On the structure of 1-generator quasi-polycyclic codes over finite chain rings *

Rongsheng Wu† Minjia Shi‡ and Patrick Solé§

Abstract: Quasi-polycyclic (QP for short) codes over a finite chain ring $R$ are a generalization of quasi-cyclic codes, and these codes can be viewed as an $R[x]$-submodule of $R_m^\ell$, where $R_m := R[x]/\langle f \rangle$, and $f$ is a monic polynomial of degree $m$ over $R$. If $f$ factors uniquely into monic and coprime basic irreducibles, then their algebraic structure allow us to characterize the generator polynomials and the minimal generating sets of 1-generator QP codes as $R$-modules. In addition, we also determine the parity check polynomials for these codes by using the strong Gröbner bases. In particular, via Magma system, some quaternary codes with new parameters are derived from these 1-generator QP codes.

Keywords: Polycyclic codes; Sequential codes; 1-generator quasi-polycyclic codes; duality; $Z_4$-linear codes

MSC 2010: 94B05, 94B60, 11T71

1 Introduction

Codes over finite rings have attracted vital attention in the past several decades. In 1994s, Hammons et al. [1] found that some good nonlinear binary codes can be viewed as the Gray images of cyclic codes over $Z_4$. After this seminal paper, codes over rings received lots of interest. It is worth noting that many follow-up works are related to finite chain rings.

Let $R$ be a finite commutative chain ring with maximal ideal $M$, and $\ell$ be a nonnegative integer. We say that a linear code $C$ of length $n = m\ell$, with index $\ell$ and associate vector

*This research is supported by the National Natural Science Foundation of China (12071001, 61672036), the Excellent Youth Foundation of Natural Science Foundation of Anhui Province (1808085J20), and the Academic Fund for Outstanding Talents in Universities (gxbjZD03).

†Key Laboratory of Intelligent Computing and Signal Processing, Ministry of Education, School of Mathematical Sciences, Anhui University, Hefei, 230601, P.R. China, wrs2510@163.com

‡Corresponding author, Key Laboratory of Intelligent Computing and Signal Processing, Ministry of Education, School of Mathematical Sciences, Anhui University, Hefei, 230601, P.R. China, smjucl.good@163.com

§Lab I2M (CNRS, Aix-Marseille University, Centrale Marseille), Marseilles, France; sole@enst.fr
\((c_0, c_1, \ldots, c_{m-1})\), over \(R\) is quasi-polycyclic if it is held invariant under right multiplication by the matrix \(\bar{D} = \text{diag}(D, D, \ldots, D)\) (see [2, 3] for more details), where \(c_0 \in R \setminus M\) and \(D\) is the \(m \times m\) matrix given by:

\[
D = \begin{pmatrix}
0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & 1 \\
c_0 & c_1 & c_2 & \cdots & c_{m-1}
\end{pmatrix}.
\]

Denote \(R_m := R[x]/\langle f \rangle\), where \(f = x^m - c(x)\) and \(c(x) = c_0 + c_1 x + \cdots + c_{m-1} x^{m-1} \in R[x]\). Using polynomial representation, it is easy to check that a QP code \(C\) of length \(n = m\ell\) with index \(\ell\) over \(R\) can be viewed as an \(R[x]\)-submodule of \(R^\ell_m\). Some variants of QP codes, are as follows:

- When \(f = x^n - 1\), the code \(C\) is called quasi-cyclic (QC), which is an important class of linear codes and enjoy a strong algebraic structure [4–8]. Furthermore, self-dual QC codes meet a modified GV bound [9], i.e., these codes are asymptotically good.

- It is well-known that \(C\) is a polycyclic code if \(\ell = 1\). The algebraic structures of polycyclic codes over finite chain rings with a new duality were presented in [2, 10], and it is worthy to note that polycyclic codes over Galois rings and mixed alphabet \(\mathbb{Z}_2\mathbb{Z}_4\) were studied in [11] and [12], respectively;

- When \(\ell = 2\), a 1-generator QP code is the well-known double polycirculant (DP) code. The DP codes include special class of double circulant (DC) codes and double negacirculant codes [13–15]. In [16], the isodual DP codes were investigated, and these codes were shown to be asymptotically good based on the existence of infinitely many irreducible trinomials over \(\mathbb{F}_2\).

As we know, QP codes include DP codes as a subclass. If the length is not large enough, their parameters are optimal or quasi-optimal amongst formally self-dual codes. More importantly, in the binary case, it was shown that these codes are asymptotically good. In fact, their relative distance satisfies the GV bound of rate one-half. Some DC codes of short lengths over finite fields are optimal [17], and the Gray images of some special DC codes over finite rings satisfy a modified GV bound [18–20]. The aim of this paper is to generalize the algebraic structure of quasi-cyclic codes to the QP codes, and the main tool used here is the theory of strong Gröbner basis.

Recently, some good linear (cyclic) codes over \(\mathbb{Z}_4\) were obtained from constacyclic codes or generalized QC codes over different rings [21–25], and these codes have better parameters.
than the best known $\mathbb{Z}_4$-linear codes \cite{26}. Moreover, in \cite{27}, new cyclic self-dual $\mathbb{Z}_4$-codes are obtained by employing a new representation for each cyclic code over $\mathbb{Z}_4$ of length $2n$. In this paper, we also give some concrete examples of 1-generator QP codes over $\mathbb{Z}_4$ which lead to quaternary linear codes with new parameters.

