

MDS Triple skew cyclic codes

Rachid Mammeri, Nabil Benneni[✉] and Aicha Batoul

ABSTRACT

The present paper gives a detailed study of the structural theory of triple θ -skew cyclic codes where the codes are over \mathbb{F}_q . We give a complete characterization of these codes, focusing on their representation as modules. We identify the generator polynomials for the triple skew-cyclic codes as well as those of their duals. We explore the properties of these generator polynomials and their relationship to the code's structure. Additionally, To illustrate our approach, we give concrete instances of triple θ -skew cyclic codes to demonstrate how these structures can behave in practice. The special instances we present reveal that such codes are capable of achieving strong parameters under certain conditions.

Keywords: skew cyclic code, triple θ -skew cyclic code, dual computational results

2020 Mathematics Subject Classification: 94B05, 94B15, 16S36.

1. Introduction

The developments in coding theory over finite rings, particularly finite chain rings [2, 3], have drawn the interest of numerous researchers since the early 1970s, taking advantage of the algebraic richness of finite rings, the present work extends the classical framework of coding theory formulated over \mathbb{F}_q [15].

Cyclic codes have served as a fundamental aspect of coding theory since their introduction, providing elegant algebraic structures along with efficient encoding and decoding algorithms [12]. These codes characterized by their invariance under cyclic shifts, have been extensively studied over finite fields and rings, enabling many practical applications in communication networks and storage technologies [14]. The classical framework of

* Corresponding author.

Received 07 Oct 2025; Revised 20 Mar 2026; Accepted 26 Mar 2026; Published Online 20 May 2026.

DOI: [10.61091/jmcc130-22](https://doi.org/10.61091/jmcc130-22)

© 2026 The Author(s). Published by Combinatorial Press. This is an open access article under the CC BY license (<https://creativecommons.org/licenses/by/4.0/>).

cyclic codes was later extended to skew-cyclic codes with respect to θ by introducing the ring of skew-polynomial, enabling non-commutative algebraic constructions. This generalization, pioneered by [6, 7, 8]. The exploration of multi-component cyclic codes began with double cyclic codes, which partition coordinates into two cyclic subsets in [5] characterized \mathbb{Z}_2 -double cyclic codes as $\mathbb{Z}[x]$ -submodules, while [9] extended this to \mathbb{Z}_4 . Further innovations emerged with double θ -skew cyclic codes, combining skew polynomial rings with multi-component structures. Aydogdu et al. [1] recently established the algebraic foundations of these codes over \mathbb{F}_q , determining generator polynomials and duals under Frobenius automorphisms. Concurrently, triple cyclic codes were introduced as a three-component generalization. Mostafanasab [13] investigated their structure over \mathbb{Z}_2 , demonstrating their representation as $\mathbb{Z}_2[x]$ -submodules and analyzing duality. However, the integration of skew cyclic properties into multi-component frameworks remains underexplored, particularly for triple-length codes. This gap motivates our work on triple θ -skew cyclic codes, which unify the algebraic richness of skew polynomial rings with the flexibility of tripartite cyclic structures, by the same method in [4] we investigate a relationship between the ring $\mathbb{F}_q[x, \theta]$ and $\mathbb{F}_q[x, \theta, \delta]$ and we construct a generator polynomial for triple (θ) -skew cyclic codes over \mathbb{F}_q , derived from the factorization of skew polynomials under Frobenius automorphisms, alongside the characterization of its dual via a reciprocal polynomial relationship in the non-commutative setting. This work bridges the gap between multi-component cyclic codes and skew algebraic structures, offering new tools for code design in asymmetric communication channels and quantum-resistant cryptography. Our results generalize earlier findings on double skew cyclic codes [1] and triple cyclic codes [13], while introducing novel techniques for handling three-dimensional skew cyclic invariance.

The paper is arranged as below: Section 2 includes fundamental definitions and notation. Section 3 we define the triple θ -skew cyclic codes over \mathbb{F}_q of length $n = \alpha + \beta + \gamma$. Section 4 is for the dual of this kind of codes. Section 5 We present some examples of optimal and maximum distance separable (MDS) codes (α, β, γ) over $\mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q$ illustrating how these codes can attain strong parameters in specific cases.

2. Preliminaries

Let \mathbb{F}_q be a finite field with q elements with $q = p^m$ such that p is a prime and m is a positive integer. We define the noncommutative ring $\mathbb{F}_q[x, \theta, \delta]$ as the set of polynomials

$$\{a_\alpha x^\alpha + \cdots + a_1 x + a_0 : a_i \in \mathbb{F}_q\}.$$

The structure of the ring is determined by:

- θ , which is an automorphism defined as a power of the Frobenius map ($z \mapsto z^p$).
- δ , which is a θ -derivation given by $\delta(c) = \theta(c) - c$, with $c \in \mathbb{F}_q$. Also known as an inner derivation.
- In several instances, we replaced δ with δ_a , where δ_a is the θ -derivation defined by

$$\delta_a(b) = ab - \theta(b)a, \quad \text{for all } b \in \mathbb{F}_q.$$

In $\mathbb{F}_q[x, \theta, \delta]$, addition is performed using standard polynomial addition, whereas multiplication is defined iteratively, beginning with the relation

$$x \cdot c = \theta(c)x + \delta(c), \quad \text{for all } c \in \mathbb{F}_q,$$

and this extension applies to every element in the ring via the associativity and distributivity axioms. This construction gives us the ring of skew polynomial with derivation, the elements of this ring are simply referred to as skew polynomials.

The ring $\mathbb{F}_q[x, \theta, \delta]$ possesses both left-Euclidean and right-Euclidean structures, meaning that every left and right ideal in this ring is principal, generated by a single element.

Take $f, g \in \mathbb{F}_q[x, \theta, \delta]$ satisfy $\deg f = n$ suppose that $g \mid_r f$ and $f = hg$ for some $h \in \mathbb{F}_q[x, \theta, \delta]$, then the set $\mathcal{C} = \frac{\mathbb{F}_q[x, \theta, \delta]g}{\mathbb{F}_q[x, \theta, \delta]f}$, is a left $\mathbb{F}_q[x, \theta, \delta]$ -submodule of the quotient module $\frac{\mathbb{F}_q[x, \theta, \delta]}{\mathbb{F}_q[x, \theta, \delta]f}$, and is known as a θ -module-code. This code is of length $n = \deg(f)$ and its dimension is $k = \deg(f) - \deg(g)$.

If $f = x^n - 1$ and g is right divisor of $x^n - 1$, then \mathcal{C} is θ -cyclic, for more details see [7].

A code $\mathcal{C} \subseteq \mathbb{F}_q^\alpha$ is called a skew-cyclic code (relative to the automorphism θ) if \mathcal{C} is linear over \mathbb{F}_q and for every codeword $c = (c_0, c_1, \dots, c_{\alpha-1}) \in \mathcal{C}$, it follows that the θ -skew shift

$$(\theta(c_{\alpha-1}), \theta(c_0), \dots, \theta(c_{\alpha-2})),$$

also a member of \mathcal{C} .

Proposition 2.1. [11] *Let n be a positive integer and λ be a unit in R . Then the following statements are equivalent:*

- (a) $x^n - \lambda$ is central in $R[x; \theta]$.
- (b) $\langle x^n - \lambda \rangle$ is two-sided.
- (c) n is a multiple of the order of σ and λ is fixed by σ .

If $|\langle \theta \rangle|/\alpha$ then $\mathbb{S}_\alpha = \frac{\mathbb{F}_q[x, \theta]}{(x^\alpha - 1)}$, is a ring, provided that $(x^\alpha - 1)$ is a two-sided ideal, the ideal $(x^\alpha - 1)$ in $\mathbb{F}_q[x, \theta]$ is two-sided precisely when $x^\alpha - 1$ lies in the center of the ring. In this paper we assume that $|\langle \theta \rangle|/\gcd(\alpha, \beta, \gamma)$.

Every left ideal $I \subseteq \mathbb{S}_\alpha$ is an ideal generated by $(I(x) + \langle x^\alpha - 1 \rangle)$ where $I(x) \mid_r (x^\alpha - 1)$ in $\mathbb{F}_q[x, \theta]$ (see[6], Theorem 1).

For $g(x) + (x^\alpha - 1) \in \mathbb{S}_\alpha$ and $l(x) \in \mathbb{F}_q[x, \theta]$, define the left multiplication \star

$$l(x) \star (g(x) + (x^\alpha - 1)) = l(x)g(x) + (x^\alpha - 1).$$

To represente vectors in \mathbb{F}_q^α with polynomials in \mathbb{S}_α , we use the isomorphism:

$$\begin{aligned} \xi : \mathbb{F}_q^\alpha &\rightarrow \mathbb{F}_q[x, \theta]/(x^\alpha - 1), \\ (c_0, c_1, \dots, c_{\alpha-1}) &\mapsto c_0 + c_1x + c_2x^2 + \dots + c_{\alpha-1}x^{\alpha-1}. \end{aligned}$$

This ξ is an $\mathbb{F}_q[x, \theta]$ -module isomorphism, allowing vectors and polynomials to be identified seamlessly.

We consider the set $\mathcal{S} = \mathbb{F}_q^\alpha \times \mathbb{F}_q^\beta \times \mathbb{F}_q^\gamma = \{(a_1|a_2|a_3) : a_1 \in \mathbb{F}_q^\alpha, a_2 \in \mathbb{F}_q^\beta, a_3 \in \mathbb{F}_q^\gamma\}$ where α, β and γ are positives integers.

Let $(c|c'|c'') \in \mathbb{F}_q^\alpha \times \mathbb{F}_q^\beta \times \mathbb{F}_q^\gamma$, $u \in \mathbb{F}_q$ and the operation "." defined by :

$$\begin{aligned} \mathbb{F}_q \times (\mathbb{F}_q^\alpha \times \mathbb{F}_q^\beta \times \mathbb{F}_q^\gamma) &\rightarrow \mathbb{F}_q^\alpha \times \mathbb{F}_q^\beta \times \mathbb{F}_q^\gamma, \\ u.(c|c'|c'') &\rightarrow (uc|uc'|uc''). \end{aligned}$$

It is clear that \mathcal{S} is a left \mathbb{F}_q -module with the addition and the external operation ".", this is a left \mathbb{F}_q -module with $q^{\alpha+\beta+\gamma}$ elements.

Now let $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^\alpha \times \mathbb{F}_q^\beta \times \mathbb{F}_q^\gamma$, where

$$\mathbf{u} = (u_0, \dots, u_{\alpha-1}|u'_0, \dots, u'_{\beta-1}|u''_0, \dots, u''_{\gamma-1}),$$

and

$$\mathbf{v} = (v_0, \dots, v_{\alpha-1}|v'_0, \dots, v'_{\beta-1}|v''_0, \dots, v''_{\gamma-1}).$$

Define $\langle \mathbf{u}, \mathbf{v} \rangle$ as

$$\begin{aligned} \langle \mathbf{u}, \mathbf{v} \rangle &= (u_0, \dots, u_{\alpha-1}|u'_0, \dots, u'_{\beta-1}|u''_0, \dots, u''_{\gamma-1}).(v_0, \dots, v_{\alpha-1}|v'_0, \dots, v'_{\beta-1}|v''_0, \dots, v''_{\gamma-1}) \\ &= \sum_{i=0}^{\alpha} u_i v_i + \sum_{j=0}^{\beta} u'_j v'_j + \sum_{k=0}^{\gamma} u''_k v''_k. \end{aligned}$$

Let $\mathcal{C} \subseteq \mathbb{F}_q^\alpha \times \mathbb{F}_q^\beta \times \mathbb{F}_q^\gamma$ be a code of length (α, β, γ) . Its dual is defined by

$$\mathcal{C}^\perp = \{u \in \mathbb{F}_q^\alpha \times \mathbb{F}_q^\beta \times \mathbb{F}_q^\gamma \mid \langle u, v \rangle = 0 \text{ for all } v \in \mathcal{C}\},$$

where $\langle u, v \rangle$ denotes the standard inner product.

