Skew-quasi-cyclic codes over $M_l(F_q)[X,\theta]$

Li Xiuli[1] * Tan Mingming[2†]

[1] College of Information Science and Engineering, Ocean University of China, Qingdao 266000, China

School of Mathematics and Physics, Qingdao University of Science and Technology, Qingdao 266000, China

[2] School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637371, Republic of Singapore

Abstract. Skew-quasi-cyclic codes over a finite field are viewed as skew-cyclic codes on a noncommutative ring of matrices over a finite field. This point of view gives a new construction of skew-quasi-cyclic codes. Let F_q be the Galois field with q elements and θ be an automorphism of F_q. We propose an approach to consider the relationship between left ideals in $M_l(F_q)[X,\theta]/\langle X^s-1\rangle$ and skew-quasi-cyclic codes of length sl and index l over F_q under θ which we denote by l_θ-SQC codes (or SQC codes for short when there is no ambiguity). We introduce the construction of SQC codes from the reversible divisors of X^s-1 in $M_l(F_q)[X,\theta]$. In addition, we give an algorithm to search for the generator polynomials of general SQC codes.

Keywords: Quasi-cyclic codes, Skew-quasi-cyclic codes, Skew polynomial ring

1 Introduction

Skew polynomial rings form an important family of noncommutative rings. Recently they have been applied to the construction of quasi-cyclic codes [10] and skew cyclic codes [4-6], where codes are defined as left ideals in the quotient rings of skew polynomial rings. The principal motivation

* *E-mail: lixiuli2007@aliyun.com.* *Research supported by reward fund for outstanding young and middle-aged scientists of Shandong(BS2011DX011) and Qingdao postdoctoral fund (861605040007).*

† *E-mail:MMTAN1@e.ntu.edu.sg.*

for studying codes in this setting is that polynomials in skew polynomial rings exhibit many factorizations and hence there are many more left ideals in the quotient rings of a skew polynomial ring than in the commutative case [2].

Skew-quasi-cyclic codes are defined as a common generalization of quasi-cyclic codes and skew-cyclic codes.

Definition 1 *Let F_q be the Galois field with q elements, where $q = p^{mt}$ with p a prime. Let θ be an automorphism of F_q with $|\langle\theta\rangle| = m$. A subset C of F_q^n is called a skew-quasi-cyclic code of length n and index l under θ (denoted by a l_θ-SQC code, or a SQC code for short when there is no ambiguity) where $n = sl$ if*

(1) *C is a subspace of F_q^n;*

(2) *if $c = (c_{0,0}, \cdots, c_{0,l-1}, c_{1,0}, \cdots, c_{1,l-1}, \cdots, c_{s-1,0}, \cdots, c_{s-1,l-1})$ is a codeword of C, then $T_{\theta,l}(c) = (\theta(c_{s-1,0}), \cdots, \theta(c_{s-1,l-1}), \theta(c_{0,0}), \cdots, \theta(c_{0,l-1}), \cdots, \theta(c_{s-2,0}), \cdots, \theta(c_{s-2,l-1}))$ is also a codeword in C.*

The map $T_{\theta,l}$ will be referred to as skew cyclic shift operator. Thus skew-quasi-cyclic codes are linear codes that are closed under skew cyclic shift. If θ is the identity map, then the SQC codes are just the standard QC codes defined over F_q. If $l = 1$, then the SQC codes are just the skew-cyclic codes defined over F_q.

Abualrub et al. [1] have studied skew-quasi-cyclic codes over finite fields as a generalization of classical QC codes in the new setting of a skew polynomial rings. In [2], Bhaintwal has studied skew-quasi-cyclic codes over Galois rings.

In this paper we see skew-quasi-cyclic codes as block skew-cyclic codes. We investigate the relationship between reversible divisors of $X^s - 1$ in the skew matrix polynomial ring $M_l(F_q)[X, \theta]$ and SQC codes of length sl and index l over F_q. Then we consider the idea of constructing SQC codes from reversible divisors of $X^s - 1$.

The rest of the paper is organized as follows. Section II includes a description of the skew matrix polynomial ring $M_l(F_q)[X, \theta]$. In Section III, we consider the relationship between left ideals in $M_l(F_q)[X, \theta]/\langle X^s - 1\rangle$ and SQC codes of length sl, index l over F_q. In Section IV, we introduce the construction of SQC codes from the reversible divisors of $X^s - 1$ in $M_l(F_q)[X, \theta]$. In section V, we give an algorithm to search for the generator polynomials of general SQC codes.

2 Skew matrix polynomial ring $M_l(F_q)[X,\theta]$

Let F_q be the Galois field with q elements, where $q = p^r$ with p a prime and $r \in N$. Let θ be the Frobenius automorphism of F_q with $|\langle\theta\rangle| = m$. Let K be the subfield of F_q fixed under θ. Then $[F_q : K] = m$ and $K = F_{p^t}$ where $r = tm$. We have $\theta(a) = a^{p^t}$ for all $a \in F_q$.

Let $M_l(F_q)$ be the noncommutative ring of $l \times l$ matrices with elements in F_q. For $A = (a_{ij}) \in M_l(F_q)$, we define $\theta(A) = (\theta(a_{ij}))$. For any $A, B \in M_l(F_q)$, $\theta(AB) = \theta(A)\theta(B)$.