The remainder of this paper is organized as follows. Section 2 introduces the relevant terminology and notation. In Section 3, we describe the structural properties of 1-generator QP codes over finite chain rings, including their minimal generating set. The duals of QP codes over the finite chain ring $R$ are described in Section 4. Section 5 is devoted to the construction of the new $\mathbb{Z}_4$-linear codes from 1-generator QP codes with index two and three. Section 6 concludes the paper, along with some interesting problems.

2 Preliminaries

2.1 Finite chain rings

It is well known that a finite commutative ring $R$ with identity $1 \neq 0$ is called a finite chain ring if its ideals are linearly ordered by inclusion. We start by introducing the properties for a finite chain ring. Readers interested should consult \cite{28}.

**Proposition 2.1.** Let $R$ be a finite chain ring. Let $\gamma$ be a fixed generator of $M$ and $s$ the nilpotency index index of $\gamma$, that is, the smallest positive integer for which $\gamma^s = 0$. Then

(i) the distinct proper ideals of $R$ are $\langle \gamma^i \rangle$, where $\langle \gamma^i \rangle = \gamma^i R$ for $1 \leq i \leq s - 1$;

(ii) for any element $e \in R \setminus \{0\}$, there is a unique $i$ and a unit $u \in R$ such that $e = u\gamma^i$ where $0 \leq i \leq s - 1$ and $u$ is unique modulo $\gamma^{s-i}$;

(iii) $\text{Ann}_R(\gamma^i) = \langle \gamma^{s-i} \rangle$, where the annihilator $\text{Ann}_R(a)$ of an element $a$ in $R$ is defined as $\text{Ann}_R(a) = \{x \in R : xa = 0\}$.

Let $F$ be the residue field of $R$, and the projection $R \to F$ extends naturally to a projection $R[x] \to F[x]$. Then for any $g(x) \in R[x]$ we denote by $\bar{g}(x)$ its image under this projection. In the following, a polynomial $g(x) \in \mathcal{R}_m$ or $R[x]$ will be denoted simply by $g$. It will simplify the notation to avoid writing out this each time.

2.2 Polycyclic codes

A polynomial over the field $F$ has no multiple irreducible factors is called square-free. Recall that a polynomial $g \in R[x]$ is called basic irreducible if $\bar{g}$ is irreducible over $F$. From \cite{29}, Lemma 3.1, it is not difficult to see that the ring $R[x]/\langle f \rangle$ is principal if $\bar{f}$ is square-free.
In this case, \( f \) factors uniquely into monic and coprime basic irreducibles, this assumption we use throughout this paper.

To help characterize polycyclic codes over \( R \), it is useful to introduce the content of the strong Gröbner basis over a principal ideal ring according to [30, Theorem 4.2] and the description below [30, Theorem 4.3].

**Theorem 2.2.** Let \( C \subseteq R[x]/\langle f \rangle \) be a nonzero polycyclic code. Then \( C \) admits a set of generator polynomials \( G \):

\[
G = \{ \gamma^{j_0}g_0, \gamma^{j_1}g_1, \ldots, \gamma^{j_t}g_t \},
\]

where \( 0 \leq t \leq s - 1 \) and

(i) \( 0 \leq j_0 < j_1 < \ldots < j_t \leq s - 1 \);
(ii) \( g_i \) is monic for \( i = 0, 1, \ldots, t \);
(iii) \( m > \deg(g_0) > \deg(g_1) > \ldots > \deg(g_t) \);
(iv) \( g_t | g_{t-1} | \ldots | g_0 | f \).

**Remark 2.3.** We follow the notation of Theorem 2.2, and the set \( G \) is called a generating set in standard form for the polycyclic code \( C \). Then, the proof of [31, Corollary to Theorem 6] implies that \( C = \langle \gamma^{j_0}g_0 + \gamma^{j_1}g_1 + \cdots + \gamma^{j_t}g_t \rangle \).

It should be noted that a strong Gröbner basis of \( C \) described in Theorem 2.2 is not necessarily unique [28, Theorem 7.5]. However, the cardinality of the basis, the degree of their polynomials and the exponents \( j_i \) for \( 0 \leq i \leq t \) are unique, and \( C \) has \(|F|^\Delta \) codewords, where \( \Delta = \sum_{i=0}^{t} (s - j_i)(\deg(g_{i-1}) - \deg(g_i)), \deg(g_{-1}) = m \), see [10] for more details.

**Remark 2.4.** In the light of [32, Theorem 4.4], let \( C \) be a cyclic code of length \( N \) with a unique generating set in standard form (see [32, Definition 4.1]) as \( G = \{ \gamma^{j_0}g_0, \gamma^{j_1}g_1, \ldots, \gamma^{j_t}g_t \} \) over \( R \). Consider the shortened cyclic code \( C' \) of length \( n \) obtained from \( C \). Then

\[
x^n = g_0q + r, \quad \text{where } \deg(r) < \deg(g_0).
\]

Let \( f = x^n - r \), and it is clear that \( g_t | g_{t-1} | \cdots | g_0 | f \). Note that the code \( C' \) with generating set \( G \) is an ideal of the quotient ring \( R[x]/\langle f \rangle \), i.e., a polycyclic code of length \( n \) over \( R \). In other words, every shortened cyclic code over the finite chain ring is polycyclic.

