



HAL
open science

A note on the duality of skew module codes

D Boucher

► **To cite this version:**

D Boucher. A note on the duality of skew module codes. WCC 2022: The Twelfth International Workshop on Coding and Cryptography, Mar 2002, Rostock, Germany. hal-03903929

HAL Id: hal-03903929

<https://hal.science/hal-03903929>

Submitted on 16 Dec 2022

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

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

A note on the duality of skew module codes.

D. Boucher *

December 16, 2022

Abstract

We introduce a new notion of duality inspired from the paper *On the duality and the direction of polycyclic codes* by Adel Alahmadi, Steven Dougherty, André Leroy and Patrick Solé. We get that the dual of a central skew module code is a central skew module code.

1 Introduction.

Consider the finite field \mathbb{F}_q with q elements and a non-negative integer n . A linear code over \mathbb{F}_q of length n is a subspace of \mathbb{F}_q^n . The *dual* of a linear code C of length n over \mathbb{F}_q is defined as $C^\perp = \{x \in \mathbb{F}_q^n \mid \forall y \in C, \langle x, y \rangle = 0\}$ where $\langle \cdot, \cdot \rangle$ is an inner product over $\mathbb{F}_q^n \times \mathbb{F}_q^n$. The code C is *self-dual* if C is equal to C^\perp . Cyclic codes over \mathbb{F}_q form a class of linear codes who are invariant under a cyclic shift of coordinates. This cyclicity condition enables to describe a cyclic code as an ideal $(g)/(X^n - 1)$ of $\mathbb{F}_q[X]/(X^n - 1)$ where g is a monic divisor of $X^n - 1$. If we replace $X^n - 1$ with a polynomial $f \in \mathbb{F}_q[X]$ of degree n we get a polycyclic code. It is well known that the Euclidean dual of a cyclic code is a cyclic code and self-dual cyclic codes have been extensively studied ([10], [13], ...). However the dual of a polycyclic code is not polycyclic. In [1], an inner product is defined over \mathbb{F}_q^n in such a way that the dual of a polycyclic code is a polycyclic code. In this note, we will design a new notion of duality for polycyclic codes and skew module codes.

In Section 2, we give some generalities on skew module codes. In Section 3, we design a new notion of duality based on skew polynomials. In Section 4, we characterize self-dual skew module codes by an equation called self-dual skew module equation and in Section 5, we give some clues for the resolution of this equation when $q = p^2$.

2 Generalities on skew module codes.

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

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

The ring R is called a skew polynomial ring or Ore ring (cf. [12]) and its elements are skew polynomials. When θ is not the identity, the ring R is not commutative, it is a left and right

*Univ Rennes, CNRS, IRMAR - UMR 6625, F-35000 Rennes, France

Euclidean ring whose left and right ideals are principal. Left and right gcd and lcm exist in R and can be computed using the left and right Euclidean algorithms. The center of R is the commutative polynomial ring $Z(R) = \mathbb{F}_q^\theta[X^m]$ where \mathbb{F}_q^θ is the fixed field of θ and m is the order of θ .

Definition 1 ([6]) Consider f in R of degree n . A θ -module code or skew module code C is a R -sub-module on the left $Rg/Rf \subset R/Rf$ where g is a right divisor of f in R . Its length is $n = \deg(f)$ and its dimension is $k = \deg(f) - \deg(g)$. The skew polynomial g is a (skew) generator polynomial of C . If g is monic, g is the (monic) skew generator polynomial of C .

If $f = X^n - a$ with $a \in \mathbb{F}_q$, one says that the code C is (θ, a) -constacyclic. It is θ -cyclic if $a = 1$ and θ -negacyclic if $a = -1$.

For x, y in \mathbb{F}_q^n , $\langle x, y \rangle_E := \sum_{i=1}^n x_i y_i$ is the (Euclidean) scalar product of x and y . The code C is (Euclidean) self-dual if C is equal to C^\perp . Assume that σ is an automorphism of \mathbb{F}_q of order 2. The (Hermitian) dual of a linear code C of length n over \mathbb{F}_q is defined as $C^{\perp_H} = \{x \in \mathbb{F}_q^n \mid \forall y \in C, \langle x, y \rangle_H = 0\}$ where for x, y in \mathbb{F}_q^n , $\langle x, y \rangle_H := \sum_{i=1}^n x_i \sigma(y_i)$ is the (Hermitian) scalar product of x and y . The code C is (Hermitian) self-dual if C is equal to C^{\perp_H} .

If C is θ -module code of length n , either it is θ -constacyclic and then its (Euclidean) dual is a θ -constacyclic code (Theorem 1 and Lemma 2 of [8]); either it is the shortened code of a θ -cyclic code (of length $N > n$) and its (Euclidean) dual is a punctured code of a θ -cyclic code (Proposition 3 of [8]). Furthermore, in [11], the (Euclidean) dual of a θ -module code (also called θ -polycyclic code) is identified as a θ -sequential code (see Theorem 2 of [11]).

In [1] an inner product is introduced in such a way that the dual of a polycyclic code (i.e. a θ -module code for $\theta = id$) is polycyclic. In this note, we want to design a new notion of duality such that the dual of a polycyclic code is a polycyclic code and the dual of a skew module code is a skew module code. Note that when $\theta = id$, the dual defined in this note is not the same as the one obtained in [1] (see Remark 1 and Remark 3).

