On the Construction of Skew Quasi-Cyclic Codes

Taher Abualrub, Ali Ghrayeb, *Senior Member, IEEE*, 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 noncommutative ring called the skew polynomial ring $F[x;\theta]$. 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.**

***Index Terms*—New codes, quasi-cyclic codes, skew fields.**

I. Introduction

A significant portion of the work on error correcting codes for over the last 60 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., [1], [2], [6], and [9]) 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 noncommutative rings. Research on this topic is very recent and interesting. Boucher *et al.* generalized in [4] and [5] the notion of cyclic codes by using generator polynomials in a noncommutative 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 [4].

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 [7], [15], [16], [19], [20], [23]. Many of the best known and optimal linear codes that have been constructed so far are examples of QC codes (e.g., [7], [11]–[13], and [22]).

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. In fact, we have performed a search in the class of skew QC codes over $GF(4)$, and obtained 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. Our focus in this paper has been on the one-generator skew QC codes and their properties since this class of codes share many properties of QC codes.

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, and show that the parity-check polynomial of a skew QC code is unique up to similarity. Section V includes our search results. Section VI concludes the paper.

II. 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 $q=p^{tm}$. Since the automorphism group of $F/\mathbb{Z}_p$ is cyclic, generated by the Frobenious automorphism $z \to z^p$, we have $\theta(b) = b^{p^t}$ 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 the Frobenius automorphism

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

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: Let θ be defined as above. The skew polynomial $F[x;\theta]$ is the set of polynomials over F where addition of the

Manuscript received September 15, 2008; revised August 11, 2009. Current version published April 21, 2010. The work of T. Abualrub and A. Ghrayeb was supported in part by the Natural Sciences and Engineering Research Council of Canada (NSERC) while T. Abualrub was on sabbatical in the Department of Electrical and Computer Engineering, Concordia University, Montreal, QC, Canada.

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, QC H3G 1M8, Canada (e-mail: aghrayeb@ece.concordia.ca) 514 848 2424 x 412.

N. Aydin is with the Department of Mathematics, Kenyon College, Gambier, OH 43022 USA (e-mail: aydinn@kenyon.edu).

I. Siap is with the Department of Mathematics, Yıldız Technical University, Istanbul, Turkey (e-mail: isiap@yildiz.edu.tr).

Communicated by T. Etzion, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2010.2044062

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 Example 1, 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: [17] The set $F[x;\theta]$ with respect to addition and multiplication defined above forms a noncommutative 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 in [18], and a complete treatment of this ring can be found in [14] and [17].

Theorem 2: [17] (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: [14] $F[x;\theta]$ is a noncommutative principal left (right) ideal ring. Moreover, any two sided ideal must be generated by

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

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 $F[x;\theta]$ if and only if $m|s$.

Definition 2: For any ring R, define the center of R to be the set

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

Lemma 1: $(x^s - 1) \in Z(F[x;\theta])$ for $m|s$.

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: [5] If $g \cdot h \in Z(F[x;\theta])$, then $g \cdot h = h \cdot g$.

Definition 3: 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 exists a polynomial g such that

$$f = gd.$$

Now suppose $m|s$ and consider $(x^s - 1)$. By Lemma 1, $(x^s - 1) \in Z(F[x;\theta])$. If f is a left divisor of $(x^s - 1)$, then we have

$$(x^s - 1) = fg = gf \quad (\text{by Lemma 2}).$$

Thus, if f is a left divisor of $(x^s - 1)$, 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 4: 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;
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 $\mathrm{lcrm}[a,b]$ and the least common left multiple of a and b, $\mathrm{lclm}[a,b]$

Theorem 4: [18] gcrd, gcld, lcrm, and lclm can be calculated using the left and right division algorithms.

Remark 1: By a principal ideal domain, we mean any ring (commutative or noncommutative) with no (left or right) zero divisors and all left (right) ideals are principle. The ring $F[x;\theta]$ is an example of a principal ideal domain (see [8]).