Let \( C \subseteq R[x]/\langle f \rangle \) be a nonzero polycyclic code. Define

\[
\text{Ann}_{R_m}(C) = \{ g \in R[x]/\langle f \rangle : gc = 0 \text{ for all } c \in C \}.
\]

It is clear that \( \text{Ann}_{R_m}(C) \) is a \( R[x] \)-submodule of \( R_m \). We consider now the problem of determining the standard generating set for \( \text{Ann}_{R_m}(C) \).
Proposition 2.5. Let $C = \langle g \rangle$ be a polycyclic code with the generating set $G = \{\gamma^{j_0}g_0, \gamma^{j_1}g_1, \ldots, \gamma^{j_t}g_t\}$ over $R$, where $g = \gamma^{j_0}g_0 + \gamma^{j_1}g_1 + \ldots + \gamma^{j_t}g_t$. Then the set $H = \{\gamma^{j_0}h_0, \gamma^{j_1}h_1, \ldots, \gamma^{j_{t+1}}h_{t+1}\}$ forms a strong Gröbner basis of $\text{Ann}_{R_m}(C)$, where

(i) $b_i = s - j_{i+1} - i$ for all $i \in \{0, 1, \ldots, t + 1\}$. In particular, put $j_{t+1} = s$;
(ii) $h_i$ is monic with $h_i = f/g_{t-i}$ for $i \in \{0, 1, \ldots, t + 1\}$. In particular, put $g_{-1} = f$.

Proof. Consider an $R_m$-module homomorphism $\theta$ from $R_m$ onto $\langle g \rangle$ by:

$$a \mapsto ag,$$

for all $a \in R_m$.

For $0 \leq k \leq t$ and $0 \leq r \leq t + 1$, if $j_k + b_r \geq s$, we have $\gamma^{j_k+b_r}g_th_r = 0$ since $\gamma^s = 0$; if $j_k + b_r < s$, i.e., $j_k \leq j_{t+1-r} - 1$ from condition (i), then we have $k \leq t - r$, so $g_{t-r}g_k$. Thus, we have

$$\gamma^{j_k}g_k\gamma^{b_r}h_r = \gamma^{j_k+b_r}g_k \frac{f}{g_{t-r}} = 0,$$

which implies that $\langle h \rangle \subseteq \ker(\theta)$. On the other hand, by the first isomorphism theorem we have $R_m/\ker(\theta) \cong \langle g \rangle$. Then by a simple calculation from Remark 2.3 yields $|\langle h \rangle| = |\ker(\theta)|$. Consequently, $\langle h \rangle = \ker(\theta) = \text{Ann}_{R_m}(C)$.

2.3 Quasi-sequential codes

Define linear functions $\sigma_i: R^m \to R$ for $1 \leq i \leq \ell$. Let $C$ be a linear code of length $m\ell$ over $R$. Then $C$ is called quasi-sequential if for any $(c_1, c_2, \ldots, c_{\ell}) \in C$, we have $(c'_1, c'_2, \ldots, c'_\ell) \in C$, where $c_i = (c_{i,0}, c_{i,1}, \ldots, c_{i,m-1}) \in R^m$, and $c'_i = (c_{1,i}, \ldots, c_{i,m-1}, \sigma_i(c_i))$ with $1 \leq i \leq \ell$.

Let $C$ be a quasi-sequential code with associate vector $(w_1, w_2, \ldots, w_{\ell})$, where $w_i = (w_{i,0}, w_{i,1}, \ldots, w_{i,m-1})$ with $w_{i,0} \in R \setminus M$ and $1 \leq i \leq \ell$. Similar to the argument in [3], the code $C$ is invariant under right multiplication by the matrix $M = \text{diag}(M_1, M_2, \ldots, M_{\ell})$, and for $1 \leq i \leq \ell$, the $m \times m$ matrix $M_i$ is of the form:

$$M_i = \begin{pmatrix}
0 & 0 & \cdots & 0 & w_{i,0} \\
1 & 0 & \cdots & 0 & w_{i,1} \\
0 & 1 & \cdots & 0 & w_{i,2} \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & 1 & w_{i,m-1}
\end{pmatrix}.$$

It is easy to see that quasi-sequential codes are a natural generalization of quasi-cyclic codes and even of quasi-twisted codes. In fact, sequential codes, quasi-sequential codes with $\ell = 1$, were first introduced by Hou et al. [33] in 2009s, these codes are interesting for code constructions: they can be viewed as a source in obtaining good (even optimal) codes.
3  Algebraic structure of 1-generator QP codes

An \( r \)-generator QP code is a \( R[x] \)-submodule of \( R \) generators. In this section, we only consider 1-generator QP codes over \( R \). Assume that \( C \) is a 1-generator QP code generated by \((F_1, F_2, \ldots, F_\ell) \in \mathcal{R}_m \), then \( C \) is of the form:

\[
C = \{(gF_1, gF_2, \ldots, gF_\ell) : g \in \mathcal{R}_m \}.
\]

Then we define

\[
\text{Ann}_{\mathcal{R}_m}(C) = \{g \in \mathcal{R}_m : gF_i = 0 \text{ for all } 1 \leq i \leq \ell \}.
\]

It is also clear that \( \text{Ann}_{\mathcal{R}_m}(C) \) is a \( R[x] \)-submodule of \( \mathcal{R}_m \). According to Theorem 2.2, there exists a strong Gröbner basis \( \{\gamma_{k_0}h_0', \gamma_{k_1}h_1', \ldots, \gamma_{k_{r+1}}h_{r+1}'\} \) such that \( \text{Ann}_{\mathcal{R}_m}(C) = \langle h' \rangle \), where

\[
h' = \gamma_{k_0}h_0' + \gamma_{k_1}h_1' + \cdots + \gamma_{k_{r+1}}h_{r+1}'.
\]

We call \( h' \) a parity check polynomial in standard form of the 1-generator QP code \( C \).

