Bull. Korean Math. Soc. **57** (2020), No. 2, pp. 459–479 https://doi.org/10.4134/BKMS.b190325 pISSN: 1015-8634 / eISSN: 2234-3016

ON GENERALIZATIONS OF SKEW QUASI-CYCLIC CODES

SUMEYRA BEDIR, FATMANUR GURSOY, AND IRFAN SIAP

ABSTRACT. In the last two decades, codes over noncommutative rings have been one of the main trends in coding theory. Due to the fact that noncommutativity brings many challenging problems in its nature, still there are many open problems to be addressed. In 2015, generator polynomial matrices and parity-check polynomial matrices of generalized quasi-cyclic (GQC) codes were investigated by Matsui. We extended these results to the noncommutative case. Exploring the dual structures of skew constacyclic codes, we present a direct way of obtaining parity-check polynomials of skew multi-twisted codes in terms of their generators. Further, we lay out the algebraic structures of skew multipolycyclic codes and their duals and we give some examples to illustrate the theorems.

1. Introduction

The family of linear codes is huge. So, structural subfamilies have been always on the focus. The very first is the family of cyclic codes with a rich algebraic structure and applicability. Quasi-cyclic codes have been the next generalization of cyclic codes for which some very good and applicable codes are shown to be a member of such family of codes. The main idea in all of these attempts is to find a different subfamily of linear codes with concrete algebraic structures. For the last two decades research on linear codes has been shifted to cyclic codes over noncommutative rings, known as skew cyclic codes intensively. These are larger than the commutative ones and surely contain them as subfamilies. The pace for exploring these families has not been as in the commutative case. The problems due to the skewness property are more challenging. Natural generalizations of such codes for skew case are attempted and their structures are explored. As a concrete result and a partial contribution of this paper is the formulation of parity-check polynomial for skew constacyclic codes in terms of their generators whose existence has been known since its definition (see Theorem 4.4).

 $\odot 2020$ Korean Mathematical Society

Received March 25, 2019; Revised November 11, 2019; Accepted November 19, 2019. 2010 Mathematics Subject Classification. Primary 94B05, 94B60, 11T71.

Key words and phrases. Skew cyclic codes, skew quasi-cyclic codes, generalized quasi-cyclic codes, multi-twisted codes, polycyclic codes.

The flow of the paper is formed as follows: In Section 2, we present some basic definitions and review some literature related to our problems. Next, in Section 3, we present skew multi-twisted codes, a recently introduced generalization of generalized quasi-cyclic codes over noncommutative rings. Here, we approach the definition and the representation of this family of codes by representing them via generator matrices with entries from skew polynomial rings and state some related theorems regarding their structures both for codes and their duals. In Section 4, we explore the dual structure of skew constacyclic codes. Here, in Theorem 4.4, we explicitly state the parity-check polynomial for skew constacyclic codes which will be contributing to the duality theorem for skew multi-twisted codes. In Section 5, the structure of duals of skew multitwisted codes has been established and explored. Also, Theorem 5.6 presents a lower bound for both dimension and minimum distance of skew multi-twisted codes and some concrete examples are worked out. In the last section, Section 6, a larger family that contains skew multi-twisted codes, called skew multipolycyclic codes is introduced and their structures together with their duals are also explored. Theorems 6.3 and 6.5 state parity-check polynomials of skew polycyclic and skew multi-polycyclic codes respectively.

2. Skew cyclic codes

A linear code of length n over a finite field of order q, i.e., F_q , is an F_q subspace of F_q^n . A linear code C is said to be cyclic, if it is invariant under the cyclic shift, i.e., $(c_0, c_1, \ldots, c_{n-1}) \in C \Rightarrow (c_{n-1}, c_0, \ldots, c_{n-2}) \in C$. There is a one to one correspondence between cyclic codes and ideals of the quotient ring $F_q[x]/(x^n - 1)$ [29]. Recently, cyclic codes are extended to a noncommutative case using skew polynomials [7]. Skew polynomial rings were introduced by Ore in [28] and studied further by Jacobson [19] and McDonald [27].

Definition 1 ([27]). Let F_q be a finite field of order q and θ be an automorphism of F_q . The set of polynomials

$$F_{a}[x;\theta] = \{a_{0} + a_{1}x + \dots + a_{n}x^{n} \mid a_{i} \in F_{a}, n \in \mathbb{N}\}\$$

is called skew polynomial ring over F_q where addition is ordinary but multiplication is defined as $xa = \theta(a)x$ for all $a \in F_q$.

Skew polynomial rings are noncommutative unless θ is the identity automorphism. $F_q[x;\theta]$ is left and right Euclidean, i.e., both right and left division algorithms hold and any left or right ideal is principal. Factorization is not unique in $F_q[x;\theta]$. Let f(x) be a polynomial in $F_q[x;\theta]$. If f(x)p(x) = p(x)f(x) for all $p(x) \in F_q[x;\theta]$, then f(x) is called a central polynomial. The set of central polynomials of $F_q[x;\theta]$ is called the center of $F_q[x;\theta]$ and denoted by $\mathcal{Z}(F_q[x;\theta])$. Further, f(x) is a central polynomial if and only if it is of the form,

(1)
$$f(x) = a_0 + a_1 x^m + a_2 x^{2m} + \dots + a_n x^{nm}$$

where $a_i \in F_q^{\theta}$ (the fixed field of θ in F_q) and $m = |\langle \theta \rangle|$ is the order of θ [27].

We write $g(x)|_r f(x)$, if g(x) is a right divisor of f(x). The following lemma shows that two factors of a central polynomial commute.

Lemma 2.1 ([9, Lemma 7]). Let f(x) = h(x)g(x) in $F_q[x;\theta]$. If $f(x) \in \mathcal{Z}(F_q[x;\theta])$, then h(x)g(x) = g(x)h(x).

In [7], Boucher et al. generalized cyclic codes by using skew polynomial rings. A linear code C of length n over F_q is called skew cyclic, if it is invariant under the skew cyclic shift, i.e.,

 $(c_0, c_1, \ldots, c_{n-1}) \in C \Rightarrow (\theta(c_{n-1}), \theta(c_0), \ldots, \theta(c_{n-2})) \in C.$

A codeword $c = (c_0, c_1, \ldots, c_{n-1})$ corresponds to the polynomial $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$, hence the skew cyclic shift of c corresponds to xc(x) in the quotient ring $F_q[x;\theta]/(x^n-1)$. Boucher et al. show that skew cyclic codes are ideals of the ring $F_q[x;\theta]/(x^n-1)$, whenever $x^n - 1 \in \mathcal{Z}(F_q[x;\theta])$ [7]. Later, the restriction on $x^n - 1$ to be a central polynomial is removed by considering skew cyclic codes as left $F_q[x;\theta]$ -submodules of $F_q[x;\theta]/(x^n-1)$ in [31]. Skew cyclic codes, being a generalization of cyclic codes and covering a large and rich subclass of linear codes, present many advantages while searching for linear codes with structures and in some cases good parameters. In many recent studies such as [1,7], new record breaking codes were obtained via using skew polynomials. Further, by considering $x^n - \alpha$ and f(x) instead of $x^n - 1$ respectively, some further generalizations such as skew constacyclic codes [8,20] and module θ -codes (skew polycyclic codes) [9,10,26] are also studied.

The following preliminary result can be derived directly from Theorems 6, 7 and Lemma 2 of [31] by using similar methods, hence the proof is omitted.

Lemma 2.2. Let C be a left $F_q[x;\theta]$ -submodule of $F_q[x;\theta]/(f(x))$ where $f(x) \neq 0$ and $\deg(f(x)) > 0$. Let g(x) be a monic polynomial of minimum degree in C. Then g(x) is unique and C is principally generated by g(x), i.e., C = (g(x)). Moreover, g(x) is a right divisor of f(x) in $F_q[x;\theta]$ and $|C| = q^{\deg(f(x)) - \deg(g(x))}$.

Quasi-cyclic codes are another generalization of cyclic codes. They are asymptotically good [35]. Many studies have been conducted in terms of either exploring their algebraic structures [11, 21–23] or obtaining codes with good parameters [15–17, 32]. Recently, skew quasi-cyclic codes are introduced and some skew QC codes having minimum Hamming distances larger than previously best known linear codes of the same length and dimension are obtained [1].

Generalized quasi-cyclic (GQC) codes are QC codes with cyclic components of different lengths [33]. In [25], structures of the dual codes of GQC codes were studied by identifying generator matrices of GQC codes as upper triangular matrices with entries in $F_q[x]$.

Throughout this paper, a linear code C of length n, dimension k and minimum Hamming distance d is briefly denoted by [n, k, d]. A polynomial $g(x) = g_0 + g_1 x + \cdots + g_{n-1} x^{n-1}$ and its coefficient vector $g = (g_0, g_1, \ldots, g_{n-1})$ will be used interchangeably where there is no confusion. The notation $g \cdot h$ stands for the Euclidean inner product of vectors g and h. By the term dual code, or C^{\perp} , we mean the dual code of C with respect to the Euclidean inner product. For an arbitrary matrix P, P^{tr} denotes the transpose of P.

3. Skew multi-twisted codes

Multi-twisted codes have been proposed by Aydin and Halilović [3] and their duals have been explored recently by Sharma et al. [30].

