On the Construction of Skew Quasi-Cyclic Codes[†]

Taher Abualrub, Ali Ghrayeb, Nuh Aydin, and Irfan Siap

Abstract

In this paper we study a special type of quasi-cyclic (QC) codes called skew QC codes. This set of codes is constructed using a non-commutative ring called the skew polynomial rings $F[x;\theta]$. After a brief description of the skew polynomial ring $F[x;\theta]$ it is shown that skew QC codes are left submodules of the ring $R_s^l = (F[x;\theta]/(x^s-1))^l$. The notions of generator and parity-check polynomials are given. We also introduce the notion of similar polynomials in the ring $F[x;\theta]$ and show that parity-check polynomials for skew QC codes are unique up to similarity. Our search results lead to the construction of several new codes with Hamming distances exceeding the Hamming distances of the previously best known linear codes with comparable parameters.

I. Introduction

Since the introduction of Shannon theory in 1948, coding theorists have been trying to design powerful codes that approach the Shannon capacity with reasonable complexity. Initially the focus was on designing codes that posses large minimum distances, resulting in several classes of linear block codes and convolutional codes. With the invention of turbo codes in 1993, where more focus has been given to reducing the multiplicity of the minimum distance rather than increasing the minimum distance itself, concatenated codes that perform within a few tenths of a dB from capacity have been designed and incorporated in a number of communications applications standards. However, since these codes have been developed for additive white Gaussian noise (AWGN) channels, they may not be the best choice for most wireless communications applications in which the channel normally suffers from severe fading. Such applications include cellular networks, wireless local area networks and wireless sensor networks, to name a few. To this end, a relatively new class of codes termed *space-time coding* has been introduced, which includes space-time trellis codes [1] and space-time block codes [2], [3]. Such codes are suitable for multiple-input multiple-output (MIMO) systems where the transmitter and/or receiver are equipped with multiple antennas. It has been shown that a MIMO system with N_t transmit and N_r receive antennas achieves a spatial diversity of N_tN_r [1]$-$[3]. To achieve better performance, one may need to combine error correcting coding with space-time coding since the former coding method introduces temporal diversity. For example, in a coded MIMO system, the maximum diversity that can be achieved (over block faded channels with proper interleaving) can be as high as $N_tN_rd^H_{\min}$, where $d^H_{\min}$ denotes the minimum Hamming distance of the error correcting code employed [4]. This suggests that having a code with a high minimum Hamming distance is essential since it offers significant performance improvements.

A significant portion of the work on error correcting codes for over the last sixty years has been on the construction of different types of codes defined over commutative rings. At the beginning, most of the research on error correcting codes was concentrated on codes over finite fields. More recently, it has been shown by many researchers (e.g., [5],[6],[10],[12]) that codes over rings are a very important class and many types of codes with good parameters can be constructed over rings. We believe that another important direction to consider is the construction of codes using non-commutative rings. Research on this topic is very recent and interesting. Boucher, et. al generalized in [8], [9] the notion of cyclic codes by using generator polynomials in a non-commutative polynomial ring called skew polynomial ring. They gave examples of skew cyclic codes with Hamming distances larger than previously best known linear codes of the same length and dimension [8].

Quasi-cyclic (QC) codes of index l over a finite field F are linear codes where the cyclic shift of any codeword by l positions is another codeword. QC codes of index $l = 1$ are well known cyclic codes. QC codes have been shown to be a very important class of linear codes [11], [18], [19], [22], [23], and [26]. Many of the best known and optimal linear codes that have been constructed so far are examples of QC codes (e.g., [11], [15],[16],[14], and [25].)

In this paper we study the construction of skew QC codes. This work has been motivated by the fact that the class of skew QC codes is much larger than the class of QC codes, suggesting that better codes may be found in this class. Indeed, we have found many examples of skew QC codes that meet or exceed the parameters of best known linear codes. In particular we are interested in the study of 1-generator skew QC codes and their properties. We show that this class of codes share many properties of QC codes.

T. Abualrub is with the Department of Mathematics and Statistics, American University of Sharjah, Sharjah, UAE (e-mail: abualrub@aus.edu).

A. Ghrayeb is with the Department of Electrical and Computer Engineering, Concordia University, Montreal, Quebec, Canada (e-mail: aghrayeb@ece.concordia.ca).

N. Aydin is with the Department of Mathematics, Kenyon College, Gambier, OH, USA (e-mail: aydinn@kenyon.edu).

I. Siap is with the Education Faculty, Adiyaman Univ., Adiyaman, Turkey (e-mail: isiap@adiyaman.edu.tr).

[0†]The work of T. Abualrub and A. Ghrayeb was supported in part by the Natural Sciences and Engineering Research Council of Canada (NSERC) while the first author was on sabbatical in the Department of Electrical and Computer Engineering, Concordia University, Montreal, Quebec, Canada.

The rest of the paper is organized as follows. Section II includes a brief description of the skew polynomial ring $F[x;\theta]$. In Section III, we discuss the structure of skew QC codes where we show that this type of codes is a left submodule of $R_s^l = (F[x;\theta]/(x^s-1))^l$. We also discuss the dimension and the parity check polynomial for these codes. In Section IV we introduce the notion of similar polynomials. We will show that the parity-check polynomial of a skew QC code is unique up to similarity. Section V includes our search results. As a result of a search in the class of skew QC codes over $GF(4)$, we obtain seven new linear quaternary codes with Hamming distances greater than previously best known linear codes with the given parameters. These new codes have the parameters $[48, 12, 24]$, $[72, 21, 29]$, $[48, 16, 20]$, $[96, 16, 49]$, $[100, 20, 47]$, $[140, 20, 72]$, and $[110, 22, 51]$. We also construct a large number of skew QC codes with Hamming distances equal to the Hamming distances of the best known linear codes with the given parameters. Section VI concludes the paper.

II. The Skew Polynomial Ring $F[x;\theta]$

Let F be a finite field of characteristic p. Let θ be an automorphism of F with $|\langle\theta\rangle| = m$. Let K be the subfield of F fixed under $\langle\theta\rangle$. Then, $[F : K] = m$ and $K = GF(p^t)$, $F = GF(q)$ where $q = p^{tm}$. Moreover since K is fixed under θ then we have $\theta(a) = a^{p^t}$ for all $a \in F$.

Example 1: Consider the finite field $GF(4) = \{0, 1, a, a^2\}$ where $a^2 + a + 1 = 0$. Define an automorphism

$$\begin{aligned} \theta &: GF(4) \to GF(4) \text{ by} \\ \theta(z) &= z^2. \end{aligned}$$

Then $\theta(0) = 0,\ \theta(1) = 1,\ \theta(a) = a^2$ and $\theta(a^2) = a$. Hence the fixed field K is just the binary field $GF(2)$.

Definition 1: Following the above notation, define the skew polynomial set $F[x;\theta]$ to be

$$F[x;\theta] = \left\{ \begin{array}{c} f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n| \text{ where} \\ a_i \in F \text{ for all } i = 0, 1, \ldots, n \end{array} \right\}$$

where addition of these 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: Using the same automorphism from Example1, we get

$$\begin{aligned} (ax)(a^2x) &= a\theta(a^2)x^2 \\ &= a \cdot ax^2 = a^2x^2. \end{aligned}$$

On the other hand we have,

$$\begin{aligned} (a^2x)(ax) &= a^2\theta(a)x^2 \\ &= a^2(a^2)x^2 = ax^2. \end{aligned}$$

This shows that $(ax)(a^2x) \neq (a^2x)(ax)$.