III. Skew Quasi-Cyclic Codes

Definition 5: 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 (or skew l-QC code) if:

1) C is a subspace of F^n;
2) if

$$e = \begin{pmatrix} e_{0,0}, e_{0,1}, \ldots, e_{0,l-1}, e_{1,0}, e_{1,1}, \ldots, e_{1,l-1}, \ldots \\ e_{s-1,0}, e_{s-1,1}, \ldots, e_{s-1,l-1} \end{pmatrix}$$

is a codeword in C, then

$$T_{\theta,s,l}(e) = \begin{pmatrix} \theta(e_{s-1,0}), \theta(e_{s-1,1}), \ldots, \theta(e_{s-1,l-1}) \\ \theta(e_{0,0}), \ldots, \theta(e_{0,l-1}), \ldots \\ \theta(e_{s-2,0}), \ldots, \theta(e_{s-2,l-1}) \end{pmatrix}$$

is also a codeword 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 [4], Boucher *et al.* 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 if and only if $m|s$. 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.

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

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

where

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

Then

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

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

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

Then, $\phi(c) = (g_0(x), g_1(x), \ldots, g_{l-1}(x)) \in D$, 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

$$\begin{aligned} \phi(T_{\theta,s,l}(c)) &= x\,(g_0(x), g_1(x), \ldots g_{l-1}(x)) \\ &= (xg_0(x), xg_1(x), \ldots, xg_{l-1}(x)) \in D. \end{aligned}$$

Hence, $T_{\theta,s,l}(c) \in C$. Therefore, C is a skew quasi-cyclic code C. ■

From now on, we concentrate on one-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

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

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

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

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 6: 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

$$g(x) = gcld\,(\,p_1(x)g_1(x), \ldots, p_l(x)g_l(x), x^s - 1\,)$$

is called the generator polynomial of C.

Definition 7: The monic polynomial $h(x)$ of minimal degree such that

$$h(x)\,(p_1(x)g_1(x), \ldots, p_l(x)g_l(x)) = (0, 0, \ldots, 0)$$

is called the parity-check polynomial of C

Theorem 7: Suppose $d(x) = gcrd(f, g)$, then there are 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 $g(x) = r_2(x)h(x)$. However, $d(x) = gcrd(f, g)$ 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 $g(x) = gcld\,(p_1(x)g_1(x), \ldots, p_l(x)g_l(x), x^s - 1)$, $x^s - 1 = g(x)k(x)$ for some polynomial $k(x)$. Note that by Lemma 2, we have $x^s - 1 = g(x)k(x) = k(x)g(x)$. We also have $p_i(x)g_i(x) = g(x)\alpha_i(x)$ where $\alpha_i(x)$ are polynomials in R_s for all $i = 1, \ldots, l$. Hence, we have

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

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

$$p_1(x)g_1(x)a_1(x) + \cdots + (x^s - 1)a_{l+1}(x) = g(x).$$

Therefore

$$\begin{aligned} &h(x)(p_1(x)g_1(x)a_1(x) + \cdots + (x^s - 1)a_{l+1}(x)) \\ &\qquad = h(x)g(x) = 0. \end{aligned}$$

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

Definition 8: Let $C = \langle G(x) \rangle$ be a skew QC code. The anihilator 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

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

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 codes C_1 with parity-check polynomial h_1 and C_2 with parity-check polynomial h_2 are isomorphic if and only if h_1 and h_2 are similar polynomials.

Definition 9: Two nonzero elements a and b in a principal ideal domain R are called right similar if there is a $u \in R$ such that

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

Left similar elements can be defined similarly.

Note that if there is a $u \in R$ such that

$$gcld(u,b) = 1 \quad \text{and} \quad ua = lcrm[u,b]$$

then we have $m = ua = bc$ for some $c \in R$. If $gcld(c,a) > 1$, then $m = ua \neq lcrm[u,b]$. Hence, $gcld(c,a) = 1$. The mapping

$$\Omega : R/Rc \to R/Ra \quad \text{defined by} \quad \Omega(e + Rc) = eb + Ra$$

is a module homomorphism. We have

$$\Omega(c + Rc) = \Omega(Rc) = cb + Ra \in Ra$$

which implies $cb = ak$ for some $k \in R$. Since $gcld(c,a) = 1$ then we must have $cb = lcrm[c,a]$. Therefore, the definition of right similar (or left similar) is symmetric (see [8, pp. 26–27]).

