TWMS J. Pure Appl. Math. V.9, N.2, 2018, pp.123-134

SKEW GENERALIZED QUASI-CYCLIC CODES

TAHER ABUALRUB[1], MARTIANUS FREDERIC EZERMAN[2]
PADMAPANI SENEVIRATNE[3], PATRICK SOLÉ[4]

Abstract. This article discusses skew generalized quasi-cyclic codes over any finite field $\mathbb{F}$ with Galois automorphism θ. This is a generalization of both quasi-cyclic codes and skew polynomial codes. These codes have an added advantage over quasi-cyclic codes since their lengths do not have to be multiples of the index.

After a brief description of the skew polynomial ring $\mathbb{F}[x;\theta]$, we show that a skew generalized quasi-cyclic code C is a left submodule of $R_1 \times R_2 \times \ldots \times R_\ell$, where $R_i \triangleq \mathbb{F}[x;\theta]/(x^{m_i}-1)$, with $|\langle\theta\rangle| = m$ and m divides m_i for all $i \in \{1,\ldots,\ell\}$. This description provides a direct construction of many codes with best-known parameters over $GF(4)$. As a byproduct, some good asymmetric quantum codes detecting single bit-flip error can be derived from the constructed codes.

Keywords: generalized skew quasi-cyclic codes, skew polynomial codes, quasi-cyclic codes, quantum CSS codes.

AMS Subject Classification: 94B05, 81P70, 16S36.

1. Introduction

One of the most important problems in error-correcting codes is to construct codes with good parameters, such as having a large minimum Hamming distance for a given dimension. Such a code is capable of detecting and correcting a good number of errors. One class of codes that has been studied in the literature is quasi-cyclic (QC) codes. QC codes of index ℓ over a finite field $\mathbb{F}$ are linear codes where the cyclic shift of any codeword by ℓ positions is another codeword. QC codes of index $\ell = 1$ are the well-known cyclic codes. The importance of the family of QC codes has been shown in, *e.g.*, [6], [18], [19], [20], [24], and [28]. Many of the optimal and currently best-known linear codes are QC codes as established in, *e.g.*, [6], [12], [13], [14], and [26].

Some recent works in the literature, such as [1], [3], [4], [10], and [25], focussed on the construction of error-correcting codes using non-commutative rings. D. Boucher *et al.* in [3] and in [4], generalized the notion of cyclic codes by using generator polynomials in a non-commutative polynomial ring called skew polynomial ring. They gave some examples of skew cyclic codes with minimum distances as good as the best-known comparable linear codes of the same lengths and dimensions. Extending the non-commutative framework to quasi-cyclic codes, Abualrub *et al.* derived many new optimal linear codes from skew QC codes in [1].

Siap and Kulhan [27] introduced the concept of generalized quasi-cyclic (GQC) codes over finite fields. These codes are generalization of QC codes. Esmaili and Yari [7] gave examples of

[1]Department of Mathematics and Statistics, American University of Sharjah, Sharjah, UAE
[2]School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore
[3]Department of Mathematics, Texas A&M University-Commerce, TX, USA
[4] CNRS/LAGA, University of Paris 8, 93 526 Saint-Denis, France
e-mail: abualrub@aus.edu, fredezerman@ntu.edu.sg, padmapani.seneviratne@tamuc.edu, sole@telecom-paristech.fr
Manuscript received March 2016.

GQC codes with parameters equalling those of the then best-known linear codes. J. Gao *et al.* in [10] studied skew GQC codes using the Chinese Remainder Theorem.

In this work we study skew GQC codes and give a direct approach to the construction of these codes. We will show that both classical and quantum codes with good parameters can be derived from them. The paper is organized as follows. After this introduction, we give a preliminary introduction on the skew polynomial ring $\mathbb{F}[x;\theta]$ in Section 2. Properties of skew GQC codes and their duals over finite fields are discussed in Section 2. Section 3 provides our search results for good classical and quantum codes that can be derived from skew GQC codes. Section 4 wraps the paper up with conclusions and open problems. A last section is dedicated to Acknowledgements.

2. The skew polynomial ring $\mathbb{F}[x,\theta]$

To make this work self-contained, we begin with a brief introduction on skew polynomial rings over finite fields and their properties.

Let $\mathbb{F}$ be any finite field of characteristic p. Let θ be an automorphism of $\mathbb{F}$ with $|\langle\theta\rangle| = m$. Let $\mathbb{K}$ be the subfield of $\mathbb{F}$ fixed by θ. Then, $[\mathbb{F} : \mathbb{K}] = m$, $\mathbb{K} = GF(p^t)$, and $\mathbb{F} = GF(q = p^{tm})$. Since θ fixes $\mathbb{K}$, $\theta(a) = a^{p^t}$ for all $a \in \mathbb{F}$.

Definition 2.1. *Keeping the above notations, a skew polynomial set $\mathbb{F}[x;\theta]$ is given by*

$$\mathbb{F}[x;\theta] = \{f(x) = a_0 + a_1x + \ldots + a_nx^n \text{ with } a_i \in \mathbb{F} \text{ for all } i \in \{0,1,\ldots,n\}\}.$$

Addition is defined in the usual manner, while multiplication is associative, distributive on the addition, and follows the rule

$$(ax^i)\ (bx^j) = a\ \theta^i(b)\ x^{i+j}.$$

Theorem 2.1. [21] *The set $\mathbb{F}[x;\theta]$ with respect to addition and multiplication in Definition 2.1. forms a non-commutative ring called a skew polynomial ring.*

Some facts are straightforward. The ring $\mathbb{F}[x;\theta]$ has no nonzero zero-divisors. Its units are the units of $\mathbb{F}$. Due to how the operations are defined, $\deg(f(x)+g(x)) \leq \max\{\deg(f(x)), \deg(g(x))\}$ and $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$. The ring $\mathbb{F}[x;\theta]$ was introduced by Ore [22] in 1933, and a complete treatment of this ring can be found in [17] and in [21].

Theorem 2.2. [21, The Right Division Algoritheorem]. *For $f(x) \neq 0$ and $g(x)$ in $\mathbb{F}[x;\theta]$ there exist unique polynomials $q(x)$ and $r(x)$ in $\mathbb{F}[x;\theta]$ such that*

$$g(x) = q(x)f(x) + r(x) \text{ with } \deg(r(x)) < \deg(f(x)).$$

The above result is called *division on the right by $f(x)$*. A similar result holds regarding *division on the left by $f(x)$*. Applying the division algoritheorem one can prove the following result.