Theorem 1: [20] The set $F[x;\theta]$ with respect to addition and multiplication defined above forms a non-commutative ring called the skew polynomial ring.

The following facts are straightforward for the ring $F[x;\theta]$:

1. It has no nonzero zero-divisors.
2. The units of $F[x;\theta]$ are the units of F.
3. $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$
4. $\deg(fg) = \deg(f) + \deg(g)$.

The skew polynomial ring $F[x;\theta]$ was introduced by Ore [21] in 1933, and a complete treatment of this ring can be found in [17] and in [20].

Theorem 2: [20] (The Right Division Algorithm) For any polynomials f and g in $F[x;\theta]$ with $f \neq 0$ there exist unique polynomials q and r such that

$$g = qf + r \text{ where } \deg(r) < \deg(f).$$

The above result is called division on the right by f. A similar result can be proved regarding division on left by f.

Applying the division algorithm above one can easily prove the following Theorem.

Theorem 3: [17] $F[x;\theta]$ is a non-commutative principal left (right) ideal ring. Moreover any two sided ideal must be generated by

$$f(x) = \left(a_0 + a_1x^m + a_2x^{2m} + \ldots + a_rx^{rm}\right)x^t,$$

where $|\langle\theta\rangle| = m$.

Corollary 1: Let θ be an automorphism of F with $|\langle\theta\rangle| = m$. Then $(x^s - 1)$ is a two sided ideal in $F[x;\theta]$ iff $m|s$.

Lemma 1: $(x^s - 1) \in Z(F[x;\theta])$ for $m|s$, where $Z(F[x;\theta])$ is the center of $F[x;\theta]$.

Proof: Let $f(x) = a_0 + a_1x + \cdots + a_rx^r \in F[x;\theta]$. Since $m|s$, then $\theta^s(a) = a$ for any $a \in F$. Hence,

$$\begin{aligned}(x^s-1)f(x) &= (x^s-1)(a_0 + a_1x + \cdots + a_rx^r)\\ &= a_0x^s + a_1x^{s+1} + \cdots + a_rx^{s+r}\\ &\quad -a_0 - a_1x + \cdots - a_rx^r\\ &= (a_0 + a_1x + \cdots + a_rx^r)(x^s-1)\\ &= f(x)(x^s-1).\end{aligned}$$

■

Lemma 2: [9] If $g \cdot h \in Z(F[x;\theta])$ then $g \cdot h = h \cdot g$

From Theorem 3, Lemma 1, and Lemma 2, we may conclude that the factors of $x^s - 1$ commute. Thus if f is a left divisor then it is a right divisor as well. This fact will help in reducing the complexity of factoring $x^s - 1$ in $F[x;\theta]$. From now on we will say divisors or factors of $x^s - 1$ without specifying left or right.

Definition 2: A polynomial f is called a left multiple of a polynomial d (in this case d will be called a right divisor of f) if there exits a polynomial g such that

$$f = gd.$$

Definition 3: A monic polynomial d is called the greatest common right divisor (gcrd) of f and g if
1. d is a right divisor of f and g, and
2. If e is another right divisor of f and g then $d = ke$ for some polynomial k.

The greatest common left divisor (gcld) of a and b is a monic polynomial defined in a similar way. Similarly we define the least common right multiple of a and b lcrm$[a, b]$ and the least common left multiple of a and b, lclm$[a, b]$

Theorem 4: [21] gcrd, gcld, lcrm, and lclm can be calculated using the left and right division algorithms.

III. Skew Quasi Cyclic Codes

Definition 4: Let F be a finite field of characteristic p with $q = p^{mt}$ elements, and let θ be an automorphism of F with $|\langle\theta\rangle| = m$. A subset C of F^n is called a skew quasi-cyclic code of length n where $n = sl$, $m|s$, and index l if
1. C is a subspace of F^n.
2. If

$$c = \begin{pmatrix} c_{0,0}, c_{0,1}, \ldots, c_{0,l-1}, c_{1,0}, c_{1,1}, \ldots, c_{1,l-1}, \ldots, \\ c_{s-1,0}, c_{s-1,1}, \ldots, c_{s-1,l-1} \end{pmatrix} \in C$$

then

$$T_{\theta,s,l}(c) = \begin{pmatrix} \theta(c_{s-1,0}), \theta(c_{s-1,1}), \ldots, \theta(c_{s-1,l-1}), \theta(c_{0,0}), \\ \ldots, \theta(c_{0,l-1}), \ldots, \theta(c_{s-2,0}), \ldots, \theta(c_{s-2,l-1}) \end{pmatrix} \in C.$$

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

In [8], Boucher, etc. studied skew cyclic codes over F. They showed that a code C is a skew cyclic code if and only if C is a left ideal generated by $g(x)$ where $g(x)$ is a right divisor of $x^n - 1$.

Recall from Corollary 1 that $x^s - 1$ is a two sided ideal iff $m|s$. Because of this, we will always assume that C is a skew quasi-cyclic code of length n where $n = sl$, $m|s$, and index l.

In this paper we focus on skew QC codes over the finite field $F = GF(4)$ even though most results can be generalized to any finite field.

The ring $R_s^l = (F[x;\theta]/(x^s - 1))^l$ is a left $R_s = F[x;\theta]/(x^s - 1)$ module where we define multiplication from left by

$$\begin{aligned}&f(x)(g_1(x), g_2(x), \ldots, g_l(x))\\ =\ &(f(x)g_1(x), f(x)g_2(x), \ldots, f(x)g_l(x)).\end{aligned}$$

Let $c = \begin{pmatrix} c_{0,0}, c_{0,1}, \ldots, c_{0,s-1}, c_{1,0}, c_{1,1}, \ldots, c_{1,l-1}, \\ \ldots, c_{l-1,0}, c_{l-1,1}, \ldots, c_{l-1,s-1} \end{pmatrix}$ be an element in F^{sl}. Define a map $\phi : F^{sl} \to R_s^l$ by

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

where

$$c_j(x) = \sum_{i=0}^{s-1} c_{i,j}x^i \in F[x;\theta]/(x^s - 1) \text{ for } j = 0, 1, \ldots, l-1.$$

The map ϕ gives a one to one correspondence between the ring F^{sl} and the ring R_s^l. It is also a vector space isomorphism between F^{sl} and R_s^l, when considered as vector spaces over F.

Theorem 5: A subset C of F^n is a skew QC code of length $n = sl$ and index l if and only if $\phi(C)$ is a left submodule of the ring R_s^l.

Proof: Let C be a skew QC code of index l over F. We claim that $\phi(C)$ forms a submodule of R_s^l where ϕ is the map defined above. Clearly, $\phi(C)$ is closed under addition and scalar multiplication (by elements of F). Let

$$\phi(c) = (c_0(x), c_1(x), \ldots, c_{l-1}(x)) \in \phi(C).$$

for

$$c = \begin{pmatrix} c_{0,0}, c_{0,1}, \ldots, c_{0,s-1}, c_{1,0}, c_{1,1}, \ldots, \\ c_{1,s-1}, \ldots, c_{l-1,0}, c_{l-1,1}, \ldots, c_{l-1,s-1} \end{pmatrix} \in C$$

.

