As r and k are odd, $p^{kr} \equiv 3 \pmod 4$ so $p^{kr} - 1 \equiv 2 \pmod 4$ and $\frac{p^{kr}-1}{2} \equiv 1 \pmod 2$. Therefore $\alpha^{p^{kr}-1} = (\alpha^2)^{\frac{p^{kr}-1}{2}} = (-1)^{\frac{p^{kr}-1}{2}} = -1$ i.e. $\theta^k(\alpha) + \alpha = 0$.

  Conversely, consider α in $\mathbb{F}_q$ such that $\theta^k(\alpha) + \alpha = \alpha^2 + 1 = 0$. Assume that $p \equiv 1 \pmod 4$ then -1 is a square in $\mathbb{F}_p$ so α belongs to $\mathbb{F}_p$ and α is left fixed by θ. The equality $\theta^k(\alpha) + \alpha = 0$ implies that $2\alpha = 0$, which is impossible as p is odd. Therefore $p \equiv 3 \pmod 4$ and as -1 is a square in $\mathbb{F}_q$, e must be even. As $\theta^k(\alpha) + \alpha = 0 = \alpha^2 + 1$, one gets $-1 = \alpha^{p^{kr}-1} = (\alpha^2)^{\frac{p^{kr}-1}{2}} = (-1)^{\frac{p^{kr}-1}{2}}$ so $\frac{p^{kr}-1}{2}$ is odd, and $p^{kr} - 1 \equiv 2 \pmod 4$. As $p \equiv 3 \pmod 4$, kr must be odd.

- Lastly one proves that there exists $\alpha \in \mathbb{F}_q$ such that $\theta^k(\alpha) - \alpha = \alpha^2 + 1 = 0$ if and only if $p \equiv 1 \pmod 4$ or ($p \equiv 3 \pmod 4$, e and $r \times k$ are even).

  First if $p \equiv 1 \pmod 4$ then -1 is a square in $\mathbb{F}_p$. Consider α in $\mathbb{F}_p$ such that $\alpha^2 = -1$, then $\theta^k(\alpha) - \alpha = 0$ because $\alpha \in \mathbb{F}_p$ is left fixed by θ. If $p \equiv 3 \pmod 4$, $e \equiv 0 \pmod 2$ and $rk \equiv 0 \pmod 2$, then -1 has a square root in $\mathbb{F}_q$ and $p^{kr} - 1 \equiv 0 \pmod 4$. Consider $\alpha \in \mathbb{F}_q$ such that $\alpha^2 = -1$. Then $\alpha^{p^{kr}-1} = (\alpha^2)^{\frac{p^{kr}-1}{2}} = 1$ because $\alpha^2 = -1$ and $(p^{kr} - 1)/2$ is even.

  Conversely, consider $\alpha \in \mathbb{F}_q$ such that $\theta^k(\alpha) - \alpha = \alpha^2 + 1 = 0$. Therefore -1 is a square in $\mathbb{F}_q$ and either $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$ and $e \equiv 0 \pmod 2$. If $p \equiv 3 \pmod 4$ and $rk \equiv 1 \pmod 2$ then $p^{kr} - 1 \equiv 2 \pmod 4$ so $(p^{kr} - 1)/2$ would be odd and $\alpha^{p^{kr}-1}$ would be equal to -1. As $\mathbb{F}_q$ has an odd characteristic, this contradicts the hypothesis $\alpha^{p^{kr}-1} = 1$. Therefore $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$, $e \equiv 0 \pmod 2$ and $rk \equiv 0 \pmod 2$.

■

Corollary 1 *Assume that $\mathbb{F}_q$ is a finite field with $q = p^e$, p odd prime number, $e \in \mathbb{N}^*$ and $q \equiv 1 \pmod 4$. Consider $r \in \mathbb{N}$, θ the automorphism of $\mathbb{F}_q$ defined by $\theta : x \mapsto x^{p^r}$ and k a nonnegative integer. Then there exists a self-dual θ-code of dimension k.*

Proof. According to Proposition 1, if $p \equiv 1 \pmod 4$ there exists a self-dual θ-negacyclic code of dimension k; if $p \equiv 3 \pmod 4$ and $e \equiv 0 \pmod 2$, then there exists a self-dual θ-cyclic code of dimension k if $r \times k$ is odd and there exists a self-dual θ-negacyclic code of dimension k if $r \times k$ is even. ∎