Theorem 2.3. [17] *The ring $\mathbb{F}[x;\theta]$ is a noncommutative principal left and right ideal ring. Any two-sided ideal must be generated by*

$$f(x) = (a_0 + a_1x^m + a_2x^{2m} + \ldots + a_rx^{rm})\ x^e, \text{ where } |\langle\theta\rangle| = m.$$

In particular, the ideal generated by $(x^s - 1)$ with $m \mid s$ is a two-sided ideal.

The next two results state some properties of the center $Z(\mathbb{F}[x;\theta])$ of $\mathbb{F}[x;\theta]$.

Lemma 2.1. [1, Lemma 1] *If $m \mid s$, then $Z(\mathbb{F}[x;\theta])$ contains (x^s-1).*

Lemma 2.2. [5, Lemma 7] *If $g(x)\ h(x) \in Z(\mathbb{F}[x;\theta])$, then $g(x)h(x) = h(x)g(x)$.*

From Lemmas 2 and 2, we may conclude that the factors of x^s-1 commute. Thus, if $f(x)$ is a left divisor of x^s-1, then it is also a right divisor. This fact helps in reducing the complexity of factoring x^s-1 in $\mathbb{F}[x;\theta]$. Henceforth, we say divisors or factors of x^s-1 without specifying left or right.

Definition 2.2. *We say that $f(x)$ is a* right multiple *of $h(x)$ if there exists $g(x)$ such that $f(x) = h(x)\ g(x)$. When this is the case, $h(x)$ is called a left divisor of $f(x)$.*

Definition 2.3. *A monic polynomial $h(x)$ is the* greatest common left divisor *of $a(x)$ and $b(x)$, denoted by* $\mathrm{gcld}(a(x),b(x))$, *if $h(x)$ is a left divisor of* both *$a(x)$ and $b(x)$ and if, for any other left divisor $e(x)$ of $a(x)$ and $b(x)$, there exists $k(x)$ satisfying $h(x) = e(x)\ k(x)$.*

Since θ is an automorphism of $\mathbb{F}$, then the *greatest common right divisor* gcrd of $a(x)$ and $b(x)$ is a monic polynomial defined analogously. The *least common left multiple*, denoted by lclm, and *least common right multiple*, denoted by lcrm, are well-defined in $\mathbb{F}[x;\theta]$.

3. Skew generalized quasi cyclic codes

In this section we define skew generalized quasi-cyclic (GQC) codes and establish their most important properties.

Definition 3.1. *Let $\mathbb{F}$ be a finite field of characteristic p with $q = p^{mt}$ elements, and let θ be an automorphism of $\mathbb{F}$ with $|\langle\theta\rangle| = m$. Let $(a_1, a_2, \ldots, a_n) \in \mathbb{F}^n$. Define the function*

$$\mathrm{T} : \mathbb{F}^n \to \mathbb{F}^n \text{ by } (a_1, a_2, \ldots, a_n) \mapsto (\theta(a_n), \theta(a_1), \ldots, \theta(a_{n-1})). \tag{1}$$

Let $m_1, m_2, \ldots, m_\ell$ be positive integers with $m \mid m_i$ for all $i \in \{1, 2, \ldots, \ell\}$ and $n := \sum_{i=1}^{\ell} m_i$. A subset C of $\mathbb{F}^{m_1} \times \mathbb{F}^{m_2} \times \ldots \times \mathbb{F}^{m_\ell}$ is called a skew generalized quasi-cyclic code *of length n and index ℓ (or a skew ℓ-GQC code) if both of the following conditions hold.*

1. *The code C is a subspace of $\mathbb{F}^{m_1} \times \mathbb{F}^{m_2} \times \ldots \times \mathbb{F}^{m_\ell}$.*
2. *Let $\mathbf{v}_j \triangleq (v_{j,1}, v_{j,2}, \ldots, v_{j,m_j}) \in \mathbb{F}^{m_j}$ for all $j \in \{1, \ldots, \ell\}$. If $\mathbf{v} = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_\ell) \in C$, then $\mathrm{T}(\mathbf{v}) = (\mathrm{T}(\mathbf{v}_1), \mathrm{T}(\mathbf{v}_2), \ldots, \mathrm{T}(\mathbf{v}_\ell)) \in C$.*

Thus, skew ℓ-GQC codes are linear codes that are closed under skew quasi-cyclic shift. If θ is the identity map, then skew ℓ-GQC codes are just the standard GQC codes over $\mathbb{F}$. For brevity, henceforth we assume that $n := \sum_{i=1}^{\ell} m_i$, and $m \mid m_i$ for all $i \in \{1, 2, \ldots, \ell\}$.

With each $\mathbf{v}_j = (v_{j,1}, v_{j,2}, \ldots, v_{j,m_j}) \in \mathbb{F}^{m_j}$ we associate the polynomial $v_j(x) = \sum_{i=1}^{m_j} v_{j,i}x^{i-1}$ for all $j \in \{1, \ldots, \ell\}$. This gives a one to one correspondence between $\mathbb{F}^{m_1} \times \mathbb{F}^{m_2} \times \ldots \times \mathbb{F}^{m_\ell}$ and the ring $R = R_1 \times R_2 \times \ldots \times R_\ell$ where $R_j \triangleq \mathbb{F}[x;\theta]/(x^{m_j}-1)$ for all $j \in \{1, \ldots, \ell\}$. In fact, the following result is straightforward from the definition

Theorem 3.1. *Let $R_j \triangleq \mathbb{F}[x;\theta]/(x^{m_j}-1)$ and $g(x) \in \mathbb{F}[x;\theta]$. Then the ring*

$$R \triangleq R_1 \times R_2 \times \ldots \times R_\ell$$

is a left $\mathbb{F}[x;\theta]$-module with multiplication defined by

$$\begin{aligned} g(x)(f_1(x) + (x^{m_1}-1), \ldots, f_\ell(x) + (x^{m_\ell}-1)) \\ = (g(x)f_1(x) + (x^{m_1}-1), \ldots, g(x)f_\ell(x) + (x^{m_\ell}-1)). \end{aligned} \tag{2}$$

At this point it is easy to see that Definition 3 is equivalent to the following definition.