Then

$$\begin{aligned} x\phi(c) &= (xc_0(x), xc_1(x), \ldots, xc_{l-1}(x)) \\ &= \begin{pmatrix} \theta(c_{s-1,0}) + \theta(c_{0,0})\, x + \cdots + \\ \theta(c_{s-2,0})\, x^{s-1}, \theta(c_{s-1,1}) + \theta(c_{0,1})\, x + \cdots \\ +\theta(c_{s-1,1})\, x^{s-1}, \ldots, \theta(c_{s-1,l-1}) + \\ \theta(c_{0,l-1})\, x + \cdots + \theta(c_{s-1,l-1})\, x^{s-1} \end{pmatrix} \\ &= \phi \begin{pmatrix} \theta(c_{s-1,0}), \theta(c_{s-1,1}), \ldots, \\ \theta(c_{s-1,l-1}), \theta(c_{0,0}), \theta(c_{0,1}), \ldots, \\ \theta(c_{0,l-1}), \ldots, \theta(c_{s-2,0}), \\ \theta(c_{s-2,1}), \ldots, \theta(c_{s-2,l-1}) \end{pmatrix} \in \phi(C). \end{aligned}$$

Then, by linearity it follows that $p(x)\phi(c) \in \phi(C)$ for any $p(x) \in R_s$. Hence $\phi(C)$ is a left submodule of R_s^l.

Conversely, suppose D is an R_s left submodule of R_s^l. Let $C = \phi^{-1}(D) = \{c \in F^n : \phi(c) \in D\}$. We claim that C is a skew QC code over F. Since ϕ is a vector space isomorphism, C is a linear code of length n over F. To show that C is closed under skew cyclic shift, let $c = (c_{0,0}, c_{0,1}, \ldots, c_{0,s-1}, c_{1,0}, c_{1,1}, \ldots, c_{1,s-1}, \ldots, c_{l-1,0}, c_{l-1,1}, \ldots, c_{l-1,s-1}) \in C$. Then, $\phi(c) = (g_0(x), g_1(x), \ldots, g_{l-1}(x)) \in D$, where $g_j(x) = \sum_{i=0}^{s-1} c_{i,j}x^i$ for $j = 0, 1, \ldots, l-1$. From the above discussion, it is easy to see that $\phi(T_{\theta,s,l}(c)) = x(g_0(x), g_1(x), \ldots g_{l-1}(x)) = (xg_0(x), xg_1(x), \ldots, xg_{l-1}(x)) \in D$. Hence $T_{\theta,s,l}(c) \in C$. Therefore C is a skew quasi-cyclic code C. ■

From now on we concentrate on 1-generator skew QC codes that are cyclic left submodules of R_s^l. i.e. any skew QC code C that has the form

$$C = \{f(x)(g_1(x), g_2(x), \ldots, g_l(x)) : \ f(x) \in R_s \}.$$

Sometimes we denote this by

$$C = \left\{ \begin{array}{c} f(x)G(x) : \ f(x) \in R_s \ \text{ and } \\ G(x) = (g_1(x), g_2(x), \ldots, g_l(x)) \end{array} \right\}.$$

Theorem 6: Let C be a one generator skew QC code of length $n = sl$ and index l. Then C is generated by an element of the form

$$(p_1(x)g_1(x), p_2(x)g_2(x), \ldots, p_l(x)g_l(x))$$

where $g_i(x)$ is a divisor of $(x^s - 1)$.

Proof: Let C be a 1-generator skew QC code generated by $(f_1, \ f_2, \ldots, \ f_l)$. For all $1 \leq i \leq l$ define the following map

$$\begin{aligned} \Pi_i &: C \to R_s \text{ by} \\ \Pi_i((kf_1, kf_2, \ldots, kf_l)) &= kf_i. \end{aligned}$$

The function Π_i is a module homomorphism. It is clear that the image of Π_i is a left ideal and thus is a skew cyclic code in R_s. Therefore, $kf_i \in \Pi_i(C) = (g_i)$ for all $i = 1, 2, \ldots, l$. Hence,

$$C = (p_1(x)g_1(x), p_2(x)g_2(x), \ldots, p_l(x)g_l(x)),$$

where $g_i(x)$ is a divisor of $(x^s - 1)$. ■

Definition 5: Let

$$C = (p_1(x)g_1(x), p_2(x)g_2(x), \ldots, p_l(x)g_l(x))$$

be a skew QC code of length $n = sl$ and index l. The unique monic polynomial

$$g(x) = gcld \begin{pmatrix} p_1(x)g_1(x), p_2(x)g_2(x), \\ \ldots, p_l(x)g_l(x), x^s - 1 \end{pmatrix}$$

is called the generator polynomial of C.

Definition 6: The monic polynomial $h(x)$ of minimal degree such that

$$h(x)\begin{pmatrix} p_1(x)g_1(x), p_2(x)g_2(x), \\ \ldots, p_l(x)g_l(x) \end{pmatrix} = (0, 0, \ldots, 0)$$

is called the parity-check polynomial of C

Theorem 7: Suppose $d(x) = gcrd(f, g)$, then there are polynomials polynomials $a(x)$, and $b(x)$ such that

$$a(x)f(x) + b(x)g(x) = d(x).$$

Proof: The proof is similar to the case of $\gcd(a, b)$ when the ring is commutative. Suppose $d(x) = gcrd(f, g)$. Consider the left ideal generated by $(f(x), g(x))$. Since $F_q[x; \theta]$ is a principal left ideal ring, there exists a polynomial $h(x)$ such that $(f(x), g(x)) = (h(x))$. Hence $f(x) = r_1(x)h(x)$ and $g(x) = r_2(x)h(x)$. But $d(x) = gcrd(f, g)$ implies that $d(x) = k(x)h(x)$ and $(d(x)) \subseteq (h(x))$. Since $d(x) = gcrd(f, g)$ then $f(x)$ and $g(x) \in$left ideal $(d(x))$. Hence $(h(x)) \subseteq (d(x)$ and we have $(d(x)) = (f(x), g(x)) = (h(x))$. Therefore there are polynomials $a(x)$, and $b(x)$ such that

$$a(x)f(x) + b(x)g(x) = d(x).$$

■

Corollary 2: Suppose $d(x) = gcld(f, g)$, then there are two polynomials $a(x)$, and $b(x)$ such that

$$f(x)a(x) + g(x)b(x) = d(x).$$

Lemma 3: Let $g(x)$ and $h(x)$ be the generator and the parity-check polynomials of a skew QC code C. Then

$$x^s - 1 = h(x)g(x) = g(x)h(x).$$

Proof: Since $g(x) = gcld\begin{pmatrix} p_1(x)g_1(x), p_2(x)g_2(x), \\ \ldots, p_l(x)g_l(x), x^s - 1 \end{pmatrix}$, then $x^s - 1 = g(x)k(x)$ for some polynomial $k(x)$. Note that by Lemma 2 we have $x^s - 1 = g(x)k(x) = k(x)g(x)$. Note also that $p_i(x)g_i(x) = g(x)\alpha_i(x)$ for all $i = 1, \ldots, l$. Hence we have

$$\begin{aligned} k(x)\begin{pmatrix} p_1(x)g_1(x), p_2(x)g_2(x), \\ \ldots, p_l(x)g_l(x) \end{pmatrix} &= \\ k(x)\begin{pmatrix} g(x)\alpha_1(x), g(x)\alpha_2(x), \\ \ldots, \alpha_l(x)g(x)\alpha_l(x) \end{pmatrix} &= (0, 0, \ldots, 0). \end{aligned}$$

Hence $k(x) = q(x)h(x)$ and $\deg k(x) \geq \deg h(x)$. Now by Corollary 2, there are polynomials $a_i(x)$ such that

$$\begin{aligned} & p_1(x)g_1(x)a_1(x) + p_2(x)g_2(x)a_2(x) + \ldots \\ & +(x^s - 1)a_{l+1}(x) \\ = \; & g(x). \end{aligned}$$

Hence,

$$\begin{aligned} & h(x)p_1(x)g_1(x)a_1(x) + h(x)p_2(x)g_2(x)a_2(x) \\ & + \ldots + h(x)(x^s - 1)a_{l+1}(x) \\ = \; & h(x)g(x) \\ 0 = \; & h(x)g(x). \end{aligned}$$

This implies that $\deg h(x) \geq \deg \dfrac{x^s - 1}{g(x)} = \deg k(x)$. Therefore $k(x) = h(x)$. ■

Definition 7: Let $C = \langle G(x) \rangle$ be a skew QC code. The annihilator of C is the set

$$I = \{r(x) : r(x)F(x) = 0 \text{ for all } F(x) \in C\}.$$

It is clear that I is a left ideal in R_s.