Let $\mathcal{C} \subseteq \mathbb{F}_q^n$. Then \mathcal{C} is called a skew-cyclic code of length n over \mathbb{F}_q if whenever

$$(c_1, c_2, \dots, c_n) \in \mathcal{C},$$

it follows that

$$(\theta(c_n), \theta(c_1), \dots, \theta(c_{n-1})) \in \mathcal{C}.$$

The set $\mathbb{S}_{\alpha, \beta, \gamma} = \mathbb{S}_\alpha \times \mathbb{S}_\beta \times \mathbb{S}_\gamma = \frac{\mathbb{F}_q[x, \theta]}{(x^\alpha - 1)} \times \frac{\mathbb{F}_q[x, \theta]}{(x^\beta - 1)} \times \frac{\mathbb{F}_q[x, \theta]}{(x^\gamma - 1)}$, is a ring if the ideals $(x^\alpha - 1)$, $(x^\beta - 1)$ and $(x^\gamma - 1)$ are both left and right ideals, it means that the ordre of θ divide α , β and γ .

Moreover We define the operation \star :

$$\begin{aligned} \star : \mathbb{F}_q[x, \theta] \times \mathbb{S}_{\alpha, \beta, \gamma} &\rightarrow \mathbb{S}_{\alpha, \beta, \gamma} \\ k(x) \star (g(x) \mid h(x) \mid l(x)) & \\ &= (k(x)g(x) \bmod (x^\alpha - 1) \mid k(x)h(x) \bmod (x^\beta - 1) \mid k(x)l(x) \bmod (x^\gamma - 1)), \end{aligned}$$

where $k(x) \in \mathbb{F}_q[x, \theta]$ and $(g(x) \mid h(x) \mid l(x)) \in \mathbb{S}_{\alpha, \beta, \gamma}$. Clearly that $\mathbb{S}_\alpha \times \mathbb{S}_\beta \times \mathbb{S}_\gamma$ is a left $\mathbb{F}_q[x, \theta]$ -module with the external operation \star .

The map given by :

$$\begin{aligned} (c_0, \dots, c_{\alpha-1} \mid c'_0, \dots, c'_{\beta-1} \mid c''_0, \dots, c''_{\gamma-1}) & \\ \rightarrow (c_0 + \dots + c_{\alpha-1}x^{\alpha-1} \mid (c'_0 + \dots + c'_{\beta-1}x^{\beta-1}) \mid (c''_0 + \dots + c''_{\gamma-1}x^{\gamma-1})), & \end{aligned}$$

is a map between $\mathbb{F}_q^\alpha \times \mathbb{F}_q^\beta \times \mathbb{F}_q^\gamma$ and $\mathbb{S}_{\alpha, \beta, \gamma}$ and it is an $\mathbb{F}_q[x, \theta]$ -module isomorphism, that enables us to identify the vectors with polynomials.

3. Triple θ -skew cyclic code

In what follows, triple skew-cyclic codes over \mathbb{F}_q are investigated from an algebraic standpoint, and their generator polynomials are given.

From now on, we note $\mathbb{S}_k = \frac{\mathbb{F}_q[x, \theta]}{\langle (x^k - 1) \rangle}$ where $k = \alpha, \beta, \gamma$ and m .

Also, $\mathbb{S}_{\alpha, \beta, \gamma} = \frac{\mathbb{F}_q[x, \theta]}{\langle (x^\alpha - 1) \rangle} \times \frac{\mathbb{F}_q[x, \theta]}{\langle (x^\beta - 1) \rangle} \times \frac{\mathbb{F}_q[x, \theta]}{\langle (x^\gamma - 1) \rangle}$.

Definition 3.1. Let \mathcal{C} be a cyclic code over \mathbb{F}_q , if any

$$\mathbf{u} = (c_0, \dots, c_{\alpha-1}, c'_0, \dots, c'_{\beta-1}, c''_0, \dots, c''_{\gamma-1}) \in \mathcal{C},$$

implies that

$$(\theta(c_{\alpha-1}), \theta(c_0), \dots, \theta(c_{\alpha-2}), \theta(c'_{\beta-1}), \theta(c'_0), \dots, \theta(c'_{\beta-2}), \theta(c''_{\gamma-1}), \theta(c''_0), \dots, \theta(c''_{\gamma-2})) \in \mathcal{C},$$

then \mathcal{C} is triple skew-cyclic codes over \mathbb{F}_q of length $n = \alpha + \beta + \gamma$.

To analyze the algebraic structural properties of this kind of codes, together with a determination of their canonical generators we dives into this lemma :

Lemma 3.2. ([6]) \mathcal{C} is a skew-cyclic code of length $n \iff \mathcal{C}$ is a left ideal of \mathbb{S}_n

The following lemma is immediately apparent from the formulation of a \mathbb{F}_q -triple θ -skew cyclic code.

Lemma 3.3. The following are equivalent for $\mathcal{C} \in \mathbb{S}_{\alpha, \beta, \gamma}$

- \mathcal{C} is an \mathbb{F}_q -triple θ -skew cyclic code
- \mathcal{C} is left $\mathbb{F}_q[x, \theta]$ -submodule of $\mathbb{S}_{\alpha, \beta, \gamma}$

Theorem 3.4. let \mathcal{C} be an \mathbb{F}_q -triple θ -skew cyclic code then \mathcal{C} is of the form :

$$\mathcal{C} = \langle ((A_1(x)|0|0)), ((0|A_2(x)|0)) | ((B_1(x)|B_2(x)|A_3(x))) \rangle,$$

where $A_1(x)$ is a monic right divisor of $x^\alpha - 1$ and $A_2(x)$ is a monic right divisor of $x^\beta - 1$ and $A_3(x)$ is a monic right divisor of $x^\gamma - 1$, $B_1(x) \in \mathbb{S}_\alpha$, $B_2(x) \in \mathbb{S}_\beta$, $\deg(B_1(x)) < \deg(A_1(x))$ and $\deg(B_2(x)) < \deg(A_2(x))$.

Proof. Let \mathcal{C} be an \mathbb{F}_q -triple (θ, δ) -skew cyclic code. The canonical surjection

$$\phi : \mathcal{C} \rightarrow \mathbb{S}_\gamma(b_1(x)|b_2(x)|b_3(x)) \rightarrow b_3(x),$$

is a homomorphism of left $\mathbb{F}_q[x, \theta]$ -modules. Since $Im(\phi)$ is an ideal of \mathbb{S}_γ , consequently, one can find $A_3(x) \in \mathbb{F}_q[x, \theta, \delta]$ with the property that $A_3(x)$ is a monic right divisor of $x^\gamma - 1$, so $Im(\phi) = \langle A_3(x) \rangle$, it's clear that $ker(\phi) = \{(b_1(x)|b_2(x)|0) \in \mathbb{S}_{\alpha, \beta, \gamma} | (b_1(x)|b_2(x)|0) \in \mathcal{C}\}$. Define the set J to be :

$$J = \{(b_1(x)|b_2(x)) \in \mathbb{S}_{\alpha, \beta} | (b_1(x)|b_2(x)|0) \in Ker(\phi)\}.$$

It is straightforward to verify that J is a left ideal of $\mathbb{S}_{\alpha,\beta}$, then $J = J_1 \times J_2$ for some ideal $J_1 \subseteq \mathbb{S}_\alpha$ and $J_2 \subseteq \mathbb{S}_\beta$.

Note that $\mathbb{S}_{\alpha,\beta} = \mathbb{S}_\alpha \times \mathbb{S}_\beta$ is a direct product ring, with componentwise addition and multiplication:

$$(u_1, u_2) + (v_1, v_2) = (u_1 + v_1, u_2 + v_2), \quad (u_1, u_2)(v_1, v_2) = (u_1v_1, u_2v_2).$$

In particular, $(1, 0)$ and $(0, 1)$ are central idempotents in $\mathbb{S}_{\alpha,\beta}$.

Define

$$J_1 := \{u \in \mathbb{S}_\alpha \mid \exists v \in \mathbb{S}_\beta \text{ such that } (u, v) \in J\},$$

$$J_2 := \{v \in \mathbb{S}_\beta \mid \exists u \in \mathbb{S}_\alpha \text{ such that } (u, v) \in J\}.$$

Then J_1 is a left ideal of \mathbb{S}_α and J_2 is a left ideal of \mathbb{S}_β . Moreover,

$$J = J_1 \times J_2.$$

Indeed, if $(u, v) \in J$, since J is a left ideal of $\mathbb{S}_{\alpha,\beta}$ we have

$$(u, 0) = (1, 0)(u, v) \in J, \quad (0, v) = (0, 1)(u, v) \in J,$$

and hence $(u, v) = (u, 0) + (0, v) \in J_1 \times J_2$, so $J \subseteq J_1 \times J_2$. Conversely, if $u \in J_1$ and $v \in J_2$, choose v' and u' such that $(u, v') \in J$ and $(u', v) \in J$. Then $(u, 0) = (1, 0)(u, v') \in J$ and $(0, v) = (0, 1)(u', v) \in J$, so $(u, v) = (u, 0) + (0, v) \in J$. Thus $J_1 \times J_2 \subseteq J$, proving $J = J_1 \times J_2$.

There are a skew polynomials $A_1(x), A_2(x)$ such that $A_1(x), A_2(x)$ are a monic right divisors of $x^\alpha - 1$ and $x^\beta - 1$, respectively, such that $J_1 = \langle A_1(x) \rangle, J_2 = \langle A_2(x) \rangle$, therefor $J = \langle (A_1(x)|0), (0|A_2(x)) \rangle$. Now we can see easy that $\ker(\phi) = \langle (A_1|0|0), (0|A_2|0) \rangle$, by the first isomorphism theorem, we have :

$$\frac{\mathcal{C}}{\text{Ker}(\phi)} \simeq \langle A_3(x) \rangle.$$

Let $(B_1(x)|B_2(x)|A_3(x)) \in \mathcal{C}$ then $\phi((B_1(x)|B_2(x)|A_3(x))) = A_3(x)$ then

$$\mathcal{C} = \langle ((A_1(x)|0|0)), ((0|A_2(x)|0)) | ((B_1(x)|B_2(x)|A_3(x))) \rangle.$$

By the right division algorithm, there exist polynomials such that, $B_1(x) = q_1(x)A_1(x) + r_1(x)$, with

$\deg(r_1(x)) < \deg(A_1(x))$, and $B_2(x) = q_2(x)A_2(x) + r_2(x)$, with $\deg(r_2(x)) < \deg(A_2(x))$.

It follows that $(r_1(x) | r_2(x) | A_3(x)) = (B_1(x) - q_1(x)A_1(x) | B_2(x) - q_2(x)A_2(x) | A_3(x)) = (B_1(x) | B_2(x) | A_3(x)) - q_1(x)(A_1(x) | 0 | 0) - q_2(x)(0 | A_2(x) | 0) \in \mathcal{C}$. Therefore, we may assume that $\deg(B_1(x)) < \deg(A_1(x))$ and $\deg(B_2(x)) < \deg(A_2(x))$. □

There is a relationship between the ring $\mathbb{F}_q[x, \theta] \times \mathbb{F}_q[x, \theta] \times \mathbb{F}_q[x, \theta]$ and $\mathbb{F}_q[x, \theta, \delta_a] \times \mathbb{F}_q[x, \theta, \delta_a] \times \mathbb{F}_q[x, \theta, \delta_a]$, using the change of variables $y = x + a$ to transform the ring $\mathbb{F}_q[x, \theta, \delta_a] \times \mathbb{F}_q[x, \theta, \delta_a] \times \mathbb{F}_q[x, \theta, \delta_a]$ into the pure-automorphism ring $\mathbb{F}_q[y, \theta] \times \mathbb{F}_q[y, \theta] \times \mathbb{F}_q[y, \theta]$. If $\delta_a = 0$, then these two rings become the same.