Definition 2. Let C be a linear code over F_q and

$$c = (c_{1,1}, \dots, c_{1,n_1-1}, c_{1,n_1}, c_{2,1}, \dots, c_{2,n_2-1}, c_{2,n_2}, \dots, c_{l,1}, \dots, c_{l,n_l-1}, c_{l,n_l})$$

be a codeword of C. Let θ be an automorphism of F_q , $\alpha_1, \alpha_2, \ldots, \alpha_l \in F_q^*$ and $\overline{\alpha} = (\alpha_1, \ldots, \alpha_l)$. If skew $\overline{\alpha}$ -multi-twisted shift of c;

$$T_{\overline{\alpha}}(c) = (\alpha_1 \theta(c_{1,n_1}), \theta(c_{1,1}), \dots, \theta(c_{1,n_1-1}), \alpha_2 \theta(c_{2,n_2}), \theta(c_{2,1}), \dots, \theta(c_{2,n_2-1}), \dots, \alpha_l \theta(c_{l,n_l}), \theta(c_{l,1}), \dots, \theta(c_{l,n_l-1}))$$

is also a codeword in C, then C is a skew $\overline{\alpha}$ -multi-twisted code of length (n_1, n_2, \ldots, n_l) .

Briefly, a multi-twisted code is a GQC code with constacyclic components. The case where $\alpha_i = 1$ for all $1 \leq i \leq l$ corresponds to a skew GQC code [13], and the case where l = 1 corresponds to a skew constacyclic code which is invariant under skew α -constacyclic shift [8].

Let $R = F_q[x; \theta]$ and $R_i = F_q[x; \theta]/(x^{n_i} - \alpha_i)$. In polynomial representation form, a skew $\overline{\alpha}$ -multi-twisted code C is a left R-submodule of $M = R_1 \times R_2 \times \cdots \times R_l$. Here, we adopt and extend the method introduced in [25] to a family of skew $\overline{\alpha}$ -multi-twisted codes. Let

$$\phi: F_q[x;\theta]^l \to M$$

(f₁, f₂,..., f_l) \to (f₁ mod ($x^{n_1} - \alpha_1$), f₂ mod ($x^{n_2} - \alpha_2$),..., f_l mod ($x^{n_l} - \alpha_l$)).

For a skew $\overline{\alpha}$ -multi-twisted code C, define $D = \phi^{-1}(C)$. For the zero codeword $(0, 0, \ldots, 0) \in C$, its preimage $\phi^{-1}((0, 0, \ldots, 0))$ consists of the vectors of the following form:

(2)
$$(\underbrace{0,\ldots,0}_{i-1},x^{n_i}-\alpha_i,\underbrace{0,\ldots,0}_{l-i})$$

for all $1 \leq i \leq l$. Conversely, if a left *R*-submodule $D \subset F_q[x; \theta]^l$ includes l polynomial vectors of the form (2), then $\phi(D)$ determines a skew $\overline{\alpha}$ -multi-twisted code. We view a skew $\overline{\alpha}$ -multi-twisted code *C* in $F_q[x; \theta]^l$ as a submodule and identify each skew $\overline{\alpha}$ -multi-twisted code with an $l \times l$ polynomial generator matrix.

Definition 3. Let C be a skew $\overline{\alpha}$ -multi-twisted code, and let $G = [g_{i,j}(x)]$ be an $l \times l$ matrix whose entries are in $F_q[x; \theta]$ and whose rows are codewords of C. If G is upper-triangular of the form

(3)
$$G = \begin{bmatrix} g_{1,1}(x) & g_{1,2}(x) & \cdots & g_{1,l}(x) \\ 0 & g_{2,2}(x) & \cdots & g_{2,l}(x) \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & g_{l,l}(x) \end{bmatrix}_{l \times l}$$

and if for all $1 \leq i \leq l$, $g_{i,i}(x)$ has the smallest degree among all codewords of the form $(0, \ldots, 0, c_i(x), \ldots, c_l(x)) \in C$ with $c_i(x) \neq 0$, then G is a generator polynomial matrix of C. Moreover, if G satisfies the conditions that $g_{i,i}(x)$ is monic for all $1 \leq i \leq l$ and deg $g_{i,j}(x) < \deg g_{j,j}(x)$ for all $1 \leq i \neq j \leq l$, then we call G the reduced generator polynomial matrix of C.

In [25], for the commutative case, Buchberger's algorithm is applied to show the existence of polynomials in the reduced generator polynomial matrix Gwhich is uniquely determined. Since the skew polynomial ring $F_q[x;\theta]$ is right Euclidean, i.e., right division algorithm holds for polynomials in $F_q[x;\theta]$ [27], the same approach can be applied to a skew $\overline{\alpha}$ -multi-twisted code C to obtain the reduced generator polynomial matrix given in Definition 3. In this case, division should be considered as the right division in $F_q[x;\theta]$ and gcd of polynomials as gcrd (greatest common right divisor).

Considering the results in [25] and [34], and by Definition 3, we can state the following remark on the dimension of a code C.

Remark 3.1 (Dimension of C). Let C be a skew $\overline{\alpha}$ -multi-twisted code and G be the reduced generator polynomial matrix of C. Then, the dimension of C is

$$\dim(C) = \sum_{i=1}^{l} n_i - \deg(g_{i,i}(x)).$$

Given a reduced generator polynomial matrix for a code C, the problem of obtaining a reduced parity-check polynomial matrix H will be resolved later in Theorem 5.3. Here, we define a reduced parity-check polynomial matrix as follows:

Definition 4. Let C be a skew $\overline{\alpha}$ -multi-twisted code, and let $H = [h_{i,j}(x)]$ be an $l \times l$ matrix whose entries are in $F_q[x; \theta]$ and whose rows are codewords from C^{\perp} . If H is in a lower-triangular form as follows

(4)
$$H = \begin{bmatrix} h_{1,1}(x) & 0 & \cdots & 0 \\ h_{2,1}(x) & h_{2,2}(x) & \ddots & \vdots \\ \vdots & \vdots & \ddots & 0 \\ h_{l,1}(x) & h_{l,2}(x) & \cdots & h_{l,l}(x) \end{bmatrix}_{l \times l}$$

and if for all $1 \leq i \leq l, h_{i,i}(x)$ have the minimum degrees among all codewords of the form $(c_1(x), \ldots, c_i(x), 0, \ldots, 0) \in C^{\perp}$ with $c_i(x) \neq 0$, then *H* is a *paritycheck polynomial matrix* of *C*. Moreover, if *H* satisfies the conditions that $h_{i,i}(x)$ are also monic for all $1 \leq i \leq l$ and $\deg h_{i,j}(x) < \deg h_{j,j}(x)$ for all $1 \leq i \neq j \leq l$, then we call *H* the *reduced parity-check polynomial matrix* of *C*.

The following propositions can be derived similar to their corresponding commutative cases given as Propositions 2, 3 and 5 in [25], so we omit their proofs.

Proposition 3.2. Let G be an $l \times l$ reduced polynomial matrix as in (3). Then G is the reduced generator polynomial matrix of a skew $\overline{\alpha}$ -multi-twisted code C if and only if there exists an $l \times l$ matrix A with entries in $F_q[x; \theta]$ such that

(5)
$$AG = diag[x^{n_1} - \alpha_1, \dots, x^{n_l} - \alpha_l].$$

Proposition 3.3. Let G be an $l \times l$ reduced polynomial matrix as in (3) and $A = [a_{i,j}]$ be a matrix satisfying (5). Then A is an upper triangular matrix, satisfying deg $(a_{i,i}) > deg (a_{i,j})$ for all $1 \le i \ne j \le l$.

4. Duality theorem for skew constacyclic codes

Skew multi-twisted codes with l = 1 are skew constacyclic codes which are introduced in [8] and some properties of this family are given in [12] and [20]. In polynomial representation, skew α -constacyclic codes correspond to left $F_q[x;\theta]$ -submodules of $F_q[x;\theta]/(x^n - \alpha)$. In fact, a skew α -constacyclic code Cof length n is principally generated by a right divisor g(x) of $x^n - \alpha$ in $F_q[x;\theta]$, i.e., C = (g(x)). In this section, given the generator of a skew constacyclic code, we introduce a direct method of finding the generator of the dual code explicitly. Throughout this section we set $m \mid n$, where $m = |\langle \theta \rangle|$.

Lemma 4.1. Let $x^n - \alpha \in F_q[x; \theta]$, $o(\alpha)$ be the multiplicative order of α in F_q^* and $N = o(\alpha)n$. Then, $x^n - \alpha$ is a right divisor of the central polynomial $x^N - 1$ in $F_q[x; \theta]$.

Proof. Let $N = o(\alpha)n$. Then,

$$x^{N} - 1 = (\alpha^{-1} + \alpha^{-2}x^{n} + \alpha^{-3}x^{2n} + \dots + \alpha^{-o(\alpha)}x^{(o(\alpha)-1)n})(x^{n} - \alpha).$$

Since $m \mid n$, we have $x^N - 1 \in \mathcal{Z}(F_q[x;\theta])$ and from Lemma 2.1, $x^N - 1 = (x^n - \alpha)(\alpha^{-1} + \alpha^{-2}x^n + \alpha^{-3}x^2n + \dots + \alpha^{-o(\alpha)}x^{(o(\alpha)-1)n})$. We simply use the expression $\frac{x^N - 1}{x^n - \alpha}$ for the right division of $x^N - 1$ by $x^n - \alpha$.