Definition 3.2. ([10, Definition 3.1].) *A subset C is called a skew ℓ-GQC code of length n if C is a left $\mathbb{F}[x;\theta]$-submodule of R.*

We say that C is a 1-*generator skew ℓ-GQC code* if it has the form

$$C = \{f(x)(s_1(x), s_2(x), \ldots, s_\ell(x)) \ : \ f(x) \in \mathbb{F}[x;\theta] \text{ and } s_j(x) \in R_j\}. \tag{3}$$

We often denote such a code by $C = \langle S(x)\rangle$ where $S(x) := (s_1(x), \ldots, s_\ell(x))$. The following lemma was established in [10, Section 4].

Lemma 3.1. *Let C be a 1-generator skew ℓ-GQC code of length n. Then there exist polynomials $g_i(x)$ and $p_i(x) \in R_i$ such that $g_i(x)$ divides $x^{m_i} - 1$ and*

$$C = \langle (p_1(x)g_1(x), p_2(x)g_2(x), \ldots, p_\ell(x)g_\ell(x))\rangle.$$

The next result is similar to [10, Theorem 4.2]. Here we give a direct proof of the theorem instead of via the parity-check polynomial as was done in the said reference.

Theorem 3.2. *Let C be a skew ℓ-GQC code C of length n given by*

$$C = \langle (p_1(x)g_1(x), p_2(x)g_2(x), \ldots, p_\ell(x)g_\ell(x))\rangle$$

and let $\mu_i(x) := \operatorname{gcld}(p_i(x)g_i(x), x^{m_i} - 1)$. Write $x^{m_i} - 1 = \beta_i(x)\ \mu_i(x) = \mu_i(x)\ \beta_i(x)$, and define $u(x) := \operatorname{lclm}(\beta_1(x), \beta_2(x), \ldots, \beta_\ell(x))$. Then $\dim(C) = \deg(u(x))$.

Proof. Since $\mu_i(x) = \operatorname{gcld}(p_i(x)g_i(x), x^{m_i} - 1)$, there exist $\alpha_i(x)$ and $\beta_i(x)$ such that

$$p_i(x)\ g_i(x) = \mu_i(x)\ \alpha_i(x) \text{ and } x^{m_i} - 1 = \beta_i(x)\ \mu_i(x) = \mu_i(x)\ \beta_i(x). \tag{4}$$

Hence, we can write

$$\beta_i(x) = \frac{x^{m_i} - 1}{\mu_i(x)}. \tag{5}$$

By definition, for each i there exists $\gamma_i(x)$ for which $u(x) = \gamma_i(x)\ \beta_i(x)$. By Eq. (5),

$$u(x) = \gamma_i(x)\ \frac{x^{m_i} - 1}{\mu_i(x)}.$$

Suppose $c(x) = f(x)\ (p_1(x)\ g_1(x), \ldots, p_\ell(x)\ g_\ell(x)) \in C$. Applying the right division algoritheorem, there exist $q(x)$ and $r_i(x)$, for each i, such that

$$f(x) = q(x)\ u(x) + r_i(x) \text{ with } 0 = r_i(x) \text{ or } \deg(r_i(x)) < \deg(u(x)).$$

This implies that

$$\begin{aligned} f(x)\ p_i(x)\ g_i(x) &= (q(x)\ u(x) + r_i(x))\ p_i(x)\ g_i(x) = q(x)\ u(x)\ p_i(x)\ g_i(x) + r_i(x)\ p_i(x)\ g_i(x) \\ &= q(x)\ \gamma_i(x)\ \frac{x^{m_i} - 1}{\mu_i(x)}\ \mu_i(x)\ \alpha_i(x) + r_i(x)\ p_i(x)\ g_i(x) \\ &\equiv r_i(x)\ p_i(x)\ g_i(x) \text{ modulo } (x^{m_i} - 1). \end{aligned}$$

Using the notations $p(x) := (p_1(x), \ldots, p_\ell(x))$, $g(x) := (g_1(x), \ldots, g_\ell(x))$, and

$$p(x)\ g(x) \triangleq (p_1(x)\ g_1(x), p_2(x)\ g_2(x), \ldots, p_\ell(x)\ g_\ell(x)),$$

we obtain $C = \langle S\rangle$ with $S = \left\{x^j\ p(x)\ g(x)\right\}_{j=0}^{\deg(u(x))-1}$. Next, we show that S is linearly independent.

Suppose, for a contradiction, that there exists $f(x) \in \mathbb{F}[x;\theta]$ with $\deg f(x) < \deg u(x)$ satisfying

$$f(x)\ (p_1(x)\ g_1(x), p_2(x)\ g_2(x), \ldots, p_\ell(x)\ g_\ell(x)) = (0, 0, \ldots, 0).$$

Hence,

$$f(x)\ p_i(x)\ g_i(x) = y_i(x)\ (x^{m_i}-1) \text{ for some } y_i(x). \tag{6}$$

Since $\mu_i(x) = \text{gcld}\,(p_i(x)g_i(x), x^{m_i}-1)$, there exist polynomials $w_1(x)$ and $w_2(x)$ satisfying

$$f(x)\ p_i(x)\ g_i(x)\ w_1(x) + f(x)\ (x^{m_i}-1)\ w_2(x) = f(x)\ \mu_i(x).$$

By Eq. (6) and since $(x^{m_i}-1) \in Z(\mathbb{F}[x;\theta])$, we can write

$$(y_i(x)\ w_1(x) + f(x)\ w_2(x))\ (x^{m_i}-1) = f(x)\ \mu_i(x).$$

Now, Eq. (4) allows us to infer that $(y_i(x)\ w_1(x)+f(x)\ w_2(x))\ \beta_i(x)\ \mu_i(x) = f(x)\ \mu_i(x)$, implying that $(y_i(x)\ w_1(x)+f(x)\ w_2(x))\ \beta_i(x) = f(x)$. Thus, $f(x)$ is a common left multiple of $\beta_i(x)$ for all i. Hence, there exists $d(x)$ such that $f(x) = d(x)\ u(x)$ since $u(x) = \text{lclm}\,(\beta_1(x), \ldots, \beta_\ell(x))$. This is a contradiction since $\deg(f(x)) < \deg(u(x))$. □