The factorization of $(x^\alpha - 1)$, $(x^\beta - 1)$ and $(x^\gamma - 1)$ over $\mathbb{F}_q[x, \theta, \delta_a]$ are not unique. We use the change of variables $y = x + a$ to transform the rings $\mathbb{F}_q[x, \theta, \delta_a]$ into the pure-automorphism rings $\mathbb{F}_q[y, \theta]$. We then obtain the factorizations of $(y^\alpha - 1)$, $(y^\beta - 1)$ and $(y^\gamma - 1)$ over the new rings and they are the same as the factorizations of $(y^\alpha - 1)$, $(y^\beta - 1)$ and $(y^\gamma - 1)$ over $\mathbb{F}_q[x, \theta, \delta_a]$. For this correspondence we have:

Proposition 3.5. *The map*

$$\Psi : \mathbb{F}_q[x; \theta, \delta_a] \longrightarrow \mathbb{F}_q[y, \theta], \quad \Psi(c) = c \ (c \in \mathbb{F}_q), \quad \Psi(x) = y - a,$$

is a ring isomorphism. Equivalently, for $f(x) = \sum_{i=0}^t c_i x^i$ one has

$$\Psi \left(\sum_{i=0}^t c_i x^i \right) = \sum_{i=0}^t c_i (y - a)^i.$$

Its inverse is given by $\Psi^{-1}(c) = c$ and $\Psi^{-1}(y) = x + a$.

Proof. Let $R = \mathbb{F}_q[x, \theta, \delta_a]$ and $S = \mathbb{F}_q[y; \theta]$, where $\delta_a(c) = \theta(c)a - ac \quad (c \in \mathbb{F}_q)$.

Recall that R is generated by \mathbb{F}_q and x subject to the rule $xc = \theta(c)x + \delta_a(c) \quad (c \in \mathbb{F}_q)$, and S is generated by \mathbb{F}_q and y subject to

$$yc = \theta(c)y \quad (c \in \mathbb{F}_q).$$

Define Ψ on generators by $\Psi(c) = c$ for $c \in \mathbb{F}_q$ and $\Psi(x) = y - a$. To see that this extends to a ring homomorphism $R \rightarrow S$, it suffices to check that the defining relation of R is preserved. For $c \in \mathbb{F}_q$ we compute in S :

$$\Psi(x)c = (y - a)c = yc - ac = \theta(c)y - ac = \theta(c)(y - a) + \theta(c)a - ac = \theta(c)\Psi(x) + \delta_a(c).$$

Since $\Psi(\theta(c)x + \delta_a(c)) = \theta(c)\Psi(x) + \delta_a(c)$, we obtain

$$\Psi(xc) = \Psi(\theta(c)x + \delta_a(c)),$$

so Ψ is a well-defined ring homomorphism.

Define $\Psi^{-1} : S \rightarrow R$ by $\Psi^{-1}(c) = c$ for $c \in \mathbb{F}_q$ and $\Psi^{-1}(y) = x + a$. Again, it suffices to verify the defining relation of S : for $c \in \mathbb{F}_q$, using $xc = \theta(c)x + \delta_a(c)$ in R ,

$$(x + a)c = xc + ac = \theta(c)x + \delta_a(c) + ac = \theta(c)x + \theta(c)a - ac + ac = \theta(c)(x + a).$$

Hence $\Psi^{-1}(y)c = \theta(c)\Psi^{-1}(y)$, so Ψ^{-1} is a well-defined ring homomorphism.

Finally,

$$\Psi^{-1}(\Psi(x)) = \Psi^{-1}(y - a) = x \quad \text{and} \quad \Psi(\Psi^{-1}(y)) = \Psi(x + a) = y,$$

and both maps fix \mathbb{F}_q . Therefore Ψ and Ψ^{-1} are inverses, and Ψ is a ring isomorphism. □

From Theorem 3.4 and the ring homomorphism Ψ , we have the following corollary which classifies all:

Corollary 3.6. *Let \mathcal{C} triple θ -skew cyclic code over \mathbb{F}_q generated by*

$$\mathcal{C} = \langle ((A_1(x)|0|0)), ((0|A_2(x)|0)) | ((B_1(x)|B_2(x)|A_3(x))) \rangle,$$

then $\mathcal{C} = \langle ((A_1(y)|0|0)), ((0|A_2(y)|0)) | ((B_1(y)|B_2(y)|A_3(y))) \rangle$ where $A_1(y), A_2(y)$ and $A_3(y)$ are monic right divisor of $y^\alpha - 1, y^\beta - 1$ and $y^\gamma - 1$ respectively, $B_1(y)$ and $B_2(y) \in \frac{\mathbb{F}_q[y;\theta]}{(y^\alpha-1)}$ and $\frac{\mathbb{F}_q[y;\theta]}{(y^\beta-1)}$ respectively, also $\deg B_1(y) < \deg A_1(y)$ and $\deg B_2(y) < \deg A_2(y)$.

Example 3.7. Let $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$ with $\omega^2 = \omega + 1$. Let $\theta(\alpha) = \alpha^2$ for $\alpha \in \mathbb{F}_4$, and let δ_{ω^2} be the derivation defined by $\delta_{\omega^2}(b) = \theta(b)\omega^2 - \omega^2b$.

Consider the triple θ -skew cyclic code over $\mathbb{F}_4[x, \theta, \delta_{\omega^2}]$:

$$\mathcal{C} = \langle ((x^2 + \omega^2 | 0 | 0)), ((0 | x^2 + x | 0)) | ((1 | \omega | x + \omega^2)) \rangle.$$

Apply the change of variables $y = x + \omega^2$, transforming the ring $\mathbb{F}_4[x, \theta, \delta_{\omega^2}]$ into $\mathbb{F}_4[y, \theta]$ via the homomorphism Ψ :

$$\Psi(x) = y - \omega^2, \quad \phi \left(\sum a_i x^i \right) = \sum a_i (y - \omega^2)^i.$$

Transformations:

- $\Psi (x^2 + \omega^2) = (y - \omega^2)^2 + \omega^2 = y^2 + \omega + \omega^2 = y^2 + 1$
- $\Psi (x^2 + x) = (y - \omega^2)^2 + (y - \omega^2) = y^2 + \omega + y - \omega^2 = y^2 + y + 1$
- $\Psi (1) = 1, \Psi (\omega) = \omega, \Psi (x + \omega^2) = y$

The transformed code over $\mathbb{F}_4[y, \theta]$ is:

$$\tilde{\mathcal{C}} = \langle ((y^2 + 1 | 0 | 0)), ((0 | y^2 + y + 1 | 0)) | ((1 | \omega | y)) \rangle.$$

From now on, we note $\mathbb{S}_k = \frac{\mathbb{F}_q[x,\theta]}{\langle (x^k-1) \rangle}$ where $k = \alpha, \beta, \gamma$ and m . Also, $\mathbb{S}_{\alpha,\beta,\gamma} = \frac{\mathbb{F}_q[x,\theta]}{\langle (x^\alpha-1) \rangle} \times \frac{\mathbb{F}_q[x,\theta]}{\langle (x^\beta-1) \rangle} \times \frac{\mathbb{F}_q[x,\theta]}{\langle (x^\gamma-1) \rangle}$

Corollary 3.8. *Let \mathcal{C} be triple θ -skew cyclic code over \mathbb{F}_q generated by*

$$\mathcal{C} = \langle ((A_1(x)|0|0)), ((0|A_2(x)|0)) | ((B_1(x)|B_2(x)|A_3(x))) \rangle,$$

then \mathcal{C} can holds 8 types, which are all the possible forms of \mathcal{C} :

- 1 : The two trivial forms "0, $\mathbb{S}_{\alpha,\beta,\gamma}$ "
- 2 : $\mathbb{S}_n((A_1(x)|0|0))$
- 3 : $\mathbb{S}_n((0|A_2(x)|0))$
- 4 : $\mathbb{S}_n((B_1(x)|B_2(x)|A_3(x)))$
- 5 : $\mathbb{S}_n((A_1(x)|0|0)) + \mathbb{S}_n((0|A_2(x)|0))$
- 6 : $\mathbb{S}_n((A_1(x)|0|0)) + \mathbb{S}_n((B_1(x)|B_2(x)|A_3(x)))$
- 7 : $\mathbb{S}_n((0|A_2(x)|0)) + \mathbb{S}_n((B_1(x)|B_2(x)|A_3(x)))$
- 8 : $\mathbb{S}_n((A_1(x)|0|0)) + \mathbb{S}_n((0|A_2(x)|0)) + \mathbb{S}_n((B_1(x)|B_2(x)|A_3(x)))$

Proof. Let \mathcal{C} be an \mathbb{F}_q -triple skew cyclic code of length (α, β, γ) ,

$$\mathcal{C} = \langle ((A_1(x)|0|0)), ((0|A_2(x)|0))|((B_1(x)|B_2(x)|A_3(x))) \rangle.$$

- (Type 1) we have two trival cases:

(a)- if we take $\text{deg}(A_1(x)) = \text{deg}(A_2(x)) = \text{deg}(A_3(x)) = 0$ and $B_1(x) = B_2(x) = 0$ then $\mathcal{C} = \mathbb{S}_{\alpha, \beta, \gamma}$.

(b)- if we take $A_1(x) = x^\alpha - 1, A_2(x) = x^\beta - 1, A_3(x) = x^\gamma - 1$ and $B_1(x) = B_2(x) = 0$ then $\mathcal{C} = 0$.

- (Type 2) if we take : $0 < \text{deg}(A_1(x)) < \alpha$, $A_2(x) = x^\beta - 1, A_3(x) = x^\gamma - 1$ and $B_1(x) = B_2(x) = 0$

then $\mathcal{C} = \mathbb{S}_n((A_1(x)|0|0))$.

-(Type 3) if we take : $0 < \text{deg}(A_2(x)) < \beta$, $A_1(x) = x^\alpha - 1, A_3(x) = x^\gamma - 1$ and $B_1(x) = B_2(x) = 0$

then $\mathcal{C} = \mathbb{S}_n((0|A_2(x)|0))$.

-(Type 4) if we take : $0 < \text{deg}(A_3(x)) < \gamma$, $A_1(x) = x^\alpha - 1, A_2(x) = x^\beta - 1$ then $\mathcal{C} = \mathbb{S}_n(B_1(x)|B_2(x)|A_3(x))$.

-(Type 5) if we take ; $0 < \text{deg}(A_1(x)) < \alpha$, $0 < \text{deg}(A_2(x)) < \beta$, $A_3(x) = x^\gamma - 1$ and $B_1(x) = B_2(x) = 0$

then $\mathcal{C} = \mathbb{S}_n((A_1(x)|0|0)) + \mathbb{S}_n((0|A_2(x)|0))$.

-(Type 6) if we take : $0 < \text{deg}(A_1(x)) < \alpha$, $0 < \text{deg}(A_3(x)) < \gamma$, $A_2(x) = x^\beta - 1$ then $\mathcal{C} = \mathbb{S}_n((A_1(x)|0|0)) + \mathbb{S}_n(B_1(x)|B_2(x)|A_3(x))$.