Remark 2.1 *For a matrix $A = (a_{ij}) \in M_l(F_q)$, A is invertible if and only if $\theta(A)$ is invertible.*

Proof. Since $|\theta(A)| = \theta^l(|A|)$, the result follows from the fact that θ is an automorphism of F_q. □

Definition 2.2 *The skew matrix polynomial ring $M_l(F_q)[X,\theta]$ is the set of polynomials over $M_l(F_q)$ where addition of the polynomials is defined in the usual way while multiplication is defined using the distributive law and the rule $(AX^i) * (BX^j) = A\theta^i(B)X^{i+j}$.*

Example 2.3 Consider the finite field $F_4 = \{0, 1, \omega, \omega^2\}$ where $\omega^2+\omega+1 = 0$. Define the Frobenius automorphism $\theta : F_4 \to F_4$ by $\theta(z) = z^2$.

Let

$$f(X) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} X^2 + \begin{pmatrix} \omega & \omega^2 \\ 1 & \omega \end{pmatrix} X + \begin{pmatrix} 1 & \omega^2 \\ 1 & 1 \end{pmatrix},$$

$$g(X) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} X^2 + \begin{pmatrix} \omega^2 & \omega \\ 1 & \omega^2 \end{pmatrix} X + \begin{pmatrix} 1 & \omega \\ 1 & 1 \end{pmatrix}.$$

We have

$$f(X) * g(X) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} X^4 + \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} X^3 + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} X^2 + \begin{pmatrix} 1 & \omega \\ 1 & 0 \end{pmatrix} X + \begin{pmatrix} \omega & 1 \\ 0 & \omega^2 \end{pmatrix},$$

$$g(X) * f(X) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} X^4 + \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} X^3 + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} X^2$$

$$+\begin{pmatrix} 1 & \omega^2 \\ 1 & 0 \end{pmatrix} X + \begin{pmatrix} \omega^2 & 1 \\ 0 & \omega \end{pmatrix}.$$

Remark 2.4 (1) The commutative law does not hold in $M_l(F_q)[X, \theta]$.

(2) The associative law holds in $M_l(F_q)[X, \theta]$.

(3) $deg(f(X) + g(X)) \leq \max\{deg(f(X)), deg(g(X))\}$.

(4) $deg(f(X) * g(X)) \leq deg(f(X)) + deg(g(X))$, the equation holds if the leading coefficient of $f(X)$ or $g(X)$ is invertible in $M_l(F_q)$.

Definition 2.5 *We call a polynomial $f(X) \in M_l(F_q)[X, \theta]$ reversible if its leading and constant coefficients are invertible matrices.*

Now we give the following result. The proof is similar to the division process for polynomials in polynomial ring $F_q)[X]$. So we omit it.

Lemma 2.6 *Let $g(X)$ be a polynomial in $M_l(F_q)[X, \theta]$ whose leading coefficient is invertible. For any polynomial $f(X) \in M_l(F_q)[X, \theta]$, there exist unique polynomials $q(X)$ and $r(X)$ in $M_l(F_q)[X, \theta]$ such that*

$$f(X) = q(X) * g(X) + r(X),$$

where $r(X) = 0$ or $deg(r(X)) < deg(g(X))$.

The above result is called division on the right by $g(X)$. When $r(X) = 0$, we call $g(X)$ divides $f(X)$ on the right side, or $g(X)$ is a right divisor of $f(X)$. A similar result can be proved regarding division on the left by $g(X)$. If $g(X)$ is both a left and right divisor of $f(X)$, we call it a two sided divisor (or divisor) of $f(X)$.

The following theorem generalize the result of Cao and Gao [8] which deals with $M_l(F_q)[X]$. The proof is similar to that in [8]. So we omit it.

Lemma 2.7 *Let $f(X) \in M_l(F_q)[X, \theta]$ be reversible. Then there exists a positive integer e such that $f(X)$ is a right divisor of $X^e - 1$.*

Definition 2.8 *For any ring R, define the center of R to be the set*

$$Z(R) = \{a | a \cdot b = b \cdot a \text{ for all } b \in R\}.$$

Definition 2.9 *Let $f(X)$ and $g(X)$ be reversible polynomials. A monic polynomial $d(X)$ is called the greatest common right divisor of $f(X)$ and $g(X)$ ($gcrd(f, g)$) if*

(1) *$d(X)$ is a right divisor of $f(X)$ and $g(X)$;*

(2) *if $h(X)$ is another right divisor of $f(X)$ and $g(X)$, then $d(X) =$*

$k(X) * h(X)$ *for some polynomial* $k(X)$.

The greatest common left divisor of $f(X)$ and $g(X)$ ($gcld(f,g)$) is a monic polynomial defined in a similar way. As in [7], we may have the following results.

Lemma 2.10 $X^s - 1 \in Z(M_l(F_q)[X,\theta])$ *for* $m \mid s$, *where* $m = |\langle\theta\rangle|$.

Lemma 2.11 *Let* $f(X)$ *and* $g(X)$ *be reversible polynomials in* $M_l(F_q)[X,\theta]$. *If* $f(X) * g(X) \in Z(M_l(F_q)[X,\theta])$, *then* $f(X) * g(X) = g(X) * f(X)$.

Corollary 2.12 *Let* $f(X)$ *be a reversible polynomial in* $M_l(F_q)[X,\theta]$. *If* $f(X)$ *is a right divisor of* $X^s - 1$ *with* $m \mid s$ *where* $m = |\langle\theta\rangle|$, *then* $f(X)$ *is a two sided divisor of* $X^s - 1$.