We conclude this introductory part with some material on skew reciprocal polynomials which will be useful in this note.

Definition 2 (Definition 3 of [8] or Definition 2 of [2]) Consider $h = \sum_{i=0}^k h_i X^i \in R$ of degree k . The skew reciprocal polynomial of h is

$$h^* = \sum_{i=0}^k X^{k-i} \cdot h_i = \sum_{i=0}^{k-v} \theta^i(h_{k-i}) X^i$$

and the monic skew reciprocal polynomial of h is

$$h^\natural = \frac{1}{\theta^{k-v}(h_v)} h^* = X^{k-v} + \sum_{i=0}^{k-v-1} \frac{\theta^i(h_{k-i})}{\theta^{k-v}(h_v)}$$

where $v = \min\{i \mid h_i \neq 0\}$ is the valuation of h .

In what follows, we will denote

$$\theta : \begin{cases} R & \rightarrow R \\ \sum a_i X^i & \mapsto \sum \theta(a_i) X^i \end{cases} \quad \text{and} \quad \sigma : \begin{cases} R & \rightarrow R \\ \sum a_i X^i & \mapsto \sum \sigma(a_i) X^i. \end{cases}$$

Lemma 1 (Lemma 1 of [8]) Consider f, g, h in R non zero.

1. $(h \cdot g)^* = \theta^{\deg(h)}(g^*) \cdot h^*$.
2. Let d be the degree of f and let v be the valuation of f , then $(f^*)^* \cdot X^v = \theta^{d-v}(f)$.

We will use a slight modification of the skew reciprocal polynomial : for $h \in R$ of degree less than n , the n -skew reciprocal polynomial of h is

$$r_n(h) := X^{n-\deg(h)} \cdot h^* = \sum_{i=n-k}^{n-v} \theta^i(h_{n-i})X^i \quad (2)$$

where k is the degree of h and v is its valuation.

In particular, for g, h in R of degree less than n we have

$$r_n(g + h) = r_n(g) + r_n(h).$$

3 A notion of duality based on skew polynomials.

In [1], an inner product $\langle \cdot, \cdot \rangle_f$ is defined over \mathbb{F}_q^n in the following way. Consider f in $\mathbb{F}_q[X]$ of degree n and $a = (a_0, \dots, a_{n-1}), b = (b_0, \dots, b_{n-1})$ in \mathbb{F}_q^n . Associate to a, b the polynomials $a(X) = \sum_{i=0}^{n-1} a_i X^i$ and $b(X) = \sum_{i=0}^{n-1} b_i X^i$ in $\mathbb{F}_q[X]$. The f -scalar product of a and b is defined as $\langle a, b \rangle_f = Q(0)$ where $Q(X)$ is the remainder in the division of $a(X)b(X) \in \mathbb{F}_q[X]$ by $f(X)$. Inspired by the work of [1], we consider here a new map $\langle \cdot, \cdot \rangle_{f,\theta,\sigma}$ where $f(X)$ is a monic central polynomial of $R = \mathbb{F}_q[X; \theta]$, θ is an automorphism of \mathbb{F}_q and σ is an automorphism of \mathbb{F}_q such that $\sigma^2 = id$.

In what follows, we associate to $a = (a_0, \dots, a_{n-1}) \in \mathbb{F}_q^n$ the skew polynomial $a(X) = \sum_{i=0}^{n-1} a_i X^i$ in R . Furthermore we assume that f is a monic central polynomial.

Definition 3 The map $\langle \cdot, \cdot \rangle_{f,\theta,\sigma}$ from $\mathbb{F}_q^n \times \mathbb{F}_q^n$ to \mathbb{F}_q is defined by : for a, b in \mathbb{F}_q^n

$$\langle a, b \rangle_{f,\theta,\sigma} = P(0) \quad (3)$$

where $P(X)$ is the remainder in the division on the right of the skew polynomial $a(X) \cdot \sigma(r_n(b(X)))$ by $f(X)$ and $P(0)$ is the constant coefficient of $P(X)$.

Remark 1 Consider $\theta = \sigma = id$, $f \in \mathbb{F}_q[X]$ of degree n , $a \in \mathbb{F}_q^n$ and $b \in \mathbb{F}_q^n$. We have $\langle a, b \rangle_{f,id,\sigma} = P(0)$ where $P(X)$ is the remainder in the division of $a(X) \cdot r_n(b(X))$ by $f(X)$ in $\mathbb{F}_q[X]$. Meanwhile the scalar product defined in [1] $\langle \cdot, \cdot \rangle_f$ is defined by $\langle a, b \rangle_f = Q(0)$ where $Q(X)$ is the remainder in the division of $a(X)b(X)$ by $f(X)$ in $\mathbb{F}_q[X]$.