Lemma 4.2. Let $\alpha_i \in F_q^*$ and n_i be a positive integer such that $m|n_i$ for $1 \leq i \leq l$. Then

$$x^{n_i} - \alpha_i|_r x^N - 1$$

where $N = \operatorname{lcm}(n_1, n_2, \ldots, n_l)\operatorname{lcm}(o(\alpha_1), \ldots, o(\alpha_l)).$

Proof. By Lemma 4.1, we have

$$(\alpha_i^{-1} + \alpha_i^{-2}x^{n_i} + \alpha_i^{-3}x^{2n_i} + \dots + \alpha_i^{-o(\alpha_i)}x^{(o(\alpha_i)-1)n_i})(x^{n_i} - \alpha_i) = x^{n_i o(\alpha_i)} - 1$$

and we also have

$$o(\alpha_i)n_i \mid \operatorname{lcm}(n_1, n_2, \ldots, n_l)\operatorname{lcm}(o(\alpha_1), \ldots, o(\alpha_l)).$$

Hence,

$$x^{n_i o(\alpha_i)} - 1|_r x^N - 1.$$

Therefore $x^{n_i} - \alpha_i |_r x^N - 1$.

In [20], Lemma 3.1 shows that the dual of a skew α -constacyclic code is a skew α^{-1} -constacyclic code, with a restriction on α being fixed by θ . This lemma holds for any $\alpha \in F_q^*$, and can be proved by using the same method.

Lemma 4.3 ([20], Lemma 3.1). Let C be a skew α -constacyclic code of length n over F_q , where $\alpha \in F_q^*$. Then the dual code C^{\perp} is a skew α^{-1} -constacyclic code of length n over F_q .

In order to determine the generator polynomials of dual codes, the following definition will be crucial.

Definition 5. Let n be a positive integer and $a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} \in F_q[x;\theta]$ with $\deg(a(x)) \leq n-1$. We define

$$a^{\langle n,\alpha\rangle}(x) = \alpha^{-1}a_0 + \theta(a_{n-1})x + \theta^2(a_{n-2})x^2 + \dots + \theta^{n-1}(a_1)x^{n-1}.$$

Let $x^n - \alpha = a(x)g(x)$ with $\deg(a(x)) = k$ and C = (g(x)). If we were dealing with the case $\alpha = 1$, i.e., skew cyclic case, skew reciprocal polynomial of a(x), which is defined as $a^R(x) = a_k + \theta(a_{k-1})x + \cdots + \theta^k(a_0)x^k$, would be a right divisor of $x^n - 1$ and thus a generator polynomial for C^{\perp} [9]. However, for the skew constacyclic case, $x^n - \alpha = a(x)g(x)$ does not imply $a^R(x)|_r x^n - \alpha^{-1}$ nor does it imply $C^{\perp} = (a^R(x))$. In [10] the authors determined that $C^{\perp} = (h^R(x))$ where h(x) is a polynomial satisfying $x^n - \theta^{-k}(\alpha) = g(x)h(x)$, this guarantees the existence but is implicit and the process involves a query to find such a polynomial h(x). Later in [12] in Theorem 6.1, authors obtained the generator of the dual code in terms of h(x), while $x^n - \alpha = h(x)g(x)$, by using the properties of skew generalized circulant matrices.

In the following theorem, we give an alternative algorithm to find the generator polynomial of C^{\perp} directly by using $a^{\langle n,\alpha\rangle}(x)$.

Theorem 4.4. Let $x^n - \alpha = a(x)g(x)$ in $F_q[x; \theta]$ and C be a skew α -constacyclic code generated by g(x). Then, $a^{\langle n, \alpha \rangle} \in C^{\perp}$. Moreover, $C^{\perp} = (x^k a^{\langle n, \alpha \rangle}(x))$, where $k = \deg(a(x))$.

Proof. Let $g(x) = g_0 + g_1 x + \dots + g_{n-1} x^{n-1}$ and $a(x) = a_0 + a_1 x + \dots + a_{n-1} x^{n-1}$. Let us multiply both sides of $x^n - \alpha = a(x)g(x)$ from left by $\frac{x^N - 1}{x^n - \alpha}$, where

465

 $N = o(\alpha)n$. We obtain,

$$x^N - 1 = \frac{x^N - 1}{x^n - \alpha} a(x)g(x).$$

Since $x^N - 1 \in \mathcal{Z}(F_q[x;\theta])$, from Lemma 2.1 we can write

$$x^{N} - 1 = g(x)\frac{x^{N} - 1}{x^{n} - \alpha}a(x),$$

which means

 $g(x)(\alpha^{-1} + \alpha^{-2}x^n + \alpha^{-3}x^{2n} + \dots + \alpha^{-o(\alpha)}x^{(o(\alpha)-1)n})a(x) = 0 \pmod{x^N - 1}.$ This is equivalent to

(6)

 $g(x)\alpha^{-1}a(x) + g(x)\alpha^{-2}a(x)x^n + \dots + g(x)a(x)x^{(o(\alpha)-1)n} = 0 \pmod{x^N - 1}$ since $\alpha^{-o(\alpha)} = 1$ and $x^n \in \mathcal{Z}(F_a[x;\theta]).$

The coefficient of x^0 in Equation (6) is $g_0 \alpha^{-1} a_0 + g_1 \theta(a_{n-1}) + g_2 \theta^2(a_{n-2}) + \cdots + g_{n-1} \theta^{n-1}(a_1) = 0$ which implies $g \cdot a^{\langle n, \alpha \rangle} = 0$. To prove $a^{\langle n, \alpha \rangle} \in C^{\perp}$, we need to show that $a^{\langle n, \alpha \rangle}$ is orthogonal to all skew α -constacyclic shifts of g. Let us denote the skew α -constacyclic shift by T_{α} . If we multiply Equation

(6) with x from left, then the coefficient of x^0 becomes

$$\theta(g_{n-1})a_0 + \theta(g_0)\theta(a_{n-1}) + \theta(g_1)\theta^2(a_{n-2}) + \dots + \theta(g_{n-2})\theta^{n-1}(a_1) = 0.$$

This implies that $T_{\alpha}(g) \cdot a^{\langle n, \alpha \rangle} = 0$. Similarly, if we multiply Equation (6) with x^i from left, we obtain $T^i_{\alpha}(g) \cdot a^{\langle n, \alpha \rangle} = 0$. Thus, we have $a^{\langle n, \alpha \rangle} \in C^{\perp}$.

Now let us show that $C^{\perp} = (x^k a^{\langle n, \alpha \rangle}(x))$. Since C^{\perp} is a skew α^{-1} constacyclic code, it is a left $F_q[x; \theta]$ -submodule of $F_q[x; \theta]/(x^n - \alpha^{-1})$. Thus $x^i a^{\langle n, \alpha \rangle}(x) \in F_q[x; \theta]/(x^n - \alpha^{-1})$ also belongs to C^{\perp} . We have,

$$\deg(a(x)) = k \implies \deg(x^k a^{\langle n, \alpha \rangle}(x)) = k \text{ in } F_q[x; \theta] / (x^n - \alpha^{-1}).$$

Since the quotient ring is principal and the dimension of C^{\perp} is n-k, there is no polynomial in C^{\perp} with degree less than k. Therefore C^{\perp} is indeed generated by $x^k a^{\langle n, \alpha \rangle}(x)$.

5. Duality theorem for skew multi-twisted codes

In this section, we state and prove a theorem that reveals the structure of dual codes of skew $(\alpha_1, \ldots, \alpha_l)$ -multi-twisted codes. This goal is achieved by generalizing Theorem 4.4 for l > 1 and obtaining the reduced parity-check polynomial matrices of skew $(\alpha_1, \ldots, \alpha_l)$ -multi-twisted codes from their reduced generator polynomial matrices. Throughout this section we set $m | n_i$, where $m = |\langle \theta \rangle|$.

Theorem 5.1. Let C be a skew $(\alpha_1, \ldots, \alpha_l)$ -multi-twisted code of length (n_1, \ldots, n_l) over F_q . Then, the dual code C^{\perp} is a skew $(\alpha_1^{-1}, \ldots, \alpha_l^{-1})$ -multi-twisted code.

Proof. Let $T_{\overline{\alpha}^{-1}}(c)$ be the skew $(\alpha_1^{-1}, \ldots, \alpha_l^{-1})$ -multi-twisted shift of c. Let

$$c = (c_{1,1}, \dots, c_{1,n_1-1}, c_{1,n_1}, c_{2,1}, \dots, c_{2,n_2-1}, c_{2,n_2}, \dots, c_{l,1}, \dots, c_{l,n_l-1}, c_{l,n_l}) \in C$$

and

$$d = (d_{1,1}, \dots, d_{1,n_1-1}, d_{1,n_1}, d_{2,1}, \dots, d_{2,n_2-1}, d_{2,n_2}, \dots, d_{l,1}, \dots, d_{l,n_l-1}, d_{l,n_l}) \in C^{\perp},$$

then $c \cdot d = \sum_{j=1}^{l} \sum_{i=1}^{n_j} c_{j,i} d_{j,i} = 0$. We want to show that $c \cdot T_{\overline{\alpha}^{-1}}(d) = 0$, i.e., $T_{\overline{\alpha}^{-1}}(d) \in C^{\perp}$.