-(Type 7) if we take : $0 < \text{deg}(A_2(x)) < \beta$, $0 < \text{deg}(A_3(x)) < \gamma$, $A_1(x) = x^\alpha - 1$ then $\mathcal{C} = \mathbb{S}_n((0|A_2(x)|0)) + \mathbb{S}_n(B_1(x)|B_2(x)|A_3(x))$.

-(Type 8) if we take : $0 < \text{deg}(A_1(x)) < \alpha$, $0 < \text{deg}(A_2(x)) < \beta$, $0 < \text{deg}(A_3(x)) < \gamma$, then $\mathcal{C} = \mathbb{S}_n((A_1(x)|0|0)) + \mathbb{S}_n((0|A_2(x)|0)) + \mathbb{S}_n(B_1(x)|B_2(x)|A_3(x))$. □

Theorem 3.9. Let $\mathcal{C} = \langle (A_1(x)|0|0), (0|A_2(x)|0), (B_1(x)|B_2(x)|A_3(x)) \rangle$ be a triple skew cyclic code of length (α, β, γ) over \mathbb{F}_q . Define the sets

$$M_1 = \bigcup_{i=0}^{\alpha - \text{deg}(A_1(x)) - 1} \{x^i * (A_1(x)|0|0)\},$$

$$M_2 = \bigcup_{i=0}^{\beta - \text{deg}(A_2(x)) - 1} \{x^i * (0|A_2(x)|0)\},$$

$$M_3 = \bigcup_{i=0}^{\gamma - \text{deg}(A_3(x)) - 1} \{x^i * (B_1(x)|B_2(x)|A_3(x))\}.$$

Then the following statements hold :

- (1) $\langle M_1 \rangle = \langle (A_1(x)|0|0) \rangle$
- (2) $\langle M_2 \rangle = \langle (0|A_2(x)|0) \rangle$
- (3) $\langle (B_1(x)|B_2(x)|A_3(x)) \rangle \subseteq \langle M_1 \cup M_2 \cup M_3 \rangle$
- (4) The set $M_1 \cup M_2 \cup M_3$ generates \mathcal{C} minimally.
- (5) $|\mathcal{C}| = q^{\alpha + \beta + \gamma - \text{deg}(A_1(x)) - \text{deg}(A_2(x)) - \text{deg}(A_3(x))}$.

Proof. (1) It is clear that

$$\langle M_1 \rangle \subseteq \langle (A_1(x) \mid 0 \mid 0) \rangle.$$

Now let $p_1(x) \in R = \mathbb{F}_q[x, \theta]$. We show that

$$p_1(x) * (A_1(x) \mid 0 \mid 0) \in \langle M_1 \rangle.$$

Since $\mathbb{F}_q[x, \theta]$ is right Euclidean, by right division there exist $q_1(x), r_1(x) \in \mathbb{F}_q[x, \theta]$ such that

$$p_1(x) = q_1(x)h_1(x) + r_1(x),$$

where either $r_1(x) = 0$ or

$$\deg r_1(x) < \deg h_1(x) = \alpha - \deg(A_1(x)).$$

Therefore

$$\begin{aligned} p_1(x) * (A_1(x) \mid 0 \mid 0) &= (q_1(x)h_1(x) + r_1(x)) * (A_1(x) \mid 0 \mid 0) \\ &= q_1(x) * (h_1(x)A_1(x) \mid 0 \mid 0) + r_1(x) * (A_1(x) \mid 0 \mid 0) \\ &= q_1(x) * (x^\alpha - 1 \mid 0 \mid 0) + r_1(x) * (A_1(x) \mid 0 \mid 0) \\ &= r_1(x) * (A_1(x) \mid 0 \mid 0). \end{aligned}$$

Since $\deg r_1(x) < \alpha - \deg(A_1(x))$, the polynomial $r_1(x)$ is an \mathbb{F}_q -linear combination of $1, x, \dots, x^{\alpha - \deg(A_1(x)) - 1}$. Hence

$$r_1(x) * (A_1(x) \mid 0 \mid 0) \in \langle M_1 \rangle.$$

Thus

$$\langle (A_1(x) \mid 0 \mid 0) \rangle_R \subseteq \langle M_1 \rangle,$$

and the equality follows.

(2) The proof is exactly the same as in part (1). Let $p_2(x) \in R$. By right division,

$$p_2(x) = q_2(x)h_2(x) + r_2(x),$$

where either $r_2(x) = 0$ or

$$\deg r_2(x) < \deg h_2(x) = \beta - \deg(A_2(x)).$$

Then

$$\begin{aligned} p_2(x) * (0 \mid A_2(x) \mid 0) &= (q_2(x)h_2(x) + r_2(x)) * (0 \mid A_2(x) \mid 0) \\ &= q_2(x) * (0 \mid h_2(x)A_2(x) \mid 0) + r_2(x) * (0 \mid A_2(x) \mid 0) \\ &= q_2(x) * (0 \mid x^\beta - 1 \mid 0) + r_2(x) * (0 \mid A_2(x) \mid 0) \\ &= r_2(x) * (0 \mid A_2(x) \mid 0), \end{aligned}$$

which belongs to $\langle M_2 \rangle$. Therefore

$$\langle M_2 \rangle = \langle (0 \mid A_2(x) \mid 0) \rangle.$$

(3) Let $p_3(x) \in R$. We prove that

$$p_3(x) * (B_1(x) \mid B_2(x) \mid A_3(x)) \in \langle M_1 \cup M_2 \cup M_3 \rangle.$$

Again by right division, there exist $q_3(x), r_3(x) \in R$ such that

$$p_3(x) = q_3(x)h_3(x) + r_3(x),$$

where either $r_3(x) = 0$ or

$$\deg r_3(x) < \deg h_3(x) = \gamma - \deg(A_3(x)).$$

Hence

$$\begin{aligned} p_3(x) * (B_1(x) \mid B_2(x) \mid A_3(x)) &= (q_3(x)h_3(x) + r_3(x)) * (B_1(x) \mid B_2(x) \mid A_3(x)) \\ &= q_3(x) * (h_3(x)B_1(x) \mid h_3(x)B_2(x) \mid h_3(x)A_3(x)) \\ &\quad + r_3(x) * (B_1(x) \mid B_2(x) \mid A_3(x)) \\ &= q_3(x) * (h_3(x)B_1(x) \mid h_3(x)B_2(x) \mid 0) \\ &\quad + r_3(x) * (B_1(x) \mid B_2(x) \mid A_3(x)). \end{aligned}$$

Since $\deg r_3(x) < \gamma - \deg(A_3(x))$, we have

$$r_3(x) * (B_1(x) \mid B_2(x) \mid A_3(x)) \in \langle M_3 \rangle.$$

Now, by the assumptions

$$A_1(x) \mid_r h_3(x)B_1(x), \quad A_2(x) \mid_r h_3(x)B_2(x),$$

there exist $\lambda_1(x), \lambda_2(x) \in R$ such that

$$h_3(x)B_1(x) = \lambda_1(x)A_1(x), \quad h_3(x)B_2(x) = \lambda_2(x)A_2(x).$$

Therefore

$$\begin{aligned} q_3(x) * (h_3(x)B_1(x) \mid h_3(x)B_2(x) \mid 0) &= q_3(x) * (\lambda_1(x)A_1(x) \mid \lambda_2(x)A_2(x) \mid 0) \\ &= (q_3(x)\lambda_1(x)) * (A_1(x) \mid 0 \mid 0) \\ &\quad + (q_3(x)\lambda_2(x)) * (0 \mid A_2(x) \mid 0). \end{aligned}$$

By parts (1) and (2), this belongs to

$$\langle (S_1 \cup S_2) \rangle.$$

Consequently,

$$p_3(x) * (B_1(x) \mid B_2(x) \mid A_3(x)) \in \langle M_1 \cup M_2 \cup M_3 \rangle,$$

and part (3) follows.

(4) From the definition of C and parts (1)–(3), we obtain

$$\begin{aligned} C &= \langle (A_1(x) \mid 0 \mid 0) \rangle + \langle (0 \mid A_2(x) \mid 0) \rangle + \langle (B_1(x) \mid B_2(x) \mid A_3(x)) \rangle \\ &\subseteq \langle M_1 \cup M_2 \cup M_3 \rangle. \end{aligned}$$

The reverse inclusion is obvious because every element of $M_1 \cup M_2 \cup M_3$ belongs to C . Hence

$$C = \langle M_1 \cup M_2 \cup M_3 \rangle.$$

It remains to prove that $M_1 \cup M_2 \cup M_3$ is linearly independent. Assume that $u(x) * (A_1(x) \mid 0 \mid 0) + v(x) * (0 \mid A_2(x) \mid 0) + w(x) * (B_1(x) \mid B_2(x) \mid A_3(x)) = (0 \mid 0 \mid 0)$, where

$$\deg u(x) < \alpha - \deg(A_1(x)), \quad \deg v(x) < \beta - \deg(A_2(x)), \quad \deg w(x) < \gamma - \deg(A_3(x)).$$

Looking at the third component, we get

$$w(x)A_3(x) = 0 \quad \text{in } \mathbb{S}_\gamma.$$

Thus $w(x)A_3(x)$ is a left multiple of $x^\gamma - 1 = h_3(x)A_3(x)$. Since $\mathbb{F}_q[x, \theta]$ is a domain, we can cancel $A_3(x)$ on the right and obtain

$$w(x) = \mu(x)h_3(x),$$

for some $\mu(x) \in \mathbb{F}_q[x, \theta]$. But

$$\deg w(x) < \deg h_3(x),$$

so necessarily $w(x) = 0$.

Now the relation becomes

$$u(x) * (A_1(x) \mid 0 \mid 0) + v(x) * (0 \mid A_2(x) \mid 0) = (0 \mid 0 \mid 0).$$

Looking at the second component, we obtain

$$v(x)A_2(x) = 0 \quad \text{in } \mathbb{S}_\beta.$$

As above, $v(x)A_2(x)$ is a left multiple of $x^\beta - 1 = h_2(x)A_2(x)$, hence $v(x) = \nu(x)h_2(x)$ for some $\nu(x) \in R$. Since

$$\deg v(x) < \deg h_2(x),$$

we conclude that $v(x) = 0$.

Finally, looking at the first component gives

$$u(x)A_1(x) = 0 \quad \text{in } \mathbb{S}_\alpha.$$

Again $u(x)$ must be a left multiple of $h_1(x)$, but

$$\deg u(x) < \deg h_1(x),$$

so $u(x) = 0$.

Hence $M_1 \cup M_2 \cup M_3$ is linearly independent. Therefore it is a minimal generating set of \mathcal{C} as an \mathbb{F}_q -vector space.

(5) Since $M_1 \cup M_2 \cup M_3$ is a basis of \mathcal{C} ,

$$\dim \mathcal{C} = |M_1| + |M_2| + |M_3|.$$

Now

$$|M_1| = \alpha - \deg(A_1(x)), \quad |M_2| = \beta - \deg(A_2(x)), \quad |M_3| = \gamma - \deg(A_3(x)).$$

Therefore

$$\dim \mathcal{C} = \alpha + \beta + \gamma - \deg(A_1(x)) - \deg(A_2(x)) - \deg(A_3(x)).$$

Hence

$$|\mathcal{C}| = q^{\alpha + \beta + \gamma - \deg(A_1(x)) - \deg(A_2(x)) - \deg(A_3(x))}.$$

□

Remark 3.10. The rows M_1, M_2 and M_3 form the generator matrix of the code \mathcal{C} .

Note 3.11. For the rest of the paper, when we mention \mathcal{C} it is always

$$\mathcal{C} = \langle (A_1(x)|0|0), (0|A_2(x)|0), (B_1(x)|B_2(x)|A_3(x)) \rangle,$$

a triple skew cyclic code of length $n = \alpha + \beta + \gamma$ over \mathbb{F}_q .