We recall that a σ -sesquilinear form (see [14]) on \mathbb{F}_q^n is defined as a map $\langle \cdot, \cdot \rangle : \mathbb{F}_q^n \times \mathbb{F}_q^n \rightarrow \mathbb{F}_q$ such that if $x, y, z \in \mathbb{F}_q^n$ and $a \in \mathbb{F}_q$ then $\langle x+z, y \rangle = \langle x, y \rangle + \langle z, y \rangle$, $\langle x, y+z \rangle = \langle x, y \rangle + \langle x, z \rangle$, $\langle ax, y \rangle = a \langle x, y \rangle$ and $\langle x, ay \rangle = \langle x, y \rangle \sigma(a)$.

Proposition 1 The map $\langle \cdot, \cdot \rangle_{f,\theta,\sigma}$ is a σ -sesquilinear form.

Proof. We denote $\langle \cdot, \cdot \rangle = \langle \cdot, \cdot \rangle_{f, \theta, \sigma}$. Consider a, b, c in \mathbb{F}_q^n and λ in \mathbb{F}_q . We have $(a(X) + b(X)) \cdot \sigma(r_n(c(X))) = a(X) \cdot \sigma(r_n(c(X))) + b(X) \cdot \sigma(r_n(c(X)))$ therefore $\langle a + b, c \rangle = \langle a, c \rangle + \langle b, c \rangle$. We have $r_n(b(X) + c(X)) = r_n(b(X)) + r_n(c(X))$ therefore $a(X) \cdot \sigma(r_n(b(X) + c(X))) = a(X) \cdot \sigma(r_n(b(X))) + a(X) \cdot \sigma(r_n(c(X)))$ and $\langle a, b + c \rangle = \langle a, b \rangle + \langle a, c \rangle$.

Consider $P(X)$ the remainder in the division on the right of $a(X) \cdot \sigma(r_n(b(X)))$ by $f(X)$ in R . Then $\lambda P(X)$ is the remainder in the division on the right of $\lambda a(X) \cdot \sigma(r_n(b(X)))$ by $f(X)$ in R and we have $\langle \lambda a, b \rangle = (\lambda P)(0) = \lambda \langle a, b \rangle$. We have $a(X) \sigma(r_n(\lambda b(X))) = a(X) \cdot \sigma(r_n(b(X))) \sigma(\lambda)$ and as $f(X)$ is central, the remainder in the division of $a(X) \cdot \sigma(r_n(b(X))) \lambda$ by $f(X)$ on the right is $P(X) \cdot \sigma(\lambda)$, therefore $\langle a, \lambda b \rangle = (P \cdot \sigma(\lambda))(0) = \sigma(\lambda) P(0) = \langle a, b \rangle \sigma(\lambda)$.
■

Definition 4 Consider a linear code C over \mathbb{F}_q with length n .

The left dual of C for $\langle \cdot, \cdot \rangle_{f, \theta, \sigma}$ is defined as

$$l(C) = l_{f, \theta, \sigma}(C) = \{x \in \mathbb{F}_q^n \mid \forall c \in C, \langle x, c \rangle_{f, \theta, \sigma} = 0\}. \quad (4)$$

The right dual of C is defined as

$$r(C) = r_{f, \theta, \sigma}(C) = \{x \in \mathbb{F}_q^n \mid \forall c \in C, \langle c, x \rangle_{f, \theta, \sigma} = 0\}. \quad (5)$$

In the proposition below, we make the link with the Euclidean dual and the Hermitian dual of linear codes.

Proposition 2 Assume that $f = X^n - \epsilon$ is a central polynomial with $\epsilon \neq 0$.

- If $\sigma = id$, then $r(C) = l(C)$ is the dual C^\perp of C for the Euclidean scalar product.
- If σ has order 2, then $r(C) = l(C)$ is the dual $C^{\perp H}$ of C for the Hermitian scalar product.

Proof. Consider $a, b \in \mathbb{F}_q^n$. The constant coefficient of $P(X) = a(X) \cdot \sigma(r_n(b(X))) = \sum_{i=0}^{n-1} a_i X^i \cdot \sum_{j=0}^{n-1} X^{n-j} \cdot \sigma(b_j) \in R/Rf$ is $\epsilon \times \sum_{i=0}^{n-1} a_i \theta^{i+n-i}(\sigma(b_i)) = \epsilon \times \sum_{i=0}^{n-1} a_i \sigma(b_i)$. Therefore for $a, b \in \mathbb{F}_q^n$, $\langle a, b \rangle_{f, \theta, \sigma} = 0 \Leftrightarrow \sum_{i=0}^{n-1} a_i \times \sigma(b_i) = 0$.
■

In what follows, we give an analogue of the MacWilliams formula for $l(C)$ and $r(C)$ inspired from [1].

Lemma 2 If $f(0) \neq 0$, then the σ -sesquilinear form $\langle \cdot, \cdot \rangle_{f, \theta, \sigma}$ is non-degenerate.

Proof. We denote $\langle \cdot, \cdot \rangle = \langle \cdot, \cdot \rangle_{f, \theta, \sigma}$ and $F(X) = \frac{-1}{f(0)} \frac{f(X) - f(0)}{X}$, which is well-defined as $f(0) \neq 0$. We have $F(X) \cdot X = X \cdot F(X) = 1$ in R/Rf .