Example 3: Let F be any field of characteristic p. We will show when two linear polynomials $p_1(x) = x - \alpha$ and $p_2(x) = x - \beta$ 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, $lcrm[u, p_2] = cp_1$ if and only if

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

Hence

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

This implies that

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

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

If we consider the field $GF(2^2)$ and the Frobenius 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

$$gcld(u,b) = 1 \quad \text{and} \quad m = ua = lcrm[u,b].$$

Suppose $gcrd(c,a) = d \neq 1$, 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, $gcrd(c,a) = 1$. Since

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

then $m = ua = bc$ for some $c \in R$. This implies that m is a common right multiple of u and b. Now suppose $v = lclm[c,a]$. Then $v = \beta_1 c = \beta_2 a$ for some $\beta_1, \beta_2 \in R$. Since m is a common right multiple of u and b, $m = \beta_3 v$ for some $\beta_3 \in R$. Hence

$$ua = m = \beta_3 v = \beta_3\beta_2 a$$
$$(u - \beta_3\beta_2)\, a = 0.$$

Since a is not a (right or a left) zero divisor, $u = \beta_3\beta_2$. Similarly, we have

$$bc = m = \beta_3 v = \beta_3\beta_1 c.$$

Again, we will have $b = \beta_3\beta_1$. This implies that β_3 is a left divisor of u and b. Since $gcld(u,b) = 1$, we must have $m = lclm[c,a]$. ■

From now on, 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 if and only if 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 $C_1 \cong C_2$ if and only if $h_1(x)$ is similar to $h_2(x)$.

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

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

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

$$ca-1=l(x)h_2(x)$$

or

$$ca-l(x)h_2(x)=1.$$

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, $\alpha_1=t_1h_1(x)$ and $k=t_1h_1(x)a$. However, we have $h_1a=r_2h_2=m$. Therefore

$$lclm[a,h_2(x)]=h_1a. \tag{3}$$

From (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

$$gcrd(u,h_2)=1 \text{ and}$$
$$lclm[u,h_2]=h_1u.$$

Define

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

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 $c_1u+c_2h_2=1$ for some c_1 and $c_2\in R_s$. This implies that

$$\Psi(c_1+(h_1(x))=c_1u+(h_2(x))=1+(h_2(x)).$$

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 $lclm[u,h_2]=h_1u$, we have

$$su=t_1h_1u.$$

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

$$s=q_1h_1+r_1 \text{ where } \deg r_1<\deg h_1.$$

This implies that

$$su=q_1h_1u+r_1u\Rightarrow r_1u\in(h_2(x)).$$

Since $lclm[u,h_2]=h_1u$, $r_1u=t_2h_1u\in(h_1(x))$. If $r_1\in(h_1(x))$ then

$$s=q_1h_1+r_1\in(h_1(x))$$

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

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

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 i.

The smallest nonzero 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 [10]. The computer algebra system Magma also has such a database [3]. 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

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	$a^2a1a^210a^20a0a^2a^2a^20a^211$
$[44,12,20]$	$11111aa11a^21$	$a000a^2a^2aa0a^2a1$
$[48,11,24]$	$1aa^21a0a^2a100101$	$aaaaa^21a10a1$
$[48,12,23]$	$a110a^21a^2a11a^2a^21$	$1a^20110010a11$
$[48,13,22]$	$a^2aa^200a100111$	$0001a0a^2a^2a^2aaa^21$
$[48,14,21]$	$11a^2a^2a10a^2101$	$1a11010a1a^2aa11$
$[48,15,20]$	$a^2a01a1a^2111$	$1aa^2a^2a^2a^2a^2a0aa1a11$
$[48,16,19]$	$a00101a^2a1$	$a^2a0a1a1aa1aa^2aa^2a^21$
$[52,13,24]$	$a^2a^2aa^210a^21a11aa1$	$aa^211aa^21a^2a^2a^2a^211$
$[60,11,32]$	$aaa^2a^2a^2a^211aa110000aa11$	$aa^2aa^20aa^2a1a^21$
$[60,14,28]$	$11a^2a11a^2a^2a^2a^2aa^2a^2a^2a^2a1$	$a^20a^2a0a110a^21011$