4. Dual of the triple skew cyclic code

The section develops the dual theory for triple skew-cyclic codes over \mathbb{F}_q , exhibiting how generator polynomials transform under passage to the dual.

Definition 4.1. ([7]) The reciprocal polynomial of $b(x) = b_0x^0 + \dots + b_\gamma x^\gamma \in \mathbb{F}_q[x, \theta]$ where $b_\gamma \neq 0$, is defined by :

$$b^*(x) = b_\gamma + \theta(b_{\gamma-1})x + \dots + \theta^\gamma(b_0)x^\gamma.$$

We can also expressed the reciprocal polynomial by

$$b^*(x) = \sum_{i=0}^{\gamma} \theta^i(b_{\gamma-i})x^i.$$

Lemma 4.2. ([8]) Let b_i be an element of \mathbb{F}_q , the map ϕ defined by:

$$\begin{aligned} \phi : \mathbb{F}_q[x, \theta] &\longrightarrow \mathbb{F}_q[x, \theta], \\ \sum_{i=0}^n b_i x^i &\longmapsto \sum_{i=0}^n \theta(b_i) x^i, \end{aligned}$$

is a ring homomorphism.

Lemma 4.3. ([1]) *Let $A(x), B(x)$ be two skew polynomial in $\mathbb{F}_q[x, \theta]$, assume $\deg(A)$ less than $\deg(B)$, then*

- $(A(x) + B(x))^* = A^*(x) + x^{\deg A - \deg B} B^*(x)$.
- $(AB)^* = \phi^{\deg A}(B^*)A^*$.
- $(A^*)^* = \phi^n(A)$, where $\deg(A) = n$.

Set $\sigma_\nu(x) = \sum_{j=0}^{\nu-1} x^j$, Since the unit element 1 is invariant by the automorphism θ . Consequently, the subsequent lemma is immediate;

Lemma 4.4. *Let $r, s \in \mathbb{N}$. Then $x^{rs} - 1 = (x^r - 1) \sigma_s(x^r) = \sigma_s(x^r)(x^r - 1)$.*

Proof.

We compute $(x^\alpha - 1)\sigma_s(x^r) = (x^\alpha - 1) \sum_{j=0}^{\beta-1} x^{rj} = \sum_{j=0}^{\beta-1} (x^{r(j+1)} - x^{rj}) = x^{rs} - 1$.

The equality $\sigma_s(x^r)(x^\alpha - 1) = x^{rs} - 1$ is proved analogously. Here no commutativity with coefficients is needed, since only powers of x and the scalar 1 appear. □

In what follows, we work in the quotient rings

$$\mathbb{S}_m := \mathbb{F}_q[x, \theta] / \langle x^m - 1 \rangle \quad m = \text{lcm}(\alpha, \beta, \gamma),$$

where $\langle x^m - 1 \rangle$ denotes the two-sided ideal generated by $x^m - 1$. (Throughout we assume $\text{ord}(\theta) \mid m$ for the relevant lengths m so that $x^m - 1$ is central and $\langle x^m - 1 \rangle$ is indeed two-sided.) For $f \in \mathbb{F}_q[x, \theta]$, we denote by \bar{f} its residue class in \mathbb{S}_m . All congruences “mod $(x^m - 1)$ ” are taken in $\mathbb{F}_q[x, \theta]$ modulo the ideal $\langle x^m - 1 \rangle$.

Definition 4.5. Let $f(x) = (A_1(x) | A_2(x) | A_3(x))$ and $g(x) = (B_1(x) | B_2(x) | B_3(x))$ be two elements of $\mathbb{S}_{\alpha, \beta, \gamma}$, and $m = \text{lcm}(\alpha, \beta, \gamma)$. Consider the mapping \circ :

$$\mathbb{S}_{\alpha, \beta, \gamma} \times \mathbb{S}_{\alpha, \beta, \gamma} \rightarrow \mathbb{S}_m,$$

with

$$\begin{aligned} \circ(f(x), g(x)) &= A_1(x) \phi^{m - \deg(B_1(x))} (B_1^*(x)) x^{m-1 - \deg(B_1(x))} \sigma_{\frac{m}{\alpha}}(x^\alpha) \\ &\quad + A_2(x) \phi^{m - \deg(B_2(x))} (B_2^*(x)) x^{m-1 - \deg(B_2(x))} \sigma_{\frac{m}{\beta}}(x^\beta) \\ &\quad + A_3(x) \phi^{m - \deg(B_3(x))} (B_3^*(x)) x^{m-1 - \deg(B_3(x))} \sigma_{\frac{m}{\gamma}}(x^\gamma). \end{aligned}$$

The composition \circ is an bilinear map with respect to the $\mathbb{F}_q[x, \theta]$ -modules.

Proposition 4.6. *The mapping*

$$\circ : \mathbb{S}_{\alpha, \beta, \gamma} \times \mathbb{S}_{\alpha, \beta, \gamma} \rightarrow \mathbb{S}_m,$$

given in Definition 4.5 is well-defined, i.e. it does not depend on the choice of representatives modulo $\langle x^\alpha - 1 \rangle$, $\langle x^\beta - 1 \rangle$, and $\langle x^\gamma - 1 \rangle$.

Proof. We show independence in the first coordinate; the other two are identical.

Let $A_1, A'_1 \in \mathbb{F}_q[x, \theta]$ be two representatives of $\overline{A_1} \in \mathbb{S}_\alpha$. Then $A'_1 - A_1 \in \langle x^\alpha - 1 \rangle$, so there exists $U \in \mathbb{F}_q[x, \theta]$ with $A'_1 - A_1 = (x^\alpha - 1)U$. Consider the difference of the corresponding first summands in Definition 4.5:

$$\begin{aligned} & (A'_1 - A_1) \phi^{m-\deg(B_1)}(B_1^*) x^{m-1-\deg(B_1)} \sigma_{m/\alpha}(x^\alpha) \\ &= (x^\alpha - 1)U \phi^{m-\deg(B_1)}(B_1^*) x^{m-1-\deg(B_1)} \sigma_{m/\alpha}(x^\alpha). \end{aligned}$$

Since $x^\alpha - 1$ is central under our standing assumption $ord(\theta) \mid \alpha$, we may move it to the right:

$$= U \phi^{m-\deg(B_1)}(B_1^*) x^{m-1-\deg(B_1)} (x^\alpha - 1) \sigma_{m/\alpha}(x^\alpha).$$

By Lemma 4.4 with $r = \alpha$ and $s = m/\alpha$,

$$(x^\alpha - 1)\sigma_{m/\alpha}(x^\alpha) = x^m - 1.$$

Hence the above difference lies in $\langle x^m - 1 \rangle$, and therefore becomes zero after reduction modulo $\langle x^m - 1 \rangle$ in \mathbb{S}_m . This proves that changing the representative of $\overline{A_1} \in R_\alpha$ does not change $f \circ g$ in \mathbb{S}_m .

The same argument applies to A_2 (using $(x^\beta - 1)\sigma_{m/\beta}(x^\beta) = x^m - 1$) and to A_3 (using $(x^\gamma - 1)\sigma_{m/\gamma}(x^\gamma) = x^m - 1$).

Finally, the choice of representatives for $\overline{B_i} \in \mathbb{S}_\alpha, \mathbb{S}_\beta, \mathbb{S}_\gamma$ does not affect the value either: if $B'_1 \equiv B_1 \pmod{\langle x^\alpha - 1 \rangle}$, then $B'_1 - B_1 \in \langle x^\alpha - 1 \rangle$, and since ϕ is a ring automorphism of R and the involution/reciprocal $*$ stabilizes the ideal $\langle x^\alpha - 1 \rangle$, the difference

$$\phi^{m-\deg(B'_1)}(B_1'^*) x^{m-1-\deg(B'_1)} - \phi^{m-\deg(B_1)}(B_1^*) x^{m-1-\deg(B_1)},$$

is congruent to 0 modulo $\langle x^\alpha - 1 \rangle$. Multiplying on the right by $\sigma_{m/\alpha}(x^\alpha)$ yields a multiple of $x^m - 1$ by the same lemma, hence it vanishes in \mathbb{S}_m . The arguments for B_2, B_3 are identical. □

Proposition 4.7. *Let $\mathbf{A}(x) = (A_1(x) \mid A_2(x) \mid A_3(x))$ and $\mathbf{B}(x) = (B_1(x) \mid B_2(x) \mid B_3(x))$ be two elements of $\mathbb{S}_{\alpha, \beta, \gamma}$. Then $\mathbf{A} \circ \mathbf{B} \equiv 0 \pmod{(x^m - 1)}$ if and only if \mathbf{A} is orthogonal to \mathbf{B} and all its shifts.*

Proof. Let

$$\mathbf{A} = (a_0, a_1, \dots, a_{\alpha-1} \mid a'_0, a'_1, \dots, a'_{\beta-1} \mid a''_0, a''_1, \dots, a''_{\gamma-1}),$$

and

$$\mathbf{B} = (b_0, b_1, \dots, b_{\alpha-1} \mid b'_0, b'_1, \dots, b'_{\beta-1} \mid b''_0, b''_1, \dots, b''_{\gamma-1}).$$

For $0 \leq i \leq m - 1$, let $\mathbf{A}^{(i)}$ be the i -th cyclic θ -shift of \mathbf{A} , i.e.,

$$\begin{aligned} \mathbf{A}^{(i)} = & (\theta^i(a_{0-i}), \theta^i(a_{1-i}), \dots, \theta^i(a_{\alpha-1-i}) \mid \theta^i(a'_{0-i}), \theta^i(a'_{1-i}), \dots, \theta^i(a'_{\beta-1-i}) \\ & \mid \theta^i(a''_{0-i}), \theta^i(a''_{1-i}), \dots, \theta^i(a''_{\gamma-1-i})), \end{aligned}$$

where indices are taken modulo α , β , and γ in each block. Then $\mathbf{A}^{(i)} \cdot \mathbf{B} = 0$ if and only if

$$\sum_{j=0}^{\alpha-1} \theta^i(a_{j-i})b_j + \sum_{\nu=0}^{\beta-1} \theta^i(a'_{\nu-i})b'_\nu + \sum_{t=0}^{\gamma-1} \theta^i(a''_{\gamma-i})b''_t = 0.$$

Set

$$S_i = \sum_{j=0}^{\alpha-1} \theta^i(a_{j-i})b_j + \sum_{\nu=0}^{\beta-1} \theta^i(a'_{\nu-i})b'_\nu + \sum_{t=0}^{\gamma-1} \theta^i(a''_{\gamma-i})b''_t \in \mathbb{F}_q.$$

Using Definition of \circ and expanding, we obtain

$$\begin{aligned} \mathbf{A}(x) \circ \mathbf{B}(x) = & \left[\sum_{\mu=0}^{\alpha-1} \sum_{j=\mu}^{\alpha-1} a_{j-\mu} \theta^{m-\mu}(b_j) x^{m-1-\mu} + \sum_{\mu=1}^{\alpha-1} \sum_{j=0}^{\mu-1} a_{j+\alpha-\mu} \theta^\mu(b_j) x^{m-1+\mu} \right] \sigma_{\frac{m}{\alpha}}(x^\alpha) \\ & + \left[\sum_{\eta=0}^{\beta-1} \sum_{\nu=\eta}^{\beta-1} a'_{\nu-\eta} \theta^{m-\eta}(b'_\nu) x^{m-1-\eta} + \sum_{\eta=1}^{\beta-1} \sum_{\nu=0}^{\eta-1} a'_{\nu+\beta-\eta} \theta^\eta(b'_\nu) x^{m-1+\eta} \right] \sigma_{\frac{m}{\beta}}(x^\beta) \\ & + \left[\sum_{\kappa=0}^{\gamma-1} \sum_{t=\kappa}^{\gamma-1} a''_{\gamma-\kappa} \theta^{m-\kappa}(b''_t) x^{m-1-\kappa} + \sum_{\kappa=1}^{\gamma-1} \sum_{t=0}^{\kappa-1} a''_{t+\gamma-\kappa} \theta^\kappa(b''_t) x^{m-1+\kappa} \right] \sigma_{\frac{m}{\gamma}}(x^\gamma). \end{aligned}$$