Consider a in \mathbb{F}_q^n and assume that for all b non-zero in \mathbb{F}_q^n we have $\langle a, b \rangle = 0$. Then for $b = 1$, we get $\langle a, 1 \rangle = 0$ therefore $a(0) = 0$ and $a(X) = a'(X)X$. Denote v the degree of the lowest term of $F(X)$ and consider $b(X) = r_n(F(X))$. Then $b(X) = X \cdot F^*(X)$, therefore $\deg(b) = 1 + n - 1 - v = n - v$ and $b^*(X)X^v = (XF^*(X))^* X^v = (F^*(X))^* X^v = F(X)$. We conclude that $r_n(b(X)) = X^{n-(n-v)} b^*(X) = F(X)$, therefore $\langle a, b \rangle = a'(0) = 0$. Repeating the operation, we obtain $a = 0$.

Consider b in \mathbb{F}_q^n and assume that for all a non-zero in \mathbb{F}_q^n we have $\langle a, b \rangle = 0$. For $a = 1$ we get $\langle 1, b \rangle = 0$, therefore $\sigma(r_n(b))(0) = 0$ and $\sigma(r_n(b(X))) = Xb'(X)$. For $a(X) = F(X)$,

we get $\langle F, b \rangle = 0$, therefore $F(X)\sigma(r_n(b(X))) = b'(X) \in R/Rf$ cancels at 0. Repeating the operation, we get $\sigma(r_n(b)) = 0$ and $b = 0$.

■

The *weight enumerator* of a code C of length n over \mathbb{F}_q is

$$W_C(x, y) = \sum_{i=0}^n A_i x^{n-i} y^i \in \mathbb{Z}[x, y]$$

where A_i is the number of codewords of weight i .

Consider a function ϕ defined over \mathbb{F}_q^n . Following [1], we consider two Fourier transforms $\hat{\phi}_l$ and $\hat{\phi}_r$ defined by

$$\hat{\phi}_l(c) = \sum_{d \in \mathbb{F}_q^n} \Psi(\langle c, d \rangle_{f, \theta, \sigma}) \phi(d)$$

and

$$\hat{\phi}_r(c) = \sum_{d \in \mathbb{F}_q^n} \Psi(\langle d, c \rangle_{f, \theta, \sigma}) \phi(d)$$

where Ψ is the character defined over $\mathbb{F}_q = \mathbb{F}_{p^r}$ by $\Psi(x) = w^{Tr(x)}$ with w a complex primitive root of unity of order the characteristic p of \mathbb{F}_q and Tr is the trace map from \mathbb{F}_q to \mathbb{F}_p defined by $Tr(x) = x + x^p + \dots + x^{p^{r-1}}$.

Lemma 3 Assume that $f(0) \neq 0$. Consider a linear code C of length n over \mathbb{F}_q and a function ϕ defined over \mathbb{F}_q^n . We have the summation formulas

$$\sum_{c \in l(C)} \phi(c) = \frac{1}{|C|} \sum_{c \in C} \hat{\phi}_l(c)$$

and

$$\sum_{c \in r(C)} \phi(c) = \frac{1}{|C|} \sum_{c \in C} \hat{\phi}_r(c).$$

Proof. We denote $\langle \cdot, \cdot \rangle = \langle \cdot, \cdot \rangle_{f, \theta, \sigma}$. We have

$$\sum_{c \in C} \hat{\phi}_l(c) = \sum_{d \in l(C)} \phi(d) \sum_{c \in C} \Psi(\langle c, d \rangle) + \sum_{d \notin l(C)} \phi(d) \sum_{c \in C} \Psi(\langle c, d \rangle).$$

The first term is equal to $\sum_{d \in l(C)} \phi(d) \sum_{c \in C} 1 = |C| \sum_{d \in l(C)} \phi(d)$. Let us prove that the second term of this sum vanishes. Consider $d \notin l(C)$ and ϕ_d the map from C to \mathbb{F}_q which maps c to $\langle c, d \rangle$. This map is a morphism according to Proposition 1, therefore $\sum_{c \in C} \Psi(\langle c, d \rangle) = |Ker(\phi_d)| \sum_{\alpha \in Im(\phi_d)} \Psi(\alpha)$. Furthermore $\langle \cdot, \cdot \rangle$ is non-degenerate and $d \notin l(C)$ therefore $Im(\phi_d) \neq \{0\}$. We conclude using the orthogonality relation for group characters.

The same conclusion holds for $\hat{\phi}_r$ because the map from C to \mathbb{F}_q which maps c to $\langle d, c \rangle_{f, \theta, \sigma}$ is also a morphism.

■

Proposition 3 Consider C a linear code over \mathbb{F}_q of length n . The weight enumerators of $l(C) = l_{f,\theta,\sigma}(C)$ and $r(C) = r_{f,\theta,\sigma}(C)$ are

$$W_{l(C)}(x, y) = \frac{1}{|C|} \sum_{c \in C} \sum_{d \in \mathbb{F}_q^n} \Psi(\langle c, d \rangle_{f,\theta,\sigma}) x^{n-w(d)} y^{w(d)}$$

and

$$W_{r(C)}(x, y) = \frac{1}{|C|} \sum_{c \in C} \sum_{d \in \mathbb{F}_q^n} \Psi(\langle d, c \rangle_{f,\theta,\sigma}) x^{n-w(d)} y^{w(d)}.$$

Proof. Apply Lemma 3 with $\phi : c \mapsto x^{w(c)} y^{n-w(c)}$ ■

4 Central skew module codes and self-duality.

In this section we arrive to the main result of this note about the dual of a central skew module code, that means a code Rg/Rf where f is a monic central polynomial and g is a monic right divisor of f in $R = \mathbb{F}_q[X; \theta]$. We recall that σ is an automorphism of \mathbb{F}_q such that $\sigma^2 = id$.