Definition 3.3. *Let C be a skew ℓ-GQC code C of length n. Let $\mathbf{v}_i = (v_{i,1}, \ldots, v_{i,m_i}) \in \mathbb{F}^{m_i}$. The dual code $C^\perp$ of C is given by*

$$C^\perp = \left\{ \mathbf{v} = (\mathbf{v}_1, \ldots, \mathbf{v}_\ell) \in \mathbb{F}^{m_1} \times \mathbb{F}^{m_2} \times \ldots \times \mathbb{F}^{m_\ell} \ : \ \langle \mathbf{v}, \mathbf{c} \rangle := \sum_{i=1}^{\ell} \sum_{j=1}^{m_i} v_{i,j} c_{i,j} = 0 \right\}.$$

The next results establishes that if C is a skew ℓ-GQC code then $C^\perp$ is also a skew ℓ-GQC code.

Theorem 3.3. *Let C be a skew GQC code of length $n = m_1 + m_2 + \ldots m_\ell$ and index ℓ. Then $C^\perp$ is also a skew GQC code of length n and index ℓ.*

Proof. Let

$$\mathbf{a} = (\mathbf{a}_1, \ldots, \mathbf{a}_\ell) = (a_{1,0}, a_{1,1}, \ldots, a_{1,m_1-1}, a_{2,0}, a_{2,1}, \ldots, a_{2,m_2-1}, \ldots, a_{\ell,0}, a_{\ell,1}, \ldots, a_{\ell,m_\ell-1}) \in C^\perp.$$

To show that $C^\perp$ is a skew GQC code of length $n = m_1 + m_2 + \ldots + m_\ell$ and index ℓ, it suffices to show that

$$\mathrm{T}(\mathbf{a}) = (\theta(a_{1,m_1-1}), \theta(a_{1,0}), \ldots, \theta(a_{1,m_1-2}), \theta(a_{2,m_2-1}), \theta(a_{2,0}), \ldots, \theta(a_{2,m_2-2}), \ldots, \theta(a_{\ell,m_\ell-1}), \theta(a_{\ell,0}), \ldots, \theta(a_{\ell,m_\ell-2})) \in C^\perp,$$

i.e., for any

$$\mathbf{c} = (\mathbf{c}_1, \ldots, \mathbf{c}_\ell) = (c_{1,0}, c_{1,1}, \ldots, c_{1,m_1-1}, c_{2,0}, c_{2,1}, \ldots, c_{2,m_2-1}, \ldots, c_{\ell,0}, c_{\ell,1}, \ldots, c_{\ell,m_\ell-1}) \in C$$

we must show that $\langle \mathrm{T}(\mathbf{a}), \mathbf{c} \rangle = 0$. Writing explicitly,

$$\begin{aligned}\langle \mathrm{T}(\mathbf{a}), \mathbf{c} \rangle =& c_{1,0}\theta(a_{1,m_1-1}) + c_{1,1}\theta(a_{1,0}) + \ldots + c_{1,m_1-1}\theta(a_{1,m_1-2}) + \ldots + \\ & c_{\ell,0}\theta(a_{\ell,m_\ell-1}) + c_{\ell,1}\theta(a_{\ell,0}) + \ldots + c_{\ell,m_\ell-1}\theta(a_{\ell,m_\ell-2}).\end{aligned} \tag{7}$$

Since C is skew GQC code, $\mathrm{T}^k(\mathbf{c}) \in C$. Let $M := \text{lcm}(m_1, m_2, \ldots, m_\ell)$. Since $|\langle\theta\rangle| = m$ and $m \mid m_i$ for all $i \in \{1, \ldots, \ell\}$, we know that $m \mid M$. Hence, $\theta^M(x) = x$ for any x, $\theta^{M-1}(x) = \theta^{-1}(x)$, and $\mathrm{T}^M(\mathbf{c}) = \mathbf{c}$. Thus,

$$\begin{aligned}\mathrm{T}^{M-1}(\mathbf{c}) = (&\theta^{-1}(c_{1,1}), \theta^{-1}(c_{1,2}), \ldots, \theta^{-1}(c_{1,m_1-1}), \theta^{-1}(c_{1,0}), \ldots, \\ &\theta^{-1}(c_{\ell,1}), \theta^{-1}(c_{\ell,2}), \ldots, \theta^{-1}(c_{\ell,m_\ell-1}), \theta^{-1}(c_{\ell,0})).\end{aligned}$$

Since C is a skew GQC code, we have $\left\langle \mathbf{a}, \mathrm{T}^{M-1}(\mathbf{c}) \right\rangle = 0$. Hence,

$$\begin{aligned}&a_{1,0}\theta^{-1}(c_{1,1}) + a_{1,1}\theta^{-1}(c_{1,2}) + \ldots + a_{1,m_1-1}\theta^{-1}(c_{1,0}) + \ldots + \\ &a_{\ell,0}\theta^{-1}(c_{\ell,1}) + a_{\ell,1}\theta^{-1}(c_{\ell,2}) + \ldots + a_{\ell,m_\ell-1}\theta^{-1}(c_{\ell,0}) = 0.\end{aligned} \tag{8}$$

Apply θ to both sides of Eq. (8) to get

$$c_{1,1}\theta(a_{1,0}) + c_{1,2}\theta(a_{1,1}) + \ldots + c_{1,0}\theta(a_{1,m_1-1}) + \ldots + c_{\ell,1}\theta(a_{\ell,0}) + c_{\ell,2}\theta(a_{\ell,1}) + \ldots + c_{\ell,0}\theta(a_{\ell,m_\ell-1}) = 0. \quad (9)$$

Notice that the left hand side of Eq. (9) is the right hand side of Eq. (7) after some rearrangement. Therefore, $C^{\perp}$ is indeed a skew GQC code of length $n = m_1 + m_2 + \ldots + m_\ell$ and index ℓ. □

Remark 3.1. *Theorem 3.3 states that if C is a skew ℓ-GQC code, then $C^{\perp}$ is also a skew ℓ-GQC code. Note, however, that if C is a 1-generator skew ℓ-GQC code, then $C^{\perp}$ is not necessarily 1-generator as well.*

Table 1. Good Skew ℓ-GQC codes over $GF(4)$.