For \( 1 \leq i \leq \ell \), the projection of \( \mathcal{R}_m^\ell \) on \( \mathcal{R}_m \) according to its \( i \)-th component is the mapping \( \phi_i : \mathcal{R}_m^\ell \rightarrow \mathcal{R}_m \) by \((a_1, a_2, \ldots, a_\ell) \rightarrow a_i\). Then we have the following proposition.

**Proposition 3.1.** Let \( C \) be a 1-generator QP code with the generator \( G = (F_1, F_2, \ldots, F_\ell) \in \mathcal{R}_m^\ell \). Then \( F_i \in C_i = \phi_i(C) \), where \( C_i \) is a polycyclic code of length \( m \) over \( R \). Furthermore, \( \text{Ann}_{\mathcal{R}_m}(C) \) is a \( R[x] \)-submodule of \( \text{Ann}_{\mathcal{R}_m}(C_i) \) for \( 1 \leq i \leq \ell \).

**Proof.** Following the projection map defined above, it is easy to check that the code \( \phi_i(C) \) is polycyclic over \( R \). Therefore, the remainder of the argument follows from the fact that \( \text{Ann}_{\mathcal{R}_m}(C_i) \) is also a \( R[x] \)-submodule of \( \mathcal{R}_m \). \( \square \)

Next, we give a characterization of the parity check polynomial by using the strong Gröbner basis with respect to the ideal generated by \( F_1, F_2, \ldots, F_\ell \). Suppose that \( \tilde{C} = \langle F_1, F_2, \ldots, F_\ell \rangle \) with the strong Gröbner basis \( \{\gamma^{a_0}f_0, \gamma^{a_1}f_1, \ldots, \gamma^{a_r}f_r\} \). Then the exact form of \( h' \) is shown by the following result.

**Proposition 3.2.** Keep the above notation. Then \( \{\gamma_{k_0}h_0', \gamma_{k_1}h_1', \ldots, \gamma_{k_{r+1}}h_{r+1}'\} \) forms a strong Gröbner basis for \( \text{Ann}_{\mathcal{R}_m}(C) \), where

\[
\begin{align*}
(i) \ & k_i = s - a_{r+1 - i} \text{ for all } i \in \{0, 1, \ldots, r + 1\}. \text{ In particular, put } a_{r+1} = s; \\
(ii) \ & h'_i \text{ is monic with } h'_i = f/f_{r-i} \text{ for } i \in \{0, 1, \ldots, r + 1\}. \text{ In particular, put } f_{-1} = f.
\end{align*}
\]

**Proof.** The result follows from \( \text{Ann}_{\mathcal{R}_m}(C) = \text{Ann}_{\mathcal{R}_m}(\tilde{C}) \) and Proposition 2.5. \( \square \)

Before the start of studying the minimal generating set of the QP code as \( R \)-module, we first introduce the following lemma.
Lemma 3.3. Let $C$ be a 1-generator QP code over $R$ with generator $G = (F_1, F_2, \ldots, F_\ell) \in \mathcal{R}_m$. Then $F_i$ can be selected to be of the form $F_i = f_{i,0} + \gamma f_{i,1} + \cdots + \gamma^{s-1} f_{i,s-1}$, where $f_{i,j}$’s are monic or 0 in $R[x]$ with $1 \leq i \leq \ell$ and $0 \leq j \leq s - 1$.

Proof. From Proposition 3.1 it is easy to check that $F_i \in C_i$, where $C_i$ is a polycyclic code over $R$. By Theorem 2.2, there exist polynomials $g_{i,0}, g_{i,1}, \ldots, g_{i,t} \in R[x]$ such that

$$C_i = \langle \gamma^{j_i,0} g_{i,0} + \gamma^{j_i,1} g_{i,1} + \cdots + \gamma^{j_i,t} g_{i,t} \rangle.$$

Since $F_i \in C_i$, there exists a polynomial $f_i \in R[x]$ such that

$$F_i = f_i(\gamma^{j_i,0} g_{i,0} + \gamma^{j_i,1} g_{i,1} + \cdots + \gamma^{j_i,t} g_{i,t}) = f_{i,0} + \gamma f_{i,1} + \cdots + \gamma^{s-1} f_{i,s-1},$$

where $f_{i,j}$’s are monic polynomials in $R[x]$ for all $1 \leq i \leq \ell$ and $0 \leq j \leq s - 1$. In particular, let $f_{i,j} = 0$ (or $f$) if there is no term of $\gamma^j$ in $F_i$. \qed

Example 3.4. Let $R = \mathbb{Z}_8$, $f = (x + 3)(x^2 + x + 1)(x^4 + 2x^2 + 3x + 1)$, and

$$F_1 = 2x^3((x + 3)(x^4 + 2x^2 + 3x + 1) + 2(x^4 + 2x^2 + 3x + 1) + 4) \
\equiv 2x^5 + 2x^4 + 4x^3 + 2x^2 + 2 \quad (\text{mod } f),$$

where $f_1 = 2x^3, g_{1,0} = (x + 3)(x^4 + 2x^2 + 3x + 1), g_{1,1} = x^4 + 2x^2 + 3x + 1, g_{1,2} = 1$. Then we can choose $f_{1,0} = 0, f_{1,1} = x^5 + x^4 + x^2 + 1, f_{1,2} = x^3$ such that

$$F_1 = f_{1,0} + 2f_{1,1} + 4f_{1,2},$$

where $f_{1,j}$ are monic or 0 with $0 \leq j \leq 2$.