Since C has a finite number of codewords, there exists a number s such that $T^s_{\overline{\alpha}}(c) = c$. Let

$$w = T_{\overline{\alpha}}^{s-1}(c) = (\theta^{-1}(c_{1,2}), \dots, \theta^{-1}(c_{1,n_1}), \theta^{-1}(\alpha_1^{-1}c_{1,1}), \\ \theta^{-1}(c_{2,2}), \dots, \theta^{-1}(c_{2,n_2}), \theta^{-1}(\alpha_2^{-1}c_{2,1}), \dots, \\ \theta^{-1}(c_{l,2}), \dots, \theta^{-1}(c_{l,n_l}), \theta^{-1}(\alpha_l^{-1}c_{l,1})).$$

Then,

$$0 = w \cdot d = (\theta^{-1}(c_{1,2})d_{1,1} + \dots + \theta^{-1}(c_{1,n_1})d_{1,n_1-1} + \theta^{-1}(\alpha_1^{-1}c_{1,1})d_{1,n_1}) + (\theta^{-1}(c_{2,2})d_{2,1} + \dots + \theta^{-1}(c_{2,n_2})d_{2,n_2-1} + \theta^{-1}(\alpha_2^{-1}c_{2,1})d_{2,n_2}) + \dots + (\theta^{-1}(c_{l,2})d_{l,1} + \dots + \theta^{-1}(c_{l,n_l})d_{l,n_l-1} + \theta^{-1}(\alpha_l^{-1}c_{l,1})d_{l,n_l}).$$

Since $\theta(0) = 0$, we have

$$0 = [(c_{1,1}, c_{1,2}, \dots, c_{1,n_1}) \cdot (\alpha_1^{-1}\theta(d_{1,n_1}), \theta(d_{1,1}), \dots, \theta(d_{1,n_{1-1}}))] + [(c_{2,1}, c_{2,2}, \dots, c_{2,n_1}) \cdot (\alpha_2^{-1}\theta(d_{2,n_2}), \theta(d_{2,1}), \dots, \theta(d_{2,n_{2-1}}))] + \dots + [(c_{l,1}, c_{l,2}, \dots, c_{l,n_l}) \cdot (\alpha_l^{-1}\theta(d_{l,n_l}), \theta(d_{l,1}), \dots, \theta(d_{l,n_{l-1}}))] = c \cdot T_{\overline{\alpha}^{-1}}(d).$$

Therefore C^{\perp} is a skew $(\alpha_1^{-1}, \ldots, \alpha_l^{-1})$ -multi-twisted code.

Lemma 5.2. Let G be the reduced generator polynomial matrix of a skew $\overline{\alpha}$ -multi-twisted code C, A be the $l \times l$ upper triangular polynomial matrix satisfying $AG = diag[x^{n_1} - \alpha_1, \ldots, x^{n_l} - \alpha_l]$, and $N = lcm(n_1, \ldots, n_l)lcm(o(\alpha_1), \ldots, o(\alpha_l))$. Then $G'A = diag[x^N - 1, \ldots, x^N - 1]$, where

$$G' = G \operatorname{diag} \left[\frac{x^N - 1}{x^{n_1} - \alpha_1}, \dots, \frac{x^N - 1}{x^{n_l} - \alpha_l} \right].$$

Proof. Let I be the $l \times l$ identity matrix.

$$AG = diag [x^{n_1} - \alpha_1, \dots, x^{n_l} - \alpha_l]$$

$$\Rightarrow diag [\frac{x^N - 1}{x^{n_1} - \alpha_1}, \dots, \frac{x^N - 1}{x^{n_l} - \alpha_l}]AG = (x^N - 1)I$$

467

S. BEDIR, F. GURSOY, AND I. SIAP

$$\Rightarrow Gdiag[\frac{x^N - 1}{x^{n_1} - \alpha_1}, \dots, \frac{x^N - 1}{x^{n_l} - \alpha_l}]AG = G(x^N - 1)I \Rightarrow G'AG = (x^N - 1)G, \text{ since } x^N - 1 \in \mathcal{Z}(F_q[x; \theta]) \Rightarrow G'AG - (x^N - 1)G = 0 \Rightarrow (G'A - (x^N - 1)I)G = 0.$$

Since G is an upper triangular polynomial matrix with nonzero diagonal entries and $F_q[x;\theta]$ has no zero divisors, $G'A - (x^N - 1)I = 0$ which implies $G'A = (x^N - 1)I = diag [x^N - 1, \dots, x^N - 1]$.

Theorem 5.3. Let $G = [g_{i,j}(x)]$ be the reduced generator polynomial matrix of a skew $\overline{\alpha}$ -multi-twisted code C of length (n_1, \ldots, n_l) over F_q where $\overline{\alpha} = (\alpha_1, \ldots, \alpha_l) \in (F_q^*)^l$, and let $A = [a_{i,j}(x)]$ be the polynomial matrix which satisfies $AG = diag[x^{n_1} - \alpha_1, \ldots, x^{n_l} - \alpha_l]$. Then,

$$H = \begin{bmatrix} x^{\deg a_{1,1}} a_{1,1}^{\langle n_1, \alpha_1 \rangle}(x) & 0 & \cdots & 0 \\ x^{\deg a_{2,2}} a_{1,2}^{\langle n_1, \alpha_1 \rangle}(x) & x^{\deg a_{2,2}} a_{2,2}^{\langle n_2, \alpha_2 \rangle}(x) & \ddots & \vdots \\ \vdots & \vdots & \ddots & 0 \\ x^{\deg a_{l,l}} a_{1,l}^{\langle n_1, \alpha_1 \rangle}(x) & x^{\deg a_{l,l}} a_{2,l}^{\langle n_2, \alpha_2 \rangle}(x) & \cdots & x^{\deg a_{l,l}} a_{l,l}^{\langle n_l, \alpha_l \rangle}(x) \end{bmatrix}_{l \times l}$$

where each i^{th} column of H is considered modulo $x^{n_i} - \alpha_i^{-1}$. If $a_{i,i}(x) = x^{n_i} - \alpha_i$, then we set $x^{\deg a_{i,i}} a_{i,i}^{\langle n_i, \alpha_i \rangle}(x) = x^{n_i} - \alpha_i^{-1}$. Then, H is a parity-check polynomial matrix of C.

Proof. Let $N = lcm(n_1, \ldots, n_k)lcm(o(\alpha_1), \ldots, o(\alpha_l))$ and G' be defined as in Lemma 5.2. From Lemma 5.2 we have $G'A = diag[x^N - 1, \ldots, x^N - 1]$ where

$$\sum_{k=1}^{l} g_{i,k}(x) \frac{x^N - 1}{x^{n_k} - \alpha_k} a_{k,j}(x) = \begin{cases} 0, & i \neq j \\ x^N - 1, & i = j \end{cases}$$

for $1 \leq i, j \leq l$. Thus, for a fixed i and j we have

(7)
$$g_{i,1}(x)\frac{x^N-1}{x^{n_1}-\alpha_1}a_{1,j}(x) + g_{i,2}(x)\frac{x^N-1}{x^{n_2}-\alpha_2}a_{2,j}(x) + \dots + g_{i,l}(x)\frac{x^N-1}{x^{n_l}-\alpha_l}a_{l,j}(x) = 0 \pmod{x^N-1}.$$

From Theorem 4.4, the coefficient of x^0 in Equation (7) is

$$g_{i,1} \cdot a_{1,j}^{\langle n_1,\alpha_1 \rangle} + g_{i,2} \cdot a_{2,j}^{\langle n_2,\alpha_2 \rangle} + \dots + g_{i,l} \cdot a_{l,j}^{\langle n_l,\alpha_l \rangle} = 0,$$

which implies $(g_{i,1}, g_{i,2}, \ldots, g_{i,l}) \cdot (a_{1,j}^{\langle n_1, \alpha_1 \rangle}, a_{2,j}^{\langle n_2, \alpha_2 \rangle}, \ldots, a_{l,j}^{\langle n_l, \alpha_l \rangle}) = 0.$ Using the same approach as in the proof of Theorem 4.4, if we multiply Equa-

Using the same approach as in the proof of Theorem 4.4, if we multiply Equation (7) with x^b from left, then the coefficient of x^0 gives $T^b_{\alpha}((g_{i,1}, g_{i,2}, \ldots, g_{i,l})) \cdot (a_{1,j}^{\langle n_1, \alpha_1 \rangle}, a_{2,j}^{\langle n_2, \alpha_2 \rangle}, \ldots, a_{l,j}^{\langle n_l, \alpha_l \rangle}) = 0$. Hence, $(a_{1,j}^{\langle n_1, \alpha_1 \rangle}, a_{2,j}^{\langle n_2, \alpha_2 \rangle}, \ldots, a_{l,j}^{\langle n_l, \alpha_l \rangle})$ is in C^{\perp} for all $i, j \in \{1, \ldots, l\}$.

Thus $x^{\deg a_{j,j}}(a_{1,j}^{\langle n_1,\alpha_1 \rangle}(x), a_{2,j}^{\langle n_2,\alpha_2 \rangle}(x), \ldots, a_{l,j}^{\langle n_l,\alpha_l \rangle}(x))$, which is exactly the *j*th row of H, also belongs to C^{\perp} . Lastly, we need to show that the diagonal entries of H satisfy the minimum degree condition in Definition 4. This can be shown by using similar tools as in Theorem 1 of [25]. The same arguments hold for the skew polynomial case since we are working on left modules.