Lemma 4: Let $C = G(x)$ be a skew quasi-cyclic code with annihilator I. Then $I = (h(x))$ and

$$\begin{aligned} C &\cong R_s/I, \text{ and} \\ \dim C &= \deg h(x). \end{aligned}$$

Proof: Define the map

$$\begin{aligned} \Psi &: R_s \to C \text{ by} \\ \Psi(r(x)) &= r(x)G(x) \end{aligned}$$

Ψ is an onto module homomorphism with $\ker \Psi = I = (h(x))$. Therefore $C \cong R_s/(h(x))$ and hence $\dim C = \deg h(x)$. ■

IV. Similar Polynomials in $F[x;\theta]$.

In the case of QC codes in the ring $F[x]$, we know that the parity-check polynomials are unique up to a unit. In the case of skew QC codes things are not as straightforward as in the case of QC codes. To study the parity-check polynomials we need to introduce the notion of similar polynomials in the ring $F[x;\theta]$. Our main result is to show that two polynomials h_1 and h_2 are parity-check polynomials for a code C if and only if h_1 and h_2 are similar polynomials.

Definition 8: Two elements a and b in a ring R are called right similar if there is a $u \in R$ such that

$$\begin{aligned} gcld(u,b) &= 1 \text{ and} \\ ua &= lcrm[u,b]. \end{aligned}$$

Left similar elements can be defined similarly.

Example 3: Let F be any field of characteristic p. We will show when two linear polynomials $p_1(x) = x - \alpha$ and $p_2 = x - \beta$ are right similar.

Let $u = c \in F$, then $gcld\,(u, p_2) = 1$ and $cc^{-1}p_2$ is a right multiple of u and p_2. Hence, $[u, p_2] = cp_1$ iff

$$cc^{-1}p_2 = cp_1\gamma = c(x-\alpha)\gamma \text{ for some } \gamma \in F.$$

Hence,

$$x - \beta = c\theta(\gamma) - ca\gamma = c\gamma^{p^t} - ca\gamma.$$

This implies that

$$\begin{aligned} 1 &= c\gamma^{p^t} \text{ and } \beta = ca\gamma. \text{ This implies} \\ \beta &= a\gamma^{1-p^t} \text{ or } \alpha\beta^{-1} = \gamma^{p^t-1} \in F \end{aligned}$$

Therefore, $x - \alpha$ is similar to $x - \beta$ iff $\alpha\beta^{-1} = \gamma^{p^t-1} \in F$.

If we consider the field $GF(2^2)$ and the frobenoius automorphism we can conclude that the polynomials $p_1(x) = x-1$, $p_2(x) = x - \alpha$ and $p_3(x) = x - \alpha^2$ are all right similar.

Theorem 8: If a and b are right similar then they are left similar.

Proof: Suppose there is a $u \in R$ such that

$$\begin{aligned} gcld(u,b) &= 1 \text{ and} \\ ua &= lcrm[u,b]. \end{aligned}$$

Let

$$m = ua = lcrm[u,b].$$

Then $m = ua = bc$ for some c. This shows that

$$lclm[c,a] = m.$$

Now suppose $gcrd(c,a) = d$, then

$$c = \alpha_1 d \text{ and } a = \alpha_2 d.$$

Hence,

$$m = ua = u\alpha_2 d = bc = b\alpha_1 d.$$

This implies that

$$lcrm[u,b] = u\alpha_2 = b\alpha_1 \neq m.$$

A contradiction. Hence $gcrd(c,a) = 1$. This shows that a and b are left similar. ■

From now on we if a and b are right similar we will say that they are similar. In the case that the ring is commutative then two elements are similar iff they differ by a unit.

Theorem 9: Let $h_1(x)$ be a parity-check polynomial of a skew QC code C_1, and let $h_2(x)$ be a parity-check polynomial of a skew QC code C_2 then $C_1 = C_2$ iff $h_1(x)$ is similar to $h_2(x)$.

Proof: Suppose $C_1 = C_2$. Then $R_s/\left(h_1(x)\right) \cong R_s/\left(h_2(x)\right)$. Let

$$\Phi : R_s/\left(h_1(x)\right) \to R_s/\left(h_2(x)\right)$$

be such a module isomorphism. Suppose $\Phi(1 + (h_1(x))) = a + (h_2(x))$ then

$$\Phi(r + (h_1(x))) = ra + (h_2(x)) \text{ for any } r \in R_s. \tag{1}$$

In particular we have

$$\Phi(h_1 + (h_1(x))) = h_1 a + (h_2(x)).$$

Since Φ is a module isomorphism we must have

$$\Phi(h_1 + (h_1(x))) = h_2(x) = 0.$$

This implies that $h_1 a \in (h_2(x))$ and hence $h_1 a = r_2 h_2 = m$.

Since Φ is surjective then there is $c \in R$ such that

$$\Phi(c + (h_1(x))) = ca + (h_2(x)) = 1 + (h_2(x)).$$

Hence $ca - 1 \in (h_2(x))$. This gives

$$\begin{aligned} ca - 1 &= l(x)h_2(x). \text{ Or} \\ ca - l(x)h_2(x) &= 1. \end{aligned}$$

Hence

$$gcrd(a, h_2(x)) = 1. \tag{2}$$

Suppose $lclm[a, h_2(x)] = k$. Then

$$k = \alpha_1 a = \alpha_2 h_2 \in (h_2(x)).$$

Since Φ is injective then $\alpha_1 \in (h_1(x))$. Hence $\alpha_1 = t_1 h_1(x)$ and $k = t_1 h_1(x) a$. But we have $h_1 a = r_2 h_2 = m$. Therefore

$$lclm[a, h_2(x)] = h_1 a. \tag{3}$$

From equations 2 and 3, we get that $h_1(x)$ and $h_2(x)$ are (left) similar.

Now suppose $h_1(x)$ is (left) similar to $h_2(x)$. Then there is u such that

$$\begin{aligned} gcrd(u, h_2) &= 1 \text{ and} \\ lclm[u, h_2] &= h_1 u \end{aligned}$$

Define

$$\Psi : R_s/\left(h_1(x)\right) \to R_s/\left(h_2(x)\right)$$

by

$$\Psi(r + (h_1(x)) = ru + (h_2(x)).$$

It is clear that Ψ is a module homomorphism. It is left to show that Ψ is a bijective function.