Example 2 *Consider $\mathbb{F}_{3^2} = \mathbb{F}_3(a)$ with $a^2 - a - 1 = 0$ and $\theta : x \mapsto x^3$. For $k \in \mathbb{N}^*$, there exists α such that $X^k + \alpha$ is the skew check polynomial of a self-dual θ-cyclic code if and only if k is odd. In this case α satisfies $\alpha^2 + 1 = 0$ and $\theta^k(\alpha) + \alpha = 0$ i.e. $\alpha^2 + 1 = 0$ and $\alpha(\alpha^2 + 1) = 0$ (because $\theta^k = \theta$ if k is odd). So α must be equal to $\pm a^2$ (see Example 1).*

Remark 1 *When $r = 0$ (i.e. θ is the identity), Proposition 1 gives necessary and sufficient conditions of existence of self-dual cyclic and negacyclic codes generated by binomials over finite fields of odd characteristic. If $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$ and $e \equiv 0 \pmod 2$, there always exists a self-dual negacyclic code of any dimension (see also Corollary 3.3 of [4] when the dimension is p^s for $s > 0$). This seems to contradict Example 3.8 of [6] which states that a "self-dual negacyclic code of length 70 over $\mathbb{F}_5$ does not exist" and that there "is no self-dual negacyclic code of length 30 over $\mathbb{F}_9$". Namely, over $\mathbb{F}_5$, $X^{35} + 2$ generates a self-dual negacyclic code of dimension 35 whereas over $\mathbb{F}_9$, $X^{15} + a$ (with $a^2 = -1$) generates a self-dual negacyclic code of dimension 15.*

4 Self-dual skew codes generated by least common left multiples of skew polynomials

The following Lemma is inspired from Theorem 16 and Theorem 18 of [14] which state that a θ-cyclic code is either a cyclic code or a quasi-cyclic code.

Lemma 2 *Consider $\mathbb{F}_q$ a finite field, $\theta \in Aut(\mathbb{F}_q)$, $R = \mathbb{F}_q[X;\theta]$, n a nonnegative integer, ℓ the greatest common divisor of n and of the order of θ, $a \in (\mathbb{F}_q)^\theta \setminus \{0\}$ and h a right divisor of $X^n - a$ in R. Then $X^\ell h = hX^\ell$ (which means that the coefficients of h belong to the fixed field of θ^ℓ, $(\mathbb{F}_q)^{\theta^\ell}$).*

Proof. Consider m the order of θ, $u, v \in \mathbb{N}$ such that $\ell = mu - nv$. Consider $\frac{1}{a^v} X^{mu} h \in Rh/R(X^n - a)$, one has $\frac{1}{a^v} X^{mu} h = hX^{mu} \times \frac{1}{a^v} = hX^\ell X^{nv} \times \frac{1}{a^v} = hX^\ell$ in $R/R(X^n - a)$, therefore $hX^\ell \in Rh/R(X^n - a)$ and there exists $Q \in R$ monic of degree ℓ such that $hX^\ell = Qh$. The constant coefficient Q_0 of Q satisfies $Q_0 h_0 = 0$, as $h_0 \neq 0$, one gets $Q_0 = 0$. Furthermore, from the coefficients of degree $1, \ldots, \ell - 1$ of $hX^\ell - Qh$, one gets that the terms of Q with degrees $\leq \ell - 1$ all cancel, therefore $hX^\ell = X^\ell h$. ∎

The following proposition is a generalization of Proposition 28 of [2] (where θ was of order 2).

Proposition 2 *Consider $\mathbb{F}_q$ a finite field, $\theta \in Aut(\mathbb{F}_q)$, $R = \mathbb{F}_q[X;\theta]$, k a nonnegative integer and ℓ the greatest common divisor of $2k$ and of the order of θ, $\tilde{R} = (\mathbb{F}_q)^{\theta^\ell}[X;\tilde{\theta}]$ where $\tilde{\theta}$ is the restriction of θ to $(\mathbb{F}_q)^{\theta^\ell}$. Consider $s \in \mathbb{N}$ and $t \in \mathbb{N}$ not multiple of p, such that $2k = \ell \times p^s \times t$. Let $\varepsilon \in \{-1, 1\}$ and $Y^t - \varepsilon = f_1(Y) f_2(Y) \cdots f_m(Y) \in (\mathbb{F}_q)^\theta[Y]$, where $f_i(Y)$ are monic polynomials that are pairwise coprime with the property that $f_i^\natural = f_i$. The equation $h^\natural h = X^{2k} - \epsilon \in R$ is equivalent to $h^\natural h = X^{2k} - \epsilon \in \tilde{R}$. Its solutions are the skew polynomials h defined by $h = \mathrm{lcrm}(h_1, \ldots, h_m) \in \tilde{R}$ where for $i = 1, \ldots, m$, $h_i^\natural h_i = f_i^{p^s}(X^\ell) \in \tilde{R}$.*