Collecting coefficients modulo $(x^m - 1)$ yields

$$\mathbf{A}(x) \circ \mathbf{B}(x) = \sum_{i=0}^{m-1} \theta^{m-i}(S_i) x^{m-1-i} \quad \text{in } \mathbb{S}_m.$$

Therefore, $\mathbf{A} \circ \mathbf{B} \equiv 0 \pmod{x^m - 1}$ if and only if $S_i = 0$ for all $0 \leq i \leq m - 1$. Equivalently, $\mathbf{A}^{(i)} \cdot \mathbf{B} = 0$ for all i , i.e., \mathbf{B} is orthogonal to \mathbf{A} and all its θ -shifts. \square

Proposition 4.8. *Let $\mathbf{A}(x) = (A_1(x) | A_2(x) | A_3(x))$ and $\mathbf{B}(x) = (B_1(x) | B_2(x) | B_3(x))$ be two elements of $\mathbb{S}_{\alpha,\beta,\gamma}$ with $\mathbf{A}(x) \circ \mathbf{B}(x) \equiv 0 \pmod{x^m - 1}$ then :*

(1) *if $A_2(x) = 0$ or $B_2(x) = 0$, and $A_3(x) = 0$ or $B_3(x) = 0$ then*

$$A_1(x) \phi^{m-\deg(B_1(x))} B_1^*(x) \equiv 0 \pmod{x^\alpha - 1}.$$

(2) *if $A_1(x) = 0$ or $B_1(x) = 0$, and $A_3(x) = 0$ or $B_3(x) = 0$ then*

$$A_2(x) \phi^{m-\deg(B_2(x))} B_2^*(x) \equiv 0 \pmod{x^\beta - 1}.$$

(3) *if $A_1(x) = 0$ or $B_1(x) = 0$, and $A_2(x) = 0$ or $B_2(x) = 0$ then*

$$A_3(x) \phi^{m-\deg(B_3(x))} B_3^*(x) \equiv 0 \pmod{x^\gamma - 1}.$$

Proof. (1) Assume $A_2(x) = 0$ or $B_2(x) = 0$, and $A_3(x) = 0$ or $B_3(x) = 0$. Therefore,

$$\mathbf{A}(x) \circ \mathbf{B}(x) = A_1(x) \phi^{m-\deg(B_1(x))} (B_1^*(x)) x^{m-1-\deg(B_1(x))} \theta_{\frac{m}{\alpha}}(x^\alpha) + 0 \equiv 0 \pmod{x^m - 1}.$$

Therefore, one obtains the existence of a skew polynomial $\alpha(x)$ where :

$$A_1(x) \phi^{m-\deg(B_1(x))} (B_1^*(x)) x^{m-1-\deg(B_1(x))} \theta_{\frac{m}{\alpha}}(x^\alpha) = \alpha(x) (x^m - 1).$$

Since $\theta_{\frac{m}{r}}(x^\alpha) = \frac{x^m-1}{x^\alpha-1}$ and $(x^m-1)(x^\alpha-1) = (x^\alpha-1)(x^m-1)$, we obtain

$$A_1(x)\phi^{m-\deg(B_1(x))}(B_1^*(x))x^m = \alpha(x)x^{\deg(B_1(x))+1}(x^\alpha-1).$$

Hence

$$A_1(x)\phi^{m-\deg(B_1(x))}B_1^*(x) \equiv 0 \pmod{(x^\alpha-1)}.$$

(2) Suppose that $A_1(x) = 0$ or $B_1(x) = 0$, and $A_3(x) = 0$ or $B_3(x) = 0$. Therefore,

$$\mathbf{A}(x) \circ \mathbf{B}(x) = A_2(x)\phi^{m-\deg(B_2(x))}(B_2^*(x))x^{m-1-\deg(B_2(x))}\theta_{\frac{m}{s}}(x^\beta) + 0 \equiv 0 \pmod{(x^m-1)}.$$

Therefore, one obtains the existence of $\beta(x) \in \mathbb{F}_q[x, \theta]$ where :

$$A_2(x)\phi^{m-\deg(B_2(x))}(B_2^*(x))x^{m-1-\deg(B_2(x))}\theta_{\frac{m}{s}}(x^\beta) = \beta(x)(x^m-1).$$

Since $\theta_{\frac{m}{s}}(x^\beta) = \frac{x^m-1}{x^\beta-1}$ and $(x^m-1)(x^\beta-1) = (x^\beta-1)(x^m-1)$, we obtain

$$A_2(x)\phi^{m-\deg(B_2(x))}(B_2^*(x))x^m = \beta(x)x^{\deg(B_2(x))+1}(x^\beta-1).$$

Hence

$$A_2(x)\phi^{m-\deg(B_2(x))}B_2^*(x) = 0 \pmod{(x^\beta-1)}.$$

(3) Suppose that $A_1(x) = 0$ or $B_1(x) = 0$, and $A_2(x) = 0$ or $B_2(x) = 0$. Therefore,

$$\mathbf{A}(x) \circ \mathbf{B}(x) = A_3(x)\phi^{m-\deg(B_3(x))}(B_3^*(x))x^{m-1-\deg(B_3(x))}\theta_{\frac{m}{t}}(x^\gamma) + 0 = 0 \pmod{(x^m-1)}.$$

Therefore, one obtains the existence of $\gamma(x) \in \mathbb{F}_q[x, \theta]$ where :

$$A_3(x)\phi^{m-\deg(B_3(x))}(B_3^*(x))x^{m-1-\deg(B_3(x))}\theta_{\frac{m}{t}}(x^\gamma) = \gamma(x)(x^m-1).$$

Since $\theta_{\frac{m}{t}}(x^\gamma) = \frac{x^m-1}{x^\gamma-1}$ and $(x^m-1)(x^\gamma-1) = (x^\gamma-1)(x^m-1)$, we obtain

$$A_3(x)\phi^{m-\deg(B_3(x))}(B_3^*(x))x^m = \gamma(x)x^{\deg(B_3(x))+1}(x^\gamma-1).$$

Hence

$$A_3(x)\phi^{m-\deg(B_3(x))}B_3^*(x) = 0 \pmod{(x^\gamma-1)}.$$

□

Definition 4.9. \mathcal{C} is a triple skew cyclic code of length (α, β, γ) over \mathbb{F}_q we define the sets:

- (1) $(C_\alpha)^\perp = \{\mathbf{A} \in \mathbb{F}_q^\alpha \mid (\mathbf{A}|0|0) \in C^\perp\} = \left\{ f(x) \in \frac{\mathbb{F}_q[x;\theta]}{\langle x^\alpha-1 \rangle} \mid (f(x)|0|0) \in C^\perp \right\}.$
- (2) $(C_\beta)^\perp = \{\mathbf{B} \in \mathbb{F}_q^\beta \mid (0|\mathbf{B}|0) \in C^\perp\} = \left\{ g(x) \in \frac{\mathbb{F}_q[x;\theta]}{\langle x^\beta-1 \rangle} \mid (0|g(x)|0) \in C^\perp \right\}.$
- (3) $(C_\gamma)^\perp = \{\mathbf{h} \in \mathbb{F}_q^\gamma \mid (0|0|\mathbf{h}) \in C^\perp\} = \left\{ h(x) \in \frac{\mathbb{F}_q[x;\theta]}{\langle x^\gamma-1 \rangle} \mid (0|0|h(x)) \in C^\perp \right\}.$

Lemma 4.10. \mathcal{C} is a triple skew cyclic code of length (α, β, γ) over \mathbb{F}_q . Then :

- (1) $|C_\alpha| = q^{\alpha-\deg(\gcd_r(A_1(x), B_1(x)))}$, $\left| (C_\alpha)^\perp \right| = q^{\deg(\gcd_r(A_1(x), B_1(x)))}$
- (2) $|C_\beta| = q^{\beta-\deg(\gcd_r(A_2(x), B_2(x)))}$, $\left| (C_\beta)^\perp \right| = q^{\deg(\gcd_r(A_2(x), B_2(x)))}$
- (3) $\deg(\bar{A}_1(x)) = \alpha - \deg(\gcd_r(A_1(x), B_1(x)))$.
- (4) $\deg(\bar{A}_2(x)) = \beta - \deg(\gcd_r(A_2(x), B_2(x)))$.

Proof. The proofs of the cardinality statements in (1) and (2) follow the same arguments as in [13], with the only modification that the base field size 2 is replaced by q .

For the degree statements in (3) and (4), the proof is analogous to [13, Proposition 4.4]. The argument carries over directly because the non-commutativity of the skew polynomial ring does not affect the degree of the product of polynomials. Hence the same reasoning used in [13] applies in our setting. \square

Theorem 4.11. *Let $R = \mathbb{F}_q[x, \theta]$, where $\text{ord}(\theta) \mid \text{lcm}(\alpha, \beta, \gamma)$, and let*

$$m = \text{lcm}(\alpha, \beta, \gamma).$$

For $f(x) \in R$, define its skew adjoint by

$$f^\natural(x) := \phi^{m-\deg f}(f^*(x)).$$

Let

$$\mathcal{C} = \mathbb{S}_n(A_1(x) \mid 0 \mid 0) + \mathbb{S}_n(0 \mid A_2(x) \mid 0) + \mathbb{S}_n(B_1(x) \mid B_2(x) \mid A_3(x)),$$

and let

$$\mathcal{C}^\perp = \mathbb{S}_n(\bar{A}_1(x) \mid 0 \mid 0) + \mathbb{S}_n(0 \mid \bar{A}_2(x) \mid 0) + \mathbb{S}_n(\bar{B}_1(x) \mid \bar{B}_2(x) \mid \bar{A}_3(x)).$$

Set

$$D_1(x) := \text{gcd}(A_1^\natural(x), B_1^\natural(x)), \quad D_2(x) := \text{gcd}(A_2^\natural(x), B_2^\natural(x)),$$

where gcd denotes the greatest common left divisor in R , then

$$\bar{A}_1(x) = \frac{x^\alpha - 1}{D_1(x)}, \quad \bar{A}_2(x) = \frac{x^\beta - 1}{D_2(x)}.$$

Equivalently,

$$\bar{A}_1(x)D_1(x) = x^\alpha - 1, \quad \bar{A}_2(x)D_2(x) = x^\beta - 1.$$

In particular,

$$\deg \bar{A}_1(x) = \alpha - \deg \text{gcd}(A_1(x), B_1(x)),$$

$$\deg \bar{A}_2(x) = \beta - \deg \text{gcd}(A_2(x), B_2(x)),$$

where gcd denotes the greatest common right divisor.