Since $gcrd(u, h_2) = 1$ then $c_1 u + c_2 h_2 = 1$ for some c_1 and $c_2 \in R_s$. This implies that

$$\Psi(c_1 + (h_1(x)) = c_1 u + (h_2(x)) = 1 + (h_2(x)).$$

So for any $r + (h_2(x)) \in R_s/(h_2(x))$ we have

$$\Psi(rc_1 + (h_2(x))) = r\Psi(c_1 + (h_2(x))) = r + (h_2(x)).$$

Therefore Ψ is surjective. Suppose

$$\Psi(s + (h_1(x)) = su + (h_2(x)) = h_2(x)$$

for some s. Then $su \in (h_2(x))$. So,

$$su = rh_2(x) \text{ for some } r.$$

Since $lclm[u, h_2] = h_1 u$, we have

$$su = t_1 h_1 u.$$

To show Ψ is injective we need to show that $s \in (h_1(x))$. By the right division algorithm we have

$$s = q_1 h_1 + r_1 \text{ where } \deg r_1 < \deg h_1.$$

This implies that

$$su = q_1 h_1 u + r_1 u \Rightarrow r_1 u \in (h_2(x))$$

Since $lclm[u, h_2] = h_1 u$ then $r_1 u = t_2 h_1 u \in (h_1(x))$. If $r_1 \in (h_1(x))$ then

$$s = q_1 h_1 + r_1 \in (h_1(x)),$$

and hence Ψ is injective. If $r_1 \notin (h_1(x))$ then repeat the right division algorithm again until we get a remainder $r_i \in (h_1(x))$. This implies $r_{i-1}, r_{i-2}, \ldots, s \in (h_1(x))$. Therefore Ψ is injective and hence it is an isomorphism. ■

V. Search Results

The **Hamming weight enumerator**, $W_C(y)$, of a code C is defined by

$$W_C(y) = \sum_{c \in C} y^{w(c)} = \sum_i A_i y^i \tag{4}$$

where $w(c)$ is the number of the nonzero coordinates of the codeword c and $A_i = |\{c \in C | w(c) = i\}|$, i.e. the number of codewords in C whose weights equal to i.

The smallest non-zero exponent of y with a nonzero coefficient in $W_C(y)$ is equal to the minimum distance of the code.

We know that the ring $F[x]$ is a unique factorization domain and the polynomial $x^s - 1$ has a unique factorization as a product of irreducible polynomials in $F[x]$. Things are different in the ring $F[x;\theta]$. The skew polynomial ring $F[x;\theta]$ is not a unique factorization domain and hence polynomials in general do not have a unique factorization as a product of irreducible polynomials.

Example 4: Consider $x^4 - 1$ over $F = GF(4)$. We have

$$\begin{aligned} x^2 - 1 &= (x-1)(x-1) \\ &= (x-a)(x-a^2), \end{aligned}$$

and

$$\begin{aligned} x^4 - 1 &= (x-1)^4 \\ &= (x+a)(x+a^2)(x+a)(x+a^2) \\ &= (x+a)(x+a)(x+a^2)(x+a^2) \\ &= (x+a)(x+a^2)(x+1)(x+1). \end{aligned}$$

One of the main problems of coding theory is to construct codes with best possible parameters. There is a well known table of linear codes with best known parameters over small finite fields [13]. The computer algebra system Magma also has such a database [7]. Researchers continuously update these tables as new codes are discovered. As the gaps narrow in the tables, it gets more and more difficult to find new codes. Many of the new codes discovered in recent years have come from the class of QC and QT codes (e.g., [6],[14],[15],[25]). One advantage of studying codes in $F[x;\theta]$ compared to codes over $F[x]$ is that the number of factors of $x^s - 1$ in $F[x;\theta]$ is much larger. Therefore, there are many more skew cyclic and skew QC codes in $F[x;\theta]$ than there are cyclic and QC codes in $F[x]$. This suggests that it may be possible to find new codes in the ring $F[x;\theta]$ with larger Hamming distances. Our search has yielded a number of skew QC codes with best known parameters. We call such codes "good codes". Seven of these codes lead to improvements in the table [13]. These are called "new codes". The improvement on minimum distance is 1 unit in each case. We present these codes in the rest of this section. These results show that the class of skew QC is a promising class that deserve further attention.

In view of the previos sectiond and the findings obtained therin, our strategy to search for new codes or good codes is as follows: Choose an integer s, and find a factor g of $x^s - 1$ in $F[x;\theta]$ (where $F = GF(4) = \{0, 1, a, a^2\}$). Then search for polynomials $f_1, f_2, \ldots, f_{l-1}$ so that the skew QC codes of the form $(g, f_1 \cdot g, \ldots, f_{l-1}g)$ have large minimum distances. We have used the computer algebra system Magma to carry out all of the computations.

Example 5: We consider a skew 2-QC code of length 48. Hence, we need a factorization of $x^{24} - 1$. One such factorization is $x^s - 1 = g \cdot h$ where $g = x^{12} + ax^9 + x^8 + ax^7 + ax^6 + x^5 + a^2x^4 + ax^3 + ax^2 + a^2x + a^2$ and $h = x^{12} + ax^9 + x^8 + ax^7 + a^2x^6 + x^5 + ax^4 + ax^3 + a^2x^2 + a^2x + a$. Letting $f = x^{11} + a^2x^10 + ax^9 + a^2x^7 + x^6 + a^2x^5 + ax^4 + ax^3 + x + a$, the code generated by $(g, f \cdot g)$ has parameters $[48, 12, 24]$ over $GF(4)$. This code has a larger minimum distance than the previously best known code with the same length and dimension.

The weight enumerator of this code is as follows:

$W_C = 1 + 3390y^{24} + 4608y^{25} + 19944y^{26} + 25968y^{27} + 99612y^{28} + 124272y^{29} + 388872y^{30} + 427392y^{31} + 1125315y^{32} + 958464y^{33} + 2102544y^{34} + 1529568y^{35} + 2798568y^{36} + 1613664y^{37} + 2320272y^{38} + 1078272y^{39} + 1224378y^{40} + 436608y^{41} + 345096y^{42} + 84528y^{43} + 54972y^{44} + 8112y^{45} + 2664y^{46} + 132y^{48}$.

Example 6: Let us consider a skew 3-QC code of length 72. We again need a factorization of $x^{24} - 1$. Here is another factorization of $x^{24} - 1$: $x^{24} - 1 = g \cdot h$, where $g = x^3 + a^2x^2 + 1$ and $h = x^{21} + ax^{20} + x^{19} + a^2x^{18} + x^{16} + x^{13} + ax^{12} + x^{11} + a^2x^{10} + x^8 + x^5 + ax^4 + x^3 + a^2x^2 + 1$. Now let $f_1 = x^{20} + x^{19} + x^{17} + a^2x^{15} + ax^{14} + a^2x^{13} + a^2x^{12} + a^2x^{11} + x^{10} + a^2x^9 + x^8 + x^7 + ax^6 + a^2x^5 + ax^2 + 1$ and $f_2 = x^{13} + a^2x^{12} + x^{10} + x^9 + x^8 + a^2x^7 + ax^3 + ax$ and consider the code C generated by $(g, f_1 \cdot g, f_2 \cdot g)$. It is a $[72, 21, 29]$ code and therefore better than the previously best known code with parameters $[72, 21, 28]$. The weight enumerator of C is also available (but not printed here).