For each $1 \leq j \leq s - 1$, let

$$h^{(j)} = \frac{f}{\gcd(f_{1,j} \prod_{e=0}^{j-1} h^{(e)}), f_{2,j} \prod_{e=0}^{j-1} h^{(e)}, \ldots, f_{\ell,j} \prod_{e=0}^{j-1} h^{(e)}, f)} \quad \text{and} \quad \gcd(f_{1,0}, f_{2,0}, \ldots, f_{\ell,0}, f),$$

where $\deg(h^{(j)}) = r_j$. In particular, if $j = 0$, let

$$h^{(0)} = \frac{f}{\gcd(f_{1,0}, f_{2,0}, \ldots, f_{\ell,0}, f)},$$

where $\deg(h^{(0)}) = r_0$. It should be noted that the expression of $f_{i,j}$ is not necessary unique, but the degree of $h^{(j)}$ is unique. Then the following theorem gives the minimal generating set for a 1-generator QP code $C$ as an $R$-module.
Theorem 3.5. Keep the above notation. Suppose that $\sum_{e=0}^{s-1} \gamma^e f_{i,e}$ is not a zero divisor for $1 \leq i \leq \ell$. Let

\[
G_0 = \{ G, xG, \ldots, x^{r_0-1}G \},
\]

\[
B_i = \left( \sum_{e=i}^{s-1} \gamma^e f_{j,e} \prod_{r=0}^{\ell} h^{(r)} \right), \quad 1 \leq i \leq s-1,
\]

\[
S_i = \{ B_i, xB_i, \ldots, x^{r_i-1}B_i \}, \quad 1 \leq i \leq s-1.
\]

Then $G_0 \bigcup_{i=1}^{s-1} S_i$ forms a minimal generating set for $C$ as an $R$-module. In addition, the 1-generator QP code $C$ has $|F|^\sum_{i=0}^{s-1} (s-i)r_i$ codewords.

Proof. Let $c = kG$ be a codeword in $C$ with $k \in R[x]$. Recall the Division Algorithm, there exist two unique polynomials $p_1$ and $q_1$ such that $k = p_1 h^{(0)} + q_1$, where $\deg(q_1) < r_0$ or $q_1 = 0$. Thus we have

\[
c = kG = (p_1 h^{(0)} + q_1)G = p_1 h^{(0)} \left( \sum_{i=0}^{s-1} \gamma^i f_{1,i}, \ldots, \sum_{i=0}^{s-1} \gamma^i f_{\ell,i} \right) + q_1 G.
\]

Note that $q_1 G \in \text{Span}(G_0)$. For $1 \leq i \leq s - 1$, there exist unique $p_{i+1}$ and $q_{i+1}$ such that $p_i = p_{i+1} h^{(i)} + q_{i+1}$ with $\deg(q_{i+1}) < r_i$ from the Division Algorithm. Then we continue the steps above, it is easy to check that $c \in \text{Span}(G_0) \bigcup_{i=1}^{s-1} \text{Span}(S_i)$.

Therefore, it remains to show that $\text{Span}(G_0), \text{Span}(S_1), \ldots, \text{Span}(S_{s-1})$ are pairwise disjoint. We just give a partial proof here, that is, $\text{Span}(G_0) \cap \text{Span}(S_1) = \{0\}$, and a similar argument for the rest of the cases. Let $Q = (Q_1, Q_2, \ldots, Q_\ell) \in \text{Span}(G_0) \cap \text{Span}(S_1)$. Then there are $u, v \in R[x]$ such that

\[
Q_i = \sum_{e=0}^{s-1} \gamma^e f_{i,e} u, \quad \text{where } \deg(u) < r_0, \ 1 \leq i \leq \ell,
\]  

(1)

\[
Q_i = \sum_{e=1}^{s-1} \gamma^e f_{i,e} h^{(0)} v, \quad \text{where } \deg(v) < r_1, \ 1 \leq i \leq \ell.
\]  

(2)

Therefore, Eqns. (1) and (2) imply that $\sum_{e=0}^{s-1} \gamma^e f_{i,e} (u - h^{(0)} v) = 0$ due to $h^{(0)} f_{i,0} = 0$. Since $\sum_{e=0}^{s-1} \gamma^e f_{i,e} v$ is not a zero divisor for $1 \leq i \leq \ell$, we have $u = h^{(0)} v$. On the other hand, it is easy to check the coefficients of $u$ belong to $\langle \gamma^{j_1-j_0} \rangle$ since $\gamma^{s-j_1} Q_i = 0$ from Eq. (2). The discussion above implies that $u = v = 0$, which completes the proof.\[\square\]
4 Duality

Define the dual of the QP code $C$ of length $m\ell$ over $R$ by

$$C^\perp = \{x \in R^{m\ell} : x \cdot y = 0 \text{ for all } y \in C\}.$$

In general the linear code $C^\perp$ is not quasi-polycyclic. Then an alternate duality introduced in [2, 10] on $R_m$ is necessary. Let $g, h \in R_m$ with degree less than $m$, define

$$\langle g, h \rangle_f = gh(0).$$

From now on, let $C$ be a QP code of length $n = m\ell$ with index $\ell$ over $R$. Then we define the annihilator dual $C^0$ of $C$ by the formula

$$C^0 = \{g \in R_\ell^m : \langle g, h \rangle_f = \sum_{i=1}^\ell \langle g_i, h_i \rangle_f = 0 \text{ for all } h \in C\},$$

where $g = (g_1, g_2, \ldots, g_\ell)$ and $h = (h_1, h_2, \ldots, h_\ell) \in R_\ell^m$.

**Proposition 4.1.** Let $C$ be a $R[x]$-submodule of $R_\ell^m$, that is, a QP code of length $n = m\ell$ with index $\ell$ over $R$. Then $C^0$ is also a $R[x]$-submodule of $R_\ell^m$.