Proof. Since $(\bar{A}_1(x) \mid 0 \mid 0) \in \mathcal{C}^\perp$, it is orthogonal to $(A_1(x) \mid 0 \mid 0)$ and $(B_1(x) \mid B_2(x) \mid A_3(x))$. By Proposition 4.8, this yields

$$\bar{A}_1(x)A_1^\natural(x) \equiv 0 \pmod{x^\alpha - 1}, \quad \bar{A}_1(x)B_1^\natural(x) \equiv 0 \pmod{x^\alpha - 1}.$$

Hence $\bar{A}_1(x)$ annihilates every common left divisor of $A_1^\natural(x)$ and $B_1^\natural(x)$, and therefore

$$\bar{A}_1(x)D_1(x) \equiv 0 \pmod{x^\alpha - 1}.$$

Since $x^\alpha - 1$ is central in R , there exists $u_1(x) \in R$ such that

$$\bar{A}_1(x)D_1(x) = u_1(x)(x^\alpha - 1).$$

Now

$$\deg \bar{A}_1(x) = \alpha - \deg \gcd(A_1(x), B_1(x)),$$

by the preceding degree lemma, and

$$\deg D_1(x) = \deg \gcd(A_1(x), B_1(x)).$$

Therefore

$$\deg \bar{A}_1(x) + \deg D_1(x) = \alpha = \deg(x^\alpha - 1),$$

so $u_1(x)$ must be a nonzero constant. Since all polynomials are chosen monic, we obtain $u_1(x) = 1$. Thus

$$\bar{A}_1(x)D_1(x) = x^\alpha - 1,$$

that is,

$$\bar{A}_1(x) = \frac{x^\alpha - 1}{D_1(x)}.$$

The proof for $\bar{A}_2(x)$ is identical. Indeed,

$$\bar{A}_2(x)A_2^{\natural}(x) \equiv 0 \pmod{x^\beta - 1}, \quad \bar{A}_2(x)B_2^{\natural}(x) \equiv 0 \pmod{x^\beta - 1},$$

so

$$\bar{A}_2(x)D_2(x) = x^\beta - 1,$$

and hence

$$\bar{A}_2(x) = \frac{x^\beta - 1}{D_2(x)}.$$

□

Proposition 4.12. *With the notation of Theorem 4.11, the mixed dual generator $(\bar{B}_1(x) \mid \bar{B}_2(x) \mid \bar{A}_3(x))$ is characterized by the following relations:*

(1)

$$\bar{B}_1(x)A_1^{\natural}(x) \equiv 0 \pmod{x^\alpha - 1}, \quad \bar{B}_2(x)A_2^{\natural}(x) \equiv 0 \pmod{x^\beta - 1}.$$

(2) *Let*

$$L_1(x) := \text{lcm}(A_1(x), B_1(x)), \quad L_2(x) := \text{lcm}(A_2(x), B_2(x)),$$

and choose $U_1(x), V_1(x), U_2(x), V_2(x) \in R$ such that

$$L_1(x) = U_1(x)B_1(x) = V_1(x)A_1(x),$$

$$L_2(x) = U_2(x)B_2(x) = V_2(x)A_2(x).$$

Then

$$(0 \mid U_1(x)B_2(x) \mid U_1(x)A_3(x)) \in \mathcal{C},$$

$$(U_2(x)B_1(x) \mid 0 \mid U_2(x)A_3(x)) \in \mathcal{C},$$

and orthogonality gives

$$\bar{B}_2(x)(U_1(x)B_2(x))^{\natural} + \bar{A}_3(x)(U_1(x)A_3(x))^{\natural} \equiv 0 \pmod{x^m - 1},$$

$$\bar{B}_1(x)(U_2(x)B_1(x))^{\natural} + \bar{A}_3(x)(U_2(x)A_3(x))^{\natural} \equiv 0 \pmod{x^m - 1}.$$

(3) Under the usual normal-form conditions

$$\deg \bar{B}_1(x) < \deg \bar{A}_1(x), \quad \deg \bar{B}_2(x) < \deg \bar{A}_2(x),$$

together with the requirement that $\bar{A}_3(x)$ is monic and $\bar{A}_3(x) \mid_r (x^\gamma - 1)$, these congruences determine the mixed dual generator.

Proof. Since $(\bar{B}_1(x) \mid \bar{B}_2(x) \mid \bar{A}_3(x)) \in \mathcal{C}^\perp$, it is orthogonal to $(A_1(x) \mid 0 \mid 0)$ and $(0 \mid A_2(x) \mid 0)$. By Proposition 4.8,

$$\bar{B}_1(x)A_1^{\natural}(x) \equiv 0 \pmod{x^\alpha - 1}, \quad \bar{B}_2(x)A_2^{\natural}(x) \equiv 0 \pmod{x^\beta - 1}.$$

Now let $L_1(x) = \text{lclm}(A_1(x), B_1(x))$, and choose $U_1(x), V_1(x) \in R$ such that

$$L_1(x) = U_1(x)B_1(x) = V_1(x)A_1(x).$$

Then

$$U_1(x)(B_1(x) \mid B_2(x) \mid A_3(x)) - V_1(x)(A_1(x) \mid 0 \mid 0) = (0 \mid U_1(x)B_2(x) \mid U_1(x)A_3(x)) \in \mathcal{C}.$$

Since $(\bar{B}_1(x) \mid \bar{B}_2(x) \mid \bar{A}_3(x)) \in \mathcal{C}^\perp$, we get

$$(\bar{B}_1(x) \mid \bar{B}_2(x) \mid \bar{A}_3(x)) \circ (0 \mid U_1(x)B_2(x) \mid U_1(x)A_3(x)) = 0.$$

Applying Proposition 4.8 again yields

$$\bar{B}_2(x)(U_1(x)B_2(x))^{\natural} + \bar{A}_3(x)(U_1(x)A_3(x))^{\natural} \equiv 0 \pmod{x^m - 1}.$$

The second congruence is obtained in the same way from $L_2(x) = \text{lclm}(A_2(x), B_2(x))$. This proves the proposition. \square

Corollary 4.13. *With the notation above,*

$$\dim_{\mathbb{F}_q}(\mathcal{C}^\perp) = \alpha + \beta + \gamma - \dim_{\mathbb{F}_q}(\mathcal{C}) = \deg A_1(x) + \deg A_2(x) + \deg A_3(x).$$

Consequently,

$$\begin{aligned} \deg \bar{A}_3(x) = & \gamma - \deg A_3(x) - \deg A_1(x) - \deg A_2(x) + \deg \text{gcd}(A_1(x), B_1(x)) \\ & + \deg \text{gcd}(A_2(x), B_2(x)). \end{aligned}$$

Proof. By the dimension formula for triple skew cyclic codes,

$$\dim_{\mathbb{F}_q}(\mathcal{C}) = (\alpha - \deg A_1(x)) + (\beta - \deg A_2(x)) + (\gamma - \deg A_3(x)).$$

Hence

$$\dim_{\mathbb{F}_q}(\mathcal{C}^\perp) = \alpha + \beta + \gamma - \dim_{\mathbb{F}_q}(\mathcal{C}) = \deg A_1(x) + \deg A_2(x) + \deg A_3(x).$$

On the other hand,

$$\dim_{\mathbb{F}_q}(\mathcal{C}^\perp) = (\alpha - \deg \bar{A}_1(x)) + (\beta - \deg \bar{A}_2(x)) + (\gamma - \deg \bar{A}_3(x)).$$

Substituting the formulas from Theorem 4.11,

$$\deg \bar{A}_1(x) = \alpha - \deg \gcd(A_1(x), B_1(x)),$$

$$\deg \bar{A}_2(x) = \beta - \deg \gcd(A_2(x), B_2(x)),$$

and comparing both expressions for $\dim_{\mathbb{F}_q}(\mathcal{C}^\perp)$, we obtain

$$\begin{aligned} \deg \bar{A}_3(x) = & \gamma - \deg A_3(x) - \deg A_1(x) - \deg A_2(x) + \deg \gcd(A_1(x), B_1(x)) \\ & + \deg \gcd(A_2(x), B_2(x)). \end{aligned}$$

□

Example 4.14. Consider the commutative specialization $\theta = \text{id}$ over \mathbb{F}_2 , with

$$\alpha = \beta = \gamma = 3, \quad m = 3,$$

and

$$A_1(x) = A_2(x) = A_3(x) = x + 1, \quad B_1(x) = B_2(x) = x + 1.$$

Then

$$x^3 - 1 = (x + 1)(x^2 + x + 1) \quad \text{in } \mathbb{F}_2[x].$$

Since $\theta = \text{id}$, the skew adjoint f^\natural reduces to the usual reciprocal polynomial, and $A_i^\natural(x) = B_i^\natural(x) = x + 1$. Hence

$$D_1(x) = \gcd(A_1^\natural(x), B_1^\natural(x)) = x + 1, \quad D_2(x) = \gcd(A_2^\natural(x), B_2^\natural(x)) = x + 1.$$

By Theorem 4.11,

$$\bar{A}_1(x) = \frac{x^3 - 1}{x + 1} = x^2 + x + 1, \quad \bar{A}_2(x) = \frac{x^3 - 1}{x + 1} = x^2 + x + 1.$$

Moreover,

$$\dim_{\mathbb{F}_2}(\mathcal{C}) = (3 - 1) + (3 - 1) + (3 - 1) = 6,$$

so

$$\dim_{\mathbb{F}_2}(\mathcal{C}^\perp) = 9 - 6 = 3.$$

Therefore $\deg \bar{A}_3(x) = 2$, and we may take

$$\bar{B}_1(x) = 0, \quad \bar{B}_2(x) = 0, \quad \bar{A}_3(x) = x^2 + x + 1.$$

Thus

$$\mathcal{C}^\perp = \mathbb{S}_n(x^2 + x + 1 \mid 0 \mid 0) + \mathbb{S}_n(0 \mid x^2 + x + 1 \mid 0) + \mathbb{S}_n(0 \mid 0 \mid x^2 + x + 1).$$

To verify orthogonality, observe that

$$(x^2 + x + 1)(x + 1) = x^3 + 1 \equiv 0 \pmod{x^3 - 1},$$

over \mathbb{F}_2 . Hence each generator of \mathcal{C}^\perp is orthogonal to each generator of \mathcal{C} , and therefore

$$\mathcal{C}^\perp \subseteq \mathcal{C}_{\text{alg}}^\perp.$$

Since both spaces have dimension 3, they are equal. In particular,

$$\dim_{\mathbb{F}_2}(\mathcal{C}) + \dim_{\mathbb{F}_2}(\mathcal{C}^\perp) = 6 + 3 = 9 = \alpha + \beta + \gamma.$$

5. Computational results of triple skew cyclic code

This section provides an MDS and optimal according to [10], using some spacial cases in Corollary 3.8, generated by the monics right divisor of $x^\alpha - 1, x^\beta - 1$ and $x^\gamma - 1$ in \mathbb{F}_q . The computational algebra system Magma was employed to obtain the factorization and to compute the minimum distance. The example showcases the construction process, including the definition of skew polynomial rings and the generator polynomial of codes.

Example 5.1. (1) Let $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$, ω is a primitive element ($\omega^2 = \omega + 1$). A Factorization of $x^4 - 1$ in $\mathbb{F}_4[x; \theta]$, where $\theta(a) = a^2$ for all $a \in \mathbb{F}_4$, is:

$$x^4 - 1 = (x - 1)(x - \omega^2)(x - \omega)(x - 1).$$

(2) Let $\mathbb{F}_{16} = \{0, \varsigma, \varsigma^2, \dots, \varsigma^{14}, \varsigma^{15} = 1\}$ where ς is the 15th primitive root of unity in \mathbb{F}_{16} . We can factorize the polynomial $x^4 - 1$ in $\mathbb{F}_{16}[x; \theta]$, where $\theta(a) = a^2$ for all $a \in \mathbb{F}_{16}$. as following :

$$x^4 - 1 = (x - 1) (x - \varsigma^5) (x - \varsigma^{10}) (x - 1).$$

Consider

$$\mathcal{C} = \mathbb{S}_{12}(x^3 + x^2 + x + 1 \mid 0 \mid 0) + \mathbb{S}_{12}(0 \mid x^3 + x^2 + x + 1 \mid 0) + \mathbb{S}_{12}(w \mid w^2 \mid (x + 1)^2).$$

Hence

$$G_1 = \left[\begin{array}{cccc|cccc|cccc} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ \omega & 0 & 0 & 0 & \omega^2 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & \omega^2 & 0 & 0 & 0 & \omega & 0 & 0 & 0 & 1 & 0 & 1 \end{array} \right],$$

is a generator matrix of \mathcal{C} . $n = 4 + 4 + 4 = 12$

$k = \dim_{\mathbb{F}_q}(\mathcal{C}) = (\alpha - \deg A_1(x)) + (\beta - \deg A_2(x)) + (\gamma - \deg A_3(x)) = (4 - 3) + (4 - 3) + (4 - 2) = 4.$

After using magma we found $d = 4$. Therefore, the code \mathcal{C} has parameters $[12, 4, 4]$.