In the rest of the examples, we use the trivial factor of 1, therefore the generators of the codes are of the form $(f_1, f_2, \ldots, f_l)$. We shall refer to such codes as non-degenerate skew QC codes (since the codes of the form $(f_1g, f_2g, \ldots, f_lg)$

TABLE I
PARAMETERS AND GENERATORS OF THE GOOD SKEW QC CODES OF INDEX 2

Parameters	g	f
$[40, 9, 21]$	$aa^200a1a^2a^210a1$	$a0000aa^201$
$[40, 10, 20]$	$a^2a^2a01a0aa^211$	$a^2a^2a^200a1aa^21$
$[40, 11, 19]$	$a10aaaa^21a1$	$a11aa^2100a^201$
$[40, 12, 18]$	$101a^200aa^21$	$1a100aaaaa^2a1$
$[40, 14, 16]$	$10a^21a01$	$11aaa^2a011$
$[40, 16, 15]$	10001	$aa0a^201011a^21a^20a^2$
$[40, 17, 14]$	a^21a^21	$a^2a1a^210a^20a0a^2a^2a^20a^211$
$[44, 12, 20]$	$11111aa11a^21$	$a000a^2a^2aa0a^2a1$
$[48, 11, 24]$	$1aa^21a0a^2a100101$	$aaaaa^21a10a1$
$[48, 12, 23]$	$a110a^21a^2a11a^2a^21$	$1a^20110010a11$
$[48, 13, 22]$	$a^2aa^200a100111$	$0001a0a^2a^2a^2aaa^21$
$[48, 14, 21]$	$11a^2a^2a10a^2101$	$1a11010a1a^2aa11$
$[48, 15, 20]$	$a^2a01a1a^2111$	$1aa^2a^2a^2a^2a^2a0aa1a11$
$[48, 16, 19]$	$a00101a^2a1$	$a^2a0a1a1aa1aa^2aa^2a^21$
$[52, 13, 24]$	$a^2a^2aa^210a^21a11aa1$	$aa^211aa^21a^2a^2a^2a^211$
$[60, 11, 32]$	$aaa^2a^2a^2a^211aa110000aa11$	$aa^2aa^20aa^2a1a^21$
$[60, 14, 28]$	$11a^2a11a^2a^2a^2a^2aa^2a^2a^2a^2a1$	$a^20a^2a0a110a^21011$

with $\deg g > 0$ are sometimes referred to as degenerate QC codes in the literature). The polynomials are represented by a list of coefficients of increasing powers. Hence, the sequence $a001aa^21$ represents the polynomial $x^6+a^2x^5+ax^4+x^3+a$.

Example 7: A $[48, 16, 20]$-code generated by $f1 = 0a^2a^2a0a^210a^20a11a^2a^21$, $f2 = 100a^20a^2a^2aa^21a^21a^20a^20$, $f3 = a^2aa0a^20aa1a^2aaa0aa$.

Example 8: A $[96, 16, 49]$-code generated by $f1 = 0a^2a^21aa^20aa100a^2a0a$, $f2 = 1a^2a^2aa00a^2a^211a^21a0a^2$, $f3 = 0a^2a^200aaaa^21a1a^20aa^2$, $f4 = a0a^200a0a^2aa0aa1a^21$, $f5 = a^2011011a^21a1a^2a111$, $f6 = a100a^2a^2a^2a1a001aa^2a^2$

Example 9: A $[100, 20, 47]$-code generated by
$f1 = a00a^2a^2001a^2a^2a^2011a1a^2a11$,
$f2 = 01a^20a1a01a^21a1a01001a^2$,
$f3 = a1aa1001aa^20000a^2a1a^2a^21$,
$f4 = 1a1aa11a^2a^2aa^20a^2a0010a^21$,
$f5 = a^20111aa^21a^2aa^2a^2a0a^201a11$

Example 10: A $[140, 20, 72]$-code generated by
$f1 = 1a^2a^2aa1a10aa^210a01a^2a^201$,
$f2 = aa0a^201a^2aa0a0a1aa1a10$,
$f3 = a^2a^2a^21aa^2a1a0aaa^2a^20aa0aa$,
$f4 = 10001aaa^20a010a^2a^2a0010$,
$f5 = a11001a1a^2a^21aa^210aa^21a^2a$,
$f6 = a^20a^210a^211a^2a^2a^21a^2a^20a^20110$,
$f7 = a^21011000a^2a^201a^201a^2aa^2a^21$

Example 11: A $[110, 22, 51]$-code generated by
$f1 = 1a^2010aa0a^201a^2100a0a^2a0a^20$,
$f2 = a^2a0101aa^21a^2a^21a^211aaa^200a^21$,
$f3 = 00a^2a00a^201a^2aa100a0a^2a11a^2$,
$f4 = 01a01010a^211a01100a^2a^2a1a$,
$f5 = a^20a0a^2a^2a00a^2a10a0aaa1a^21a$

We summarize the rest of the results of our search that yielded good codes in the following three tables.

VI. CONCLUSION

In this paper, we study the structure of 1-generator skew QC codes in the non-commutative ring $F[x;\theta]$. We have shown that skew QC codes are left submodules of the ring $R_s^l = (F[x;\theta]/(x^s-1))^l$. We also introduced the notion of similar polynomials in the ring $F[x;\theta]$ and showed that parity-check polynomials are unique up to similarity. Our search

results showed the construction of several new linear codes with Hamming distance larger than the Hamming distance of the best linear codes with similar parameters. An important problem that needs to be addressed is an efficient method of obtaining all factorizations of $x^n - 1$ in the skew polynomial ring. Also, a BCH type bound for skew cyclic and skew QC codes is a future topic of interest.

References

[1] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: Performance criterion and code construction," IEEE Trans. Inform. Theory, vol. 44, pp. 744–765, Mar. 1998.

[2] S. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE J. Select. Areas Commun.*, vol. 16, pp. 1451–1468, Oct. 1998.

[3] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Trans. Inform. Theory*, vol. 45, no. 5, pp. 1456-1467, July 1999.

[4] T. M. Duman and A. Ghrayeb, *Coding for MIMO Communication Systems*, Wiley and Sons, 2008.

[5] N. Aydin, and D.K. Ray-Chaudhuri, *Quasi Cyclic Codes Over* $\mathbb{Z}_{\not 2}$ *and Some New Binary Codes, IEEE Trans. on Information Theory*, vol. 48, number 7, pp.2065-2069, July 2002.

[6] N. Aydin and T. A. Gulliver, *Some good cyclic and quasi-twisted* $\mathbb{Z}_{\not 2}$*-linear codes,* to appear in *Ars Comb.*

[7] W. Bosma, J. J. Cannon, and C. Playoust, The Magma algebra system I: The user language, *J. Symbolic Computation*, vol. 24, pp. 235-266, 1997.

[8] D. Boucher, W. Geismann, and F. Ulmer, "Skew-Cyclic Codes*," Applicable Algebra in Engineering, Communication and Computing*, vo. 18, issue 4, july 2007, P. 379-389.

[9] D. Boucher, W. Geismann, and F. Ulmer, "Coding with Skew Polynomial Ring," Preprint.

[10] A. R. Calderbank and G. McGuire, "Construction of a $(64, 2^{37}, 12)$ code via Galois rings " *Des., Codes Cryptogr.*, vol. 10, pp. 157-165, 1997.

[11] Z. Chen, "Six New Binary Quasi-Cyclic Codes," *IEEE Trans. on Information Theory*, Vol. 40, No. 5, p. 1666-1667, September 1994.