**Proof.** Let $\lambda \in R[x]$ with degree less than $m$. Suppose that $u \in C$ and $v \in C^0$. Notice that $\langle u, v \rangle_f = 0$, we have

$$\langle u, \lambda v \rangle_f = \lambda(0)\langle u, v \rangle_f = 0.$$

This implies that $\lambda v \in C^0$. Thus, $C^0$ is a $R[x]$-submodule of $R_\ell^m$, i.e., a QP code of length $m\ell$ with index $\ell$ over $R$. \qed

**Remark 4.2.** Let $f = x^m - c(x)$ with $c(x) = c_0 + c_1 x + \cdots + c_{m-1} x^{m-1} \in R[x]$ and $c_0 \in R \setminus M$. It is easy to check that the inner product $\langle \cdot, \cdot \rangle_f$ on $R_\ell^m$ is a nondegenerate bilinear form from a similar argument in [2, Lemma 3.1] (see also [17, Lemma 3]). Moreover, if $\ell = 1$, i.e., $C$ is a polycyclic code over $R$, then we have $C^0 = \text{Ann}_{R_m}(C)$.

However, since the dual of a QP code is not quasi-polycyclic in general, there is a mathematical interest of the connection between the quasi-polycyclic code $C$ and its dual which is quasi-sequential.

**Theorem 4.3.** Let $C$ be a linear code over $R$. Then $C$ is quasi-polycyclic if and only if $C^\perp$ is quasi-sequential with the same associate vector in each component.

**Proof.** Let $H$ be the parity check matrix of $C$, this yields $CH^T = 0$. If $C$ is quasi-polycyclic, we can choose $M_i = D^T$ for $1 \leq i \leq \ell$, that is, $M = \bar{D}^T$. Then we have

$$C\bar{D}HT = C(H\bar{D}^T)^T = C( HM)^T = 0.$$

Therefore, the dual code $C^\perp$ is invariant under right multiplication by the matrix $M$. \qed
5 New $\mathbb{Z}_4$-linear codes from 1-generator QP codes

In this section, we present some examples of 1-generator QP codes with indexes 2 and 3 over $\mathbb{Z}_4$ by using the computer algebra system Magma [34]. These quaternary codes have better parameters than the ones in [26]. For this purpose, we limit our search scope to the case of free codes. The following corollary gives a characterization for a quaternary 1-generator QP code with index $\ell$ to be free.

**Corollary 5.1.** Let $C$ be a 1-generator QP code with the generator $G = (f_{1,0}, f_{2,0}, \ldots, f_{\ell,0})$ over $\mathbb{Z}_4$. If $f_{i,0}$ is not a zero divisor for all $1 \leq i \leq \ell$, then $C$ is a free QP code with $4^r$ codewords, where $r = \deg(h^{(0)})$, and

$$h^{(0)} = \frac{f}{\gcd(f_{1,0}, f_{2,0}, \ldots, f_{\ell,0}, f)}.$$

**Proof.** According to Theorem 5.5, if $f_{i,0}$ is not a zero divisor for all $1 \leq i \leq \ell$, then $h^{(0)} = f$ and $B_1 = 0$. Therefore, the code $C$ is a free quaternary QP code of size $4^r$ with the minimal generating set $\{G, xG, \ldots, x^{r-1}G\}$. $\square$

We are now in a position to present some computational examples of new $\mathbb{Z}_4$-linear codes from 1-generator QP codes with indexes two and three in Table 1 and Table 2, respectively.

For convenience, we write the coefficients of the generator polynomials of QP codes in decreasing order. For example, let $10^21321$ denote the polynomial $x^8 + x^5 + x^4 + x^3 + 3x^2 + 2x + 1$. The linear codes in Tables 1 and 2 all have better parameters than the best known $\mathbb{Z}_4$-linear codes [26], i.e., these codes have larger minimum Lee distance than the ones in [26] with given length and code size. In particular, there are some linear codes in the tables that have the same minimum Lee distance with the best known nonlinear codes. For example, let $f = 102013$ in Table 1 and $f = 12^20122$ in Table 2, then the linear codes with the parameters $(10, 4^2, 10)$ and $(18, 4^2, 18)$ are the same as the best known quaternary nonlinear codes [26].

On the other hand, in Table 1, the symbol “*” denotes the obtained linear codes which have bigger code size than the best known $\mathbb{Z}_4$-linear codes [26] with given code length and minimum Lee distance. For example, in Table 1, for $f = 12^201^22$ and $1210210213$, the codes of length 12 and 18 with minimum Lee distances both 9, have sizes $4^3$ and $4^6$, respectively, while the codes in [26] only have sizes $4^2$ and $4^32$, respectively.

Note that Table 1 and Table 2 contain only very small values of the length $n$. One can continue to construct more interesting linear codes from Theorem 5.5 and Corollary 5.1 even for non-free case using Magma [34].
Table 1:
Some new quaternary linear codes constructed by 1-generator QP codes with index two.