No.	C	$(m_1, \ldots, m_\ell)$	$\{p_i(x)\}_{i=1}^{\ell}$ and $\{g_i(x)\}_{i=1}^{\ell}$
1	$[18, 8, 8]$	$(8, 8, 2)$	$p_1 = a^2 0 a^2 1 aaaa$; $g_1 = aaa^2 a1$ $p_2 = 11100 a^2 aa$; $g_2 = a11 a^2 a$ $p_3 = aa^2$; $g_3 = 1a$
2	$[26, 9, 12]$	$(12, 12, 2)$	$p_1 = 1 a^2 aa^2 10 a^2 011 aa$; $g_1 = a^2 a^2 11 a^2 a1$ $p_2 = a^2 1 a^2 aa^2 a11 aa^2 0 a^2$; $g_2 = a^2 110 a^2 110 a^2 11$ $p_3 = a$; $g_3 = a^2 a$
3	$[34, 15, 12]$	$(16, 16, 2)$	$p_1 = a^2 a^2 a^2 a^2 1 a10100 a^2 01$; $g_1 = a^2 00 aa01 a101$ $p_2 = aa^2 100 a^2 11 aa^2 a^2 x^3 aa^2 a$; $g_2 = a1a1a1a1a1a1a1a1$ $p_3 = g_3 = 1a$
4	$[36, 16, 12]$	$(30, 6)$	$p_1 = 1$; $g_1 = 110 a111 a1 aa^2 0 a^2 aa^2$ $p_2 = a^2 111$; $g_2 = a^2 aa^2 aa^2 a$
5	$[38, 18, 12]$	$(18, 18, 2)$	$p_1 = 1 a^2 a^2 1 a^2 10 aaa^2 0 a^2$; $g_1 = 11 aa^2 00 aaa^2 1$ $p_2 = a100 a^2 a^2 a^2 a^2 00 a^2 a^2$; $g_2 = 111111111111111111$ $p_3 = 1a$; $g_3 = aa$
6	$[40, 14, 16]$	$(16, 16, 8)$	$p_1 = a^2 a^2 1 aaaa^2 a^2 11010001$; $g_1 = a^2 00 aa01 a101$ $p_2 = a^2 a^2 1 a^2 a^2 a^2 0 a^2 a^2 a^2 aaa^2 1$; $g_2 = a^2 11 a^2 01 aa1$ $p_3 = a^2 a^2 a^2 1 a1 aa$; $g_3 = 1$
7	$[42, 18, 14]$	$(20, 20, 2)$	$p_1 = a^2 a^2 a^2 aa^2 a^2 110 a1 a^2 1 a^2 1 a010$; $g_1 = a1 a0 a^2 0 a^2 0 a0 a1$ $p_2 = 110 a^2 1 a^2 10 a^2 101 a^2 a^2 10100 a^2$; $g_2 = aa1 a1 aa^2 a^2 a^2 a^2 1$ $p_3 = 1a$; $g_3 = aa$
8	$[44, 14, 18]$	$(14, 14, 14, 2)$	$p_1 = 1 a^2 01 a1 a^2 1 a110 a$; $g_1 = a^2 a110 a1 a^2$ $p_2 = 10 aaaa1 aa^2 a00 a^2 a$; $g_2 = a^2 a110 a1 a^2$ $p_3 = a1 a^2 a^2 11 a^2 aaa^2 1 a1 a^2$; $g_3 = a^2 1 a11 a^2 1 a$ $p_4 = 1a$; $g_4 = a^2 1$
9	$[54, 21, 18]$	$(24, 24, 6)$	$p_1 = aa1 a^2 a^2 10 a^2 a^2 101 a^2 1 a^2 a^2 a^2 a^2 a^2 aa^2 a$ $g_1 = a^2 a1 a^2 01 a^2 aaa1 a^2 01 a^2 a1$ $p_2 = a1 a^2 010 a01 a^2 a0 a0 aa^2 0 aa^2 a^2 0 a$ $g_2 = a^2 a1 a^2 01 a^2 aaa1 a^2 01 a^2 a1$ $p_3 = aa0 a^2 1 a^2$; $g_3 = a^2 a^2 a^2$

Consider the finite field $GF(4) = \{0, 1, a, a^2\}$ where $a^2 + a + 1 = 0$ and let θ be the Frobenius automorphism that fixes $GF(2)$, sending z to z^2. We say that a $GF(4)$-linear code is *good* if it satisfies at least one the following conditions.

(1) Given (n, k), it has the best-known minimum distance d among all comparable codes.
(2) Given (n, d), it has the best-known dimension k among all comparable codes.

When the parameters (n, k) and (n, d) are understood from the context, we call the code, respectively, BKLC and BDLC.

This section contains three distinct but related search results. Good skew ℓ-GQC codes found are discussed in the first subsection. The second one gives the results upon applying shortening and puncturing methods. To highlight the benefit of constructing skew ℓ-GQC codes we show how to derive some asymmetric quantum codes detecting single bit-flip error in the third one. These quantum codes cannot presently be derived from the BKLC and BDLC codes stored in the MAGMA database or the codes recorded in the Grassl Table [11].

3.1. **Good Skew ℓ-GQC codes over $GF(4)$.** We wrote a program in MAGMA (Ver. 2.20) [2] to search for good $GF(4)$-linear skew ℓ-GQC codes based on the results obtained in previous sections. The program first generates positive even integers $m_1, \ldots, m_\ell$. It then searches for a divisor $g_i(x)$ of $x^{m_i} - 1$ in $\mathbb{F}[x; \theta]$. Next, it looks for polynomials $p_i(x)$ so that the skew ℓ-GQC code of the form

$$C := \langle p_1(x)\ g_1(x), p_2(x)\ g_2(x), \ldots, p_\ell(x)\ g_\ell(x) \rangle$$

has a large minimum distance d. The product $p_i(x)\ g_i(x)$ is then computed modulo $(x^{m_i} - 1)$.