From now on, we regard the divisors of $X^s - 1$ without specifying left or right while $m \mid s$.

Lemma 2.13 *Let* $f(X)$ *be a divisor of* $X^s - 1$ *in* $M_l(F_q)[X,\theta]$ *with* $|\langle\theta\rangle| = m$ *and* $m \mid s$.

(1) *If* $f(X)$ *is reversible, then there exists a unique reversible polynomial* $g(X)$ *such that* $f(X) * g(X) = g(X) * f(X) = X^s - 1$.

(2) *If the leading coefficient of* $f(X)$ *is invertible, then* $f(X)$ *is reversible.*

Proof. (1) The result follows from Lemma 2.10 and 2.11.

(2) $X^s - 1 = g(X) * f(X)$ implies $-I_l = g(0)f(0)$ where $f(0)$ and $g(0)$ are constant coefficients of $f(X)$ and $g(X)$ respectively. Therefore, $f(0)$ is an invertible matrix. □

Definition 2.14 *The period of a reversible polynomial* $f(X)$ *in* $M_l(F_q)[X,\theta]$ *is the smallest positive integer* e *such that* $f(X)$ *divides* $X^e - 1$ *on the right side. We denote* e *by* $per(f)$.

Theorem 2.15 *Let* $f(X)$ *be a reversible polynomial in* $M_l(F_q)[X,\theta]$. *For any positive integer* d, $f(X)$ *is a right divisor of* $X^d - 1$ *if and only if* $per(f) \mid d$.

Proof. Let $e = per(f)$. Suppose that $e \mid d$. Let t be a positive integer such that $d = et$. There exists $g(X) \in M_l(F_q)[X,\theta]$ such that $X^e - 1 = g(X) * f(X)$. We have

$$X^d - 1 = X^{et} - 1 = ((X^e)^{t-1} + (X^e)^{t-2} + \cdots + X^e + 1) * (X^e - 1)$$

$$= ((X^e)^{t-1} + (X^e)^{t-2} + \cdots + X^e + 1) * (g(X) * f(X))$$
$$= (((X^e)^{t-1} + (X^e)^{t-2} + \cdots + X^e + 1) * g(X)) * f(X).$$

Conversely, suppose that $f(X)$ is a right divisor of $X^d - 1$. There exist $g(X)$ and $h(X)$ in $M_l(F_q)[X, \theta]$ such that $X^e - 1 = g(X) * f(X)$ and $X^d - 1 = h(X) * f(X)$.

Let q and r be integers such that $d = qe + r$, $0 \leq r < e$. Then

$$\begin{aligned} h(X) * f(X) &= X^d - 1 = X^{qe+r} - 1 = (X^e)^q * X^r - 1 \\ &= (g(X) * f(X) + 1)^q * X^r - 1 \\ &= \left(1 + \sum_{i=1}^{q} \binom{q}{i} (g(X) * f(X))^i\right) * X^r - 1. \end{aligned}$$

Thus

$$\begin{aligned} X^r - 1 &= h(X) * f(X) - \left(\sum_{i=1}^{q} \binom{q}{i} (g(X) * f(X))^i\right) * X^r \\ &= h(X) * f(X) - \left(\sum_{i=1}^{q} \binom{q}{i} (X^e - 1)^i\right) * X^r \\ &= h(X) * f(X) - \sum_{i=1}^{q} \binom{q}{i} (X^e - 1)^{i-1} * (X^e - 1) * X^r \\ &= h(X) * f(X) - \sum_{i=1}^{q} \binom{q}{i} (X^e - 1)^{i-1} * X^r * (X^e - 1) \\ &= h(X) * f(X) - \sum_{i=1}^{q} \binom{q}{i} (X^e - 1)^{i-1} * X^r * (g(X) * f(X)) \\ &= h(X) * f(X) - \left(\sum_{i=1}^{q} \binom{q}{i} (X^e - 1)^{i-1} * X^r * g(X)\right) * f(X) \\ &= \left[h(X) - \sum_{i=1}^{q} \binom{q}{i} (X^e - 1)^{i-1} * X^r * g(X)\right] * f(X). \end{aligned}$$

So $f(X)$ is a right divisor of $X^r - 1$. By the smallest property of $per(f)$ we have $r = 0$. Thus $per(f) \mid d$. □

Let s be a multiple of m where $m = |\langle\theta\rangle|$. We have $X^s - 1 \in Z(M_l(F_q)[X, \theta])$ and hence $\langle X^s - 1\rangle \subset M_l(F_q)[X, \theta]$ is a two sided ideal. In the non-commutative ring $M_l(F_q)[X, \theta]$ we identify the image of $f(X)$ under the canonical homorphism ψ: $M_l(F_q)[X, \theta] \to M_l(F_q)[X, \theta]/\langle X^s - 1\rangle$ with the

remainder $r(X)$ of $f(X)$ by the division with $X^s - 1$.

Theorem 2.16 *Let D be a left ideal of $M_l(F_q)[X,\theta]/\langle X^s - 1\rangle$. If there exists a polynomial with invertible leading coefficient $\overline{g(X)}$ which has minimum degree in D. Then D is a principal left ideal generated by $\overline{g(X)}$, and $\overline{g(X)}$ is a divisor of $X^s - 1$ in $M_l(F_q)[X,\theta]$.*

Proof. If $D = 0$, then $D = \langle 0\rangle$.