Proposition 4 Consider g in R and $h \in R$ monic such that $g \cdot h = h \cdot g = f$. Assume that $f = f^\natural$. Consider the skew module code $C = Rg/Rf$ with monic skew generator polynomial g . Then $l(C) = r(C)$ is the skew module code RH/Rf where $H = \sigma(h^\natural)$.

Proof. Let us denote k the dimension of C . We have $\deg(g) = n - k$ and $\deg(h) = k$. As $f(0) \neq 0$, $\deg(h^\natural) = \deg(h) = k$. Consider $i \in \{0, \dots, k-1\}$ and $j \in \{0, \dots, n-k-1\}$.

1. Consider $H = \sigma^{-1}(h^\natural)$. Let us prove that $\langle X^i \cdot g, X^j \cdot H \rangle_{f,\theta,\sigma} = 0$.

We have $\langle X^i \cdot g, X^j \cdot H \rangle_{f,\theta,\sigma} = P(0)$ where P is the remainder in the division of $(X^i \cdot g \cdot \sigma(r_n(X^j \cdot H)))$ by f on the right. Furthermore

$$\begin{aligned} X^i \cdot g \cdot \sigma(r_n(X^j \cdot H)) &= X^i \cdot g \cdot \sigma(X^{n-(k+j)}(X^j \cdot H)^*) \\ &= X^i \cdot g \cdot \theta^{n-k-j}(\theta^j(\sigma(H)^*)) X^{n-(k+j)} \quad \text{because } (X^j \cdot H)^* = \theta^j(H^*) \\ &= X^i \cdot (g \cdot \theta^{n-k}(\sigma(H)^*)) X^{n-(k+j)}. \end{aligned}$$

Furthermore $\theta^{n-k}(\sigma(H)^*) = h \cdot \lambda$ where λ is a non-zero constant. As $g \cdot h = f$ is central, we get $P = 0$ therefore $\langle X^i \cdot g, X^j \cdot H \rangle_{f,\theta,\sigma} = 0$.

2. Consider $H = \sigma(h^\natural)$. Let us prove that $\langle X^j \cdot H, X^i \cdot g \rangle_{f,\theta,\sigma} = 0$. We have

$$\begin{aligned} X^j \cdot H \cdot \sigma(r_n(X^i \cdot g)) &= \sigma(X^j \cdot h^\natural \cdot X^{n-(n-k+i)}(X^i \cdot g)^*) \\ &= \sigma(X^j \cdot h^\natural \cdot \theta^{k-i}(\theta^i(g^*))) X^{k-i} \\ &= \sigma(X^j \cdot 1/\theta^k(h_0)h^* \cdot \theta^k(g^*)) X^{k-i} \\ &= \sigma(X^j \cdot \theta^k(1/h_0)\theta^k(\theta^{n-k}(h^*) \cdot g^*)) X^{k-i}. \end{aligned}$$

Furthermore $\theta^{n-k}(h^*) \cdot g^* = (g \cdot h)^* = 0$ in R/Rf^* , therefore $\langle X^j \cdot H, X^i \cdot g \rangle_{f,\theta,\sigma} = 0$.

3. As $\sigma = \sigma^{-1}$ we get $\sigma(h^\natural) = \sigma^{-1}(h^\natural)$ therefore $l(C) = r(C) = RH/Rf$ where $H = \sigma(h^\natural)$.

■

Proposition 5 (Self-dual skew module equation) Consider g in R and $h \in R$ monic such that $g \cdot h = h \cdot g = f$. Consider the skew module code $C = Rg/Rf$ with monic skew generator polynomial g . The code C is self-dual for $\langle \cdot, \cdot \rangle_{f, \theta, \sigma}$ if, and only if, the skew polynomial h defined by $g \cdot h = h \cdot g = f$ satisfies

$$\sigma(h^\natural) \cdot h = f. \quad (6)$$

In this case we have $f = f^\natural$.

Remark 2 When $f = X^n - \epsilon$ with $\epsilon^2 = 1$, the self-dual skew module equation (6) is called self-dual skew equation (Corollary 1 of [9]) and existence conditions were given in [4] for this equation. In next section, we will give some existence conditions to equation (6) when θ has order 2 and f is any monic central element.

Remark 3 When $\theta = \sigma = id$, one can check that there exists a self-dual polycyclic code for $\langle \cdot, \cdot \rangle_{f, \theta, \sigma}$ if, and only if, the product of the self-reciprocal irreducible factors which divide f is a square. In particular, if $f = X^n - 1$, we recover that there exists a (Euclidean) self-dual cyclic code if and only if q is a power of 2 and n is even (see [10]). Note that in [1], self-dual polycyclic codes for $\langle \cdot, \cdot \rangle_f$ are those for which f is a square (Theorem 3 of [1]) therefore when $f = X^n - 1$, self-dual polycyclic codes for $\langle \cdot, \cdot \rangle_f$ are not (Euclidean) self-dual cyclic codes.