| $f$            | $f_{1,0}$ | $f_{2,0}$ | Parameters |
|----------------|-----------|-----------|------------|
| 102013         | 101$^2$3  | 130102    | (10, 4$^2$, 10) |
| 102013         | 12$^2$1   | 1$^2$32$^2$ | (10, 4$^3$, 7) |
| 12$^2$01$^2$2  | 101$^2$3  | 13$^2$23   | (12, 4$^3$, 9)$^*$ |
| 102$^2$3231$^2$| 1302102   | 1$^2$0$^2$12 | (16, 4$^4$, 11) |
| 1013$^2$213$^2$1| 10323$^3$2 | 12101$^2$32$^2$ | (18, 4$^6$, 14) |
| 1210210213     | 1$^2$21$^2$3 | 1$^2$321   | (18, 4$^6$, 9)$^*$ |
| 12310$^2$3123231| 120$^2$1$^2$032 | 1020130102 | (24, 4$^5$, 16) |
| 1231$^2$021013$^2$| 1313$^2$021 | 1202$^2$101$^2$ | (24, 4$^6$, 14) |
| 1$^3$2030$^3$3121 | 12$^2$3$^2$2 | 10$^2$3$^2$1$^2$ | (24, 4$^7$, 12) |
| 120323131201$^2$ | 10$^3$3 | 13$^2$12$^2$ | (24, 4$^4$, 10) |
| 102$^1$032$^3$1213 | 12$^2$3$^2$2 | 10$^2$3$^2$1$^2$ | (26, 4$^4$, 11) |
| 102$^2$13$^2$10312$^2$31 | 1$^2$0$^2$31$^2$23012 | 13023$^2$1212302 | (28, 4$^4$, 22) |

Table 2:
Some new quaternary linear codes constructed by 1-generator QP codes with index three.

| $f$            | $f_{1,0}$ | $f_{2,0}$ | $f_{3,0}$ | Parameters |
|----------------|-----------|-----------|-----------|------------|
| 102013         | 12$^2$1   | 13$^2$2   | 1$^2$32$^2$ | (15, 4$^4$, 12) |
| 12$^2$01$^2$2  | 121312    | 1$^3$0232 | 1$^3$032   | (18, 4$^2$, 18) |
| 12$^2$01$^2$2  | 101$^2$3  | 13$^2$2$^2$3 | 1323       | (18, 4$^3$, 15) |
| 12$^2$32$^2$3$^3$1 | 13132132$^2$ | 1$^3$32312 | 1202$^2$101$^2$ | (27, 4$^3$, 24) |
| 1$^2$321023$^3$ | 121$^4$2$^2$ | 10$^3$1$^2$2 | 12313$^2$0  | (27, 4$^4$, 20) |
| 10310$^2$1301  | 1302102   | 1$^2$0$^2$12 | 132010     | (27, 4$^5$, 17) |
| 1$^2$301$^2$23$^2$1$^2$ | 12302302 | 1012032   | 1$^2$3$^2$31 | (30, 4$^4$, 21) |
| 10201201231    | 10$^2$312$^2$ | 12$^3$3$^2$2 | 1$^2$2101   | (30, 4$^5$, 18) |
| 1$^2$2310102$^2$1 | 130102  | 1$^2$032   | 1231$^2$    | (30, 4$^7$, 16) |
| 1021$^2$31$^3$23 | 12101$^2$32$^2$ | 10$^3$23$^3$2 | 12301$^2$3  | (33, 4$^5$, 22) |
| 123$^2$3$^2$1213 | 10232102  | 1203032   | 1$^2$031$^2$3 | (33, 4$^5$, 20) |
| 12$^2$3$^2$1$^3$3$^2$3 | 10$^2$312$^2$ | 12$^3$2$^2$ | 102310     | (33, 4$^7$, 18) |
| 1231$^2$0210131$^2$ | 1313$^2$021 | 132120121 | 1202$^2$101$^2$ | (36, 4$^4$, 24) |
| 123$^2$30$^2$101323 | 1$^3$2$^2$30$^1$3$^2$ | 1$^2$302323$^2$12$^2$ | 1$^3$203213$^2$0  | (39, 4$^4$, 29) |
| 1210$^2$3012023$^3$ | 1$^2$3$^2$10$^2$12 | 10$^2$3$^1$2012 | 1023132010 | (39, 4$^5$, 27) |
6 Conclusion

In this paper, we generalize some previous studies on 1-generator quasi-cyclic codes over the finite fields to finite chain ring. Using the Gröbner basis theory, we determine their minimal generating sets and their parity check polynomials. Moreover, we have constructed some $\mathbb{Z}_4$-linear codes with parameters better than the best known $\mathbb{Z}_4$-linear codes [26]. Unlike the quasi-cyclic codes, for a positive integer $m$, we can choose different $f \in R[x]$ with $\text{deg}(f) = m$ and $\bar{f}$ square free, not only $f = x^m - 1$. Thus this extra flexibility is a suitable approach for constructing codes with good parameters over finite chain rings by using the Gray map or codes over finite fields.

In the future work, the problem of characterization of the self-annihilator quasi-polycyclic codes over $R$ with the inner product defined in Section 4 is open, and it might be easier to start with the 1-generator case. Another topic is to see if the results in this paper can be extended to more general cases, for example, the quasi-polycyclic codes with $r (\geq 2)$ generators.

Acknowledgement: The authors would like to thank the anonymous referees for their careful checking and helpful suggestions which have improved the manuscript. The authors are also grateful to the Assoc. Prof. Edgar Martínez-Moro for helpful discussions.

References

[1] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, IEEE Trans. Inform. Theory, 1994, 40(2):301–319.
[2] A. Alahmadi, S. Dougherty, A. Leroy, P. Solé, On the duality and the direction of polycyclic codes, Adv. Math. Commun., 2016, 10(4):921–929.
[3] S.R. López-Permouth, B.R. Parra-Avila, S. Szabo, Dual generalizations of the concept of cyclicity of codes, Adv. Math. Commun., 2009, 3(3):227–234.
[4] Y. Cao, 1-generator quasi-cyclic codes over finite chain rings, AAECC, 2013, 24(1):53–72.
[5] J. Conan, C. Séguin, Structural properties and enumeration of quasi-cyclic codes, AAECC, 1993, 4(1):25–39.
[6] J. Gao, L. Shen, F.-W. Fu, Bounds on quasi-cyclic codes over finite chain rings, J. Appl. Math. Comput., 2016, 50(1):577–587.
[7] J. Gao, L. Shen, A class of 1-generator quasi-cyclic codes over finite chain rings, Int. J. Comput. Math., 2016, 93(1):40–54.
[8] S. Ling, P. Solé, On the algebraic structure of quasi-cyclic codes II: chain rings, Des. Codes Cryptogr., 2003, 30(1):113–130.