Suppose that $D \neq 0$, firstly we first prove that the leading matrices of all the polynomials with minimal degree in D are all invertible.

Let $\overline{g(X)} \in D$ be a polynomial with minimum degree and write $\overline{g(X)} = B_k X^k + \cdots + B_1 X + B_0$, $0 < k < s$, B_k is invertible in $M_l(F_q)$.

By the above notation we identify the element $\overline{g(X)} \in D$ with itself in $M_l(F_q)[X,\theta]$. That is $\psi(\overline{g(X)}) = \overline{g(X)}$ with $deg(g(X)) < s$. For any $\overline{f(X)} \in D$, there exists $f(X) \in M_l(F_q)[X,\theta]$ such that $\psi(f(X)) = \overline{f(X)}$. Performing a right division of $f(X)$ by $\overline{g(X)}$ in $M_l(F_q)[X,\theta]$ we get

$$f(X) = q(X) * \overline{g(X)} + r(X),$$

where $r(X) = 0$ or $deg(r(X)) < deg(\overline{g(X)}) < s$. Thus we have $f(X) - q(X) * \overline{g(X)} = r(X) = \psi(r(X)) = \overline{f(X)} - \psi(q(X)) * \overline{g(X)} \in D$. By the minimum property of the degree of $\overline{g(X)}$ we have $r(X) = \psi(r(X)) = 0$. Then $\overline{f(x)} = \psi(q(X)) * \overline{g(X)}$. Thus $D = \langle \overline{g(X)}\rangle$.

Similarly as above we have $X^s - 1 = h(X) * \overline{g(X)}$, where $h(X) \in M_l(F_q)[X,\theta]$, i.e. $\overline{g(X)}$ is a divisor of $X^s - 1$. □

In the next section we will prove that any left ideal of $M_l(F_q)[X,\theta]/\langle X^s - 1\rangle$ is a principal left ideal. But it is not easy to find the generating element in general situations.

3 Skew-quasi-cyclic codes over $M_l(F_q)[X,\theta]$

In this section, we will build the corresponding relationship between left ideals of $M_l(F_q)[X,\theta]/\langle X^s - 1\rangle$ and SQC codes and prove that $M_l(F_q)[X,\theta]/\langle X^s - 1\rangle$ is a principal left ideal ring. We always assume that $m \mid s$.

Following M. Barbier et al. [3] we may build a one-to-one correspondence between SQC codes and left ideals of $M_l(F_q)[X,\theta]/\langle X^s - 1\rangle$ through left submodules of $(F_q[X,\theta]/\langle X^s - 1\rangle)^l$. Note that $F_q[X,\theta]$ is a skew polynomial ring over F_q. For more details about $F_q[X,\theta]$ see [4-6]

Lemma 3.1 *Let l be a positive integer and R be a principal left ideal ring. Then there is a one-to-one correspondence between the left submod-*

ules of R^l and the left ideals of $M_l(R)$.

Proof. Given a left submodule $N \subseteq R^l$, we can build a left ideal of $M_l(R)$ whose elements have rows in N. Conversely, given a left ideal $D \subseteq M_l(R)$ we associate the left submodule of R^l generated by all the rows of all the elements of D. It is easy to check that these maps are inverse to each other. □

Theorem 3.2 *There is a one-to-one correspondence between SQC codes over F_q of length $n = sl$ and left ideals of $M_l(F_q)[X,\theta]/\langle X^s - 1\rangle$.*

Proof. Let $c = (c_{0,0}, \cdots, c_{0,l-1}, c_{1,0}, \cdots, c_{1,l-1}, \cdots, c_{s-1,0}, \cdots, c_{s-1,l-1})$ be an element in F_q^n. Define a map

$$\phi : F_q^n \to (F_q[X,\theta]/\langle X^s - 1\rangle)^l$$

by

$$\phi(c) = (c_0(X), c_1(X), \cdots, c_{l-1}(X)),$$

where $c_j(X) = \sum_{i=0}^{s-1} c_{ij}X^i \in F_q[X,\theta]/\langle X^s - 1\rangle$ for $j = 0, 1, \cdots, l-1$.

The map ϕ gives a one-to-one correspondence between SQC codes over F_q of length n and left submodules of $(F_q[X,\theta]/\langle X^s - 1\rangle)^l$.

Let the ring $R_s = F_q[X,\theta]/\langle X^s - 1\rangle$. Then R_s is a principal left ideal ring [4-5]. Note that $M_l(F_q)[X,\theta]/\langle X^s - 1\rangle$ and $M_l(F_q[X,\theta]/\langle X^s - 1\rangle)$ are isomorphic. The assertion now follows from Lemma 3.1. □

R_s^l is a free module with rank l. Any left submodule of R_s^l can be generated by at most l elements. Then we obtain the following result.

Theorem 3.3 *Any left ideal D of $M_l(F_q)[X,\theta]/\langle X^s - 1\rangle$ is a left principal ideal.*

Thus we may denote a SQC code C by $\langle g(X)\rangle$ which is a left principal ideal of $M_l(F_q)[X,\theta]/\langle X^s - 1\rangle$. We call such $g(X)$ the *generator polynomial* of C.