Example 1 Consider $R = \mathbb{F}_4[X; \theta]$ where $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, $\alpha^2 + \alpha + 1 = 0$ and θ is the Frobenius automorphism. There are three central monic polynomials f of degree 8 satisfying $f = f^\natural$: $X^8 + 1$, $X^8 + X^4 + 1$ and $X^8 + X^6 + X^4 + X^2 + 1$. We consider the self dual skew module codes Rg/Rf for the scalar products $\langle \cdot, \cdot \rangle_{f, \theta, id}$. For $f = X^8 + 1$ we obtain the three already known (Euclidean) self-dual θ -cyclic codes. For $f = X^8 + X^4 + 1$ there are 7 self-dual skew module codes Rg/Rf for the scalar products $\langle \cdot, \cdot \rangle_{f, \theta, id}$. For $f = X^8 + X^6 + X^4 + X^2 + 1$, we have 5 self-dual codes and give one of them here : consider $h = X^4 + \alpha X^3 + \alpha X + \alpha$ and $g = h^\natural = X^4 + \alpha X^3 + \alpha X + \alpha^2$. The skew module code $C = Rg/Rf$ is a $[8, 4, 4]_4$ code. As $h^\natural \cdot h = X^8 + X^6 + X^4 + X^2 + 1$, C is self-dual for the scalar product $\langle \cdot, \cdot \rangle_{f, \theta, id}$.

Example 2 Consider $R = \mathbb{F}_9[X; \theta]$ where $\mathbb{F}_9 = \mathbb{F}_2(w)$, $w^2 = w + 1$ and θ is the Frobenius automorphism. There are six monic central polynomials f of degree 6 satisfying $f = f^\natural$: $X^6 + 1$, $X^6 - 1$, $X^6 + X^4 + X^2 + 1$, $X^6 + X^4 + 2X^2 + 2$, $X^6 + 2X^4 + X^2 + 2$ and $X^6 + 2X^4 + 2X^2 + 1$. If $f \in \{X^6 + 1, X^6 + X^4 + X^2 + 1, X^6 + 2X^4 + 2X^2 + 1\}$ there is no self-dual skew module code Rg/Rf for $\langle \cdot, \cdot \rangle_{f, \theta, id}$. Consider $f = X^6 + 2X^4 + X^2 + 2$. The skew polynomial $g = X^3 + w^5 X^2 + w^3 X + w^2$ generates a $[6, 3, 4]_9$ skew module code Rg/Rf which is self-dual for $\langle \cdot, \cdot \rangle_{f, \theta, id}$.

5 Self-dual central skew module codes over \mathbb{F}_{p^2} .

Self-dual θ -cyclic codes and θ -negacyclic codes have been studied over \mathbb{F}_{p^2} in [2, 3]. Using and completing the material developed in these two previous works, we give here a necessary and sufficient condition of existence of self dual skew module codes Rg/Rf for $\langle \cdot, \cdot \rangle_{f, \theta, \sigma}$ when f is a monic central polynomial and $\sigma^2 = id$.

Consider, for a monic central polynomial $f(X^2) \in \mathbb{F}_p[X^2]$ the set :

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

Necessarily if $\mathcal{H}_{f(X^2)}^{(\sigma)}$ is non empty then $f = f^\natural$.

Proposition 6 (Proposition 2 of [3]) Consider \mathbb{F}_q a finite field with $q = p^2$ elements where p is a prime number, $\theta : x \mapsto x^p$ the Frobenius automorphism over \mathbb{F}_{p^2} , $R = \mathbb{F}_q[X; \theta]$. Consider $f(X^2) = f_1(X^2) \cdots f_r(X^2)$ where $f_1(X^2), \dots, f_r(X^2)$ are pairwise coprime polynomials of $\mathbb{F}_p[X^2]$ satisfying $f_i^\natural = f_i$. The application

$$\phi : \begin{cases} \mathcal{H}_{f_1(X^2)}^{(\sigma)} \times \cdots \times \mathcal{H}_{f_r(X^2)}^{(\sigma)} & \rightarrow \mathcal{H}_{f(X^2)}^{(\sigma)} \\ (h_1, \dots, h_r) & \mapsto \text{lcrm}(h_1, \dots, h_r) \end{cases}$$

is bijective.

Example 3 Consider $R = \mathbb{F}_4[X; \theta]$ where $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, $\alpha^2 + \alpha + 1 = 0$, θ is the Frobenius automorphism and $f(X^2) = X^{16} + X^{14} + X^{12} + X^{10} + X^8 + X^6 + X^4 + X^2 + 1 = (X^4 + X^2 + 1)(X^{12} + X^6 + 1)$. Consider $h_1 = X^2 + \alpha$ and $h_2 = X^6 + \alpha^2 X^5 + \alpha X^4 + \alpha X^2 + \alpha^2 X + \alpha^2$. We have $h_1^\natural \cdot h_1 = X^4 + X^2 + 1$ and $h_2^\natural \cdot h_2 = X^{12} + X^6 + 1$. Consider $h = \text{lcrm}(h_1, h_2) = X^8 + \alpha^2 X^7 + X^6 + X^5 + \alpha^2 X^4 + \alpha^2 X^3 + \alpha X^2 + X + \alpha$ then $h^\natural \cdot h = f(X^2)$. The skew module code Rg/Rf with skew generator polynomial $g = h^\natural$ is a self-dual $[16, 8, 6]_4$ for $\langle \cdot, \cdot \rangle_{f, \theta, id}$ and we improve the best distance for all Euclidean self-dual θ -cyclic codes of length 16 over \mathbb{F}_4 (4 according to Section 4 of [7]).