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	$a^2a^21aaaa^2a^20aaa01$	$1a^2aa01a^21$	-
$[48,15,20]$	$a1$	$0a^2a^211a0a^21aa^20aa1$	$aaa1100a^21$	-
$[54,13,26]$	$a1a1a1$	$a1a^201a^2a0a^2a101$	$a^2a^21a^20001$	-
$[54,15,24]$	$aa11$	$a^2a^2a^21aaa1aa^20a^20a1$	$a0aa^20a^2a^2a11a^21$	-
$[60,14,28]$	$a^20aaa01$	$111a00aa^210a0a^21$	$10a111aa^2a1a^2aa1$	-
$[60,18,25]$	$aa1$	$1a1a01aa^2a^2a^2aa^200a^21a^21$	$a^2a^2a011a^21aa^2101$	-
$[60,19,24]$	$a1$	$00a^2a^2aaaa^21a^21a^2a^2a^2aa^2111$	$1aa^20a^21a11a^2a11$	-
$[72,21,28]$	$1aa1$	$000a1aa^21a^200aaaa^2aa^2a^2011$	$0aa1a^20a^211aa00a1$	-
$[72,19,30]$	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	$a^21a^2a1a0a^2a^21110a^211$	$11a1a^2a^210a11a0a^2$	$0a^20aaa^2a100a^21a^2a^2$
$[120,21,57]$	$aa1aa^2a^211a1$	$a^21a^2aa^2a011aa00aa1$	$00aa^2aa^21a^20a^200a^2a^20a^2a^2$	$1aa0a^2a^2100a^2$
$[120,23,54]$	$a010a0a^21$	$1a^211a0a00aa^2100a$	$010a110aa^200a^211a^2aa^2$	$aa0aa^200a^21a11001a1a$
$[120,25,52]$	$11a^2a^211$	$001a00a^2a^21a^21aaaa111$	$a^20a^2aa1a^21a^2aaa11a^2a$	$a^21a^2a00aaa^2a^21a000$ $aaa^2a^2a^21a^2$

of QC and QT codes (e.g., [2], [11], [12], and [22]). 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 [10]. 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 deserves further attention.

In view of the previous section and the findings obtained therein, 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 $(g,f_1g,\ldots,f_{l-1}g)$ 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

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
$[40, 20, 12]$	$a^21aaa^2a^2aaaa1aa1010aaa$	$0a10a1aa11a10a011010$	$-$	-
$[30, 10, 14]$	$a^2aa00a10aa$	$000a^2a^2a1a1a^2$	$0a^21aa^20aa^21a$	-
$[36, 12, 16]$	$0aa^200a00a^2a^2a^2a$	$011a1a^21a^20aa^20$	$a^2a00a^2aaa11aa$	-
$[42, 14, 18]$	$aaaa^21a^2aa10a^2a^2aa$	$a^2a^20a^2a^2aaa100a^200$	$100a^2a^21a^2a^2a^21a^2100$	-
$[48, 16, 19]$	$a^2a^200a^2aaa0110aa1a$	$0010a^20a^2a1a0aaa^2aa$	$a^21a^21a^2101a1a^2a00a^20$	-
$[66, 22, 25]$	$a^210aa^2a^2a1a00$ $a^200010a1a01$	$001a0a^201a^20a^2aaa$ $0a011aa0$	$100000a^2110aaaaa^2$ $0a0a0a^2a^2$	-
$[40, 10, 20]$	$1a^2a^2aa^2a^2a^2a^2a^2a$	$0a^2110aa^2a11$	$a^2aa^2a000a^2a^21$	$a^2a0a^21a0aa0$
$[48, 12, 23]$	$01a^2a^2aa^20a^2a^2a^201$	$a^20aaa^21aaa^20a1$	$aaaa^2a^210a^2a^2000$	$0a^2aaaaa01a^2a0$
$[72, 18, 32]$	$a0a^211aa^2a^20a11a^2a^20a^200$	$1001011a1a0aa011a^20$	$010aa^20a^2a0a^2a^2a0000a0$	$aa1000a10a001a0a^21a$
$[80, 20, 35]$	$a^2a^211a1a^2a11aa01a^200aa^20$	$10a^2aa^2aa1aa^2a0a^21aaa^20a^20$	$a^21aa^20a^2a^2111a^201011aa1a$	$10a0a^200a^2a^2a^2110a^2$ a^211aa0
$[96, 24, 40]$	$a0a001011a^2a^2$ $a1111a^2a^20a000a^2$	$0a^2111000a^21000$ $101aaa^20a^201a$	$a1aa^20a^2a^2aa^2a1a^2a^2001a^2$ $a^2aa0a0a$	$aa01a101a^21a010$ $a^2011a00aaa$