For ease of verification, when presenting the good codes that the program finds we list down $p_i(x)$ and $g_i(x)$. The polynomials are represented by a sequence of coefficients of decreasing powers. For example, the sequence $1a0a^20a$ represents the polynomial $x^5 + ax^4 + a^2x^2 + a$. Table 1 lists down skew ℓ-GQC codes having the parameters specified by BKLC$(GF(4), n, k)$. They are, however, not BDLC. The main advantage of these codes over most of the corresponding codes in the Grassl Table is that they can be directly constructed as opposed to being obtained through some rather *ad hoc* steps.

Example 3.1. Consider the skew 3-GQC $[18, 8, 8]$ code C listed as Entry 1 in Table 1. Note that $d(C) = 8$, equaling the minimum distance specified by BKLC$(GF(4), 18, 8)$. The best-known code in the Grassl Table was obtained indirectly in two steps. First, an $[18, 9, 8]_4$-code is constructed from a stored generator matrix. Taking a subcode of the resulting code then yields an $[18, 8, 8]_4$-code.

Table 2. Good Nondegenerate Skew ℓ-GQC Codes over $GF(4)$.

No.	C	$(m_1, \ldots, m_\ell)$	$\{p_i(x)\}_{i=1}^{\ell}$
1	$[40, 12, 18]$	$(12, 12, 12, 4)$	$p_1 = aa1a^200a^2a1a^2aa^2$; $p_2 = a^2a^20a^21aa^2aa10$ $p_3 = 10a^2aaa^20a111$; $p_4 = a^200a$
2	$[52, 10, 28]$	$(10, 10, 10, 10, 10, 2)$	$p_1 = aa^21a^211a^2a00$; $p_2 = aa01a^21a0aa$ $p_3 = 111000a^2a^2a^20$; $p_4 = a^2aa^21110a^2a^20$ $p_5 = a^20a10a1011$; $p_6 = a0$
3	$[72, 14, 36]$	$(14, 14, 14, 14, 14, 2)$	$p_1 = a^21aa000aaaa^2a^2$; $p_2 = a01011a^2110a^2$ $p_3 = 1aa1a1a1a110$; $p_4 = 1a^2aaa^20aa^20a^2a^2$ $p_5 = 1a^21a^20a^200a^20a^21$; $p_6 = 10$
4	$[76, 24, 28]$	$(24, 24, 24, 4)$	$p_1 = a^2a^2a0a^2011aaaa^2a^2a$ $p_2 = 1001a^20a^2101a^2aa0$ $p_3 = 110a^20a^211aa1a^2010$; $p_4 = a1aa$
5	$[78, 24, 29]$	$(24, 24, 24, 6)$	$p_1 = 1a^201a^20a^2a^2a010a^2a11$ $p_2 = a11a0a^2aaa^2a^2a010$ $p_3 = 1a0aaa^2010110a^2a^2a^2$; $p_4 = aa^2aa^2aa^2$
6	$[112, 22, 51]$	$(22, 22, 22, 22, 22, 2)$	$p_1 = a^2a^21011a^20aa^2a^2101a^20aa11$ $p_2 = a01a^2aa^2aaa111a^2a^2aa^2aa^2a1$ $p_3 = a^201a^2aa^2a0a^2101a^21a^2a^2a111$ $p_4 = aa^2a^211a^21a^2a00a^2a^2a^2aa00a^21$ $p_5 = a^211a^2a0010a1011aa^21a^2a^2a$; $p_6 = a1$

It is also possible to construct good skew ℓ-GQC codes having the trivial factor $g(x) = 1$. They are of the form

$$C := \langle p_1(x), p_2(x), \ldots, p_\ell(x) \rangle .$$

Following [1], these codes are called *non-degenerate* skew ℓ-GQC codes. Table 2 presents such codes found in our search. They all satisfy both the BKLC and the BDLC conditions, except for Entry 4, which is only BKLC, since the largest known dimension for $(n = 76, d = 28)$ is $k = 26$.

3.2. **Good Codes from Puncturing or Shortening.** Taking a closer look at the obtained codes, we consider both the codes and their component codes, which are the skew cyclic codes C_i of length m_i for each $i \in \{1, \ldots, \ell\}$ generated by $p_i(x)$ $g_i(x)$, and apply puncturing and shortening to search for good codes. Table 3 lists down the good codes obtained. The code listed as Entry 1, for instance, comes from shortening the code C listed as Entry 1 in Table 1 at the first position. Entry 5 is derived by puncturing the first component C_1 of the code listed as Entry 4 in Table 1 at position 1.

Table 3. Good Codes from Puncturing or Shortening.

No.	C	Method	No.	C	Method
1	$[17, 7, 8]$	Shorten(T1,1) at 1	9	$[35, 15, 12]$	Shorten(T1,5) at $\{1, 2, 3\}$
2	$[16, 6, 8]$	Shorten(T1,1) at $\{1, 2\}$	10	$[53, 20, 18]$	Shorten(T1,9) at 1
3	$[15, 5, 8]$	Shorten(T1,1) at $\{1, 2, 3\}$	11	$[52, 19, 18]$	Shorten(T1,9) at $\{1, 2\}$
4	$[25, 8, 12]$	Shorten(T1,2) at 1	12	$[39, 11, 18]$	Shorten(T1,1) at 1
5	$[29, 16, 8]$	Puncture(C_1,T1,4) at 1	13	$[75, 23, 28]$	Shorten(T1,4) at 1
6	$[35, 15, 12]$	Shorten(T1,4) at 1	14	$[74, 22, 28]$	Shorten(T1,4) at $\{1, 2\}$
7	$[37, 17, 12]$	Shorten(T1,5) at 1	15	$[77, 23, 29]$	Shorten(T1,5) at 1
8	$[36, 16, 12]$	Shorten(T1,5) at $\{1, 2\}$			

Remark 4.1. *The codes in Entry 4 of Table 1 and Entry 8 of Table 3 are not equivalent since they have different weight enumerators. Similarly, in Table 3, Entries 6 and 9 are not equivalent.*

3.3. **Some Derived Asymmetric Quantum CSS Codes.** We begin by defining an asymmetric quantum code (AQC) and briefly reproduce the CSS construction yielding AQCs capable of detecting a single bit-flip error and correcting multiple phase-flip errors. Further details on AQCs and how we can link them to classical linear codes by way of the so-called CSS construction are given in [23, 8, 9]. The physical motivation behind asymmetric quantum codes for the qubit case ($q = 2$) and some experimental evidences showing that phase-flip errors are much more likely to occur than bit-flip errors do are presented in [16].