Theorem 3.4 *Let $C = \langle g(X)\rangle_l \subseteq M_l(F_q)[X,\theta]/\langle X^s - 1\rangle$ be a SQC code over $M_l(F_q)[X,\theta]$. If the leading coefficient of $g(X)$ is invertible, then $g(X)$ is a reversible divisor of $X^s - 1$.*

Proof. Firstly we see $g(X)$ as a polynomial in $M_l(F_q)[X,\theta]$. By Lemma 2.6, there exist $f(X), r(X) \in M_l(F_q)[X,\theta]$ such that $X^s - 1 = f(X) * g(X) + r(X)$ and $r(X) = 0$ or $deg(r(X)) < deg(g(X))$.

Since $-r(X) \equiv f(X) * g(X)\ mod\ (X_s - 1)$, we have $r(X) \in \langle g(X)\rangle$.

We declare that $r(X) = 0$. Otherwise, it follows from the fact that the leading coefficient of $g(X)$ is invertible that $deg(r(X)) \geq deg(g(X))$, a contradiction. So $r(X) = 0$ and $g(X)$ is a divisor of $X^s - 1$.

By Lemma 14, $g(X)$ is a reversible polynomial. □

4 SQC codes determined by divisors of $X^s - 1$

In this section we will introduce the construction of SQC codes from divisors of $X^s - 1$ in $M_l(F_q)[X, \theta]$. The generator matrices and parity check matrices of the codes are proposed as well.

Construction Let $g(X)$ be a divisor of $X^s - 1$ in $M_l(F_q)[X, \theta]$ with $|\langle\theta\rangle| = m$, $m \mid s$. Suppose that $g(X)$ is a reversible polynomial.

Let $g(X) = \sum_{j=0}^{k} A_j X^j$ $(1 \leq k \leq s-1)$, where A_0 and A_k are invertible matrices. Let

$$A_j = \begin{pmatrix} c_{0,0}^{(j)} & \cdots & c_{0,l-1}^{(j)} \\ \vdots & \vdots & \vdots \\ c_{l-1,0}^{(j)} & \cdots & c_{l-1,l-1}^{(j)} \end{pmatrix}, \ j = 0, 1, \cdots, k.$$

Suppose that $X^s - 1 = g(X) * h(X) (= h(X) * g(X))$ and $h(X) = \sum_{j=0}^{s-k} B_j X^j$. B_0 and B_{s-k} are clearly also invertible matrices. As in section II, we identify the image of $f(X) \in M_l(F_q)[X, \theta]$ under the canonical homorphism ψ: $M_l(F_q)[X, \theta] \to M_l(F_q)[X, \theta]/\langle X^s - 1\rangle$ with the remainder of $f(X)$ by the division with $X^s - 1$. From Lemma 2.6 it follows that there exist unique polynomials $q(X)$ and $r(X)$ such that $f(X) = q(X) * h(X) + r(X)$ where $r(X) = 0$ or $deg(r(X)) < deg(h(X))$. Then

$$\psi(f(X) * g(X)) = \psi((q(X) * h(X) + r(X)) * g(X)) = r(X) * g(X).$$

Thus we know that any element of the left ideal $\langle g(X)\rangle$ in $M_l(F_q)[X, \theta]$ $/\langle X^s - 1\rangle$ can be denoted by

$$r(X) * g(X) = R_0 g(X) + R_1(X * g(X)) + \cdots + R_{s-k-1}(X^{s-k-1} * g(X)),$$

where R_i are matrices in $M_l(F_q)$, $i = 0, 1, \cdots, s - k - 1$.

Let

$$c_i = (c_{i,0}^{(0)}, \cdots, c_{i,l-1}^{(0)}, c_{i,0}^{(1)}, \cdots, c_{i,l-1}^{(1)}, \cdots, c_{i,0}^{(k)}, \cdots, c_{i,l-1}^{(k)}, 0, \cdots, 0),$$

$i = 0, 1, \cdots, l - 1$, where the number of zero is $n - (k + 1)l = (s - k - 1)l$. Then $c_0, \cdots, c_{l-1}, T_{\theta,l}(c_0), \cdots, T_{\theta,l}(c_{l-1}), \cdots, T_{\theta,l}^{s-k-1}(c_0), \cdots, T_{\theta,l}^{s-k-1}(c_{l-1})$ span a SQC code. Denote the SQC code by C.

Since A_0 is an invertible matrix in $M_l(F_q)$,

$$c_0, \cdots, c_{l-1}, T_{\theta,l}(c_0), \cdots, T_{\theta,l}(c_{l-1}), \cdots, T_{\theta,l}^{s-k-1}(c_0), \cdots, T_{\theta,l}^{s-k-1}(c_{l-1})$$

are independent. Thus they form a basis of C and $dim(C) = (s-k)l = n - kl$.