Proof. According to Lemma 2, the equation $h^\natural h = X^{2k} - \epsilon$ in $R = \mathbb{F}_q[X;\theta]$ is equivalent to $h^\natural h = X^{2k} - \epsilon$ in $\tilde{R} = (\mathbb{F}_q)^{\theta^\ell}[X;\tilde{\theta}]$ where $(\mathbb{F}_q)^{\theta^\ell}$ is the fixed field of θ^ℓ and $\tilde{\theta}$ is the restriction of θ to $(\mathbb{F}_q)^{\theta^\ell}$. As $\tilde{\theta}^\ell$ fixes $(\mathbb{F}_q)^{\theta^\ell}$, the order of $\tilde{\theta}$ divides ℓ and therefore it divides $2k$.

Therefore in the following, without loss of generality, one can consider the equation $h^\natural h = X^{2k} - \epsilon$ in $R = \mathbb{F}_q[X;\theta]$ with $\theta \in Aut(\mathbb{F}_q)$ of order ℓ dividing $2k$. The proof of Proposition 28 of [2] can be adapted to this context and not all details are given.

1. ($\Leftarrow$) From $h = \mathrm{lcrm}(h_1, \ldots, h_m)$ one obtains that $h = h_i q_i$ with $q_i \in R$. Lemma 1 shows that there exists $\tilde{q}_i \in R$ such that $h^\natural = \tilde{q}_i h_i^\natural$. Therefore $h^\natural h = \tilde{q}_i(h_i^\natural h_i)q_i = \tilde{q}_i {f_i}^{p^s}(X^\ell)q_i = \tilde{q}_i q_i {f_i}^{p^s}(X^\ell)$ (because $f_i^{p^s}(X^\ell) \in (\mathbb{F}_q)^\theta[X^\ell]$ is central), showing that $\mathrm{lclm}(({f_1})^{p^s}(X^\ell), \ldots, ({f_m})^{p^s}(X^\ell)) = f_1^{p^s}(X^\ell) \cdots f_m^{p^s}(X^\ell) = X^n - \varepsilon$ is a right divisor of $h^\natural h$ in R. Furthermore, the degree of h is equal to the sum of the degrees of the skew polynomials h_i (because they are pairwise coprime), therefore the degree of $h^\natural h$ is equal to $\sum_{i=1}^m \deg(({f_i})^{p^s}(X^\ell)) = 2k$ which enables to conclude that $h^\natural h = X^{2k} - \epsilon$.

2. ($\Rightarrow$): According to ([5], Theorem 4.1), $h^\natural = \mathrm{lclm}(h_1^\natural, \ldots, h_m^\natural)$ where $h_i^\natural = \mathrm{gcrd}(f_i^{p^s}(X^\ell), h^\natural)$ are pairwise coprime in R. In particular, according to [13],

   $\deg(\mathrm{lclm}(h_i^\natural, h_j^\natural)) = \deg(h_i^\natural) + \deg(h_j^\natural)$ for $i \neq j$ and $\deg(h^\natural) = \deg(\mathrm{lclm}(h_i^\natural)) = \sum \deg(h_i^\natural)$.

   Let us now show that h_i divides ${f_i}^{p^s}(X^\ell)$ and h on the left :

   - Let δ_i be the degree of ${f_i}^{p^s}(X^\ell)$ and d_i be the degree of h_i. Applying Lemma 1 to ${f_i}^{p^s}(X^\ell) = q_i h_i^*$ one obtains $({f_i}^{p^s}(X^\ell))^* = \Theta^{\delta_i - d_i}(h_i^{**})q_i^* = \Theta^{\delta_i - d_i}(\Theta^{d_i}(h_i))q_i^* = \Theta^{\delta_i}(h_i)q_i^* = h_i q_i^*$ (because δ_i is a multiple of the order ℓ of θ). One concludes that h_i divides on the left $({f_i}^{p^s}(X^\ell))^*$ and h_i divides on the left $({f_i}^{p^s})^\natural(X^\ell) = {f_i}^{p^s}(X^\ell)$.
   - Since $h_i^\natural$ divides $h^\natural$ on the right, $h^* = p_i h_i^*$ for some p_i in R. Using Lemma 1, one obtains $\Theta^k(h) = h^{**} = \Theta^{k-d_i}(h_i^{**})p_i^*$. Therefore
     $\Theta^k(h) = \Theta^{k-d_i}(\Theta^{d_i}(h_i))p_i^* = \Theta^k(h_i)p_i^*$. Since Θ is a morphism of rings, h_i divides h on the left.