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	$1a^2a0aa10$ $a^20aa111a$ $1a^20a$	$a10a^210a0$ $a^2a^21100aa$
-	-	-	-	-	-	-	-	-	-	$a^201a1aa^21$ $00aaa0a^2a$

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.

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

$$\begin{aligned} h = x^{21} + ax^{20} + x^{19} + a^2x^{18} + x^{16} + x^{13} + ax^{12} \\ + x^{11} + a^2x^{10} + x^8 + x^5 + ax^4 + x^3 + a^2x^2 + 1. \end{aligned}$$

Now let

$$\begin{aligned} f_1 = x^{20} + x^{19} + x^{17} + a^2x^{15} + ax^{14} + a^2x^{13} + a^2x^{12} \\ + a^2x^{11} + x^{10} + a^2x^9 + x^8 + x^7 + ax^6 + a^2x^5 + ax^2 + 1 \end{aligned}$$

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_1g, f_2g). It is a [72, 21, 29] code and, therefore, better than the previously best known code with parameters [72, 21, 28].

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 nondegenerate skew QC codes (since the codes of the form $(f_1g, f_2g, \ldots, f_lg)$ 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 $a001aa^{2}1$ represents the polynomial $x^6 + a^2x^5 + ax^4 + x^3 + a$.

Example 7: A [48, 16, 20]-quasi-cyclic linear code generated by $f_1 = 0a^{2}a^{2}a0a^{2}10a^{2}0a11a^{2}a^{2}1$, $f_2 = 100a^{2}0a^{2}a^{2}aa^{2}1a^{2}1a^{2}0a^{2}0$, $f_3 = a^{2}aa0a^{2}0aa1a^{2}aaa0aa$.

Example 8: A [96, 16, 49]-quasi-cyclic linear code generated by $f_1 = 0a^{2}a^{2}1aa^{2}0aa100a^{2}a0a$, $f_2 = 1a^{2}a^{2}aa00a^{2}a^{2}11a^{2}1a0a^{2}$, $f_3 = 0a^{2}a^{2}00aaaa^{2}1a1a^{2}0aa^{2}$, $f_4 = a0a^{2}00a0a^{2}aa0aa1a^{2}1$, $f_5 = a^{2}011011a^{2}1a1a^{2}a111$, $f_6 = a100a^{2}a^{2}a^{2}a1a001aa^{2}a^{2}$.

Example 9: A [100, 20, 47]- quasi-cyclic linear code generated by

$$\begin{aligned} f_1 &= a00a^{2}a^{2}001a^{2}a^{2}a^{2}011a1a^{2}a11 \\ f_2 &= 01a^{2}0a1a01a^{2}1a1a01001a^{2} \\ f_3 &= a1aa1001aa^{2}0000a^{2}a1a^{2}a^{2}1 \\ f_4 &= 1a1aa11a^{2}a^{2}aa^{2}0a^{2}a0010a^{2}1 \\ f_5 &= a^{2}0111aa^{2}1a^{2}aa^{2}a^{2}a0a^{2}01a11. \end{aligned}$$