The generator matrix of C is

$$\begin{pmatrix} A_0 & \cdots & A_k & 0 & \cdots & 0 \\ 0 & \theta(A_0) & \cdots & \theta(A_k) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & \theta^{s-k-1}(A_0) & \cdots & \theta^{s-k-1}(A_k) \end{pmatrix}.$$

The parity check matrix of C is

$$\begin{pmatrix} B'_{s-k} & \theta(B'_{s-k-1}) & \cdots & \theta^{s-k}(B'_0) & 0 & \cdots & 0 \\ 0 & \theta(B'_{s-k}) & \theta^2(B'_{s-k-1}) & \cdots & \theta^{s-k+1}(B'_0) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \theta^{k-1}(B'_{s-k}) & \theta^k(B'_{s-k-1}) & \cdots & \theta^{s-1}(B'_0) \end{pmatrix}.$$

Example 4.1 Let $F_4 = \{0, 1, \omega, \omega+1\}$ where $\omega^2 + \omega + 1 = 0$. Let θ be the automorphism of F_4 with $\theta(\alpha) = \alpha^2$ for $\alpha \in F_4$. Then $|\langle\theta\rangle| = 2$. We have

$$X^6 - 1 = \left(X^3 + \begin{pmatrix} \omega & 1 \\ \omega^2 & \omega \end{pmatrix} X^2 + \begin{pmatrix} 1 & 1 \\ \omega & \omega \end{pmatrix} X + \begin{pmatrix} 1 & 1 \\ 1 & \omega^2 \end{pmatrix} \right)$$

$$* \left(X^3 + \begin{pmatrix} \omega^2 & 1 \\ \omega & \omega^2 \end{pmatrix} X^2 + \begin{pmatrix} \omega^2 & 0 \\ \omega & 0 \end{pmatrix} X + \begin{pmatrix} \omega & \omega^2 \\ \omega^2 & \omega^2 \end{pmatrix} \right).$$

Thus we obtain two 2_θ-SQC codes with length 12 whose generator matrices are

$$G_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & \omega & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & \omega^2 & \omega & \omega & \omega^2 & \omega & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & \omega^2 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & \omega & \omega^2 & \omega^2 & \omega & \omega^2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \omega & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & \omega^2 & \omega & \omega & \omega^2 & \omega & 0 & 1 \end{pmatrix}$$

and

$$G_2 = \begin{pmatrix} \omega & \omega^2 & \omega^2 & 0 & \omega^2 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ \omega^2 & \omega^2 & \omega & 0 & \omega & \omega^2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & \omega^2 & \omega & \omega & 0 & \omega & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & \omega & \omega & \omega^2 & 0 & \omega^2 & \omega & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \omega & \omega^2 & \omega^2 & 0 & \omega^2 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & \omega^2 & \omega^2 & \omega & 0 & \omega & \omega^2 & 0 & 1 \end{pmatrix}$$

respectively.

In the calculation we obtain more than 30 pairs of monic polynomials $f(X)$ and $g(x)$ with $X^6 - 1 = f(X) * g(X)$. We may construct quite a lot SQC codes by such a decomposition method.

The above construction begins with a divisor of $X^s - 1$ to get a SQC code. A variation of the construction can be done by first selecting a reversible polynomial $f(X)$ in $M_l(q)[X, \theta]$. Then, by Lemma 2.7 we know that there exits a positive integer e such that $f(X)$ is a right divisor of $X^e - 1$. We denote the smallest positive integer e by $per(f)$. Let $s = lcm(per(f), m)$ where $\theta = |\langle\theta\rangle|$. It follows from Theorem 2.15 that $f(X)$ is a divisor of $X^s - 1$ and this give us a SQC code of length $n = sl$.

5 The generator polynomials of general SQC codes

In this section we demonstrate a way to search for the generator polynomials of general SQC codes. The main idea comes from M. Barbier et al. [3].

Lemma 5.1 *Let C be a SQC code over F_q of dimension k and length $n = sl$. Then there exists an integer r such that $1 \leq r \leq k$ and for any generator matrix G of C and $0 \leq i \leq s-1$, the rank of the matrix formed by columns $il+1, il+2, \cdots, (i+1)l$ of G is r.*

Proof. Let $G_1 = (A_0, A_1, \cdots, A_{s-1})$ and $G_2 = (B_0, B_1, \cdots, B_{s-1})$ be two generator matrices of C, where A_i and B_i are $k \times l$ matrices for $i = 0, 1, \cdots, s-1$. Then $G_3 = (\theta(A_{s-1}), \theta(A_0), \cdots, \theta(A_{s-2}))$ is also a generator matrix of C. Thus there exist invertible matrices P and Q such that $G_2 = PG_1 = P(A_0, A_1, \cdots, A_{s-1}) = (PA_0, PA_1, \cdots, PA_{s-1})$ and $G_3 = QG_1 = Q(A_0, A_1, \cdots, A_{s-1}) = (QA_0, QA_1, \cdots, QA_{s-1})$. So $B_i = PA_i$ and $\theta(A_{i-1}) = QA_i$ for $i = 0, 1, \cdots, s-1$. Hence we have $rank(B_i) = rank(A_i) = rank(\theta(A_{i-1})) = rank(A_{i-1})$ for $i = 0, 1, \cdots, s-1$.

It is clear that $r \leq l$. □

Definition 5.2 *Following the notation in Lemma 5.1 we call the inte-*

ger r the block rank of C. Note that r depends only on C and not on any particular generator matrix of C.

Let C be a SQC code over $M_l(F_q)[X,\theta]$. If $l = 1$, then C is a skew cyclic code of length n with generator matrix

$$\begin{pmatrix} g(X) & & & \\ & X * g(X) & & \\ & & \cdots & \\ & & & X^{n-deg(g(X))} * g(X) \end{pmatrix},$$

where $g(X) \in F_q[X,\theta]$ is the generator polynomial of C over F_q. The block rank of C is 1 and we can write a generator matrix of C with only one vector and its skew shifts.