Consider

$$\mathcal{C} = \mathbb{S}_{12}((x - \zeta^5)(x - \zeta^{10}) \mid 0 \mid 0) + \mathbb{S}_{12}(0 \mid (x - \zeta^5)(x - \zeta^{10}) \mid 0) + \mathbb{S}_{12}(\zeta^{10} \mid \zeta^5 \mid x + \zeta^{10}),$$

Hence

$$G_1 = \left(\begin{array}{cccc|cccc|cccc} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ \zeta^{10} & 0 & 0 & 0 & \zeta^5 & 0 & 0 & 0 & \zeta^{10} & 1 & 0 & 0 \\ 0 & \zeta^5 & 0 & 0 & 0 & \zeta^{10} & 0 & 0 & 0 & \zeta^5 & 1 & 0 \\ 0 & 0 & \zeta^{10} & 0 & 0 & 0 & \zeta^5 & 0 & 0 & 0 & \zeta^{10} & 1 \end{array} \right),$$

is a generator matrix of \mathcal{C} .

$$n = 4 + 4 + 4 = 12$$

$k = \dim_{\mathbb{F}_q}(\mathcal{C}) = (\alpha - \deg A_1(x)) + (\beta - \deg A_2(x)) + (\gamma - \deg A_3(x)) = (4 - 2) + (4 - 2) + (4 - 1) = 7.$

After using Magma we found $d = 2$. Therefore, the code \mathcal{C} has parameters $[12, 7, 2]$.

Using Types 6 and 7 in Corollary 3.8, we derive families of codes with good parameters.

Consider

$$\mathcal{C} = \mathbb{S}_{12}((x - 1)(x - \zeta^5)(x - \zeta^{10}) \mid 0 \mid 0) + \mathbb{S}_{12}(x^2 + \zeta x + 1 \mid 0 \mid \zeta^2),$$

Hence

$$G_1 = \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & \zeta & 1 & 0 & \zeta^2 & 0 & 0 & 0 \\ 0 & 1 & \zeta^2 & 1 & 0 & \zeta^4 & 0 & 0 \\ 1 & 0 & 1 & \zeta^4 & 0 & 0 & \zeta^8 & 0 \\ \zeta^8 & 1 & 0 & 1 & 0 & 0 & 0 & \zeta \end{array} \right),$$

is a generator matrix of \mathcal{C} .

$$n = 4 + 0 + 4 = 8$$

$k = \dim_{\mathbb{F}_q}(\mathcal{C}) = (\alpha - \deg A_1(x)) + (\beta - \deg A_2(x)) + (\gamma - \deg A_3(x)) = (4 - 3) + (0 - 0) + (4 - 0) = 5.$

After using Magma we found $d = 4$. Therefore, the code \mathcal{C} has parameters $[8, 5, 4]$.

Since $d = n - k + 1 = 8 - 5 + 1 = 4$, \mathcal{C} is an MDS code.

Consider

$$\mathcal{C} = \mathbb{S}_{12}(0 \mid (x - 1)(x - \zeta^5)(x - \zeta^{10}) \mid 0) + \mathbb{S}_{12}(0 \mid x - \zeta^{10} \mid x - \zeta^5).$$

Hence

$$G = \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ \zeta^{10} & 1 & 0 & 0 & \zeta^5 & 1 & 0 & 0 \\ 0 & \zeta^5 & 1 & 0 & 0 & \zeta^{10} & 1 & 0 \\ 0 & 0 & \zeta^{10} & 1 & 0 & 0 & \zeta^5 & 1 \end{array} \right),$$

is a generator matrix of \mathcal{C} .

$$n = 0 + 4 + 4 = 8$$

$$k = \dim_{\mathbb{F}_q}(\mathcal{C}) = (\alpha - \deg A_1(x)) + (\beta - \deg A_2(x)) + (\gamma - \deg A_3(x)) = +(0 - 0) + (4 - 3) + (4 - 1) = 4$$

After using magma we found $d = 4$. Therefore, the code \mathcal{C} has parameters $[8, 4, 4]$.

According to [10] Grassl's tables of bounds on the minimum distance of linear codes, the code \mathcal{C} is optimal.

Example 5.2. $\mathbb{F}_{27} = \{a_0 + a_1\omega + a_2\omega^2 \mid a_i \in \mathbb{F}_3\}$, where ω is a root of the irreducible polynomial $x^3 + 2x + 1 \in \mathbb{F}_3[x]$.

Let $\zeta = \omega^2 + 2\omega + 1 \in \mathbb{F}_{27}$.

Then ζ has order 13.

The polynomial $x^3 - 1$ can be factorized in the skew polynomial ring $\mathbb{F}_{27}[x; \theta]$, where

$$\theta(a) = a^3 \quad \text{for all } a \in \mathbb{F}_{27}.$$

as follows:

$$x^3 - 1 = (x - \zeta)(x - \zeta^9)(x - \zeta^3).$$

Using Types 6 in Corollary 3.8. Consider

$$\mathcal{C} = \mathbb{S}_6(x^2 + \zeta x + \zeta^{10} \mid 0 \mid 0) + \mathbb{S}_6(x - \zeta^3 \mid 0 \mid \zeta^9).$$

Hence

$$G = \left(\begin{array}{ccc|ccc} \zeta^{10} & \zeta & 1 & 0 & 0 & 0 \\ -\zeta^3 & 1 & 0 & \zeta^9 & 0 & 0 \\ 0 & -\zeta^9 & 1 & 0 & \zeta & 0 \\ 1 & 0 & -\zeta & 0 & 0 & \zeta^3 \end{array} \right),$$

is a generator matrix of \mathcal{C} .

$$n = 3 + 0 + 3 = 6$$

$$k = \dim_{\mathbb{F}_q}(\mathcal{C}) = (\alpha - \deg A_1(x)) + (\beta - \deg A_2(x)) + (\gamma - \deg A_3(x)) = +(3 - 2) + (0 - 0) + (3 - 0) = 4.$$

After using magma we found $d = 3$. Therefore, the code \mathcal{C} has parameters $[6, 4, 3]$.

Since $d = n - k + 1 = 6 - 4 + 1 = 3$, \mathcal{C} is an MDS code.

6. Conclusion

Triple θ -skew cyclic codes over \mathbb{F}_q generalize classical cyclic codes by employing skew polynomial rings endowed with multiple automorphisms. These codes, defined by generator polynomials in a noncommutative framework, demand a nuanced treatment of their duality properties; indeed, under certain conditions, the duals also exhibit skew cyclic structure. Practical implementations demonstrated using Magma confirm their error correcting capabilities and parameter settings. This innovative framework paves the way for new applications in coding theory, particularly in contexts where the interplay of symmetry and noncommutativity can be exploited to improve code performance. Future research is anticipated to further investigate their theoretical properties and potential generalizations.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

- [1] I. Aydogdu, R. M. Hesari, and K. Samei. Double skew cyclic codes over $f q$. *Computational and Applied Mathematics*, 41(3):126, 2022. <https://doi.org/10.1007/s40314-022-01833-2>.
- [2] A. Batoul, K. Guenda, and T. A. Gulliver. On self-dual cyclic codes over finite chain rings. *Designs, codes and cryptography*, 70(3):347–358, 2014. <https://doi.org/10.1007/s10623-012-9696-0>.
- [3] A. Batoul, K. Guenda, and T. A. Gulliver. Some constacyclic codes over finite chain rings. *Advances in Mathematics of Communications*, 10(4):683–694, 2016. <https://doi.org/10.3934/amc.2016034>.
- [4] N. Bennenni, N. Benbelkacem, N. Aydin, and P. Liu. Mixed skew cyclic codes over rings. *Journal of Algebra Combinatorics Discrete Structures and Applications*, 12(1):19–29, 2025. <https://doi.org/10.13069/jacodesmath.v12i1.339>.
- [5] J. Borges, C. Fernández-Córdoba, and R. Ten-Valls. $\mathbb{Z}_2\mathbb{Z}_2$ -double cyclic codes. *Designs, Codes and Cryptography*, 86(3):463–479, 2018. <https://doi.org/10.1007/s10623-017-0334-8>.
- [6] D. Boucher, W. Geiselmann, and F. Ulmer. Skew-cyclic codes. *Applicable Algebra in Engineering, Communication and Computing*, 18:379–389, 2007. <https://doi.org/10.1007/s00200-007-0043-z>.
- [7] D. Boucher and F. Ulmer. A note on the dual codes of module skew codes. In *IMA International Conference on Cryptography and Coding*, pages 230–243. Springer, 2011. https://doi.org/10.1007/978-3-642-25516-8_14.
- [8] L. Chaussade, P. Loidreau, and F. Ulmer. Skew codes of prescribed distance or rank. *Designs, Codes and Cryptography*, 50:267–284, 2009.
- [9] J. Gao, M. Shi, T. Wu, and F.-W. Fu. On double cyclic codes over \mathbb{Z}_4 . *Finite Fields and Their Applications*, 39:233–250, 2016. <https://doi.org/10.1016/j.ffa.2016.02.003>.
- [10] M. Grassl. Bounds on the minimum distance of linear codes and quantum codes. Online available at <http://www.codetables.de>, 2007. Accessed on 2025-08-16.
- [11] S. Jitman, S. Ling, and P. Udomkavanich. Skew constacyclic codes over finite chain rings. *Advances in Mathematics of Communications*, 6(1):39–63, 2012. <https://doi.org/10.3934/amc.2012.6.39>.
- [12] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*, volume 16. Elsevier, 1977.
- [13] H. Mostafanasab. Triple cyclic codes over \mathbb{Z}_2 . *Palestine Journal of Mathematics*, 6, 2017.
- [14] W. W. Peterson and D. T. Brown. Cyclic codes for error detection. *Proceedings of the IRE*, 49(1):228–235, 1961. <https://doi.org/10.1109/JRPROC.1961.287814>.

- [15] S. Verdu and T. S. Han. A general formula for channel capacity. *IEEE Transactions on Information Theory*, 40(4):1147–1157, 1994. <https://doi.org/10.1109/18.335960>.

Rachid Mammeri

Algebra and Number Theory Laboratory, Department of Algebra and Number Theory
Faculty of Mathematics, University of Science and Technology Houari Boumediene
BP 32, El Alia, 16111 Bab Ezzouar, Algiers, Algeria
E-mail rmammeri@usthb.dz

Nabil Bennenni

Algebra and Number Theory Laboratory, Department of Algebra and Number Theory
Faculty of Mathematics, University of Science and Technology Houari Boumediene
BP 32, El Alia, 16111 Bab Ezzouar, Algiers, Algeria
E-mail nabil.bennenni@gmail.com

Aicha Batoul

Algebra and Number Theory Laboratory, Department of Algebra and Number Theory
Faculty of Mathematics, University of Science and Technology Houari Boumediene
BP 32, El Alia, 16111 Bab Ezzouar, Algiers, Algeria
E-mail aicha.batoul@usthb.edu.dz