Using the same construction, we get a self-dual $[24, 12, 8]_4$ code for $\langle \cdot, \cdot \rangle_{f, \theta, id}$ with $f(X^2) = X^{24} + X^{22} + X^{12} + X^2 + 1$ and a self-dual $[32, 16, 9]_4$ code for $\langle \cdot, \cdot \rangle_{f, \theta, id}$ with $f(X^2) = X^{32} + X^{22} + X^{20} + X^{18} + X^{16} + X^{14} + X^{12} + X^{10} + 1$. The best Euclidean self-dual θ -cyclic codes over \mathbb{F}_4 of lengths 24 and 32 are $[24, 12, 7]_4$ and $[32, 16, 4]_4$ (Section 4 of [7]).

We now derive necessary and sufficient existence conditions for self-dual skew module codes defined over \mathbb{F}_{p^2} .

Lemma 4 Consider \mathbb{F}_q a finite field with $q = p^2$ elements where p is a prime number, $\theta : x \mapsto x^p$ the Frobenius automorphism over \mathbb{F}_{p^2} , $\sigma \in \{id, \theta\}$, $R = \mathbb{F}_q[X; \theta]$. Consider $f(X^2) = f^\natural(X^2)$ which is either irreducible in $\mathbb{F}_p[X^2]$ or the product of two irreducible polynomials $g(X^2) \neq g^\natural(X^2)$. The set $\mathcal{H}_{f(X^2)}^{(\sigma)}$ is non-empty if, and only if, one of the following conditions is fulfilled :

1. m is even;
2. m is odd and $\deg_{X^2}(f(X^2)) > 1$;
3. m is odd, $p = 2$ and $f = X^2 + 1$;
4. m is odd, p is odd, $\sigma = id$ and $f = X^2 - (-1)^{\frac{p+1}{2}}$;
5. m is odd, p is odd, $\sigma = \theta$ and $f = X^2 + 1$.

Proof.

1. If m is even then $f^{m/2} \in \mathcal{H}_{f(X^2)^m}^{(\sigma)}$.
2. If $\deg_{X^2}(f(X^2)) > 1$, according to Lemma 3.3 and Lemma 3.5 of [3], the set $\mathcal{H}_{f(X^2)}^{(\sigma)}$ is non-empty. Consider $H \in \mathcal{H}_{f(X^2)}^{(\sigma)}$, then $f^{(m-1)/2}H = Hf^{(m-1)/2} \in \mathcal{H}_{f(X^2)^m}^{(\sigma)}$.

3. If m is odd, $p = 2$ and $f = X^2 + 1$, then $(X + 1)^m \in \mathcal{H}_{f(X^2)^m}^{(\sigma)}$.
4. If m is odd, p is odd, $\sigma = id$ and $f = X^2 - \epsilon$, with $\epsilon^2 = 1$, according to Proposition 2 of [2], the set $\mathcal{H}_{f(X^2)^m}^{(\sigma)}$ is non-empty if and only if $(-1)^{\frac{p+1}{2}} = \epsilon$.
5. Assume that m is odd, p is odd, $\sigma = \theta$ and $f = X^2 - \epsilon$, with $\epsilon^2 = 1$. The set $\mathcal{H}_{f(X^2)^m}^{(\sigma)}$ is the disjoint union $\sqcup_{j=0}^{(m-1)/2} f(X^2)^j \overline{\mathcal{H}^{(\sigma)}_{f(X^2)^{m-2j}}}$ where for $i \geq 0$, $\overline{\mathcal{H}^{(\sigma)}_{f(X^2)^i}} := \{h \in \mathcal{H}_{f(X^2)^i}^{(\sigma)} \mid f(X^2) \nmid h\}$ is the set of elements of $\mathcal{H}_{f(X^2)^i}^{(\sigma)}$ which are not divisible by $f(X^2) = X^2 - \epsilon$. One can adapt the proof of Lemma 4.1 of [2] to get that for $i \geq 1$, the set $\overline{\mathcal{H}^{(\sigma)}_{f(X^2)^i}}$ is non-empty if and only if $\epsilon = -1$. The conclusion follows.