Example 10: A [140, 20, 72]-quasi-cyclic linear code generated by

$$\begin{aligned} f_1 &= 1a^{2}a^{2}aa1a10aa^{2}10a01a^{2}a^{2}01 \\ f_2 &= aa0a^{2}01a^{2}aa0a0a1aa1a10 \\ f_3 &= a^{2}a^{2}a^{2}1aa^{2}a1a0aaa^{2}a^{2}0aa0aa \\ f_4 &= 10001aaa^{2}0a010a^{2}a^{2}a0010 \\ f_5 &= a11001a1a^{2}a^{2}1aa^{2}10aa^{2}1a^{2}a \\ f_6 &= a^{2}0a^{2}10a^{2}11a^{2}a^{2}a^{2}1a^{2}a^{2}0a^{2}0110 \\ f_7 &= a^{2}1011000a^{2}a^{2}01a^{2}01a^{2}aa^{2}a^{2}1. \end{aligned}$$

Example 11: A [110, 22, 51]-quasi-cyclic linear code generated by

$$\begin{aligned} f_1 &= 1a^{2}010aa0a^{2}01a^{2}100a0a^{2}a0a^{2}0 \\ f_2 &= a^{2}a0101aa^{2}1a^{2}a^{2}1a^{2}11aaa^{2}00a^{2}1 \\ f_3 &= 00a^{2}a00a^{2}01a^{2}aa100a0a^{2}a11a^{2} \\ f_4 &= 01a01010a^{2}11a01100a^{2}a^{2}a1a \\ f_5 &= a^{2}0a0a^{2}a^{2}a00a^{2}a10a0aaa1a^{2}1a. \end{aligned}$$

We summarize the rest of the results of our search that yielded good codes in Tables I–IV.

VI. Conclusion

In this paper, we study the structure of 1-generator skew QC codes in the noncommutative 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 yield to 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.

Acknowledgment

The authors would like to thank the reviewers for their valuable comments and remarks that helped a lot in improving the presentation of the paper.

References

[1] N. Aydin and D. K. Ray-Chaudhuri, "Quasi cyclic codes over $\mathbb{Z}_4$ and some new binary codes," *IEEE Trans. Inf. Theory*, vol. 48, no. 7, pp. 2065–2069, Jul. 2002.

[2] N. Aydin and T. A. Gulliver, "Some good cyclic and quasi-twisted $\mathbb{Z}_4$-linear codes," *Ars Comb.*, to be published.

[3] W. Bosma, J. J. Cannon, and C. Playoust, "The Magma algebra system I: The user language," *J. Symbol. Comput.*, vol. 24, pp. 235–266, 1997.

[4] D. Boucher, W. Geismann, and F. Ulmer, "Skew-cyclic codes," *Appl. Algebra Eng., Commun., Comput.*, vol. 18, no. 4, pp. 379–389, Jul. 2007.

[5] D. Boucher, W. Geismann, and F. Ulmer, "Coding with skew polynomial ring,", to be published.

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

[7] Z. Chen, "Six new binary quasi-cyclic codes," *IEEE Trans. Inf. Theory*, vol. 40, no. 5, pp. 1666–1667, Sep. 1994.

[8] P. M. Cohn*, Skew Fields: Theory of General Division Rings*. Cambridge, U.K.: Cambridge Univ. Press, 1995.

[9] 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. Inf. Theory*, vol. 40, no. 2, pp. 301–319, Mar. 1994.

[10] M. Grassl, Table of Bounds on Linear Codes [Online]. Available: http://www.codetables.de

[11] P. P. Greenough and R. Hill, "Optimal ternary quasi-cyclic codes," *Designs Codes Cryptogr.*, vol. 2, pp. 81–91, 1992.

[12] T. A. Gulliver and V. K. Bhargava, "Nine good rate $(m-1)/pm$ quasi-cyclic codes," *IEEE Trans. Inf. Theory*, vol. 38, no. 4, pp. 1366–1369, Jul. 1992.