   Since $h_i^\natural$ divides $h^\natural$ on the right and h_i divides h on the left, there exist $g_i, \tilde{g}_i$ such that $h^\natural h = \tilde{g}_i h_i^\natural h_i g_i$. Since two factors of a decomposition of the central polynomial $h^\natural h = \tilde{g}_i h_i^\natural h_i g_i$ into two factors commute, $h_i^\natural h_i$ divides $h^\natural h = X^n - \varepsilon$ on the right. According to Theorem 4.1 of [5], $h_i^\natural h_i = \mathrm{lclm}(\mathrm{gcrd}(h_i^\natural h_i, ({f_j})^{p^s}(X^\ell)), j = 1, \ldots m)$. As both $h_i^\natural$ and h_i divide the central polynomial ${f_i}^{p^s}(X^\ell)$, the product $h_i^\natural h_i$ divides $({f_i}^{p^s})^2(X^\ell)$. For $j \neq i$, $\mathrm{gcrd}(h_i^\natural h_i, ({f_j})^{p^s}(X^\ell)) = 1$ and $h_i^\natural h_i = \mathrm{gcrd}(h_i^\natural h_i, {f_i}^{p^s}(X^\ell))$, in particular, $h_i^\natural h_i$ divides ${f_i}^{p^s}(X^\ell)$.

   For $i \in \{1, \ldots, m\}$ the polynomials ${f_i}^{p^s}(X^\ell)$ are pairwise coprime, showing that their divisors $h_i^\natural h_i$ are also pairwise coprime. Therefore

$$\deg(\mathrm{lclm}(h_i^\natural h_i)) = \sum_{i=1}^m \deg(h_i^\natural h_i) = 2\deg(h^\natural) = \sum_{i=1}^m \deg({f_i}^{p^s}(X^\ell)).$$

   From $\sum_{i=1}^m \deg(h_i^\natural h_i) = \sum_{i=1}^m \deg({f_i}^{p^s}(X^\ell))$ and the fact that $h_i^\natural h_i$ divides ${f_i}^{p^s}(X^\ell)$, we obtain $h_i^\natural h_i = {f_i}^{p^s}(X^\ell)$.

As h_i divides h on the left, $\mathrm{lcrm}(h_i, i = 1, \ldots, m)$ also divides h on the left. Since $\mathrm{gcrd}(h_i^\natural, h_j^\natural) = 1$ implies $\mathrm{gcld}(h_i, h_j) = 1$, one gets $\deg(\mathrm{lcrm}(h_i, i = 1, \ldots, m)) = \sum \deg(h_i) = \deg(h)$. Therefore $h = \mathrm{lcrm}(h_i, i = 1, \ldots, m)$.

■

Corollary 2 *Consider $\mathbb{F}_q$ a finite field with odd characteristic p, $\theta \in Aut(\mathbb{F}_q)$, $R = \mathbb{F}_q[X;\theta]$. Consider ℓ the greatest common divisor of $2 \times k$ and of the order of θ, $k \in \mathbb{N}^*$, $s \in \mathbb{N}$ and $t \in \mathbb{N}$ not multiple of p such that $2 \times k = \ell \times p^s \times t$.*

1. *If the order of θ is odd then there does not exist a self-dual θ-cyclic code of dimension k over $\mathbb{F}_q$.*
2. *If the order of θ is odd and if $Y^t + 1 \in (\mathbb{F}_q)^\theta[Y]$ has a self-reciprocal irreducible factor of degree > 1, then there does not exist a self-dual θ-negacyclic code of dimension k over $\mathbb{F}_q$.*

Proof.