[12] A.R. Hammons Jr., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane and P. Sole, *The* Z_4*-Linearity of Kerdock, Preparata, Goethals and Related Codes*, IEEE Trans. Inform. Theory, Vol. 40 , p. 301-319, March 1994.

[13] M. Grassl, Table of bounds on linear codes, Available at: http://www.codetables.de.

[14] P. P. Greenough and R. Hill, "Optimal Ternary Quasi-Cyclic Codes," *Designs Codes and Cryptography*, Vol. 2, p. 81-91, 1992.

[15] T. A. Gulliver, and V. K. Bhargava, "Nine Good Rate $(m-1)/pm$ Quasi-Cyclic Codes," *IEEE Trans. on Information Theory*, Vol. 38, No 4, p. 1366-1369, July 1992.

[16] T. A. Gulliver, and V. K. Bhargava, "Some Best Rate $1/p$ and Rate $(p-1)/p$ Systematic Quasi-Cyclic Codes over GF(3) and GF(4)," *IEEE Trans. on Information Theory*, Vol. 38, No 4, p. 1369-1374, July 1992.

[17] N. Jacobson, *The Theory of Rings,* Amer. Math. Soc., 1943.

[18] T. Kasami, "A Gilbert-Varshamov Bound for Quasi-Cyclic Codes of Rate 1/2," *IEEE Trans. Inform. Theory*, Vol. 20 , p. 679, 1974.

[19] K. Lally and P. Fitzpatrick, "Algebraic Structure of Quasi-Cyclic Codes," *Discr. Appl. Math.*, Vol. 111, p. 157-175, 2001.

[20] B. R. McDonald, *Finite Rings With Identity,* Marcel Dekker Inc., New York, 1974.

[21] O. Ore, "Theory of Non-commutative Polynomials," *Annals of Math.*, 34 (1933), 0. 480-508.

[22] S. Ling and P. Sole, "On the Algebraic Structure of the Quasi-Cyclic Codes I: Finite Fields," *IEEE Trans. Inform. Theory*, Vol. 47, No. 7, p. 2751-2759, 2001.

[23] G. E. Séguin and G. Drolet, "The Theory Of 1-Generator Quasi-Cyclic Codes," preprint 1990.

[24] Irfan Siap, "New Codes over GF(8) with Improved Minimum Distances," *Ars Combinatoria*, Vol 71., p. 239-247, April 2004.

[25] I. Siap, N. Aydin and D. K. Ray-Chaudhuri, "New Ternary Quasi-Cyclic Codes with Better Minimum Distances," *IEEE Information Theory*, Vol. 46 N. 4, p. 1554-1558, July 2000.

[26] K. Thomas, "Polynomial Approach to Quasi-Cyclic Codes," *Bul. Cal. Math.* Soc. 69, p.51-59, 1977.

TABLE II

Parameters and Generators of the Good skew QC Codes of index 3 and 4

Parameters	g	f_1	f_2	f_3
$[48, 11, 24]$	$1a01a^21$	$1aa^21a1aa111$	a^2a^2aa111	-
$[48, 13, 22]$	$a1a1$	$aa^2a0aa01aa101$	$aa^2a^2011a11$	-
$[48, 14, 21]$	a^2a^21	$a^2a^21aaaa^2a^20aaa01$	$1a^2aa01a^21$	-
$[48, 15, 20]$	$a1$	$0a^2a^211a0a^21aa^20aa1$	$aaa1100a^21$	-
$[54, 13, 26]$	$a1a1a1$	$a1a^201a^2a0a^2a101$	$a^2a^21a^20001$	-
$[54, 15, 24]$	$aa11$	$a^2a^2a^21aaa1aa^20a^20a1$	$a0aa^20a^2a^2a11a^21$	-
$[60, 14, 28]$	$a^20aaa01$	$111a00aa^210a0a^21$	$10a111aa^2a1a^2aa1$	-
$[60, 18, 25]$	$aa1$	$1a1a01aa^2a^2a^2aa^200a^21a^21$	$a^2a^2a011a^21aa^2101$	-
$[60, 19, 24]$	$a1$	$00a^2a^2aaaa^21a^21a^2a^2a^2aa^211$	$11aa^20a^21a11a^2a11$	-
$[72, 21, 28]$	$1aa1$	$000a1aa^21a^200aaaa^2aa^2a^2011$	$0aa1a^20a^211aa00a1$	-
$[72, 19, 30]$	a^2a1001	$1a^2a10a^2a0a^2aa01aaaaa1$	$1a^21a^2a^2a1111$	-
$[72, 15, 34]$	aaa^21a1aa^211	$a^20a0aa^2a^211a^2aa0a^21$	$01aa10a0a^2a^21$	-
$[56, 11, 29]$	$11a1$	$0a^200a01a^2$	$0a^21a1aa^21$	$1a^210aa1a^2a^2$
$[56, 12, 28]$	101	$aa^20a^2a100aa$	$a^21a^2a^2a0aa^2aa^2a^2$	a^2a0aaa^21
$[64, 13, 32]$	$a1a1$	$11aa1011a^2a^2a$	a^2000a	$10a1a^2011$
$[64, 14, 31]$	101	$0a1a01a^2a^20aa^2$	$1aaa^2a000a^2a^21a$	$aa^2a^211a^20aa$
$[64, 15, 30]$	a^21	$aa11aa^21aaaa$	$a^2a^201aa^2aa^2001$	$1a^201a1a1$
$[80, 17, 38]$	1111	$a^2a^201aaaa01a^2aa^2a$	$11a11aa00aaa^2$	$a^2111aa^21aaa1a^20a^2$
$[72, 15, 34]$	$1a^2a1$	$0a1011a^2a^20aa^21a$	$a010a0a^2a^210aa$	a^201aaa^2
$[96, 20, 44]$	10101	$11a^2a000110a^2a^2a0aa^2aa^2$	$a0111aaa^20aaa^20a^2a^2$	$a^2a^210a^210a$
$[96, 23, 41]$	a^21	$01aa^2a^21a^200aa^210aaa^2a1$	$0aaa^2a^2a^2a^2aa0a^2a00a^2a^2a$	$a^2101a^2aaa^21a01a10aa$
$[112, 24, 48]$	$1a^2a01$	$00a1a^2a^21000a^2a^21a^200a0a101$	$a^2aa^2a^2a^21aa^2a01a1a^2a^211a1$	$00a^2a00a^2a0a^21a^2101$
$[112, 22, 50]$	aaa^2a^2a11	$a^21a^2a1a0a^2a^21110a^211$	$11a1a^2a^210a11a0a^2$	$0a^20aaa^2a100a^21a^2a^2$
$[120, 21, 57]$	$aa1aa^2a^211a1$	$a^21a^2aa^2a011aa00aa1$	$00aa^2aa^21a^20a^200a^2a^20a^2a^2$	$1aa0a^2a^2100a^2$
$[120, 23, 54]$	$a010a0a^21$	$1a^211a0a00aa^2100a$	$010a110aa^200a^211a^2aa^2$	$aa0aa^200a^21a11001a1a$
$[120, 25, 52]$	$11a^2a^211$	$001a00a^2a^21a^21aaaa111$	$a^20a^2aa1a^21a^2aaa11a^2a$	$a^21a^2a00aaa^2a^21a000aaa^2a^2a^21a^2$

TABLE III

Parameters and Generators of the Good non-degenerate skew QC Codes of index up to 4