[13] T. A. Gulliver and V. K. Bhargava, "Some best rate $1/p$ and rate $(p-1)/p$ systematic quasi-cyclic codes over $\mathrm{GF}(3)$ and $\mathrm{GF}(4)$," *IEEE Trans. Inf. Theory*, vol. 38, no. 4, pp. 1369–1374, Jul. 1992.

[14] N. Jacobson, "The theory of rings," *Amer. Math. Soc.*, 1943.

[15] T. Kasami, "A Gilbert-Varshamov bound for quasi-cyclic codes of rate 1/2," *IEEE Trans. Inf. Theory*, vol. 20, no. 5, p. 679, Sep. 1974.

[16] K. Lally and P. Fitzpatrick, "Algebraic structure of quasi-cyclic codes," *Discr. Appl. Math.*, vol. 111, pp. 157–175, 2001.

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

[18] O. Ore, "Theory of non-commutative polynomials," *Ann. Math.*, vol. 34, pp. 480–508, 1933.

[19] S. Ling and P. Sole, "On the algebraic structure of the quasi-cyclic codes I: Finite fields," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 2751–2759, Jul. 2001.

[20] G. E. Séguin and G. Drolet, "The theory of 1-generator quasi-cyclic codes,", to be published.

[21] I. Siap, "New codes over $\mathrm{GF}(8)$ with improved minimum distances," *Ars Combin.*, vol. 71, pp. 239–247, Apr. 2004.

[22] I. Siap, N. Aydin, and D. K. Ray-Chaudhuri, "New ternary quasi-cyclic codes with better minimum distances," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1554–1558, Jul. 2000.

[23] K. Thomas, "Polynomial approach to quasi-cyclic codes," *Bull. Cal. Math. Soc.*, vol. 69, pp. 51–59, 1977.

Taher Abualrub received the Ph.D. degree in mathematics from The University of Iowa, Iowa City, IA, in May 1998.

He is currently an Associate Professor of mathematics at the American University of Sharjah, UAE. In 1998, he joined The American University of Sharjah as an Assistant Professor in the Mathematics and Statistics Department, where he became an Associate Professor of mathematics in June 2004. His research interests include error correcting codes, DNA computing, wavelet theory, and control theory. He has published over 18 refereed journal papers and more than 20 conference proceeding papers.

Ali Ghrayeb (S'97–M'00–SM'06) received the Ph.D. degree in electrical engineering from the University of Arizona, Tucson, in 2000.

He is currently an Associate Professor with the Department of Electrical and Computer Engineering, Concordia University, Montreal, QC, Canada. He holds a Concordia University Research Chair in Wireless Communications. He is the coauthor of the book *Coding for MIMO Communication Systems* (Wiley, 2008). His research interests include wireless and mobile communications, information theory and coding, MIMO systems, wireless cooperative networks, and CDMA/WCDMA systems.

Dr. Ghrayeb has instructed/coinstructed technical tutorials at several major IEEE conferences. He serves as an Associate Editor of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY and the IEEE TRANSACTIONS ON SIGNAL PROCESSING. He served as an Associate Editor of the Wiley *Wireless Communications and Mobile Computing Journal* from 2004–2008.

Nuh Aydin received the Ph.D. degree from The Ohio State University in 2002.

He is currently with Kenyon College, Gambier, OH. His primary research area is algebraic coding theory. He is also interested in theoretical computer science and pedagogy. He introduces coding theory to undergraduate students at a liberal arts college and coauthors papers with them.

Irfan Siap received the B.Sc. degree from Istanbul University, Turkey, in 1992, and the M.Sc. and Ph.D. degrees from The Ohio State University in mathematics in 1993 and 1999, respectively.

He has taught and conducted research at several universities: The Ohio State University, Sakarya University, Gaziantep University, and Adiyaman University. Currently, he is with Department of Mathematics at Yildiz Technical University, Istanbul, Turkey, where he holds the position of Professor of Mathematics. His main research focus is on algebraic coding theory. He has published over 25 referred articles in well-known international journals and also presented his work at many international conferences.

Dr. Siap has refereed many research articles submitted to distinguished journals and conferences. He currently serves as an Associate Editor for the *Journal of The Franklin Institute*.