1. Assume that there is a self-dual θ-cyclic code of dimension k, then the equation $h^\natural h = X^{2k} - 1$ has a solution in R. Furthermore $Y - 1$ divides $Y^t - 1$ and is self-reciprocal, therefore, according to Proposition 2, the intermediate equation $H^\natural H = (X^l - 1)^{p^s}$ has a solution. But the order of θ is odd so ℓ is odd, therefore the right hand side of this intermediate equation has an odd degree which is impossible as the degree of the left hand side is even.
2. Consider $f(Y) = f^\natural(Y) \in (\mathbb{F}_q)^\theta[Y]$ irreducible dividing $Y^t + 1$, then the irreducible skew factors of $f(X^\ell)$ have the same degree as $\deg(f(Y))$ and therefore a factorization of $f(X^\ell)^{p^s}$ into irreducible skew polynomials has $\ell \times p^s$ factors of degree $\deg(f(Y))$. As the order of θ is odd, ℓ is odd and $\ell \times p^s$ is odd, therefore each factorization of $f(X^\ell)^{p^s}$ into the product of irreducible factors has an odd number of irreducible factors with the same degree. Consider $H \in R$ satisfying the intermediate equation $H^\natural H = f(X^\ell)^{p^s}$. The skew polynomials H and $H^\natural$ must have the same number of irreducible factors, with the same degree and dividing $f(X^\ell)^{p^s}$. This contradicts the fact that $f(X^\ell)^{p^s}$ has an odd number of irreducible factors with the same degree. Therefore, according to Proposition 2, the equation $h^\natural h = X^{2k} + 1$ has no solution in R.

■

Remark 2 *According to Theorem 2.2 of [6], there does not exist a self-dual negacyclic code of length $2k$ over $\mathbb{F}_q$, with $\mathbb{F}_q$ of odd characteristic, if the polynomial $X^{2k} + 1 \in \mathbb{F}_q[X]$ has an irreducible factor f such that $f = f^\natural$.*

From Proposition 1 one deduces that there cannot exist both a self-dual θ-cyclic code generated by a binomial and a self-dual θ-negacyclic code generated by a binomial and having the same dimension. The following proposition shows that more generally there cannot exist both a self-dual θ-cyclic and a self-dual θ-negacyclic code with the same dimension.

Proposition 3 *Consider $\mathbb{F}_q$ a finite field with odd characteristic p and θ an automorphism of $\mathbb{F}_q$. There cannot exist both a self-dual θ-cyclic code and a self-dual θ-negacyclic code with the same dimension over $\mathbb{F}_q$.*

Proof. Consider $k \in \mathbb{N}$, $\epsilon \in \{-1, 1\}$. According to Lemma 2, the equation $h^{\natural}h = X^{2k} - \epsilon$ in $R = \mathbb{F}_q[X;\theta]$ is equivalent to $h^{\natural}h = X^{2k} - \epsilon$ in $\tilde{R} = (\mathbb{F}_q)^{\theta^\ell}[X;\tilde{\theta}]$ where $(\mathbb{F}_q)^{\theta^\ell}$ is the fixed field of θ^ℓ and $\tilde{\theta}$ is the restriction of θ to $(\mathbb{F}_q)^{\theta^\ell}$. As $\tilde{\theta}^\ell$ fixes $(\mathbb{F}_q)^{\theta^\ell}$, the order of $\tilde{\theta}$ divides ℓ and therefore it divides $2k$. Therefore in the following, without loss of generality, one can consider that the order ℓ of $\theta \in Aut(\mathbb{F}_q)$ divides $2 \times k$. Consider $s \in \mathbb{N}$ and $t \in \mathbb{N}$ such that $2 \times k = \ell \times p^s \times t$ where t is not a multiple of p.

1. One first considers the particular case when $t = 1$ i.e. $2 \times k = \ell \times p^s$. Assume that there exists a self-dual θ-cyclic code of dimension k. Consider $h \in R$ monic such that $h^{\natural}h = X^{2k} - 1$ and α the constant coefficient of h. The skew polynomial $X^\ell - \epsilon$ belongs to $(\mathbb{F}_q)^{\theta}[X^\ell]$ therefore it is central of degree 1 in X^ℓ and the skew factors of any of its factorizations are all of degree 1. The skew polynomial $X^{2k} - \epsilon = (X^\ell - \epsilon)^{p^s}$ shares the same property. As h divides $X^{2k} - 1$ and as $X^{2k} - 1$ factors as a product of linear skew polynomials, a factorization of h is $h = (X - \alpha_1) \cdots (X - \alpha_k)$ where $\alpha_i \in \mathbb{F}_q$ and $X - \alpha_i$ divides on the right $X^{2k} - 1$ (because $X^{2k} - 1$ is central). According to Equation (11) of [10], one has $N_{2k}(\alpha_i) = 1$ where for $m \in \mathbb{N}^*$ and $u \in \mathbb{F}_q$, $N_m(u) := u\theta(u) \cdots \theta^{m-1}(u)$ is the norm of u. As $\alpha = (-1)^k \prod_{i=1}^{k} \alpha_i$, one gets $N_{2k}(\alpha) = 1$. Furthermore the constant term of $h^{\natural}h$ is equal to $\alpha/\theta^k(\alpha)$ therefore, $\theta^k(\alpha) = -\alpha$ and $1 = N_{2k}(\alpha) = (-1)^k N_k(\alpha)^2$. Similarly if there exists a self-dual θ-negacyclic code of dimension k, then there exists β in $\mathbb{F}_q$ such that $N_{2k}(\beta) = (-1)^k$, $\theta^k(\beta) = \beta$ and $N_k(\beta)^2 = (-1)^k$. If k is even then $N_k(\alpha)^2 = 1$, therefore $N_k(\alpha) = \pm 1$ so $\alpha^{\frac{p^k-1}{p-1}} = \pm 1$ and $\alpha^{p^k-1} = (\pm 1)^{p-1}$. As p is odd, one gets $\alpha^{p^k-1} = 1$, which contradicts $\theta^k(\alpha) = -\alpha$. If k is odd then $N_k(\beta)^2 = -1 = N_k(\alpha)^2$, so $N_k(\alpha) = \pm N_k(\beta)$ and $N_{2k}(\alpha) = N_k(\beta)^2 = -1$, which contradicts $N_{2k}(\alpha) = 1$. Therefore if $t = 1$, there cannot exist both a self-dual θ-cyclic code and a self-dual θ-negacyclic code with dimension k over $\mathbb{F}_q$.