Here, we give some concrete examples to illustrate our theoretical results.

Example 5.4. Let θ be an automorphism of F_4 defined by $\theta(\beta) = \beta^2$ for any $\beta \in F_4$, in this case $|\langle \theta \rangle| = 2$. We consider the skew polynomial ring $F_4[x; \theta]$ where $F_4 = \{0, 1, \alpha, \alpha^2\}$. Let

$$A = \begin{bmatrix} x^4 + \alpha^2 x^3 + \alpha^2 x + 1 & x^3 + x^2 + \alpha^2 x + \alpha & x^3 + \alpha^2 x^2 + x \\ 0 & x + 1 & \alpha^2 \\ 0 & 0 & 1 \end{bmatrix}_{3 \times 3}$$

and

$$G = \left[\begin{array}{cccc} x^2 + \alpha^2 x + 1 & x^2 + \alpha^2 x + \alpha & x^3 + \alpha^2 x^2 + 1 \\ 0 & x^3 + x^2 + x + 1 & \alpha x^3 + \alpha^2 x^2 + \alpha x + \alpha^2 \\ 0 & 0 & x^4 + 1 \end{array} \right]_{3 \times 3}.$$

The above matrices satisfy $AG = diag[x^6 - 1, x^4 - 1, x^4 - 1]$. Therefore G is a generator matrix for a skew GQC code C of length (6,4,4) and C is a [14,5,4] code. By Theorem 5.3, the parity-check polynomial matrix for C is

$$H = \begin{bmatrix} x^4 + \alpha x^3 + \alpha x + 1 & 0 & 0\\ x^5 + x^4 + \alpha^2 x + \alpha^2 & x + 1 & 0\\ x^5 + \alpha^2 x^4 + x^3 & \alpha^2 & 1 \end{bmatrix}_{3\times 3}$$

Further, we present their corresponding generator matrices of the code and its dual

Now, one can easily check that $G \cdot H^{tr} = 0$ and the dual code C^{\perp} is a [14, 9, 3] code.

Example 5.5. Next we consider again the skew polynomial ring $F_4[x;\theta]$ given in Example 5.4, with the following moderate size matrices:

$$A = \begin{bmatrix} x^2 + \alpha & 1 & 0 \\ 0 & x^4 + \alpha^2 & x^2 + \alpha \\ 0 & 0 & 1 \end{bmatrix}_{3\times 3}^{3\times 3},$$
$$G = \begin{bmatrix} x^2 + \alpha & x^2 + \alpha & x^4 + \alpha^2 \\ 0 & x^4 + \alpha^2 & x^6 + \alpha x^4 + \alpha^2 x^2 + 1 \\ 0 & 0 & x^8 + \alpha \end{bmatrix}_{3\times 3}$$

It can be easily shown that $AG = diag[x^4 - \alpha^2, x^8 - \alpha, x^8 - \alpha]$. Therefore G is a generator matrix for a skew $\overline{\alpha}$ -multi-twisted code C of length (4, 8, 8), where $\overline{\alpha} = (\alpha^2, \alpha, \alpha)$,

From Theorem 3.1, $\dim(C) = \sum n_i - \deg(g_{i,i}) = 2 + 4 + 0 = 6$. *C* is a [20, 6, 4] code. By Theorem 5.3, the parity-check polynomial matrix for *C* is

$$H = \left[\begin{array}{ccc} x^2 + \alpha^2 & 0 & 0 \\ \alpha & x^4 + \alpha & 0 \\ 0 & x^6 + 1 & \alpha^2 \end{array} \right]_{3 \times 3}$$

Now, we state the following theorem as a note on the minimum distance bound for 1-generator skew $\overline{\alpha}$ -multi-twisted codes. Moreover, Corollary 5.7 is an application of Theorem 2.2 given in [3] for a noncommutative case.

Theorem 5.6. Let C be a skew $\overline{\alpha}$ -multi-twisted code over F_q with $\overline{\alpha} = (\alpha_1, \ldots, \alpha_l)$ and length (n_1, \ldots, n_l) . Let $x^{n_i} - \alpha_i = a_i(x)g_i(x)$ and C_{g_i} be the skew α_i constacyclic code generated by $g_i(x)$ of length n_i . Suppose that C is generated
by $(f_1(x)g_1(x), f_2(x)g_2(x), \ldots, f_l(x)g_l(x))$ where $f_i(x)$ are in $\mathcal{Z}(F_q[x;\theta])$ and $gcrd(f_i(x), a_i(x)) = 1$ for all $1 \leq i \leq l$. Then, C is a $[\sum_{i=1}^l n_i, k, d]$ code where $k \geq \max\{\deg(a_i(x))\}$ and $d \geq \min\{d(C_{g_i})\}$.

Corollary 5.7. Let $\alpha \in F_q^*$ and $x^n - \alpha = a(x)g(x)$ in $F_q[x;\theta]$. Let C_g be the skew α -constacyclic code generated by g(x) of length n. Let C be a skew $\overline{\alpha}$ -multi-twisted code over F_q with $\alpha_i = \alpha$ and $n_i = n$ for all $1 \leq i \leq l$. Suppose that C is generated by $(f_1(x)g(x), f_2(x)g(x), \ldots, f_l(x)g(x))$ where $f_i(x)$ are in $\mathcal{Z}(F_q[x;\theta])$ and $gcrd(f_i(x), a(x)) = 1$ for all $1 \leq i \leq l$. Then, C is a $[nl, n - \deg(g(x)), d]$ code where $d \geq n \cdot d(C_q)$.

Proof. First, since $f_i(x) \in \mathcal{Z}(F_q[x;\theta])$, we have

$$a(x)f_i(x)g(x) = f_i(x)a(x)g(x) = 0 \pmod{x^n - \alpha}, \ 1 \le i \le l.$$

We need to show that there is no other polynomial p(x) with degree less than $\deg(a(x))$ that makes either of the components zero, i.e., $p(x)f_i(x)g(x) \neq 0$ (mod $x^n - \alpha$).

470

and

Suppose that we have such a polynomial p(x). Then, $p(x)f_i(x)g(x) = 0$ (mod $x^n - \alpha$) for some *i*. In this case, $a(x)|_r p(x)f_i(x)$, thus, $p(x)f_i(x) = q(x)a(x)$ for some $q(x) \in F_q[x;\theta]$, which implies $gcrd(a(x), f_i(x)) \neq 1$ and leads to a contradiction. The rest of the proof can be completed in a similar way as in Theorem 3.2 of [4]. So, we omit the details.

Now we present some examples in order to illustrate the results obtained above.

Example 5.8. We consider the skew polynomial ring $F_4[x; \theta]$ given in Example 5.4.

A factorization of $x^{14} - 1$ in $F_4[x; \theta]$ is as follows

 $\begin{aligned} x^{14} - 1 &= (x^6 + \alpha^2 x^5 + x^4 + \alpha^2 x + \alpha)(x^8 + \alpha^2 x^7 + \alpha^2 x^5 + x^4 + \alpha^2 x^3 + \alpha^2 x^2 + \alpha^2 x + \alpha^2). \\ \text{Let } g(x) &= x^8 + \alpha^2 x^7 + \alpha^2 x^5 + x^4 + \alpha^2 x^3 + \alpha^2 x^2 + \alpha^2 x + \alpha^2 \text{ and } f_1(x) = x^2, \\ f_2(x) &= x^4 + x^2 + 1. \text{ Then } C_g = (g(x)) \text{ is a skew cyclic code with parameters} \\ [14, 6, 7]. \end{aligned}$

We consider the skew $\overline{\alpha}$ -multi-twisted code C generated by

 $(f_1(x)g(x), f_2(x)g(x))$

over F_4 with length (14, 14) and $\overline{\alpha} = (1, 1)$. *C* is a near-optimal code with parameters [28, 6, 16] (while [28, 6, 17] is optimal, [14]).

Example 5.9. Let θ be an automorphism of F_{16} defined by $\theta(\beta) = \beta^4$ for any $\beta \in F_{16}$ and $F_{16}^* = \langle \alpha \rangle$ where $\alpha^4 = \alpha + 1$. We again consider the skew polynomial ring $F_{16}[x;\theta]$. In this particular case, we have $|\langle \theta \rangle| = 2$ and $F_{16}^{\theta} = \{0, 1, \alpha^5, \alpha^{10}\}$.

A factorization of $x^6 - a^5$ in $F_{16}[x; \theta]$ is as follows

$$x^{6} - a^{5} = (x^{3} + x^{2} + \alpha x + \alpha^{13})(x^{3} + x^{2} + \alpha x + \alpha^{7}).$$

Let $g(x) = x^3 + x^2 + \alpha x + \alpha^7$. Then $C_g = (g(x))$ is skew α^5 -constacyclic code over F_{16} with parameters [6, 3, 4]. Let $f_1(x) = 1$, $f_2(x) = x^4 + \alpha^{10}x^2$ and $f_3(x) = x^6 + x^2 + 1$. Now, we consider

Let $f_1(x) = 1$, $f_2(x) = x^4 + \alpha^{10}x^2$ and $f_3(x) = x^6 + x^2 + 1$. Now, we consider the skew $\overline{\alpha}$ -multi-twisted code C generated by

$$(f_1(x)g(x), f_2(x)g(x), f_3(x)g(x)))$$

over F_{16} with length (6, 6, 6) and $\overline{\alpha} = (\alpha^5, \alpha^5, \alpha^5)$. C is a [18, 3, 14] code.