The following algorithm attributes to M. Barbier et al. [3], the improvement that we make is the step 14. For the algorithm, the proof is omitted as it is similar with the proof in [3]. However, the complexity and computation cost of our algorithm is higher.

Let r be the block rank of C, the following algorithm computes a basis of C from r vectors of C and their skew shifts. Given a nonzero vector $x = (x_1, \cdots, x_{sl})$, let i be the smallest integer such that $0 \leq i \leq s-1$ and $(x_{il+1}, \cdots, x_{(i+1)l}) \neq 0$. Such integer i is called the first index and is denoted by $F(x) = F(x_1, \cdots, x_{sl})$. Let

$$\zeta : F_q^{sl} \to F_q^l,$$

$$x = (x_1, \cdots, x_{sl}) \mapsto (x_{il+1}, \cdots, x_{(i+1)l}),$$

where $i = F(x_1, \cdots, x_{sl})$ if $x \neq 0$ and $\zeta(0) = 0$.

Algorithm *Basis computation with the block rank*

Input: *A generator matrix G of C.*

Output: *A generator matrix formed by r rows from G and some of their skew shifts.*

1: $G' \leftarrow$ *a row echelon form of* G
2: *Denote by* $g_1, \cdots, g_k$ *the rows of* G'
3: $M \leftarrow \max F(g_i), i \in 1, 2, \cdots, k$
4: $B'_M \leftarrow \emptyset$
5: $G_{M+1} \leftarrow \emptyset$
6: *for* $j = M$ *to* 0 *do*
7: $B_j \leftarrow g_i, i \in 1, \cdots, k$ *and* $F(g_i) = j$
8: *for each element* x *of* B_j *do*
9: *if* $\zeta(B'_j) \cup \zeta(x)$ *are independent then*
10: $B'_j \leftarrow B'_j \cup \{x\}$

11: *end if*
12: *end for*
13: $G_j \leftarrow G_{j+1} \cup B'_j$
14: $B'_{j-1} \leftarrow T^{s-1}_{\theta,l}(B'_j) = (T_{\theta,l})^{-1}(B'_j)$
15: *end for*
16: *return* G_0

This algorithm works correctly as expected and returns a generator matrix G of C made of r linearly independent vectors of C and some of their skew shifts.

Proposition 5.3 *There exist $g_1, g_2, \cdots, g_r$ linear independent vectors in C such that $g_1, \cdots, g_r, T_{\theta,l}(g_1), \cdots, T_{\theta,l}(g_r), \cdots, T^{s-1}_{\theta,l}(g_1), \cdots, T^{s-1}_{\theta,l}(g_r)$ span C. For $r \leq l$, we denote by $g_{i,j}$ the $j-th$ coordinate of g_i. Let*

$$G_i = \begin{pmatrix} g_{1,il+1} & \cdots & g_{1,(i+1)l} \\ \vdots & & \vdots \\ g_{r,il+1} & \cdots & g_{r,(i+1)l} \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \in M_l(F_q)$$

and

$$g(X) = \frac{1}{X^v} \sum_{i=0}^{s-1} G_i X^i \in M_l(F_q)[X, \theta],$$

where v is the least integer such that $G_i \neq 0$, then C corresponds to the left ideal $\langle g(X) \rangle$.

The polynomial $g(X) \in M_l(F_q)[X, \theta]$ obtained above is the generator polynomial of C.

Example 5.4 Let $F_4 = \{0, 1, \omega, \omega + 1\}$ where $\omega^2 + \omega + 1 = 0$. Let θ be the automorphism of F_4 with $\theta(\alpha) = \alpha^2$ for $\alpha \in F_4$. Then $|\langle \theta \rangle| = 2$. Let C be a 3_θ-SQC code from $\langle p(X), q(X) \rangle$ in $M_l(F_q)[X, \theta]/\langle X^6 - 1 \rangle$ where

$$p(X) = X^5 + \begin{pmatrix} \omega^2 & \omega & \omega^2 \\ \omega & 0 & \omega^2 \\ \omega^2 & \omega & \omega \end{pmatrix} X^4 + \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & \omega \\ \omega & 1 & 1 \end{pmatrix} X^3$$

$$+\begin{pmatrix} 1 & \omega & 1 \\ \omega^2 & \omega & 1 \\ 1 & \omega^2 & 1 \end{pmatrix} X^2 + \begin{pmatrix} 1 & 0 & \omega \\ 1 & \omega & \omega^2 \\ 0 & 1 & \omega \end{pmatrix} X + \begin{pmatrix} 0 & 0 & 0 \\ 1 & \omega^2 & 1 \\ 0 & 0 & 0 \end{pmatrix},$$

$$q(X) = X^5 + \begin{pmatrix} \omega^2 & \omega & \omega^2 \\ \omega & 0 & \omega^2 \\ \omega^2 & \omega & \omega \end{pmatrix} X^4 + \begin{pmatrix} \omega^2 & \omega^2 & 0 \\ 1 & \omega^2 & 0 \\ 1 & \omega^2 & \omega \end{pmatrix} X^3$$

$$+\begin{pmatrix} 1 & \omega & \omega^2 \\ 0 & 0 & 1 \\ 0 & 0 & \omega \end{pmatrix} X^2 + \begin{pmatrix} 0 & 1 & 0 \\ \omega^2 & 1 & \omega \\ 1 & \omega & \omega^2 \end{pmatrix} X + \begin{pmatrix} 1 & \omega^2 & 1 \\ \omega^2 & \omega & \omega^2 \\ 1 & \omega^2 & 1 \end{pmatrix}.$$