2. Consider now the case when $t > 1$. If t is even, then $Y - 1$ and $Y + 1$ divides $Y^t - 1$ in $(\mathbb{F}_q)^{\theta}[Y]$. If there is a self-dual θ-cyclic code of dimension k then according to Proposition 2, the intermediate skew equation $h_1^{\natural}h_1 = X^{\ell p^s} - 1$ and $h_2^{\natural}h_2 = X^{\ell p^s} + 1$ must have monic solutions $h_1, h_2 \in R$, which is impossible according to the first part of the proof. Therefore no self-dual θ-cyclic code of dimension k exists. If t is odd then $Y - 1$ divides $Y^t - 1$ and $Y + 1$ divides $Y^t + 1$ in $(\mathbb{F}_q)^{\theta}[Y]$. According to Proposition 2, if there is a self-dual θ-cyclic code of dimension k, then the skew equation $h_1^{\natural}h_1 = X^{\ell p^s} - 1$ must have a monic solution $h_1 \in R$. If there is a self-dual θ-negacyclic code of dimension k, then the skew equation $h_2^{\natural}h_2 = X^{\ell p^s} + 1$ must also have a monic solution $h_2 \in R$. This is impossible according to the first part of the proof.

■

5 Existence of self-dual skew codes over finite fields with odd characteristic

According to Proposition 1, if $q \equiv 3 \pmod 4$, then there is no self-dual θ-code generated by skew binomials over $\mathbb{F}_q$. The following proposition gives a necessary and sufficient condition of existence of self-dual θ-codes when $q \equiv 3 \pmod 4$. The proof uses Corollary 2.

Proposition 4 *Assume that $\mathbb{F}_q$ is a finite field of characteristic p with $q \equiv 3 \pmod 4$. Consider θ an automorphism of $\mathbb{F}_q$ and $\mu \geq 2$ the biggest integer such that 2^μ divides $p+1$ (i.e. 2^μ divides exactly $p+1$).*

1. *There does not exist a self-dual θ-cyclic code of dimension k over $\mathbb{F}_q$.*
2. *There exists a self-dual θ-negacyclic code of dimension k over $\mathbb{F}_q$ if, and only if, $k \equiv 0 \pmod{2^{\mu-1}}$.*

Proof.

Assume that $q = p^e \equiv 3 \pmod 4$ i.e. $p \equiv 3 \pmod 4$ and $e \equiv 1 \pmod 2$. Consider $r \in \mathbb{N}$ such that θ is defined by $x \mapsto x^{p^r}$.

1. The order of θ is $e/\gcd(e,r)$, therefore as e is odd, the order of θ is also odd. According to point 1. of Corollary 2, there cannot exist a self-dual θ-cyclic code of dimension k over $\mathbb{F}_q$.