6. Skew multi-polycyclic codes and their duals

Polycyclicity is the most general case in terms of cyclicity of linear codes. Polycyclic codes were first introduced in [29] and referred to as pseudo-cyclic codes. Since they are direct representations of shortened cyclic codes, with a rich algebraic structure, there have been many studies on properties of polycyclic codes [2, 5, 24, 26]. In one hand, they may seem not interesting since they are punctured cyclic codes, but on the other hand being a broad family of linear codes they surely deserve and are important to be studied for their own sake. A structural study is not easy because of their general nature, but getting some results leads to direct constructions which avoid puncturing processes. Skew polycyclic codes correspond to left $F_q[x,\theta]$ -submodules of $F_q[x,\theta]/(f(x))$, for any monic polynomial $f(x) = x^n - v(x) \in F_q[x,\theta]$ with a nonzero constant term. In this case, the companion matrix of f(x) represents the transformation corresponding to the polycyclic shift with respect to v, and we denote it by M_v , where v is the coefficient vector of v(x). From now on we take a companion matrix with its last row identifying it and any linear transformation will be applied as a right multiplication by its representation matrix. Namely, for

$$M_{v} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ v_{0} & v_{1} & \cdots & v_{n-2} & v_{n-1} \end{bmatrix}_{n \times n}$$

we obtain the v-polycyclic shift for a codeword c by

$$M_v(c) = (c_0, c_1, \dots, c_{n-1}) \cdot M_v$$

Clearly, any cyclic code is *polycyclic* with respect to v = (1, 0, ..., 0) and any α -constacyclic code is *polycyclic* with respect to $v = (\alpha, 0, ..., 0)$.

Recently, polycyclic codes have been extended to noncommutative case [26]. It is shown that a skew polycyclic code generated by a right divisor g(x) of f(x) is invariant under $M_v \circ \Theta$, where $\Theta(c) := (\theta(c_0), \theta(c_1), \ldots, \theta(c_{n-1}))$. For this case, a *v*-skew polycyclic shift of a codeword *c* is obtained by

$$(M_v \circ \Theta)(c) = (\theta(c_0), \theta(c_1), \dots, \theta(c_{n-1})) \cdot M_v.$$

The following lemma can be directly proved by applying the results in [10, 24] and [26].

Lemma 6.1. Let C be a skew polycyclic code generated by a right divisor g(x)of $f(x) = x^n - v(x) \in F_q[x, \theta]$. Then, C^{\perp} is a sequential code and invariant under $(M_v^{-1})^{tr} \circ \Theta$.

In order to obtain the generating vector for the dual code of a skew polycyclic code we need to start with the following lemma.

Lemma 6.2. Let $f(x) \in F_q[x; \theta]$ be a polynomial with a nonzero constant term. Then, there exist a central polynomial $x^N - 1$ such that $f(x)|_r x^N - 1$ in $F_q[x; \theta]$.

Proof. By Lemma 10 in [9], there exists a polynomial $b(x) = (b_0 + b_1 x^m + \dots + b_s x^{sm})x^t$ where $m = |\langle \theta \rangle|$, $b_i \in F_q^{\theta}$ and $s, t \in \mathbb{N}$ such that $f(x)|_r b(x)$. Since f(x) has a nonzero constant term, we get $x^t = 1$ and $b(x) \in \mathcal{Z}(F_q[x;\theta])$.

We know that $\mathcal{Z}(F_q[x;\theta]) = F_q^{\theta}[x^m]$. Also, there exists a finite field extension of F_q^{θ} where b(x) splits. These imply that there exists a central polynomial $x^N - 1$ such that $b(x)|x^N - 1$ which completes the proof.

Let C be a skew polycyclic code generated by $g(x)|_r f(x)$ where $\deg(g(x)) = n - k$. Let $x^N - 1$ be a central polynomial such that $f(x)|_r x^N - 1$. In this case, C corresponds to the shortened code applied to the last N - n coordinates of the skew cyclic code C' = (g(x)) of length N. Further, the dual code of C corresponds to the punctured code applied to the last N - (n - k) coordinates of the dual code C'^{\perp} , which is generated by $a'^{\langle N, 1 \rangle}(x)$ where $a'(x)g(x) = x^N - 1$. The punctured code, being in the form of a sequential code, does not have an ideal or module structure and multiplication by x does not correspond to the sequential shift under which the code is invariant. However, in the sequel, we find a representative generating vector from which a generator matrix for the dual code can be obtained directly.

Theorem 6.3. Let $a(x)g(x) = f(x) = x^n - v(x)$ with a nonzero constant term and $\deg(g(x)) = n - k$ and $p(x) = \frac{x^N - 1}{f(x)} = \sum_{i=0}^{N-n} p_i x^i$. Suppose C is a skew polycyclic code generated by g(x). Then, the dual code C^{\perp} is generated by the vector $h = (h_0, h_1, \dots, h_{n-1})$ and its n - k - 1 sequential shifts, i.e., $\{h, ((M_v^{-1})^{tr} \circ \Theta)(h), \dots, ((M_v^{-1})^{tr} \circ \Theta)^{n-k-1}(h)\}$, where

$$h_0 = p_0 a_0$$
, and $h_i = \sum_{j=0}^{i-1} \theta^i(p_{N-n-j}) \theta^{N-n+i-j}(a_{n-i+j}), \ 1 \le i \le n-1.$

Proof. Since $x^N - 1$ is a central polynomial such that $f(x)|_r x^N - 1$, we have

$$x^{N} - 1 = g(x) \frac{x^{N} - 1}{f(x)} a(x).$$

This implies that

(8) $g(x)(p_0 + p_1x + \dots + p_{N-n}x^{N-n})a(x) = 0 \pmod{x^N - 1}.$ Thus, the coefficient of x^0 in (8) is

$$g_0 p_0 a_0 + g_1 \theta(p_{N-n}) \theta^{N-n+1}(a_{n-1}) + g_2(\theta^2(p_{N-n}) \theta^{N-n+2}(a_{n-2}) + \theta^2(p_{N-n-1}) \theta^{N-n+1}(a_{n-1})) + \dots + g_{n-1}(\theta^{n-1}(p_{N-n}) \theta^{N-1}(a_1) + \dots + \theta^{n-1}(p_{N-2n+2}) \theta^{N-n+1}(a_{n-1})) = 0$$

which implies $g \cdot h = 0$. Multiplying (8) by x^i from the left, we obtain $M_v^i(g) \cdot h = 0$.

Now, we consider a skew cyclic code C' of length N generated by g(x). From Theorem 4.4, the dual code of C' of dimension n-k is also generated by $a'^{\langle N,1\rangle}(x)$, where $a'(x) = \frac{x^N-1}{g(x)} = p(x)a(x)$. Let H' be the generator matrix for C'^{\perp} obtained from $a'^{\langle N,1\rangle}$. Now, we show that the first n coordinates of $a'^{\langle N,1\rangle}$ form exactly the coordinates of h in the same order. We have

$$a'(x) = (p_0 + p_1 x + \dots + p_{N-n} x^{N-n})(a_0 + a_1 x + \dots + a_{n-1} x^{n-1})$$

= $p_0 a_0 + (p_0 a_1 + p_1 \theta(a_0))x + \dots$
+ $(p_{N-n} \theta^{N-n}(a_{n-2}) + p_{N-n-1} \theta^{N-n-1}(a_{n-1}))x^{N-2}$

$$+(p_{N-n}\theta^{N-n}(a_{n-1}))x^{N-1}$$

This implies that

$$a^{\langle N,1\rangle}(x) = p_0 a_0 + \theta(p_{N-n}\theta^{N-n}(a_{n-1}))x + \theta^2(p_{N-n}\theta^{N-n}(a_{n-2}) + p_{N-n-1}\theta^{N-n-1}(a_{n-1}))x^2 + \dots + \theta^{n-1}(p_0 a_1 + p_1\theta(a_0))x^{N-1}.$$

Similarly one can show that the first n coordinates of $x^{i}a^{\prime(N,1)}(x) \pmod{x^{N}-1}$, i.e., the first n coordinates of the *i*th row of H', give the coordinates of $((M_v^{-1})^{tr} \circ \theta)^i(h)$ in the same order. This completes the proof since puncturing C'^{\perp} at the last N-n coordinates results in exactly n-k linearly independent rows.

The following example illustrates the above theorem.