Let d_x and d_z be positive integers. A quantum code Q in $V_n = (\mathbb{C}^q)^{\otimes n}$ of dimension $K \geq 1$ is called an *asymmetric quantum code* with parameters $((n, K, \{d_z, d_x\}))_q$, or $[[n, k, \{d_z, d_x\}]]_q$ with $k = \log_q K$ whenever Q is a stabilizer code, if Q is able to detect any combination of up to $d_x - 1$ bit-flips (or X-errors) and up to $d_z - 1$ phase-flips (or Z-errors) simultaneously.

The standard CSS construction is given in, *e.g.*, [29].

Theorem 3.4. *Let C_i be linear codes with parameters $[n, k_i, d_i]_q$ for $i \in \{1, 2\}$ with $C_1^\perp \subseteq C_2$. Let*

$$d_z := \mathrm{wt}(C_2 \setminus C_1^\perp) \text{ and } d_x := \mathrm{wt}(C_1 \setminus C_2^\perp). \tag{10}$$

Then there exists an AQC Q with parameters $[[n, k_1 + k_2 - n, \{d_z, d_x\}]]_q$. The code Q is said to be pure whenever $d_z = d_2$ and $d_x = d_1$.

For our purpose, we make use of the following result, which was shown to be a direct consequence of Theorem 3.4 in [9].

Theorem 3.5. *Let C be a linear $[n, k, d]_q$-code. If C has a codeword $\mathbf{v}$ such that $\mathrm{wt}(\mathbf{v}) = n$, then there exists an $[[n, k-1, \{d, 2\}]]_q$-code Q.*

Table 4. Good Derived AQCs Detecting Single Bit-Flip Error.

No.	AQC Q	Derived From	No.	AQC Q	Derived From
1	$[[17, 6, \{8, 2\}]]_4$	Table 3 Entry 1	6	$[[37, 16, \{12, 2\}]]_4$	Table 3 Entry 7
2	$[[15, 4, \{8, 2\}]]_4$	Table 3 Entry 3	7	$[[39, 10, \{18, 2\}]]_4$	Shorten(T2,1) at 1
3	$[[25, 7, \{12, 2\}]]_4$	Table 3 Entry 4	8	$[[40, 11, \{18, 2\}]]_4$	Table 2 Entry 1
4	$[[35, 14, \{12, 2\}]]_4$	Table 3 Entry 6	9	$[[54, 19, \{18, 2\}]]_4$	Table 3 Entry 10
5	$[[35, 14, \{12, 2\}]]_4$	Table 3 Entry 9			

As discussed in [9, Subsection IV.C], on many occasions, the database of BKLC and BDLC of MAGMA as well as the Grassl Table host good codes not having any codewords of weight equals the length of the codes. We derive good AQCs by applying Theorem 3.5 to codes listed in Table 1 to Table 3 and present them here in Table 4 only if AQCs of the same parameters cannot be inferred from the good codes listed in either MAGMA's database or in the Grassl Table for $q = 4$. This highlights another usefulness of studying skew ℓ-GQC.

4. Conclusion

In this article, we study the structure and properties of skew generalized quasi-cyclic codes in the noncommutative ring $\mathbb{F}[x; \theta]$. We prove that such codes are left submodules of the ring $R_1 \times R_2 \times \cdots R_\ell$, where $R_i = \mathbb{F}[x; \theta]/(x^{m_i} - 1)$. We determine the generator polynomials of these codes and compute their dimension in terms of the degrees of the generator polynomials. Further, we establish that if C is a skew ℓ-GQC code of length $n = m_1 + m_2 + \ldots + m_\ell$, then the dual code $C^\perp$ is also a skew ℓ-GQC code of length n.

Our approach is independent of the work of Gao *et al.* in [10] that studies skew generalized quasi-cyclic codes from the Chinese Remainder approach. Further, in this work, we show that good skew ℓ-GQC codes exist for $q = 4$, partially answering an open problem stated in [10].

Implementing the results as a search program over $GF(4)$, we find many codes with good parameters. In many cases, puncturing or shortening skew ℓ-GQC codes yield codes with good parameters. The structure of the skew ℓ-GQC codes fits perfectly into the CSS construction of quantum codes. Their nestedness is evident and the dual of such a code is also skew ℓ-GQC. Applying the CSS construction for asymmetric quantum codes allows us to derive good quantum codes detecting a single bit-flip error whose existence can not be inferred from good codes recorded in either the MAGMA database or in the Grassl Table. These results are encouraging and show that skew ℓ-GQC codes deserve further attention.

Some open problems remain. One is to express the generator polynomials of $C^\perp$ in terms of the generator polynomials of C. A more challenging one is to derive good lower bounds on the minimum distance of a skew ℓ-GQC code.

5. Acknowledgment

We thank the anonymous reviewer for the valuable comments that lead us to improve the paper.