2. Consider α the biggest integer such that 2^α divides k and assume that $\alpha + 1 \geq \mu$. Therefore $2k$ is divisible by 2^μ and the skew polynomial $X^{2k}+1$ is equal to $(X^{k/2^{\mu-1}})^{2^\mu} + 1$. One proves that the polynomial $Y^{2^\mu}+1$ factors in $\mathbb{F}_p[Y]$ as the product of two polynomials $h(Y)$ and $h^\natural(Y)$. Namely, consider w a primitive $2^{\mu+1}$-th root of unity in $\overline{\mathbb{F}_p}$. As 2^μ divides $p+1$, $2^{\mu+1}$ divides p^2-1 and w belongs to $\mathbb{F}_{p^2} - \mathbb{F}_p$. The polynomial $Y^{2^\mu}+1 = (Y^{2^{\mu+1}}-1)/(Y^{2^\mu}-1)$ factors in $\mathbb{F}_{p^2}[Y]$ as the product of $Y - w^i$ where i describes the odd numbers of $\{0, \ldots, 2^{\mu+1}-1\}$. This polynomial can also be written as the product of the polynomials $h_i(Y)h_i^\natural(Y)$ where $h_i(Y) = Y^2 - (w^i + w^{ip})Y + w^{i(p+1)}$ is in $\mathbb{F}_p[Y]$. One concludes that $Y^{2^\mu}+1$ factors in $\mathbb{F}_p[Y]$ as the product of two polynomials $h(Y)$ and $h^\natural(Y)$. From this factorization, one deduces that $X^{2k}+1 = H^\natural(X)H(X) \in \mathbb{F}_p[X]$ where $H(X) = h(X^{k/2^{\mu-1}})$. So there exists a $[2k,k]_p$ self-dual negacyclic code and as $\mathbb{F}_p$ is fixed by θ, the relation $X^{2k}+1 = H^\natural(X)H(X)$ still holds in $\mathbb{F}_q[X;\theta]$.

   Conversely, assume that $\alpha < \mu - 1$. Consider ℓ the greatest common divisor of $2k$ and of the order of θ, and t, s such that $2k = \ell \times t \times p^s$ where p does not divide t. Let us prove that $Y^t + 1 \in (\mathbb{F}_q)^\theta[Y]$ has an irreducible factor $f(Y)$ such that $f^\natural(Y) = f(Y)$. Consider $e' = \gcd(e,r)$ and $q' = p^{e'}$, then $(\mathbb{F}_q)^\theta = \mathbb{F}_{q'}$. As e is odd, and as the order of θ is equal to $e/\gcd(e,r)$, the order of θ is odd and ℓ is also odd. As $p \equiv -1 \pmod{2^\mu}$ and $q' = p^{e'}$ with e' odd, $q' \equiv -1 \pmod{2^\mu}$, furthermore $\alpha \leq \mu - 2$, $q' \equiv -1 \pmod{4 \times 2^\alpha}$. Let us consider w a primitive $4 \times 2^\alpha$-th root of unity in $\mathbb{F}_{q'^2}$. Such an w does exist as $q'^2 - 1 \equiv 0 \pmod{4 \times 2^\alpha}$, furthermore $w^{q'} = w^{-1}$ because $4 \times 2^\alpha$ divides $q'+1$. As $2^{\alpha+1}$ divides exactly $2k$ and as $2k = \ell \times t \times p^s$, $2^{\alpha+1}$ divides exactly t, therefore $4 \times 2^\alpha$ divides exactly $2t$, $w^{2t} = 1$ and $w^t = -1$. The minimal polynomial $f \in \mathbb{F}_{q'}[Y]$ of w divides $Y^{2t}-1$ but not $Y^t - 1$, so it divides $Y^t + 1$. Furthermore $f(w^{q'}) = 0$ and $w^{q'} = w^{-1}$ therefore $f(w^{-1}) = 0$ and $f = f^\natural$. Therefore $Y^t + 1$ has an irreducible factor $f \in \mathbb{F}_{q'}[Y] = (\mathbb{F}_q)^\theta[Y]$ such that $f = f^\natural$. Furthermore, the order of θ is odd, so according to Corollary 2, there cannot exist a self-dual θ-negacyclic code of dimension k.

■

Remark 3 *Assume that $p \equiv 3 \pmod 4$, e is odd. Consider $\mu \geq 2$ the biggest integer such that 2^μ divides $p+1$. Consider $k = p^s$ with $s \in \mathbb{N}$, then $k \not\equiv 0 \pmod{2^{\mu-1}}$ and according to*

Proposition 4, there is no negacyclic code of dimension k. This result was previously obtained in Corollary 3.3. of [4].