Example 6.4. Let $g(x) = x^3 + \alpha x^2 + \alpha^2 |_r f(x) = x^5 + x^2 + \alpha^2 x + \alpha^2$ in $F_4[x;\theta]$ with $|\langle\theta\rangle| = 2$. In this case, $a(x) = x^2 + \alpha x + 1$ and f(x) = a(x)g(x). C = (g(x)) becomes a skew *v*-polycyclic code of length 5, where $v = (\alpha^2, \alpha^2, 1, 0, 0)$. We have N = 24, i.e., $f(x)|_r x^{24} - 1$ and $p(x) = \frac{x^{24} - 1}{f(x)}$. By Theorem 6.3, we get $h = (\alpha, 0, 0, 1, \alpha^2)$ which is exactly the first 5 coordinates of $a'^{\langle 24, 1 \rangle}$. The parity check matrix for C can be obtained from $\{h, ((M_v^{-1})^{tr} \circ \theta)(h), ((M_v^{-1})^{tr} \circ \theta)^2(h)\}$ as

$$H = \begin{bmatrix} \alpha & 0 & 0 & 1 & \alpha^2 \\ 0 & \alpha^2 & 0 & 0 & 1 \\ 1 & 0 & \alpha & 0 & 0 \end{bmatrix}$$

Now, we define quasi-cyclic codes obtained from l skew polycyclic components of different lengths. We have seen, for the case l = 1, that h is obtained from the first n coordinates of $a'^{(N,1)}$, where $a'(x) = \frac{x^N-1}{f(x)}a(x)$. In order to easily interpret this situation in the sequel, let us denote the first n coordinates of $a'^{(N,1)}$ by $(a'^{(N,1)})_n$.

Definition 6. Let C be a linear code over F_q and

$$c = (c_{1,1}, \dots, c_{1,n_1-1}, c_{1,n_1}, c_{2,1}, \dots, c_{2,n_2-1}, c_{2,n_2}, \dots, c_{l,1}, \dots, c_{l,n_l-1}, c_{l,n_l})$$

be a codeword of C. Let θ be an automorphism of F_q , $f_1 = x^{n_1} - v_1(x), \ldots, f_l = x^{n_l} - v_l(x) \in F_q[x; \theta]$ polynomials with nonzero constant terms and $\overline{v} = (v_1, \ldots, v_l)$. If a skew \overline{v} -multi-polycyclic shift of c,

$$T_{\overline{v}}(c) = (M_{v_1}(\theta(c_{1,1}), \dots, \theta(c_{1,n_1})), M_{v_2}(\theta(c_{2,1}), \dots, \theta(c_{2,n_2})), \dots, M_{v_l}(\theta(c_{l,1}), \dots, \theta(c_{l,n_l})))$$

is also a codeword in C, then C is called a skew \overline{v} -multi-polycyclic code of length (n_1, n_2, \ldots, n_l) .

Reduced generator polynomial matrices of skew \overline{v} -multi-polycyclic codes can be defined in a similar way as in the case of skew $\overline{\alpha}$ -multi-twisted codes.

Theorem 6.5. Let $f_i(x) = x^{n_i} - v_i(x) \in F_q[x;\theta]$ be polynomials with nonzero constant terms, $\overline{v} = (v_1, \ldots, v_l)$, and $x^N - 1$ be a central polynomial such that $f_i(x)|_r x^N - 1$ for all $1 \leq i \leq l$. Let $G = [g_{i,j}(x)]$ be the reduced generator polynomial matrix of a skew \overline{v} -multi-polycyclic code C of length (n_1, \ldots, n_l) over F_q . Let $A = [a_{i,j}(x)]$ be the polynomial matrix which satisfies $AG = diag[f_1(x), \ldots, f_l(x)]$.

Then,

$$\sum_{k=1}^{l} g_{i,k}(x) \frac{x^N - 1}{f_k(x)} a_{k,j}(x) = \begin{cases} 0, & i \neq j \\ x^N - 1, & i = j \end{cases}$$

holds. Moreover, if $h_{i,j} = (a'^{\langle N,1 \rangle}_{j,i})_{n_j}$ where $a'_{j,i}(x) = \frac{x^N - 1}{f_j(x)}a_{j,i}(x)$, then the block matrix

$$H = \begin{bmatrix} [h_{1,1}]_{\deg(g_{1,1})} & 0 & \cdots & 0\\ [h_{2,1}]_{\deg(g_{2,2})} & [h_{2,2}]_{\deg(g_{2,2})} & 0 & \vdots\\ \vdots & \vdots & \ddots & 0\\ [h_{l,1}]_{\deg(g_{l,l})} & [h_{l,2}]_{\deg(g_{l,l})} & \cdots & [h_{l,l}]_{\deg(g_{l,l})} \end{bmatrix}_{l \times l}$$

is a parity-check matrix of C, where

$$[h_{i,j}]_{\deg(g_{i,i})} := \begin{bmatrix} h_{i,j} \\ ((M_{v_j}^{-1})^{tr} \circ \Theta)(h_{i,j}) \\ \vdots \\ ((M_{v_j}^{-1})^{tr} \circ \Theta)^{\deg(g_{i,i})-1}(h_{i,j}) \end{bmatrix}$$

Proof. Applying Lemma 5.2, $G'A = diag[x^N - 1, \dots, x^N - 1]$ implies

$$\sum_{k=1}^{l} g_{i,k}(x) \frac{x^N - 1}{f_k(x)} a_{k,j}(x) = \begin{cases} 0, & i \neq j \\ x^N - 1, & i = j, \end{cases}$$

for $1 \leq i, j \leq l$, where $G' = Gdiag[\frac{x^N-1}{f_1}, \dots, \frac{x^N-1}{f_l}]$. For a fixed *i* and *j* we have

+

(9)
$$g_{i,1}(x)\frac{x^N-1}{f_1(x)}a_{1,j}(x) + g_{i,2}(x)\frac{x^N-1}{f_2(x)}a_{2,j}(x) + \cdots$$
$$g_{i,l}(x)\frac{x^N-1}{f_l(x)}a_{l,j}(x) = 0 \pmod{x^N-1}.$$

As in Theorem 6.3, the coefficient of x^0 is;

$$g_{i,1} \cdot (a_{1,j}^{\langle N,1 \rangle})_{n_1} + g_{i,2} \cdot (a_{2,j}^{\langle N,1 \rangle})_{n_2} + \dots + g_{i,l} \cdot (a_{l,j}^{\langle N,1 \rangle})_{n_l} = 0,$$

which implies $(g_{i,1}, g_{i,2}, \ldots, g_{i,l}) \cdot ((a_{1,j}^{\langle N,1 \rangle})_{n_1}, (a_{2,j}^{\langle N,1 \rangle})_{n_2}, \ldots, (a_{l,j}^{\langle N,1 \rangle})_{n_l}) = 0.$ Multiplying Equation (9) with x^b from the left, we obtain

$$T_{\overline{v}}^{b}((g_{i,1}, g_{i,2}, \dots, g_{i,l})) \cdot ((a_{1,j}^{\langle N,1 \rangle})_{n_{1}}, (a_{2,j}^{\langle N,1 \rangle})_{n_{2}}, \dots, (a_{l,j}^{\langle N,1 \rangle})_{n_{l}}) = 0$$

from the coefficient of x^0 . Hence $(h_{j,1}, h_{j,2}, \ldots, h_{j,l}) \in C^{\perp}$ for all $j \in \{1, \ldots, l\}$. For each diagonal block of H we have $a_{i,i}(x)g_{i,i}(x) = f_i(x)$. From Theorem 6.3, the set $\{h_{i,i}, ((M_{v_i}^{-1})^{tr} \circ \Theta)(h_{i,i}), \ldots, ((M_{v_i}^{-1})^{tr} \circ \Theta)^{\deg(g_{i,i})-1}(h_{i,i})\}$ is linearly independent for all $1 \leq i \leq l$. Therefore the rows of H are also linearly independent. Since the dimension of C^{\perp} is exactly $\sum_{i=0}^{l} \deg(g_{i,i}(x)), H$ is a parity-check polynomial matrix of C.

Example 6.6. Let us take the skew polynomial ring $F_4[x;\theta]$ given in Example 5.4. Let $f_1(x) = x^6 + \alpha^2 x^2 + \alpha^2$, $f_2(x) = x^8 + \alpha^2 x^6 + x^4 + \alpha x^2 + a$ and $f_3(x) = x^{10} + \alpha x^6 + x^4 + \alpha$. In this case, we have N = 120, and $f_1(x), f_2(x), f_3(x)|_r x^{120} - 1$. Now let us form the following matrices

$$A = \begin{bmatrix} x^2 + \alpha^2 & 0 & 1 \\ 0 & x^4 + \alpha x^2 + 1 & 0 \\ 0 & 0 & x^2 + \alpha \end{bmatrix}_{3\times 3}^{,}$$
$$G = \begin{bmatrix} x^4 + \alpha^2 x^2 + 1 & 0 & x^6 + x^4 + \alpha x^2 + \alpha \\ 0 & x^4 + x^2 + \alpha & 0 \\ 0 & 0 & x^8 + \alpha x^6 + x^4 + \alpha^2 x^2 + 1 \\ 0 & 0 & x^8 + \alpha x^6 + x^4 + \alpha^2 x^2 + 1 \end{bmatrix}_{3\times 3}^{,}$$

We have $AG = diag[f_1(x), f_2(x), f_3(x)]$. Then $G = [g_{i,j}(x)]$ is the reduced generator polynomial matrix of a skew $\overline{v} = (v_1, v_2, v_3)$ -multi-polycyclic code C of length (6, 8, 10), where $v_1 = (\alpha^2, 0, \alpha^2, 0, 0, 0), v_2 = (\alpha, 0, \alpha, 0, 1, 0, \alpha^2, 0)$ and $v_3 = (\alpha, 0, 0, 0, 1, 0, a, 0, 0, 0)$.