[9] S. Ling, P. Solé, Good self-dual quasi-cyclic codes exist, IEEE Trans. Inform. Theory, 2003, 49(4):1052–1053.

[10] A. Fotue-Tabue, E. Martínez-Moro, J.T. Blackford, On polycyclic codes over a finite chain ring, Adv. Math. Commun., 2020, 14(3):455–466.

[11] S.R. López-Permooth, H. Özadam, F. Özbudak, S. Szabo, Polycyclic codes over Galois rings with applications to repeated-root constacyclic codes, Finite Fields Appl., 2013, 19(1):16–38.

[12] R. Wu, M. Shi, On $\mathbb{Z}_2\mathbb{Z}_4$-additive polycyclic codes and their Gray images, Des. Codes Cryptogr., 2021, doi: 10.1007/s10623-021-00917-0.

[13] G.F.M. Beenker, On double circulant codes, Rep. 80-WSK-04, Dep. Math., Technol. Univ. Eindhoven, The Netherlands, 1980.

[14] M. Shi, L. Qian, P. Solé, On self-dual negacirculant codes of index two and four, Des. Codes Cryptogr., 2018, 86(11):2485–2494.

[15] M. Shi, H. Zhu, L. Qian, L. Sok, P. Solé, On self-dual and LCD double circulant and double negacirculant codes over $\mathbb{F}_q + u\mathbb{F}_q$, Cryptogr. Commun., 2020, 12(1):53–70.

[16] M. Shi, L. Xu, P. Solé, Construction of isodual codes from polycirculant matrices, Des. Codes Cryptogr., 2020, 88(12):2547–2560.

[17] T.A. Gulliver, Optimal double circulant self-dual codes over $\mathbb{F}_4$, IEEE Trans. Inform. Theory, 2000, 46(1):271–274.

[18] A. Alahmadi, F. Ödemir, P. Solé, On self-dual double circulant codes, Des. Codes Cryptogr., 2018, 86(6):1257–1265.

[19] D. Huang, M. Shi, P. Solé, Double circulant self-dual and LCD codes over $\mathbb{Z}_{q^2}$, Int. J. Found. Comput. S., 2019, 30(3):407–416.

[20] M. Shi, D. Huang, L. Sok, P. Solé, Double circulant LCD codes over $\mathbb{Z}_4$, Finite Fields Appl., 34 (2019):133–144.

[21] M. Shi, L. Qian, L. Sok, N. Aydin, P. Solé, On constacyclic codes over $\mathbb{Z}_4[u]/\langle u^2 - 1 \rangle$ and their Gray images, Finite Fields Appl., 45 (2017):86–95.

[22] Y. Gao, J. Gao, T. Wu, F.-W. Fu, 1-generator quasi-cyclic and generalized quasi-cyclic codes over the ring $\mathbb{Z}_4[u]/\langle u^2 - 1 \rangle$, AAECC, 2017, 28(6):457–467.

[23] R. Bandi, M. Bhaintwal, N. Aydin, A mass formula for negacyclic codes of length $2^k$ and some good negacyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, Cryptogr. Commun., 2017, 9(2):241–272.

[24] M. Özen, F. Uzekmek, N. Aydin, Cyclic and some constacyclic codes over the ring $\mathbb{Z}_4[u]/\langle u^2 - 1 \rangle$, Finite Fields Appl., 38 (2016):27–39.
[25] T. Wu, J. Gao, F.-W. Fu, 1-generator generalized quasi-cyclic codes over $\mathbb{Z}_4$, Cryptogr. Commun., 2015, 9(2):291–299.

[26] N. Aydin, T. Asamov, The $\mathbb{Z}_4$ Database [Online]. Available: http://z4codes.info/, accessed on 28.08.2015.

[27] Y. Cao, Y. Cao, S. Dougherty, S. Ling, Construction and enumeration for self-dual cyclic codes over $\mathbb{Z}_4$ of oddly even length, Des. Codes Cryptogr., 2019, 87(10):2419–2446.

[28] G.H. Norton, A. Sălăgean, Strong Gröbner basis for polynomials over a principal ideal ring, Bull. Austral. Math. Soc., 2001, 64(3):505–528.

[29] A. Sălăgean, Repeated-root cyclic and negacyclic codes over a finite chain ring, Discrete Applied Math., 2006, 154(2):413–419.

[30] G.H. Norton, A. Sălăgean, Cyclic codes and minimal strong Gröbner basis over a principal ideal ring, Finite Fields Appl., 9 (2003):237–249.

[31] A.R. Calderbank, A.R. Sloane, Modular and $p$-adic codes, Des. Codes Cryptogr., 1995, 6(1):21–35.

[32] G.H. Norton, A. Sălăgean, On the structure of linear and cyclic codes over a finite chain ring, AAECC, 2000, 10(6):489–506.

[33] X. Hou, S. R. López-Permouh, B. Parra-Avila, Rational power series, sequential codes and periodicity of sequences, J. Pure Appl. Algebra, 2009, 213(6):1157–1169.

[34] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system I: the user language, J. Symbolic Comput., 24 (1997):235–265.