To conclude, it remains to decide, when $q \equiv 1 \pmod 4$, if the existing self-dual θ-codes are θ-cyclic or θ-negacyclic. According to Theorem 1 of [3], over $\mathbb{F}_q = \mathbb{F}_{p^2}$ with $\theta : x \mapsto x^p$ and p prime number, there exists a self-dual θ-cyclic code of length $2k$ if and only if k is an odd number and $p \equiv 3 \pmod 4$ whereas 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 is even. The following proposition generalizes this result and states that the sufficient conditions of existence of self-dual skew codes given in Proposition 1 for $q \equiv 1 \pmod 4$ are also necessary. Its proofs uses Proposition 3 which states that there cannot exist simultaneously a self-dual θ-cyclic code and a self-dual θ-negacyclic code with the same dimension :

Proposition 5 *Consider a finite field $\mathbb{F}_q$ with $q = p^e$, p odd prime number, $e \in \mathbb{N}^*$ and $q \equiv 1 \pmod 4$ (i.e. $p \equiv 3 \pmod 4$ and e even or $p \equiv 1 \pmod 4$). Consider $r \in \mathbb{N}$, θ the automorphism of $\mathbb{F}_q$ defined by $\theta : x \mapsto x^{p^r}$ and k a nonnegative integer.*

1. *There exists a self-dual θ-cyclic code of dimension k over $\mathbb{F}_q$ if and only if $p \equiv 3 \pmod 4$, e is even and $r \times k$ is odd.*
2. *There exists a self-dual θ-negacyclic code of dimension k over $\mathbb{F}_q$ if and only if $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$, e is even and $r \times k$ is even.*

Proof.

1. According to Proposition 1 point 1., if $p \equiv 3 \pmod 4$, e is even and $r \times k$ is odd, there exists a self-dual θ-cyclic code of dimension k (generated by a skew binomial). Conversely, assume that there exists a self-dual θ-cyclic code of dimension k, then according to Proposition 3, there is no θ-negacyclic code with dimension k therefore according to Proposition 1 point 2., $p \equiv 3 \pmod 4$, $e \equiv 0 \pmod 2$ and $r \times k \equiv 1 \pmod 2$.
2. According to Proposition 1 point 2., if $p \equiv 3 \pmod 4$, $e \equiv 0 \pmod 2$ and $r \times k \equiv 0 \pmod 2$ or $p \equiv 1 \pmod 4$, there exists a self-dual θ-negacyclic code of dimension k (generated by a skew binomial). Conversely, assume that there exists a self-dual θ-negacyclic code of dimension k, then according to Proposition 3, there is no θ-cyclic code with dimension k therefore according to Proposition 1 point 1., $p \equiv 3 \pmod 4$, $e \equiv 0 \pmod 2$ and $r \times k \equiv 0 \pmod 2$ or $p \equiv 1 \pmod 4$.

■

To conclude, Proposition 4 ($q \equiv 3 \pmod 4$) and Proposition 5 ($q \equiv 1 \pmod 4$) are summed up in Table 1 below.

References

[1] 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

	Self-dual θ-cyclic	Self-dual θ-negacyclic
$q \equiv 1 \pmod 4$, $p \equiv 3 \pmod 4$	$r \times k \equiv 1 \pmod 2$	$r \times k \equiv 0 \pmod 2$
$q \equiv 1 \pmod 4$, $p \equiv 1 \pmod 4$	no k	$k \in \mathbb{N}^*$
$q \equiv 3 \pmod 4$	no k	$k \equiv 0 \pmod{2^{\mu-1}}$

Table 1: Necessary and sufficient conditions for the existence of self-dual θ-cyclic and θ-negacyclic codes of dimension k over $\mathbb{F}_q$ where $\mathbb{F}_q$ has odd characteristic p, $\mu \in \mathbb{N}$ is such that 2^μ divides exactly $p+1$ and $\theta : x \mapsto x^{p^r}$.

[2] Boucher D., Ulmer F. *Self-dual skew codes and factorization of skew polynomials* Journal of Symbolic Computation, Volume 60, January 2014, 47-61

[3] Boucher D. *Construction and number of self-dual skew codes over* $\mathbb{F}_{p^2}$, preprint, https://hal.archives-ouvertes.fr/hal-01090922, 2014

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

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

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

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

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

[9] Kai, Xiaoshan and Zhu, Shixin *On Cyclic Self-Dual Codes* Applicable Algebra in Engineering, Communication and Computing, 19, 2008, 6, 509–525,

[10] T.Y. Lam , *A general theory of Vandermonde matrices*, Expositiones Mathematicae, 4, 193-215 (1986)

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

[12] Ling, San and Solé, Patrick, *On the algebraic structure of quasi-cyclic codes. II. Chain rings*, Designs, Codes and Cryptography., 30, 2003, 1, 113–130

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

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