Now, by applying the algorithm presented in Theorem 6.5, we obtain a parity-check matrix for C as

$$H = \begin{bmatrix} [h_{1,1}]_{\deg(g_{1,1})} & 0 & 0\\ [h_{2,1}]_{\deg(g_{2,2})} & [h_{2,2}]_{\deg(g_{2,2})} & 0\\ [h_{3,1}]_{\deg(g_{3,3})} & [h_{3,2}]_{\deg(g_{3,3})} & [h_{3,3}]_{\deg(g_{3,3})} \end{bmatrix}_{3\times3}$$

where $h_{1,1} = (1,0,0,0,1,0), h_{2,1} = \overline{0}, h_{2,2} = (\alpha^2, 0, 0, 0, 1, 0, 1, 0), h_{3,1} = (\alpha, 0, 0, 0, 0, 0), h_{3,2} = \overline{0}$ and $h_{3,3} = (1,0,0,0,0,0,0,0,1,0).$

7. Conclusion

In this paper, we derive algorithms to find generators of dual codes of both skew constacyclic and skew polycyclic codes. Further, we present a generalization of the method given in [25] to skew multi-twisted codes and skew multi-polycyclic codes. Although we have restricted the length n as $m \mid n$ in Sections 4 and 5 which led us to a concise proof, the generalized formula given in Section 6 also works for the case where $m \mid n$. We give examples that are implemented through computational algebra system MAGMA [6] in order to illustrate the theorems. Also we note that, GQC codes have shown to be asymptotically good [18] recently. This result together with the rich algebraic structure of these families of codes will encourage researchers for further explorations on

this direction. Challenging and interesting problems would be studying self duality and finding new codes within these families with optimal parameters.

Acknowledgment. We would like to thank to the anonymous reviewers for their valuable remarks.

References

- T. Abualrub, A. Ghrayeb, N. Aydin, and I. Siap, On the construction of skew quasicyclic codes, IEEE Trans. Inform. Theory 56 (2010), no. 5, 2081–2090. https://doi. org/10.1109/TIT.2010.2044062
- [2] A. Alahamdi, S. Dougherty, A. Leroy, and P. Solé, On the duality and the direction of polycyclic codes, Adv. Math. Commun. 10 (2016), no. 4, 921–929. https://doi.org/ 10.3934/amc.2016049
- [3] N. Aydin and A. Halilović, A generalization of quasi-twisted codes: multi-twisted codes, Finite Fields Appl. 45 (2017), 96-106. https://doi.org/10.1016/j.ffa.2016.12.002
- [4] N. Aydin, I. Siap, and D. Ray-Chaudhuri, The structure of 1-generator quasi-twisted codes and new linear codes, Des. Codes Cryptogr., 23 (2001), no. 3, 313–326.
- [5] S. Bedir and I. Siap, *Polycyclic codes over finite chain rings*, International Conference on Coding and Cryptography, Algeria, 2015.
- [6] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. 24 (1997), no. 3-4, 235-265. https://doi.org/10.1006/ jsco.1996.0125
- [7] D. Boucher, W. Geiselmann, and F. Ulmer, *Skew-cyclic codes*, Appl. Algebra Engrg. Comm. Comput. **18** (2007), no. 4, 379–389. https://doi.org/10.1007/s00200-007-0043-z
- [8] D. Boucher, P. Solé, and F. Ulmer, Skew constacyclic codes over Galois rings, Adv. Math. Commun. 2 (2008), no. 3, 273–292. https://doi.org/10.3934/amc.2008.2.273
- [9] D. Boucher and F. Ulmer, Coding with skew polynomial rings, J. Symbolic Comput. 44 (2009), no. 12, 1644–1656. https://doi.org/10.1016/j.jsc.2007.11.008
- [10] _____, A note on the dual codes of module skew codes, in Cryptography and coding, 230-243, Lecture Notes in Comput. Sci., 7089, Springer, Heidelberg, 2011. https:// doi.org/10.1007/978-3-642-25516-8_14
- [11] J. Conan and G. Séguin, Structural properties and enumeration of quasi-cyclic codes, Appl. Algebra Engrg. Comm. Comput. 4 (1993), no. 1, 25–39. https://doi.org/10. 1007/BF01270398
- [12] N. Fogarty and H. Gluesing-Luerssen, A circulant approach to skew-constacyclic codes, Finite Fields Appl. 35 (2015), 92-114. https://doi.org/10.1016/j.ffa.2015.03.008
- [13] J. Gao, L. Shen, and F.-W. Fu, A Chinese remainder theorem approach to skew generalized quasi-cyclic codes over finite fields, Cryptogr. Commun. 8 (2016), no. 1, 51-66. https://doi.org/10.1007/s12095-015-0140-y
- [14] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, available at http://www.codetables.de.
- [15] P. P. Greenough and R. Hill, Optimal ternary quasi-cyclic codes, Des. Codes Cryptogr. 2 (1992), no. 1, 81–91. https://doi.org/10.1007/BF00124211
- [16] T. A. Gulliver and V. K. Bhargava, Nine good rate (m 1)/pm quasi-cyclic codes, IEEE Trans. Inform. Theory 38 (1992), no. 4, 1366-1369. https://doi.org/10.1109/ 18.144718
- [17] _____, Some best rate 1/p and rate (p-1)/p systematic quasi-cyclic codes over GF(3) and GF(4), IEEE Trans. Inform. Theory 38 (1992), no. 4, 1369–1374. https://doi.org/10.1109/18.144719

- [18] C. Güneri, F. Özbudak, B. Özkaya, E. Saçıkara, Z. Sepasdar, and P. Solé, Structure and performance of generalized quasi-cyclic codes, Finite Fields Appl. 47 (2017), 183–202.
- [19] N. Jacobson, Finite-Dimensional Division Algebras over Fields, Springer-Verlag, Berlin, 1996. https://doi.org/10.1007/978-3-642-02429-0
- [20] S. Jitman, S. Ling, and P. Udomkavanich, Skew constacyclic codes over finite chain rings, Adv. Math. Commun. 6 (2012), no. 1, 39-63. https://doi.org/10.3934/amc. 2012.6.39
- [21] T. Koshy, Polynomial approach to quasi-cyclic codes, Bull. Calcutta Math. Soc. 69 (1977), no. 2, 51–59.
- [22] K. Lally and P. Fitzpatrick, Algebraic structure of quasicyclic codes, Discrete Appl. Math. 111 (2001), no. 1-2, 157–175. https://doi.org/10.1016/S0166-218X(00)00350-4
- [23] S. Ling and P. Solé, On the algebraic structure of quasi-cyclic codes. I. Finite fields, IEEE Trans. Inform. Theory 47 (2001), no. 7, 2751-2760. https://doi.org/10.1109/ 18.959257
- [24] S. R. López-Permouth, B. R. Parra-Avila, and S. Szabo, Dual generalizations of the concept of cyclicity of codes, Adv. Math. Commun. 3 (2009), no. 3, 227–234. https: //doi.org/10.3934/amc.2009.3.227
- [25] H. Matsui, On generator and parity-check polynomial matrices of generalized quasicyclic codes, Finite Fields Appl. 34 (2015), 280-304. https://doi.org/10.1016/j.ffa. 2015.02.003
- [26] M. Matsuoka, θ-polycyclic codes and θ-sequential codes over finite fields, Int. J. Algebra 5 (2011), no. 1-4, 65–70.
- [27] B. R. McDonald, Finite Rings with Identity, Marcel Dekker, Inc., New York, 1974.
- [28] O. Ore, Theory of non-commutative polynomials, Ann. of Math. (2) 34 (1933), no. 3, 480–508. https://doi.org/10.2307/1968173
- [29] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*, second edition, The M.I.T. Press, Cambridge, MA, 1972.
- [30] A. Sharma, V. Chauhan, and H. Singh, Multi-twisted codes over finite fields and their dual codes, Finite Fields Appl. 51 (2018), 270-297. https://doi.org/10.1016/j.ffa. 2018.01.012
- [31] I. Siap, T. Abualrub, N. Aydin, and P. Seneviratne, Skew cyclic codes of arbitrary length, Int. J. Inf. Coding Theory 2 (2011), no. 1, 10–20. https://doi.org/10.1504/IJICOT. 2011.044674
- [32] I. Siap, N. Aydin, and D. K. Ray-Chaudhuri, New ternary quasi-cyclic codes with better minimum distances, IEEE Trans. Inform. Theory 46 (2000), no. 4, 1554–1558. https: //doi.org/10.1109/18.850694
- [33] I. Siap and N. Kulhan, The structure of generalized quasi cyclic codes, Appl. Math. E-Notes 5 (2005), 24–30.
- [34] V. T. Van, H. Matsui, and S. Mita, Computation of Grobner basis for systematic encoding of generalized quasi-cyclic codes, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences E92-A (2009), no.9, 2345–2359.
- [35] E. J. Weldon, Jr., Long quasi-cyclic codes are good, IEEE Trans. Inform. Theory, IT-16 (1970), pp. 130.

SUMEYRA BEDIR DEPARTMENT OF MATHEMATICS YILDIZ TECHNICAL UNIVERSITY ISTANBUL 34220, TURKEY Email address: smyrbdr@gmail.com

FATMANUR GURSOY DEPARTMENT OF MATHEMATICS YILDIZ TECHNICAL UNIVERSITY ISTANBUL 34220, TURKEY Email address: fnurgursoy@gmail.com

IRFAN SIAP JACODESMATH INSTITUTE ISTANBUL 34220, TURKEY *Email address*: irfan.siap@gmail.com