References

[1] Abualrub, T., Ghrayeb, A., Aydin, N., and Siap, I., (2010), On the construction of skew quasi-cyclic codes, IEEE Trans. Inf. Theory, 56(2), pp.2081-2090.
[2] Bosma, W., Canon, J.J., Playoust, C., (1997), The magma algebra system I: The user language, J. Symbol. Comput., 24, pp.235-266.
[3] Boucher, D., Geismann, W., Ulmer, F., (2007), Skew-cyclic codes, Appl. Algebra Engrg. Comm. Comput., 18(4), pp.379-389.
[4] Boucher, D., Solé, P., Ulmer, F., (2008), Skew constacyclic codes over Galois Rings, Adv. Math. Commun., 2(3), pp.273-292.
[5] Boucher, D., Ulmer, F., (2009), Coding with skew polynomial rings, J. Symbol. Comput., 44, pp.1644-1656.
[6] Chen, Z., (1994), Six new binary quasi-cyclic codes, IEEE Trans. Inf. Theory, 40(5), pp.1666-1667.
[7] Esmaeili, M., Yari, S., (2009), Generalized quasi-cyclic codes: Structural properties and code construction, Appl. Algebra Engrg. Comm. Comput., 20, pp.159-173.
[8] Ezerman, M.F., Jitman, S., Ling, S., Solé, P., (2011), Additive Asymmetric Quantum Codes, IEEE Trans. on Information Theory, IT-57, pp.5536-5550.
[9] Ezerman, M.F., Jitman, S., Ling, S., Pasechnik, D.V., (2013), CSS-like constructions of asymmetric quantum codes, IEEE Trans. Inf. Theory, 59(10), pp.6732-6754.
[10] Gao,J., Shen, L., Fu, F., (2016), A Chinese remainder theorem approach to skew generalized quasi-cyclic codes over finite fields, Cryptogr. Commun., 8, pp.51-66.
[11] Grassl, M.,(2018), Bounds on the minimum distance of linear codes and quantum codes, Online available at http://www.codetables.de, accessed on January 2.
[12] Greenough, P.P., Hill, R., (1992), Optimal ternary quasi-cyclic codes, Des. Codes Cryptogr., 2, pp.81-91.
[13] Gulliver, T.A., Bhargava, V.K., (1992), Nine good rate $(m-1)/pm$ quasi-cyclic codes,"IEEE Trans. Inf. Theory, 38(4), pp.1366-1369.
[14] Gulliver, T.A., Bhargava, V.K., (1992), Some best rate $1/p$ and rate $(p-1)/p$ systematic quasi-cyclic codes over $GF(3)$ and $GF(4)$, IEEE Trans. Inf. Theory, 38(4), pp.1369-1374.
[15] Hammons A.R., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A., Solé, P., (1994), The Z_4-linearity of Kerdock, Preparata, Goethals and related codes, IEEE Trans. Inf. Theory, 40, pp.301-319.
[16] Ioffe, L., Mézard, M., (2007), Asymmetric quantum error-correcting codes, Phys. Rev. A, 75(3), pp.32345.
[17] Jacobson, N.,(1943), The Theory of Rings, Amer. Math. Soc. Math., New York.
[18] Kasami, T., (1974), A Gilbert-Varshamov Bound for Quasi-cyclic Codes of Rate 1/2, IEEE Trans. Inf. Theory, 20, p. 679.
[19] Lally, K., Fitzpatrick, P., (2001), Algebraic structure of quasi-cyclic codes, Discr. Appl. Math., 111, pp.157-175.
[20] Ling, S., Solé, P., (2001), On the algebraic structure of the quasi-cyclic codes I: Finite fields, IEEE Trans. Inf. Theory, 47(7), pp.2751-2759.
[21] McDonald, B.R., (1974), Finite Rings with Identity, Marcel Dekker Inc., New York.
[22] Ore, O., (1933), Theory of non-commutative polynomials, Annals of Math., 34, pp.480-508.
[23] Sarvepalli, P.K., Klappenecker, A., Rötteler, M., (2009), Asymmetric quantum codes: Constructions, bounds, and performance, Proc. Royal Society London A, 465(2105), pp.1645-1672.
[24] Séguin, G.E., Drolet, G., (1990), The theory of 1-generator quasi-cyclic codes, Preprint, Royal Military College of Canada, Kingston, Ontario.
[25] Siap, I., Abualrub, T., Aydin, N., Seneviratne, P., (2011), Skew cyclic codes of arbitrary lengtht, Int. J. Inf. Coding Theory, 2(1), pp.10-20.
[26] Siap, I., Aydin, N., Ray-Chaudhuri, D.K., (2000), New ternary quasi-cyclic codes with better minimum distances, IEEE Trans. Inf. Theory, 46(4), pp.1554-1558.
[27] Siap, I., Kulhan, N., (2005), The structure of generalized quasi cyclic codes, Appl. Math. E-Notes, 5, pp.24-30.
[28] Thomas, K., (1977), Polynomial approach to quasi-cyclic codes, Bul. Cal. Math. Soc., 69, pp.51-59.

[29] Wang, L., Feng, K., Ling, S., Xing, C., (2010), Asymmetric quantum codes: Characterization and constructions, IEEE Trans. Inf. Theory, 56, pp.2938-2945.

Taher Abualrub - is a professor of Mathematics at the American University of Sharjah. He received his Master and Ph.D. degrees in Mathematics from the University of Iowa, USA, in August 1994 and May 1998, respectively. In 1998 he joined the American University of Sharjah (AUS) as an Assistant Professor in the department of Mathematics and Statistics. Currently, he is a professor of mathematics at AUS. His research interests include error correcting codes, DNA computing, wavelet theory, and control theory.

Martianus Frederic Ezerman - grew up in East Java Indonesia. He received the B.A. Phil. and the B.Sc. Math. degrees in 2005 and the M.Sc. Math. degree in 2007, all from Ateneo de Manila University, Philippines, and obtained the Ph.D. degree in mathematics from Nanyang Technological University, Singapore in 2011. After research fellowships at Université Libre de Bruxelles, Belgium and at the Centre for Quantum Technologies, National University of Singapore, he returned in March 2014 to NTU where he is currently a Senior Research Fellow. His main interests are coding theory, cryptography, and quantum information processing.

Padmapani Seneviratne - received the Ph.D. degree from Clemson University, South Carolina in 2007 under the supervision of Dr. Jennifer D. Key. After graduation, he joined the American University of Sharjah, UAE, as an Assistant Professor and was promoted to Associate Professor in 2014. He is currently a tenured Associate Professor of Mathematics at Texas A&M University Commerce, USA. His research interests include algebraic coding theory and applications of discrete mathematics.

Patrick Solé - received the Ingénieur and Docteur-Ingénieur degrees both from Ecole Nationale Supérieure des Télécommunications, Paris, France, in 1984 and 1987, respectively, and the habilitation à diriger des recherches from Université de Nice-Sophia Antipolis, Sophia Antipolis, France, in 1993. He has held visiting positions in Syracuse University, Syracuse, NY, from 1987 to 1989, Macquarie University, Sydney, Australia, from 1994 to 1996, and Lille University, Lille, France, from 1999 to 2000. Since 1989, he has been a permanent member of the CNRS and became Directeur de Recherche in 1996.

He is currently member of the CNRS lab LAGA at University of Paris 8. His research interests include coding theory, interconnection networks (graph spectra, expanders), vector quantization (lattices), and cryptography (Boolean functions, pseudorandom sequences).