■

Proposition 7 Consider \mathbb{F}_q a finite field with $q = p^2$ elements where p is an odd prime number, $\theta : x \mapsto x^p$ the Frobenius automorphism over \mathbb{F}_{p^2} , $\sigma \in \{id, \theta\}$, $R = \mathbb{F}_q[X; \theta]$. Consider $f(X^2) = f^{\natural}(X^2)$ in $\mathbb{F}_p[X^2]$. Consider $m_1, m_2 \in \mathbb{N}$ such that $f(X^2) = (X^2 - 1)^{m_1}(X^2 + 1)^{m_2}F(X^2)$ and F is not divisible by $X^2 + 1$ or $X^2 - 1$. There exists a self-dual skew module code Rg/Rf for $\langle \cdot, \cdot \rangle_{f, \theta, \sigma}$ if, and only if, one of these conditions is satisfied :

- m_1 and m_2 are even;
- m_1 is odd, m_2 is even, $p \equiv 3 \pmod{4}$, $\sigma = id$;
- m_1 is even, m_2 is odd, $p \equiv 1 \pmod{4}$, $\sigma = id$;
- m_1 is even, m_2 is odd, $\sigma = \theta$.

Proof. The proof is deduced from Proposition 6 and Lemma 4.

■

Example 4 In Example 2, we have seen that there is no self-dual skew module code Rg/Rf over \mathbb{F}_9 for the scalar product $\langle \cdot, \cdot \rangle_{f, \theta, id}$ when $f(X^2)$ is one of the following monic central polynomials : $X^6 + 1 = (X^2 + 1)^3$, $X^6 + X^4 + X^2 + 1 = (X^2 + 1)(X^4 + 1)$ and $X^6 + 2X^4 + 2X^2 + 1 = (X^2 + 1)(X^2 - 1)^2$ while there exists a self-dual skew module code Rg/Rf over \mathbb{F}_9 if $f(X^2)$ is one of the following monic central polynomials : $X^6 - 1 = (X^2 - 1)^3$, $X^6 + X^4 + 2X^2 + 2 = (X^2 + 1)^2(X^2 - 1)$ and $X^6 + 2X^4 + X^2 + 2 = (X^2 - 1)(X^4 + 1)$.

6 Conclusion.

In this note, inspired by [1], we have constructed a new notion of duality for polycyclic codes and for central skew module codes. With this new notion of duality, we consider self-dual central θ -module codes Rg/Rf for any monic central self-reciprocal skew polynomial f . When $f = X^n - \epsilon$ with $\epsilon^2 = 1$, we get Euclidean and Hermitian self-dual θ -constacyclic codes. When the order of θ is 2, we give necessary and sufficient existence conditions of self-dual central skew module codes by using the results previously obtained in [2, 3]. It could be interesting to study these self-dual codes more deeply for any monic central skew polynomial $f \neq X^n - \epsilon$, especially when the automorphism θ has an order $\neq 1, 2, n$.

Acknowledgements

I thank Steve Dougherty for encouraging me to look at this topic during 2021 ACA conference. I thank the referees for their remarks and suggestions.

References

- [1] A. Alahmadi, S. Dougherty, A. Leroy and P. Solé. On the duality and the direction of polycyclic codes. *Advances in Mathematics of Communications*, 10, 4, 921–929, 2016.
- [2] D. Boucher. Construction and number of self-dual skew codes over \mathbb{F}_{p^2} . *Adv. Math. Commun.*, 10(4):765–795, 2016.
- [3] D. Boucher. A first step towards the skew duadic codes. *Adv. Math. Commun.*, 12(3):553–577, 2018.
- [4] D. Boucher. A note on the existence of self-dual skew codes over finite fields. In *Codes, cryptology, and information security*, volume 9084 of *Lecture Notes in Comput. Sci.*, pages 228–239. Springer, Cham, 2015.
- [5] D. Boucher, W. Geiselmann, and F. Ulmer. Skew-cyclic codes. *Appl. Algebra Engrg. Comm. Comput.*, 18(4):379–389, 2007.
- [6] D. Boucher and F. Ulmer. Codes as modules over skew polynomial rings. In *Cryptography and coding*, volume 5921 of *Lecture Notes in Comput. Sci.*, pages 38–55. Springer, Berlin, 2009.
- [7] D. Boucher and F. Ulmer. Coding with skew polynomial rings. *J. Symbolic Comput.*, 44(12):1644–1656, 2009.
- [8] D. Boucher and F. Ulmer. A note on the dual codes of module skew codes. In *Cryptography and coding*, volume 7089 of *Lecture Notes in Comput. Sci.*, pages 230–243. Springer, Heidelberg, 2011.
- [9] D. Boucher and F. Ulmer. Self-dual skew codes and factorization of skew polynomials. *J. Symbolic Comput.*, 60:47–61, 2014.
- [10] Y. Jia, S. Ling and C. Xing. On self-dual cyclic codes over finite fields. *IEEE Trans. Inform. Theory*, **57** (2011), 2243–2251.
- [11] M. Matsuoka. θ -polycyclic codes and θ -sequential codes over finite fields. *Int. J. Algebra*, 5 (2011), 65–70.
- [12] O. Ore. Theory of non-commutative polynomials. *Annals of Mathematics. Second Series*, 34, 1933, 3, 480–508.
- [13] N. J. A. Sloane and J. G. Thompson. Cyclic self-dual codes. *IEEE Trans. Inform. Theory*, **29** (1983), 364–366.
- [14] S. Szabo and J. A. Wood. Properties of dual codes defined by nondegenerate forms. *J. Algebra Comb. Discrete Struct. Appl.*, 4, 2, 105–113, 2017.