Parameters	f_1	f_2	f_3	f_4
$[40, 20, 12]$	$a^21aaa^2a^2aaaa1aa1010aaa$	$0a10a1aa11a10a011010$	$-$	-
$[30, 10, 14]$	$a^2aa00a10aa$	$000a^2a^2a1a1a^2$	$0a^21aa^20aa^21a$	-
$[36, 12, 16]$	$0aa^200a00a^2a^2a^2a$	$011a1a^21a^20aa^20$	$a^2a00a^2aaa11aa$	-
$[42, 14, 18]$	$aaaa^21a^2aa10a^2a^2aa$	$a^2a^20a^2a^2aaa100a^200$	$100a^2a^21a^2a^2a^21a^2100$	-
$[48, 16, 19]$	$a^2a^200a^2aaa0110aa1a$	$0010a^20a^2a1a0aaa^2aa$	$a^21a^21a^2101a1a^2a00a^20$	-
$[66, 22, 25]$	$a^210aa^2a^2a1a00a^200010a1a01$	$001a0a^201a^20a^2aaa0a011aa0$	$100000a^2110aaaaa^20a0a0a^2a^2$	-
$[40, 10, 20]$	$1a^2a^2aa^2a^2a^2a^2a^2a$	$0a^2110aa^2a11$	$a^2aa^2a000a^2a^21$	$a^2a0a^21a0aa0$
$[48, 12, 23]$	$01a^2a^2aa^20a^2a^2a^201$	$a^20aaa^21aaa^20a1$	$aaaa^2a^210a^2a^2000$	$0a^2aaaaa01a^2a0$
$[72, 18, 32]$	$a0a^211aa^2a^20a11a^2a^20a^200$	$1001011a1a0aa011a^20$	$010aa^20a^2a0a^2a^2a0000a0$	$aa1000a10a001a0a^21a$
$[80, 20, 35]$	$a^2a^211a1a^2a11aa01a^200aa^20$	$10a^2aa^2aa1aa^2a0a^21aaa^20a^20$	$a^21aa^20a^2a^2111a^201011aa1a$	$10a0a^200a^2a^2a^2110a^2a^211aa0$
$[96, 24, 40]$	$a0a001011a^2a^2a1111a^2a^20a000a^2$	$0a^2111000a^21000101aaa^20a^201a$	$a1aa^20a^2a^2aa^2a1a^2a^2001a^2a^2aa0a0a$	$aa01a101a^21a010a^2011a00aaa$

TABLE IV

PARAMETERS AND GENERATORS OF THE GOOD NON-DEGENERATE SKEW QC CODES OF LARGER INDICES

[60,12,31	[60,10,33]	[100,20,46]	[110,22,50]	[72,12,38]	[96,16,48]	[70,10,40]	[140,20,71]	[96,12,54]	[160,20,84]	[144,16,80]
$a^2a^2aa^2a^2a$ $1a1010$	$1a^2010a^2$ $0a^210$	$a^2a^201aa1a^2$ $001aa^2a^20a1$ $01a^21a^20$	$10aa0$ a^201a^2100 $a0a^2a0a^20$	$0a^20a^201$ aa^2a^21a0	$00aa^2aa$ $0a^20a^20a^2$ $a^20a^2a^2$	$0a^2aa^20$ $011a^2a$	$1a^21a^2aa^2$ $a^2a1a^2a^20a^2$ $aa^20a^2aa^20$	$a^2a^20aa^20$ $1000a1$	$aa^2a^2a^210$ $a^200a1a1$ $aa1a^20aa^2$	$11a10a^21$ $a^200010aa^2a$
$aa1a^2011$ aa^21aa^2	$aa1a^21a$ $00a^20$	$11a^2aa^20a$ $11a^2010a$ $a^2a^2a^2a10$	$a^2a0101a$ $a^21a^2a^21a^211$ aaa^200a^21	$a0a^2a^2a1$ a^211a1a^2	$aaa0101$ $1111a^210$ a^2a^2	$aa0100$ $101a^2$	a^2011aa^2a $0a^2a^21a^2a0$ $a01a^2aa$	$0a^2010a^2$ a^2aaaa^20	$0aa1a^200$ $1a^21aa^2aa$ a^2a0a^2aa	$a^2a^20aaa^2$ $aa^2a^2a^20a$ $11a^21$
$0a^21aa^2a^2$ $aaaa^210$	$a0a110$ a^2a^2a1	$1aa001a$ $a^210a^2a^2a0$ $1aa^2110$	$0aa^201a0a$ $a^2aaaa^21a^2$ $101a^2a^2a^21$	a^21aa^201 $00aa^20a^2$	$0111a^200$ $aa^2aa^2a^2a^2$ $0aa$	$a^2a^211a^2$ aa^21a^20	$aaa^2aa^2aa^2$ $1a1a^2a10$ aa^2aaa^20	$1aa01a$ $101aa^2a^2$	a^2100a^2a1a $a10a^2a^20a^2$ $0aaa^21$	$01a^211aa$ $1a01aa^2$ $1a^2a$
$a^20a^2a1a^2$ $a0a^2011$	$001aa$ $1aa0a$	$1a00a^2aa^2$ $100a^2a^2a0$ $1011a^2a$	$1a1a0000$ $aa^2a^2a0a^21$ $101a1a^20$	$11aa^200$ $1a^2a1aa$	$0a1a0a^21$ $a00101$ a^211	$01a^201$ a^2011a^2	$a^2aa^20a^2aa^2$ $1a^2aa010$ aa^2aa01	a^2aa^20a0 $aa^201a^2a^2$	$01a^211a1$ $1aa1a^201$ $1a^20aaa$	$110a^20aa$ $00aaa^2a$ aa^2a^2
$a100a^21$ $1aa^21aa$	$11a01a^2$ a^21a^20	$1a^21a^21a0$ $10a^20111$ a^20a^21a1	$a^210000a^20$ $a^2aaa01a^2$ $aa^2aaa^2aa^2$	$1a^2aa^2a1$ aa^2a^2a11	$00a10a^2$ $1a1a1a$ $a10a^2$	$00a^20a$ $1a^2aa^2a^2$	$1a^2010aa^2$ $1aa^2a0a^2a^2$ $a0a0a^21$	110101 $a0a^2a01$	$0a101a01$ $0a^2a^2a^2a1$ a^200100	$a010a0111$ $aa^20a^2aa^20$
-	a^210a1 $0a^2a10$	-	-	$a^2a^2a^2aa1$ $a^2a^2101a^2$	aa^21a^201 $a^2a^2a^2a^2a$ 01111	$a^2a00111a0a$	$a^21a^201a^2a$ $10a100a^2$ a^2aa10a^2	$0aa^2110$ a^2000aa	$1aa00a^21$ $a^2101a01$ $01a^2001$	$0a0a^210a^21$ $0101111a^2$
-	-	-	-	-	-	$0a^210a^2$ aa^21a^2a	$01a^2a^21a^2a$ $1a^2a^2a^2a^21$ $a^20a^2000a^2$	a^2aaa0a^2 $10a^20a^2a^2$	$1011aa^2a^21$ a^2aaaa^210 $a11a^2a^2$	$aa11a01a^2$ $11a1a^2a1a$
-	-	-	-	-	-	-	-	$a001a^2a^2$ a^2a10a0	$1a^2a0aa10$ $a^20aa111a$ $1a^20a$	$a10a^210a0$ $a^2a^21100aa$
-	-	-	-	-	-	-	-	-	-	$a^201a1aa^21$ $00aaa0a^2a$