One generator matrix of C is

$$\begin{pmatrix}
0 & 0 & 0 & 1 & 0 & \omega & 1 & \omega & 1 & 1 & 1 & 0 & \omega^2 & \omega & \omega^2 & 1 & 0 & 0 \\
1 & \omega^2 & 1 & 1 & \omega & \omega^2 & \omega^2 & \omega & 1 & 1 & 0 & \omega & \omega & 0 & \omega^2 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & \omega & 1 & \omega^2 & 1 & \omega & 1 & 1 & \omega^2 & \omega & \omega & 0 & 0 & 1 \\
1 & \omega^2 & 1 & 0 & 1 & 0 & 1 & \omega & \omega^2 & \omega^2 & \omega^2 & 0 & \omega^2 & \omega & \omega^2 & 1 & 0 & 0 \\
\omega^2 & \omega & \omega^2 & \omega^2 & 1 & \omega & 0 & 0 & 1 & 1 & \omega^2 & 0 & \omega & 0 & \omega^2 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \omega^2 & 1 & \omega^2 & 1 & 1 & 1 & 0 & \omega^2 & \omega^2 & \omega \\
0 & 1 & 0 & 1 & \omega & 1 & 1 & \omega^2 & \omega & \omega & \omega^2 & 1 & 1 & 0 & \omega^2 & \omega^2 & 0 & \omega \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & \omega^2 & 1 & \omega & 1 & \omega^2 & 1 & 1 & \omega & \omega^2 & \omega^2 \\
1 & 0 & 0 & 1 & \omega & 1 & 0 & 1 & 0 & 1 & \omega^2 & \omega & \omega & \omega & 0 & \omega & \omega^2 & \omega \\
0 & 1 & 0 & \omega & \omega^2 & \omega & \omega & 1 & \omega^2 & 0 & 0 & 1 & 1 & \omega & 0 & \omega^2 & 0 & \omega \\
\omega^2 & \omega & \omega^2 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \omega^2 & 1 & \omega & 1 & 1 & 1 & 0 \\
\omega & 0 & \omega & 0 & 1 & 0 & 1 & \omega^2 & 1 & 1 & \omega & \omega^2 & \omega^2 & \omega & 1 & 1 & 0 & \omega \\
\omega^2 & \omega & \omega^2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & \omega & 1 & \omega^2 & 1 & 1 & 1 & 1 \\
\omega^2 & \omega & \omega^2 & 1 & 0 & 0 & 1 & \omega^2 & 1 & 0 & 1 & 0 & 1 & \omega & \omega^2 & \omega^2 & \omega^2 & 0 \\
\omega & \omega & 0 & \omega & \omega^2 & \omega & 1 & 0 & 0 & 1 & \omega & 1 & 0 & 1 & 0 & 1 & \omega^2 & \omega
\end{pmatrix}$$

The above algorithm gives a generator polynomial of C which is

$$g(X) = \begin{pmatrix} \omega^2 & 0 & \omega^2 \\ \omega & 0 & 0 \\ 0 & 1 & \omega \end{pmatrix} X + \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

6 Acknowledgments

The authors wish to express sincere thanks to the anonymous referees who gave helpful comments and suggestions to improve the presentation of the paper.

References

[1] Taher Abualrub, Ali Ghrayeb, Nuh Aydin and Irfan Siap, On the Construction of Skew-quasi-cyclic Codes, *IEEE Transactions On Information Theory*, 2010, 56(5):2081-2090.

[2] Maheshanand Bhaintwal, Skew-quasi-cyclic codes over Galois rings, *Design Codes Cryptogr.*, 2012, 62(1):85-101.

[3] M. Barbier, C. Chabot and G. Quintin, On quasi-cyclic codes as a generalization of cyclic codes, *Finite Fields and Their Applications*, 2011, 18(96):904-919.

[4] D. Boucher, W. Geiselmann and F. Ulmer, Skew-cyclic codes, *Applicable Algebra In Engineering Communication And Computing*, 2007, 18(4):379-389.

[5] Delphine Boucher and Felix Ulmer, Coding with skew polynomial rings, *Journal of Symbolic Computation*, 2009, 44(12):1644-1656.

[6] Delphine Boucher, Patrick Sole and Felix Ulmer, Skew constacyclic codes over Galois rings , *Advances In Mathematics Of Communications*, 2008, 2(3):273-292.

[7] Pierre-Louis Cayrel, Christophe Chabot and Abdelkader Necer, Quasi-cyclic codes as codes over rings of matrices, *Finite Fields and Their Applications*, 2010, 16(2):100-115.

[8] Yonglin Cao and Jian Gao,Constructing quasi-cyclic codes from linear algebra theory, *Design Codes Cryptogr.*, 2013, 67(1):59-75.

[9] Sunghyu Han, Jon-Lark Kim, Heisook Lee and Yoonjin Lee, Construction of quasi-cyclic self-dual codes, *Finite Fields and Their Applications*, 2012, 18(3):613-633.

[10] Patrick Sole and Olfa Yemen, Binary quasi-cyclic codes of index 2 and skew polynomial rings, *Finite Fields and Their Applications*, 2012, 18(4):685-699.